Fraunhofer VVS

Future Security
Security Research Conference

FRAUNHOFER GROUP FOR DEFENSE AND SECURITY VVS

SECURITY RESEARCH CONFERENCE 10TH FUTURE SECURITY

BERLIN, SEPTEMBER 15 – 17, 2015
PROCEEDINGS

Jürgen Beyerer, Andreas Meissner, Jürgen Geisler (Eds.)

FRAUNHOFER VERLAG

FRAUNHOFER VVS

SECURITY RESEARCH CONFERENCE 10TH FUTURE SECURITY

BERLIN, SEPTEMBER 15 – 17, 2015 PROCEEDINGS

Jürgen Beyerer, Andreas Meissner, Jürgen Geisler (Eds.)

PREFACE BY THE EDITORS:

CURRENT STATE-OF-THE-ART OF SECURITY RESEARCH AT FUTURE SECURITY 2015

Established in 2006 by the Fraunhofer Group for Defense and Security, the yearly Future Security Research Conference has become one of the world's main forums for security research.

2015 marks the 10th anniversary of Future Security. Having looked into a wide range of topical issues in the past years, this year's conference theme is "Free but secure", that is, in short: How can we ensure individual people and society as a whole are safe and secure, without abridging the freedom of the individual? When we selected the theme more than a year before the conference, we were confident that this was going to be of high relevance to the community. Watching recent public debate, we feel that we could not have made a better choice. Ensuring safety and security in a socio-economic and socio-technical context requires a holistic perspective to merge contributions from various disciplines.

More than ever, Future Security is an interdisciplinary, international exchange platform for scientists and experts from research, industry and authorities, and it provides direct insight into current security research projects. Submitted by authors from 16 countries, this year 56 papers have been accepted for oral presentation in 16 technical sessions, and 20 have been selected for poster presentation. We sincerely thank the 43 members of the international program committee for reviewing abstracts and papers and helping put together such an excellent program.

The proceedings comprise more than 500 pages of technical text documenting the high level of commitment of the security research community. Besides the printed proceedings, the conference proceedings are published by Fraunhofer e-prints via Open Access for further increasing their impact and accessibility (http://eprints.fraunhofer.de). Moreover, we have now secured a SCOPUS listing of the proceedings.

We thank the authors, keynote speakers, panelists and panel moderators, the conference attendees including representatives of end-users, SMEs, industry, ministries and research funding agencies, the respectable members of the program committee, the program and conference management teams and the Fraunhofer publishing house.

The Editors
Jürgen Beyerer (Conference Chair)
Andreas Meissner (Program Chair)
Jürgen Geisler (Program Chair)

PROGRAM COMMITTEE

Prof. Dr. Oliver Ambacher
Fraunhofer IAF

Dr. Richard Arning
SES Satellite Leasing Ltd

Prof. Dr. Jürgen Beyerer
Fraunhofer IOSB

Dr. Antje Bierwisch
Fraunhofer ISI

Gerhard Coors
Federal Ministry of Defence BMVg

Prof. Dr. Claudia Eckert
Fraunhofer AISEC

Prof. Dr. Peter Elsner
Fraunhofer ICT

Prof. Dr. Joachim Ender
Fraunhofer FHR

Dr. E. Anders Eriksson
FOI - Swedish Defence Research Agency

Achim Friedl
Federal Ministry of the Interior BMI

Dr. Ludwig Frühauf
German Police University

Dr. Jürgen Geisler
Fraunhofer IOSB

Prof. Dr. Hans-Joachim Grallert
Fraunhofer HHI

Dr. Matthias Grüne
Fraunhofer INT

Prof. Dr. Albert Heuberger
Fraunhofer IIS

Dietmar Hilke
Thales Germany

Dr. Rüdiger Klein
Fraunhofer IAIS

Andreas Könen
Federal Office for Information Security BSI

Rüdiger Koppe
Airbus Defence and Space

Dr. Horst Krause
Fraunhofer ICT

Prof. Dr. Dr. Michael Lauster
Fraunhofer INT

Dr. Tobias Leismann
Fraunhofer EMI

Khoen Liem
European Commission

Peter Löffler
Siemens Switzerland Ltd.

Prof. Dr. Peter Martini
Fraunhofer FKIE

Sadhbh McCarthy
Centre for Irish and European Security CIES

Dr. Andreas Meissner
Fraunhofer IOSB

Dr. Karsten Michael
Federal Office of Civil Protection and Disaster Assistance BBK

Prof. Dr. Jörn Müller-Quade
Karlsruhe Institute of Technology KIT

Dr. Harald Olschok
Association of German Private Security Industry (BDSW)

Prof. Dr. Stefan Pickl
University of the German Federal Armed Forces - UBw Munich

Dr. Wolfgang Rosenstock
Fraunhofer INT

Prof. Dr. Christopher Schlick
Fraunhofer FKIE

Prof. Dr. Viola Schmid
TU Darmstadt

Gunther Schwarz
BDSV, Airbus Defence & Space

Dr. Michael Suhrke
Fraunhofer INT

Prof. Dr. Klaus Thoma
Fraunhofer EMI

Thomas Tschersich
Deutsche Telekom AG

Prof. Dr. Markus Ullmann
Federal Office for Information Security BSI

Dr. Marcel van Berlo
TNO

Norbert Weber
Federal Ministry of Defence BMVg

Dr. Karin Wey
VDI Technologiezentrum GmbH

TABLE OF CONTENTS

PROCEEDINGS

Session 5: Sensors and Sensor Data Exploitation 1: Laser and Optical Image Analysis

Session 6: Crisis Management

Session 7: Privacy Concerns and Legal Aspects

TABLE OF CONTENTS

TABLE OF CONTENTS

INTER-ORGANISATIONAL COOPERATION FOR THE PROFESSIONAL INTEGRATION OF VOLUNTEERS IN CRISIS MANAGEMENT

Jana Mauthner[1], Karin Hamann[2], Wolf Engelbach[3]

[1] *jana.mauthner@iao.fraunhofer.de*
University of Stuttgart, Institute for Human Factors and Technology Management (IAT) / Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart (Germany)

[2]*karin.hamann@iao.fraunhofer.de.*
Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart (Germany)

[3]*wolf.engelbach@iao.fraunhofer.de.*
Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart (Germany)

Abstract

In crisis situations volunteers provide support. In many countries well established is their affiliation to crisis management organisations, but in addition unaffiliated, spontaneous volunteers are coming on site and offer their help. Facing a continuous declining willingness of volunteers to get involved for a long period, as observed for some time in Germany, improving volunteer management in crisis response is considered crucial when addressing crisis management as a whole [13]. Also the corporate sector plays an increasingly important role in volunteer management by supporting crisis management with financial, material and personnel resources. This role includes both, the corporate social responsibility aspects of companies being civil society actors, and more specifically the role of companies being employers of privately engaged volunteers. There is a suggestion for improved inter-organisational cooperation, starting from specific projects, with synergetic effects for the companies, the response organisations and the volunteers themselves [8].

Keywords: Inter-organisational cooperation, corporate volunteering, volunteer management, unaffiliated volunteers, spontaneous volunteers, affiliated volunteers, crisis management.

1 RECENT CHALLENGES FOR VOLUNTEER MANAGEMENT

Natural and man-made disasters, such as river floods or major earthquakes, where various organisations and participating actors need to work in close cooperation and joint action to respond to and reduce the impacts of crisis, have caused more severe impacts in the last years [15], [3]. At the same time cities and infrastructures become more dense and vulnerable to these disasters, due to the high technological development among others [11]. These crisis situations pose new challenges not only for all actors involved in crisis management (policy makers, crisis management organisations and authorities, etc.), but also for civil societal actors, the private sector and especially the affected population [16].

The German crisis management system mainly relies on citizens as volunteers who are willing provide their help in response to disasters within fire brigades and rescue organisations. However, in the last years the formal and enduring (affiliated) membership in voluntary crisis management organisations is constantly decreasing because of demographic change and the dynamic of people's urban lifestyles [7]. Because of this as well as the emergence of new types of volunteerism, the German

crisis management organisations, such as Red Cross, and also emergency services such as fire-brigades, police, etc., are looking for new ways and strategies in view of membership recruitment, coordination and integration of volunteers according to their individual specific competencies and living situation [4]. Such new approaches also imply an adaptation of organisational structures to make volunteering more attractive and crisis response effective.

In this context it is emphasised that also the corporate sector plays an increasingly important role in crisis management. This particularly includes the support of engagement by volunteering programs as a part of corporate social responsibility strategies. Corporate Social Responsibility (CSR) is a key term coming from the area of business ethics, dealing with various methods how to contribute to societal sustainability and responsibility from perspective of a company. The term often comprises concepts such as Corporate Governance, Sustainability Management, or Corporate Citizenship through to Corporate Volunteering (CV). Corporate Volunteering means that companies support their employees in voluntary commitment for societal benefit[1]. Reasons for this kind of companies' engagement include extrinsic motivation such as strengthening the reputation towards clients, and increasing the attractiveness for potential staff as well as intrinsic motivation such as taking over social responsibility and contributing own resources for maintaining a stable environment. Furthermore, the majority of companies agree that volunteers bring an added value for the team spirit and a high sense of responsibility into their business work [8].

In addition, crisis management organisations can benefit from technical or medical experts and expertise from companies. Business models and regulations for the integration of volunteer work can support successful response during disasters. This topic has been addressed in the German security research project INKA (professional integration of volunteers in crisis management).

Within the framework of INKA the focus is on a detailed analysis of volunteer management, volunteer types and inter-organisational cooperation between crisis management organisations, governmental authorities and the private sector. The project INKA combines three complementary perspectives (see Fig. 1):

- the motivation of volunteers,
- the organisational structures of crisis management institutions and
- the private sector, especially companies.

This paper is mainly devoted to study the cooperation between companies and crisis management organisations. It focuses in particular on the following questions:

- How can crisis management organisations and companies support the integration of different types of volunteers?
- To what extend can companies and crisis management organisations cooperate in membership recruitment, retention and volunteer management in general?
- What are the future needs for an effective and efficient inter-organisational cooperation in volunteer management?

We conducted interviews and several workshops with experts from fire departments, Malteser Germany, Johanniter-Unfall-Hilfe (JUH), Arbeiter-Samariter-Bund (ASB), German Red Cross (DRK), the German Life Saving Association (DLRG), the Federal Agency for Technical Relief (THW), the Ministry of the Interior and members of the parliament. In regard of the business perspective a survey was conducted with the central question 'Promotion of volunteer involvement as an important task in society –

[1] http://wirtschaftslexikon.gabler.de/Definition/corporate-social-responsibility.html

what do companies think?'. For this purpose personnel managers of companies from various sectors were addressed to give their opinion [10]. In addition workshops with company representatives and representatives of crisis management organisations have been arranged to push the direct exchange about concerns and ideas around inter-organisational cooperation.

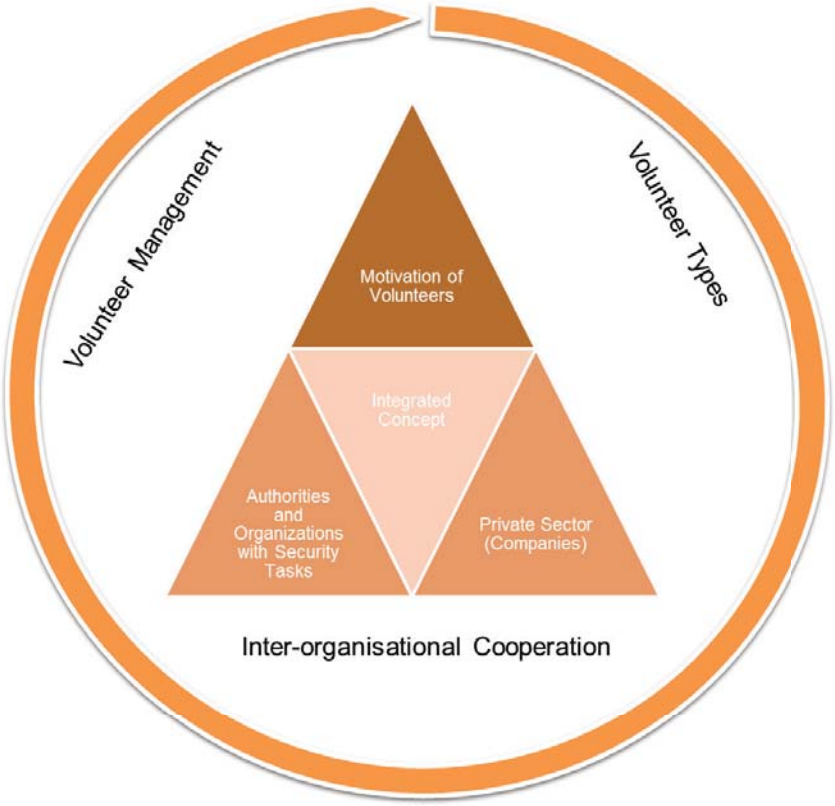


Figure 1 INKA Research Approach

The next chapters of the paper will focus on inter-organisational cooperation from both the perspective of crisis management organisations and the perspective of companies in the private sector. It will outline the main results achieved within INKA and in other projects in the domain of crisis management. Besides motivation, challenges and benefits, specific examples will expand the view on new innovative concepts for the cooperation between companies and crisis management organisations and authorities. Chapter three will shed light on the benefits, challenges and the (options of) synergies in inter-organisational cooperation.

2 INTERORGANISATIONAL COOPERATION IN CRISIS MANAGEMENT

Large scale and even small scale crisis events require the cooperation of a large variety of actors, ranging from civil protection agencies and first responder organisations' to companies and private persons. Longer term cooperation between companies and crisis management organisations allows the sharing of know-how and resources in order to develop solutions in view of constant societal challenges. Such an inter-organisational cooperation should typically be arranged around shared values of a company and the crisis management organisation. The better projects concerning volunteer management suit to the business field, to the values and to the products of a company, the more likely a high mutual benefit will arise from unique short projects as

well as from long-term cooperation agreements. Sustainable entrepreneurial commitment needs to be authentical [18]. Such partnerships will increase requirements for a systematic coordination and project management. This in turn will generate a joint understanding of companies in crisis management acting as an employer on the one hand and as a strategic partner on the other hand. Furthermore, the role of companies supporting their employees who can serve as volunteers will be concretised [8]. The following section will explore both, the role of crisis management organisations and the role of companies in inter-organisational cooperation processes.

2.1 The role of crisis management organisations in volunteer management

When disaster – natural or man-made – strikes a community, specific emergency management and nonprofit organisations automatically respond according to pre-established plans. Each of these designated organisations has a specific role to play in ensuring an effective response to and recovery from the crisis's devastation [6]. Crisis management activities are generally provided by a large variety of public and private institutions on different spatial levels in most European countries. Moreover, in some European countries, there is a strong interlinkage between professional and voluntary structures in crisis management [17]. Currently, especially German crisis management organisations are concerned about a lower willingness of volunteers to get involved in crisis management organisations and activities for a long period [4].

In Germany crisis management organisations are commissioned to handle crises and disasters. Preparation, response and recovery are typically arranged around existing concepts of volunteer management. These most often line out requirements for training of disaster competencies and conducting exercises. Thus, through crisis management organisations volunteers and their efforts are integrated and channelled to places needed. The emergence of new types and roles of volunteers and the lack of long term affiliated involvement of volunteers reinforced the need for new integrated volunteer management concepts [13],[17].

The results of the interview study, the survey with companies and the workshops conducted in the framework of the project INKA highlighted the importance of a thought-through communication and coordination between companies and crisis management organisations for an effective and efficient volunteer management. Companies can encourage their employees to serve as volunteers. One motivator is considering the competencies volunteers can gain from their engagement. The other way round, from perspective of the organisations, volunteers often bring professional competencies and qualifications into crisis response [12]. In order to support the cooperation with companies, crisis management organisations need to consider the following steps:

- Identify all potential partner companies in order to fathom cooperative relationships.
- Double-check and outline the organisation's profile and increase the visibility
- Generate awareness for crisis management activities by a flexible outreach strategy via Social Media, Public Relations Management, etc.
- Depict opportunities for involvement of volunteers by providing access to current information in volunteer recruitment. Utilize available Information and Communication Technologies (ICT), such as Web sites, data bases, listservs, Social Media, etc.
- Provide companies with concrete offers for common projects or cooperation, including information such as volunteer database access, screening, and other ongoing support.

- Ensure that companies and employees are aware of their opportunities and responsibilities by strengthening public relations work.
- Support the knowledge exchange of existing skills and qualifications by introducing or advancing mutual acknowledgement and certification systems.

All in all, improving the inter-organisational cooperation already previous to a crisis situation can bring new ways for crisis management organisations to counteract the decline in memberships. While only a minority of persons in companies are affiliated volunteers, almost any employee of a company could become an unaffiliated volunteer [5], [14].

For starting any kind of cooperation crisis management organisations need to find an adequate way to get into contact with companies. Therefore they ideally develop a concrete suggestion for joint projects when meeting the first time. Project ideas and suggestions need to be tailored to the concrete business field the company is working in and the core competencies of employees. Furthermore, crisis management organisations can offer organisation's specific expertise and competencies that can support the work of the companies (e.g. first aid certificates, expertise in safety, accident and critical infrastructure protection or similar) [5], [12].

2.2 The role of companies in crisis and volunteer management

Supporting volunteer engagement became a natural part of companies CSR-strategies. The Anglo-Saxon culture is said to contribute more strongly to general welfare and security as a tradition than most of European countries do. However, when looking at the heterogeneity how CSR is made manifest in different parts over the world according to historical, cultural and socio-economic factors, with regard to definitions and management concepts it becomes clear that 'one size does not fit all' [1]. In Germany there is the tendency that Corporate Volunteering (CV), which is considered as one elementary tool of Corporate Social Responsibility management, has gained in importance in favour of donations and monetary means in recent years [9]. The INKA project evinced crucial questions about how and in which way CSR activities can be implemented long-term in a sustainable and effective way. The first essential starting point is the integration in the business strategy. The more stable CSR activities are implemented in business strategies and the better they suit to the core business in an authentic way the higher is the chance to take advantage from added value as a company. The benefits range from improving the team spirit up to exploring new business segments.

A big potential for companies still to explore is in the area of Personnel Management [10]. Firstly, the attractiveness as an employer is possible to increase by supporting social engagement, by offering models for exemption, by offering concrete Corporate Volunteering projects to join or other means. Furthermore, CV projects can be used in the human resources development by combining social engagement with acquainting or strengthening social or technical competencies. Last but not least there is a growing trend for using Corporate Volunteering as a transition for employees starting their retirement. This is done for example by arranging suitable places to engage or by providing former staff members with insurance coverage for their activities.

However, except open potentials in personnel management and business development, another topic is becoming increasingly important for companies – this is how their stakeholders perceive and assess the companies' consequence in living ethical and social values, both, on a global and on a regional level [18]. Within the regional context many companies see the necessity for a contribution to societal and their own security not only by meeting standards on industrial safety and accident prevention regulated by law, but also by initiating proactive measures. Such measures may be awareness and information campaigns for own staff or flexible time models for joining

trainings at the volunteer fire brigade as an example. Supporting the local community thereby can result in new networks bringing new forms of cooperation as for example purchasing groups, sharing models for infrastructure up to rotation models for personnel in different companies.

In summary the study conducted within the INKA project has shown that:

- The meaning of Corporate Volunteering does increase, while financial commitment does decrease. Furthermore, corporate Volunteering is always connected to the time of individuals working in companies.
- There is a tendency towards competence-based Corporate Volunteering including Know-how transfer.
- New methods for personnel recruitment and personnel commitment will become more and more important to cope with demographic change and shortage of skilled labour.

This requires a clearly defined time management, competence management and personnel development strategies that are ideally coordinated with crisis management organisations. Such a systematic approach to volunteering can be supported by inter-organisational cooperation as a precondition for improving the situation of decreasing volunteers in organisations.

3 SYNERGIES OF INTER-ORGANISATIONAL COOPERATION BETWEEN COMPANIES AND ORGANISATIONS WITH SECURITY TASKS

Volunteering is a very valuable and relevant part of societies. Volunteers need to be anticipated, planned and managed regardless if they are affiliated with an established organisation or unaffiliated [2], [14].

A close cooperation and communication between crisis management organisations and companies can help to draw interest to and enhance the understanding of crisis management activities. This is the basis to identify and to create synergies. The previous chapters highlighted that crisis management organisations need to support the development of local networks in order to allow for flexible involvement of volunteers in times of continuing decline of affiliated, long term membership in crisis management organisations.

This cooperation is never and should be never a one way relationship with benefits for only one side. Moreover, companies that encourage their employees to serve as volunteers, considering competencies and qualifications, should also gain from volunteering and the professional competencies and qualifications their employees can refine in active crisis response and training. Many companies report that they benefit from social skills learned in crisis management training. Furthermore, attending trainings of crisis management organisations can help to decrease the number of work accidents because of the higher awareness of the volunteering employees for potential risks.

The analysis of the interviews and the workshops conducted in the framework of the INKA project has all in all shed light on the fact that an integrated volunteer management concept needs to:

- Analyse volunteer motivation, employer’s goals and organisational structures.
- Allow for discussion between crisis management organisations and companies.
- Consider the individual, strategic and economic goals of companies in an extended manner.
- Support collective learning.

- Develop integrated solutions and guidelines taking into account the different profiles of crisis management organisations and the specific conditions in companies.

4 CONCLUSION: TOWARDS A NEW MODE OF COOPERATION BETWEEN COMPANIES AND ORGANISATIONS WITH SECURITY TASKS IN VOLUNTEER MANAGEMENT

Effective and efficient volunteer management requires a detailed understanding of different roles, types of involvement, cooperation opportunities and permanent new challenges for modern crisis management, arising from technological changes, climate and demographic changes as well as turning intrinsic and extrinsic motivations for social engagement. The latter two are most often associated with different lifestyles [3].

For a better understanding of the involvement of volunteers in crisis management, the INKA project combined three complementary aspects in a detailed analysis in order to define integrated solutions: (1) The motivation of volunteers, which may be diverse and differ between affiliated and spontaneous volunteers. (2) The organisational structures of crisis management organisations that need to guide and manage affiliated and spontaneous volunteers and (3) the role companies can take in crisis and volunteer management.

This paper gives an insight in the results of the INKA studies on inter-organisational cooperation opportunities of crisis management organisations and companies. It draws attention to the finding that crisis management organisations need to support local cooperation networks with civil societal actors as well as companies to counteract the decline in memberships. Any means to strengthen the development of lasting win-win cooperation need to be explored, evaluated and constantly improved. Fundamental basis for this approach is for both, crisis management organisations and for companies, a high awareness of their own profile, values and aims.

The results of the project INKA shed further light on the high relevance of integrated cooperation concepts between governmental authorities, crisis management organisations and companies. The relevance is even growing due to changing society as well as changing environmental risks combined with new technical opportunities for crisis management.

REFERENCES

[1] Argandona, A., von Weltzein Hoivik, H. (2009). Corporate Social Responsibility: One size does not fit all. Collecting evidence from Europe. IESE Business School, University of Navarra. Working Paper 834.

[2] Australian Red Cross (2011). *Research report. A survey of spontaneous volunteers.* URL http://www.redcross.org.au/agencies.aspx (accessed 25.05.2015).

[3] BBK (2010). Neue Strategie zum Schutz der Bevölkerung in Deutschland. Wissenschaftsforum Band 4.

[4] BMI (2014).*Unterstützung des Ehrenamts im Bevölkerungsschutz.* URL http://www.bmi.bund.de/DE/Themen/Bevoelkerungsschutz/Ehrenamt/ehrenamt_node.html. (accessed 06.05.2015).

[5] DKKV (2015). Das Hochwasser 2013. Bewährungsprobe für das Hochwasserrisikomanagement in Deutschland. DKKV Schriftenreihe 53.

[6] DRK (2014). Die Rolle von ungebundenen HelferInnen bei der Bewältigung von Schadensereignissen. Teil 1. Schriften der Sicherheitsforschung. Band 1.

[7] GHK (2010). Volunteering in the European Union – Final Report. Studie im Auftrag der Generaldirektion Bildung und Kultur. URL http://ec.europa.eu/citizenship/pdf/doc1018_en.pdf (accessed 20.05.2015)

[8] Grant, A. M. (2012). Giving Time, Time After Time: Work Design and Sustained Employee Participation in Corporate Volunteering. ACAD MANAGE REV 37 (4), pp. 589-615. doi: 10.5465/amr.2010.0280

[9] Habisch A., Wegener, M. (2004). Gesetze und Anreizstrukturen für CSR in Deutschland. Praxisexpertise im Auftrag der Bertelsmann Stiftung, p.7.

[10] Hamann, K., Strittmatter, M. (2014). Unternehmerisches Engagement im Katastrophenschutz. Fraunhofer Verlag.

[11] Högl, J. (2013). Herausforderungen durch Krisen und Katastrophen. In: Neumayr, A., Schinnerl, A., Baubin, M. (eds.).Qualitätsmanagement im prähospitalen Notfallwesen. Bestandsaufnahme, Ziele und Herausforderungen, pp. 43-50.

[12] Kalisch, D., Engelbach, W., Hahn, C., Meyer, A. (2014). Integration von Freiwilligen in das Krisenmanagement. Herausforderungen und Ansätze für das Freiwilligenmanagement von Behörden und Organisationen mit Sicherheitsaufgaben (BOS).

[13] Kircher, F. (2014). Ungebundene Helfer im Katastrophenschutz. Die Sicht der Behörden und Organisationen mit Sicherheitsaufgaben. Deutsche Feuerwehr-Zeitung Brandschutz 8 (14), pp. 593-597.

[14] Lange, H.-J. (2012). Ehrenamt im Bevölkerungsschutz. Helfer vor neuen Herausforderungen in Zeiten des demographischen Wandels, knapper Finanzressourcen und zunehmender Schadensereignisse. URL http://www.inka-sicherheitsforschung.de/fileadmin/Daten/pdf-Downloads/Dokumentation_Symposium_Ehrenamt.pdf (accessed 31.05.2015).

[15] Merrill, M. (2006). Global trends and the challenges for volunteering. The International Journal of Volunteer Administration 24 (1), pp. 9-14.

[16] Perrow, C. (2007). *The Next Catastrophe*.

[17] Points of Light Foundation & Volunteer Center National Network (2006). Managing Spontaneous Volunteers in Times of Disaster: The Synergy of Structure and Good Intentions.

[18] Roy, P., Schiffelmann, T. (2014). CSR: Echter Erfolg durch soziales Engagement. Sonderdruck Unternehmer Edition. Know-how für den Mittelstand. p. 3.

Acknowledgements

The research leading to these results has received funding from national research ministry in Germany (BMBF) in the security research programme (FKZ 13N12195 and 13N12197). We thank the INKA project partners for fruitful discussions about concepts, solutions and approaches. The paper reflects only the authors' views, the BMBF and the Project are not liable for any use that may be made of the information contained therein.

CROWD TASKING – REALISING THE UNEXPLOITED POTENTIAL OF SPONTANEOUS VOLUNTEERS

Christian Flachberger[1], Georg Neubauer[2], Christoph Ruggenthaler[3], Gerald Czech[4]

[1] christian.flachberger@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria

[2] georg.neubauer@ait.ac.at
AIT Austrian Institute of Technology GmbH, 2444 Seibersdorf, Austria

[3] christoph.ruggenthaler@ait.ac.at
AIT Austrian Institute of Technology GmbH, 1220 Vienna, Austria

[4] gerald.czech@roteskreuz.at
Austrian Read Cross, Headquarters, 1040 Vienna, Austria

Abstract

Volunteers play an increasingly important role during disaster relief activities. In addition to pre-organised, well-trained volunteers, spontaneous volunteers appear at the scene. They are organising themselves rapidly, typically via social media. However, spontaneous volunteers are not managed within the command chains of the responder organisations. They may be seen as an unexploited additional resource, provided they are adequately guided and managed. This paper describes a new concept for the management of pre-registered spontaneous volunteers called “crowd tasking”, developed by the authors and their organisations within the multi-disciplinary research project RE-ACTA. The concept was validated during a field exercise involving 20 volunteers. The paper provides a brief classification of volunteers, it explains the RE-ACTA operational concept of crowd tasking, associated requirements, design principles, system architecture and implementation aspects of the proof of concept which was used for a practical validation during a field exercise.

Keywords: crisis management; crisis and disaster management; volunteer management; crowd tasking; humanitarian non-governmental organizations

1 CLASSIFICATION OF VOLUNTEERS

In several countries such as Austria voluntarism is a fundamental pillar of the social service system. A major attribute of voluntarism is the fact that the actions executed by volunteers are performed at their own choice without expecting and obtaining financial compensation [1]. In this context we consider both, formal and informal forms of volunteering independent of the extent in terms of working hours (full-time / part-time) or location of action (at home / abroad).

Formal voluntary assistance is typically performed in an institutional context whereas informal types of volunteer engagement can be described by individual engagement beyond the context of an organization. Informal engagement is often referred to as neighbourly help. For many decades the Austrian disaster relief actors such as fire brigades or the Red Cross have mostly relied on formal types of volunteering. However, this type of volunteer engagement does not address all parts of the population. Younger people are less willing to formally bind themselves to an organization for longer periods but are ready to help in a flexible and task based way.

According to [2] target groups for voluntary engagement can be classified as shown in Fig. 1.

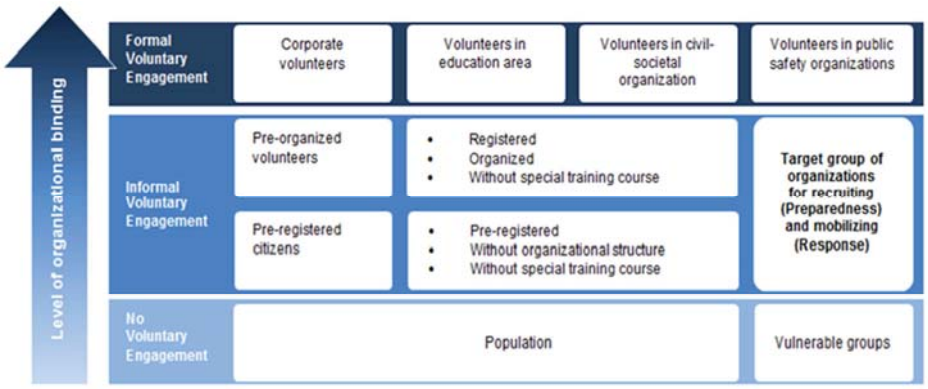


Fig. 1 Classification scheme for target groups of volunteers involved in crisis management [2]

The different types of volunteers shown in Fig. 1 differ in their commitment to a specific organization. Looking at informal engagement, pre-registered citizens are generally willing to assist in crisis situations having very limited binding to an organization by formal structures. In contrast to pre-registered citizens, pre-organized volunteers are ready to accept a higher level of binding to an organization. These two groups can be subsumed to the category of spontaneous volunteers. This specific category can be addressed using the following crowd tasking concept.

2 VOLUNTEER MANAGEMENT – STATE OF THE ART

Multiple solutions for volunteer management in crisis and disaster management are implemented worldwide. In order to categorize them, a distinction between crowdsourcing and crowd tasking solutions can be made. According to [3] crowdsourcing can be defined by assigning tasks to a non-specific group of people whereas crowd tasking means the selection of predefined, known volunteers qualified for specific scenarios and to communicate with them via specific interfaces during the execution of the tasks. Within this paper we focus on crowd tasking solutions that are specifically designed for provision of relief in crisis and disasters.

In the context of this paper the crowd tasking approach “Team Österreich” of the Austrian Red Cross is of outstanding relevance [4]. Basically, people ready to become member of the Team Österreich have to submit themselves to an online registration process and are obliged to be in possession of an email address and a cell phone. After registration and a training course they become an active member and can engage in coordinated relief actions according to their skills and interests. Both the Czech Team Morawa [5] as well as the German Team MV [6] are following a similar approach.

Apart from the concept of Team Österreich and similar initiatives, multiple web platforms exist that allow registration and organisation of volunteers in different ways. In the domain of self-help of citizens the Swiss platform Benevol Jobs [7] distributes tasks to volunteers. However, interactive communication with volunteers is not provided. The recruitment and mobilization of volunteers during the Libyan conflict in 2011 was realised using the platform United Nation Volunteers [8]. Another initiative for inclusion of volunteers is CrisisCommons [9]. Technology skilled volunteers are trained in camps to provide support by performing IT tasks. VolunteerMatch [10] provides a platform in order to enhance co-operation between non-profit organisations and volunteers that was applied in the aftermath of the hurricane Katrina. Similar to VolunteerMatch, All for Good [11] is a free software resource to reach and attract

volunteers for non-profit projects in arbitrary domains including disaster relief. FEMA from the US provides also a platform for the National Preparedness Community [12] enhancing the social interaction of volunteers with emergency management personnel as well as the preparedness of the volunteers for multiple natural disasters.

Several institutions provide apps that can be downloaded for the purpose of involvement of volunteers in disaster relief a few among them are shortly discussed here. For instance Volunteer App [13] from the American Red Cross enables the management of volunteers during crisis using an app as interface to the volunteers. A similar approach is followed by Rapid Rescue [14] from the Singapore Red Cross notifying qualified volunteers if someone in their neighbourhood is requesting their help. In Queensland the free iPhone App ReadyQld [15] is available to prepare communities for disasters and emergencies, the Self Recovery App [16] focuses on preparation for and mitigation of effects of disasters. Finally, Emergency Australia [17] is an app providing warning and incident information for whole Australia.

The analysis of the state of the art shows the need for the combination of different concepts in order to optimize pre-registered volunteers management. The possibility to contact specific volunteers selectively depending on their qualifications and their availability is regarded as very important. The possibility of both, using predefined sets of tasks as well as defining additional tasks ad-hoc is also required. In addition the opportunity to interact with volunteers during their relief action using new media such as apps is also of considerable importance. The concept developed within RE-ACTA combines these concepts and is therefore a relevant step forward concerning the involvement of pre-registered volunteers. A more detailed analysis of the state of the art can be found in [2] and [3].

3 CROWD TASKING – A NEW CONCEPT FOR MANAGING SPONTANEOUS, PRE-REGISTERED VOLUNTEERS

Following the analysis of the state of the art, this paper is now focusing on citizens, how pre-registered themselves and expressed their willingness to contribute during a crisis. Crowd tasking is a comprehensive concept for addressing pre-registered volunteers, composed of structures, processes and tools with the goal to build up and maintain an informal community of pre-defined and informal volunteers, mobilize them when needed, control their activity and collect data provided by them for enhancing situational awareness of all actors involved in the disaster relief [2].

The specific tasks are defined when they are needed by the responsible actor of the emergency management. They can either facilitate the volunteers as sensors (e.g. “look out of the window and report back if you see no / some / a lot of debris on the street” in case of an earthquake) or also as actors (e.g. “knock at the door of your neighbours and ask them whether you could help them with some daily goods or medicine” in case of a pandemic).

3.1 Actors and Use Cases

The main actors within the crowd tasking concept are on the one hand specific members of the emergency management with their individual roles: the RE-ACTA Team Coordinator, the RE-ACTA Coordinator and the RE-ACTA Redactor. On the other hand, there are the volunteers on the spot as shown in Fig. 2.

The basic processes composing the RE-ACTA crowd tasking system are described by six elementary use cases (UC) for the RE-ACTA technical system:

UC 1 Community building
As a continuous process, the RE-ACTA Redactor builds up and maintains

the community of volunteers. This task involves promotional activities as well as continuous care about already registered volunteers.

UC 2 Registration and Data Maintenance
New volunteers register themselves and provide basic information like their contact data, their interests and their capabilities. Once submitted, volunteer's data are regularly maintained.

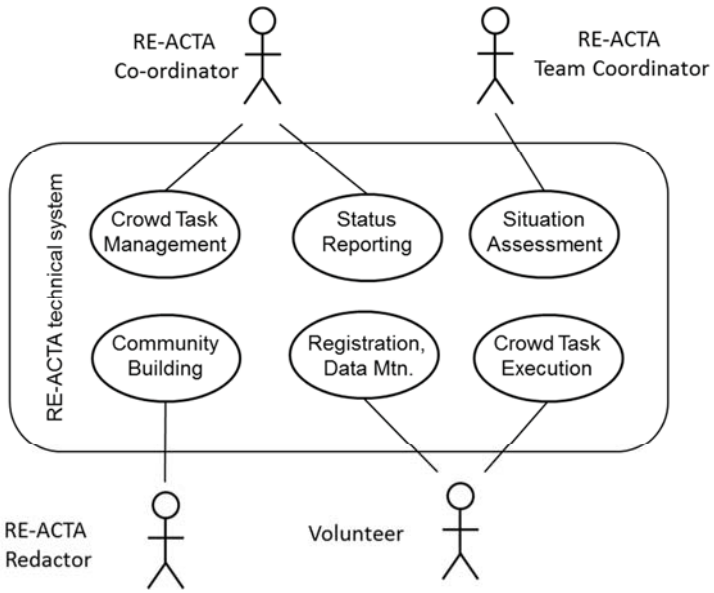


Fig. 2 Actors and main use cases of the RE-ACTA crowd tasking concept (simplified)

UC 3 Crowd task management
When needed, the RE-ACTA Coordinator makes use of the database of pre-registered volunteers to select a subgroup which will be alerted. Task lists are defined and advertised to specific groups among the alerted volunteers.

UC 4 Crowd task execution
Volunteers receive tasks assigned by the RE-ACTA Coordinator. They can accept and execute tasks from the advertised list or reject them, respectively. For accepted tasks, they provide feedback via their smartphone app.

UC 5 Status Reporting
The RE-ACTA Coordinator consumes status reports about the crowd task distribution and execution.

UC 6 Situation Assessment
The RE-ACTA Team Coordinator analyses and evaluates the feedback data. He uses the dataset for situation assessment and exports situation reports.

3.2 RE-ACTA-Specific Non-Functional Requirements

The following three requirements are specific to the RE-ACTA crowd tasking concept:

1. Structured data: In order to support electronic information processing, task- and feedback data is required to be strictly structured including the prescription of defined values and their meaning.
2. Flexibility: Any sequence of specific tasks and any kind of required structured feedback (e.g. selectable values from a predefined list) shall be possible.
3. Ease of Use: The volunteers must be able to use their part of the system (i.e. the mobile app) without any training within a few minutes of orientation

A number of further non-functional requirements complement the functional requirements upon the RE-ACTA technical system, among them requirements on data-security, system-availability and cost.

4 CROWD TASKING TOOL FOR CRISIS- AND DISASTER MANAGEMENT

4.1 Technical Architecture

As shown in Fig. 3, the system consists of 3 interlinked main components which are separated according to their specific technical and functional requirements in order to enable a fault-tolerant, high-availability system architecture.

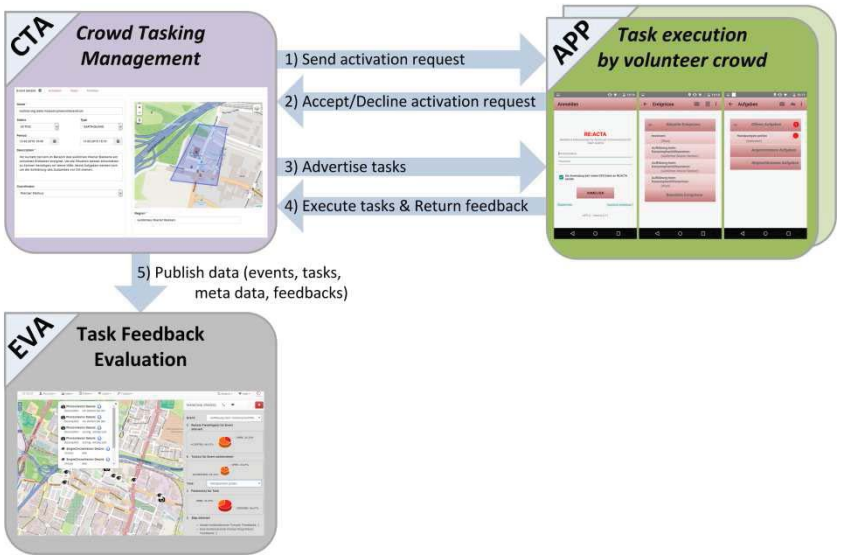


Fig. 3 Communication flow between the RE-ACTA components during an ongoing crowd tasking operation

The Crowd Tasking Application (CTA) is responsible for task administration, volunteer selection based on their declared capabilities and location data; task distribution, and task feedback towards the Evaluation and Reporting Tool (EVA) and the distributed mobile device applications (APP).

The APP provides the uniform communication channel between the professional crisis manager (RE-ACTA Coordinator) and each individual volunteer. This component is used for providing relevant information about ongoing crisis events with associated task details. The APP also locally supports the task assignment and task feedback workflow where each volunteer executes the specifically assigned tasks and returns the requested data in the appropriate form (e.g. picture, single / multiple choice, free text). This information is stored in the local mobile database and transferred from the APP to the central RE-ACTA back-end (CTA). In order to maintain full functionality on the mobile device even when the internet connection is temporarily disrupted, the APP is able to handle online and offline situations with smart replication and synchronization mechanisms.

The returned task data is validated and forwarded to the Evaluation and Reporting Tool (EVA). Here the data is structured and aggregated to generate an up-to-date common operational picture (CoP) based on the returned volunteer feedback. The communication between CTA and EVA is established by using a state of the art event driven architecture with support of fault-tolerance, scalability and high availability features. On the other hand, the data exchange to and from the mobile application is done using NoSQL replication technologies based on standard HTTP protocols to maintain easy extension and adaptation to other systems and platforms [18].

4.2 Proof of Concept

Based on the discussed use cases, a proof of concept prototype (PoC) for the three RE-ACTA components (CTA, APP and EVA) was implemented in order to support the evaluation and demonstration of the RE-ACTA crowd tasking concept within a field trial. For designing the PoC implementation, individual process steps of the RE-ACTA operational processes were mapped to specific functional blocks of the PoC. Fig. 4 shows this mapping.

Fig. 4 High-level Process mapped to PoC Application Screens

The first phase covers the event creation and sending of activation requests from the crowd tasking management application CTA directly to relevant volunteer groups within the concerned area. On the mobile device application (APP), each recipient is asked to confirm his or her willingness and availability for the task execution. In the next step, tasks are created/selected by the RE-ACTA coordinator using CTA, each task comprising a specified area of interest, task description and detailed step-by-step instructions. The tasks are distributed to the volunteers in the field. Each volunteer receives a notification and can select the tasks he is willing to execute. The RE-ACTA APP provides detailed step-by-step workflows for each task. In phase three the information captured by all participating volunteers is processed by the RE-ACTA backend. Data is transferred to the visualization and evaluation tool (EVA) where it is aggregated and finally displayed on an interactive map, with supplementing windows and diagrams.

5 VALIDATION

In February 2015, the prototype was used for a first validation of the crowd tasking concept within a field trial performed by the Austrian Red Cross in cooperation with the Vienna University of Technology. 20 volunteers were involved in a small scale exercise at the Austrian Red Cross Disaster Management Center in Vienna. Three of them – advanced regional disaster-managers – were selected as coordinators; the others were grouped by three as “crowd” to fulfil the prepared tasks as volunteers. The redactor part was fulfilled by the RE-ACTA-Team.

The volunteers had to perform several tasks, such as describing traffic on a nearby road and taking a picture to illustrate their findings; estimating the count of people at a

nearby church; assessing the waterline of a nearby river. This multi-perspectival approach validated all three parts of the RE-ACTA toolset on usability, accessibility and user interface design on the one hand and on process-level for crowd tasking and management of these processes on the other hand. The participants were interviewed before and after the evaluation in order to gather their findings on the different questions. Each volunteer team was accompanied by a silent observer; also the coordinators were closely monitored by evaluators from the Vienna University of Technology. Results of the field trial where collected via semi-structured interviews from the actors and observers after the trial. Main categories for the evaluation were: practical fit of the process, usability of the technical solution. general acceptance.

All actors engaged themselves positively in the field trial. As general result, the feedback was very encouraging and proved the applicability of the concept and the RE-ACTA technical system. A number of specific suggestions for improvement were found. On process-level, an interesting point was the discovery that the volunteers only wanted to get pieces of information, which are directly relevant for their concrete acting. News about things happening in their surroundings was seen as disturbing while they were working on concrete tasks. Another interesting point was the requirement for providing a supervisor with the possibility to overrule all activities in case of a safety-critical development of the situation. On usability level several volunteers had difficulties with finding the right location for their specific task. Improved navigation aids are required. From the co-ordinators the need was articulated for having re-usable templates available to ease the setup of recurring tasks. Concerning the acceptance of the concept in general and also the PoC implementation, the general reaction was very positive. As possible improvement for the acceptance, volunteers raised the wish for being able to propose tasks from the field to the coordinator at their own initiative. This observation fits well to the general consideration that spontaneous volunteers are very much driven by their own initiative and want also to remain pro-active when coordinated within a crowd tasking process.

6 DISCUSSION OF THE RESULTS AND OUTLOOK

Spontaneous volunteers can be seen as huge unexploited potential of capabilities and resources within a disaster relief activity. However, they can also become an obstacle for the emergency management if they are not guided and integrated into an appropriate collaboration process together with the professional emergency management. The experiences with the RE-ACTA crowd tasking concept shows, how such collaboration can successfully be organized based on state of the art tools for communication and information management. Spontaneous volunteers become a valuable resource for disaster relief – both as actors and as sensors for improved situation awareness for the professionals.

The field exercise also showed a number of possible improvements, which were articulated by the different users of the RE-ACTA system themselves. The European research project DRIVER [19] provides the opportunity to further enhance, test and demonstrate the RE-ACTA crowd tasking concept and the RE-ACTA technical system within an international environment.

During the project, additional ideas for possible applications of the concept outside of the emergency and disaster management domain could be identified: Processes, where organisations need information from the field in order to validate fore- and now casts (e.g. weather service providers) may benefit greatly. They also could rely on this concept to calibrate simulation models, in order to increase their effectiveness. Another important perspective is resilience-building before disasters occur. Micro messages and “gamified” tasks can educate population in the right behaviour for crises and disasters.

ACKNOWLEDGEMENTS

RE-ACTA was funded by the Austrian security research programme KIRAS of the Federal Ministry for Transport, Innovation and Technology (bmvit).

REFERENCES

[1] EC, “EUR-LEX, L345/75, Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,” 8 12 2008. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&qid=1427458338597&from=EN. [Accessed 11 June 2015].

[2] G. Neubauer, A. Nowak, B. Jager, C. Kloyber, C. Flachberger, G. Foitik and G. Schimak, "Crowdtasking - a new concept for volunteer management in disaster relief," in *Environmental Software Systems*, Heidelberg New York Dordrecht London, Springer, 2013, pp. 345 - 356.

[3] G. Neubauer, A. Nowak, B. Jager, D. Havlik, G. Foitik, C. Kloyber and C. Flachberger, "Crowdtasking for crisis and disaster management - opportunities and challenges," in *IDIMT - 2013 Information Technology - Human Values, Innovation and Economy*, Linz, Johannes Kepler Universität Linz, 2013, pp. 47-55.

[4] T. Österreich. [Online]. Available: http://apps.teamoesterreich.at/. [Accessed 2 June 2015].

[5] T. Morawa. [Online]. Available: http://www.teammorava.cz/en/who-is-team-morava. [Accessed 2 June 2015].

[6] T. MV. [Online]. Available: http://www.team-mv.info. [Accessed 2 June 2015].

[7] B. jobs. [Online]. Available: https://www.benevol-jobs.ch. [Accessed 2 June 2015].

[8] U. Nations. [Online]. Available: http://unv.org. [Accessed 2 June 2015].

[9] C. Commons. [Online]. Available: http://crisiscommons.org . [Accessed 2 June 2015].

[10] V. Match. [Online]. Available: http://www.volunteermatch.org. [Accessed 2 June 2015].

[11] A. f. Good. [Online]. Available: www.allforgood.org. [Accessed 2 June 2015].

[12] N. P. Community. [Online]. Available: http://www.community.fema.gov/connect.ti/readynpm. [Accessed 2 June 2015].

[13] V. App. [Online]. Available: http://www.redcross.org/mobile-apps/volunteer-app. [Accessed 9 June 2015].

[14] R. Rescue. [Online]. Available: https://www.jwt.com/en/singapore/work/rapidrescue. [Accessed 2 June 2015].

[15] R. Qld. [Online]. Available: http://www.emergencyvolunteering.com.au/home/disaster-ready/menu/emergency-smartphone-app. [Accessed 2 June 2015].

[16] S. R. App. [Online]. Available: https://www.qld.gov.au/community/disasters-emergencies/self-recovery-app. [Accessed 2 June 2015].

[17] E. Australia. [Online]. Available: http://emergencyaus.info/map. [Accessed 2 June 2015].

[18] Ch. Ruggenthaler, "Expanding NoSQL Technologies to Mobile Devices," in *IDC Datahub Conference*, Vienna, 2015.

[19] Atos, "driver - Driving Innovation in Crisis Management for European Resilience," [Online]. Available: http://driver-project.eu/. [Accessed 10 June 2015].

EXPERIMENTING TOWARDS CIVIL SOCIETY RESILIENCE

Dr Wolf Engelbach[1], Christian Kloyber[2], Eric Rigaud[3], Willi Wendt[4]

[1] *wolf.engelbach@iao.fraunhofer.de*
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO,
Nobelstr. 12, 70569 Stuttgart (Germany)

[2] *christian.kloyber@research.roteskreuz.at*
Austrian Red Cross Research, Wiedner Hauptstrasse 32, 1040 Vienna (Austria)

[3] *eric.rigaud@mines-paristech.fr*
MINES ParisTech, PSL Research University, Centre de recherche sur les risques et les crises CRC, CS 10207 rue Claude Daunesse, 06904 Sophia Antipolis (France)

[4] *willi.wendt@iat.uni-stuttgart.de*
Universität Stuttgart, Institut für Arbeitswissenschaft und Technologiemanagement IAT,
Nobelstr. 12, 70569 Stuttgart (Germany)

Abstract

Civil Society Resilience is an area of crisis management that is complementary to professional response. Crisis managers and response organizations need to integrate individuals, communities and local governments in their management efforts, among others by efficient crisis communication via media and the mobilization and handling of citizens as spontaneous volunteers. DRIVER aims at a campaign of experiments: organizational concepts and IT-solutions will be iteratively tested and assessed under realistic conditions to understand and improve their operational benefits.

Therefore, this paper outlines the DRIVER approach of addressing the civil society in the context of resilience towards crisis situations. This does not only include a society oriented definition of local resilience as well as an introduction into the DRIVER perspectives of the society to be included in the DRIVER framework, rather it will be explained how DRIVERs consecutive experimentation approach supports the sustainable development of local societal resilience.

Keywords: crisis management, resilience, civil society, experimentation, individual, community, local government, crisis communication, spontaneous volunteer

1 INTRODUCTION AND MOTIVATION

Crisis management is an ever evolving challenge, not only globally, but also within Europe. Hazards change, among others due to climatic change, and other vulnerability patterns evolve, e.g. by new settlements and higher population density within cities. Further, the digitalization of the society creates new options for cooperation, but at the same time new threats by failure or misuse. Within societies new mobility concepts and socio cultural changes lead to new and diversified forms of responsibility and flexibility, which are increasingly important to be reflected in crisis management strategies.

European crisis management capabilities already form a mature and competent System-of-Systems: a federation of heterogeneous and loosely coupled local, regional and national systems able to collaborate in varying configurations and with different levels of interoperability. Radical changes to these capabilities would be very costly and likely to induce an unacceptable loss of capabilities during a long transition phase.

Further, crisis management is not only a matter of dedicated first responders, it also involves spontaneous reactions, community engagement and civil institutions,

contributing to complex and situation specific adapted response activities. In the EU security demonstration project DRIVER we therefore consider Civil Society Resilience as an area of crisis management complementary to professional response in order to anticipate the crisis, reduce its impact and recover from the effects. This requires changing the crisis management attitude and concepts as well as organisation and information systems.

DRIVER aims to improve the crisis management in Europe and its uptake of innovative solutions. Since its initiation in May 2014 it also started with the development of a pan-European test-bed enabling the benchmarking of new crisis management solutions and thereby facilitating capability development through the provision of respective methodologies and infrastructure. All developed solutions of the DRIVER project will be consecutively tested in this environment, including solutions for civil society resilience. The clear scope of DRIVER is on Europe, assuming to have a basic level of infrastructure, governance and education compared to developing countries. Moreover, resilience culture and discussion can differ from experiences in the US or Australia.

2 HISTORIC COMPONENTS TO DEFINE CIVIL SOCIETY RESILIENCE

Resilience is an integrative concept that became prominent in 21st century scientific thinking and on the political agenda. It encompasses two main ideas: response to stressful events and sustainability of systems in coping with stressful events [1]. There is no consensus on a common definition of system resilience. Resilience is sometimes considered a process, a characteristic of system, a dynamic of development, an outcome, and sometimes all of the above [2]. Resilience is applied to many systems. In DRIVER resilience relates to the crisis management domain, and within the SP3 of DRIVER it narrows down to the involvement of civil society in crisis management.

A current definition of civil society is a combination between two perspectives. The first one is the “area related” perspective where civil society refers to a space for social action that is located between the state, the economy and the private sphere, characterized by a high degree of social self-organisation in which the actors are a social movement and non-governmental organisations. The second one is the “action related” perspective, focusing on the normative assumptions concerning the quality of social actions in the establishment and stabilization of democracy, in the regulation of democratic self-governance and the development of democratic learning process [3].

Disaster resilience can be defined as the capability to prepare for, prevent, protect against, respond to or mitigate any anticipated or unexpected significant threat or event, including natural disasters or terrorist attacks, to adapt to changing conditions and rapidly bounce back to a normal or a “new normal”, and reconstitute critical assets, operations and services with minimum damage and disruption to public health and safety, the economy, environment and national security [4]. This comprehensive definition requests a specification for capable actors and responsibilities. In DRIVER SP3 we understand disaster resilience as a property of a region of any scale, or an entity such as an individual, a community or an organisation. Such regions and entities can be affected by a large diversity of hazards (economic, environmental, geopolitical, societal and technological, etc.) and thus need a generic coping capacity besides hazard specific strategies.

Community and organisation differ in their level of formal structures, but there are not necessarily clear boundaries between them. Both community resilience and organisational resilience can be defined as “the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions” [5] or as the “ability to recognize and adapt to handle unanticipated perturbations that call into question the model of competence, and demand a shift of processes, strategies and

coordination" [6]. Therefore, organisational resilience integrates business continuity [7]. However, the scope of DRIVER SP3 is not primarily on resilience of organisations, but on contributions of organisations to the resilience of a region in crisis management.

From an analysis of the different meanings related to resilience of individuals, ecological systems and organisations, the following key characteristics of a resilient system can be concluded for both the contribution of civil society to disaster resilience and the resilience capacity of individuals and organisations:

(1) Resilience is about a system's capacity to respond to or cope with unwanted respectively unexpected situations as well as overcoming them. Therefore, system adaptations are necessary quite often, including a broad set of possible transformations.

(2) Resilience is a question of culture. Confronted with the same situation, some people consider it as a threat and others as an opportunity. Likewise, the resilience of a system can be estimated differently, depending on the perspective of the actor.

(3) Moreover, interactions between the different scales (individual, group, organisation, territory, etc.) have to be considered when defining resilience. A resilient performance at one level may affect the performance at another level negatively.

3 A FRAMEWORK FOR CIVIL SOCIETY RESILIENCE

This civil society resilience framework has the purpose to outline the scope of DRIVER SP3 and the aspects tackled by its activities. The civil society dimension of crisis management addresses the contribution of relevant players outside professional crisis management to resilience and how they can be supported by organisational as well as IT solutions, what includes interlinks and shared responsibility between the civil society and the professional response forces. The local government is understood as one important player especially with its non-crisis-management activities and as a managing organisation for citizens' engagement. At the core of this interpretation of civil society lies a relationship where the activities of crisis management experts who aim to address or activate non-crisis-management entities are intrinsically tied to the capabilities and contributions of the non-crisis management civil society actors.

We assume that resilience has two complementary dimensions, being a status of a system and also a process to become more able to anticipate, reduce, cope and recover. Both dimensions are influenced by many factors that cannot be completely controlled. Thus, it is always relevant to clearly state the assumed context conditions for solutions and experiments and to be careful with generalisations. This framework provides a common ground, but cannot address specific crisis situations or the conditions in one country. Even within one state, the civil society is heterogeneous in many dimensions, such as education, language, political believes, religious traditions, family relations and social activities. Solutions in SP3 thus should reflect if and how they can be aware of or adapted to the cultural context of sub-groups in society, among others related to their risk perception.

Civil society resilience in the crisis management context refers to the resilience of actors outside the professional response such as individuals, communities or cities. Complementary the term societal resilience constitutes an overarching concept that refers to the value-dimension of society as a whole. In that sense positive and negative societal implications of civil society resilience solutions can be assessed. Already without any major disaster, each society is constantly evolving, has a dynamic character and is permanently transforming. Thus there cannot be an ideal status with regards to resilience, which should be achieved or conserved. However, organisational

memory and a common culture are important to stabilize a society and support the involvement of people. In that respect, it is also relevant to consider non-citizens (e.g. refugees, tourists and transients) as a relevant group for resilience improvement strategies since they are often less integrated and specifically vulnerable.

SP3 is experimentation driven and thus needs to concentrate on some core challenges. This covers only part of the overall civil society resilience arena, since for example the role of educational systems, companies or infrastructure providers is not addressed (compare Fig. 1). The solutions developed and tested within this framework will be derived from existing concepts and tools within EU research and crisis management activities. The solutions should lead to adaptive capacities of the system that allow coping and overcoming unwanted situations. Within the DRIVER experiments they should be tested in different contexts and against scenarios, which describe unwanted situations and thus allow challenging the generic resilience capacities.

Fig. 1: Civil Society Resilience Framework

4 SELECTED ASPECTS FOR CIVIL SOCIETY RESILIENCE

In order to help crisis managers and response organizations to understand and guide these developments and to integrate them in their management efforts optimally, DRIVER addresses three levels of society's organization:

(1) Individuals: Each individual, including affiliated volunteers, perceives risks differently and behaves accordingly in crisis situations. The specific psycho-social crisis dynamics are addressed by dedicated training kits, which are tested under different conditions.

(2) Communities: Communities are complex compositions of individuals which share common traits such as location or identity and are therefore a

fundamental element in building resilience within a society. Based on assessments and simulations, DRIVER provides recommendations for measuring and strengthening community engagement before and during crisis.

(3) Local governments: Cities and regional authorities are not only involved in professional crisis management, they can also foster actions, decisions and processes to support local civil society resilience. With this intention, DRIVER suggests self-assessment methodologies as well as communication processes involving different local stakeholders.

Additionally DRIVER focuses on two themes within the target groups: Crisis communication via media and the mobilization and handling of citizens as spontaneous volunteers. The first aims at optimizing the communication management between citizens and critical stakeholders (specifically media and public policy makers) before, during and after a crisis to ensure comprehensive, understandable and fast information delivery. Regarding people that have not been trained for disaster management, DRIVER tests and improves strategies to organize and coordinate unaffiliated individuals and civil groups.

5 EXPERIMENTATION APPROACH IN CIVIL SOCIETY RESILIENCE

DRIVER being a demonstration project aims at a campaign of experiments that increases in complexity, e.g. covering first one and then more of the above-mentioned topics. Organizational concepts and IT-solutions will be iteratively tested and assessed under realistic conditions to understand and improve their operational benefits.

This aims for a better evidence-base for crisis management capability investment decisions. However, the complexity of crisis management makes it hard predicting analytically the potential benefits of new solutions and approaches, particularly considering the wide scope of potentially relevant contingencies. Therefore the DRIVER approach will test, benchmark and evaluate the proposed solutions in close to real environments with real users in the context of their actual legacy resources.

For that both physical and virtual “platforms” as well as common guidelines for experimentation are provided to all thematic research strands of DRIVER. This shall facilitate an overarching evaluation approach with common scenarios, data, infra-structures and involved groups for different experiments. In addition, simulation, historical experience and expert judgment will be used to reflect the experiments and come up with reliable recommendations for policy and stakeholders.

5.1 The specific challenge of experimentation in SP3

The above sketched experimentation approach poses some specific challenges for SP3 as in addition to crisis management, SP3 deals with another even more complex system of systems – civil society and its actors. Actors which despite of increasing global mobility and interconnectedness remain social human beings locally embedded into specific institutional, legal, social and cultural contexts.

5.1.1 The reductionist fallacy

Civil society resilience experimentation activities must navigate through two extremes: the fallacy of methodological reductionism and the lacking explanatory power of methodological particularism. Reductionism seeks to reduce the complexity of a whole by breaking it into its smaller parts, which in isolation are simpler to explain. Thus in natural sciences experimentation serves to describe, explain and predict the relation between different constituent parts and the whole with reduction being a necessary process to isolate the effects of variables in a controlled environment.

Within the social sphere however, reductionism is confronted with the criticism that it renders the multidimensional as uni-dimensional. By isolating parts in order to study them it tends to ignore the properties of the complex whole, thus often discarding the socio-cultural context as noise and underestimating the importance of social interactions. The other extreme position sometimes found in humanities is particularism which focuses on understanding the characteristics of a group or a culture without making generalisations or comparing it to another. In that way particularism fails to explain the interconnectedness of sub-parts such as similar crisis management processes or institutional and cultural similarities among EU member states. The fact that there are huge historically derived cultural and legal differences throughout the EU member states doesn't mean that one solution originated in one member state can't be applied in another, but that it has to be adapted to the new socio-cultural context.

5.1.2 The proposed experimentation methodology

As SP3 is dealing with the multiple social interactions between crisis management actors and civil society it strives to avoid both, oversimplification deriving from reductionist fallacy and in-transferability of concepts deriving from particularism. Thus SP3 seeks on the one hand to capitalise on methodical support and physical platforms SP2 provides to the whole project. For simplicity, platforms can be imagined as crisis-management training grounds (indoor and outdoor) provided by organisations such as THW or MSB which are equipped with technical and human resources (professional responders and volunteers) for testing new crisis management solutions.

On the other hand, SP3 is well aware of the limited explanatory power of single experiments which are run in SP3 – thus the "laboratories" of SP3 are always interactive formats like expert workshops, focus groups, training events, table-top exercises or small scale field exercises. These settings facilitate the recreation of the social interactions which are inherent to crisis management processes, while enabling the researchers to observe and assess these processes.

This is achieved by following a dialectic approach combining qualitative and quantitative methodology in theory building and evaluation. Qualitative methods are used for describing the socio-cultural context of solutions and also for generating new hypothesis – an indispensable function for facilitating innovation. In SP3 experiments, methods like expert interviews or focus groups are used in initial experiments and in preparation of later table-top or field experiments. This allows understanding the context crisis management concepts and IT-solutions stem from and thus enables building hypotheses that shall be tested.

Ex-post evaluation by means of standardised questionnaires following quantitative performance indicators (e.g. percentage of people acting upon a warning or taking certain protective measures) will be complemented with qualitative methods like participant observation or oral debriefings to better capture the social interactions and the lessons learned of participating responders and civil society actors.

5.1.3 Towards a transferability approach

SP3 sees its strengths in testing innovative concepts in different socio-cultural settings and contributing to a context sensitive transferring of innovative resilience enhancement solutions among EU member states, its local governments and its population on local and community level.

Key supporting process is contextualisation, making explicit the institutional, legal and cultural context of tested solutions. This will be reached through a dialectic process of induction and deduction: solutions will be described by categories derived from other sub-projects dealing with legal and societal aspects. They originate from deducting from a comparative country studies (e.g. categories like institutional context, legal conditions, organizational cooperation) and from deduction from ethical assessments

(e.g. categories like trust, inclusiveness, openness, etc.). These categories will also be used for guiding evaluation to reach a better understanding of factors for successful transmission of ideas and solutions between different European member states.

5.2 Thematic strands of experimentation

In crisis management the relationship between societal actors and response is an asymmetrical one, with responders being regulated by an organisational and legislative framework, standard operating procedures and expert knowledge acquired through regular training in simulated and real emergency situations, while civil society actors are often not aware of the disaster risks they face, the preparative and protective measures they can take as individuals and how to support fellow members of their local communities before and during a disaster situation. The following experiments will embark on these topics:

(1) Training in psychosocial support: A strengthened individual resilience of volunteers and the population affected by crises is important for coping with the aftermath of disaster situations. Three existing psychosocial support tool kits are delivered in a new train-the-trainer cascade to trainers and responders.

(2) Community resilience: The immediate response to crisis is mainly a local one, thus preparing local communities and building up their capacities and the relationship between local actors is a key investment in enhanced community resilience. Measurement tools for comparing the resilience of communities, participatory methods for raising awareness and triggering action as well as guidelines for professionals on capitalizing on active citizens are being experimented with in different countries.

(3) Local government resilience: Cities and regional authorities are responsible for people, infrastructures and local policies which constitute society and lay the baseline for resilience. Therefore, DRIVER aims to develop a method helping local governments to assess the resilience of all relevant aspects within their territory. The experiments will focus on the evaluation of this assessment method in order to develop a tool that is adaptable by the targeted end users on governmental level as well as for all local stakeholders.

(4) Crisis communication: Informing the public is not confined to the immediate occurrence of a disaster, when people need to be informed on the hazard, protective measures and required interventions to take. Resilience of the population is very much linked on what and how it is communicated before a disaster when there is much less media attention. Target group sensitive communication of simple preparative measures is still a gap. Thus experimentation will focus on the impact of different key messages on target groups and on how to share the knowledge on simple and impactful communication with communicators – which can be local government decision makers or crisis management organisations.

(5) Organising and mobilising spontaneous volunteers: When alarmed and emotionalised by media, un-affected civil society actors often want to help posing a coordination challenge to the response. Experimentation is focused on two aspects: whether pre-configuration does make individuals and groups better prepared to assist the response and conversely minimise the efforts on side of the response to incorporate the influx of spontaneous helpers. A second aspect is focusing on the tasking of the population via a smart phone app.

6 CONCLUSIONS AND OUTLOOK

This paper outlined the DRIVER strategy to address the civil society within disaster resilience activities. Due to the high complexity of the civil society, it is necessary to develop solutions addressing the specific needs of all parts of the society and building a combining framework that allows an integrated resilience strategy.

In the next steps of the DRIVER project, the civil resilience solutions will be part of experiments in an even wider crisis management setting. For example, crowd tasking apps will be combined with IT-tools for responder collaboration, or competence frameworks used to understand the effects of psychosocial support. In two joint experiments (JE) even further combinations will be tested over an extended period along the same scenarios addressing floods and ice storms. A final demo based on a Mediterranean tsunami will then illustrate integrated approaches and consecutive solution testing in established pan-European test-beds.

REFERENCES

[1] Reich J. W., Zautra A. J., Stuart Hall J., 2010. Handbook for adult resilience. New York: The Guilford Press.

[2] Zautra A. J., Stuart Hall J., Murray K.E., 2010. Resilience, a new definition of health for people and communities. In Reich . W., Zautra A. J., Stuart Hall J. (eds), Handbook of adult resilience.

[3] Gosewinkel, D., 2001. Civil Society. In: European History Online (EGO), Mainz: Institute of European History (IEG).

[4] TISP (The Infrastructure Security Partnership), 2011. Regional disaster resilience, a guide for developing an action plan. The infrastructure security partnership.

[5] Hollnagel E., 2011. Prologue: The Scope of Resilience Engineering. In Hollnagel E., Pariès J., Woods D. D. and Wreathall J., Resilience Engineering in Practice. Ashgate Studies in Resilience Engineering.

[6] Woods D. D., 2006. Essential Characteristics of Resilience. In Hollnagel E., Woods D., Leveson N., Resilience Engineering: Concepts and Precepts, Ashgate.

[7] ISO 22301:2012. Societal security -- Business continuity management systems – Requirements. International Standardization Organisation.

[8] IFRC, 2012. The road to resilience. Bridging relief and development for a more sustainable future. Geneva: IFRC discussion paper on resilience – June 2012.

[9] Levins, R., & Lewontin, R., 1980. Dialectics and reductionism in ecology. Synthese, 43(1), 47–78.

Acknowledgements

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement n°607798. We thank the DRIVER project partners, especially those involved in Sub-Project 3, for fruitful discussions about concepts, solutions and approaches. The paper reflects only the authors' views, the Commission and the Project are not liable for any use that may be made of the information contained therein.

COMMUNICATION TECHNOLOGIES IN DISASTER SITUATIONS: HEAVEN OR HELL?

Daniel Auferbauer[1], Gerald Czech[2], and Hilda Tellioglu[3]

[1] *daniel.auferbauer@student.tuwien.ac.at*
AIT Austrian Institute of Technology GmbH, 2444 Seibersdorf, Austria /
Vienna University of Technology, Multidisciplinary Design Group, Favoritenstraße 9-11, 1040 Vienna, Austria

[2] *gerald.czech@roteskreuz.at*
Austrian Red Cross, Marketing and Communications, Wiedner Hauptstraße 32, 1040 Wien (Austria)

[3] *hilda.tellioglu@tuwien.ac.at*
Vienna University of Technology, Multidisciplinary Design Group, Favoritenstraße 9-11, 1040 Vienna (Austria)

Abstract

In this paper, we present two initiatives for volunteer management that are currently being conducted in Austria. By comparing them, we see a shift towards the use of Information and Communication Technology (ICT), which brings with it issues concerning the segregation of certain segments of the population. These, we wish to bring to the reader's attention and discuss their implications for the use of ICT in disaster situations.

Keywords: Crisis management; crowd tasking; resilience; communication technology; segregation.

1 INTRODUCTION

Disasters and the efforts to cope with them are not new to humankind. Historical reports of such events date far back, then being attributed to acts of deities and the stars, the later indeed being part of the etymological origin of the word "disaster" [12]. While the concept of catastrophes and their mitigation is certainly not new, we have technology at our disposal now that opens new ways for disaster management. Information and Communication Technology (ICT) is becoming ever more ubiquitous, permeating the lives of our society in Europe. The possibilities provided through this have been recognised and academia has given attention to the topic (compare section 2). Yet while the rise of ICT offers many possibilities, a selection of which will be discussed in this paper, it also brings challenges and possible pitfalls. Technology is changing and advancing at a very fast pace. What about those that are not comfortable with the new developments? Do we, by employing new options for disaster mitigation, foster segregation within our society? How may we prevent this and encourage inclusion, to improve resilience? We seek to explore and discuss these questions based on recent developments and efforts towards community management for raising disaster resilience in Austria.

This paper will proceed as follows: Section 2 introduces literature and prior work that is relevant to the topic of ICT in disaster management. Section 3 presents two approaches to community management in disaster situations that have been developed in Austria. Based on that, Section 4 discusses the differences between these approaches and the implications that this development has for segregation and inclusion in communities. Lastly, we present our conclusions in Section 5.

2 RELATED WORK

A lot of work has been done towards the investigation of ICT usage among the general public in case of extreme events. Palen *et al.* describe the usage of various forms of ICT for information gathering and collective sense-making during and after the Virginia Tech shooting in [11]. Starbird and Palen describe how the microblogging service Twitter was used in the Haiti Earthquake of 2010 to support self-organising of volunteers [15]. They also describe how various ICTs are used for collaborative work of volunteers to help, on their own initiative, remotely with relief efforts [14]. Vieweg *et al.* investigate the information distributed in Twitter during two natural hazard events [16]. Apart from these purely self-organised grassroots approaches, there are also works that report on collaborative efforts between relief organisations and volunteers. Cobb *et al.* describe in [6] how emergency response units use "digital volunteers", i.e. people that want to help from a remote location, to curate social media data in disaster situations. Hofman *et al.* introduced a mobile phone-based application called "Hands2Help" for coordinating volunteers by matching the demand for volunteer work with the nearest, available volunteers [7]. Lanfranchi *et al.* present a collaboration platform called WeSenseIt in [8], where citizens and authorities work together in flood management for the benefit of both parties. The concept of "crowd tasking", which will also play a role in this paper, has been described in [10] by Neubauer *et al*. It also features in [13], wherein Schimak *et al.* investigate the topic of crowd sourcing in crisis management.

3 APPROACHES IN AUSTRIA

Currently there are two approaches in Austria to engage volunteers in disaster relief efforts. In this section we will introduce both of them. This allows us to establish differences between the approaches. Thereupon we will base our discussion concerning ICT in disaster situations in Section 4.

3.1 Team Österreich

Team Österreich (TÖ) is an initiative for volunteer management and volunteer engagement for disaster mitigation currently being carried out in Austria. It was conceived in August 2007 as cooperative effort between the Austrian Red Cross (ARC) and a nationwide radio station. The idea came up after a flood disaster, which struck Austria in 2002. No one was able to cope with the supply of potential, spontaneous volunteers, that showed up in the affected regions [9]. As of 2013, the number of volunteers affiliated with TÖ had grown to 35.000[1]. As volunteer convergence may pose a real problem [7], one aim of TÖ is to manage and coordinate volunteers during disasters in such a way that their presence is indeed of help rather than an impediment.

Team Österreich mainly works with pre-registered volunteers. Initially, potential participants are required to sign up through a website. They are asked to provide contact information and information regarding their abilities and skills. TÖ does not require volunteers to be affiliated with the Red Cross in any way. After having completed the sign up process online, people are invited to attend introduction courses that are hosted on a regular basis by the ARC. In the event of a disaster, should the Red Cross be of the opinion that involving TÖ be advisable, invitations for participation will be sent out to volunteers. These will go out to selected recipients, the criteria being for example age or place of residence, and are delivered through the Short Message Service. The recipients are to respond to these messages with standardised replies, either accepting or declining the invitation. Replies that are not formatted according to

[1] http://oe3.orf.at/teamoesterreich/stories/2605842/ last visited 2015/6/7

the standard template cannot be parsed automatically and have to be sifted through by hand. The process of sending out invitations, with iteratively changing selection criteria, may be repeated until the number of confirmed volunteers is agreeable to the coordinating ARC staff. Once a sufficient number of potential participants have reported, information concerning the time and place of a pre-deployment briefing is passed along to all that had accepted. At this briefing, attendees are provided with detailed information about the nature of the deployment. Attending persons that are not yet members of Team Österreich have the opportunity to sign up on the spot. Volunteers that do still want to participate sign a waiver stating their informed consent to legal implications of their actions. This is the ARC's method of avoiding punishment or regression caused by legal transgressions of volunteers during the course of their work for TÖ. For the duration of the deployment, volunteers are split into groups. Each group is assigned a supervisor that is affiliated with the Red Cross. Transport to the disaster site is organised by the Red Cross, as are accommodations in case of deployments spanning multiple days. Tasks of TÖ volunteers mostly involve physical labour, such as helping to erect improvised flood barriers or cleaning up debris. Afterwards, the ARC arranges for the volunteers to be transported back and holds a de-briefing event.

With this approach, Team Österreich offers a closely governed and supervised form of crowd sourcing. Transport and accommodations for volunteers are organised by the ARC and supervision is provided throughout the operation. For participants, this offers a lot of "face time" with the relief organisation. This concept has been tried and tested: TÖ has been involved in the relief efforts during the 2013 floods, fielding 3.250 volunteers[2]. The concept has also been successfully implemented into other societies, for example in the Czech Republic as Team Morawa[3] and in Germany in Mecklenburg-Vorpommern[4] and Bayern[5].

3.2 RE-ACTA

"Resilience Enhancement by Advanced Communication for Team Austria" (RE-ACTA) is a current research project in Austria. As the name implies, RE-ACTA has been founded on the experiences gathered through the management of Team Österreich ("Team Austria"). The aim of the project is to improve resilience by utilising new media technologies, especially through mobile handheld devices (i.e. smartphones). RE-ACTA is a collaborative research and development effort between the Austrian Red Cross, the Austrian Institute of Technology GmbH (AIT), Frequentis AG, the Vienna University of Technology (TUW) and Inset Advisory. The core concept of RE-ACTA is to offer a workflow for the selective distribution of certain tasks and information to specific groups of volunteers. This concept we are referring to as "crowd-tasking" [10].

On the technological side, RE-ACTA is composed of three distinct parts: a tool for creating and distributing tasks for the crowd (Crowd-Tasking Management, CTA) as well as an interface for visualising data gathered from volunteers through these tasks (Task Feedback Evaluation, EVA). The third component is a mobile phone application, which enables volunteers to receive and execute tasks (APP). Through these tools, personnel responsible for managing crowd tasking (whom we will henceforth refer to as coordinators) may use RE-ACTA to selectively relay tasks and information to volunteers. Thereby, it is possible to use participants as human sensors or provide them with instructions for action.

[2] http://oe3.orf.at/teamoesterreich/stories/2591639/ last visited 2015/6/12

[3] http://www.teammorava.cz/ last visited 2015/6/7

[4] http://www.team-mv.info/ last visited 2015/6/7

[5] http://www.br.de/radio/bayern3/inhalt/team-bayern/team-bayern-100.html last visited 2015/6/7

The workflow of RE-ACTA's crowd-tasking approach may be roughly separated into three phases: 1) Preparation and mobilisation, 2) task distribution and execution, and 3) analysis of results. As with Team Österreich, RE-ACTA works with pre-registered volunteers. Potential participants first need to sign up via a webpage, though the amount of personal data required to be submitted during this process is lessened. Volunteers then receive their login credentials, which they can use to log into the RE-ACTA smartphone app. In the case of an emergency where the Red Cross decides that it requires the help of RE-ACTA volunteers, invitations for participation are sent out through CTA and displayed to the recipients via APP. Criteria by which the target audience for these invitations may be selected include: current position of the volunteer, place of residence or a number of skills and certifications like, e.g., driver's license or spoken languages. Users may react to the request by confirming, declining or accepting conditionally if they are available only for a certain timespan or at a certain location. Volunteers that have accepted are eligible to receive tasks for the remainder of the operation. This concludes the preparation and mobilisation phase.

During phase two, the task distribution and execution, coordinators may define tasks and select their recipients through CTA. As during the activation, it is possible to restrict the target audience of tasks by, e.g., their current position or a set of skills. Tasks are structured in such a way that they consist of an arbitrary amount of steps, where their exact number is at the coordinator's discretion. Each of these steps is of a certain type, defined through its end result (e.g., an image or selection of pre-defined answers). The coordinator defines tasks by selecting templates for these short steps, adapting them to his/her need and defining their order in relation to each other. Having done so, s/he may select a target audience (a crowd). The selected volunteers receive this task in their smartphone APP. They can decide to accept or decline each task individually after reading a short summary about it. Accepted tasks are completed sequentially, one step at a time.

During the last phase, the information that was gathered from the volunteers through tasks may be analysed and assessed. To this end, EVA displays an interactive map of the operation area. Data from the volunteers is displayed on this map at the position that it was transmitted from. Aggregation options for data are available where applicable – e.g. if the coordinator asked during one step for volunteers to check which infrastructure still worked in their household (electricity, water or gas) the answers of all volunteers will be aggregated rather than displayed individually to preserve clearness of the visualisation. These phases are of course not discrete and may run in parallel. The outlining of phases as used above is meant to depict one "lifecycle" of the RE-ACTA workflow to better illustrate the core concept for you, the reader. In a real world scenario, they are expected to be continuous processes, repeated until the situation is considered resolved.

The workflow described above constitutes the core, the main idea, of RE-ACTA. However, that is not the full extent of the proposed system. An extensive process model for RE-ACTA was designed in a collaborative effort of the involved partners, founded on best practices and lessons learned from Team Österreich. The design was an iterative and user-centred process. The Austrian Red Cross provided guidance and feedback in each iteration of the development, acting as the essential user and ensuring the practicability of the result. In the end, the process model consisted, among other things, of almost six dozen pages of sequence diagrams and is too extensive to be described here in detail. The main workflow as illustrated in this section was then implemented to demonstrate the viability of our approach, both technological and concerning the general principle of operation. The demonstrator was put to the test during a field exercise in February 2015. It passed muster in all aspects, receiving favourable feedback, especially from operators using CTA and EVA, as well as good acceptance from volunteers executing tasks through APP.

4 IMPLICATIONS

4.1 Differences: RE-ACTA and Team Österreich

The Team Österreich approach was invented to coordinate spontaneous volunteers flowing into the damaged areas after floods. It is a real-life organization with virtual coordination mechanisms. Team Österreich volunteers are doing physical work like shoveling, cleaning or filling sandbags, while being supported by ICT for coordination purposes. The REACTA process tries to use the organizational concept of Team Österreich to manage online and online-supported offline-volunteering as crowd tasking.

RE-ACTA is built upon the experience that the Red Cross has gathered with Team Österreich. This is evident in some aspects, most notable in how volunteers are mobilised: in Team Österreich, there is a two-step process of first sending short messages to potential participants and see who reacts, then tweak the candidate pool as required. In RE-ACTA, the principle remains the same, the only difference being the coordinator has more options available (such as real time positions of volunteers) and that volunteers are notified through APP. This procedure is a best practice that has proven itself for gauging how many people are at command's disposal for crowd tasking. Yet from there onwards, TÖ and RE-ACTA follow different paths.

Probably the most obvious difference between the two approaches is the expected level of volunteer involvement. This is closely coupled with RE-ACTA's goal to provide lower entry barriers. RE-ACTA works fast and provides easy access. Potential volunteers may sign up at any time through the web. As soon as that is done, they are eligible to receive mobilisation requests. There is no need to attend introduction courses or briefings. Tasks are supposedly shorter in RE-ACTA (compared to TÖ), as they are targeted at crowds local to the area of operation, meaning little to no travel time is required. In short, RE-ACTA offers low entry barriers by providing fast and easy access to volunteer work through ICT.

By taking into account only data that was explicitly requested through tasks, the quantity of information is lessened compared to crowd sourcing approaches that facilitate spontaneous volunteer contributions. However, we claim that its relevance and usability for automated processing is increased. During our evaluation of the demonstrator, coordinators (each of them experienced in disaster management scenarios) working with the system to gather data from the field were very positive towards to the possibilities it offered them. Especially the visualisation of content was received favourable. This would not be possible without defining a data structure that volunteers need to adhere to and at the same time limiting the amount of data by only consulting that which was specifically asked for.

So with RE-ACTA, we have seen a shift towards an ICT-centred form of volunteer management. It serves different needs than Team Österreich, being complementary rather than a rival or successor, and points out a new way to approach crowd tasking for disaster mitigation. Evaluation under exercise conditions in the field has shown the RE-ACTA approach to be valid and having good acceptance from users. However, this shift towards an ICT-focused process has implications we want to address.

4.2 Raising Resilience

Resilience is the ability of individuals, communities, organisations, or countries exposed to disasters, crises, and underlying vulnerabilities to: anticipate, reduce the impact of, cope with, and recover from the effects of adversity without compromising their long term prospects [17]. Resilience is a social function, which is more than just relying on good infrastructure. Raising resilience can be achieved by various measures, such as healthy living, disaster risk reduction, preparedness or first aid

trainings. Following the social theories of Pierre Bourdieu [5], resilience can be explained with personal and social skills, arising from wealth, education, and social recognition. They can be shared and used as (social-) network capacity in groups. In order to raise resilience within this project, it is important to provide support for particularly vulnerable target groups, or not to exclude these segments of the population through the choice of technology, language, or user interface.

Segregation as a social phenomenon

Segregation is a sociological process of rising inequality in society. In the narrower sense, it describes the inequality of opportunities and possibilities for different people. Groups of people who are socially excluded often do not only have fewer opportunities, but are particularly vulnerable, especially in the context of disasters and crises [1]. In modern societies the risk for crises and disasters seem to be the same for rich and poor, as Ulrich Beck [3] proclaimed, but the effects differ significantly depending on where in the world and in which milieu of the society a person is living [4]. This means that disasters, which affect a country or society as a whole, normally have more devastating effects in social groups which are more vulnerable. On the one hand, this happens because their resilience is particularly low. On the other hand, the ability to cope with those effects is also significantly lower. Both phenomena tend to raise segregation and the difference in opportunities and possibilities in disaster-prune societies. Sociologists are calling those phenomena perpetuating differences. One of the basic aims for the RE-ACTA tool, consequently, is to prevent any additional exclusion of social milieus by the use of certain technologies.

4.3 Inclusion as aim

As RE-ACTA fosters and relies on ICT to raise disaster resilience, we tried to implement the perspective of vulnerable groups within this technology. The main focus of these measures (survey, focus groups) has been preventing further segregation through this technology. Yet the decision to use mobile platforms for RE-ACTA is already the first exclusion of specific target audiences, namely people without the possibility to use these devices in the first place. Still this system design decision is to be seen against the background of ever-growing, global pervasion of mobile phones[6]. We expect this particular form of segregation to be temporary and have vanished in some year's time.

In the social sciences, there are large numbers of different approaches to the issue of social inclusion [2]. Especially in discourses on the topics of poverty, migration, health, and disability, but also in diversity, there are different conceptual and theoretical models for inclusion. Generally, it is about the ways to prevent social exclusion and to increase the possibilities of social participation. During the RE-ACTA project we tried to understand the concept of social exclusion and segregation, and the underlying phenomena, to include as many social milieus into the process as possible and to prevent building higher barriers towards vulnerable groups. We are in the process of establishing guidelines for user interface design and the language that is being used, in order to include as many social milieus as possible, thus avoiding the target audiences becoming a form of digital elite. For example, we aimed to provide all the tools necessary for executing tasks, bundled with the mobile app. This way, users do not need to know how to, e.g., use the camera app on their phone. Everything should be provided for them from within APP. This also includes interactive maps or even navigation, which we have found to be very important tools during an evaluation in the field. Furthermore, when designing for inclusion in disaster management, one should not stop with the technological aspects of crowd tasking; equally important is the way these tools are being used. Investigation, through focus groups, of potential issues

[6] http://data.worldbank.org/products/wdi, last visited 2015/6/8

regarding inclusion have shown the importance of using precise, understandable language when defining tasks for volunteers. Such a thing cannot be solved through technology, but rather awareness and training of operators.

Because RE-ACTA is still ongoing as of the time of this writing, we cannot yet provide a complete set of guidelines to avoid segregations and foster inclusion – this will be forthcoming in a future work. Furthermore, the concepts conceived from RE-ACTA as well as the insights gained from implementing and evaluating them will support and facilitate further research and development in the European FP7 project DRIVER[7].

5 CONCLUSION

In this paper, we have presented two initiatives for crowd management and community engagement that are currently being conducted in Austria. On the one hand, there is Team Österreich (TÖ), which has been active since 2007 and was born of the need to better manage volunteer convergence. On the other hand, there is RE-ACTA, an on-going research program that tries to use the organisational concept of TÖ and apply it to the use of new media for crowd tasking. This move has shown both the great potential of ICT, but also the importance and relevance of social phenomena like inclusion and segregation when using these technologies.We argue that, when designing for crowd tasking, it is necessary to be aware of the issues surrounding segregation and inclusion. Using ICT may be of great benefit to the population as well as relief organisations. Yet relying exclusively on any one technology, while helping one segment of the population, may be of detriment to those without access to it, who are thus excluded. This is even true in the broader scope of ICT usage in disaster management in general.

As far as disaster management as a whole is concerned, we should consider these issues for the long term, so that we do not create further divide and gaps among the population. We need to consider disaster management as the multidisciplinary, multi-stakeholder topic that it is. It cannot be approached solely by looking at it through one single perspective, from one single field of research. Aspects like inclusion and segregation cannot be solved by technology alone. Thus to finally answer the titular question, we conclude that communication technology in disaster situations can be heaven if used responsively – yet caution should be taken to not narrow our view too much on technological aspects.

6 ACKNOWLEDGEMENTS

RE-ACTA has been funded by the Austrian security research programme KIRAS of the Federal Ministry for Transport, Innovation and Technology (bmvit).

REFERENCES

[1] Adger, W.N., Hughes, T.P., Folke, C., Carpenter, S.R., and Rockström, J. Social-Ecological Resilience to Coastal Disasters. *Science 309*, 5737 (2005), 1036–1039.

[2] Balz, H.-J., Benz, B., and Kuhlmann, C. Soziale Inklusion. *Grundlagen, Strategien und Projekte in der Sozialen Arbeit*, (2012).

[3] Beck, U. *Risk society: Towards a new modernity.* Sage, 1992.

[4] Beck, U. Weltrisikogesellschaft. *Auf der Suche nach der verlorenen Sicherheit. Frankfurt aM: Suhrkamp*, (2007).

[7] http://driver-project.eu/ last visited 2015/06/10

[5] Bourdieu, P. Ökonomisches Kapital, kulturelles Kapital, soziales Kapital. In *Soziale Ungleichheiten*. 1983, 183–198.

[6] Cobb, C., Mccarthy, T., Perkins, A., et al. Designing for the Deluge : Understanding & Supporting the Distributed , Collaborative Work of Crisis Volunteers. (2014), 888–899.

[7] Hofmann, M., Betke, H., and Sackmann, S. Hands2Help – Ein App-basiertes Konzept zur Koordination Freiwilliger Helfer/ Hands2Help – An App-based Concept for Coordination of Disaster Response Volunteers. *i-com 13*, 1 (2014), 36–45.

[8] Lanfranchi, V., Wrigley, S.N., Ireson, N., Ciravegna, F., and Wehn, U. Citizens ' Observatories for Situation Awareness in Flooding. *Proceedings of the 11th International ISCRAM Conference*, (2014), 145–154.

[9] Malli, A. Die sozialen Aktivitäten von Ö3 und das Team Österreich als Paradebeispiel für Public Value. In *Die multimediale Zukunft des Qualitätsjournalismus*. Springer, (2013), 155–169.

[10] Neubauer, G., Nowak, A., Jager, B., et al. Crowdtasking – A New Concept for Volunteer Management in Disaster Relief. In J. Hřebíček, G. Schimak, M. Kubásek and A. Rizzoli, eds., *Environmental Software Systems. Fostering Information Sharing SE - 33*. Springer Berlin Heidelberg, 2013, 345–356.

[11] Palen, L., Vieweg, S., Liu, S.B., and Hughes, a. L. Crisis in a Networked World: Features of Computer-Mediated Communication in the April 16, 2007, Virginia Tech Event. *Social Science Computer Review 27*, (2009), 467–480.

[12] Quarantelli, E.L. *Disaster planning, emergency management and civil protection - the historical development of organized efforts to plan for and to respond to disasters.* Delaware, 2000.

[13] Schimak, G., Havlik, D., and Pielorz, J. *Environmental Software Systems. Infrastructures, Services and Applications.* 2015.

[14] Starbird, K. and Palen, L.Working and sustaining the virtual “Disaster Desk.” *Proceedings of the 2013 conference on Computer supported cooperative work - CSCW ’13*, (2013), 491.

[15] Starbird, K. and Stamberger, J. Tweak the tweet: Leveraging microblogging proliferation with a prescriptive syntax to support citizen reporting. *Proceedings of the 7th International ISCRAM Conference – Seattle, USA, May 2010*, May (2010), 1–5.

[16] Vieweg, S., Hughes, A.L., Starbird, K., and Palen, L. Microblogging during two natural hazards events. *Proceedings of the 28th international conference on Human factors in computing systems - CHI ’10*, (2010), 1079.

[17] The road to resilience. Bridging relief and development for a more sustainable future. 2012. http://www.ifrc.org/PageFiles/96178/1224500-Road to resilience-EN-LowRes %282%29.pdf.

GERMAN EFFORTS ON ESTABLISHING A SPACE SITUATIONAL AWARENESS CAPABILITY

K. Auras[1], G. Braun[2], I. Heinisch[4], S. Huland[3], K. Pixius[4], T. Spangenberg[5]

[1]Bundesministerium der Verteidigung (BMVg), [2]Deutsches Zentrum für Luft- und Raumfahrt, Raumfahrtmanagement, [3]Kommando Luftwaffe, [4]Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw), [5]Weltraumlagezentrum

Abstract

Almost ten years ago, initial considerations and studies were carried out to pave the way for the set-up of own national Space Situational Awareness (SSA) capabilities for the Bundeswehr. Since then, a bunch of different efforts was launched spanning from R&D, establishing a nucleus for a military SSA-centre, making sensors available, and also embracing efforts of various international co-operations.

Presently, from a Bundeswehr point of view, some of these efforts were identified as dead-ends, while others are regarded as only at a pre-mature level for an operational use, yet. However, the Bundeswehr in cooperation with DLR establishes a national SSA capability and takes a first step for a contribution to international SSA.

This paper presents an overview of the efforts undertaken so far, the present situation of military SSA in Germany and concludes with a view of the potential way ahead. For the time being, the Bundeswehr relies heavily on research institutes like DLR or Fraunhofer, while the ministries of defense (BMVg) and economics (BMWi) are preparing the setting to motivate private enterprises to engage in SSA technologies.

Keywords: space situational awareness, Bundeswehr, laser-tracking.

1. INTRODUCTION

With the rising consciousness that space assets, e.g. satellites, or the International Space Station ISS, not only provide valuable contributions to the scientific progress, but also are absolutely vital for modern economies, the need for space situational awareness (SSA) aroused.

Meanwhile, it is publicly noted that space debris imply a considerable threat to space assets and even Hollywood has brought the matter on celluloid with its 2013 released movie ‘Gravity’.

Despite the overwhelming importance of the topic, many nations, including Germany, rely basically on the United States’ Strategic Command that provides SSA data on ca. 16.000 orbital space objects through their web site[1].

In Europe, SSA activities were initially driven by the European Space Agency (ESA)[2] thereby complementing its space debris expertise. However, due to the fact that a detailed awareness and analysis of some space objects for obvious reasons is less suited for organisations used to handle only non-classified information, the Bundeswehr decided to investigate on SSA almost ten years ago.

Since then, capacity and knowledge building was introduced in the Bundeswehr that meanwhile has led to the establishment of the German Space Situational Awareness Center, (‘Weltraumlagezentrum’) located in Uedem, which in run in close cooperation with the Space Administration of the German Aerospace Center (DLR RFM).

This paper presents a short overview about previous efforts and current activities on the Bundeswehr approach to SSA with a special focus on technological challenges. It concludes

with an outlook, on how these efforts could pave the way for more dedicated contributions to the international SSA community.

2. PREVIOUS EFFORTS

With the launch of Bundeswehr owned, but contractor operated, satellites for telecommunications and surveillance, respectively, it became clear, that the Bundeswehr is somehow 'gambling' with the life-time of these assets, since a detailed awareness of the situation in space was not available for the Bundeswehr. Hence, one had to rely on the calculations by the contractors operating the satellites.

When the European Space Agency (ESA) announced to kick-off a preparatory SSA programme, the Bundeswehr took the opportunity and co-financed the German share to that programme. Despite the valuable technological achievements, it soon became clear, that the question on the organisational or institutional governance of a European SSA capability is by far exceeding or even disregarding the requirements of the Bundeswehr. Therefore, the decision was taken to establish a national SSA centre. In a first step only as a precursor or test-bed to explore, if the needed investments in money and personnel proof to be justified. Very soon, the German MoD (BMVg) was backed by the Federal Ministry of Economics (BMWi)[3] and it was decided to run this precursor SSA centre commonly with the DLR Space Administration.

Although, the Bundeswehr has only recently begun to run their SSA centre, it is financing SSA related technologies through its Federal Office for Equipment, Information Technology and In-Service Support (BAAINBw) for many years. While in previous years, mainly the research for advanced radar techniques[4] at the Fraunhofer Institute for High Frequency Physics and Radar Techniques (FHR) was supported, meanwhile also research on laser-tracking techniques at the DLR Institute of Technical Physics[5] is sponsored.

3. CURRENT ACTIVITIES

Building upon experiences that German research institutes has been delivering already for years to e.g. the European Space Agency (ESA), or the Inter-Agency Space Debris Coordination Committee (IADC), the Bundeswehr decided to further investigate and to sponsor these activities with a special focus on SSA, hence supporting its recently established Space Situational Awareness Center ('Weltraumlagezentrum', WRLageZ), which is run in close cooperation with the Space Administration of the German Aerospace Center (DLR RFM).

3.1. Operational efforts

Supported by the Technical University Braunschweig, the Bundeswehr established training courses for 'Space' at its German Federal Armed Forces Command and Staff College in Hamburg. This shall provide young officers with a sound knowledge about space assets for military application in general and space situational awareness in particular. The then skilled personnel is thus prepared for assignments to the WRLageZ.

As the significance of SSA was obvious to the BMVg as well as to the BMWi, the Bundeswehr through its BAAINBw is equipping the WRLageZ with the required hard- and software, while through DLR RFM co-equipping was realised to enable a total of ca. 30 military and scientific personnel to operate the WRLageZ.

Multiple national and international cooperations allow for an exchange of relevant data and information thereby respecting the 'need-to-know' approach and classification restrictions.

Despite the rapid establishment of the WRLageZ and its soon after performed operational successes, it has to be recognised that further investment and capability building is necessary to become fully operational and professional in the international SSA community.

3.2. Research and Development

SSA-related research in Germany is mainly (among others) carried out at institutes of the Fraunhofer-Gesellschaft, the German Aerospace Center (DLR), and the Technical University of Braunschweig. While e.g. the ESA[6] at its 'space debris office' is focusing on small sizes space objects, the Bundeswehr is especially looking for technologies suited for tracking of space objects sized > 10 cm orbiting in LEO. Although radar is undoubtedly the best suited technology for SSA, it is also quite expensive in terms of first-installation investment. Therefore, also the laser-tracking techniques are sponsored, which are much cheaper, and could potentially also cover ranges beyond LEO.

3.2.1. Lasertracking

At the Institute for Technical Physics of the German Aerospace Center, research in the field of laser-tracking, sponsored also by the BAAINBw, aims at applying a technique well-known from satellite laser tracking (SLR) to the tracking of space objects, which scales as small as 10 cm, being on orbits only roughly known, and are not equipped with reflectors (as satellites are).

The general concept[7] of this technology is simply that a space object can be first detected by passive-optical means using solar illumination and then be tracked by illuminating it with an intense highly repetitive illumination laser. Backscattered photons are detected by single photon detectors mounted in the receiver telescope. After successful demonstration performed in campaigns at the SLR station Graz- Lustbühel, where space objects sized 1 m were consistently monitored over distances of up to 2500 km, further research is carried out to allow for tracking of smaller objects. Successful observation of cube sats sized 10 cm was already possible in tracking mode. The tracking accuracy in closed-loop mode was reported with ~2 arcsecs, corresponding to 10 m at a distance of 1000 km.

3.2.2. Radar-Technology

The Tracking and Imaging Radar TIRA, operated by the Fraunhofer Institute for High Frequency Physics and Radar Techniques (FHR) is among the most powerful devices in the world to track space objects. Although the radar was originally built in the late 1960s, it is still a highly appreciated tool. Thanks to the implementation of sophisticated algorithms and because of being equipped with a second radar chain operating in the k-band, it is used also for creation of radar-images using ISAR-techniques.

Despite the impressing capabilities of TIRA in terms of tracking and imaging, it is not a suited device for detection and surveillance, i.e. determination of orbits at a first glance. Hence, TIRA has to rely on orbital data, provided by e.g. the JSPOC database or other sources.

In complementing the radar capabilities of TIRA, the DLR RFM has very recently announced[8] that Fraunhofer's FHR was awarded a contract to develop a German Experimental Space Surveillance and Tracking Radar (GESTRA) for research purposes.

3.3. Paving the way

Although SSA has become widely recognised as an important capability not only for the purpose of research & development and in support of safeguarding own space assets, but also as a contribution for the peaceful surveillance of space assets operated by various nations, it is still under review and assessment by German government's decision makers.

Since the ESA as well as the European Commission are also very active in promoting SSA for Europe, it cannot be opted out that Germany will focus its efforts fully towards ESA's SSA programme, in which Germany is already taking part.

However, by investing in new SSA technologies, like laser-tracking, optimising well-established radar techniques, and introducing new radar assets, like a surveillance radar, Germany is on a promising way to catch up with other nations.

4. OUTLOOK

Given that the recently launched efforts, i.e. the WRLageZ, R&D activities, modernisation of existing radar assets, development of new radar assets, turn out to be successful and being evaluated as promising, Germany could enter the international SSA community by end of the decade as a strong and capable provider of SSA data.

Wether these capabilities will be fully shared with others, or run as service providing, remains to be decided.

In any case, SSA relies heavily on highly sophisticated technologies and after the present phase of R&D, heavy investments are required, that turn demonstrators built by research institutes towards professionally designed, built and fielded systems that can only be provided by the industry.

5. SUMMARY AND CONCLUSION

Space Situational Awareness as a pre-requisite for the safety of space assets is meanwhile internationally regarded as important. Consequently, two federal ministries, the BMVg and the BMWi, are jointly investing in this topic and their common approach cumulated in the establishment of the German SSA centre. The Bundeswehr has slightly different requirements towards a comprehensive 'recognised space picture' and is therefore supporting also the research on technologies suited for tracking and also 'radar-imaging' space objects. While research efforts are still ongoing, and a decision on the extent of further investments in this topic in pending, yet, it is probable that the technological hurdles can be taken.

Equipped with basic SSA capabilities that are complemented by advanced surveillance and tracking technologies, German authorities can contribute significantly to bilateral as well as international, or super-national cooperations.

REFERENCES

1 www.space-track.org

2 http://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness

3. "Making Germany's space sector fit for the future - The space strategy of the German Federal Government"; Federal Ministry of Economics and Technology (BMWi). Public Relations/L210115, Berlin. http://www.bmwi.de/DE/Mediathek/publikationen,did=370794.html

4 Ender, J. Leushacke, L. ; Brenner, A. ; Wilden, H.: "Radar techniques for space situational awareness"; IEEE Radar Symposium (IRS), 2011 Proceedings International, Leipzig, 7-9 Sept. 2011, pp.21.

5 http://www.dlr.de/tp/en/desktopdefault.aspx/tabid-10062/17177_read-41487/

6 http://www.esa.int/Our_Activities/Operations/Space_Debris

7 Hampf, Daniel und Wagner, Paul und Riede, Wolfgang (2014) "Optical technologies for observation of low Earth orbit objects"; In: 65th International Astronautical Congress. 65th International Astronautical Congress 2014, 29. Sep - 03. Okt 2014, Toronto, Canada.

8 "Ein Weltraumradar für die Ortung von Trümmern im All"; accessed 10.6.2015; http://www.dlr.de/dlr/desktopdefault.aspx/tabid-10081/151_read-13251/#/gallery/19080

SYNTHETIC BIOLOGY – THE NEXT "DUAL USE" RISK!/?

Dr. Annika Vergin[1], Dr. Erik Riebeseel[2] and Dr. Olaf Theiler[3]

[1] *annikavergin@bundeswehr.org*
Planungsamt der Bundeswehr, Referat Zukunftsanalyse,
Oberspreestrasse 61L, 12439 Berlin (Germany)

[2]*erikriebeseel@bundeswehr.org*
Planungsamt der Bundeswehr, Referat Zukunftsanalyse,
Oberspreestrasse 61L, 12439 Berlin (Germany)

[3] *olaftheiler@bundeswehr.org*
Planungsamt der Bundeswehr, Referat Zukunftsanalyse,
Oberspreestrasse 61L, 12439 Berlin (Germany)

Abstract

With methods of synthetic biology (SynBio) simple biological systems can already be generated artificially. The long term goal of SynBio science is to create artificial com-plex biological systems with new defined properties.

In addition to a wide range of profitable applications these technologies also have the potential for abuse und dangers. The consequences of it besides health and environmental implications can also have important political impact and high economic damage potential.

The future analysis branch of the Bundeswehr Planning Office will introduce the ongoing work on this field of interest. The current study will answer the following question: should SynBio be considered as an own weapons system or just as an evolution of the already known B and C weapons. The answer will have influence on the necessary responses in armed forces capabilities and concepts regarding SynBio.

Keywords: Synthetic biology, dual use, German armed forces, future analysis, Resilience, B and C Weapons, crisis management

1 INTRODUCTION

The quite new area of research Synthetic biology (SynBio) is a conglomerate of different scientific fields like as molecular biology and organic chemistry but also engineering and information technology. With methods of SynBio simple biological systems can already be generated artificially. The long term goal of SynBio science is to create artificial complex biological systems with new defined properties. In addition to a wide range of profitable applications these technologies also have the potential for abuse und dangers. On the one hand aspects of the deliberate as well as the unintentional sturgeon components are to be considered. On the other hand the dual use opportunity of SynBio technics can lead to misuse of the technologies such as dual use research of concern/DURC. The consequences of it besides health and environmental implications can also have important political impact and high economic damage potential.

2 PROJECT VISION AND GOALS

Against this background it is clear that the German armed forces have to deal with the issue. Obviously SynBio is a new field of research where we will have to keep our own ability to judge on a high level. As a first step we have to identify our own state of knowledge and have to expand it. Existing knowledge gaps have to be closed. Second we have to answer

questions like: whether SynBio should be considered as an own weapons system or just as an evolution of the already known B and C weapons. Will the German armed forces need new structures or regimes to handle SynBio systems and technologies and how are our partners and enemies dealing with the subject? Where are the biggest harm potentials? And last but not least will be a change in current conflict pictures, scenarios and concepts necessary or do we need new ones? To answer these questions the future analysis branch of the Planungsamt der Bundeswehr has started a new project in February 2015. The project has an elapsed time of six months. In this paper the concept of the project will be introduced.

3 PROJECT METHODS

The project is planned in four sections. Each of these sections will be handled with different cooperation partners to assure a high quality and full autonomy of the results.

3.1 Identification of main areas of interest and definition of study design

In a previous project for SynBio the following four general areas of interest were identified: research in, detection of, response to and forensics of SynBio. As first step a literature research should give an overview about the main activities in SynBio. Second the results have to be summarised in specific characteristics for each research activity. Each characteristic has to include general description, stage of development, dual use options, detection options if known, security policies if existent, side effects and other collateral information. On the basis of these characteristics it should be possible to identify research activities with potentially high security impact. The identified SynBio areas would be analysed with methods mentioned in 4.3 and 4.4.

3.2 Attempt to transfer current Counter B and C weapon concepts to artificial biological systems

In parallel we are going to clarify whether and how current Counter B and C weapon concepts can be transferred to artificial biological systems. Here we will work together with B and C weapon specialists of the German armed forces. On the background of the characteristics from 4.1 we will compare SynBio systems with B and C weapons to identify commons and differences. At the same time we will evaluate the full range of counter concepts in order to evaluate their ability to be transferred to SynBio systems.

3.3 Scenario Building

A main tool for future analysts is the scenario analysis method. In the past we developed different Conflict pictures with this method. In order to assess the potential damage of the new emerging technologies of SynBio, we will examine our stock of Conflict pictures whether they can be adapted to cover the use of artificial biological systems. If this seems not to be possible we will need completely new scenarios in order to fully capture the disruptive potential of SynBio technologies. If that is the case we will probably have to start a full new scenario analysis method cycle.

3.4 Risk and damage analysis

As last step a computer based combination of a risk and a damage analysis will be performed for a selected group of scenarios.

We want to do this analysis in cooperation with experienced partners from the civil security sector. The reason behind is simply our hope to profit from existing experiences especially in the field of critical infrastructure simulations.

4 RESULTS

The expected results should give us the opportunity to judge about SynBio technologies, especially to identify the dual use opportunities (positive and negative) and potential implications for security purposes. If SynBio is a new Dual Use Risk like mentioned in the headline it will be important to increase the vigilance in the German armed forces, in institutions and the general public. Once the danger is identified the work on appropriate pre-emptive or counter measures can start, either by adaptation of old regimens or the build-up of adequate new regimes.

5 CONCLUSION

SynBio technologies are an important field of interest in future generally and in future security aspects particularly. With the current short study of the future analysis branch of the Planungsamt der Bundeswehr we want to contribute to the discussion of the benefits and the dangers of SynBio technologies and systems. The main focuses of our work are security aspects and the implications of the dual use risk. Our work is to support the German armed forces in the first place and other security institutions as well in dealing with the challenges of the future.

ENHANCED MARITIME TRAFFIC PICTURE FOR THE CANADIAN ARCTIC

Giulia Battistello, Martin Ulmke, Camilla Mohrdieck

{giulia.battistello, martin.ulmke}@fkie.fraunhofer.de
Fraunhofer FKIE, Sensor Data and Information Fusion, Wachtberg, Germany

camilla.mohrdieck@airbus.com
Airbus Defence and Space, Data Fusion Concepts, Integration & Tests, Ulm, Germany

Abstract

The Northwest Passage (NWP) in Canada's arctic region represents an interesting and promising navigation path for connecting the Atlantic and Pacific Oceans, since it allows saving nautical miles and costs with respect to the conventional routes. However, the continuous changes in ice conditions, the extremely harsh weather conditions (e.g. low visibility, freezing spray and high winds) and the limited infrastructure (communication gaps, lack of sensors and navigation aids) make the whole NWP area unsafe and extremely risky for navigation. The goal of the Canadian-German research project PASSAGES (Protection and Advanced Surveillance System for the Arctic: Green, Efficient, Secure) is to develop a concept for a traffic monitoring system, which minimizes the navigation risks for vessels sailing in and through the NWP. As first objective, this monitoring system should provide a continuous and comprehensive traffic picture for those vessels navigating in the area, which at present is often fragmented and characterized by information gaps due to the scarceness of monitoring sensors in the Canadian Artic. Subsequently, navigation risk maps are generated or improved and used as support for the navigation itself (i.e. route planning). This paper focuses on the first objective. Specifically, real and simulated vessel traffic data from heterogeneous sensors (shore and space-based) are considered for some exemplary realistic and "strategic" operational scenarios and locations in the NWP, such as entry/exit points, choke points and open water corridors. Suitable positions of in-situ sensors are defined on the basis of sensor performance models. The aim is to guarantee the continuity of the vessel traffic monitoring service by combining and fusing complementary multisensor data and contextual information. The improvement of the maritime situation picture is demonstrated for an operationally relevant scenario.

Keywords: maritime traffic monitoring, passive radar, PASSAGES project.

1 INTRODUCTION

The combination of technological, economical, and climatic factors nowadays leads to a growth in maritime traffic in the Arctic. The observed reduction in ice coverage, thickness, and duration - combined with improved ship building - facilitates Arctic shipping for longer periods of the year and at higher latitudes. This enhances the investment in – and operation of - resource extraction vessels, transarctic shipping, vessels for resupply of the local communities, cruise ship and adventurer tourism in these waters. On the other hand, the remoteness, the harsh weather and ice conditions, and the lack of emergency response facilities lead to serious risks for the ships operating in the Arctic, as well as for communities and the environment. It is therefore important to monitor continually the vessel traffic in the Arctic in order to provide government agencies and mariners with the degree of Maritime Domain Awareness (MDA) that they need to conduct safe operations and voyages and to manage risks such as maritime accidents or spills or transiting of illegitimate vessels.

The Canadian-German research project PASSAGES (Protection and Advanced Surveillance System for the Arctic: Green, Efficient, Secure)[1] aims at specifying the requirements and the design of a novel traffic monitoring system that is able to provide a continuous and comprehensive MDA for those vessels navigating in Canadian arctic waters. At present, the backbone for MDA in the Arctic is the Satellite-based Automatic Identification System (S-AIS)[2]. Operating in the VHF range, the AIS transponders on board ships are a very effective cooperative data source for monitoring coastal and territorial waters from shore-based base stations. Through the installation of ad hoc AIS receivers on board a network of Low Earth Orbit satellites, the satellite based AIS (S-AIS) has extended the coverage of the system over the global seas, and it is now a powerful, standardized and proven technology[3] for vessel traffic monitoring. It turns out, however, that S-AIS alone is not sufficient to provide continuous and comprehensive MDA. Reasons are (i) temporal gaps due to limited satellite coverage and low reporting frequency, (ii) AIS transponders are not mandatory for small vessels and, (iii) the existence of false AIS reports due to technical failure or even spoofing.

It is therefore necessary to research additional sensors and techniques that are able to complement the data provided by the S-AIS. Space borne sensors such as Synthetic Aperture Radars (SAR) and optical imagery can be considered for the scope, even if they are also subject to observation gaps due to satellite orbits. For locations of high interest (e.g. choke points or entry/exit points) or for specific operations (e.g. search and rescue), local sensors such as active and passive radar systems (ground-based, air- or shipborne) can be considered to supplement the space-based sensor data. However, the use of local sensors introduces challenges in terms of installation, operations and maintenance costs due to the remoteness of the considered Arctic areas (e.g., no access point to the power grid). The collected sensor data can be fused in order to compile a common operational picture, which is the basis for MDA. In addition, the collected information can be combined with bathymetric data and ice charts in order to (i) predict vessel positions and bridge possible sensor coverage gaps, and (ii) optimize the ship route by minimizing the navigation risk. Ice charts, bathymetric maps, historical traffic data and ice classes of ships contribute to the risk maps, which compute integrated risk indices for specific areas and times of operation.

In this paper we focus on one exemplary scenario, which is the entry/exit point to the Frobisher Bay and Hudson Bay of the NWP. Through a preliminary analysis of historical data we demonstrate the limits of the current MDA capability, and subsequently suggest a strategy for enhancing it through the use of passive sensors and illuminators of opportunity (i.e., GSM base stations and VHF radio stations) in order to implement a covert surveillance for non-cooperative vessels, minimize the impact on the environment (e.g. electromagnetic pollution) and the costs for future implementation.

This paper is organized as follows. The analysis of historical data for a reference scenario is reported in Section 2, while the considered sensors are recalled in Section 3. Section 4 introduces the reference scenario and the approach suggested for enhanced MDA. Finally, some results for the optimized procedure based on historical data are shown in Section 5.

---

[1] PASSAGES website: http://passages.ie.dal.ca/

[2] AIS is a mandatory navigation safety communication system under the provisions of the Safety of Life at Sea Convention, which requires ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages, and all passenger ships to be fitted with transponders that broadcast the position of the ship and the identification number of the ship. (http://www.exactearth.com/technology/satellite-ais/)

[3] Several companies provide S-AIS data service in near-real time to authorities and private users. The distributed information consists of standard AIS messages containing position, kinematics, and ship identification information

2 TRAFFIC ANALYSIS

The geography of the NWP presents a limited set of options for a transiting vessel, which varies according to the ice and weather conditions and the season of the year. The analysis of historical data on maritime traffic (e.g. S-AIS data collected in the years 2011-2013) led to the identification of the major traffic routes in the Arctic (Figure 2-1):

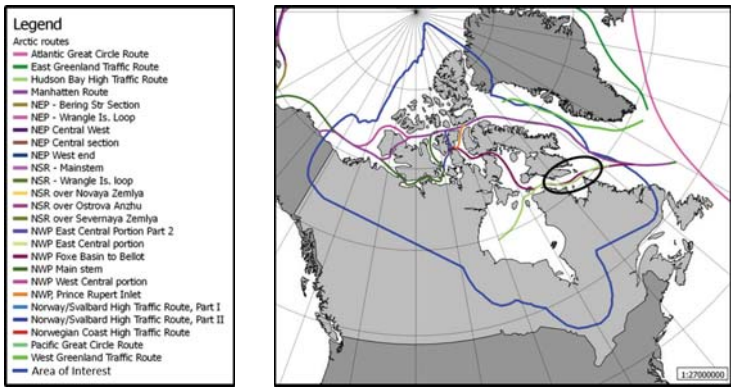


Figure 2-1: The Arctic Ocean with Routes

In this paper we focus on the high traffic route to the Hudson Bay and Frobisher Bay (black circle in Figure 2-1) as the reference corridor for demonstrating one MDA Service investigated within the PASSAGES project. Figure 2-2 shows the maritime traffic obtained from the available S-AIS data in that area, covering a time period of 8 days in August 2013.

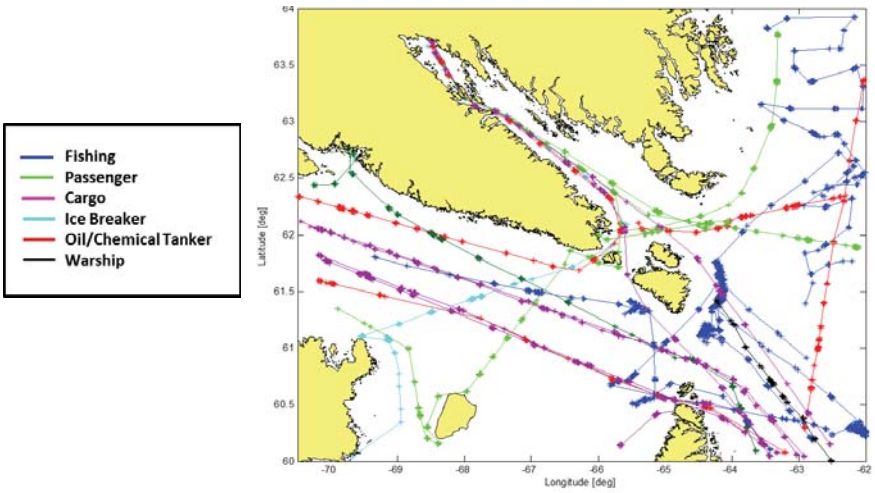


Figure 2-2: S-AIS Dataset for August 2013

The analysis led to the identification of different types of vessels crossing the selected area, such as fishing and passenger vessels, cargo ships and tankers (occasionally transporting hazardous materials), which have similar or different routes according to their specific destinations. Whatever the ship class, the S-AIS measurement reports come as bursts (groups of crosses in Figure 2-2), and inter-bursts gaps of 90 minutes (segments connecting the crosses) are experienced on average. This clearly hinders the desired persistent MDA capability, since the risk of “inaccuracy” of the vessel track during the uncovered intervals is high. For this reason, the S-AIS tracks have to be realistically interpolated in order to define preferred – or most likely - routes that the ships might have used. In Section 4 we explain how the entire data, observed and interpolated, is used to optimize the persistency of MDA. The result of the interpolation shows how the vessel behaviors largely diverge according to their class, their goal and destination. For example, while cargo and passenger ships proceed along well defined routes, fishing vessels are characterized by irregular traffic patterns.

In order to characterize the routes, we associated to each cell in the map of the Area of Interest (AoI, approximately [300km x 300km]) a velocity vector with heading and amplitude, which is the averaged value of all the vessel tracks passing by that cell. The cells that are not crossed by the available tracks are simply labelled with “no preferred route”. An example related to a smaller region in the AoI is shown in Figure 2-3.

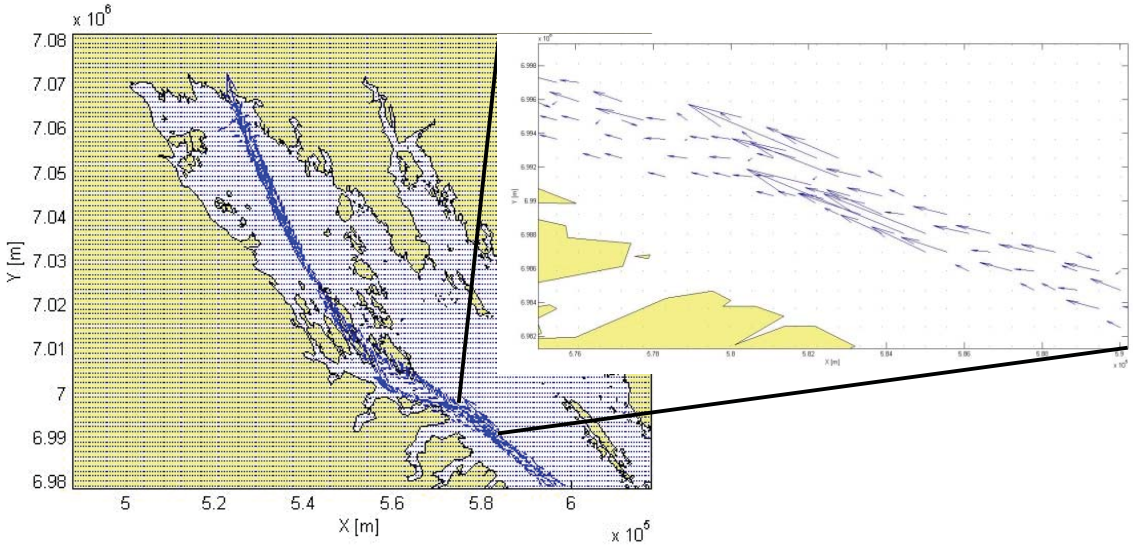


Figure 2-3: Preferred routes and velocity vectors extracted from S-AIS Dataset

The information on velocity vectors and favorite vessel routes is fundamental for optimizing the sensor layout, as explained in the following Section.

3 IN-SITU SENSORS CONTRIBUTING TO MDA

Active radars are used for maritime traffic control and maritime traffic services, such as Vessel Traffic Service (VTS), since decades. Recently, passive means for vessel detection and tracking have gained attention due to their clear advantages with respect to active systems: (i) reduced electro-magnetic pollution and interference to pre-existing radio-frequency systems, (ii) reduced installation and maintenance costs, and (iii) not subject to authorization by safety authorities. In this paper we refer to Passive Radars (PRs) that exploit illuminators of opportunity (i.e., signals already present in the surveillance area) through Passive Coherent Location (PCL) techniques ([1]). An example is the GAMMA system developed by Fraunhofer FKIE ([2]), which relies on signals emitted by GSM base stations. The principle for detecting a moving vessel is straightforward: the passive radar receiver (RX) intercepts the direct signal coming from the base station (TX) and simultaneously any echo of such signal coming from the monitored area. If the echo from a particular angle of arrival and cell in range is Doppler-shifted with respect to the direct GSM signal, it means that an object, which caused the reflection, is moving in that cell (our “moving target”). The presence of a Doppler component for a moving target largely depends on the observation geometry between transmitter, receiver and target. Specifically, all targets moving tangentially to the iso-range curves (e.g. ellipses with foci located at TX and RX), yield a zero “radial” component of the velocity, hence a signal echo with zero Doppler. Therefore, the radar cannot detect them. This effect is taken into account in the sensor performance model. Other PCL techniques exist and exploit other illuminators of opportunity, such as VHF radio transmissions, digital television (DVB-T), etc. The VHF PR is also of main interest for maritime traffic monitoring, due to the transmission characteristics of these stations (position, power), even if the spatial resolution is somehow limited and varies over time according to the transmission.

4 IMPROVED MDA BY USING A PASSIVE RADAR NETWORK

The main objective of the innovative monitoring service in the areas of Frobisher Bay and Hudson Strait is to ensure a higher update rate of maritime tracks (currently given only by intermittent S-AIS reports) in the common operational picture through a minimal deployment of new sensors. This is needed for the user in order to check routes and the behaviours of the observed vessels against: (i) prohibited activities or perpetration of activities in prohibited areas (e.g. illegal fishing), (ii) navigation in risky areas (e.g. presence of ice), (iii) deviation from the declared route (e.g. vessels transporting hazardous materials, passengers ships) and (iv) oil spills. The pre-requisite is to reduce the gaps in the measurements in order to have an improved average track update rate that is sufficient to the goals listed above. Moreover, information of non-cooperative vessels (e.g. not equipped with AIS or not using it) should also – partially – be made available to the service user, without the need of deploying visible radar installations ("covert" tracking). Due to the expected stringent requirements for installation and maintenance of a newly deployed sensor network, we analyse hereinafter the advantages coming from the use of an **optimized network of passive sensors** that exploit different illuminators of opportunity (GSM base stations, VHF radio stations). Such sensors provide measurements in terms of position and velocity of moving vessels, which can be merged with the S-AIS reports to provide the higher refresh rate for the track. The feasibility for such design depends on the selection of the sensor type, the availability of the illuminators (i.e. transmitters), their relative geometry and the specific traffic scenario, which are taken into account in our sensor performance model.

4.1 Service Design

The setup of the entry-point monitoring service is tackled through different steps. First of all the Area of Interest (AoI) and the reference traffic picture is defined on the basis of historical data (Figure 2-2). The vessel kinematics (e.g. position, course over ground and speed over ground) and the vessel type (e.g. cargo, tanker, fishing, passenger, etc.) are relevant for the design of transmitters-receiver configurations. Specifically, this requires an iterative analysis. The first step foresees the identification of available transmitters in the AoI (e.g. already existent GSM base stations and/or VHF radio stations) and the deployment of the passive receiving station, together with the specification of their major characteristics and operative parameters (e.g. position, height, orientation, operative frequency, transmitting power, etc…). Then the evaluation of the vessel detection probability (P_D) is carried out for each TX-RX pair. To this aim the Bistatic Signal to Noise Ratio (SNR) is calculated for the entire AoI under the assumption of a stationary target, whose Radar Cross Section (RCS) is constant throughout a single radar scan (e.g. Swerling I Model) and for a given Probability of False Alarm (P_{FA}). In addition the P_D is affected by the target Doppler as the observation geometry and the velocity vector set a Minimum Detectable Velocity (MDV) for that configuration. If the achieved performance is not satisfactory, new transmitters are introduced and the configuration is iteratively optimized. Then, passive radar measurements are simulated for the reference traffic picture given by interpolated Satellite AIS data, and PR tracks are generated by resorting to a Multi Hypothesis Tracking algorithm (MHT, [3]). Finally, the passive radar tracks and the S-AIS tracks represent the inputs for the data fusion stage, which outputs multi sensor vessel tracks with enhanced persistence and quality. It has to be stressed that the results showed in this paper deal with the design of the transmitter-receiver configuration only.

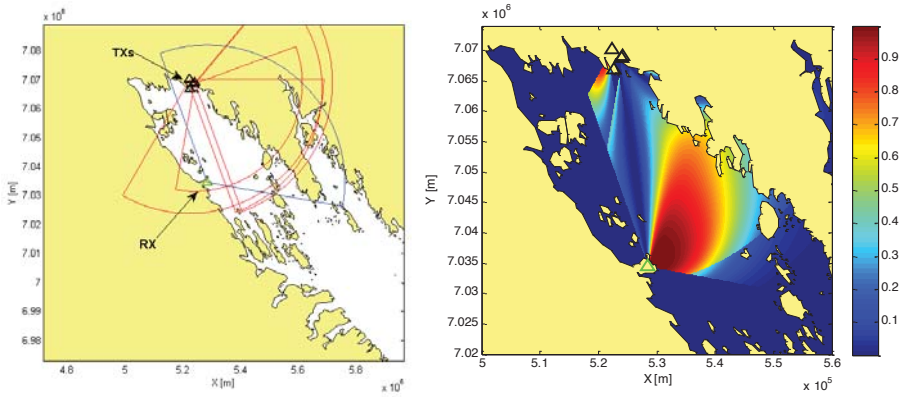
4.2 Design Configuration

The definition of the bistatic radar geometry in the AoI is a crucial point in the service design. Given its direct impact on the vessel track estimation process, the choice of a

proper configuration should be done with the aim to maximise the target detection capability (P_D) along the entire vessel route. For this reason, the optimisation of the TX-RX geometry and the choice of the illuminator of opportunity have been conducted for small regions in the AoI. Figure 4-1 reports an example of this optimization process. Specifically, TX-RX geometries are reported in the left figures, while the cumulative P_D maps are shown in the right side.

Configuration 1

4 GSM Base Stations are present in few km^2. The RX is located in the West shore of the Bay. As per TX-RX mutual visibility, only 2 out of 4 transmitters can be used. The direct path between the TX and RX represents a blind zone for the target detection. For this geometry, the route to enter/exit the Iqaluit port is not covered.

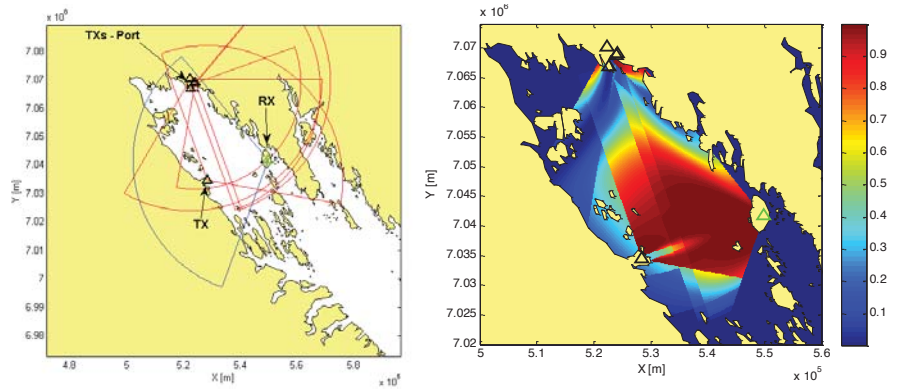


Simulation Param.

TX
2 GSM @1900MHz
Field of View = 120°
RX
BW = 83.5KHz
Angular Res = 3.2°
Target:
RCS = 100 m2
Height = 20 m
MDV = 4 m/s
P_{FA} = 10^-3

Configuration 2

The positioning of the RX on the opposite coast allows using all the 4 GSM Base stations located in Iqaluit. Moreover, the blind zone for TX-RX direct path is located very close to the East coast, leading to higher P_D values wrt the previous configuration along the route to/from the port. The installation of an additional GSM Base Station (opposite to the RX) allows extending the target detection to the area close to the West coast.

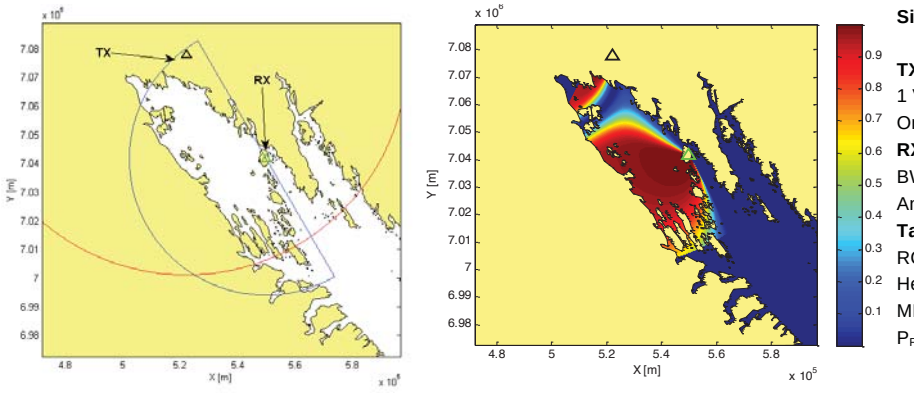


Simulation Param.

TX
5 GSM @1900MHz
Field of View = 120°
RX
BW = 83.5KHz
Angular Res = 3.2°
Target:
RCS = 100 m2
Height = 20 m
MDV = 4 m/s
P_{FA} = 10^-3

Configuration 3

A VHF transmitter is the only illuminator of opportunity in the area. The coverage in range is better than the GSM case but suffers from poor angular resolution.



Simulation Param.

TX
1 VHF @100MHz
Omnidirectional
RX
BW = 15KHz
Angular Res = 10°
Target:
RCS = 100 m2
Height = 20 m
MDV = 4 m/s
P_{FA} = 10^-3

Figure 4-1: Optimization Process for the Choice of TX-RX Geometry

5 REAL DATA APPLICATION

If we consider the entire route of a vessel entering/exiting the Frobisher Bay from/to the Davis Strait and try to predict the improvement coming from the deployment of MDA Service in that area, we can use the design guidelines described in Section 4 and then observe what detection probability is achieved along this route. The optimization process for the sensor layout is currently not yet completed, but just by observing some of the intermediate results, the advantage is evident. Figure 5-1 shows the TX-RX geometries for three relevant areas along the scenario and the correspondent P_D maps, which include the vessel routes of the real data set.

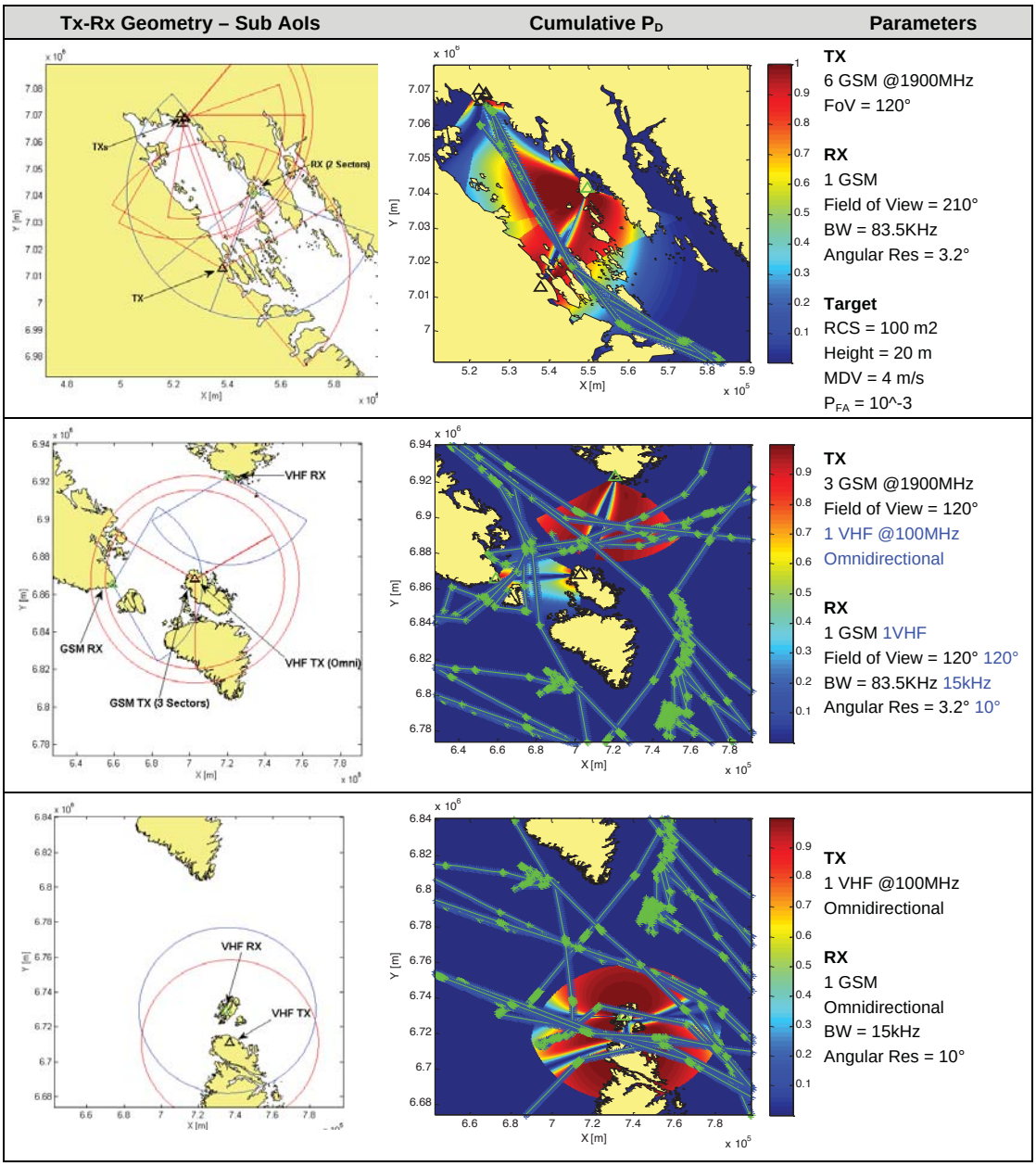


Figure 5-1: TX-RX Geometries and P_D Maps for selected areas in the scenario

Figure 5-2 (b, c and d) show the resulting "performance level" of the service for three vessels (passenger, tanker and cargo), whose routes are depicted in Figure 5-2 (a). Specifically, blue plots show the sensors data availability (both from S-AIS and PR) along the vessel route, while red plots show the P_D values for each vessel when PR measurements are the only ones in a given time instant. It is evident the gap-filling effect resulting from the PR sensors.

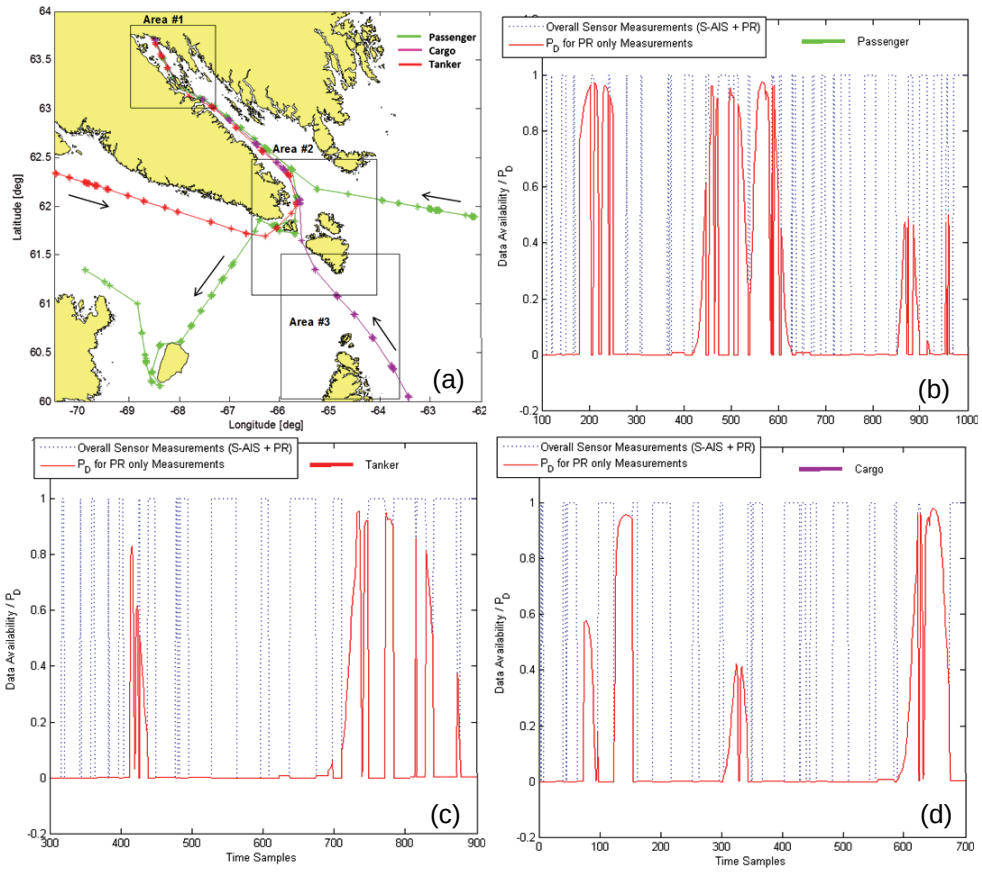


Figure 5-2: Performance Level of the Service for 3 Vessels (passenger, tanker and cargo)

6 CONCLUSIONS

This paper illustrates the approach followed by the PASSAGES project team to design new monitoring services supporting the Maritime Domain Awareness in the Arctic areas. The existing surveillance capability is seriously limited by the scarceness and revisit time of satellite-based data acquisitions (e.g., S-AIS); therefore, the use of terrestrial illuminators of opportunity (GSM base stations, VHF transmitters) is envisaged as well as new installations of such transmitters. This would allow deploying a network of mobile passive receivers that – exploiting the existing signals – increase the probability of detection along the main traffic routes in the Arctic. The presented approach represents a viable, effective trade-off among system costs and performance in order to achieve an adequate level of MDA in such remote areas.

ACKNOWLEDGMENTS

The work presented in this paper has been developed within the project PASSAGES, funded by the German Federal Ministry for Economic Affairs and Energy (03SX355B).

REFERENCES

[1] Griffiths, H.D., Baker, C.J. (2005). *Passive Coherent Location Radar Systems. Part 1: Performance Prediction.* Radar, Sonar and Navigation, IEE Proc, v.152, n°3, pp.153-159.

[2] Zemmari, R., Daun, M., Nickel, U. (2012). *Maritime Surveillance Using GSM Passive Radar*. Int. Radar Symposium.

[3] Zemmari, R.; Daun, M.; Battistello, G.; Nickel, U. (2012). *Target Estimation Improvement of GSM Passive Coherent Location System.* Proc. of IET Int. Conf. on Radar Systems.

NEST-CROWDCONTROL

ADVANCED VIDEO-BASED CROWD MONITORING FOR LARGE PUBLIC EVENTS

Eduardo Monari[1] Yvonne Fischer[1] and Mathias Anneken[1]

[1] *{eduardo.monari, yvonne.fischer, mathias.anneken}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

Abstract

Current video surveillance systems still lack of intelligent video and data analysis modules for supporting situation awareness of decision makers. Especially in mass gatherings like large public events, the decision maker would benefit from different views of the area, especially from crowd density estimations. This article describes a multi-camera system called NEST and its application for crowd density analysis. First, the overall system design is presented. Based on this, the crowd density estimation method is explained. The graphical user interface consists of two components: a georeferenced dynamic heat-map visualization and an interactive video stream visualization. Both components allow a direct camera control. In addition, the system is equipped with an adaptive privacy masking for privacy protection.

Keywords: NEST, video surveillance, crowd density estimation, crowd monitoring

1 INTRODUCTION

Mass gatherings, especially in urban environments, have a potential risk to lead to critical situations in terms of safety (due to fire, etc.) but also escalation (panic, aggressive behavior of individuals, etc.) and therefore may pose a threat to the safety of humans and the security of the citizen. LEA (Law Enforcement Agencies) representatives as well as people in the crowd and in the neighborhood are regularly injured, sometimes seriously, during the course of such critical events.

Research is needed to identify, test and assess new means of protecting citizens in crowd environments. Hereby most of research activities focus on automated detection of suspicious and/or aggressive behavior, usually observable at politically motivated demonstrations, large festivals due to consumption of alcohol and drugs, etc., or even in critical situations like terroristic attacks. For such scenarios, crowd monitoring could be helpful to detect aggressive or unusual behavior in the crowd as soon as possible, and to enable security personnel to act at an early stage of escalation.

However, crowd monitoring is also of high importance in events, which are considered to be peaceful, but overcrowded due to large number of visitors. For safety reasons, monitoring of crowd density and flow behavior is also of high importance, in particular in cases of limited number of escape paths. Unfortunately, especially for open and public events, with no explicitly given entry/exit points like it is the case inside buildings or private sites, there is no (fully developed) technology solution available on the market, to enable security personnel and LEAs to capture and monitor large and spatially distributed crowds. This can only be done if crowd management instruments are improved significantly with new sensors and processing technologies. At the same time, it should always be taken into account that new monitoring technologies should be in line with legal and ethical rules of operation, to ensure the acceptance of citizens of the new monitoring systems.

2 SYSTEM DESIGN, ARCHITECTURE AND PROTOTYPE SETUP

Since 2007, the Fraunhofer IOSB is developing the system NEST (Network Enabled Surveillance and Tracking). The NEST-System is a research and prototype platform for distributed intelligent video-based monitoring. The main objective was to develop a modular and adaptable software system for video monitoring, which is independent from the application domain and can be easily extended with intelligent video and data analysis modules [1].

The first realization of the system was a multi-camera indoor surveillance application. Main modules that have been developed at this stage were person detection, person tracking and alarm generation [2], [3]. Another application was realized in recent years, where the system was used for outdoor surveillance applications, i.e. for infrastructure protection.

In the next step, the system should be used as a deployable version in order to allow crowd density analysis in big public events. The system design for this version is visualized in Figure 1. Crowd-density estimation is done on each single camera stream first. These results can of course be visualized directly in a video stream visualization component. As an additional privacy protection method, an adaptive privacy masking for pan-tilt-zoom-cameras (PTZ) was developed and integrated into the visualization component. Furthermore, the system estimates a combined version of the crowd density estimations, which results in a georeferenced and map-based estimation. This fusion component is especially important, when several camera streams overlap. The georeferenced crowd density estimation is then visualized in a dynamic heat map visualization component, which is based on a GIS-viewer. As the camera footprints can also be visualized in the GIS-viewer, the user interaction allows also the map-based control of the PTZ-cameras by changing the footprints inside the viewer. Additionally, PTZ-cameras can be controlled directly in the video stream visualization by clicking inside the video. The PTZ-camera then moves the focus to this point.

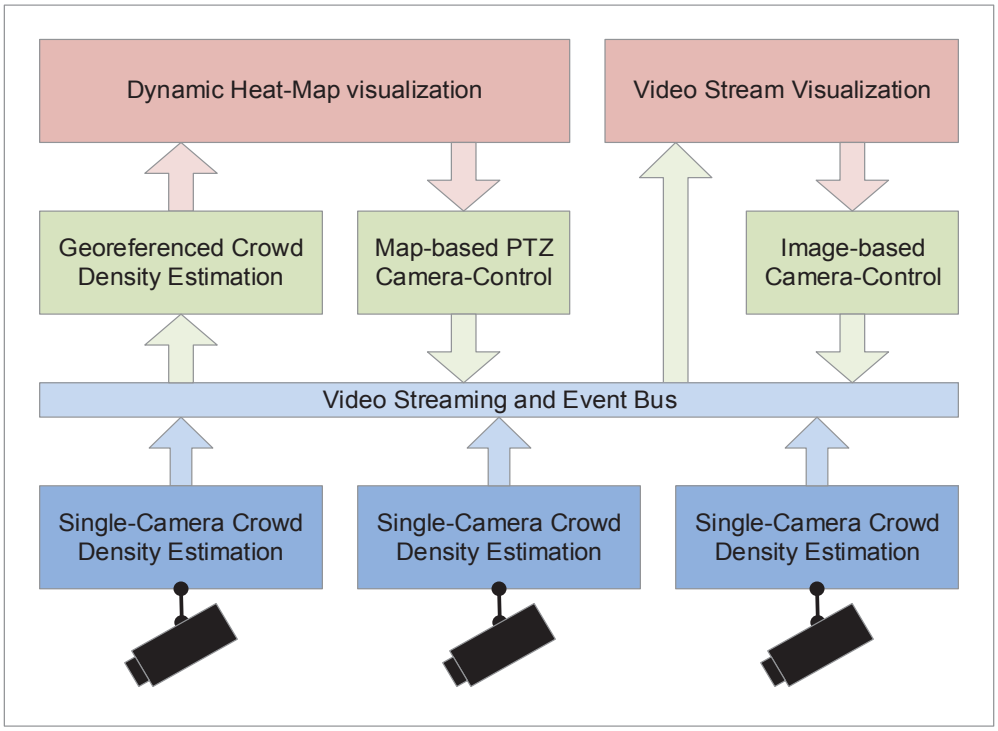


Fig. 1: System design of deployable version for crowd density monitoring

3 VIDEO ANALYTICS FOR CROWD DENSITY ESTIMATION

One key capability for ensure safety at large events is the possibility to measure and control the number of persons for a specific local area (crowd density), and if possible to recognize critical situations (over-crowded areas). This is a challenging task in case of urban events, which do not always allow for installation of entry/exit gates and people counting to control number of visitors. For such scenarios, the applicability of distributed cameras for real-time crowd density estimation has been investigated in this work. In particular, *flow/motion density* as a possible crowd density metric has been evaluated.

Hereby, flow/motion density is defined as a relative, basically unit-less measure, which provides information on spatial and temporal changes in crowd density. Given a video stream from a surveillance camera, density of the moving crowd is determined as follows:

1. **Feature Extraction**: In a first processing step so-called “good features to track”, proposed bei Shi and Tomai [4] are extracted. These features are basically image corners, which turn out to be very robust for tracking in consecutive video frames, and therefore have been used in many applications for local motion and flow estimation in video processing. In our application these features are used, since textures of person groups in videos turn out to contain a suitable number of such local “corner structures”.
2. **Motion Estimation**: For those image pixels identified as “good features to track”, motion estimation is performed. As a result, for each corner pixel in the image motion vectors are determined. Motion vectors includes information about motion direction (vector orientation) and speed (magnitude/length), which is an important information to suppress noise and outliers in measurement.
3. **Thresholding, Spatio-Temporal Filtering, and Normalization**: Noise suppression and outlier detection in motion estimation can be easily done by simple thresholding based on velocity and direction of motion vectors. Given the camera calibration information (extrinsic parameter) such thresholding parameter can be defined in metric units (e.g. minimum and maximum velocity of persons in m/sec). Additionally spatial and temporal filtering by Kernel Density Estimation is applied for robustification and at the same time for clustering of estimation results. For spatial clustering we used a two dimensional Gaussian Kernel, with the standard deviation σ set to approx. twice the size of persons in the image. The results of this Gaussian filtering is afterwards post-processed by a temporal smoothing consisting of a pixel-wise mean filter. A parameter which defines the number of consecutive frames considered for mean calculation allows to set priority to low noise of the overall estimates (large number of averaged frames) vs. observation of quick changes and high dynamics (low number of averaged frames). Finally, the density estimation results are normalized to a predefined scale for heat-map generation (color coding).

The reason for usage of relative measures instead of absolute ones (e.g. person counting) is justified by the significantly higher complexity and lower robustness of today’s real-time people counting algorithms. In particular, using standard video surveillance cameras (even in case of high resolution PTZ-cameras), high accuracy people detection and counting algorithms are only applicable in scenarios with low or mid-level density. Higher densities lead to (partial) occlusions of persons, which in turn lead to significant miss rates of person detection and as a consequence to unreliable counting results.

The advantage of relative density estimation, e.g. by flow density metrics, is its simplicity and effectiveness. Without providing an absolute number of persons in an area, flow density estimation can be used to intuitively provide information on spatial density distribution over large areas, and to highlight local spots with unusual high densities compared to other areas. These hints can be used as basis for visual investigation by human operators.

Similar, the proposed relative metric is a sufficient feature for estimation and prediction of dynamics of the crowd. Fast changes of densities are always a reason for visual investigation by the human operators, to be able to act in time, in case of expected critical situations. Such unusual dynamics can be detected automatically by algorithms, even without an absolute metric.

Fig. 2: Corner detection and flow estimation for filtered motion vectors using method of Shi-Tomasi [4].

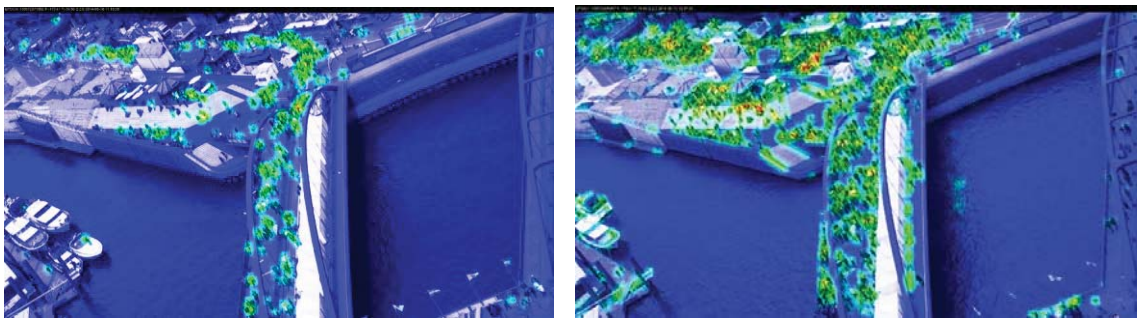


Fig. 3: Exemplary results of short-term crowd density estimation by spatio-temporal Gaussian kernel density estimation (low density on the left, higher crowd density on the right).

4 GEOREFERENCED DYNAMIC HEAT-MAP VISUALIZATION

To help security personnel to improve their situation awareness the results of the video analytics for the crowed density estimation have to be visualized in an appropriate way. Therefore dynamic heat-map visualization has been integrated into the NEST system. As seen in Figure 4, the continuously generated heat-maps are georeferenced and can be used as an overlay for the map showing the area of interest. Furthermore, the camera positions as well as the current field of view for each camera are visualized in the map. Additionally, a real-time video stream viewer for multi-camera systems is shown, see Figure 5. These two components enable the personnel to view the camera images as well as a map-based view and, together with the interaction concept, allow active PTZ-cameras to be controlled simultaneously by map-based as well as video-based interaction.

Due to performance issues, it was not possible to draw the heat-map in a decent resolution as polygons on top of the map. Therefore the heat-map is rendered as

GeoTIFF using the geotools library. Rendering a GeoTIFF as overlay for the map is by far faster than the first approach.

A heat-map is generated by quantizing the data. This quantization can be done by using a grid consisting of rectangles. Each rectangle is then called a bucket. A simple and intuitive way to fill these buckets is to count the number of density estimates falling into each bucket. The buckets are then projected to a prior specified color scale. This results in a rough heat-map, which can be smoothed by filtering. As stated by Lampe and Hauser [5], another approach is to use a kernel density estimation for calculating the density function underlying the crowd distribution. This function is then evaluated for each bucket and the resulting values are projected to the color scale. For further information on the kernel density estimation see [6] or [7].

Fig. 4: Heat-map of surveillance area with fine grained resolution

Fig. 5: Overview of video streams as exemplary shown in the NEST system. In the center image, the detected motion is shown.

By adjusting the parameters for the generation of the heat-map, the heat-map can represent rather a high resolution or give a rough overview about the surveillance area. In Fig. 4 and Fig. 6, two example heat-maps are shown, which illustrate the impact of different parameter sets. The first gives a detailed view of the area, in which even small densities can easily be spotted. The second heat-map gives only a coarse overview. Here, the overall amount of densities is more important than local density variations.

Fig. 6: Heat-map of surveillance area with coarse-grained resolution

5 PRIVACY PROTECTION METHODS

In video surveillance, especially on public spaces, privacy is always an important aspect that has to be taken into account. Especially in case of a system like proposed in this paper, which uses high resolution PTZ-cameras able to provide very high level of detail of observed areas.

On one hand, in most cases it is very helpful for security personnel to have video streams with the highest level of detail as possible. High resolution allows to recognize specific activities (e.g. suspicious movements in the crowd) even in “wide angle” mode of a zoom camera.

On the other hand in many cases, resolution provided by cameras and visualized to security staff is unnecessary high, e.g. when cameras enables to zoom in to a level of detail which allows to recognize people’s faces one by one.

This high dynamics in optical zooming as well as the possibility to steer pan/tilt cameras to different positions of the scene makes is impossible to use common privacy masking approaches like blackening, pixalization, or blurring. All these methods are mainly used for cameras with static field of views.

For our system, advanced privacy masking algorithms has been developed, which firstly can be used with pan/tilt cameras, in particular taking into account absolute camera orientation for blackening of predefined areas (e.g. public areas, windows of houses, etc.). And secondly, our approach allows to adapt pixelization (level of detail) of the video stream in real-time, depending on zoom level.

Orientation adaptive blackening is basically achieved by a real-time registration of the current image-to-360°-panorama registration approach. The idea hereby is to define

“black areas” statically on a previously automatically generated 360° panorama of the camera’s environment. This settings are a part of the camera setup and calibration task. After definition of “back areas”, in real-time processing the algorithm is performing a real-time image-to-panorama registration to determine which subset of the 360°-panorama is currently captured by the PTZ-camera. Once the subset is determined, black areas in this subset are back-projected to the current camera image and those pixels are replaced by black pixels. This filtered video stream is forwarded to visualization, while the original one is neglected from further processing.

Similar, for different zoom levels of the camera, an adaptive pixelization filter is used as privacy preserving technique. While pixelization of the whole image is a standard approach for privacy protection, our approach is taking into account camera position and orientation to estimate the distance of the camera to each point in the scene projected to each image pixel. Depending on the distance between camera scene point for each pixel, and taking into account the zoom level of the camera (lens aperture), an appropriate pixelization level is chosen for this pixel. The more far away the scene point from the camera and/or the lower the zoom level (wide angle view) the higher level of detail is allowed, since spatial resolution of an object becomes lower. The nearer the scene point or the higher the zoom level of the optics, the higher the level of details for this pixels, and as a consequence the higher the pixelization level (artificial reduction of image resolution locally).

In summary, these two privacy masking approaches allow for application of high resolution PTZ-cameras, but still allows for performing privacy masking in real-time. Adaptive pixelization provides the “best” possible image resolution to human operators, but taking into account privacy protection. While an area in an image showing persons quite far away from the camera and due to this captured in low resolution, may not been affected by pixelization, another area with persons nearer to the camera and in higher resolution might be pixelized for privacy protection.

6 CONCLUSION

This article describes a multi-camera system called NEST and its application for crowd density analysis. First, the overall system design was presented. Based on this, the crowd density estimation method was explained. The graphical user interface consists of two components: a georeferenced dynamic heat-map visualization and an interactive video stream visualization. Both components allow a direct camera control. In addition, the system is equipped with an adaptive privacy masking for privacy protection.

Equipped with these modules, the NEST CrowdControl-System is able to be used for crowd monitoring for large public events. The system is not intended to make its own decisions but to support situation awareness of a decision maker by visualizing him condensed information on crowd density and allowing him to interactively controlling the cameras.

As a next step of development, system evaluations (proofs of concept) at real large events are planned. In particular, qualitative evaluation regarding the added value of geo-referenced dynamic crowd density estimation for crowd manager (security personnel) is in scope of the research work. Furthermore, evaluation of the advanced privacy masking techniques will be also in focus of system evaluation by end users.

REFERENCES

[1] Mossgraber, J.; Reinert, F.; Vagts, H., "An Architecture for a Task-Oriented Surveillance System: A Service- and Event-Based Approach," Systems (ICONS), 2010 Fifth International Conference on , pp.146-151, 11-16 April 2010

[2] Moßgraber, J.; Monari, E.; Reinert, F.; Eckel, S.; Bauer, A.; Emter, T.; Laubenheimer, A. “N.E.S.T. – Network Enabled Surveillance and Tracking”. Future Security – 3rd Security Research Conference Karlsruhe, Germany. 2008.

[3] Fischer, Y.; Krempel, E.; Birnstill, P.; Unmüßig, G.; Monari, E.; Moßgraber, J.; Schenk, M.; Beyerer, J.: “Privacy-aware Smart Video Surveillance Revisited”. 9th Future Security, Security Research Conference, Berlin, September 16-18, 2014.

[4] Shi and C. Tomasi. Good Features to Track. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 593-600, June 1994.

[5] Lampe O. D. and Hauser H. (2011). Interactive Visualization of Streaming Data with Kernel Density Estimation, Proceedings of the IEEE Pacific Visualization Symposium (PacificVis 2011)

[6] Barber, D., (2012). Bayesian Reasoning and Machine Learning, Cambridge University Press

[7] Murphy, K.P. (2012), Machine learning: a probabilistic perspective, MIT Press, Cambridge, MA

SECURUS - A PROVABLE SECURE DATABASE OUTSOURCING SCHEME

Tobias Nilges[1] and Jens Köhler[2]

[1] *tobias.nilges@kit.edu*
Karlsruhe Institute of Technology (KIT), Institute of Theoretical Informatics (ITI),
76131 Karlsruhe (Germany)

[2] *jens.koehler@kit.edu*
Karlsruhe Institute of Technology (KIT), Institute of Telematics (TM),
76131 Karlsruhe (Germany)

Abstract

Databases can be encrypted before being outsourced to honest-but-curious cloud storage providers to enforce the confidentiality of the contained data. However, securely encrypting the entire database induces high efficiency costs as the storage providers cannot evaluate database queries on encrypted data and the entire database has to be transferred to a trusted party to be decrypted. To reduce those efficiency costs, confidentiality preserving indexing approaches (CPIs) were proposed to allow storage providers to participate in the execution of queries. While the security properties of single CPIs are typically well studied, the security properties of the frameworks that make use of multiple CPIs to outsource real databases are not. In this paper, we provide a security proof for the Securus framework which makes use of CPIs to enforce the confidentiality of outsourced databases. We conduct the proof by successfully applying the Universal Composability proof methodology. Thus, the contributions of this paper not only show that the Securus database outsourcing framework is secure, but also that the Universal Composability proof technique cannot only be applied for low-level cryptographic schemes but also for complex real world system.

Keywords: Confidential Database Outsourcing, Securus, Composability, Provable Security.

1 INTRODUCTION

Secure outsourcing of databases to cloud storage providers (CSPs) is a major research direction. CSPs are often considered as honest-but-curious attackers who might try to collect as much data as possible. The naive approach of enforcing data confidentiality by encrypting the entire database before outsourcing it cannot always be applied since this would imply to download and decrypt the entire database when a database query has to be processed. Downloading the entire database from the CSPs induces efficiency costs that outweigh the cost-savings that are to be expected by making use of CSPs. To address this problem, confidentiality preserving indexing approaches (CPIs) were proposed that allow the CSP to participate in the execution of database queries and reduce efficiency costs. The CPIs include special encryption schemes [1,2,3,4] and/or partial distribution of the data to several cloud providers [5]. Furthermore, database outsourcing frameworks exist that integrate various CPIs to leverage the individual strengths of each CPIs when outsourcing databases with multiple attributes [6,7,8]. While the security properties of CPIs are typically well studied, the security properties of the frameworks that make use of multiple CPIs at once are not.

In this paper, we provide a security proof for the Securus framework [6]. In this framework, the user has to specify a Policy Profile that states exactly which database attribute values and attribute value associations have to remain confidential as well as how the data will be queried. Additionally, the user can specify that the confidentiality of specific attributes can be considered protected even if the applied CPIs leak specific information on the outsourced plaintext values of these attributes. Securus then automatically implements a mediator that can be used by applications to apply CPIs before outsourcing data and to seamlessly execute queries on the outsourced encrypted data. Securus mediators are expected to be *secure* in the sense that the applied CPI combination only leaks the information that the Policy Profile permits to leak.

Our contribution: In this paper, we provide a proof for the security of Securus mediators. In a first step we provide a formal description of the Securus mediators' functionality in the Universal Composability (UC) framework [9]. Our description of the functionality makes all assumptions explicit that we have to make in order to provide a formal security proof. Moreover, it models exactly the information that an adversarial provider can learn. It thus defines the ideal functionality that Securus mediators are supposed to implement. We then move on to show that Securus mediators actually provide the security properties that are required in the Policy Profile by giving a formal proof that the protocol implements the ideal functionality. To the best of our knowledge, this is the first formal proof of security for a complex database outsourcing framework.

The paper is organized as follows. We provide related work in Section 2. In Section 3, we introduce the parts of the Securus framework that are relevant for the security of the generated mediators and the security proof that is presented in this paper. In Section 4, we provide an overview of cryptographic fundamentals that are vital to understand our security proof that is presented in Section 5. In Section 6, we conclude the paper and highlight future research directions.

2 RELATED WORK

To make query execution on encrypted databases more efficient a variety of *confidentiality preserving indexing approaches* (CPIs) were proposed. CPIs allow CSPs to participate in the execution of queries and thus avoid transmitting encrypted data records to the issuer of the query that do not match the executed query. In particular, CPIs include structure-preserving encryption such as order-preserving [2] and deterministic encryption schemes [3], as well as partially-homomorphic encryption schemes [4] that allow the CSPs to aggregate ciphertexts before transmitting them to the query issuer.

Multiple frameworks apply CPIs to securely outsource databases. Among them are Securus [6] and CryptDB [7]. The security proof we present in this work is designed for Securus. CryptDB does not provide static security guarantees but weakens the provided security guarantees over time by decrypting attribute values as much as necessary to evaluate incoming database queries efficiently. While the security proof we present in this paper can be adapted to show that the CPIs that are used by CryptDB can be considered "secure" at a given point in time, it makes no assertion on CryptDB's security properties over time.

In the area of UC-secure protocols, the results focus on obtaining composable variants of cryptographic primitives, such as commitments [10] and oblivious transfer [11]. Given these primitives, even secure multi-party computation can be proven UC-secure (e.g. [12]). However, without a so-called setup assumption, it is not possible to obtain such protocols with security against active adversaries [10]. Since we only consider passive adversaries, we do not need a setup assumption.

3 OVERVIEW OF THE SECURUS FRAMEWORK

In this section we introduce Securus, the object of investigation for the security proofs that we contribute in this paper. An overview of Securus' architecture is shown in Figure 1. Securus allows the user to specify the outsourcing requirements with regard to confidentiality and query workload in a so-called policy profile. Based on these requirements, Securus automatically selects a suitable, efficiency-optimized set of CPIs that satisfy the confidentiality requirements and implements them in a so-called mediator. A mediator constitutes a software component that can be used by the user to seamlessly outsource database records and query them without worrying about the application of CPIs. The mediator receives plaintext records from the user, encrypts them by applying CPIs and outsources the encrypted records to the CSPs. Furthermore, it evaluates plaintext SQL queries of the user by re-writing them so that they can be evaluated on CPIs and passing the re-written queries to the CSPs. The encrypted records that are returned by the CSPs are decrypted by the mediator and passed to the user as a result to the original query.

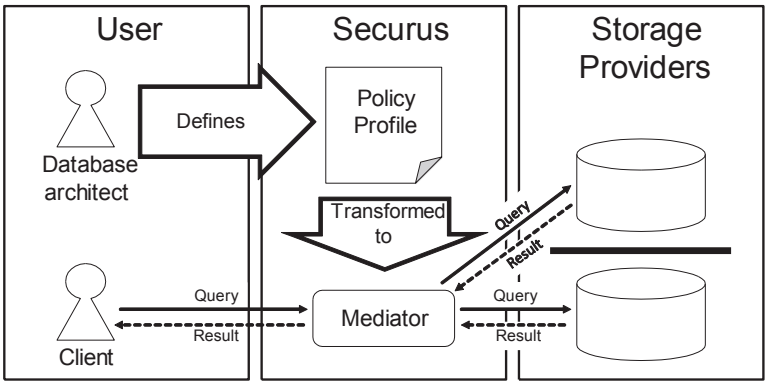


Figure 1: Architecture of Securus [6]

3.1 Policy Profiles

Securus allows the user to specify confidentiality requirements of the data as well as the queries that have to be efficiently executable on the data. In particular, Securus users can make use of the following policy elements to specify their requirements.

Query Policies (QP): The queries that have to be executed efficiently in the future can be specified by listing the according SQL queries in the policy profile. As the satisfaction of QPs is not relevant for the proof that we present in this paper, we refer interested readers to [6] for a more detailed description of how Securus satisfies QPs.

Confidentiality Constraints (CC): CCs can be used to specify that single attributes have to be protected via CPIs. Furthermore, Securus allows to express that associations between attribute values have to be kept confidential. In this case it suffices to protect one attribute that is contained in the CC via a CPI.

Most CPIs leak information on the plaintext values to the CSP. We define that attributes can be represented as four different *attribute types* at the CSP: plaintext (*clr*) attributes leak plaintext attribute values, order-preserving ciphertexts (*ord*) leak the order of plaintext values, distinguishable ciphertexts (*det*) leak equality of plaintext values and indistinguishable ciphertexts (*prb*) leak no information on the attribute values.

Inference Constraints (IC): In order to make use of CPI approaches to protect attribute values, the user has to explicitly state which information leakage is considered acceptable by so-called inference constraints. We distinguish between two different types of inference constraints.

- **Order Inference Constraints (OIC)** on an attribute *i* state that attribute *i* can be considered protected even if the order of the plaintext values leaks to the CSP.
- **Deterministic Inference Constraints (DIC)** on an attribute *i* state that attribute *i* can be considered protected even if it leaks to the CSP which plaintext values are the same.

3.2 Policy Transformation

We define a mediator to be "secure" if it satisfies the following security condition: For each CC, at least one attribute that is contained in the CC has to be protected at each CSP. An attribute can be considered protected if only indistinguishable ciphertexts of it are outsourced, or - if the according OICs/DICs are specified - order-preserving/distinguishable ciphertexts are outsourced.

Example: Given a CC that contains A as well as B and a DIC on attribute A. At each CSP either attribute A has to be protected, i.e., the attribute type of A has to be *prb,* or attribute B has to be protected, i.e., the attribute type of B has to be one of *prb* and *det*.

Securus models this security condition along with conditions that originate from QPs that are not listed in this paper as constraints in an ILP problem. The ILP problem is solved based on existing ILP solvers to determine an efficiency-optimized CPI combination that is implemented in a mediator. As ILP solutions are bound to satisfy the specified constraints, the mediator satisfies the listed security condition *if* the underlying CPIs can be considered secure. Thus, for Securus mediators to be secure, it remains to be shown that the applied CPIs indeed only leak the amount of information regardless of the context in which they are applied.

4 FUNDAMENTALS OF THE SECURITY PROOF

4.1 Security Notions for Encryption Schemes

Security for encryption schemes is usually defined via games that are supposed to capture the security requirement. Consider the following games that define security for probabilistic (Figure 2) and deterministic (Figure 3) encryption.

IND-CPA-b
$(pk, sk) \leftarrow KeyGen(1^k)$
$(m_0, m_1) \leftarrow \mathcal{A}(pk, 1^k)$
$b \leftarrow \{0,1\}$
$c \leftarrow Enc(pk, m_b)$
$b' \leftarrow \mathcal{A}(pk, c, 1^k)$
Output $b = b'$?

Figure 2: IND-CPA security game

IND-DCPA-b
$K \leftarrow KeyGen(1^k)$
$b' \leftarrow \mathcal{A}^{Enc_K(\cdot,\cdot,b)}(1^k)$
Output $b = b'$?

Let $Enc_K(m_0, m_1, b)$ return $Enc_K(m_b)$.

Figure 3: IND-DCPA security game

For probabilistic encryption, an adversary gets the public key and then has to present two messages. The challenger then encrypts one of the messages at random and gives it back to the adversary. If the adversary guesses correctly which message was encrypted, he wins the game. An encryption scheme is IND-CPA-secure, if the adversary wins only with probability $\frac{1}{2} + \varepsilon$, with ε being a negligible function.

In the security game IND-DCPA for deterministic encryption, the adversary can query an oracle that encrypts message pairs, but for all input pairs the message b is encrypted. The messages m_j^i that the adversary may send to the oracle have to be distinct. The adversary wins if he can predict b with higher probability than guessing.

The definition of IND-OCPA for order-preserving encryption is similar to IND-DCPA, except that additionally it has to hold that the messages sent to the encryption oracle satisfy the following constraint: $m_0^i < m_0^j$ iff $m_1^i < m_1^j$.

4.2 The Universal Composability Framework

The UC framework was introduced by Canetti [9] and provides strong security guarantees. To prove security in the framework, in a first step an ideal functionality $\mathcal{F}$ is modelled that is supposed to capture the security requirements of a task (in our case confidential database outsourcing with an explicitly admitted information leakage), and cannot be corrupted. Then, a protocol π is said to realize $\mathcal{F}$ if the following holds: for every adversary $\mathcal{A}$ on the real protocol there has to be a simulator $\mathcal{S}$ on the ideal functionality such that for any environment $\mathcal{Z}$ the output of the real and the ideal protocol execution are indistinguishable. This means that the environment can give the input to the protocol parties and observe the output. This is formalized as follows:

$$\forall \mathcal{A} \exists \mathcal{S} \forall \mathcal{Z}: Real_{\mathcal{A}}^{\pi}(\mathcal{Z}) \approx Ideal_{\mathcal{S}}^{\mathcal{F}}(\mathcal{Z})$$

The main idea behind this paradigm is that if the attacker was able to extract to extract information from the real protocol that is not present in the simulator, the attacker would be able to distinguish the real and the simulated protocol.

5 A SECURITY PROOF FOR SECURUS

This section describes the proof of security for Securus in the Universal Composability (UC) framework. The main reason to choose the framework is that it guarantees that protocols proven secure in the framework can be composed, i.e. combined, with any other protocol without losing security. This is not the case for standard cryptographic security notions, where concurrent or interleaved execution of the protocol might render the protocol insecure. If one wants to execute a protocol in arbitrary environments (e.g. the Internet in the case of Securus), the UC framework guarantees meaningful security.

In the following we will first provide a description of the ideal functionality of Securus. We then give an abstract representation of the real protocol underlying Securus. As all security-relevant operations in Securus are performed by the mediator, the client only provides the input to the mediator.

5.1 The Ideal Functionality

To simplify our exposition, we only assume two parties, a server S and a client C. The model can be straightforwardly extended to show multiple providers and/or users. To be able to model the functionality (cf. Figure 4) according to the real protocol, we have to define an information-leakage function f as follows. It takes as input an attribute value x and an attribute type a.

$$f(a,x) = \begin{cases} x, & if\ a\ is\ of\ type\ clr \\ Ord(x), & if\ a\ is\ of\ type\ ord \\ Sym(x), & if\ a\ is\ of\ type\ det \\ \perp, & else \end{cases}$$

This function removes the real input and replaces it according to the attribute type with (1) the real input, (2) the order of the element $Ord(x)$, (3) a random symbol for the element $Sym(x)$, or (4) no information at all. It models the information leakage of the different CPI encryption schemes that are used in Securus. This leakage is inherent and cannot be prevented, so it has to be modelled in the ideal model as well. Consider the following example:

$$q = SELECT * FROM\ table\ WHERE\ salary = 10000$$

Let salary be an attribute of type ord and let the value 10000 be the 8th highest value in the dataset. By applying f to q, we obtain:

$$f(q) = SELECT * FROM\ table\ WHERE\ salary = 8$$

We thus replace all secret information and only keep the structure with information that cannot be prevented from leaking.

The ideal functionality is setup with an initialization message that defines a database scheme that will be used, including which type of confidentiality constraint must hold for each attribute. In the normal query phase, the client directly provides (SQL-)queries to the functionality, which will output the query result to the client. Note that the adversary (i.e. the server) can schedule the messages. In the ideal model, the mediator is not necessary, because the whole database is securely stored in the incorruptible ideal functionality.

Functionality $\mathcal{F}_{Securus}$

Setup: Wait for a message $(init, k, a_1, \dots, a_m)$ with $a_i = (x, y), y \in \{ord, det, prb, clr\}$, $x \in \{0,1\}^*$, create a database scheme with x as the attribute's name and y as the attribute's type. Let k be the security parameter. Forward this message to the attacker $\mathcal{A}$.

Query:

- Upon receiving $(query, q)$, execute query q on the database scheme and let r be the result. Send $(leak, f(q))$ to $\mathcal{A}$.
- Upon receiving (ok) from $\mathcal{A}$, send the result $(result, r)$ to the mediator.

Figure 4: Formal description of the ideal functionality.

5.2 Protocol Description

We focus only on the relevant cryptographic operations and abstract the real protocol messages to reduce the complexity of the description. The description is split in two parts: first a setup and then the execution of queries (cf. Figure 5).

This protocol contains all the essential parts of the real protocol. The main observation is that the party interacting with the database is the mediator that applies the encryption. Let ES_{type} denote an encryption scheme of the corresponding type. The key generation is explicitly mentioned, as well as the transformation of the queries. Due to space limitations, this is not further formalized.

5.3 Proof of Security

Theorem 1. $\pi_{Securus}$ UC-realizes $\mathcal{F}_{Securus}$ (i.e. $Real_{\mathcal{A}}^{\pi_{Securus}}(\mathcal{Z}) \approx Ideal_{\mathcal{S}}^{\mathcal{F}_{Securus}}(\mathcal{Z})$) against passive adversaries given that ES_{prb} is IND-CPA-secure, ES_{ord} is IND-OCPA-secure and ES_{det} is IND-DCPA-secure.

Proof. We first state a simulator (cf. Figure 6) that can simulate a real protocol run without knowing any real data.

We now have to prove that the output of the simulator is indistinguishable from a real protocol execution for any environment. This is done by comparing so-called hybrid experiments and showing their indistinguishability.

Experiment 1: $\mathcal{S}_1$ simulates the real protocol.

Experiment 2: Same as Experiment 1, except that $\mathcal{S}_2$ replaces $c_x = ES_{prb}.Enc(x)$ by $c_r = ES_{prb}.Enc(r)$ for a random $r \in \{0,1\}^k$.

Protocol $\pi_{Securus}$

Let ES_{det} be a deterministic encryption scheme, ES_{ord} be an order preserving encryption scheme and ES_{prb} be a probabilistic encryption scheme.

Setup:

- Client: Declare the type $y \in \{ord, det, prb, clr\}$ for each attribute $a_i \in \{0,1\}^*$. If required by type y, execute the following commands:
  - $KeyGen(1^k)$ for ES_{det}
  - $KeyGen(1^k)$ for ES_{ord}
  - $KeyGen(1^k)$ for ES_{prb}

  Send a message $m_{init} = (init, k, a_1, \dots, a_m)$ to the server.
- Server: create a database scheme according to m_{init}.

Query:

- Client: Change the query q' according to the attribute types, i.e. compute $ES_{type}.Enc$ on the corresponding attribute values and obtain q. Send $(query, q)$ to the server.
- Server: Execute the query q on the database and let r be the result. Send r to the client.
- Client: If necessary compute $ES_{type}.Dec$ on the corresponding attribute values and obtain r'. Output r'.

Figure 5: Formal description of the protocol.

Simulator $\mathcal{S}$

Perform the key generation of ES_{det} , ES_{prb} and ES_{ord}.

- Upon input $m_{init} = (init, k, a_1, \dots, a_m)$, send m_{init} to $\mathcal{A}$.
- Upon input $(leak, f(q))$, change any assignment (a, x) in q as follows:
  - If a is of type ord: If x has not been part of a query before, draw a random value $r_x \in \{0,1\}^k$ and store (x, r_x) according to the order obtained from $f(q)$. Otherwise retrieve the tuple (x, r_x). Compute $c_r = ES_{ord}.Enc(r_x)$ and replace x in $f(q)$ by c_r.
  - If a is of type det: If x has not been part of a query before, draw a random value $r_x \in \{0,1\}^k$ and store (x, r_x). Otherwise retrieve the tuple (x, r_x). Compute $c_r = ES_{det}.Enc(r_x)$ and replace x in $f(q)$ by c_r.
  - If a is of type prb: Draw a random value $r \in \{0,1\}^k$, compute $c_r = ES_{prb}.Enc(r)$ and replace x in $f(q)$ by c_r.

  Send $(query, f(q))$ to $\mathcal{A}$.
- Upon input $(result, r)$, send (ok) to $\mathcal{F}_{Securus}$.

Figure 6: Simulator against a corrupted server.

Experiment 3: Same as Experiment 2, except that $\mathcal{S}_3$ replaces $c_x = ES_{ord}.Enc(x)$ by $c_r = ES_{prb}.Enc(r)$ for a random $r \in \{0,1\}^k$ of correct order and stores both values, if x was not queried before. Otherwise retrieve the corresponding value and replace x.

Experiment 4: Same as Experiment 3, except that $\mathcal{S}_4$ replaces $c_x = ES_{prb}.Enc(x)$ by $c_r = ES_{prb}.Enc(r)$ (for a new random $r \in \{0,1\}^k$ if x was not queried before). This is the ideal protocol.

Now, a careful examination of the experiments shows that experiments 1 and 2 are indistinguishable given that ES_{prb} is an IND-CPA-secure encryption scheme, experiments 2 and 3 are indistinguishable given that ES_{ord} is IND-OCPA-secure and

experiments 3 and 4 are indistinguishable given that ES_{det} is IND-DCPA-secure. We can state a reduction that shows that an adversary that breaks the security of Securus can break the security of the respective encryption schemes, but we omit the full reductions due to space restrictions.

6 CONCLUSIONS

In this paper, we were able to prove that Securus guarantees to satisfy Policy Profiles that are specified by the user and only leak the amount of information that the user permits to leak. We conducted the proof by successfully applying the UC-framework to model Securus and show that the unpreventable information leakage of CPIs matches the admitted information leakage in the Policy Profile. To the best of our knowledge, this is the first formal proof of security for a complex database outsourcing framework.

While our security proof shows that Securus in itself is secure, securely *applying Securus in practice* inherently relies on the assumption that the user correctly specifies the Policy Profile, i.e., the information that is admitted to leak in the Policy Profile may indeed leak without undermining a higher level data confidentiality objective. Thus, future work has to focus on developing methodologies which can be used to prove that a specified Policy Profile securely enforces high-level data confidentiality objectives. A first step in this direction can be to analyze semantic attribute dependencies and the ability of the attacker to make use of background knowledge on the outsourced data to leverage the admitted information leakage. In particular, achieving this algorithmically might be possible by checking if attributes are statistically correlated.

REFERENCES

[1] J. Köhler, K. Jünemann, and H. Hartenstein. *Confidential database-as-a-service approaches: Taxonomy and survey*. Journal of Cloud Computing, 4(1):1–14, 2015.Computing, 4(1):1–14, 2015.

[2] R. Popa, F. Li, and N. Zeldovich. *An ideal-security protocol for orderpreserving encoding*. In Proc. of Security & Privacy, 2013.

[3] M. Bellare, T. Kohno, and C. Namprempre. *Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm*. In Proc. of ACM TISSEC, 2004.

[4] P. Paillier. *Public-key cryptosystems based on composite degree residuosity classes*. In Proc. of EUROCRYPT, 1999.

[5] D. Achenbach, M. Gabel, and M. Huber. *Mimosecco: A middleware for secure cloud storage*. In Proc. of ICST, 2011.

[6] J. Köhler and K. Jünemann. *Securus: From confidentiality and access requirements to data outsourcing solutions*. In Privacy and Identity Management for Emerging Services and Technologies, 2014.

[7] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan. *CryptDB: Protecting confidentiality with encrypted query processing*. In Proc. of SOSP, 2011.

[8] F. Kerschbaum, M. Härterich, M. Kohler, I. Hang, A. Schaad, A. Schröpfer, and W. Tighzert. *An encrypted in-memory column store: The onion selection problem*. In Proc. of Information Systems Security, 2013.

[9] R. Canetti. *Universally composable security: a new paradigm for cryptographic protocols*. In Proc. of FOCS, 2001.

[10] R. Canetti, M. Fischlin. *Universally composable commitments*. In Proc. of CRYPTO, 2001.

[11] C. Peikert, V. Vaikuntanthan and B. Waters. *A framework for efficient and composable oblivious transfer*. In Proc. of CRYPTO, 2008.

[12] R. Canetti, Y. Lindell, R. Ostrovsky and A. Sahai. *Universally composable two-party and multi-party secure computation*. In Proc. of STOC, 2002.

PRIVACY SCORE: MAKING PRIVACY ASPECTS OF SURVEILLANCE SYSTEMS COMPARABLE

Erik Krempel[1] and Jürgen Beyerer[2]

[1] *erik.krempel@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Dept. Secure Communication Architectures, Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[2] *juergen.beyerer@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

Abstract

When authorities are faced with a security problem and decide to install surveillance technology they have to decide on a multitude of questions. Which technology to use? Which different implementations of that technology exist on the market? What is the potential privacy impact of the different solutions? What are the costs (financial and privacy) relative to the benefits? Without expert knowledge it is hard to detect where privacy risks emerge and what can be done to prevent or mitigate them.

To aid the authorities in this process and guarantee that privacy protection is a relevant part of the decision privacy score was created. Privacy score rates data protection of surveillance systems. To rate an implementation an auditor has to answer nine different questions in three categories: “Data collection”, “Data access and use” and “Technical data protection”. The result is a privacy score between 0 and 21 points that can be used as basis for further analysis.

Keywords: Privacy, technology assessment, Privacy rating

1 INTRODUCTION

The balance between security and privacy might be one of the most important challenges in today’s modern societies. While it is an ongoing argument whether we should limit privacy to achieve security [1] or if there even is a conflict between security and privacy [2], a further dimension of the problem is often overlooked.

Imagine the following scenario: An authority is responsible for the security of a public place. Ongoing security incidents lead them with the wish to install a video surveillance system. In the design of the system many requirements need to be fulfilled. The system must be capable to solve the security task present, not exceed the budget, be easy to use and of course privacy invasion should be kept to a minimum. While financial costs of a system is relative easy to measure, how should one decide between multiple systems that differ in privacy aspects? How to measure and asses the privacy impact of different systems?

Measuring privacy as a whole is next to impossible. Not only differs the perception of privacy between people [4], but also within context [5] and time. What can be measured and will directly influence the privacy perception and therefor acceptance [3] is **technical data protection** in the system. For a detailed look at rating surveillance systems, also in the aspects of human rights, financial costs and usability have a look at the deliverables of the SURVEILLE project [6].

Chapter 2 will have a look at related work in the field of privacy protection in surveillance systems and into assessing privacy properties of systems. Chapter 3 will explain the full process of privacy score before in chapter 4 an exemplary scoring is performed. Chapter 5 will give a conclusion of the work done and will give an idea of which further work is intended.

1.1 Taxonomy

In the following article the terms privacy and data protection will be used multiple times. Unfortunately those terms have conflicting definitions. In a technological context the term data protection could mean the protection of collected data against corruption, unauthorized access and unintended deletion. In this context it is of no importance whether the data includes Personal Identifiable Information (PII) or the weather forecast from last month.

In a legal context data protection might mean the right to data protection which includes all kinds of data related to a person. The term privacy in a legal context might refer to the right to privacy which in most definitions only applies to data that was collected in a private, i.e., not public, place.

For the rest of this document we will use the terms data protection and privacy as follows: Data protection describes how data is handled in a system from a technical point of view. That includes the collection, the processing and the access to data. It will not include if the collection or processing of data is lawful. As we rate the data protection of surveillance technologies it is directly related to privacy. When we speak of a high privacy risk or a high privacy impact we want to point out that the measures of data protection are not sufficient.

2 RELATED WORK

Looking at privacy aspects of (surveillance) systems one should have a look at Privacy by Design (PbD) by Ann Cavoukian [7]. Her work is a de facto standard to design privacy-aware systems and was extended [8] and commented many times to make it even more valuable for the community. Unfortunately PbD cannot be used to rate surveillance technology but should be used to improve the privacy score of systems before they are deployed.

Privacy Impact Assessments (PIA) are a powerful tool to describe, rate and improve the privacy protection of data processing systems. Many different approaches, e.g., [9], exist that all have a common process. First the system is described in detail to identify all relevant data flows. For example the auditor has to list and understand the information flows between the backend data storage and the user interface, as well as the access used by administrators during maintenance. Those flows get rated by the probability that data is lost and the possible harm resulting in the data loss. After that step the PIA process tries to solve or mitigate risks for privacy. All this detail leaves PIAs to time and resource demanding to be used for a first and fast assessment of many technologies.

Fully automatic methods for privacy rating in technology exist, but are typically limited to Smartphone Apps [10] or the terms of service [11] from websites. These systems work by parsing machine readable files, i.e., the terms of service, and rate them. As no such files exists in surveillance systems we decided to develop a semi-automatic process that guides an operator through rating a system.

3 MEASURING PRIVACY AND DATA PROTECTION

The new rating scale was designed to get a quick overview of privacy impact of existing technology. The analysis itself is not at detailed as performing a PIA but much faster and feasible for small groups or single persons. Compared with a PbD based analysis it is able to rate privacy risk, but not able to mitigate or solve them.

3.1 Pre-Assessment screening

Before the actual assessment starts the auditor should have a medium level of details on how the system works. He needs to understand which sensors collect data, how data is processed and stored and how he can interact with the system. In contrast to performing PIA no deep understanding of the underlying technology and communication of the individual parts of the system is needed.

The pre-assessment ends with an initial screening visualized in **Fig. 1**. If a (surveillance) system does not collect, process or evaluate personal identifiable information (PII), e.g., a gas chromatography drug detectors, it might not need a full assessment. In those cases the technology receives the maximum score. The second question in the pre-screening checks if the systems might produce data that can be mapped to an individual person. This might be the case, if you have a system, e.g., a GPS bug, which records only timestamps and the location of itself. This information alone is not critical for privacy. But when you are able to map this location to an individual person, i.e., you planted the bug on a suspect's car, you have to do the full assessment to understand privacy impact involved.

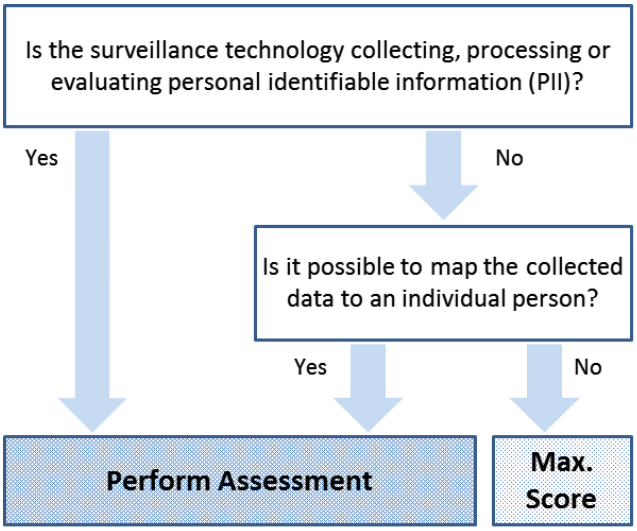


Fig. 1: Initial Screening

3.2 Assessment questions

To do the actual assessment the auditor has to answer 9 different questions about the technology and its handling of data. The answers are either yes/no or he has to choose one of up to three answers. Next to the score depending on the answer the auditor selected, every question is assigned with a weight. This weight is predefined and represents the different importance of the questions. So it is much more effective for privacy if data collection is selective, i.e., not every person but only a small number of subjects is affected, than if the data collection is minimized, i.e., the data collected from subjects is minimal. Privacy score comes with a predefined set of weights for the different questions. When the scenario demands it, an auditor can alter the weights to represents his needs. Of course one has to use the same set of weights over all assessments to allow a comparison of different systems. The assessment questions are separated into three different categories.

3.2.1 Data collection

The assessment questions shown in

Table 1 rate data collection; important factors are the selectivity of the collection, used minimization and anonymization steps.

Table 1: Data collection

Q. No.	Question	Scoring range	Weight
C1	Is the collection of data selective?	0 = no, all person are affected; 1 = some selectivity ; 2 = only subject(s) are recorded	3
C2	Is the amount of collected data from the subject minimized?	0 = no 1 = yes, only needed data is collected	1
C3	Is the collection done overtly or covertly?	0 = covertly	1

	1 = overtly

In terms of data collection the most important aspect is the selectivity of the surveillance measure. In an ideal case only the subject or subjects intended should be under surveillance. This is the case for a cell phone location tracking when the current position of a subject is collected. Even when many other people are around the subject their privacy is not affected. In case of a video surveillance this is not possible. The installed cameras will record every person in the area under video surveillance, but only when they enter such an area.

Data minimization concerns only the collected data of the subjects in the focus of surveillance not the selectivity. A system with high scoring, i.e., a cell phone location tracking, only collects data of interest. Systems that collect data that is not needed score zero points here.

The last question in data collection is, if the surveillance measure is done overtly or covertly. While important for transparency and in some cases even supportive for the surveillance task, i.e., overtly installed video surveillance cameras might discourage certain crimes, not all surveillance systems, e.g., planting a phone bug in a subject's car, can operate overtly.

3.2.2 Data access and use

The assessment questions shown in Table 2 rate data access and use; important factors are the access control to the data and how data is protected against unlawful processing.

Table 2: Data access and use

Q. No.	Question	Scoring range	Weight
A1	Who has access to the data?	0 = open access to data 1 = access is limited to reasonable stakeholders	2
A2	Is there a clear regulation who is allowed access under which circumstances?	0 = no 1 = organizational regulation exists 2 = regulation is enforced by technical measures	1
A3	Is there a protection against function creep?	0 = no 1 = yes	3

The question who has access to collected data is very important. When data is accessed by a broad variety of people a surveillance measure has a strong negative privacy impact. This could be the case when the evaluation of a CCTV system becomes crowdsourced [12].

Even when data is processed by defined users the question remains how access to the data is regulated. In the best case there is a clear regulation on who is allowed to process the collected data that is enforced by technical measures. In a less strict version this regulation exists but is only guaranteed by an organizational measure.

A protection against function creep, i.e., collecting data for a defined purpose and processing is for another one, should have high priority for data protection. This is at the same time one of the most effective measures to protect privacy and hard to achieve.

3.2.3 Data protection

The assessment questions shown in Table 3 rate data protection; important factors are the protection against theft and manipulation of data.

Table 3: Data protection

Q. No.	Question	Scoring range	Weight
P1	Is the collected data encrypted or otherwise access protected?	0 = no access restrictions 1 = yes encryption or other access control in place	1
P2	Is the data protected against	0 = no	2

	manipulation?	1 = protected against external manipulation 2 = protected against external an internal manipulation	
P3	Is the collection device secure against data theft?	0 = no 1 = yes or not applicable	1

When storing data some important questions about data protection have to be answered. As data from surveillance systems is critical to privacy the data should be encrypted or otherwise protected against unauthorized access.

Measures should be in place to protect data against internal, i.e., malicious employees, and external attackers, i.e., targeted attack against evidence by hired hackers.

When deploying mobile technology, like an audio bug or a hidden camera, that stores the data internally, this storage should be protected against attackers that steal the device and try to extract the data.

4 EXAMPLE OF TECHNOLOGY RATING

In this chapter an example for a technology rating is shown. More technology ratings and more details can be found in the deliverables of the SURVEILLE project [6].

4.1 Technology: Closed-circuit television (CCTV)

4.1.1 Description of the system under assessment

Closed-circuit television (CCTV) is a setup of video cameras to transmit a signal from a specific place to a limited set of monitors. The signal is not openly transmitted though it may employ point to point (P2P), point to multipoint, or mesh wireless links. CCTV technology is most often used for surveillance in areas that may need monitoring to prevent or prosecute crimes.

The images in a CCTV system are captured through the lens of the camera and projected onto a high resolution CCD chip that converts the image into a large collection of digital data that is stored and transmitted along the interconnects (wired or wireless) of the CCTV system to television monitors or a storage server.

The data obtained with CCTV cameras is often stored on a digital video recorder or on a computer server.

A growing development in CCTV technology is the application of internet protocol (IP) cameras. These cameras are equipped with an IP interface, enabling the incorporation of the camera in a Local Area Network (LAN) to transmit digital video data across. Optionally, the CCTV digital video data can be transmitted via the public internet, enabling users to view their cameras through any internet connection available. For professional secure applications IP video is restricted to within a private network or is recorded onto a secured remote server. IP cameras can be wired (LAN) or wireless (WLAN).

The CCTV system under assessment is placed in a busy town square. The system is operatoted by the local police and helps the security staff to fight crimes especially common for such places in the late evening and night, i.e., fighting, drug trafficking, harassmet by drunks. Collected data is live evaluated by security staff that alerts mobile security officers in emergencies. Additianly the video data is stored up to 48 hours and can be used as evidence by court or to clarify on incidents after they happened.

4.1.2 Assessment results

A video surveillance systems operating in a public place clearly processes PII and needs a full assessment. The results are shown in Table 4, overall the CCTV system described earlier achieves **11 points**. The detailed assessment is discussed in the following section.

Table 4: Assessment of a CCTV system for overt use in public places

Q. No.	Question	Points	Weight	Score
	Data collection			
C1	Is the collection of data selective?	1	3	3
C2	Is the amount of collected data from the subject minimized?	0	1	0
C3	Is the collection done overtly or covertly?	1	1	1
	Data access and use			
A1	Who has access to the data?	1	2	2
A2	Is there a clear regulation who is allowed access under which circumstances?	1	1	1
A3	Is there a protection against function creep?	0	3	0
	Data protection			
P1	Is the collected data encrypted or otherwise access protected?	1	1	1
P2	Is the data protected against manipulation?	1	2	2
P3	Is the collection device secure against data theft?	1	1	1

Data collection: As with many typical CCTV systems, this one is installed in an area with a high crime rate. The selectivity could be further increased when the system is only operated in hours with a high probability for crime. (C1:1 => some selectivity) The video data is not minimized. This could be improved by blurring subjects' faces in the operators view while still storing unmodified date for prosecution (C2:0 => no data minimization). The collection is done overtly. (C3:1 => system operates overtly)

Data access and use: The data collected by the CCTV system in the scenario is only available for a team of operators and in special cases for law enforcements. (A1:1 => access is limited to reasonable stakeholders) Regulations what the operators are allowed to do with the collected data exist and are required by law in most member states of the EU. Nonetheless no technical measure protects the people under surveillance from an operator that uses the system to look at woman instead of monitoring the area for crime. (A2:1 => organizational regulation exists) As with many surveillance systems no sufficient protection against function creep exists. (A3:1 => no)

Data protection: Typical CCTV systems store video footage in an archive, this archive is protected by access control (P1:1 => yes encryption or other access control in place). Special measures are in place to protect the archive from external attacks against the video archive. Typical no sufficient protection exists against internal attackers trying to manipulate the collected data. (P2:1 => protected against external manipulation). As the collection device does not store the data internally but in a secure data center, no data protection issues arise if the device is stolen. (P3:1 => yes or not applicable)

4.2 Assessment results

In the next chapter we will give an overview over the assessment of different surveillance technologies done in the EU project SURVEILLE [6]. This was done as an example to demonstrate how to use the assessment tool, not as an exhaustive assessment of every surveillance technology imaginable.

Table 5 gives an overview of the assessment results. The different surveillance technologies and their weighted score in the different assessment questions are shown. For example the weighted score for data collection question 1 (SC1) = score (C1) x weight score (WC1). The last column of the table gives the sum of all weighted scores.

Table 5: Overview technology assessments

Technology	SC 1	SC 2	SC 3	SA 1	SA 2	SA 3	SP 1	SP 2	SP 3	∑
Explosives detector near harbor	-	-	-	-	-	-	-	-	-	21
Gas chromatography drugs detector	-	-	-	-	-	-	-	-	-	21
Sound recording bug in subject's vehicle	3	0	0	2	1	0	1	-	1	-
Closed-circuit television (CCTV); Public place – used overtly	3	0	1	2	1	0	1	2	1	11
Closed-circuit television (CCTV); Public place – used covertly	3	0	0	2	1	0	1	2	1	10
Covert photography in a public space	6	1	0	2	1	3	0	4	0	17
Platform Micro Helicopter	6	1	0	2	1	3	0	4	0	17
AIS ship location detection and identification	0	1	1	0	0	0	0	0	0	2
Eqo security scanner ("full body scanner")	3	1	1	2	2	3	1	4	1	18
Cellular Phone Location Tracking	6	1	0	2	1	0	1	2	1	14

4.3 Analysis of results

The results of the rating done above are interesting on different levels. Although privacy score needs only a limited level of detail not every selected technology could be rated by the SURVEILLE project as some technical details are not known to the public. This of course would not be the case if privacy score was used by an end user wishing to decide between multiple different technologies matching his surveillance needs.

Some pieces of technology, like explosive detectors near harbors and gas chromatography for drug detection, fulfill highly important safety and security tasks without the need to process PII. Such system should be used whenever possible as they have no negative impact on privacy.

The score of one technologies is especially surprising. Smith's eqo security scanner, often called full body scanner or even nude scanner, has a score of 18. Therefore it is one of the best technologies in the test. In fact it is the only technology processing PII with such a high score. At first glance this is surprising as a huge privacy debate started when full body scanners where first introduced. The high score can be explained by the fact, that many different measures were introduced to prevent the privacy risk discussed in the media. Older technology, e.g., video surveillance which was introduced long before the citizens had developed a higher level of privacy concern, often lack this discussion and integration of Privacy Enhancing Technologies (PET).

5 CONCLUSION AND OUTLOOK

Rating the privacy risks of surveillance technology is an extremely complicated matter. All existing methods to rate the privacy risks of an existing technology are too complicated and typically will take months to perform on a single technology. A further restriction is that a rating is only feasible if enough details about the technology and the usage scenario are known.

To cope with those problems we developed a simplified rating system that can solve many of the existing problems. It will yield in less detailed results than a conventional audit, but it is possible to rate a technology in hours and not in months. This makes it a good tool in preselecting possible systems or decide between multiple technologies able to perform the same surveillance task.

As the same surveillance technology, i.e., a video surveillance system, could be designed in different ways, altering the audit result. This is critical for how to use the system presented. The system does not aim to provide technology operators with a catalog of all existing technologies in which they can select the best technology for their task. While such a catalog is desirable, too many small details influence the rating making it an impossible task. To correctly deploy the system an operator has to rate all available technologies with the full detail of their configuration for his special task. Only this leaves him with scoring results usable to compare technical data protection features.

So far privacy score can be used to assess the technical data protection parts of a surveillance system. While not every aspect of privacy can be measured in such a way, it is desirable to extend the system to allow for a more detailed look of privacy. Of course this has to be done in a way that does not make the system complicated to use or too time consuming.

5.1 Acknowledgment

This work was partially funded by the KASTEL project by the Federal Ministry of Education and Research, BMBF 01BY1172 and the SURVEILLE project in the 7th Framework Program by the European Commission (Project reference: 284725).The views expressed are those of the authors alone and not intended to reflect those of the Commission.

6 REFERENCES

[1] D. J. Solove, Nothing to hide: The false tradeoff between privacy and security, Yale University Press, 2011.

[2] B. Schneier, „Schneier on Security” 2008. [Online]. Available: https://www.schneier.com/essays/archives/2008/01/what_our_top_spy_doe.html. [Last accessed 11 June 2015].

[3] E. Krempel und J. Beyerer, „TAM-VS: A Technology Acceptance Model for Video Surveillance” In Privacy technologies and policy: 2nd Annual Privacy Forum, APF 2014, Athens, Greece, Springer International Publishing, 2014, pp. 86-100.

[4] S. Patil, B. Patruni, H. Lu, F. Dunkerley, J. Fox, D. Potoglou und N. Robinson, „Public Perception of Security and Privacy” RAND Corporation, 2015.

[5] A. Adams, „Multimedia information changes the whole privacy ballgame” In Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions, ACM, 2000, pp. 25-32.

[6] SURVEILLE Project, „SURVEILLE deliverables” [Online]. Available: http://surveille.eui.eu/research/publications/. [Last accessed 11 June 2015].

[7] A. Cavoukian, „Privacy by design: The 7 foundational principles” Information and Privacy Commissioner of Ontario, Canada, 2009.

[8] C. Bier, P. Birnstill, E. Krempel, H. Vagts und J. Beyerer, „Enhancing Privacy by Design from a Developer’s Perspective” In Privacy technologies and policy: 1st Annual Privacy Forum, APF 2012, Limassol, Cyprus, 2014, pp. 73-85.

[9] UK, Information Commissioner’s Office, “Privacy Impact Assessment”, UK, 2009.

[10] Carnegie Mellon University, „Privacy Grade” [Online]. Available: http://privacygrade.org/. [Last accessed 11 June 2015].

[11] Hugo Roy and ToS;DR team, „Terms of Service; Didn't Read” [Online]. Available: https://tosdr.org/. [Last accessed 11 June 2015].

[12] B. Schafer, „Crowdsourcing and Cloudsourcing CCTV Surveillance” DuD, July 2013.

ON THE SECURITY OF PUBLIC CLOUD STORAGE

Steffen Müller[1], Frank Pallas[2], and Silvia Balaban[3]

[1] st.mueller@kit.edu, [3] silvia.balaban@kit.edu
Karlsruhe Institute of Technology (KIT), Competence Center for Applied Security (KASTEL), Am Fasanengarten 5, 76131 Karlsruhe (Germany)

[2] frank.pallas@kit.edu
Karlsruhe Institute of Technology (KIT), Center for Applied Legal Studies, Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe (Germany)

Abstract

The broadly accepted and undisputed economic benefits notwithstanding, cloud computing, and particularly cloud storage, raises many security-related and legal qualms: Every enterprise considering to utilize cloud storage has to deal with compliance and security restrictions. In order to address these, cloud providers offer more and more security mechanisms for their services. At closer inspection, however, such mechanisms often are of limited value. In order to assess the security of existing cloud storage services, we build a generic usage model for public cloud storage integrating perspectives from the law and from economic agency theory as well as a respective basic threat model. Using these models, we then examine selected security mechanisms of two well-known public cloud storage services—Amazon S3 and Google Cloud Storage—and briefly sketch auspicious starting points for future research.

Keywords: Cloud Storage, Security, Threat Model, Usage Model, Data Protection, Agency.

1 INTRODUCTION

The major downside of—for other reasons often—advantageous cloud computing, and particularly of cloud storage, is that there are many security-related and legal qualms. In order to allow their customers to address and mitigate these qualms, cloud providers offer more and more security mechanisms for their services. For example, Amazon provides different ways of data encryption for Amazon Simple Storage Service (S3). Based on these mechanisms, application developers shall be able to securely employ cloud storage within higher-level applications.

The practical possibilities and implications of these mechanisms are, however, not yet sufficiently understood on a well-structured, sustainable, and transferable basis. With regard to the engineering of legally compliant cloud applications and for ensuring appropriate security within such applications in general, this is clearly unsatisfactory. In order to provide a first basis for analyses, assessments, and comparisons of existing cloud storage services in matters of security, we thus herein propose a generic usage model (section 3) as well as a basic threat model (section 4) for public cloud storage. Furthermore, we exemplarily apply these models to a single security threat and the respective security mechanisms of two well-known public cloud storage services—Amazon S3 and Google Cloud Storage—to demonstrate the fundamental applicability of our models (section 5). As we will see, our approach has the potential for making considerations about cloud storage security more structured, thorough, and comparable. First of all, however, we present some background motivating our deliberations and related work.

2 BACKGROUND AND RELATED WORK

In this section we introduce background information needed for the understanding of this paper. Therefore, we start by describing public cloud storage (section 2.1). Afterwards, we briefly introduce the relevant legal background (section 2.2). Next, we describe a notion of economic agency theory (section 2.3). We close this section with related work (section 2.4).

2.1 Public Cloud Storage

Public cloud storage provides virtually unlimited capacity to users on demand over broad network access while it is, usually, paid per use. The presumably most prominent examples of cloud storage are Dropbox and Amazon S3. However, Dropbox and Amazon S3 are of fundamentally different nature. Dropbox—like Wuala, Microsoft OneDrive, etc.—primarily approaches end users and provides file synchronization as well as sharing functionality for direct file access. Services like Amazon S3, in contrast, are rather aimed at developers using them through an application programming interface (API) to implement own functionalities upon these services. In the following, we concentrate on this Infrastructure-as-a-Service (IaaS) publicly available cloud storage for which we herein use the term "cloud storage".

For cloud storage, we distinguish—similarly to NoSQL systems that are typically running in the background of cloud storage—at least four different types: cloud storage with a key-value, column-oriented, document, and relational data model. Additionally, there are some other data models like graph data models and so on which are, though, rarely available publicly as cloud storage. Amazon S3 and Google Cloud Storage are examples for cloud storage with a key-value data model. Prominent instances for column-oriented cloud storage are Google Cloud Datastore or Amazon DynamoDB. Amazon Relational Database Service and Microsoft Azure SQL-Database are cloud storages with a relational data model. Last, Microsoft Azure DocumentDB is an example with a document data model.

Cloud storage has typically two different Application Programming Interfaces (API): A "management" and an "access API".[1] Using the "management API", a user can administer the cloud storage, e.g., he can initialize the service and manage data, user accounts, and access restrictions. The "management API" is, therefore, usually accessible over a SOAP- and/or REST-based web service and often additionally via a web application. Such "management web applications" are, for example, the Amazon Web Services (AWS) Management Console or the Google Developers Console. The "access API", on the other side, is usually only realized as a web service or—in the case of relational cloud storage—via vendor specific database drivers. For instance, if a user starts a MySQL instance in AWS, he accesses the database via the MySQL database drivers with the cloud storage's private or public IP. Through the "access API" a user can use the cloud storage, i.e., manage the data, from an own application.

As cloud storage is accessible from nearly everywhere over the Internet and all data stored in it resides in the cloud storage provider's data center, it must be secured carefully. This results in different requirements for confidentiality, integrity, availability, etc. Therefore, the security challenges and threats for cloud storage security, generally speaking, stem from diverse security sub-disciplines like database, web application, web service, and general security engineering [2]. Hence, securing cloud storage for building secure applications on top of this is of outstanding importance.

2.2 Legal Requirements for Public Cloud Storage

From a legal perspective, security aspects of cloud storage especially arise with regard to data protection regulations. Data protection law is focused on the protection of the data subject's fundamental right for informational self-determination which can be infringed by collection, processing and use of personal data. In data protection law, particularly relevant roles are the data subject (the one who needs to be protected), the controller ("cloud user"), the processor ("cloud application provider"), and the subcontractor of the processor ("cloud storage provider").

Within cloud computing cases, the relation between a cloud user and a cloud provider is usually classified as a so called "processing on behalf of the controller" [3]. This processor-controller model assigns the fulfillment of the data subject's rights to the "controller". In particular, the data subject can assert to rectify, erase, and block data which has been collected concerning him or her from the controller. The legal concept of "processing on behalf of the controller" furthermore requires the controller to supervise his processor concerning the compliance with data protection regulations. This means that the controller not only needs to verify that required

[1] This distinction is not always selective, as the API is often indistinguishable. However, it is a conceptual distinction of the functionality of the API. The distinction is based on the Storage Networking Industry Association for the Cloud Data Management Interface in [1].

technical and organizational measures are actually taken by the processor before the data processing begins but also as long as the “processing on behalf of the controller” continues. The fulfillment of all these rights and especially the data subject’s rights are, however, hardly feasible for the controller in the context of cloud computing, as he is not in the position to reliably assess the actual conduct of the cloud provider. Real control options are therefore difficult to accomplish and mostly restricted, as on-site controls and inspections basically require excessive efforts [4] and cannot guarantee a proper conduct of the cloud provider with the data of the data subject. This problem is all the more intensified in cases where cloud providers are using subcontractors, as it becomes increasingly invisible to the cloud user what happens with the data of the data subject. The use of subcontractors itself is only legally admissible within data protection law if the controller agrees in writing to the processor’s use of subcontractors. Even then, however, it has to be ensured that the legal requirements of the concept of processing on behalf of the controller are also respected within the sub contractual relationship. The cloud user therefore also has to fulfill his control rights against the subcontractors of the processor. He still remains, also across such service levels, the one who is responsible for fulfilling the data subject’s rights.

Therefore, matching cloud computing—and particularly cloud storage—to the legal model of processing on behalf of the controller is significantly challenging. A generic usage model of cloud storage like the one presented herein will clearly help clarifying the duties emanating from data protection law and assessing respective challenges related to security.

2.3 Economic Agency Theory and Public Cloud Storage

The inexpediency of established models for ensuring appropriate security in the context of cloud storage is by far not limited to the legal domain. Beyond the traditional security requirements, cloud-specific instruments also have to address a fundamental conflict of interests between the cloud storage provider and the cloud storage user: Basically, the main interest in maximizing—or at least achieving a minimum level of—security lies with the cloud storage user who might have to fulfill certain legal duties (section 2.2) or who for other reasons wants to ensure certain security criteria to be met. The cloud storage provider, in turn, accounts for the overall security architecture that stored data are subject to, holds the power to decide on the security-related efforts actually being made, and has—without further measures being taken—a clear incentive to minimize these security-related efforts. This, in turn, results in a fundamental conflict of interests between the cloud storage provider wanting to minimize his security-related efforts and the cloud storage user who would profit from higher efforts but who is not able to reliably verify the measures actually taken by the cloud storage provider. The same fundamental conflict of course also emanates in further relations, e.g. between a cloud storage user and his respective customers.

From an abstract perspective, cloud settings and the fundamental conflicts resulting from them can—not only in matters of security—be understood by means of economic agency theory [5], leading to three abstract challenges having to be solved [6]: Adverse selection, moral hazard, and hold-ups. Of these, a particular relevance for security can be identified for adverse selection, emanating from a prospective cloud storage user’s inability to assess the security capabilities of the cloud storage provider and leading to a “race to the bottom”, and for moral hazard, resulting from a cloud storage user’s general inability to monitor the cloud storage provider’s security-related conduct as well as relevant surrounding conditions, again leading to incentives for the provider to underinvest in security or even to exploit the cloud storage user’s data. In addition to those aspects already arising in traditional security-related settings, any sustainable approach to cloud storage security must also appropriately address these challenges in order to make the use of cloud storage feasible especially for those cases where simply trusting the cloud storage provider in matters of security is no viable option.

2.4 Related Work

There are several studies on security of and threats for cloud storage and cloud computing in general: For example, there are studies by the Federal Office for Information Security [7], by the Fraunhofer Institute for Secure Information Technology [8], and various other studies on cloud computing security in general [9], [10], [11], [12], and [13]. However, all these studies do not focus on publicly available IaaS-based cloud storage. As we lay out in the next sections, such cloud storage has specific properties and potential to be modeled in more detail in a generic

usage model containing the perspectives of different disciplines (section 3). Based on such a usage model a more sound threat model for cloud storage can be derived (section 4). To our knowledge, this is the first paper/study building such an interdisciplinary usage model and based on this threat model of public IaaS cloud storage.

3 A GENERIC USAGE MODEL FOR PUBLIC CLOUD STORAGE

As laid out above, security, legal, and economic aspects of cloud storage are of outstanding importance for the engineering of secure and legally compliant cloud-based applications on a profitable basis for the user and the cloud storage provider. In order to allow for well-structured interdisciplinary deliberations on cloud storage, we propose a generic usage model for cloud storage which integrates the different perspectives—the security, legal, and economic perspective—on cloud storage. The generic usage model is depicted in Figure 1.

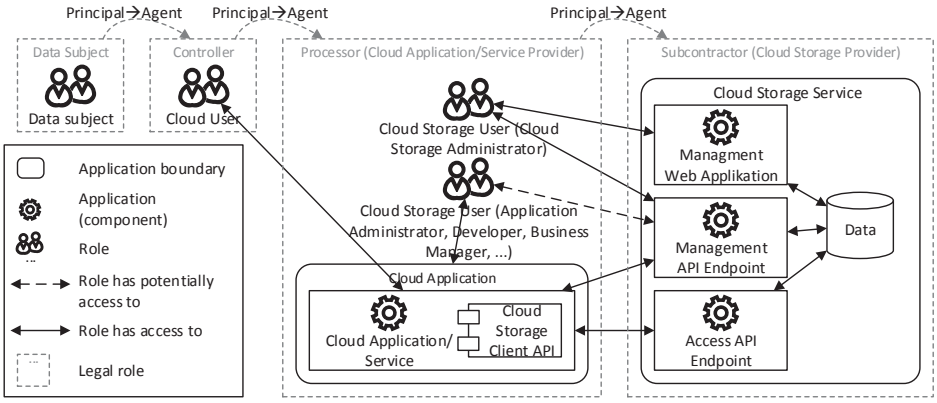


Figure 1: Generic Usage Model for Public Cloud Storage

Cloud storage systems running at a cloud storage provider's data center usually expose a "management" and an "access API" as well as a "management web application" (section 2.1). A cloud storage user employing the cloud storage of a specific provider, therefore, has to initialize the cloud storage or database over the "management web application". The initialization and initial administration of the cloud storage is done by a specific role. The "cloud storage administrator" usually has access to a root account—similar to the root account in operating systems. After initialization of the service, he can create subaccounts for other administrators, users, and applications. The further administration of the cloud storage can also be done via the "management API". For example, many functionalities of the AWS Management Console are also available directly via web services, i.e., the "management API endpoint".

To use the cloud storage within an application, cloud storage users have to utilize the "access API" of the provider. As mentioned in section 2.1, the "access API" is typically realized as a web service or it is a specific database driver. Many cloud storage providers offer downloadable and ready-to-use client API or command line tools. This "cloud storage client API" forwards the requests of the application to the web services—or the endpoints—of the cloud storage.

A cloud storage user implements an application or a service on top of the cloud storage ("cloud application"). For this, different roles can be provided, e.g., "administrators", "developers", and "business managers" which sometimes need own user accounts with specific access rights to the cloud storage. The application/service, then, is used by the "cloud user". In addition, the application may provide different further application roles. For instance, if the application is a human resource management application, there may be roles like "application manager", "case officer", "case handler", etc., which is, however, out of scope of our model. Within the implemented application, in turn, the "cloud user" may create and manage data about "data subjects" which are protected by data protection law. From the legal perspective laid out in section 2.2, the "cloud user" is thus the controller while the "cloud application/service provider" using the cloud storage is the processor and the "cloud storage provider" is a sub-contractor of the processor. Furthermore, every legal role is in a principal-agent-relationship with another legal role, as every role is in a contractual relationship with another. For example, the cloud storage user commissions the cloud storage provider to store his data in the cloud storage provider's data center (section 2.3).

4 A BASIC THREAT MODEL FOR PUBLIC CLOUD STORAGE

Having specified a generic usage model for cloud storage in the previous section, we now derive a basic threat model that can be extended for specific use cases and then can be used for threat analyses. For building the threat model, we used Microsoft's Security Development Lifecycle (SDL) that is described in more detail, e.g., in [14]. The resulting threat model is depicted in Figure 2.

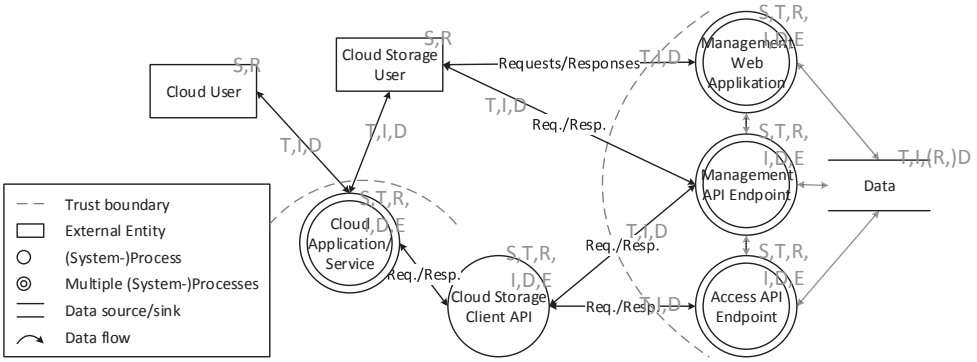


Figure 2: A Threat Model for Public Cloud Storage

A SDL-based threat model is based on a data flow model which consists of five basic elements: (System) Processes, external entities, data sources/sinks, trust boundaries, and data flow between all these entities (see: legend in Figure 2). Afterwards, every element of the data flow model can be analyzed for generic threats. Therefore, the SDL uses the STRIDE approach [14]. STRIDE is an acronym for the generic threats "spoofing", "tampering", "repudiation", "information disclosure", "denial of service", and "elevation of privileges".[2] These generic threats may occur in different model elements. For example, "spoofing" may occur in processes and external entities, i.e., in the processes "management web application", "management API endpoint", "access API endpoint", "cloud storage client API", and "cloud application/service" as well as in the external entities "cloud storage user" and "cloud user".

To apply this basic threat model to specific use cases—e.g., building a human resource SaaS-application based on Google Cloud SQL or a video streaming portal for classic music based on Amazon S3—, we then have to adopt the basic threat model. Furthermore, we have to consider the specific threats for this use case and the specific cloud storage. In doing so, we may extend the process "cloud application/service" as well as the external entities "cloud storage user" and "cloud user" with further processes and external entities. Additionally, we have to consider the security mechanisms of the cloud storage. Thereby, many generic threats can be mitigated by standard security mechanisms. For example, the threats "information disclosure" and "tampering" at the data flow—i.e., the communication link—between the "cloud storage client API" and the "access API endpoint" can be mitigated by SSL/TLS as a security mechanism.

5 THREAT ANALYSIS OF AN EXAMPLE USE CASE

In this section, we apply the basic threat model to an example use case, and carry out a threat analysis for the use case. For the implementation of the use case, we therefore imagine that the Java implementation is based on Amazon S3 (section 5.1) or Google Cloud Storage (section 5.2). In the following, we assume that we are building the, already mentioned, video streaming portal for classic music.[3] The streaming portal allows users to register and, afterward, to log in and listen to concerts. Therefore, the high definition videos and audio streams are stored at Amazon S3/Google Cloud Storage. A user has to pay a monthly fee or a fee for the access to selected content via credit card. As a consequence, we have to secure the user data and the access to the cloud storage since attackers may misuse credit card information of users.[4]

[2] For more information see, for example: http://www.microsoft.com/sdl/

[3] This example is inspired by the AWS use case Digital Concert Hall (https://www.digitalconcerthall.com) of the Berliner Philharmoniker. The story is described in more detail at: https://aws.amazon.com/de/solutions/case-studies/bph/.

[4] For reasons of simplicity, we assume that the user data is also stored in Amazon S3/Google Cloud Storage. In real use cases, highly structured user data more likely is stored within a column-oriented store or a relational database.

For reasons of space, we concentrate on the threat “information disclosure” at the process “access API endpoint” as well as the data flow between the “cloud storage client API” and the “access API endpoint” (Figure 2) for the threat analysis. Additionally, we assume that we trust the cloud service provider and thus, for the time being, exclude threats arising from the agency situation between the provider and the user laid out above. To better understand the points where the threat “information disclosure” may occur, we shortly describe an example use case and map out the typical data flow for the example use case “user registration and log in”. When a user registers at the streaming portal, a new user account is created at the client (“cloud storage client API”) containing, e.g., sensible credit card information. The data are then transferred to the cloud storage (“access API endpoint”) via a web service invocation (data flow between the two processes). Afterwards, the data are stored in the cloud storage and, then, can be accessed by the client and other clients connecting to the cloud storage to log in a user at the streaming portal.

Thus, considering concrete threats of information disclosure at the process “access API endpoint” we can derive the following four threats:

1. An attacker may passively eavesdrop the communication between the “cloud storage client API” and the “access API endpoint”. For instance, an external attacker may passively eavesdrop the data. Hence, data may be leaked to the attacker (Threat I1).
2. An attacker may actively eavesdrop the communication initiated by the “cloud storage client API”, e.g., by spoofing the “access API endpoint” (man-in-the-middle attack). As a consequence, the data may be leaked to the attacker (Threat I2).
3. An attacker may access the stored data as an authorized user (Threat I3).
4. An attacker may access the stored data as an unauthorized user (Threat I4).

5.1 Information Disclosure to External Attackers: Security Mechanisms of Amazon S3

In order to mitigate threats I1 and I2, the communication between the AWS Java Standard Development Kit (SDK) (“cloud storage client API) and the Amazon S3 web services (“access API endpoint”) is secured by SSL/TLS by default [15]. As the AWS web services are authenticated by their public key, a man-in-the-middle attack is alleviated. However, it is hard to implement public key/certificate pinning for some SDK to reduce the threat I2 even more.[5]

Additionally, every request sent to the AWS web services must be authenticated. Therefore, AWS web services use a specific way to sign every request (Signature Version 4). In Signature Version 4, the requests are signed with a secret access key id, a secret access key, and some other parameters like a timestamp [15]. This prevents replaying requests of authenticated users. Alternatively, it is possible to grant temporary access to Amazon S3 using another AWS service. For authorizing users to access data in Amazon S3, we can use bucket and user policies as well as access control lists (ACL) [15]. Bucket policies and ACL are resource-based authorization mechanisms. Therefore, policies are attached to Amazon S3 resources like buckets and objects. User policies, on the other side, can be attached to user accounts, groups, and roles to grant access. In combination, these mechanisms mitigate the threats I3 and I4.

To protect the stored data against unauthorized users (threat I4), AWS additionally proposes server-side encryption of the data. Using server-side encryption, data are sent to the web services and are then encrypted. There are three different types of server-side encryption: Server-side encryption with Amazon S3-managed keys, server-side encryption with AWS Key Management Service-managed keys, and server-side encryption with customer-provided keys [15]. For the first two types, AWS provides and manages the encryption keys. For the latter one, the customer uploads an own encryption key to AWS. However, the server-side encryption does not protect the data from an external attacker gaining access as an authorized user (threat I3), as the data are decrypted automatically on access for authorized users. Furthermore, server-side encryption is not able to secure the data against AWS employees or other attackers having access to the encryption keys. So, server-side encryption is not able to diminish any principal-agent-related problems. In addition to the server-side encryption, AWS provides an already

[5] Here, we refer to the AWS Forum: https://forums.aws.amazon.com/thread.jspa?threadID=157964

implemented client-side encryption in some SDK like the Java SDK. In client-side encryption, data are encrypted before sent to the servers of AWS which mitigates the threats I3 and I4 even more.

5.2 Information Disclosure to External Attackers: Security Mechanisms of Google Cloud Storage

For accessing Google Cloud Storage from a client ("cloud storage client API"), we can choose between different Java API: A JSON API and a XML API client [16]. Both communicate securely over SSL/TLS with the Google web services. This mitigates the threats I1 and I2.

For authentication in Google Cloud Storage, we can use three different mechanisms: OAuth 2.0, cookie-based, and service account authentication [16]. Each mechanism is recommended for different authentication use cases. The OAuth 2.0 authentication is recommended for authentication on behalf of a user, e.g., for tools and applications that are provided to other users. Cookie-based authentication is a browser-based authentication for, e.g., authenticated downloads. The service authentication is recommended for server-to-server applications like, e.g., a virtual machine running on the Google Compute Engine wants to access the data stored in Google Cloud Storage. To restrict access, Google Cloud Storage provides three mechanisms: ACL, Signed URL, and Signed Policy Documents [16]. Similar to Amazon S3, ACL in Google Cloud Storage clients allow the cloud storage user to grant access to other user accounts and groups. Using Signed URL, a user can grant time-limited read or write access to anyone in possession of the URL. Signed Policy Documents provide a way to specify what can be uploaded to a bucket. Thus, Signed Policy Documents, an enhancement of Signed URL, allow to specify parameters like size, content type, and other upload characteristics which are checked when visitors upload files to Google Cloud Storage. In combination, these mechanisms mitigate the threats I3 and I4.

In Google Cloud Storage, all data stored is encrypted by default using server-side encryption [16]. Like it is the case for Amazon S3, this does again not hinder attackers who gain access as an authenticated user (threat I3) and so on. Client-side encryption is, in contrast to the Amazon S3, not implemented in any Google Cloud Storage client API. However, a client API user can implement this feature easily on his own.

6 SUMMARY AND OUTLOOK

So far, we proposed a generic usage model for publicly available IaaS cloud storage with integrated legal and economic perspective and depicted a method for conducting a structured threat analysis based on this model. We believe that on this basis a more structured investigation of security, legal, and economic challenges in the context of cloud storage can be discussed. As the cursory threat analysis for the threat of "information disclosure" to external attackers in cloud application implementations based on Amazon S3 and Google Cloud Storage already show, our proposed model and method are practically applicable.

Even at this early stage of development, we thus foresee our proposed model and method to serve various goals for future research and development on security, legal, and economic aspects of cloud storage. First and foremost, our approach shall, like any modeling scheme, foster structuredness, completeness, and explicitness and provide a basis for communication among different stakeholders across different roles and disciplines. It shall thereby heighten the quality of security assessments as well as of respective engineering activities for settings significantly involving cloud storage. Especially our generic usage model will presumably prove valuable here as it encompasses those actors, relations and architectural entities specifically relevant in the context of cloud storage.

Besides constituting a structural basis for security analyses and respective implementation activities, our model and method may also help cloud users in demonstrating the thoroughness of their security-related considerations and precautions to external parties including their customers as well as regulatory authorities. Furthermore, having in mind the fact that cloud users are typically the controller and thus bear primary responsibility in matters of data protection law (section 2.2), our approach might also help them to better select appropriate cloud storage providers and to better identify their legal responsibilities.

This does, however, also lead us to the current opportunities for improving our model which we are going to address in the future: First of all, we have to prove and refine our models in much more use cases. Furthermore, the cloud storage provider itself is currently not explicitly addressed as a potential adversary within our usage model. As delineated in section 2.3, as recognized with regard to the value of server-side encryption in sections 5.1 and 5.2, and as also underlying many legal regulations—including, in particular, the controller's verification obligations mentioned in section 2.2—, however, security threats might also arise with regard to a storage provider being not (absolutely) trustworthy. For the future, we thus plan to explicitly integrate the storage provider as a potential adversary into our threat model, too. Last but not least, we also plan to undertake further research integrating the three disciplines—cloud storage security engineering, law, and economic agency theory—on, for example, new legally compliant security mechanisms and the security implications of nested principal-agent-relationships.

REFERENCES

[1] Storage Networking Industry Association (2014). Cloud Data Management Interface (CDMI) – Version 1.1.0. http://www.snia.org/sites/default/files/CDMI_Spec_v1.1.pdf.

[2] Winkler, V. (2011). Securing the Cloud–Cloud Computer Security Techniques and Tactics. Waltham.

[3] Art. 29 Data Protection Working Party (2010). WP 196, Opinion 05/2012 on Cloud Computing.

[4] Heidrich, J.; Wegener, C. (2010): Sichere Datenwolken - Cloud Computing und Datenschutz, MMR pp.803-808.

[5] Hauff, S.; Huntgeburth, J.; Veit, D. (2014). Exploring uncertainties in a marketplace for cloud computing: a revelatory case study. Journal of Business Economics, 84(3), pp. 441-468.

[6] Pallas, F. (2014). An Agency Perspective to Cloud Computing. Proc. of the 11th Intern. Conf. on Economics of Grids, Clouds Systems and Services (GECON), pp. 36-51.

[7] Bundesamt für Sicherheit in der Informationstechnik (2012). Überblickspapier Online-Speicher. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Online-Speicher_pdf.pdf?__blob=publicationFile.

[8] Fraunhofer Institute for Secure Information Technology (2012). On the Security of Cloud Storage Services. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf.

[9] Cloud Security Alliance (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[10] Cloud Security Alliance (2013). The Notorious Nine - Cloud Computing Top Threats in 2013. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[11] European Network and Information Security Agency (2015). Cloud Security Guide for SMEs. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes.

[12] Open Security Architecture (2015). SP-011: Cloud Computing Pattern. http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing.

[13] National Institute of Standards and Technology (2011). NIST Guidelines on Security and Privacy in Public Cloud Computing. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494.

[14] Shostack, A. (2014). Threat Modeling: Designing for Security. John Wiley & Sons.

[15] Amazon Web Services (2015). Amazon S3 Developer Guide. http://docs.aws.amazon.com/AmazonS3/latest/dev.

[16] Google (2015). Google Cloud Storage – Documentation. http://cloud.google.com/storage/docs/overview.

GRAPHICAL MODEL-BASED PRIVACY POLICY EDITING FOR SMART VIDEO SURVEILLANCE

Pascal Birnstill[1], Christian Burkert[2] and Jürgen Beyerer[1]

[1] *{pascal.birnstill, juergen.beyerer}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[2] *burkert@praedmandatum.de*
praemandatum GmbH
Goseriede 4, 30159 Hannover (Germany)

Abstract

Poor usability and, as a consequence, human errors can render powerful security and privacy mechanisms useless. Borrowing from the concept of visual programming we introduce a graphical editor for authoring privacy policies for smart video surveillance systems, i.e., systems involving computer vision technology to some extent. We built this editor upon a meta model, which we derived from a generic architecture for smart video surveillance. Employing our tool, privacy-related requirements can be assembled from readily understandable graphical blocks and exported into machine-readable usage control policies. We give a demonstration based on a smart video surveillance system employed for fall detection in medical facilities.

Keywords: Smart video surveillance, privacy, usage control, policy authoring, usability

1 INTRODUCTION

Privacy-related requirements in smart video surveillance range from *which data the system extracts and analyzes* over *which data it visualizes for situation assessment* (e.g., "only anonymized video data must be exposed") to *when data must be deleted*. We typically specify such requirements in policies using machine-readable markup languages. However, editing such policies using text editors is effortful, error-prone, and requires the knowledge of technical details.

We propose a graphical policy editor for smart video surveillance based on visual programming. Assembling privacy policies from combinable graphical blocks relieves organizations that operate video surveillance systems and particularly involved system architects and administrators from knowing syntax rules and abstracts from the technical implementation. We introduce a meta-model, which provides our editor with semantics of a generalized smart video surveillance system equipped with a usage control enforcement infrastructure. Building on this meta model, we are able to graphically represent the operation of a smart video surveillance deployment, integrate privacy-related requirements in terms of restrictions, mechanisms and obligations, and export XML-based policy syntax. We instantiate our editor for a scenario, in which smart video surveillance is deployed for fall detection in a medical facility in order to illustrated how it is employed.

This approach is application-oriented in a sense that we do not aim to entirely cover the complexity of the policy specification language. In this sense, we do not provide a usage control policy editor, but a tool for modelling common privacy requirements, which we translate into usage control policies.

Our contributions are (i) a convenient and efficient approach for specifying privacy policies for smart video surveillance measures, (ii) an easily understandable

representation of the behavior of a smart video surveillance system, and (iii) machine-readable policies understood by a usage control infrastructure.

1.1 Distributed Usage Control

Usage control [3] generalizes access control to the time after the initial access to data. Requirements include rights and duties, e.g., “data must not be forwarded”, “data must be deleted after 30 days”, “usage of data must be logged”. Usage control requirements are specified in policies referring to intercepted events in the workflow of a system. In distributed setting, i.e., forwarding data with an attached policy to another system, usage control requirements can be enforced on the receiver’s machine, too, requiring appropriate usage control enforcement mechanisms at the receiving end [6].

1.2 Usage Control Enabled Video Surveillance Architecture

Using our policies, we govern a smart video surveillance system design, which provides at least three operational modes. Its *default mode* is optimized for privacy: It collects and reveals a minimal amount of data. Event-specific *assessment modes* create views of the scene and available meta-data, such that human operators can distinguish critical incidents from false alarms. At this stage, we still protect observed people's privacy as far as possible, typically by applying anonymization techniques before exposing video data. Finally, *investigation modes* unlock additional functionality for handling a specific type of incident and may involve deeper privacy intrusions. However, usages are logged and coupled to critical incidents detected by the system. By this means, usage of such functionality in a groundless and unjustified manner can be revealed in hindsight.

2 SMART VIDEO SURVEILLANCE META MODEL

In the following paragraphs we introduce a smart video surveillance meta model, which provides entities for modelling components, data structures, data attributes, and mechanisms commonly found in such systems. It enables designers of concrete surveillance systems to model their individual deployment with particular focus on privacy-related requirements.

2.1 Sensors

A sensor is typically attached to a wall or a ceiling and does not change its position. Its capacity of capturing environmental signals has a limited scope. Both, its location and scope can be described as a set of spatial divisions of the monitored area as depicted in Fig. 1.

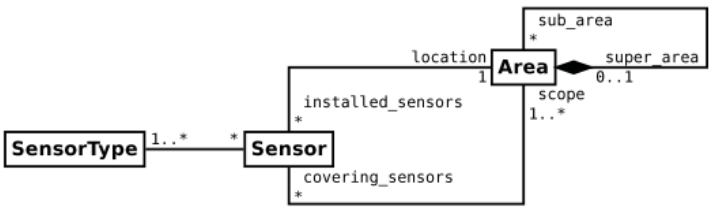


Fig. 1: Sensors have an installation location and capture signals within a spatial range

2.2 Information Persistence

In some deployments raw or processed information is stored permanently, e.g., for retrospective investigation or preservation of evidence. Smart surveillance systems usually maintain a semantic information base containing an abstraction of the observed environment's present state (*world model*) and possibly a history of state changes.

Another type of storages is archives that normally contain raw sensor data, possibly augmented with semantic tags.

A record represents a monitored object, which can be a person, but also a thing. In general, storage records comprise attributes like unique identifiers, privileges, position coordinates or face templates. Fig. 2 shows a generic storage sub-system.

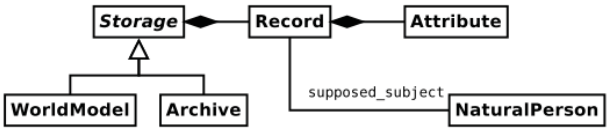


Fig. 2: State representation as records of a semantic world model and an archive

2.3 Information Embedded in Raw Sensor Data

Raw sensor data may contain information, which the surveillance system cannot extract or is not configured to extract. Unless explicitly given, the surveillance system is unaware of the possible existence of such embedded information. However, this kind of information is required, e.g., for describing privacy filters that aim at obfuscating certain features of person's visual appearance before releasing the data to a human operator.

Figure 3: Modelling which human attributes may be embedded in raw sensor data allows us to deploy according privacy mechanisms

Therefore our meta model covers human attributes, which are implicitly captured by sensors, described in record attributes, or affected by modifiers (cf. Figure 3). These attributes can be grouped into categories like visual appearance or movement behavior or, for instance, according to their privacy sensitivity as defined by company regulations or legislation (cf. § 3 (9) German Federal Data Protection Act).

2.4 Information Representation: Viewers

Human user interfaces provide operators with a suitable selection of information for assessing a recognized activity or situation. In our meta model, *viewers* generate a particular visualization of given data. We distinguish two types of viewers (cf. Fig. 4). *Raw viewers* generate a representation of raw sensor data or at least include such a one, whereas *rendering viewers* construct entirely synthetic views. This distinction accounts for the particular risk that raw sensor data may contain privacy sensitive data, which the system is not aware of when releasing data (cf. 2.3).

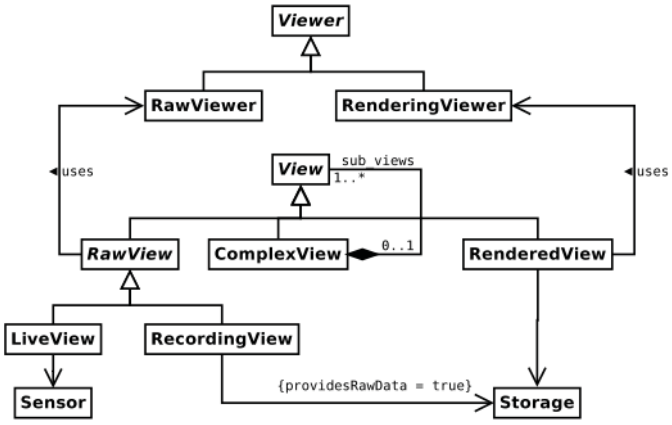


Fig. 4: Views represent a subset of their source's information, selected and composed by the used viewer

Views are concrete applications of viewers for a specific source of data. As depicted in Fig. 4, four different types of views are modelled: *live views* apply a raw viewer to a live stream of sensor data, *recording views* apply a raw viewer to recorded raw sensor data, *rendered views* create a synthetic visualization of stored meta data using a rendering viewer, and *complex views* are compositions of multiple other views.

2.5 Modification of Raw Sensor Data

Concerning raw views, privacy regulations may require an obfuscation of sensitive attributes, whereas in other applications augmenting overlays may be useful to quickly assess a critical situation. Our meta model therefore distinguishes between *data reductions* that reduce (anonymization/obfuscation techniques) and *data exploitations* that augment the information value of presented raw data. As depicted in Fig. 5, a raw view (live and recording views) can employ data modifiers to alter the raw data. A data reduction may be reversible (e.g., encryption).

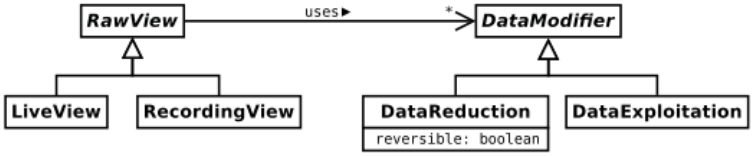


Fig. 5: Data reductions and exploitations can be associated to a raw view

2.6 Policy Structure

Our intuition of a *policy* is derived from usage control policies that can be specified as an *event-condition-action (ECA)* rule. A policy (cf. Fig. 6) is triggered by an *event*. The policy's *actions* are executed if and only if the specified *condition* concerning the event is evaluated positively by the *decider*, a so-called Policy Decision Point (PDP) in terms of usage control. An event either originates from a system internal process (e.g., the expiration of a storage permission) or from external actions (e.g., a detection of a computer vision algorithm, an operator interaction). Until now, it was not required to distinguish event origins in the meta model.

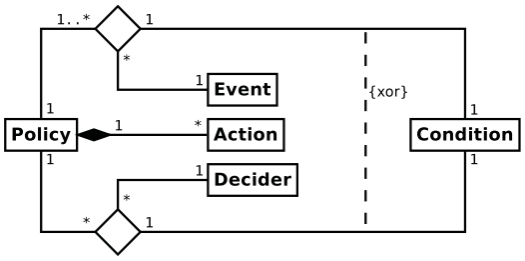


Fig. 6: Abstracted structure of (usage control) policies

3 INSTANTIATION: VIDEO-BASED FALL DETECTION IN HOSPITALS AND NURSING FACITLITIES

Due to space limitations we omit an introduction of the particular blocks provided by our graphical policy editor. Instead, we directly jump into policy authoring for the following video surveillance scenario and explain the employed blocks alongside.

3.1 Scenario: Privacy-aware Fall Detection Using Smart Video Monitoring

In our scenario, a hospital employs a smart video surveillance system for detecting falls of people in corridors and publicly accessible spaces, particularly in order to support the night shifts. We intend the system to operate according to the workflow depicted in

Fig. 7, which involves a *default mode* executing a fall detection algorithm on the video data captured by all cameras, *assessment modes* asking a nurse to differentiate between actual emergencies and false detections while preserving observed person's privacy as long as possible, and finally an *investigation mode* providing additional information for organizing emergency aid.

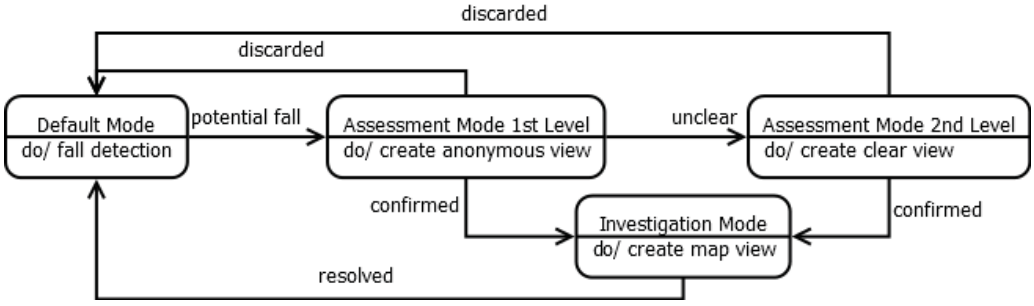


Fig. 7: Workflow for computer vision-based fall detection

3.2 Default Mode: Fall Detection Based on Computer Vision

While the system operates in its *default mode*, i.e., as long as no potential fall has been detected, data processed by the system cannot be accessed at all. Furthermore, a continously evaluated policy (cf. Fig. 8) demands that any collected data is deleted from the system's storages as soon as it is older than one minute. The storage *VideoArchive* buffers video streams from all cameras, while the storage WorldModelArchive buffers extracted meta data, such as positions of persons in the monitored area. The framing blue mechanism block represents the ECA rule structure of our policies. In addition to attaching a triggering event, a condition, and multiple actions, it can be configured to include predicates to be evaluated by some *external decider*. Policy enforcement is either *detective* or *preventive*: Detective mechanisms only react on events, while preventive mechanisms actually intercept events and are thus able to *allow*, to *inhibit*, to *modify*, or to *delay* them in case the condition has been evaluated to true.

Fig. 8 also shows the usage control policy exported into machine-readable XML format, which is understood by Fraunhofer IOSB's prototype systems *NurseEye* and *Network Enabled Surveillance and Tracking (NEST)* [7]. We omit the XML representations of the following policies due to space limitations.


```
<?xml version="1.0"?>
<policySet>
    <actionDescriptions>
        <actionDescription name="Default"/ >
    </actionDescriptions>
    <detectiveMechanism name="DefaultCleanUp">
        <description>Default mode. Periodically delete archived data.</description>
        <timestep amount="1" unit="SECONDS"/>
        <trigger action="Default" index ="ALL" isTry ="false"</trigger>
        <condition><true/></condition>
        <executeAction name="delete" pxp="WorldModelArchive">
            <constraint mode="OLDER" type ="age" unit="seconds" value="60"/>
        </executeAction>
        <executeAction name="delete" pxp="VideoArchive">
            <constraint mode="OLDER" type="age" unit="seconds" value="60" />
        </executeAction>
    </detectiveMechanism>
</policySet>
```

Fig. 8: Default mode policy, also exported as XML usage control policy

3.3 Assessment Modes: Privacy-preserving Elimination of False Alarms

Upon detecting a potential fall, the system enters the *1st level assessment mode*, which sends an alarm to the mobile device of a nurse and provides an anonymized view of the according camera's live stream and buffered video data of one minute previous to the fall detection event. As the policy *FallAssessmentL1* (cf. Fig. 9) states, the anonymized view is created using an image filter, which reduces observed people to blurred silhouettes in order to hide their identities. The nurse can proceed by either

confirming the incident, discarding the incident in case of a false detection or by requesting a *2nd level assessment mode* in case the provided view does not provide enough evidence for a proper assessment of the potential fall. Thus, false alarms of the fall detector that are recognized at this early stage do not lead to any privacy breaches for people in the range of the according camera.

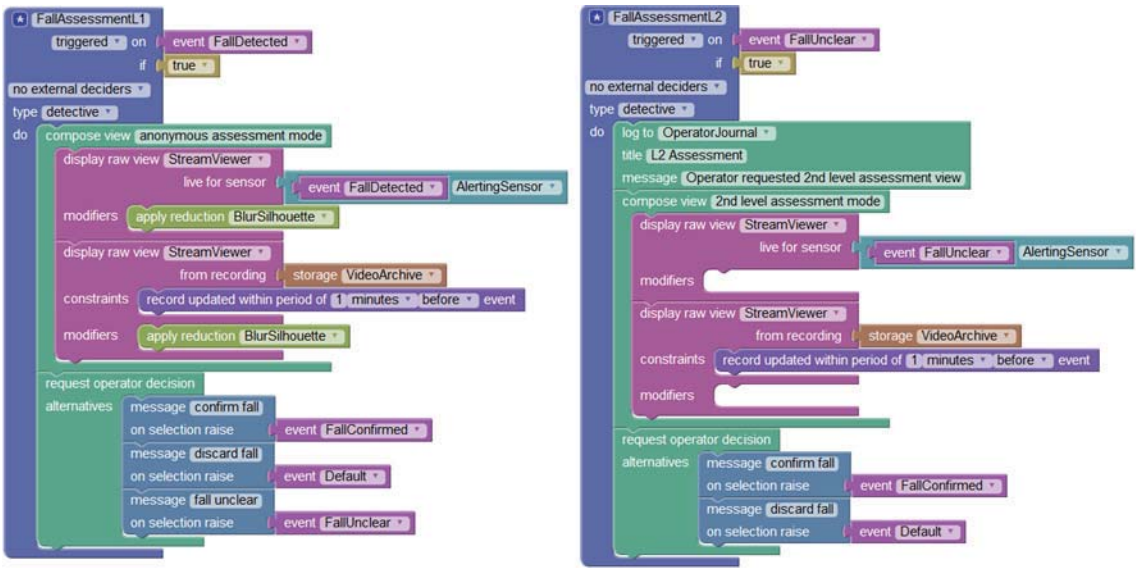


Fig. 9: Anonymized and clear assessment mode

In case the nurse cannot assess the incident properly, a *FallUnclear* event is induced, which triggers the *2nd level assessment mode*. The according policy *FallAssessmentL2* (cf. Fig. 9) grants access to the camera's live stream and the previous minute of recorded video data without enforcing the anonymization of released video data. However, each request to the 2nd level assessment mode is logged in the *OperatorJournal*, which can be accessed by employee representatives in order to detect misuse.

3.4 Investigation Mode: Handling Emergencies

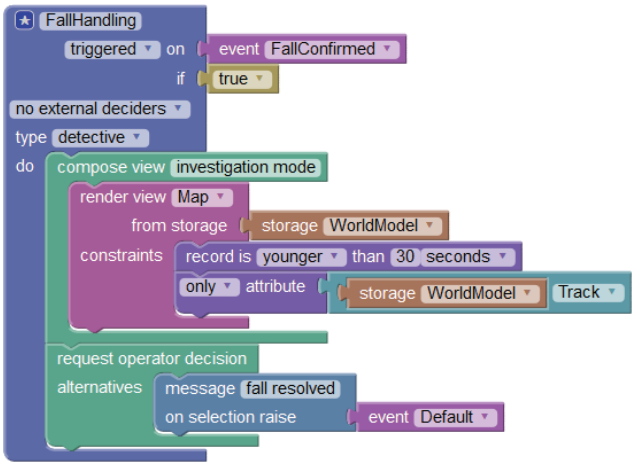


Fig. 10: Investigation mode: map view

Whenever a fall is confirmed by a nurse, the *investigation mode* of the system is triggered by the according *FallConfirmed* event. This mode creates a map view, which enables the visualization of meta data, such as positions of persons in the observed area. In our scenario, we only allow the system to release the position of the fallen person as well as the positions of other members of the medical staff. Three policies are required in order to specify these requirements.

The policy *FallHandling* depicted in Fig. 10 triggers the map view to be created and enforces global constraints: The map view is only granted access to records younger than 30 seconds from the storage *WorldModel* and, for each record, only the attribute *Track*, i.e., position records, are released. Furthermore, the system asks the nurse to give feedback after the emergency has been handled: As soon as the nurse confirms that the fall has been resolved, an *Default* event is raised, which triggers the system to switch back into its default mode.

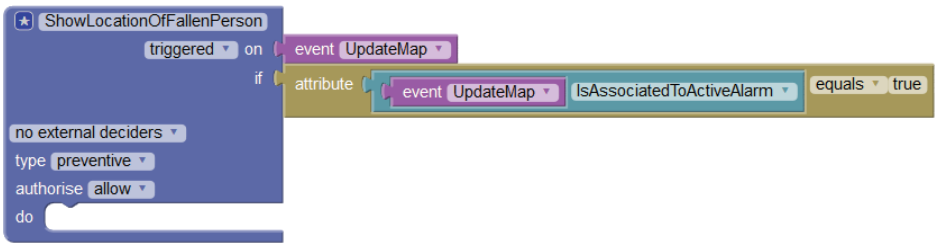


Fig. 11: Investigation mode: access to position of fallen person

Using the policy *ShowLocationOfFallenPerson* (cf. Fig. 11) we prevent the map view from accessing records other than the one associated to the active alarm to be handled, which refers to the record of the fallen person.

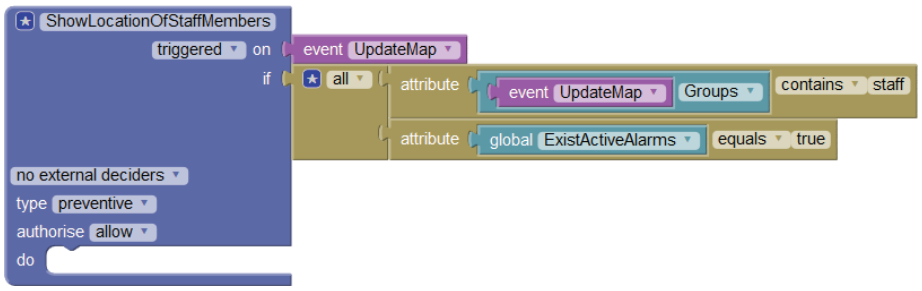


Fig. 12: Investigation mode: grant access to positions of medical staff

Finally, the policy *ShowLocationOfStaffMembers* as shown in Fig. 12 prevents the map view from accessing records other than those of members of the group *staff*. The condition also ensures that there is an active alarm whenever the records of staff members are read. By this means, the permission to access the staff members' positions expires as soon as the emergency has been handled and the system has returned into its default mode.

4 RELATED WORK

The meta model introduced in Section 2 is based on a generic usage control-enabled smart video surveillance architecture introduced in [7]. This generic architecture is derived from earlier works by Fidaleo et al. [1], Hampapur et al. [2], and Bauer et al. [4]. The meta model also incorporates the idea of establishing a "privacy grammar" in order to define privacy-sensitive (combinations of) attributes that may be embedded in or extracted from raw video data, but must not leak.

Employing dedicated assessment modes in order to implement a shifting trade-off between privacy and utility, which preserves observed people's privacy as long as at all possible is motivated by results of legal analyses conducted by Roßnagel et al. [5], as well as Bretthauer and Krempel [8]. Furthermore, the authors of [8] explicitly discuss the scenario of deploying smart video surveillance for fall detection in medical facilities, for which we instantiate our graphical policy editor in Section 3. They also argue in favor of the concept of assessment modes in order to prevent automated individual decisions entailing legal or other adverse consequences for the person(s) affected (cf. § 6 b German Federal Data Protection Act).

The presented work is clearly domain-specific, i.e., transferring the approach to another domain at least requires an according meta model to be created. However, to the best of our knowledge no prior work concerning graphical authoring of (usage control) policies has been published.

5 CONCLUSION

We presented a model-based policy editor for privacy-related requirements in smart video surveillance, which employs visual programming as an approach towards user-friendly and less error-prone policy authoring and visualization. Our meta model aims to capture the characteristics of concrete smart video surveillance systems and their applications. It can easily be adapted to future needs and upcoming features of smart surveillance systems just as the subset of usage control capabilities supported by the graphical editor can be extended in case more complex conditions have to be specified.

The obtained graphical representations of policies could also be employed to explain the operation of the system as well as the privacy mechanism in place to the people concerned in order to increase transparency. When used for this purpose, the level of abstraction of the graphical representation should be increased further in order to hide any technical details that are irrelevant from a data protection perspective.

REFERENCES

[1] D. A. Fidaleo, H.-A. Nguyen, and M. Trivedi (2004). *The networked sensor tapestry (NeST): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks*. In Proc. 2nd ACM intl. Workshop on Video Surveillance & Sensor Networks, pp. 46–53.

[2] A. Hampapur, L. Brown, J. Connell, A. Ekin, N. Haas, M. Lu, H. Merkl, and S. Pankanti (2005). *Smart video surveillance: exploring the concept of multiscale spatiotemporal tracking*. IEEE Signal Proc. Mag., 22(2), pp. 38–51.

[3] A. Pretschner, M. Hilty, and D. A. Basin (2006). *Distributed usage control*. Commun. ACM, 49(9), pp. 39–44.

[4] A. Bauer, S. Eckel, T. Emter, A. Laubenheimer, E. Monari, J. Moßgraber, and F. Reinert (2008). *N.E.S.T. - Network Enabled Surveillance and Tracking*. Future Security, 3rd Security Research Conference.

[5] A. Roßnagel, M. Desoi, and G. Hornung (2011). *Gestufte Kontrolle bei Videoüberwachungsanlagen - ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung*. In Datenschutz und Datensicherheit, 35(10), pp. 694–701.

[6] F. Kelbert and A. Pretschner (2013). *Data usage control enforcement in distributed systems*. In Proc. CODASPY, pp. 71–82.

[7] P. Birnstill and A. Pretschner (2013). *Enforcing privacy through usage-controlled video surveillance*. In 10th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 318–32.

[8] S. Bretthauer and E. Krempel (2014). *Videomonitoring zur Sturzdetektion und Alarmierung - eine technische und rechtliche Analyse*. In 17. Internationales Rechtsinformatik Symposion (IRIS) – Transparenz, pp. 525–534.

ADVANCED LASER-BASED IMAGING TECHNOLOGIES FOR SITUATIONAL AWARENESS IN UNMANNED VEHICLES

Bernd M. Fischer [1], Martin Laurenzis, Frank Christnacher, David Monnin and Alexis Matwyschuk

[1] *bernd.fischer@isl.eu*
French-German Research Institute of Saint-Louis (ISL), 5 Rue du General Cassagnou, 68301 Saint-Louis (France)

Abstract

In this article, we want to give an overview of possible application of Laser Gated Viewing in different unmanned vehicles for airborne, land/ground and submarine application. Laser Gated Viewing is studied since the 1960s as an active night-vision method. Due to enormous improvements in the development of compact and highly efficient laser sources and in the development of modern sensor technologies, the maturity of demonstrator systems rose during the past decades. Further, it was demonstrated that Laser Gated Viewing has versatile sensing capabilities with application for long range observation under all-weather condition, vision through obstacles and fog, active polarimetry and 3D imaging.

Keywords: Sensor for unmanned vehicles, Laser Gated Viewing, active polarimetry, 3D imaging

1 INTRODUCTION

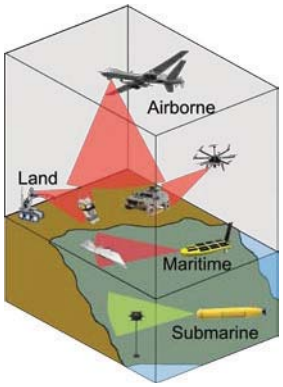


Figure 1 *Possible application of Laser Gated Viewing on different unmanned vehicles.*

Laser Gated Viewing is studied since the 1960s [1] for night vision with long range and through bad weather conditions. This method is a promising electro-optic sensor technology, which is complementary to recent night vision technologies like thermal imaging and intensified low light level image sensors. As presented in Fig. 1, Laser Gated Viewing can be used on different unmanned vehicles to deliver complimentary senor information and to assist successful mission completion. For instance, in submarine MCM (mine countermeasure) missions the search radius and identification range can be enhanced for both, a reduction of the search time and an increase of safety for man and material (i.e. “safety for staff and stuff”).

The maturity of demonstrator systems rose during the past decades, due to enormous improvements in the development of compact and highly efficient laser sources and in the development of modern sensor technologies. Scientific studies as well as high performance demonstrator systems were presented in the field of submarine vision and vision in scattering environments [2,3] and automotive applications [4,5]. Main interests

in Laser Gated Viewing can be found in target identification [6,7] and target detection by active polarimetry [8,9] as well as 3D imaging [10-13]. Laser Gated Viewing has the advantage to combine distinct sensing capabilities like the improvement of vision in poor weather conditions (fog, rain, snow, sand storm ...) or cross diffusing obstacles (smoke, turbid medium ...), the capturing of 3D scene information or the study of material properties by polarimetric analysis.

2 PRINCIPLE OF LASER GATED VIEWING

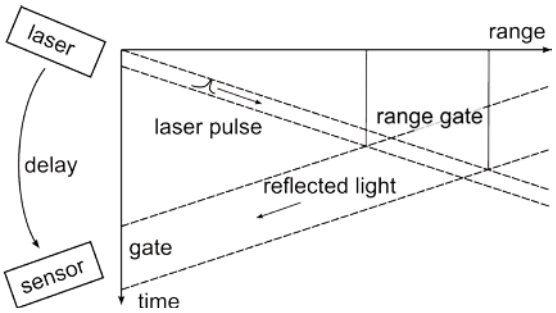


Figure 2 *Principle of Laser Gated Viewing.*

In principle, Laser Gated Viewing is the combination and synchronization of a high sensitive imaging sensor with its own pulsed laser source. This source is used to illuminate a scene at the time of observation. Usually, the divergence of the light source is matched to the sensor's field of view.

As illustrated in Fig. 2, the laser pulse illuminates a scene and is reflected or absorbed by any surfaces. A portion of the reflected light will be reflected towards the imaging sensor and carry information about the nature of the scene (like range, reflectivity and polarization). Due to the photon time-of-flight, the photons reflected at different ranges arrive at different times. The sensor gate is closed while the photons travel toward the scene and back to the sensor. The sensor is not dazzled by back-scattering photons or parasite light sources. The sensor gate opens after a certain time delay for a short integration time. Thus, only light which arrives at the sensor within the right timing window contributes to the imaging process. The range gate, which is observed in the images, is the convolution of the laser pulse and the sensor gate functions. The sensor gate delay determines the position of the range gate in the scene. Therefore, Laser Gated Viewing images contain reflectivity as well as range information.

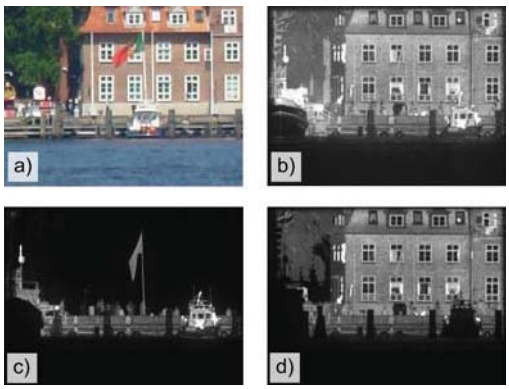


Figure 3 *Images of a scene using (a) passive imaging and Laser Gated Viewing with (b) long integration time and (c, d) short integration with different sensor gate delays.*

The differences between Laser Gated Viewing and passive imaging are depicted in Fig. 3. Here, a scene in a distance of about 1 km was observed by a passive color TV camera and an active Laser Gated Viewing system. Due to the illumination by sun light,

shadows and surface reflection can be observed in the passive image (fig. 3 a). The spectral information is represented in the color of the pixel. Using Laser Gated Viewing (fig. 3 b-d) only the reflection of the applied laser light contributes to the imaging process, the spectral information is reduced to the laser wavelength (here, λ = 1.574 µm). But, due to the low parallax between illumination and imaging device, nearly no shadow occurs in the images. Further, it is possible to look inside shadow areas and inside buildings. A long sensor integration time enables a global view on the scene with a large range gate, see Fig. 3 b). With a short sensor integration time only information from a small range gate is recorded. As depicted in Fig. 3 c)-d), it is possible to separate objects from the background and enhance their optical contrast. For example the object-to-background contrast of the flag is significantly higher in Fig. 3 c) than in Fig. 3 b). By changing the sensor gate delay it is possible to place the range gate at different distances.

3 ADVANCED LASER IMAGING

3.1 Sampling spatial three dimensional information

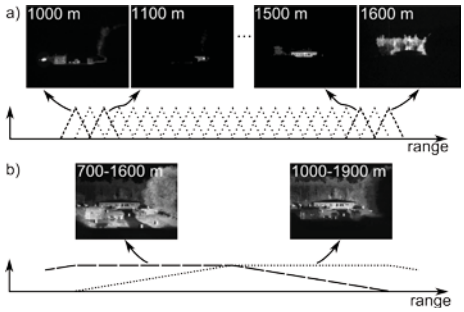


Figure 4 *Sampling range information for 3D imaging by laser gated viewing with a) a sliding range gate and b) overlapping range gates.*

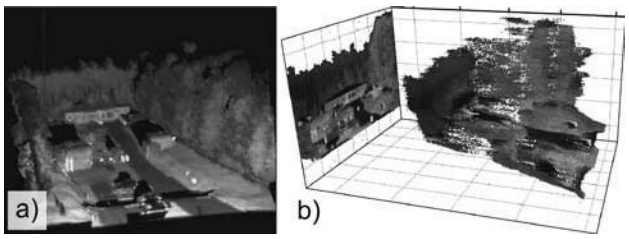


Figure 5 *Two 3D display methods of depth information: a) 3D model and b) point cloud.*

A prominent application of Laser Gated Viewing is 3D imaging. As depicted in Fig. 4, two different methods have reached high maturity and were discussed in the literature. In the sliding gate or tomography method [10] the systematic variation of the sensor gate delay is used to sample a three dimensional scene with a small range-gate (fig. 4 a). Due to the Nyquist sampling theorem, smaller range-gate and finer sensor gate delay steps lead to higher depth resolution. A huge amount of images has to be recorded to acquire a sufficient amount of data for range calculations. An alternative approach calculates depth information from a few recorded images by intensity correlation analysis [11-13]. As depicted in Fig. 4 b), this method is based on the analysis of gray level variations in overlapping range gates. Despite of the fact that the accuracy of this method depends on the signal height; it is able to significantly overcome the Nyquist sampling theorem.

The calculated depth information can be used for 3D reconstruction, 3D display and 3D analysis (point-to-point measurement). For instance, in Fig. 5, two methods of 3D display are presented. In Fig. 5 a) a 3D model of a scenario is shown. Here, the

observation point is virtually changed to an upper-left position. In Fig. b) the 3D data is depicted as a point cloud.

3.2 Active polarimetric imaging

The interaction of light with object surfaces is described in the Stokes-Muller formalism, as defined in equation (2). Here, M is the 4x4-Muller matrix which characterizes the interaction of light with the object surface. Further, S is the 4-element stokes vector which describes the properties of the light.

$$\vec{S}_{\text{detected}} = M \cdot \vec{S}_{\text{emitted}} \quad (1)$$

Polarimetric imaging is used to analyze the polarization of reflected light to reveal the nature of surfaces. Due to the nature of different surfaces, they have different impact on the polarization state. Therefore, active polarimetric imaging is a widely used method in remote sensing [8,9].

Typically, the illumination device of a Laser Gated Viewing system uses light with a strong linear or circular polarization. Even the homogenization and collimation does not harm this polarization of the illumination beam. Therefore, the polarization state of the reflected light can be analyzed to realize an active polarimetric imaging. For instance, in Fig. 6 an example of active polarimetric imaging at 808 nm and a distance of 300 m are presented. Here, the overall intensity (a) is compared with the orthogonal state contrast (OSC) for linear (b) and circular (c) polarized illumination. This measure is defined as $\mathrm{OSC} = \frac{(I_{\parallel} - I_{\perp})}{(I_{\parallel} + I_{\perp})}$ and can be calculated for each pixel from two images with perpendicular polarization. The linear and circular OSC represent the diagonal elements M22 or M33 and M44 of the Muller matrix, respectively. The OSC can be used to distinguish artificial objects from vegetation.

Figure 6 *Intensity (a) and orthogonal-state-contrast for illumination with linear (b) and circular (c) polarized laser.*

4 APPLICATION OF LASER GATED VIEWING ON UNMANNED VEHICLES

In unmanned vehicles, active imaging and Laser Gated Viewing can significantly improve sensing capabilities and can deliver complementary sensor data. Depending on the carrier and the mission, different environmental conditions and physical properties limit the ability to sample information from the environment. Here, Laser Gated Viewing has different abilities which can be applied to improve sensing capabilities and either enhance the performance of the unmanned vehicle or reduce the operation time. In the following section, we present experimental results which demonstrate the contribution of Laser Gated Viewing for some exemplary operational scenarios.

4.1 Submarine – enhancement of vision under degraded conditions

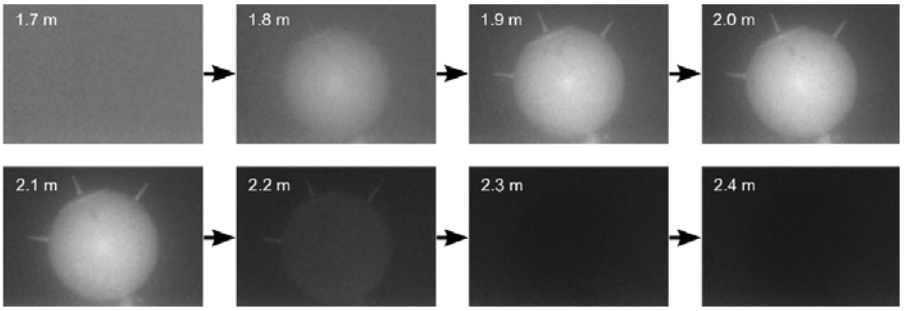


Figure 7 *ISL image data of a sea mine model (WTD71-FWG) in the Baltic Sea sampled with a sliding gate. [2,3,15]*

On board an unmanned submarine or autonomous underwater vehicle (AUV) Laser Gated Viewing can be used as an optical sensing device which delivers senor data complimentary to, e.g., sonar. For instance, active optical sensing has the ability to distinguish objects from background and to automatically identify them, e.g., by comparison to an image data base. In Fig. 7, a series of submarine image is presented recorded by Laser Gated Viewing in the Baltic Sea at an attenuation coefficient of c = 1m-1. These images show the sampling of a Sea Mine mock-up (thankfully provided by the WTD71-FWG) with a sliding range gate. The image data contain intensity as well as range information, which can be used to calculate a range model of the observed scenario. In Passive images, the optical contrast would have significantly degraded (intensity contrast ca. < 12%), while in Laser Gated Viewing a high signal from the object can be observed.

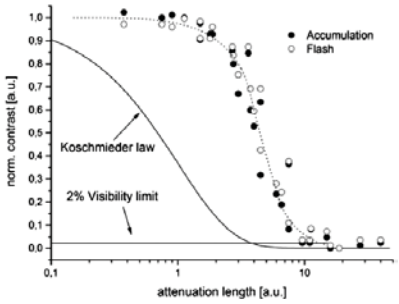


Figure 8 *Experimental evidence for the enhancement of the visual range by a factor of > 2.6 with Laser Gated Viewing.[16,17]*

The performance increase i.e. the increase of the visual range in highly diffuse environment by Laser Gated Viewing compared to passive imaging is illustrated in Fig. 8. The visual range of two Laser Gated Viewing systems with two different laser illumination methods for single laser pulse illumination (flash) and the accumulation of several laser pulses where tested in a fog tunnel. Both systems operate at a laser wavelength of 532 nm. The optical contrast of a black and white target was measured and plotted against the attenuation length i.e. the attenuation coefficient multiplied by the propagation length. From the diagram in Fig. 8, some interesting features can be derived. First, the visual range i.e. the distance (attenuation length) where the optical contract is reduced to 2% is extended by a factor of >2.6 compared to passive imaging (Koschmieder law). Further, at low attenuation length, the attenuation has nearly no impact on the optical contrast of the Laser Gated Viewing system.

4.2 Land – enhancement of illumination condition for all weather computational imaging

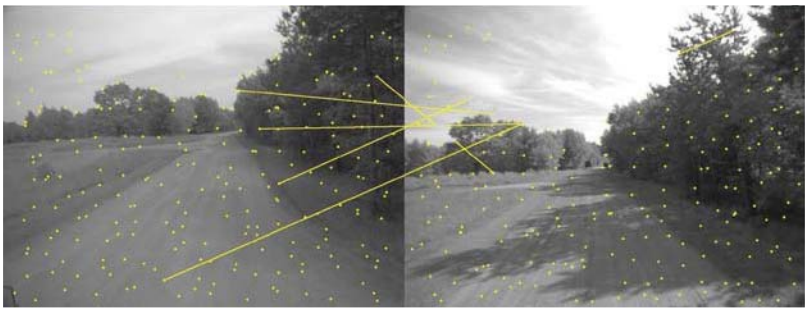


Figure 9 *Illustration of the shadow problem in passive imaging causing a high amount of false alerts in change detection. Registration errors are highlighted as yellow lines.*

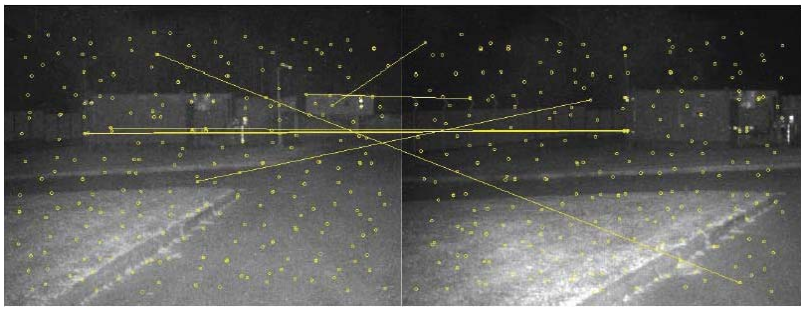


Figure 10 *Registration of Laser Gated Viewing images for active change detection and highlighting of registration errors by yellow lines.*

For land applications of unmanned ground vehicles (UGV), the analysis of images of an observed scenario is an important task for autonomous operations in complex environments. Illumination conditions can have a serious impact on the performance of image processing algorithms. For instance, at ISL, the application of image based change detection for IED (improvised explosive devices) detection is studied with great success since several years, leading to a first real time field demonstration during the EUROSATORY in 2010. This work was awarded with the prominent “Prix General Chanson” in 2011. [18]

The ISL method is based on a comparison of an actual image with an image from a data base. Both images were recorded a distinct times and slightly different viewpoints. To compare changes which occurred in the mean time, the images have to be registered i.e. an overlay has to be calculated by a transformation of one image to the view point of the second image. As illustrated in Fig. 9, different illumination conditions can lead to the appearance of different shadows. These differences can have serious impact on automated image registration algorithms. As a result a high number of false connections (indicated as yellow lines) have to be processed and sorted out in the analysis of the images.

As depicted in Fig. 10, ISL has studied the application of Laser Gated Viewing to avoid this shading problem. [19] It was possible to image scenes with constant illumination conditions by imaging only the photons used for illumination. With this approach, the appearance of shadows in the scene was significantly reduced.

4.3 Airborne

Due to its capacity to integrate active imaging systems in very small volumes, ISL has worked on different aerial platforms: artillery projectiles, missiles and unmanned aerial vehicles (UAV). For example, active imaging associated with image processing could

be a low-cost alternative to cooled infra-red imaging in missile heads. For short to medium-range missile systems, a range-gated active imaging system could replace the expensive line-of-sight stabilized infrared sensor. In this case, the only difficulty is to acquire an image within a global integration time which is compatible with the velocity of the missile to avoid motion-blurring effects.

The solution to avoid the motion blurring is to work with repetitive burst of light pulses for the illumination. The laser diode is driven at high repetition rate (80 kHz) and delivers the global energy necessary to make a luminous image within 1ms. As a matter of fact, the image will result in the integration of 80 laser illumination pulses, each of them being gated with the high speed image intensifier.

Fig 11 (left) shows an active imaging system at 808 nm ready to be integrated in a short-range missile. The field-of-view of the system is of about 17° and the resolution is calculated to permit the recognition of a tank at 2500m according to the Johnson criteria. In Fig. 11 (right), an example of image taken by the system is shown. Due to a favorable energetic balance (high-power laser diode and big diameter of collection for the imaging lens) the limit of range of the system is as big as 6500m.

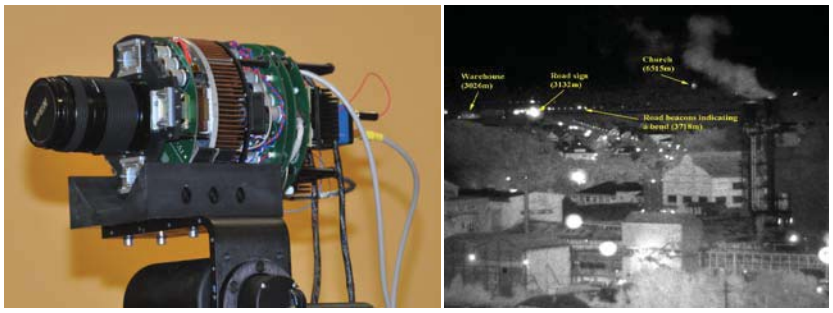


Figure 11 *Left: Laser Gated Viewing system for missile imaging at 808 nm laser wavelength. Right: Example for long range imaging under conditions of fast moving flying vector.*

ISL is also working on night vision and on change-detection for UAVs. Independently of the vision system (night: active imaging or day: passive imaging), the aim of change detection is to detect changes along frequently used itineraries. The ISL system is working in real-time and displays to an operator the changes between the present view of the camera and a corresponding view extracted from a dataset which can be considered as a "safe" itinerary. This system has been successfully tested in an UAV. An example is shown in Fig. 12. The first image is the image from the data base, the second is the one seen by the drone and the third image is the image after processing and image registration. One can see that is possible to point out small changes on the road-side, like a small can. Another typical threat can be a buried mine linked by a buried wire. Here again, the system is able to highlight where the road surface have been changed by digging activities.

Figure 12 *Example for change detection from UAV.*

5 CONCLUSIONS

Laser Gated Viewing is studied since the 1960s as an active night-vision method. Due to enormous improvements in the development of compact and highly efficient laser sources and in the development of modern sensor technologies, the maturity of demonstrator systems rose during the past decades. Further, it was demonstrated that Laser Gated Viewing has versatile sensing capabilities with application for long range observation under all-weather condition, vision through obstacles and fog, active polarimetry and 3D imaging. Thus, Laser Gated Viewing is a promising sensor technology, which is complementary to recent night vision technologies like thermal imaging and intensified low light level image sensors. Laser Gated Viewing can bring additional sensing capabilities to unmanned vehicles.

REFERENCES

[1] L. F. Gillespie, JOSA 56, 883–887 (1966)

[2] M. Laurenzis, F. Christnacher, E. Bacher, N. Metzger, S. Schertzer and T. Scholz, Proc. of SPIE 8186, 818603 (2011)

[3] M. Laurenzis, F. Christnacher, D. Monnin and T. Scholz, Opt. Eng. 51, 061303 (2012)

[4] E. Belin, F. Christnacher, F. Taillade, M. Laurenzis, Proc. of SPIE 7088, 70880O (2008)

[5] F. Christnacher, J.-M. Poyet, M. Laurenzis, J.-P. Moeglin, F. Taillade, Proc. of SPIE 7675, 76750J (2010)

[6] O. Steinvall, H. Olsson, G. Bolander, C. Carlsson, and D. Letalick, Proc. of SPIE 3707, 432–448 (1999)

[7] R. G. Driggers, R. H. Vollmerhausen, N. Devitt, C. Halford and K. J. Barnard, Opt. Eng. 42, 738-746 (2003)

[8] S. Breugnot and P. Clemenceau, Opt. Eng. 39, 2681-2688 (2000)

[9] M. Laurenzis, Y. Lutz, F. Christnacher, A. Matwyschuk and J. M. Poyet, Opt. Eng. 51, 061302 (2012)

[10] D. Monnin, A. L. Schneider, F. Christnacher and Y. Lutz, Proc. of 3DPVT06, IEEE (2006)

[11] M. Laurenzis, F. Christnacher, and D. Monnin, Opt. Let. 32, 3146-3148 (2007)

[12] X. Zhang and H. Yan, Appl. Opt. 50, 1682-1686 (2011)

[13] M. Laurenzis and E. Bacher, Appl. Opt. 50, 3824-3828 (2011)

[14] M Laurenzis, F Christnacher, Adv. Opt. Tech. 2 (5-6), 397-405 (2013)

[15] M Laurenzis, F Christnacher, T Scholz, N Metzger, S Schertzer, E Bacher, Proc. of SPIE 9250, 92500D, (2014)

[16] F Christnacher, M Laurenzis, S Schertzer, Opt. Eng. 53 (4), 043106 (2014)

[17] F Christnacher, M Laurenzis, S Schertzer, Proc. of SPIE 8896, 889606 (2013)

[18] Informationsdienst Wissenschaft, 07.06.2011,“ISL erhält "Prix General Chanson 2011" für ARCADIS: ein System zur Sicherung militärischer Konvois,“ https://idw-online.de/de/news425496

[19] AL Schneider, D Monnin, M Laurenzis, F Christnacher, Proc. of SPIE 8897, 88970L (2013)

A fast Hyperspectral Laser Induced Fluorescence application for standoff detection and online classification of biological hazardous materials

Frank Duschek[1], Thomas Fischbach[1], Anita Hausmann[1], Carsten Pargmann[1], Jim Thieser[1], Sandra Julich[2], Valeri Aleksejev[3], Larisa Poryvkina[3], Innokenti Sobolev[3], Herbert Tomaso[2], Sergey Babichenko[3], Jürgen Handke[1]

[1]Institute of Technical Physics, German Aerospace Center, Langer Grund, 74239 Hardthausen, Germany, [2]Friedrich-Loeffler-Institut, Institute of Bacterial Infections and Zoonoses, Naumburger Strasse 96a, 07743 Jena, Germany, [3]LDI Innovation OÜ, 12 Lohu, 12618 Tallinn, Estonia

E-mail: Frank.Duschek@dlr.de

Abstract

Due to a high and still increasing number of attacks by hazardous bioorganic materials there is an urgent need for their detection. Bioorganic substances need to be discriminated from other substances in various natural surroundings. In addition, living material may reproduce itself. Already one single bacterium may constitute a huge risk. Thus, a very high detection sensitivity and selectivity are essential, as well as a rapid identification with low false alarm rates. Laser based standoff detection can immediately provide information on propagation and compound type of a released hazardous material, while point sensors can collect and identify them. The coupling of both methods may be a promising solution to optimize the acquisition and detection of hazardous substances.

At DLR Lampoldshausen, bioorganic substances are measured applying hyperspectral laser induced fluorescence (LIF) technique in order to subsequently classify them. In this work, a procedure is presented, which utilizes time-dependent spectral data and predicts the presence of hazardous substances by statistical data analysis. For that purpose, measurements are carried out on a free transmission range at a standoff distance of 22 m, with two excitation wavelengths in alternating mode (i.e. 280 nm and 355 nm). A gated iCCD spectrometer system records spectral and time-dependent fluorescence data, which are processed and classified online within several seconds. Attention is drawn to physical states, concentrations, and to the photodecomposition of the samples assisted by absorption spectroscopy before and after each LIF measurement. This has a strong impact on the measurement procedure and, especially, on the training of the classifier. A further development is the capability to control the instrument remotely via a computer network connection. Thus, the risk for the operator can be minimized during the detection of hazardous materials.

Results and reliability tests of first online classification of biological materials with an improved and automated hyperspectral laser induced fluorescence application will be shown and discussed. Further studies focus on extension of a database including biological hazardous materials.

1 INTRODUCTION

Increasing numbers of attacks in public like e.g. the disposal of the neurotoxin sarin in the Tokyo subway (1995) or the transmission of anthrax to American government officials in 2012 show the need for an effective solution for the detection of chemical and biological (CB) hazards. Also unintended releases of such material, caused by earthquakes, industrial accidents, or most recently by erroneous shipment of anthrax contaminated material (2015) may lead to a high risk. A quick identification of the released material and the tracking of a potential aerosol cloud are essential for the counteractions. The potential self-replication of bacteria requires highest detection sensitivity, especially in case of aerosol particles.

Laser based techniques are well suited for standoff detection of hazardous material from secure areas with a target distance up to the kilometer range. Among these techniques (e.g. Raman [1], LIBS [2]), laser induced fluorescence (LIF) is able to map and classify aerosol clouds [3]. Though LIF is a rather inappropriate method for identification of substances, it yields valuable information on cloud distribution parameters which helps choosing the correct location for taking samples and for countermeasures [4]. LIF technique is based on the fluorescence behavior of molecules after being excited by laser light. Detected fluorescence often shows a broad and weakly structured spectrum. Therefore, additional discrimination features like spectra obtained from different excitation wavelengths together with time-resolved measurements (fluorescence lifetime measurements) can be applied.

Under real outdoor, conditions several effects might interfere and have to be taken into account, such as natural surroundings like pollen, dust, and diesel. Also different weather conditions (solar radiation, fog, rain) influence the measurements by affecting the laser light propagation and interfering with the fluorescence light. Another request is eye safety which is given for laser wavelengths below 400 nm. For these requirements, a LIF system is operated on a free space optical test range which allows for measurements of CBE substances at distances from 20 m up to 135 m under different weather conditions. Two eye-safe laser wavelengths (280 nm and 355 nm) are used to excite the target molecules. Time-resolved spectra of different chemical and biological substances (in fluid and aerosol form) are captured by a gated CCD spectrometer. After data preprocessing further analysis is done by pattern recognition software which classifies the substances into discrete classes (chemical, oil, plants, biological). The following work describes the technical details of this LIF system, discusses measured spectra, and the classification process. First results of two bacterial samples give an outlook to the extension of the database for classification of biological hazards.

2 EXPERIMENTAL

The standoff LIF detection system is operated on an outdoor free transmission range at the German Aerospace Center in Lampoldshausen. The laser and detection system is controlled from an indoor cabin and the target - a sprayed aerosol or a liquid in a cuvette - is positioned outside along the free transmission range at a distance of 22 m from the detection unit.

Fig. 1 represents the schematic optical setup of the system. 7 ns laser pulses are emitted by a Nd:YAG laser (third harmonic at 355 nm, pulse width 7ns, repetition rate 10 Hz, pulse energy ~10 mJ) and each second pulse is frequency converted to 280 nm. Both laser pulses are directed onto the target placed at a distance of 22 m. The emitted fluorescence light is collected by a Newtonian telescope with an optical diameter of 400 mm and spectrally filtered to suppress the laser lines and then split into two parts. The first part of the light is detected by a photomultiplier tube (PMT) providing information on the wavelength-independent time signal of the fluorescence pulse. The second part is analyzed by a spectrometer (resolution 1 nm, spectral range 300 nm – 600 nm) and captured by a gated iCCD camera (Princeton Instruments).

The scheme of the electronics is shown in Fig. 2. The laser acts as a master trigger for the LIF system. Each trigger pulse opens the capture gate of the iCCD camera for the response fluorescence signal of the target. A second trigger pulse is generated approximately 50 ms after each laser pulse, opens the iCCD gate and allows for the measurement of the background spectrum which is used for the correction of the previous fluorescence spectrum. The time-resolved fluorescence signal, which is captured by the PMT, is integrated by a digital oscilloscope, which is connected to the LabVIEW PC. For a proper timing of all signals a microcontroller provides information about the current timestamp within the period between two laser pulses. The microcontroller also monitors the current wavelength state of the laser system and controls a shutter which is only open during the measurement to preserve the target sample from unnecessary bleaching effects due to laser irradiation.

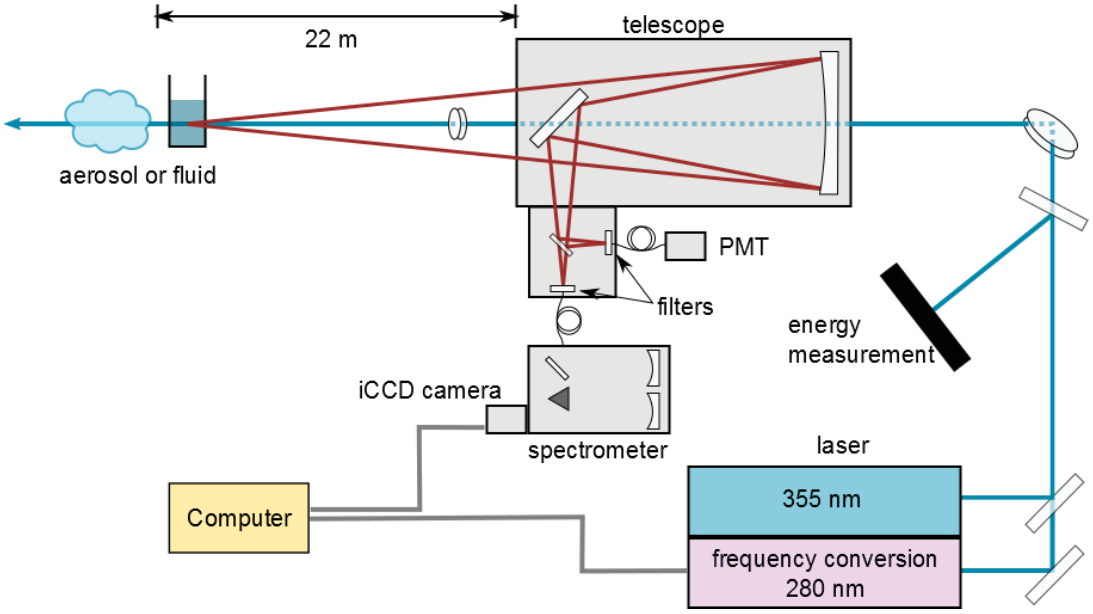


Figure 1: Schematic draft of the optical setup.

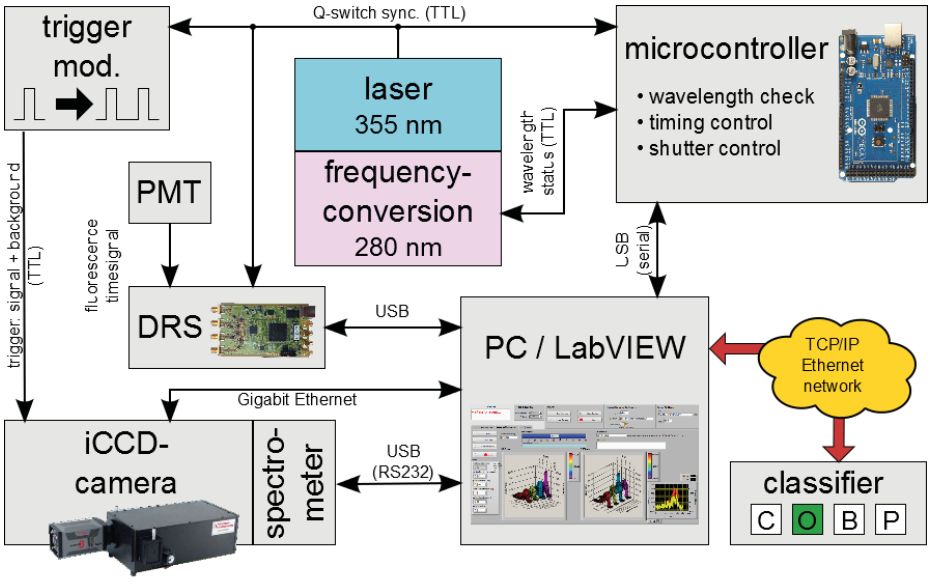


Figure 2: Schematic draft of the electronic setup.

Fig. 3 schematically shows the acquired data which is considered for the following classification process. Fluorescence spectra are captured in consecutive time shifted iCCD camera gates marked by rectangular functions. The fluorescence spectra provide additional information on the fluorescence lifetime of the sample. The first gate delay starts at an offset to the laser Q-switch, placed at the fluorescence pulse leading edge. The offset depends on the run-time of the light (target distance) and electronic signals. The following camera gate delays are shifted one by one by 2 ns to provide the fluorescence lifetime feature. Simultaneously to the acquisition of the spectrum the complete fluorescence pulse is captured and integrated. The signal strength of each spectrum can be used for a later normalization of each spectrum. For each delay a defined number of single spectra is

recorded to suppress statistical effects. Each single spectrum is linked to an individual background spectrum which is captured after the corresponding spectrum and within the second half of the period between two laser pulses. Especially in free atmosphere, background solar radiation may fluctuate within seconds. Thus, a background correction, i.e. subtraction of background from fluorescence spectra, makes measurements more independent of weather conditions.

The final measurement dataset contains N = 2 (m + 1) (n + 1) subsets, each consisting of a fluorescence spectrum, a background spectrum, the integral value of the fluorescence pulse time signal from the PMT, and meta data like the current excitation wavelength. n + 1 is the camera gate delay count, m + 1 the spectrum accumulation within each delay, and the factor 2 represents the two different excitation wavelengths. The duration of one measurement is t = N x 100 ms (e.g. t = 8 s for 4 camera gate delays and an accumulation of 10 spectra). An overhead of approximately 2 s, caused by data communication, post-data processing, and classification, has to be added to get the effective classification time. The number of resulting fluorescence spectra for one target sample is dependent on the number of gate delays (n+1) and the number of laser excitation pulses for each delay value. Each measurement consists of n + 1 camera gate delays and each delay consists of 2 (m+1) laser pulses and resulting fluorescence spectra. Because of a laser repetition rate of 10 Hz, each period between two laser pulses has a duration of 100 ms, which is split into two equally sized parts: fluorescence spectrum and background spectrum acquisition. The LabVIEW PC is connected to the classifier software via Ethernet (TCP/IP) to be able to classify the substances online and location-independent.

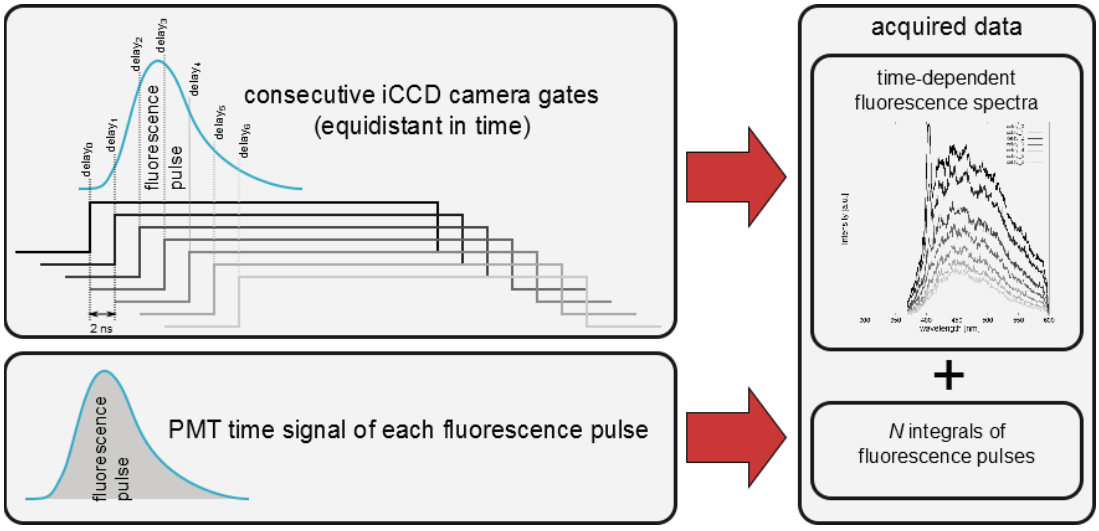


Figure 3: Data acquired during a measurement (here for one excitation wavelength). Spectra are captured with consecutive iCCD camera gates with linear increasing gate delay. A dataset consists of N subsets containing a fluorescence spectrum, a background spectrum, and a fluorescence pulse integral.

3 CREATION OF CLASSIFIER

The creation of an algorithm which is capable for ranking measured data into characteristic classes is the main objective for a classification process. The developed system provides four classes: chemicals, plants (natural surroundings), oil, and bacteria (living material). The last class represents potential hazardous bioorganic material. In our current system we are using a structural extraction combined with statistical classification for the spectral data analysis.

The classification algorithm is described briefly and a detailed explanation can be found in ref. [5]. After the measurement dataset has been imported into the software, artificial spikes

and noise is filtered out of the spectrum. The original spectrum contains 720 data points (features), many of them are redundant. Therefore, a reduction of the dimensionality to a few significant features is done by structural and statistical methods (“feature extraction”). The feature extraction process compresses the data by a factor of 60. Each remaining feature can be regarded as a representative of a spectral region within the original spectrum. In the following step important features, which contribute significantly to the discrimination process, are selected. The next goal in the classification process is to generate many weak classifiers, which can be combined to one strong classifier. A classifier is created by growing a decision tree on a set of features. Each node of a decision tree is a binary decision on the value of a feature. Leafs represent the substance classes in which the analyzed spectrum is fed in depending on the decisions which are made on its feature values. To be able to grow many decision trees (classifiers) additional sets of features are generated in the bagging process (“bootstrap aggregation”). The strong classifier is now built by voting among all decision trees. The classifier software is implemented in MATLAB with help of the Framework for Ensemble Learning from the Matlab Statistics Toolbox.

4 RESULTS

4.1 Measurements for classifier tests

For training the system and building up a spectral database substances contained in the groups fungi, bacteria, vitamins, enzymes, and aromatic amino acids are measured in liquid solution. To include interfering natural background substances different plants like dandelion or saffron are also measured. Oils like diesel or petrol complete the set of substance groups as non-dangerous anthropogenic substances. All liquid samples are solved in deionized water except for curcumin where acetone is used as solvent. Some substances are not (completely) soluble. To keep the solutions homogeneous every substance is stirred during the measurements. For the database each measurement consists of 100 spectrum accumulations to suppress statistical effects. The reproducibility of the measurements is checked three times for each sample. The following spectra are background-corrected but not corrected with the spectral response characteristics of the optical parts of the system. For the substance classification and discrimination this circumstance is irrelevant on this special apparatus.

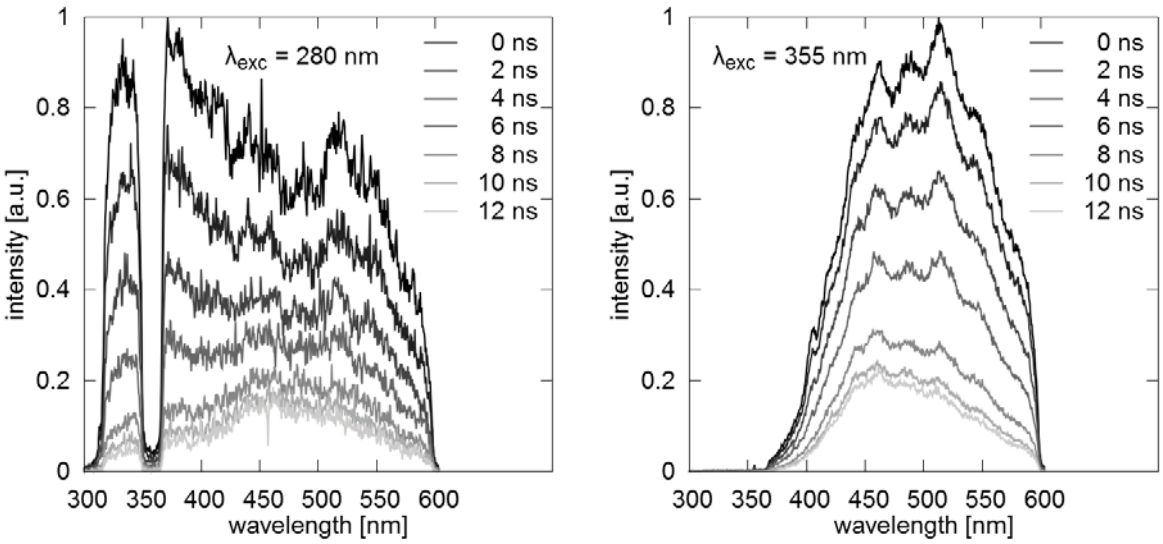


Figure 4: Fluorescence spectra of yeast (solution with a concentration of 1 mg/ml) excited at 280 nm (left) and 355 nm (right). The different spectra in one plot represent different camera gate delays measured relative to the offset. The dip between 350 nm and 370 nm is caused by a 355 nm notch filter.

As an example, Fig. 4 shows the fluorescence spectra of 1 mg/ml yeast in deionized water upon 280 nm and 355 nm excitation (Fig. 4 left and right, respectively) and camera gate delays from 0 ns to 12 ns relative to an offset. The different spectra show the improvement of the ability to discriminate different substances by using not only one excitation wavelength.

Fig. 5 shows an example of the substance discrimination by their fluorescence lifetime. Diesel and dandelion do not have big differences in their fluorescence spectrum shapes. Therefore, their corresponding time-dependent fluorescence spectra are examined by fitting signal intensities at 490 nm to an exponential decay function. Diesel (Fig. 5) has a lifetime of about 20 ns whereas dandelion (right) of about 6 ns. However, the laser pulse width is about 7 ns which is limiting for the lifetime method.

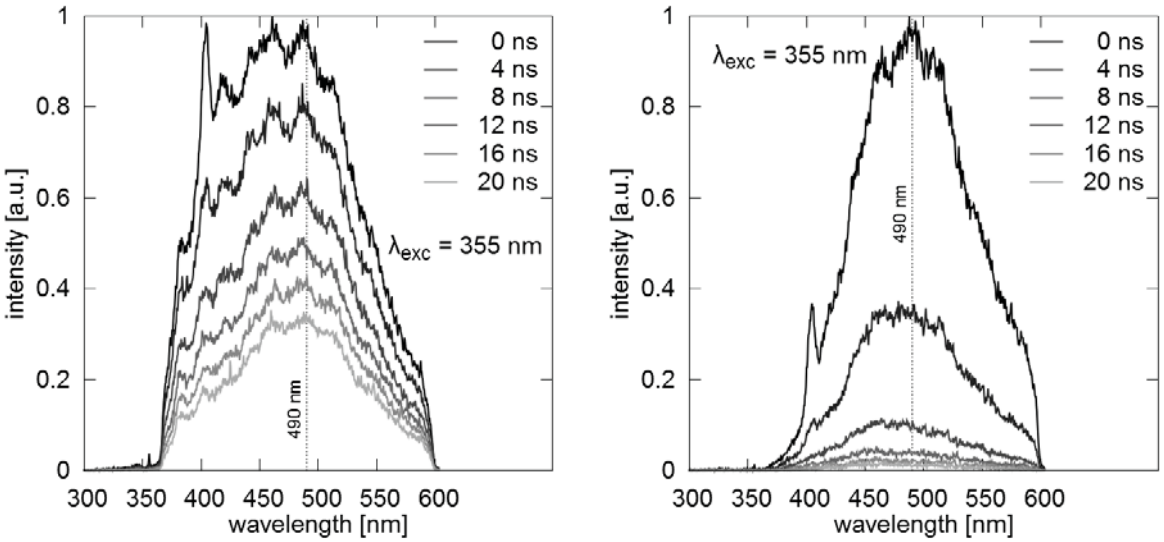


Figure 5: Fluorescence spectra of diesel (2.5 µl/ml, left) and dandelion (500 µg/ml, right) excited at 355 nm. The spectra represent different camera gate delays measured relatively to the offset. Intensities at 490 nm are used for determination of the fluorescence lifetimes.

Tab. 1 lists classification results of some test samples. Each sample was measured 10 times to get the success rate (in percentage) of a correct classification. The classification algorithm yields a classification confidence value for each measurement and class. The given confidence values are averaged for the 10 measurements and can be in the interval 0 % to 100 %. A sample is regarded as classified if the classification confidence value is larger than the defined threshold value of 40 %. 88% of the samples are classified correctly with an average confidence value of the correct classes of 71 % (highlighted values).

Table 1: Averaged confidence values for the classification of CB substances with different concentrations. Concentrations are given in µg/ml and µl/ml for solids and liquids, respectively.

Substance	Expected class	Concentration	Bacteria	Plant	Chemical	Oil
Curcumin	Plant	2.1	6%	94%	0%	0%
Curcumin	Plant	4.2	4%	96%	0%	0%
Dandelion	Plant	125.0	70%	20%	9%	1%
Dandelion	Plant	250.0	27%	70%	3%	0%
DEET	Chemical	0.5	25%	3%	67%	5%
DEET	Chemical	1.0	37%	1%	60%	3%
Diesel	Oil	2.5	29%	1%	2%	68%

Substance	Expected class	Concentration	Bacteria	Plant	Chemical	Oil
Diesel	Oil	5.0	26%	2%	2%	70%
NADH	Bacteria	3.0	73%	27%	0%	0%
NADH	Bacteria	6.0	78%	22%	0%	0%
Petrol	Oil	pure	0%	0%	10%	90%
RAID	Chemical	1.0	7%	0%	35%	57%
RAID	Chemical	2.5	4%	0%	69%	27%
Saffron	Plant	30.0	17%	82%	1%	0%
Saffron	Plant	60.0	2%	98%	0%	0%
Tryptophane	Bacteria	30.0	78%	22%	0%	0%
Tryptophane	Bacteria	60.0	75%	25%	0%	0%
Yeast	Bacteria	250.0	62%	0%	28%	10%
Yeast	Bacteria	500.0	63%	31%	4%	2%

Yet, more improvements have to be done on the classification process to increase the overall success rate. For a correct classification, confidence values have been found to be typically larger than 60 %. However, red highlighted samples are not being classified correctly at low concentrations which indicate limitations of the current system especially with low measurement times of just one second per sample.

4.2 Standoff LIF of bacteria

With the successful demonstration of the LIF system and the classification of CB substances, focus is drawn to biological hazards such as bacteria. As first examples LIF measurements of *Escherichia (E.) coli* and *Bacillus (B.) thuringiensis* are presented in Fig. 6.

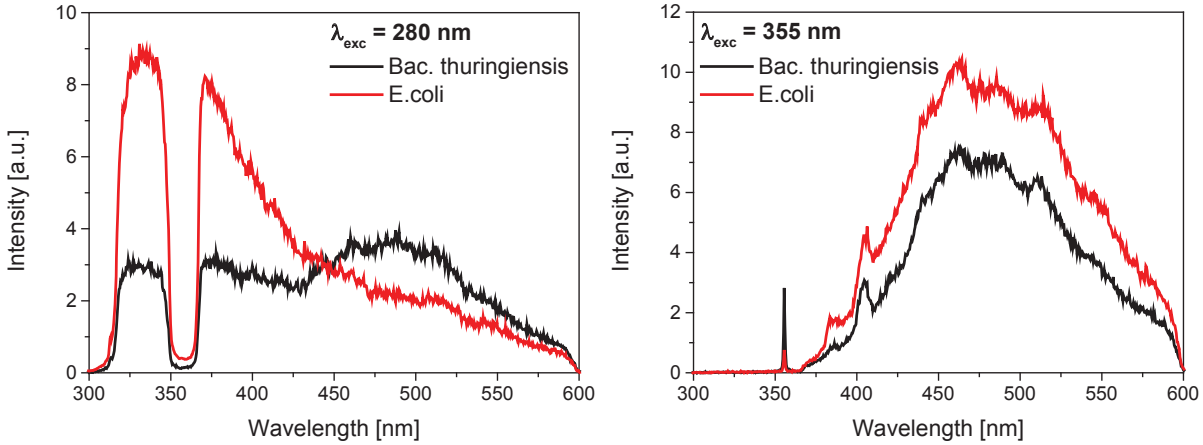


Figure 6: LIF spectra of *B. thuringiensis* (10^9 CFU in PBS) and *E. coli* (10^7 CFU in PBS) upon excitation at 280 nm (left) and 355 nm (right).

Cultivation of both bacteria species was carried out on nutrient agar with 10 % defibrinated sheep blood at 37 °C for 24 h. Colony material was suspended in 1x phosphate buffered saline (PBS) and stored at 4 °C. To determine the concentration of colony forming units (CFU) per ml serial dilutions were prepared in 1x PBS with 4 % agar and 100 µl each dripped on agar plates using identical conditions for cultivation before the colonies were counted. The concentration of *B. thuringiensis* in PBS is found to be 10^9 CFU and the one of E. coli in PBS is 10^7 CFU.

The 355 nm spectra of *E. coli* and *B. thuringiensis* (Fig. 6, right) are shaped almost identically. However, the 280 nm exited LIF spectra of both samples can easily be

distinguished by their shape. The spectral datasets are not yet fed into the classifier since it has not been trained on these samples. Though, it is very promising that the existing classifier algorithm can be trained successfully on *E. coli* and *B. thuringiensis* spectral data as well as many further bacteria.

5 CONCLUSION AND OUTLOOK

To be able to classify CB substances by using a laser based standoff technique a LIF system has been developed which is optimized to operate under realistic outdoor conditions. A set of CB substances is measured to build up a database for training the system's pattern recognition algorithm. For the excitation process the samples are repetitively illuminated by two different eye-safe wavelengths at 280 nm and 355 nm. Time resolved measurements of the fluorescence spectra increase the dimensionality of information for improved substance discrimination. Pattern recognition software classifies the material into four disjunct classes by applying binary decision trees on automatically selected important features of the measurement data. First realistic evaluations show promising results and demonstrate the qualification of the LIF technique for the classification of hazardous CB substances. LIF can provide useful information for subsequent identification techniques and counteractions. The presented LIF spectra of *E. coli* and *B. thuringiensis* look quite promising. Once the classifier has been trained on these and more bacteria, the standoff LIF system and classifier are capable of classifying biological hazards within seconds.

REFERENCES

[1] S. Wallin, A. Pettersson, H. Östmark, and A. Hobro, "Laser-based standoff detection of explosives: a critical review," *Analytical and Bioanalytical Chemistry*, vol. 395, no. 2, pp. 259–274, 2009.

[2] F. Duschek, C. Pargmann, K. Grünewald, and J. Handke, "Stand-off detection at the DLR laser test range applying laser-induced breakdown spectroscopy," in *Proc. SPIE*, 2010, vol. 7838, p. 78380I–78380I–6.

[3] V. Sivaprakasam, H.-B. Lin, A. L. Huston, and J. D. Eversole, "Spectral characterization of biological aerosol particles using two-wavelength excited laser-induced fluorescence and elastic scattering measurements," *Opt. Express*, vol. 19, no. 7, pp. 6191–6208, 2011.

[4] O. Meyer, C. Jacquelard, J. Melkonian, P. Chardard, P. Lanson, and D. Petitgas, "Stand-off biological detection by LIF (laser induced fluorescence) LIDAR," in *Optronics in Defence and Security, 4th International Symposium*, 2010.

[5] T. Fischbach, F. Duschek, A. Hausmann, C. Pargmann, V. Aleksejev, L. Poryvkina, I. Sobolev, S. Babichenko, and J. Handke, "Standoff detection and classification procedure for bioorganic compounds by hyperspectral laser-induced fluorescence," in *Proc. SPIE*, 2015, vol. 9455, p. 945508.

WAKE-UP MODE CAMERA SYSTEM TO DETECT UNAUTHORIZED PERSONS AND VEHICLES

Pasi Pyykönen[1], Tero Peippola[2], Jari Jankkari[3], Kristiina Valtanen[4] and Henrik Huovila[5]

[1] pasi.pyykonen@vtt.fi, [2] tero.peippola@vtt.fi, [3]jari.jankkari@vtt.fi, [4]kristiina.valtanen@vtt.fi, [5] henrik.huovila@vtt.fi
VTT Technical Research Centre of Finland, Tekniikankatu 1
Tampere (Finland)

Abstract

This paper introduces wake-up mode camera (WUC) system to detect persons and vehicles. The idea of the camera system is to detect unauthorized objects from camera scenery and send information to background control system. In this paper, our implementation is focused to introduce small, low cost and low power consumption wake-up camera unit to detect unauthorized object especially beyond the perimeter of some Critical Infrastructure (CI).

Keywords: WUC, wake-up camera, detection, camera, human detection, vehicle detection, low power.

1 INTRODUCTION

Traditional detection systems are usually based on one master camera which detects and processes information and gives alarm if unauthorized object are detected. These systems can be power consuming due to heavy image processing algorithms and must therefore be installed near stationary power sources. When monitoring large and wide areas i.e. oil and gas pipe lines, power plants, border lines etc. these systems need own infrastructure with cabling and can therefore be too expensive in large scale. However the benefit of these systems is that with one unit it is possible to perform the whole decision chain from detection, object recognition to alarm.

Target of the implementation is to provide detection system to wide are facilities i.e. gas, oil pipe lines and large factories where monitoring is needed on wide area and stationary power source is not available. Wake-up camera system consists of one to several wake-up camera units that are working stationary and independently around monitored area. WUC units are connected wirelessly to background system with Rule Based Engine (RUBE) that makes decision based on observations from WUC unit. RUBE estimates detection results from WUC and transforms them to security action. Security action can be alarm or backup detection with more powerful camera system.

2 WUC PLATFORM

WUC unit consists of low power hardware for imaging, data analysis and communication. Used components are mass-produced off-the-shelf products which are lowering total cost. Unlike commercial image processing solutions, this implementation only uses just the mandatory components for this application to achieve small form factor. ARM Cortex-M4F microcontroller is running RTOS and image processing algorithm. As the developer has full control over all the hardware and RTOS, available power saving modes can be efficiently be used. Image sensor [1] has also a simple DSP, offloading image compression computation.

3 COMMUNICATION BETWEEN WUC CAMERA UNITS

In a low power environment, communication with background systems is limited with data bandwidth and update frequency. Therefore a new approach for camera communication was implemented for WUC units.

The communication between WUC units is realised exploiting low cost, low power, light weight, long lifetime, but at the same time low resourced CPU and mesh Short Range Radio (SRR) network (WirelessHART). Here low resource means low computing power, low memory and low energy consumption. The challenge of this kind of video camera communication system is to balance the requirements for the communication and on the other hand the low resources of the system. This is achieved by using low level of realisation in all parts of the WUC unit, also in communication software and algorithms. It means that new ways must be found for all functions, both in camera image processing and communication instead of the former solutions. In other words, the software and hardware must be adapted to the low resource environment.

In Fig. 1 is presented the schema of WUC SRR Camera Sensor units and manager is presented. As an example here the CI comprises a gas pump station and its perimeter including a gas supply pipe.

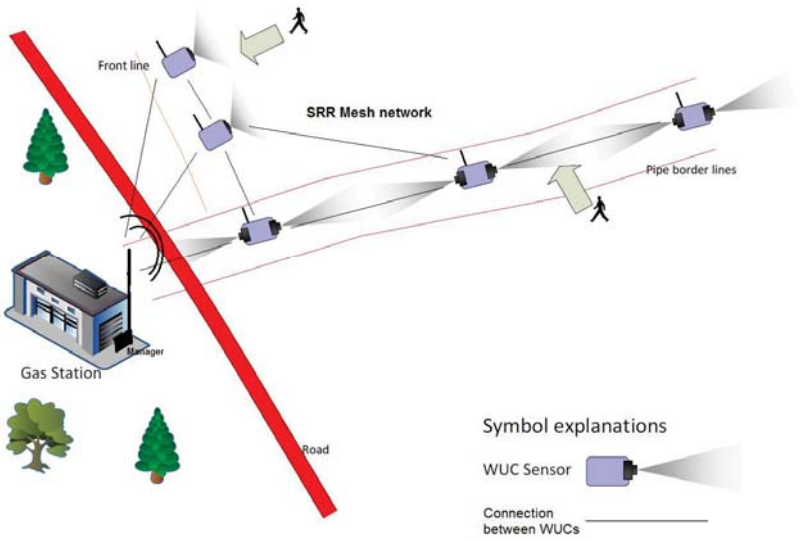


Figure 1 The schema of WUC SRR Camera Sensor units and manager.

WirelessHART radio motes included in WUC units form a mesh network between each other and finally between manager unit. The mesh topology network ensures many routes to the data collecting manager unit. If the radio mote is out of the range of the manager it transfers the data through the nearest motes and finally to the manager. So the covering of the radio network can be enlarged. In this way also linked data transferring chains can be formed, which is impossible e.g. in star topology networks with one base station.

3.1 Communication from the WUC system to other ARGOS components

The WUC platform described in the previous chapters has been used as a part of ARGOS project which is a multimodal early warning security solution for Critical Infrastructures. The communication from the WUC camera units to the rest of the ARGOS system is described in the Figure 1.

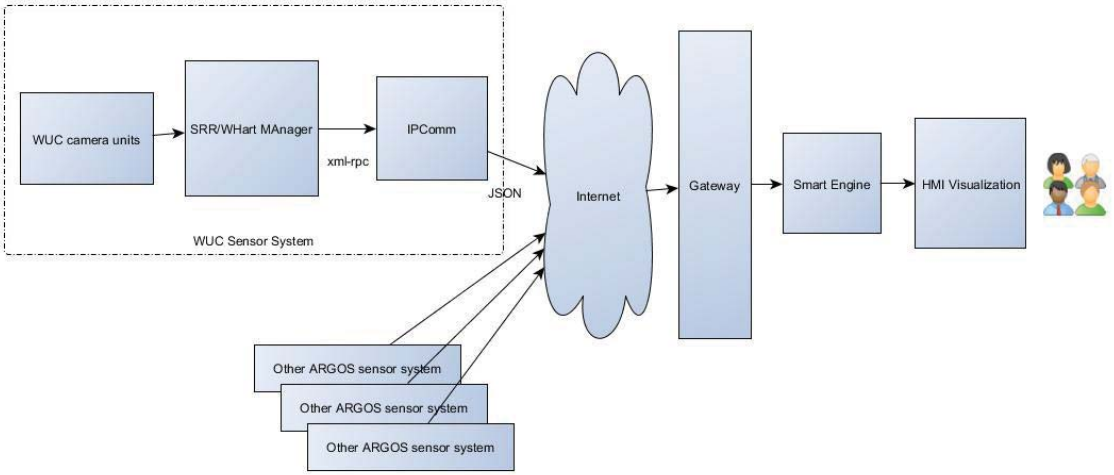


Figure 2 The ARGOS architecture overview.

As shown, in addition to the WUC camera units the WUC system, as well as the ARGOS system, also consists of various other processing units each having its own task in the ARGOS system communication. In the previous chapter the Short Range Radio network was presented. The SRR network is managed by a WHART Manager unit and it handles the initialization of the network, joining of the WUC units, supervising and the resource sharing of the network and connecting the network forward to IPComm and the gateway.

The IPComm unit acts as a link between WHART Manager and the Gateway which in turn collects data from multiple different ARGOS sensors. The Gateway both stores images and short video/audio data segments to a database and forwards some messages to the Smart Engine subsystem. The Smart Engine makes decisions about the type of a threat and generates alerts if needed. The alerts are visualized in the HMI warning visualization system.

The data moving between the ARGOS elements (not inside the WUC system) is mainly transmitted as “events” which are HTTP packages containing different kinds of JSON data. Also, some raw data is sent between the units. The format of the JSON events is strictly defined and in the case of the WUC system only a few event types are allowed: the most important ones are the incoming Wakein events (to wake up the cameras) and the outgoing Wakeout/WakeoutImage events (describing a threat).

WUC camera will wake up to operate from low power sleeping mode when it receives Wakein event from the DataFusion component. DataFusion component receives detection data from other ARGOS sensor system i.e. vibration sensors. If vibration sensor detects vibration near WUC unit, it delivers detection data to DataFusion component. DataFusion component decides, which WUC unit can detect possible target and if more detection actions with WUC camera unit is needed. If more actions is needed, DataFusion component generates Wakein event to wake up WUCC camera system. Detection results from WUC camera unit are delivered back to DataFusion component to increase detection reliability.

In the next two chapters the operation of the WHART Manager and the IPComm, both belonging to the WUC system, is described in more detail.

3.1.1 WHART Manager

WHART Manager includes two parts, the actual radio manager connected to SRR and the controlling software part running e.g. in a laptop. The role of 1st one was already explained in former chapters but here still the main tasks: network initialisation, control of WUC mote joining, overall SRR supervising & resource sharing and connection point

to IPComm and GW. The latter one links the radio part to IPComm and gateway and supervises the whole WUC system. E.g. if one of the WUC unit is triggered by a Wakein event to take an camera image and analyse it , WHART Manager takes care to put the system to a busy state. If external Wakein events or other internal triggering events are coming at the same time during the camera process, WHART Manager informs with the busy state meaning that the external or internal requirements must cancel or wait until this WUC unit is available.

3.1.2 IPComm

The IPComm unit is working as an intermediary between the WHART Manager and the outer ARGOS Gateway. Its main task is mediating event messages but also, in some level, it has to be aware of the state of WUC camera units.

IPComm is implemented using Visual Studio 2013 and the .NET framework. To the direction of the WHART Manager IPComm is communicating using XML-RPC protocol. Because IPComm has to be able to both send and receive XML-RPC requests it is working as a server as well as a client.

All the data exchange between the IPComm and the ARGOS Gateway is implemented as REST based HTTP POST messages. The POST messages include ARGOS events in JSON (JavaScript Object Notation) format. Again this data traffic is bidirectional: IPComm receives Wakein events from the Gateway but has to manage the sending of self-triggered threat events to the Gateway too. In our system the JSON generation was implemented using Json.NET framework. Because of the text based nature of JSON the pictures to be sent are converted to the base64 format.

Despite the stateless essence of the REST communication the IPComm has state awareness in some degree. For example the IPComm unit stores the status of WUC camera units in order to be able to respond to the ARGOS Ping (JSON) requests. Furthermore, the IPComm must know the relative order of threat messages and their separate picture messages.

Especially due to the uncertainties in the operation of wireless network (e.g. a connection may be lost if a truck drives between nodes) we have had to pay extra attention to the operation in failure conditions as well as to the recovery from those situations. Moreover, a wireless image transfer is quite slow and the IPComm unit has to block the incoming requests from the Gateway during the image processing and transfer.

The IPComm unit also serves as the part of the system security. The firewall of the IPComm is configured to accept incoming traffic only to one of its ports and further only to the IPComm program. In addition, the IPComm strictly inspects incoming events i.e. only the events having perfect form are accepted and intermediated.

3.2 Low power hardware

WUC unit consists of low power hardware for imaging, data analysis and communication. Used components are mass-produced off-the-shelf products which are lowering total cost. Unlike commercial image processing solutions, this implementation only uses just the mandatory components for this application to achieve small form factor.

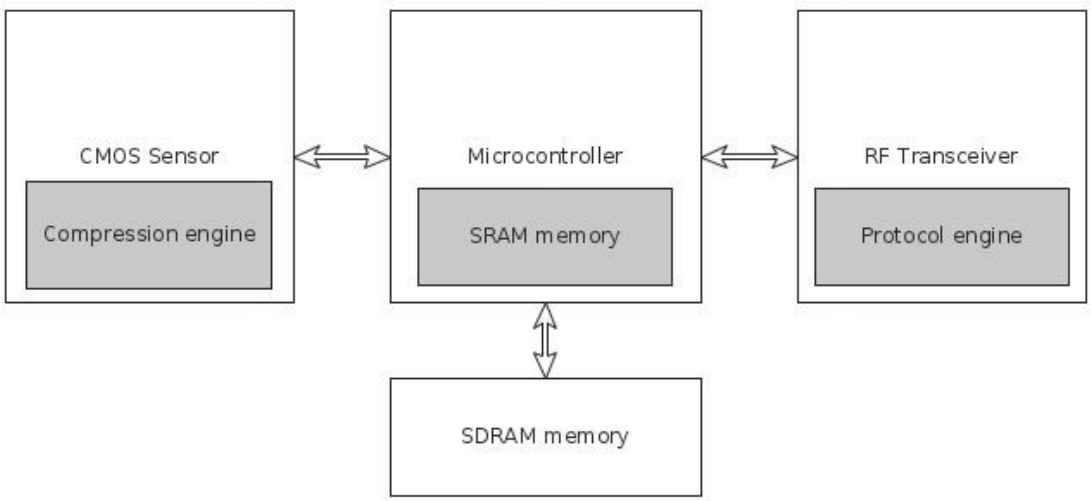


Figure 3 Embedded system hardware architecture.

ARM Cortex-M4F microcontroller is running RTOS and image processing algorithm. As the developer has a full control over all the hardware and RTOS, available power saving modes can be efficiently used. Image sensor [1] has also a simple DSP, offloading image compression computation. External SDRAM is used only for algorithm data storage and can be set to low power mode when not required.

3.3 Unauthorized persons and vehicles detection

We have implemented new image processing algorithms using an open-source image processing library, Leptonica [3] This multi-platform library was ported for a lightweight RTOS, ChibiOS/RT[4]. This enables algorithm development done in any Windows- or Linux-based machine and then transferred into our embedded system. Leptonica library provides basic image processing functions. Starting point of the algorithm is to acquire low-resolution 240x320 pixel RGB image from the camera. Acquired image is filtered from the noise and delivered to intelligent background subtraction module. Algorithm of background subtraction is based on basic principles of background subtraction within image sequence [2]. For our implementation we boosted it by filtering, HSV colour transformation and by using several sequential frames for comparison. Module estimates background movement in long time period to detect large scale movement from the background.

As a result, algorithm provides object list containing regions of interest (ROI) with object dimension and size. Based on these dimensions, object is classified to human object and non-human object i.e. vehicles or large animals. Classification module estimates also the possible threat and reliability of detection. If predetermined conditions for triggering a Threat Event are filled, WUC system triggers and sends this Threat Event to RUBE unit which decides if an alarm to the operator has to be taken. In Figures 2 and 3 is shown examples of successful human and vehicle detection. In Fig.2 is shown example of vehicle detection. Left image shows empty view from the WUC unit without moving objects. In the centre image, a van is approaching behind the trees and a smaller vehicle is following it. In the image at right, the algorithm has marked to moving objects.

Figure 4 Example of vehicle detection with WUC system. In left image scene is free of moving objects. In center image, van came visible behind the trees and other smaller vehicle is following. In right image algorithm has marked to moving objects.

In Fig. 3 is shown example of human detection in parking field. In left image is original empty field without objects. In the centre image, two persons are walking away from the WUC unit. In the image at right, the algorithm has detected and marked the moving objects and classified them as humans.

Figure 5 Example of human detection with WUC system. In left is original empty field without objects. In center image, two persons are walking away from WUC unit. In right image algorithm has detected marked to moving objects and classified as humans.

As a result detection algorithm produces classification result of detected objects. There are three classes: human, human and vehicle. Main focus is however in detecting changes in WUC camera view and in notifying background system with location of possible danger. For this purpose, WUC delivers also image coordinates of the area where objects are detected.

4 RESULTS

We have performed preliminary outdoor tests with WUC unit to estimate reliability of the unit and object detection algorithm. Tests were done in two kinds of environments, on an open field (see Fig. 4) with human and car targets. In human tests, the goal was to test how reliable this system is for detecting human objects from different ranges. With car objects, idea was the same. Based on test results we determined the distance that will significantly decrease the detection ratio.

In table 1 is an example of a test set with a human target. In this dataset two human targets were walking around an empty parking area. Nearest target was 3 meters from the WUC and farthest target 50 meters from the WUC. As shown, detection rate is 98.4% when object is distance range 3 to 30 meters from camera. After 30 meters detection rate will decrease significantly. Main idea of the algorithm is to detect movement between sequential image frames. In addition to human and vehicle objects there are also other areas in image that can be detected as moving objects. For example the wind swaying trees can be detected as a moving car. To decrease false alarms we implemented filtering for the detection results. This will filter out too small objects from image that can be classified as a background movement. For this reason

when objects are moving further than 30 meters from camera, filtering can remove these areas from image. If filtering is removed, human objects can be detected from longer distances but also false alarm ration will increase significantly.

Table 1 Detection rate and false positive rate for human objects when target is distance below 30 meters and over 30 meters.

Dataset: human		
	Distance < 30 meters	Distance > 30 meters
Detection rate	0.9830	0.0074
False positive rate	0.3012	0.0000

In table 2 is example of test set with vehicle target. In this dataset one vehicle was driving in empty parking area and closing the WUC unit. Nearest target was 5 meters from WUC and farthest target 50 meters from WUC.

As shown, detection rate is decreasing significantly distances over 30 meters. In close distance detection rate was 100 % which is expected result for large object. Large objects will tolerate filtering in image processing and therefore not filtered out as a background.

Table 2 Detection rate and false positive rate for vehicle objects when target is distance below 30 meters and over 30 meters.

Dataset: vehicle		
	Distance < 30 meters	Distance > 30 meters
Detection rate	1.0000	0.0769
False positive rate	0.1000	0.3300

In these test we were using RGB 320x240 camera sensor which is compromise between resolution, and with power and memory consumption. This also affected these test results. As shown in Figure 4, camera resolution and compression algorithms are causing blurring for the background and therefore dispose small objects from longer distances. This will help to decrease amount of movement that can be seen with higher resolution and then decrease amount of false alarms.

5 FUTURE WORK

As the image processing library is using POSIX-like resources, not all microcontroller resources are fully utilized at the moment. Memory-copy functions can be implemented using a Direct Memory Controller (DMA) controller or special 2D-DMA which handles among other things bitmap operations more efficiently.

Microcontroller also has a powerful Floating Point Unit (FPU) but algorithm uses mostly fixed point operations. Some parts of analysis could be processed using FPU, offloading main processing unit and reducing latency.

Low power modes will be implemented to the WUC unit to decrease the power consumption.

With cameras and camera algorithm, future work will focus on testing algorithm performance in different environments. Next step in project is to test WUC unit during field tests in Romania and Greek as unauthorized persons and vehicles detection unit. Based on these tests we will evaluate detection system and needs for improvements.

REFERENCES

[1] OV2640 CMOS camera datasheet, http://www.uctronics.com/download/cam_module/OV2640DS.pdf

[2] H. Parks, S. Fels “Evaluation of Background Subtraction Algorithms with Post-Processing” 19 Conference: Fifth IEEE International Conference on Advanced Video and Signal Based Surveillance, AVSS 2008, Santa Fe, New Mexico, USA, 1-3 September 2008

[3] Leptonica open-source image processing library, http://www.leptonica.com/

[4] Chibi/OS, www.chibios.org

RESULTS FROM 3D-FORENSICS - MOBILE HIGH-RESOLUTION 3D-SCANNER AND 3D DATA ANALYSIS FOR FORENSIC EVIDENCE

Stephen Crabbe[1], Peter Kühmstedt[2], Roland Ramm[3], Andre Hendrix[4], Peter Smolders[5], Willem van Spanje[6], Boreas Hesselink[7], Giorgio Maria Vassena[8], Matteo Sgrenzaroli[9], Max Lucas[10] and Marc Oberholzer[11]

[1] *stephen.crabbe@crabbe-consulting.com*
Crabbe Consulting Ltd, Allerheiligenstr. 17, 99084 Erfurt (Germany)

[2] *peter.kuehmstedt@iof.fraunhofer.de,* [3] *roland.ramm@iof.fraunhofer.de*
Fraunhofer IOF, Albert-Einstein-Straße 7, 07745 Jena (Germany)

[4] *andre.hendrix@zeeland.politie.nl,* [5] *peter.smolders@zeeland.politie.nl*
Politie Zeeland-West-Brabant, Bezoekadres Ringbaan West 232, 5038 KE Tilburg (Netherlands)

[6] *wvspanje@delfttech.com,* [7] *bhesselink@delfttech.com*
DelftTech BV, Motorenweg 12, NL-2623CR Delft (Netherlands)

[8] *giorgio.vassena@gexcel.it,* [9] *matteo.sgrenzaroli@gexcel.it*
GEXCEL Srl, via Branze 45, I-25123 Brescia (Italy)

[10] *max.lucas@lucas-jena.de*
LUCAS Instruments GmbH, Hermann Lons Straße 2, 07745 Jena (Germany)

[11] *marc.oberholzer@enclustra.com*
Enclustra GmbH, Technoparkstr. 1, CH-8005 Zurich (Switzerland)

Abstract

This paper presents the latest results of the 3D-Forensics project to develop a mobile high-resolution 3D scanning system for the recovery and analysis of footwear and tyre impression trace evidence left at crime scenes towards the end of the project's completion. The prototype 3D-scanner and analysis software are presented together with the test and evaluation methodology and the results of laboratory and field testing to date.

Keywords: forensics; crime scene; footwear impressions; tyre impressions; 3D; scanning; fringe projection; digital data.

1 INTRODUCTION

The 3D-Forensics project is developing a mobile high-resolution 3D scanning system for forensic evidence recovery at crime scenes, specifically for footwear and tyre impressions. The traditional techniques to capture these traces are typically photography or plaster casting but both techniques have disadvantages e.g. photographs contain no depth information and plaster casting is very time-consuming. Our technological approach is designed to overcome such disadvantages. Footwear and tyre impressions as well as profiles are recorded and analysed in 3D and colour enabled through optical scanning technology. 3D data analysis and processing software tools have been developed for both the investigation of crime scenes and prosecution of criminal suspects. This paper will present the prototype scanner and

analysis software realised and the results of the prototypes' test and evaluation and end user feedback to date.

2 PROTOTYPE 3D-SCANNER

The first part of the developed system is a 3D-scanner that is used directly at crime scenes. It captures footwear and tyre impressions quickly. The scanning technique is based on "fringe projection" combined with high resolution colour images. A sequence of fringe patterns is projected onto the scene while two cameras capture them from slightly different positions. This technical approach enables the calculation of a highly resolved 3D point cloud of the scene [1]. Colour images are taken by an attachable high resolution camera simultaneously with the 3D measurement. They can be later mapped onto the 3D point cloud to distinguish between characteristics in the impression trace and distortions such as small stones or leaves. Fig. 1 shows the complete prototype scanner with attachable high resolution camera.

Fig. 1 Complete prototype 3D-scanner

Fig. 2 3D-Scanner prototype in travelling case

The prototype comes equipped with an outdoor travelling case including reserve batteries, recharging devices and calibration pieces (Fig. 2). The 3D-scanner is used handheld or mounted on a tripod. Fig. 3 shows the handheld usage of the scanner. For bright outdoor conditions the scanner can be combined with a quickly assembled shadow box to avoid interference (Fig. 4).

Fig. 3 Handheld scanning with the 3D-scanner

Fig. 4 Scanning with the 3D-scanner using tripod and shadow box under bright outdoor conditions

The measurement volume of a single 3D-scan is 325 x 200 x 100 mm³. The lateral resolution is determined by a point pitch distance of 0.17 mm. A height resolution of 0.04 mm is achieved. The high level of detail in the 3D-scan is shown in Fig. 5.

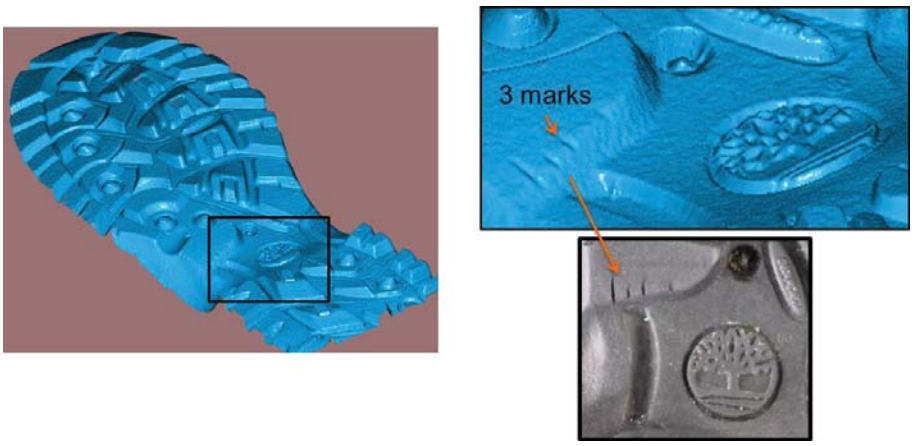


Fig. 5 High level of detail allows the detection of identification marks in 3D-scans

The 3D scanner can be used outdoors for approximately 40 minutes using rechargeable batteries which are integrated into the sensor head. For each measurement, the 3D scan result is processed and presented after some seconds in a preview. The captured colour image is presented as well. All scans are saved in a project structure, including further meta-information such as time and date, user name and brightness settings. The data from the scanner is transferred password protected and by USB-stick to the analysis software.

3 ANALYSIS SOFTWARE PROTOTYPE

The second part of the developed system is the 3D analysis software "R^3 Forensic" which is used by forensic experts in the office. The data import is realized simply by opening a dedicated project file i.e. a file for the crime scene. All scans and colour images taken in that project are opened in the correct structure. Once the data from the 3D-scanner has been uploaded to the analysis software in a first step it is prepared for the subsequent analysis step. Different shading variants are calculated which are later used to emphasize marks in the 3D-data. Optionally, if an impression was larger than the single field of view of the scanner, such as from a tyre, then multiple scans can be "stitched" together with a cloud to cloud registration process (Fig. 6).

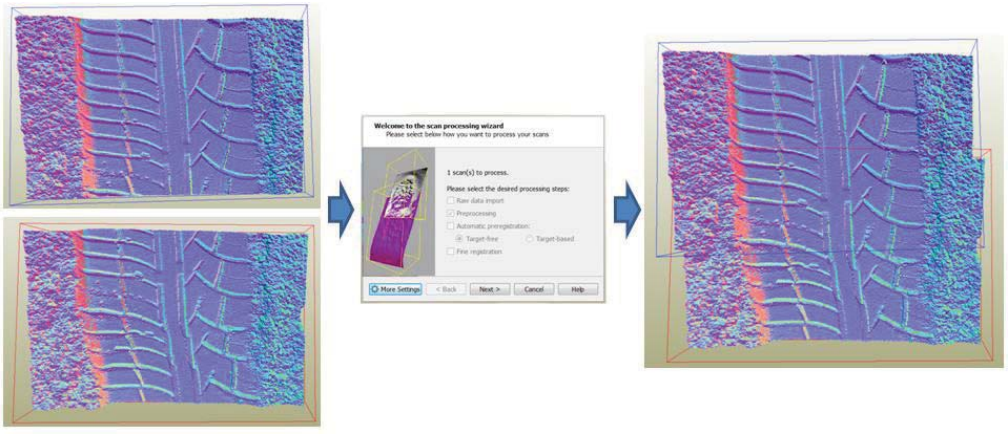


Fig. 6 Wizard guiding the user in the registration process of two scans covering two partially overlapping areas of the same tyre impression

In a further step the high resolution colour data is mapped onto the 3D data (Fig. 7).

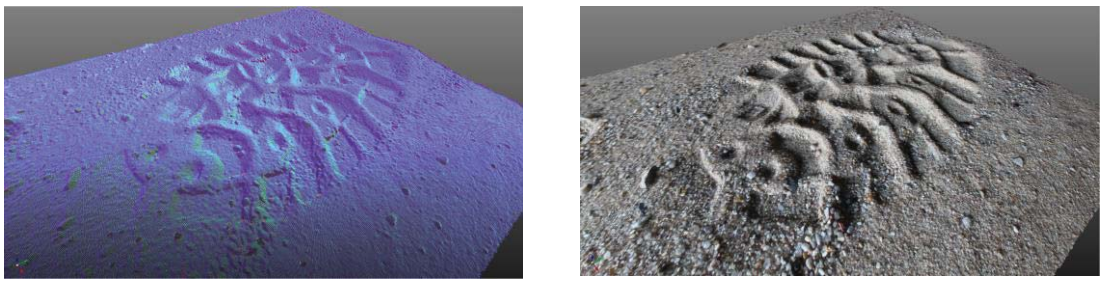


Fig. 7 Left image showing the pure 3D-data and right image with projected colour information showing that small rises are small stones from the underground and not a part of the impression trace itself

The integrated 3D measurement and colour data can then be analysed with the software to investigate characteristics of the footwear and tyre impressions. Class characteristics are determined by the user by comparing the impression with images from manufacturers' or other databases. Individual identification characteristics can be marked by the user with an annotation tool (Fig. 8). The set of possible individual marks is defined by the forensic experts beforehand according to the special rules in their country or region.

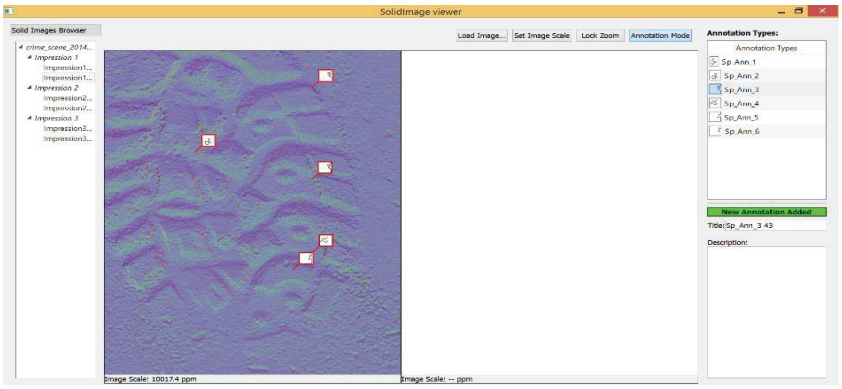


Fig. 8 Annotation tool of the R3 Forensic software which can be tailored by the users

There are further tools that allow the comparison of footwear and tyre impressions with suspects' shoes and/or vehicle tyres and other crime scenes. Two 3D-scans can be presented in two opposite windows. The user can move and zoom through both scans to identify similarities or differences (Fig. 9).

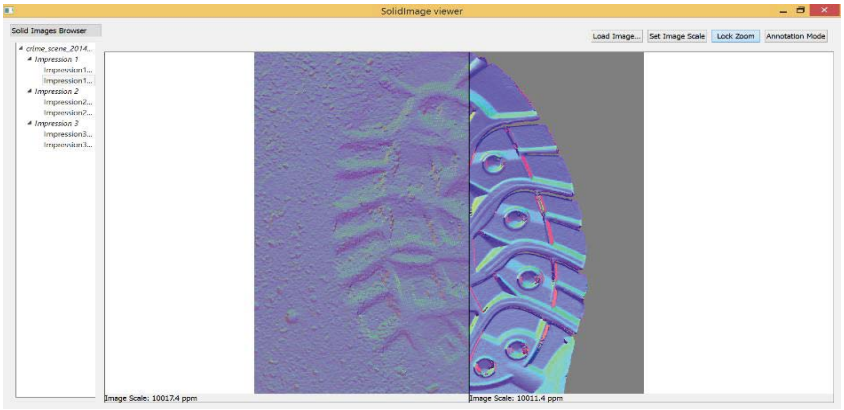


Fig. 9 An example of R3 Forensic software comparison tool

There are several possibilities to insert measurable annotations (profiles, 3D polylines), to export and to document analysis results for further reporting purposes. The data recording and analysis tools have been designed to ensure that the expert assessment

obtained with the 3D-Forensics system will be admissible as expert evidence in court. The original raw data is never changed by the software. Each analysis step is logged and can be undone. A further focus in the development was simplicity and clarity of the software.

Fig. 10 provides an overview of the workflow of the 3D Forensics system. From left to right: scanning process, data processing, comparison analysis and specific analysis.

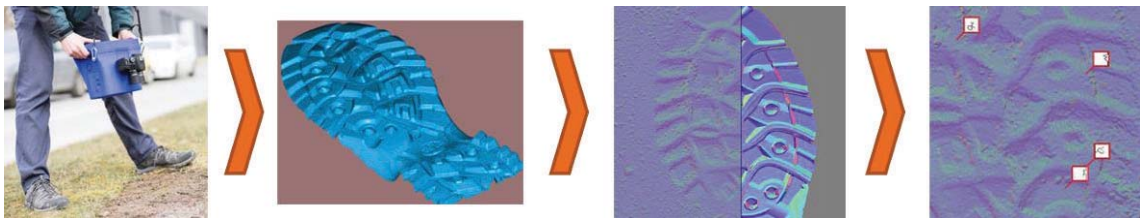


Fig. 10 Overall workflow of 3D Forensics system from scan to analysed impression traces that can be used in court

Prospectively the analysed data can be structured in a database, which contains information about each case and impression. This would allow easy research of footwear and tyre impressions that were present at different cases and can be used as a tool for forensic intelligence e.g. matching traces of the same footwear found at different crime scenes.

4 ORGANISATION OF TEST AND EVALUATION

The test and evaluation of the prototype system, consisting of the 3D-scanner and analysis software, has been organized in four phases.

In Phase I, “Technical characterization”, the basic characteristics of the system, both hardware and software, were documented by performing individual standalone tests. These tests were not dedicated to footwear or tyre impressions solely, but rather to define the operational functionality of the system.

In Phase II, “Reference testing”, the prototype scanner and its complementing software were used to scan and analyse actual footwear and tyre impressions. Within this phase, almost ideal conditions were simulated and used in an indoor laboratory environment. Impressions were also taken with dental cast and photographed in order to compare the results achieved with traditional methods of impression registration and analysis and those achievable with 3D-Forensics.

Phase III “Field testing” contains outdoor filed tests, test scenarios are being developed with representative footwear and tyre impressions, including varying environmental conditions. These tests though still under controlled conditions are enabling a good evaluation of the scanner and analysis software performance parameters in situations close to those expected at crime scenes. Here traditional techniques will also be compared to the results from the new system.

Phase IV “Expanded reference and field testing” will bring the knowledge gained from the previous tests together and simulated scenarios as close as possible to actual crime scenes will be tested up to the expected performance parameters of the system. Here traditional techniques will also be compared to the results from the new system.

At the time of writing Phases I and II have been conducted and Phases III is running and Phase IV will commence in July 2015. Phase I was carried out primarily by the technical developers Fraunhofer IOF, Lucas instruments, Enclustra and Gexcel and Phase II by DelftTech. DelftTech and the Police Zeeland-West-Brabant will primarily carry out the tests in Phases III and IV.

5 RESULTS

5.1 Phase I: Technical characterisation

The following Table 1 and Table 2 show the main characteristics of the 3D-scanner and an overview of the most important tools implemented in the analysis software.

Table 1 Main technical parameters of the 3D-scanner

Parameter	Value
Field of view	325 x 200 mm² (single field)
Measurement height	100 mm
Working distance	455 mm
Resolution	Lateral: 0.17 mm (point pitch distance) / Vertical: 0.04 mm
Accuracy	< 50 µm
Weight	3.6 kg (with attachable digital colour camera 4.4 kg)
Battery time	40 min
Time to scan	< 500 ms
Processing time	10 – 20 seconds
Colour quality	20 MPx / resolution ca. 0.08 mm

Table 2 Most important tools implemented in the 3D analysis software

Tool	Description
Alignment	▪ Semi-automatic stitching of multiple scans e.g. tyre track
Colour mapping	▪ Automatic projection of the external colour image onto the 3D point cloud
Class characteristics	▪ Loading images from manufacturer or other databases ▪ Comparison with actual scanned footwear or tyre impressions
Specific characteristics	▪ Creation of user defined identification marks e.g. scratch types ▪ Marking of identification mark positions within the scan data
Measuring tool	▪ Easy measuring of distances within the scan data e.g. shoe size and width
Distance map	▪ Coloured drawing of the height profile of the impressions e.g. to visualize the depth of the impressions
Annotation	▪ Inclusion of comments at defined positions inside the scan data
Section tool	▪ Visualizing of sections through the point cloud

5.2 Phase II: Reference testing

The reference testing was performed using two representative shoes and a single separate tyre. Impressions were created in boxes with different underground materials: sand, clay, soil and mortar (Fig. 11).

Fig. 11 Boxes with different ground materials, from left to right: sand, clay, soil & mortar

The surfaces are common at crime scenes and all have different structures and brightness. Tests were carried out indoors under controlled conditions. (Snow will be tested at an indoor snow slope later in the project.) Every underground was scanned by using different brightness settings and scan modes (scan modes correspond to

different fringe pattern sequences). The handheld and tripod mounted operation modes for the 3D-scanner were also compared

Fig. 12 shows the comparison between the original shoe, the photographed impression in sand and the 3D data (with inclination shading) collected. The result for sand is very clear and has a high level of detail. The results of the other surfaces show that the quality of the impression itself is very much dependent on the surface structure. It is more difficult to obtain detailed impressions in clay and soil. When the impression has a good quality the 3D scan captures enough level of detail to perform a forensic comparison with the original shoe. The captured 3D and colour data was successfully uploaded into the dedicated "R³ Forensic" analysis software by importing the corresponding project file and it was successfully prepared for analysis. The analysis tools provided a convenient means for analysis of the data by forensic experts.

Fig. 12 Comparison of shoe, photograph and 3D data of impression in sand under laboratory conditions

5.3 Phase III: Field testing

The field testing is being performed with the same underground materials as the reference testing before. At the time of writing the first experiments have started under outdoor conditions.

Fig. 13 shows the comparison between an original shoe, the photographed impression in clay, the plaster cast and the 3D data (with inclination shading) collected.

Fig. 13 Comparison of shoe, photograph, plaster cast and 3D data of impression in clay under field conditions

The comparison between the plaster cast and the 3D data shows that the 3D data has more fine details that match with the original shoe. The 3D data also looks less irregular than the plaster cast. The outdoor experiments have also confirmed that the

amount of surrounding light is an important disturbing factor. Using a shadow box reduces interferences strongly and improves the scan results. Forensic experts are able to compare and analyse the captured 3D data using the dedicated "R³ Forensic" under the more difficult circumstances of the testing in Phase III compared to Phase II.

5.4 Assessment of results to date

The tests carried out together with discussions with forensic experts are the basis for the following assessment. Forensic experts are very interested in having a 3D-scanner to obtain data from footwear and tyre impressions as they expect a number of operational advantages (detailed in [1]), but particularly faster recovery and analysis of the traces and because there is a general move to storing evidence digitally. In the past, the resolution of 3D-scanners which could be used at crime scenes was not enough to capture the tiny identification marks in the impressions. The tests indicate that the resolution of the 3D-Forensics system achieves this requirement. The software "R³ Forensic" dedicated to this application is a further advantage. It allows an analysis of the new 3D data in a way in which forensic experts are used to working with traditional techniques.

6 OUTLOOK

Test phases III and IV must prove the usability of the system in the field environment. As a next step, the prototype would be engineered into a product and commercialised. The main barrier to commercialisation is expected to be financial risk in connection with the investment to engineer a product without the certainty that police forces have the capital resources to procure the product. Commercialisation of the product would be supported through its validation within a relevant certified process. Future development activities could include, for example, extended functionality to enable automatic comparison of 3D data as an optional filtering support for forensic experts.

7 CONCLUSION

Optical 3D-scanning enables quick and contactless capturing of impression traces with detailed information. The analysis of digital 3D-data instead of plaster casts will ease the work of forensic experts and will enable increased linking of data from different crime scenes. 3D-Forensics has delivered a 3D-scanner prototype with integrated analysis software. The technical characterization results indicate that the technical requirements derived from the user requirements have been achieved. Reference and filed testing to date indicate that the system can provide finer 3D details than traditional techniques but that when surrounding light is strong a shadow box must be used. Further field testing and evaluation was on-going at the time of writing.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°. 312307, http://www.3D-Forensics.eu. The project started in 2013 and ends in August 2015.

REFERENCES

[1] Crabbe, S., Kühmstedt, P., Vassena, G. M., van Spanje, W., and Hendrix, A. (2014). *3D-Forensics – Mobile High-Resolution 3D Scanner and 3D Data Analysis for Forensic Evidence*. 9th Future Security - Security Research Conference; Berlin, September 16 -18, 2014; Proceedings; Klaus Thoma, Ivo Häring, Tobias Leismann (Eds.) (ISBN 978-3-8396-0778-7) pp 215-222.

TECHNICAL-SOCIO-ECONOMIC MODEL OF THE URBAN CRISIS MANAGEMENT SYSTEM FOR GRID-BOUND INFRASTRUCTURES (UCMS) TO INCREASE THE URBAN RESILIENCE, AND TO MINIMIZE CONSEQUENTIAL DAMAGES

Christoph Stroschein and Christina Bannuscher

cs@gesi.eu
Managing Director GESI Deutsche Gesellschaft für Systeminnovation mbH
Savignyplatz 1, 10623 Berlin

cb@gesi.eu
Senior Advisor GESI Deutsche Gesellschaft für Systeminnovation mbH
Savignyplatz 1, 10623 Berlin

Abstract

The research project InnoGeSi deals with the safety of energy networks in a private and economic environment. Grid-bound infrastructures are highly complex, increasingly networked and vulnerable systems. Thus, even minor incidents may have a cascading effect on other sectors and areas of life which are not obviously interconnected and result in immense subsequent damages, so fast and efficient action is necessary. This requires a coordinated and comprehensive communication within the stakeholders concerned as well as also affected infrastructure operators.
So far, there exists no dedicated body which collects all the available information and is able to provide a precise analysis of the situation (real time picture) to enable the infrastructure operators to make timely appropriate decisions in order to eliminate errors that may rise to fatal misjudgments.
Thus the central element of the project is to create a system with the above-mentioned functionalities towards the possible inclusion of additional stakeholders.

Keywords: smart city, urban resilience, security, innovation, grid-bound infrastructures, research projects, business model

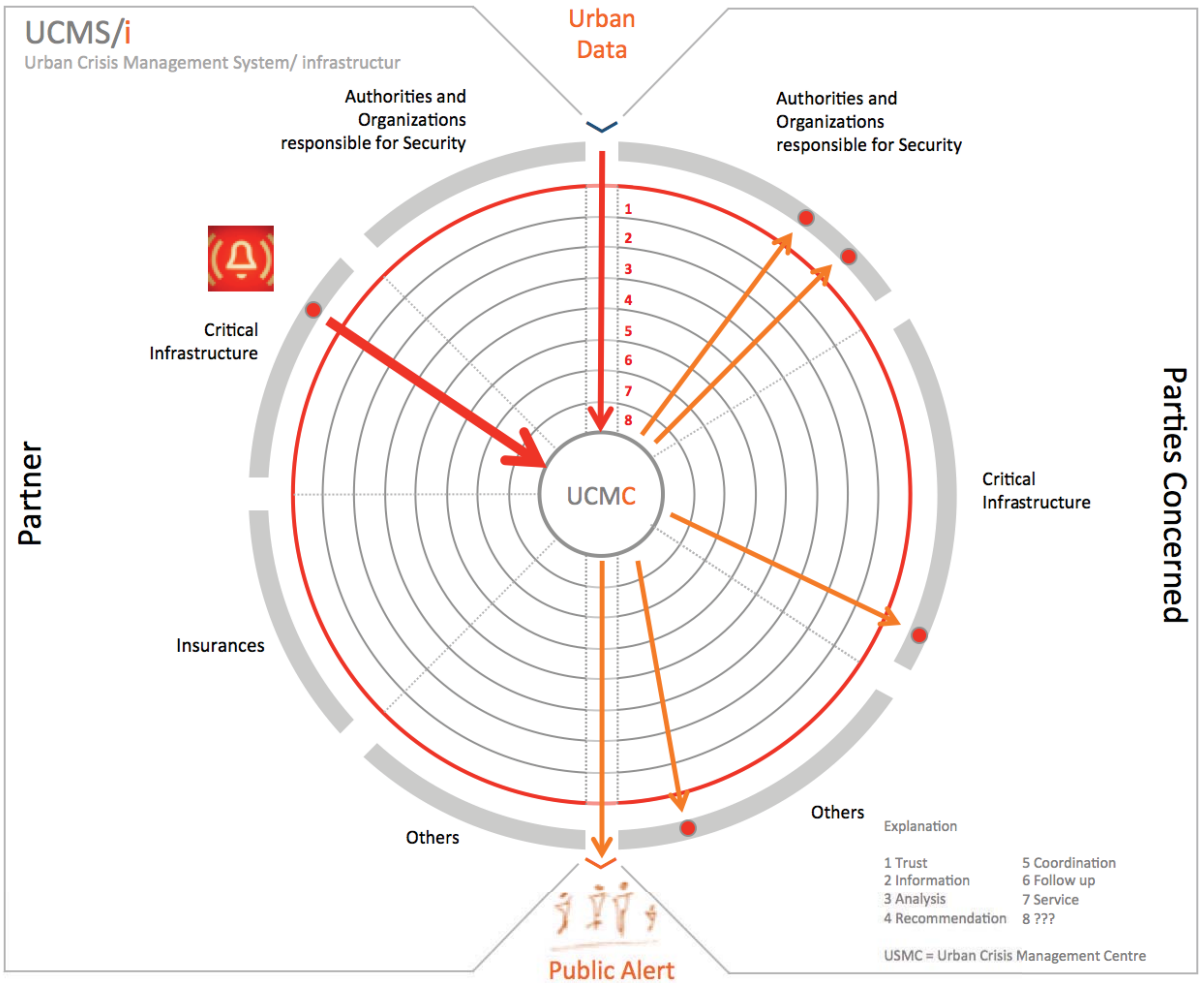


Fig.1 Pattern of the Urban Crisis Management System © GESI

The graphical representation above illustrates in a simplified manner the structure and function of an urban crisis management system (UCMS).

The different stakeholders provide the urban crisis management center (UCMC), shown in the middle of the graph, in advance and/or in case of an event with their relevant data. The UCMS is a physically existing center, in which suitably qualified staff, collects and prepares the incoming data and provides these data in the form of a real time picture to potentially affected operators of critical infrastructure.

1 INTRODUCTION

Cities are a focal point for some of the most profound economic, social, and technological issues facing the world today. They depend on the effective and reliable operation of infrastructure systems to deliver water, electricity, natural gas, food, healthcare, transport and telecommunication services. This implicitness is based on the proper operation of technical systems. Contrary to what their ubiquitous availability suggests, their structure is far more complex. Generally speaking, we only really notice them when they don't work. Supply networks are embedded in other structures, social arrangements and technologies, whose function is made possible and maintained only through them. Due to their invisibility, functioning infrastructure systems are self-understood in modern societies, not just as a state of perfect technical stability, but also to guaranty social stability, the wide spread circulation of goods and communication with high social cohesion. Thus, disruption of such infrastructure

are of major interest to the population and will have a large impact on social life and corresponding infrastructures.

Especially grid-bound infrastructures are highly complex, increasingly networked and vulnerable systems. The growing networking within and between vital infrastructures has the consequence that any kind of interference may serve in the future more and more damage. Even small, harmless at first acting disturbances can lead to a chain reaction and cause damage to the whole system and, in a worst-case scenario, can even end up in the failure of an entire system.
An important aspect of the smart city concept is resilience, the ability of cities and communities to withstand or bounce back from any incident, as well as to manage the ongoing challenges facing urban communities. In order to address these challenges cities are going to develop new, smart concepts aiming to improve the quality of their citizens lives by guaranteeing sustainable social, economic and urban development. Empirical evidence supports the conventional wisdom that primary prevention activities are frequently cost-effective. Thus, customized technological solutions are required to increase the resilience of critical infrastructures and to protect cities from significant financial damage in case of an incident, or at least reduce them.

2 PROJECT OVERVIEW

Even the most minor incidents, not to mention major crisis events, require the cooperation of different stakeholders involved and authorities. A common understanding of the current situation, unfolding events, structures, processes, data etc. is mandatory in order to achieve coordinated action and to avoid misunderstandings in the event of a crisis so that fast and reliable decisions can be made. The evaluation of exemplary events of the last few years had shown that better information and coordination through infrastructure managers would have had significant impact on the assessment of the situation and the measures taken. Better communication, so the assumption, would have significantly reduced the damage caused or, entirely or in parts, avoided.

Governmental organizations can no longer afford to fund the necessary safety concepts on their own, so more and more private economic innovative solutions are required - developed out of economic and commercial necessity.

The research project InnoGeSi recognized the growing need for a pro-active approach in the area of the security economy.

Thus the project investigates which economic, organizational and institutional changes are necessary in order to foster a stronger safety and security culture within regional, national and international energy networks. It aims to develop an innovative business model in the field of network security: a real time decision support system for complex incidents, the urban crisis management system (UCMS).

The main object of the investigation was to find out:

- How to increase awareness for the vital necessity of building up such a system?
- What requirements need to be met for operators of the grid-bound infrastructures to cooperate voluntarily without having to disclose confidential business information and trade secrets?
- Which different types of public and private finance and incentives are considerable as a common communication platform?

- How important is it to offer more comprehensive services (e.g. training, standards and technical design services)?

In this project the focus was set on the pipeline und cable-based infrastructures (gas, electricity, telecommunication, sewage, district-heating) as they create the supply channels of the urban life of which also nearly all sectors of private, public and economic life depend on. These structures are thereby simultaneously complex, increasingly interconnected and thus vulnerable, so that in the event of an incident the failure of a medium can lead to bottlenecks in supply and cascade effects, carrying high economic consequential damages. These often not only affect the infrastructure operators, in whose network the event took place, but also additional infrastructure operators, companies or private households depending on supply of grid bound structures. As a result immense subsequent damages may affect the economy in general just as private households e.g. through loss of production or data loss in public and private corporations. Often this also entails a considerable damage to the operator´s image. In addition, there is a tight cohesion between function and supply with the media of grid bound infrastructures and the function of grid unbound but yet critical infrastructures. The function and the performance of the service of general interest are thereby increasingly direct and indirect, depending on each other.

In the event of an incident, it is not only necessary to act as fast and efficient as possible to prevent high economic damages but also to be able to prevent possible time-displaced cascade-effects (time cascade/escalating cascade/cascade because of suboptimal information).To secure a smooth communication in order to overcome a critical event is inevitable. The so called "golden hour" must be used, to keep already existing as well as possibly resulting consequential damages as low as possible (minimization and avoidance of impacts of an event). Therefore a coordinated and comprehensive communication within affected companies just as possibly afflicted infrastructure operators is vital.

So far, there exists no dedicated body which collects all available information and is able to provide a maximum amount of information (real time picture) to enable the infrastructure managers to take the necessary measures in the event of an accident. But in this context errors that may rise to fatal misjudgments must be avoided. Therefore a precise analysis of the situation and an efficient oversight that enables timely decisions is necessary.

The so called Urban Crisis Management System arises through the need of a common understanding of the current situation and supports the interactions between all parties.

The project employed with comprehensive analyses, scenarios and an interdisciplinary approach to identify the specific challenges, problems and opportunities associated with resilience in a business context to enable the development of the UCMS business model. Interviews with network operators were carried out from different points of views. Discussions and workshops were held with representatives. The information obtained was analyzed and the joint linkage determined concerning the relationships of performance, communication and disruption. These relationships exists between relevant types of network components, organizational units and other relevant factors that were determined and described during the system analysis as well.

Key questions (framework) to develop the UCMS business model:

- Market innovation:
  What kind of business models may stimulate the utility market by innovative solutions combined with new impulses for safety and security?

- Macro-economic and security:
  In market economies, investment decisions are fundamentally based on cost-benefit analyses of varying degrees. So the key question was: What kind of intelligent finances solution need to be developed?

- Insurance companies:
  What kind of incentives should be created for businesses to increase their resilience?

- Standards, norms and regulations:
  What kind of standards, norms and regulations are necessary to foster an innovative security business model?

- Human resources development:
  A well-trained labor force is an important factor for investment decisions. What kind of education and training is necessary to ensure a highly-qualified workforce?

3 BUSINESS MODEL UCMS

The system is primarily a central communication management system of the city's most important infrastructures. The principle behind an urban crisis management system is the creation of a situation center, which is based on the collection of static data provided by the participants in advance. In the event of an incident a real time picture will be created on the basis of these data, as well as all other available information and will be used to create an update. This precise analysis of the situation enables the infrastructure operators to make timely and appropriate decisions for an effective crisis response in order to eliminate errors that may rise to fatal misjudgments to the actual incident situation.

Prerequisite:

- Stakeholders have to provide their network and construction plans in advance in digital form
- The data have to be periodically updated by the respective infrastructure operator
- The infrastructure operator is liable for the accuracy, topicality and completeness of all data provided by him
- Business Operators and other cooperation partners participating on a voluntary basis

To harmonize the needs of different stakeholder groups to a much greater extent this basic version of the UCMS is modularly expendable to increase preventive as well as reactive emergency management (e.g., historical analysis of past events, preparation of assessment criteria, the preparation of forecasts and the drawing up of scenarios (alternatives), public alert, public awareness, training of personnel, etc.).

In the next stage, the aim is to make the data in addition to the static format also available in dynamic format (e.g. daily plan works and data from the control center in real-time). In addition, in this phase data from other external partners, including weather data, traffic flows, information from social networks etc. shall be available and used to create actual situation pictures (Urban Data) .Currently used systems allow already, in theory, advanced data analysis e.g. to include online data or event-driven information from other sources in the communication and the creation of situation pictures. But the crucial factor is to guarantee for the accuracy of data from open sources.

From the economic perspective the UCMS can be run by non-profit or private organization (GmbH) or, as another option, by government monitoring (also this option would require

regulations of what businesses are expected to do in order to become more resilient). Even though the public and private interest is big to keep damages to a minimal, there is, until now, almost no financial cooperation between the public hand and e.g. the insurance economy.

4 PARTNERS OF THE UCMS

Partners of the UCMS are not only the operators of infrastructures themselves, but also by damages (direct or indirect) affected public services (e.g. emergency services, fire brigades etc.), fault clearance services and insurance companies, provider of meteorological services and investors.

5 BARRIERS AND POSSIBLE SOLUTIONS

- Awareness:
  A major problem for the stakeholders willingness to participate in an urban crisis management system is the lack of/or insufficient awareness. The reasons are to be found in an absence of awareness of the topic in general within companies, as well as the fact that the added value, which can be generated by the establishment of a superordinate urban crisis management system is not seen at all. The high level of supply security in Germany just as the perceived civil safety within the society have the effect that the need for increased investment in preventive safety is considered as unnecessary. In addition, there is still the fundamental problem that investment in preventive safety measures seems to influence the business result only partly or not at all.

- Trust:
  In order to participate, there is the need to establish a high level of trust between the different stakeholders, especially with respect of handling internal and sensitive company data. A contractual guarantee should help to establish this confidence. It would include that the relevant information from e.g. grid plans, network plans, switching states, service connections and geographical data, will be available to all potentially affected partners only in case of an incident as a cutout and in the minimized form of a situation report.

- Economic efficiency:
  The purpose of any company is to maximize the obtained profits from their business. The possibility to quantify and put a monetary value on any of these avoided damages is key for all participants of the UCMS. The calculation of scenarios, based on data compiled of events from the past, should provide a sound argumentation basis to demonstrate the damage for the company itself, as well as for the public/society. An additional option would be an incentive from insurers by introducing customized innovative insurance policies.

6 CONCLUSIONS AND KEY MESSAGE

Benefits of the UCMS:
- Event-driven prevention
- Early warning system enables to use the so called “golden hour”
- Real time picture of the situation
- Reliable implementation of information- and alert chains
- Exact, complete and judicially indisputable information supply of situational development
- Reliable information transfer due to stakeholder’s willingness of cooperation

Conclusions:

- Private financing to develop the UCMS is possible
- There is a barrier of trust between the stakeholders even though they are aware of the necessity to cooperate
- The sharing of sensitive data is a major problem which needs to be addressed
- In the final stage InnoGeSi project will investigate in greater detail how to overcome this key problem in order to identify appropriate mechanism

7 ACKNOWLEDGEMENTS:

The presented work was mainly carried out within the project InnoGeSi. The project is funded by the Federal Ministry of Education and Research of Germany. We are grateful to all members of the project InnoGeSi and to all partners and associated partners for their cooperation, providing access to all necessary data and for many inspiring discussions.
For more information, visit www.innogesi.net

CHALLENGES FOR THE USE OF INFORMATION TECHNOLOGY AND STANDARDS IN INTERNATIONAL DISASTER MANAGEMENT

Lina Jasmontaite[1], Uberto Delprato[2], Bettina Jager[3] and Georg Neubauer[4]

[1] *lina.jasmontaite@law.kuleuven.be*
KU Leuven, the Interdisciplinary Centre for Law & ICT (ICRI-CIR), iMinds, Sint-Michielsstraat 6 box 3443, 3000 Leuven (Belgium)

[2] *u.delprato@iessolutions.eu*
IES Solutions srl, Via Monte Senario 98, 00141 Roma (Italy)

[3] *bettina.jager@ait.ac.at*
AIT Austrian Institute of Technology GmbH, Digital Safety & Security Department, Donau-City-Strasse 1, 1220 Vienna (Austria)

[4] *georg.neubauer@ait.ac.at*
AIT Austrian Institute of Technology GmbH, Digital Safety & Security Department, Donau-City-Strasse 1, 1220 Vienna (Austria)

Abstract

In this paper we will reflect on the regulatory framework for communication exchange in case of international disasters. In particular, we will consider the potential challenges of the existing regulatory measures and standards for information exchange and disaster relief in the EU. First responders' behaviour during the disaster relief is defined by standards and local measures regulating the domain of civil protection. Sovereign states adopt legislation that determine the set-ups of civil protection mechanisms, communication channels and other relevant measures related to disaster response. States also carry responsibility for adopting laws that would enable assistance from national or international resources. Often "international disasters" challenge domestic regulations with strong requirements on flexibility and ability to accommodate a number of local teams and supporting teams from either neighbouring administrations (e.g., counties, districts or municipalities) and/or international organisations (e.g., the EU or the United Nations) and/or Non-Governmental Organisations. However, even in the event of "international" disaster relief, which results in coordination of multi-level governance structures, local teams of first responders depend on their contingency and disaster management plans and on their ability to integrate and share information with the assisting teams.

Disaster response strongly depends on the efficiency of information exchange: rich and timely information can empower stakeholders and first responders with a good situational awareness and allow an optimal allocation of resources. In general, sharing and processing data, including personal data, during emergencies is subject to legal requirements. Often legal requirements set constraints for operational staff involved in relief actions. Yet, due to the need for prompt actions and the aim for providing help, responders in disaster relief may fall short on compliance with legal requirements.

Given such contrasting predicaments, it is timely to discuss whether there is a need for legislative and policy measures that would reduce uncertainties influencing the fieldwork of first responders. Legal framework affects the way how information exchange is enabled amongst various layers at different institutional stages, which may include sharing of operational pictures, updating availability of human and material resources and forwarding individual-related data. Therefore, in this paper we will set the scene for such a debate by considering the limitations of existing regulatory frameworks and standards. We will also consider how they could be integrated with new technologies and legal initiatives.

Keywords: crisis management, disaster relief, standards, communication, legal aspects and information exchange.

1 INTRODUCTION

The word “disaster” indicates an alarming situation and may be used to refer to emergencies, crisis, critical events, terrorist attacks, technical accidents and alike events having adverse impact. The EU has adopted a definition for a disaster, it "means any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage." [1] Yet there is a number of other definitions for the term “disaster”. It can be argued that to date the most elaborate definition has been proposed by the United Nations International Strategy for Disaster Reduction (UNISDR), which defines “a disaster” as “a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources.” This definition has been recognised by various first responders and by the International Federation of Red Cross and Red Crescent Societies (IFRC). The International Disaster Database EM-DAT takes a somewhat different approach and proposes specific criteria to qualify a situation as a disaster, for example, ten or more people reported killed, a hundred or more people reported affected.

Disasters can be categorised according to different dimensions, such as source (e.g., natural or human-made), scope (e.g., local or international) and impact (e.g., low and high). “International” disasters, on which we focus throughout this paper, refer to situations either where disasters occur in cross-border areas and require a combined action by neighbouring countries, or where the impact overwhelms the response capacity of the affected country. An important indicator for the term cross-border disaster management is that it exceeds the daily-routine procedures of emergency services and requires additional capabilities. The Council of Europe Convention on Transfrontier Co-operation between Territorial Communities or Authorities (no. 106) facilitates and encourages cross-border cooperation on civil protection and mutual aid in the event of disasters occurring in frontier areas on the basis of agreements between regions and local authorities. Therefore, at the moment the cross-border cooperation is subject to international (bilateral and multilateral), national and regional treaties and/or agreements.

When it comes to organising an effective disaster response, it is not the number of different disaster definitions that may have an impact on the field work but rather the lack of common standards for emergency communication. This is of a particular concern to the EU as a crisis manager and is a specific area of research of the EPISECC project. [2] The EPISECC project aims at developing a Pan-European information space for all actors providing disaster relief. [3] The Pan-European information space would be used to improve the collaboration in disaster management situations. Setting such a system implies an EU wide standardization activity, which will expand the EU market for organizations developing solutions and tools for crisis management.

In the following sections of our paper we will reflect on the current EU approach to disaster relief that includes both regulatory measures developed by the EU and its Member States and standards developed for various purposes at different levels. The main objective of our paper is to consider whether the existing standards and procedures solve practical problems on the disaster scene or whether they clash with national laws on information management in disaster relief. The second section will discuss the EU regulatory framework for disaster management. The third section will point out some limitations of the EU Civil Protection Mechanism. The fourth section will underline challenges for available tools in disaster management. The fifth section will map and analyse the current landscape of available standards used in disaster management. The subsequent sections will analyse the impact of operational, cultural standards and good practices on disaster management. The final section of the paper will summarise the discussion and propose actions for the future.

2 THE EU APPROACH TO DISASTER MANAGEMENT

At the moment, the EU disaster management framework is highly fragmented. The civil protection field is typically subject to domestic laws and regulations. Sovereign states determine the set-up of their civil protection mechanisms, communication channels and other relevant measures related to

disaster response. Practice has shown and first responders point out clear limitations of the current approach, which often give rise to technological, sociological, and organizational challenges. [4]

The EU has recognized the need for improved and more coordinated cooperation within the Union between national civil protection services in disaster response in Communication “The EU Internal Security Strategy in Action: Five steps towards a more secure Europe”. [2] The Communication points out a need for “improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence [...] solidarity in response, and responsibility in prevention and preparedness with an emphasis on better risk assessment and risk management at EU level of all potential hazards.”[2]

At the same time, EU citizens are also in favor of a more coordinated disaster management approach. A recent Eurobarometer study shows that majority of EU citizens deem that a coordinated EU action in dealing with disasters could be more effective than actions by individual countries. [4] Moreover, a large number of EU citizens consider pooling civil protection resources in the EU to be more cost-effective than each country managing their own resources. [5]

3 THE SCOPE OF THE EU CIVIL PROTECTION MECHANISM

The EU Civil Protection Mechanism (CPM) was launched in fall 2001, just shortly after the terrorist attacks in the USA. Some argue that the EU CPM was built on old ideas but provided new tools. [7] Indeed, several EU initiatives related to the Member State cooperation in the civil protection area, in particular in the field of environmental protection, date back to the 80’s. The novelty of the EU CPM was that it provided an integrated coordination in the field of disaster response.

The EU CPM allows swift relocation of needed resources. For the mechanism to be triggered, a country hit by a disaster has to submit a request for assistance to the European Commission. Although only European countries are parties to the mechanism, the mechanism can be activated to tackle disasters outside the EU. The mechanism was used 186 times between 2007 and 2013.

The setup and advancement of the civil protection mechanism reflect the institutional and competence changes within the EU. The Lisbon Treaty (2009) has provided the EU with a new legal basis to encourage Member States’ cooperation in the civil protection matters. According to Article 196 of the Treaty on the Functioning of the European Union (TFEU), the EU can support and complement Member States actions undertaken on national, regional and local levels related to the field of civil protection [8]. The EU can also “promote swift, effective operational cooperation within the Union between national civil-protection services” and “promote consistency in international civil-protection work” [8]. Article 196 of the TFEU should be read together with the solidarity clause. The solidarity clause provides that in case of natural or man-made disasters Member States “shall act jointly in a spirit of solidarity” [8]. The wording of this article is somewhat vague and it does not set any limits as to the implementation of the provision under different circumstances. However, it underlines the existing limitations of the current approach. The mechanism is based on voluntary participation and can be triggered only in a response to “request for assistance under the Union Mechanism in the event of an imminent disaster, or during or after a disaster, to address its immediate adverse consequences”. [1] Noteworthy, it does not cover disasters of a smaller scale or occurring in cross border situations.

4 REMAINING CHALLENGES FOR DISASTER MANAGEMENT

Coping with disasters, in particular, the ones overwhelming the capacity of a country, requires coordination of multiple actors and multi-level governance structures. Disaster management across border includes stakeholders from various countries or international organisations, governmental bodies and agencies and heterogeneous legal personalities. [9] Typically, cross-border disasters demand cooperation between governmental decision-makers and disaster relief services of affected countries, response units of assisting countries and/or relief personnel of international organisations deployed to assist in disaster management. Many illustrative examples show the struggle to set up

well functioning disaster relief structures. As stated by Walle and Turoff, the distribution of responsibilities is an important issue in disaster management. [10] Responsibilities at different levels are depending on the extent of the event and the available capabilities to cope with. In cross-border disasters the resilience of an affected community – measured by its ability to recover by its own capacities – is challenged by principles of solidarity, subsidiarity and sovereignty. Coordination efforts include information sharing for the purpose of resource management (e.g. resource allocation), situational awareness (e.g. sharing geographic information) and command and control activities (e.g. deploy relief units). Sagun et al. distinguish between four channels of information flow during the Disaster Management, namely communication within an organisation, between organisations, from the public to organisations and vice versa. [11] In order to obtain a common picture of the situation by merging information, which is spreading across several stakeholders, harmonised procedures are obligatory. At each level of the command and control structure (strategic, tactical and operational) different kinds of information are available. According to specific information requirements, at the operational or field level, mainly information about available human and material resources as well as important geo-locations like hospitals will be shared. While information gathering at the tactical level focuses on collecting battlefield information, aggregating and re-providing information about domestic capabilities, standard operating procedures and maps in use for further use, at the strategic stage the so-called “big picture” is generated. Here, all activities in the course of the disaster relief process are monitored based on the information obtained from the levels below. This is the place where an overall strategy for disaster relief is developed. [12] Moreover, with the ability to overlook, the provision of additional resources, units, capacity etc. that might be requested is a major business. Therefore, most sustainable efforts to harmonise conflicting approaches in sharing information for the purpose of cross-border disaster management can be undertaken at the strategic level. Strategic actors such as legislators or policymakers have the power to initiate or pass laws favouring a common disaster management. Thus maximise the effectiveness of actions in fighting against disasters by establishing a common framework for tactical-operational stakeholders such as incident commanders and member of crisis units.

Apart from legal requirements, information exchange in disaster management is often challenged by practical problems such as language barriers, which are located at a low level. Challenges to interoperability might be due to a lack of common practice, outstanding experience, heterogeneous taxonomy, incompatibility of applied systems. Additionally, it has been observed that first responders are often challenged to comply with competing regulatory regimes while providing disaster relief. For example, in Austria, alike in the other EU Member States, information exchange (processing) that includes personal details is subject to legal rules. Obtaining information about a single person depends on the role and remits of an organisation or institutional unit, which are defined by its mandate to become active during disasters and/or emergencies. In certain cases organisations are constrained to forward personal information. For example, Austrian ambulance services are authorised to process data about missing persons to the law enforcement authorities.

Problems in coordinating disaster relief or exchanging information across different organisations become obvious at the fieldwork level, but there is some evidence that interoperability problems arose at a higher level of organisation. The holistic view on the event can be located at the strategic level, where long-term strategies, definitions of relevant terms and an appropriate framework (e.g. laws and policies), as well as risk monitoring activities and communication with the public are important tasks. For disaster relief actions the strategic level provides the framework for allocating various resources and coordinated actions. Especially in cross border events, transnational agreements concluded on the strategic level emphasize the role of actors on the strategic level. Measures of the tactical level are dedicated to ensure that the actions taken by the operational level are coordinated, coherent and integrated in order to achieve maximum effectiveness and efficiency. [13] At the tactical level, commanders of disaster relief units have to deal with difficulties of allocating resources in a coordinated way. In order to perform relief efforts in an efficient way, the harmonization of emergency operations is considered as a challenge for the operational level. Because operational forces are the staff at the field, they have best prerequisites to assess the impact and inform the tactical level about the situation needs.

5 COMMUNICATION EXCHANGE STANDARDS IN DISASTER MANAGEMENT

Standards constitute a significant part of regulatory frameworks and they may be understood in a number of ways. In a broad sense, various instruments, such as legislative measures, directives, and regulations introducing certain requirements, may result in a standard. In a narrow sense, standards can be understood as technical specifications. Therefore, often a standard is considered to be “a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose”. [14]

At the same time, standards may be grouped according to different criteria. For example, standards may be formal or informal, based on good practice or a mandate given to a particular working group. Standards in their application can be global/international, regional (e.g., European) or domestic (e.g., limited to a country).

In the following sub-subsections we analyse available standards for communication in/for disaster management. In particular we will consider several examples of standards reflecting technical, operational and cultural interoperability layers. We will reflect on the use and practical implications of these standards to a disaster response.

5.1 Interoperability layers

Interoperability is defined as “the ability of two or more systems or components to exchange information and to use the information that has been exchanged”. [14] In disaster management interoperability can be seen as the primary need at all levels for taking decisions and managing operations.

To improve the understanding of the organisational processes in emergency situations, the ESENET project adopted a structure based on the concept of “Interoperability Layers” (fig. 1). [15] The resulting "Interoperability Stack" shows how the crucial challenge of ensuring interoperability and communication in disaster management requires the implementation of several levels of interoperability, which range from the basic physical interoperability of devices to the agreement of political objectives of the organisations. The organization of the sections is bottom-up (i.e. from the Technical Layers up to the Organisational ones) and the central layer ("knowledge/awareness") is where both technical and organisational strands tend to: it represents the ultimate goal of the whole concept of interoperability in emergency management.

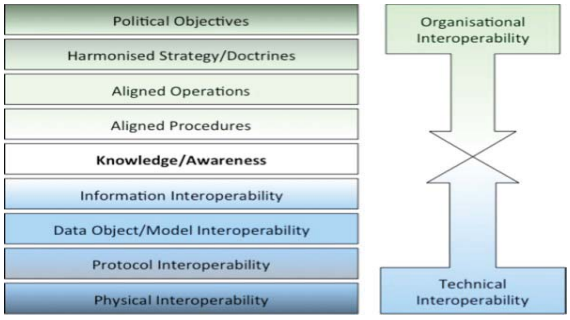


Fig. 1 - Layers of Interoperability (ESENET project)

For the purposes of this paper, we shall divide the above listed nine layers into three groups: Technical, Operational and Cultural.

5.2 Technical standards

Many Standardisation Organisations (SO) exist, combining different geographical relevance (e.g. global or regional), covered technical area (e.g. telecommunications, electronics, Internet) and application domain (e.g. engineering, emergency, transport). It is well beyond the scope of this paper to survey all the existing technical standards that are applied or are relevant for disaster management. Yet it is worth mentioning, the main SO and an important initiative from the European Commission for supporting the European Union policy on security: the Mandate 487.

The two main SO at global level are the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), whose standards span from agriculture and from electronics to packaging. Besides a large number of standards commonly used in emergency

management, the activities of the ISO Technical Committee (TC) 223 (Societal Security) are of particular relevance for disaster management. ISO/TC 223 is structured in six Working Groups (WG), covering Emergency Management, Resilience and Continuity, Communication and Mass Evacuation. Concerning data exchange, it is particularly relevant the Technical Report ISO/TR 22351 "Message structure for exchange of information" approved and ready for publication (at the date of the writing of this paper). [16]

The three main European SO are the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). Additionally, ETSI has created a dedicated project named EMTEL (Emergency TELecommunications) to work on areas of great interest for disaster management. Besides other, the Technical standards TS 102 181 (Requirements for communication between authorities/organizations during emergencies), TS 102 182 (Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies) and TS 102 410 (Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress) are relevant for this paper.

CEN and CENELEC have consolidated a close collaboration and they are now commonly referred as CEN-CENELEC. CEN/TC391 "Societal and Citizen Security" is particularly relevant for disaster management and was the leading group of the efforts carried out under the Mandate 487. More precisely, the Mandate 487 concerned the development of a work programme for the definition of European Standards and other standardisation deliverables in the area of security. It was aimed at analysing needs and possible activities for defining interoperability standards (technical, syntax, semantic and operational) and expected performances. The activities performed by CEN-CENELEC and ETSI under the mandate 487 have produced a final report "Proposed standardization work programmes and road maps".

In addition to these official SO, it is worth mentioning other initiatives aimed at defining de facto standard, such as the OASIS (Advancing Open Standards for the Information Society), a non-profit consortium that develops and promotes open standards for the global information society. Another non-profit organization relevant for emergency management is the Internet Society (ISOC), whose Internet Engineering Task Force (IETF) works on standards in emergency management through its Working Group "Emergency Context Resolution with Internet Technologies" (ECRIT).

It should be noted that when systems for disaster management are implemented, also national standards and proprietary implementation come into play, somehow contrasting the global interoperability targeted by all the mentioned standards.

5.2 Operational standards

To date, only limited literature is available on good practices that are used by organisations providing disaster response. Sharing of information across border varies from one country to another and is determined by the nature of the relationship between nations. There are no overarching standard procedures which serve as a common approach how to respond to a disaster in the best way.

Currently the European Commission is coordinating the development of a Community of Users on disaster risk and crisis management. On one hand multiple bodies of the European Commission are responsible for different policy aspects of crisis management, on the other a large multitude of European as well as national research projects is performed in different domains being relevant for crisis management. So far, systematic links between the policy makers at European level as well as other type of users and the European research activities providing operational features being relevant for crisis management are missing or, if existing at all, are only available in a fragmented way. A major challenge in European Disaster Management is therefore a “mapping” of operational features arising from the different research domains such as preparedness, prevention and response, detection and surveillance or protection and recovery with the requirements of users such as the above mentioned policy makers operating at the level of the European Commission. The Community of Users includes also other actors such as operational units, the general public or the industry. Main domains of crisis

management are the mastering of CBRN-E events, man-made as well natural disasters. In all three cases interoperability between stakeholders being active on strategic, tactical or operative level is an imperative pre-requirement for successful accomplishment of such events. Interoperability encompasses multiple aspects such as use of common taxonomies, application of systems being interoperable to each or the provision and sustenance of a common information space.

Trans-regional cooperation was established in regions with a common threat and culture, e.g. regional cooperation of the Baltic area, South-Eastern Europe and the Mediterranean. Similar to Austria, a lot of European countries have established Cooperation Agreements on mutual help in protection measures beyond borders. [19] The majority of countries covered by the ANVIL Report signed bilateral agreements on emergency and/or disaster assistance with nearly all of their neighbours and are frequently well embedded in multilateral agreements. Best practices of natural disaster prevention have been stimulated by INTERREG initiatives, launched by the Committee of the Regions and promote the establishment of protocols for cross-border cooperation. Thus should facilitate a rapid data exchange, united forecasting capabilities and coordinated mutual help in the case of emergencies.

Experiences of the Austrian Red Cross showed that communication challenges can be overcome by consulting sister organisation in the respective country. The reason why non-governmental organisations such as the International Federation of Red Cross and Red Crescent Societies (IFRC, 2007) have established Standard Operating Procedures (SOPs) lies in the fact, that legal framework is often missing. [19] Current asymmetries in the state of knowledge impede coordination processes amongst different relief organisations, which are related to heterogeneity of data pools about country-specific vulnerabilities to disasters. In cases where central data would be needed, e.g. data of federal agencies, access rights for non-governmental relief organisations are limited due to the principle of subsidiarity. In general, sharing personal data even during emergencies is subject to the data protection law, which restricts the forwarding of personal data. Flexibilities exist in the case of infectious diseases, where a special law can overrule general law.

6 CONCLUDING REMARKS

Our contribution has shown that a number of technical, operational and cultural standards have been developed to improve communication exchanged in disaster response. This somewhat leads to standard pluralism, where several standards can be invoked at once. At the same time, a desk research has shown that currently standards serve as an extension of domestic laws. Yet the use and integration of standards into national regulatory frameworks raise some questions. How to measure which standard is more worthwhile to consider? How to effectively integrate standards into domestic laws? What is the political mandate of groups that have developed a standard? Who would have a capacity to provide such a mandate? Is better to follow bottom up rather than top-down approach? Who is responsible for the implementation and enforcement of the standard? How to ensure that standards aim at enhancing interoperability of the systems rather than leading to fragmentation? What procedures should be put in place that would allow continuously upgrade the standard?

Regardless, where problems occur, a lack of interoperability in crisis and disasters might influence the performance of agencies concerned with managing disasters on strategic, tactical and operative levels. Harmonisation of procedures at higher levels that are affecting the work of practitioners in the field level seems to be needed. Especially, if national law is derogating from international law concerning the deployment of relief workers or in the case, if international procedures and domestic practices of managing disasters are not interlocking at all. This might be the case, if the structure of a state's administration does not fits with Standard Operating Procedures (SOPs) of international organisations, which provide relief personnel. Restrictions in exchanging information across organisational and/or national borders between different types of stakeholders were considered as serious hindrances for an efficient coordination of disaster management. Frequently a lack of legal and/or political provisions evoke, that Standard Operating Procedures were conceived as missing link between the legal/organisational framework of affected states and the deployment of international assistance. Indeed, peculiarities in managing disasters and the necessity of coordinated procedures to meet the requirements of international or cross-border disaster management need to find a joint

basis for collaboration across borders. A common understanding of coordination structures and decision making processes could be seen as a further step towards a comprehensive inter-agency and cross-border collaboration. Thereby national and/or organisational boundaries, which influence the efficiency of mutual assistance in disaster management procedures, should be taken into account. Efforts focusing on the improvement of planning activities as well as the field-level collaboration need to consider the whole range of multiple actors with its legal mandate, functions and the scope of their actions in disaster management. As a big challenge it should be taken into account, that framework conditions should be designed in a way to enable, and not to be a hindrance for practising solidarity in terms of mutual help and subsidiarity in terms of self-protection capacities.

REFERENCES

[1] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism.
[2] Communication, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22.11.2010 (COM (2010) 673 final).
[3] The abbreviation “EPISECC” stands for the European Commission funded project, titled “Establish Pan-European information space to Enhance seCurity of Citizens”, grant no. 607078. The EPISECC project was launched on the 1st June, 2014.
[4] B.S. Manoj, A. Hubenko Baker, “Communication Challenges in Emergency Response”.
[5] Special Eurobarometer 383 / Wave EB77.1 – TNS Opinion & Social; available at: http://ec.europa.eu/echo/files/eurobarometer/reports/CP.pdf.
[6] Communications of the ACM - Emergency response information systems: emerging trends and technologies, Volume 50 Issue 3, March 2007).]
[7] A. Boin, M. Ekengren, M. Rhinard, “Assisting overwhelmed states: the evolving use of the Civil Protection Mechanism”, The European Union as crisis manager (2013). p. 25.
[8] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01); TFEU.
[9] N. Bharosa, J. Lee, M. Janssen and H. R. Rao, “An activity theory analysis of boundary objects in cross-border information systems development for disaster management”, *Security Informatics,* pp. 1-17, 15 1 2012.
[10] B. Walle and M. Turoff, “Decision support for emergency situations,” *Information Systems and e-Business Management,* p. 295–316, 6 2008.
[11] A. Sagun, D. Bouchlaghem und C. J. Anumba, „A scenario-based study on information flow and collaboration patterns in disaster management.,“ *Disasters,* p. 214–38, 2 33 2009.
[12] H.-P. von Kirchbach, T. Popp und J. Schröder, „Bericht der Kommission der Sächsischen Staatsregierung zur Untersuchung der Flutkatastrophe 2013,“ Freistaat Sachsen, Dresden, Germany, 2013.
[13] Cabinet Office Civil Contingencies Secretariat, “Emergency Response and Recovery - Non statutory guidance accompanying the Civil Contingencies Act 2004,” London, 2013.
[14] IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries (New York, NY: 1990).
[15] ESENet – Emergency Services Europe Network (FP7 Grant 313013): http://www.esenet.org/
[16] ISO/TR 22351 Societal security – Emergency management – Message structure for exchange of informationhttp://www.isotc223.org/Published-Standards/Published-Standard-2131122/
[17] P. Quevauviller, (DG HOME), “Building up a Community of Users in the field of Disaster Risk and Crisis Management”, Brussels, Belgium, 2014.
[18] R. Bossong und H. Hegemann, „Synthesis report on comparison of civil security systems,“ in ANVIL - Analysis of Civil Security Systems in Europe, 2013.
[19] International Federation of Red Cross and Red Crescent Societies, Disaster response and contingency planning guide, Geneva, Switzerland, 2007.

COLLABORATION IN CRISIS MANAGEMENT – LEARNING FROM THE TRANSPORTATION DOMAIN

Christian Flachberger[1], Eduard Gringinger[2], Thomas Obritzhauser[3]

[1] christian.flachberger@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria
[2] eduard.gringinger@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria
[3] thomas.obritzhauser@frequentis.com
Frequentis AG, Innovationsstrasse 1, 1100 Vienna, Austria

Abstract

Cross organizational collaboration is a well-developed standard way of working within crisis management. However, the underlying information management tools today don't support integrated electronic information management in complex multi-organizational scenarios. This leads to a fragmentation of relevant information into pieces held by different stakeholders. Recently, the concept of the Common Information Space has been introduced as possible solution. This paper looks to the domain of Air Traffic Management where a similar problem was tackled by a concept called system wide information management. The paper starts with describing the operational context, the unresolved needs, and the derived requirements on possible solutions. Results and experiences from the Air Traffic Management domain are gathered and compared with current solution concepts from the public safety domain which are based on the idea of the Common Information Space. The paper concludes with learnings for the ongoing development in the public safety domain.

Keywords: crisis and disaster management, collaboration, information sharing, situation awareness, common information space, air traffic management

1 NEED FOR IMPROVEMENT OF COLLABORATION TOOLS

During the time-critical response phase within a crisis- or disaster management action, cross-organizational collaboration and the related information management today is still mostly based on face-to-face meetings, telephone calls, fax transmissions, email messages, paper charts, whiteboards, and proprietary electronic systems. We gathered this insight from our experience as supplier of control centre solutions for the public safety domain in various European member states[1]. As a consequence situation awareness and decision making is hampered by a fragmentation of relevant information into pieces held by different stakeholders. Within the highly collaborative scenarios of crisis management efforts this fragmentation causes uncertainty whether the information base for critical decisions is up-to-date, comprehensive and valid.

1.1 Operational Context

Decision making based on a comprehensive picture of the situation requires exchange, verification and integration of all the different pieces of information provided by the stakeholders with their organizational and cultural background [1]. At the same time a common understanding of the situation is also a basic pre-requisite for successful collaboration [2]. This chapter describes the stakeholders and the information involved.

[1] This was done within commercial projects in Norway, Germany and UK; but also within the European Research projects IDIRA [6], EPISECC [7], SEMNOTAM [16] and the SESAR programme [13]

1.1.1 Stakeholders

The stakeholders (cf. Fig. 1) are on the one hand organizations from the public safety domain where crisis management is part of their core business such as civil protection and first responders. On the other hand, also organizations play an important role whose core-business has per se nothing to do with crisis management (e.g. infrastructure operators). In case of a crisis they are required to contribute to the crisis management effort in addition to their own business continuity management [3], [2].

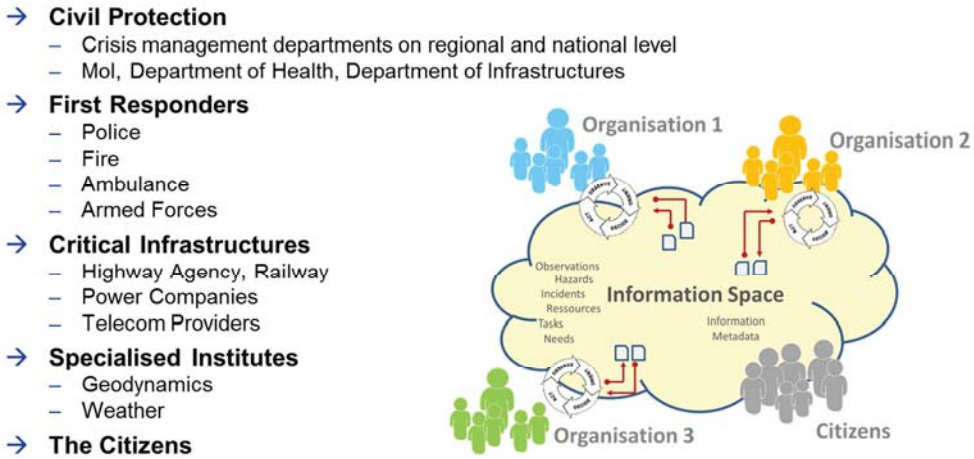


Fig. 1 Stakeholders of a Common Information Space (CIS) for crisis management

1.1.2 Information Involved

The information involved is generated within the four phases of the crisis management life-cycle (cf. Fig. 2). Without exchange and integration of these pieces of information the fragmentation leads to different views on the situation, different assessment of needs and priorities, and to an obstruction of the practical collaboration [4], [2] and [5].

Fig. 2 Phases of the crisis management life-cycle and information involved

1.2 Operational Requirements

Specific needs have been derived from user-group workshops especially within two European projects: IDIRA [6], EPISECC [7]. These needs where analysed from the perspective of their influence on the conceptual design of a possible solution, e.g. in form of a Common Information Space (CIS) [5] and are listed below:

1.2.1 Need for ad-hoc, closed, mission specific user-groups

End-users need to be able to define on-demand (i.e. in case of an event) mission specific user-groups for information sharing.

1.2.2 Need for Integration of information

Information from different sources may concern the same information object itself (e.g. information about the same single incident) or may concern the same class of objects (e.g. information about different incidents of the same type). There is a need to integrate these pieces of information into one homogenous data-set, which can be used for queries or aggregation. This seems to be trivial at the first glance but since there is no standardised taxonomy or ontology across organizations it is still a challenge today.

1.2.3 Need for Role- and Mission Specific views

There is a need for a user-defined, configurable filtering and prioritization of information in order to generate meaningful role- and mission specific pictures of the situation.

1.2.4 Need for Precision on Location, Time, Validity and Security

The quality of the information base is crucial for the trustworthiness, especially, when the user is not directly working with primary information, i.e. electronic information processing is applied beforehand. Additionally, information security is essential.

2 TECHNICAL REQUIREMENTS

2.1 Layers of Interoperability

As framework for structuring the requirements the “layers of interoperability” model presented by ESENET[2] (Fig. 3) is used. It describes layers of interoperability beginning with the lowest technical layer (physical interoperability) up to the highest organisational layer (interoperability of political objectives). This paper focuses on layer 2 to 4 since they are of most relevance for the design of a technical solution [8].

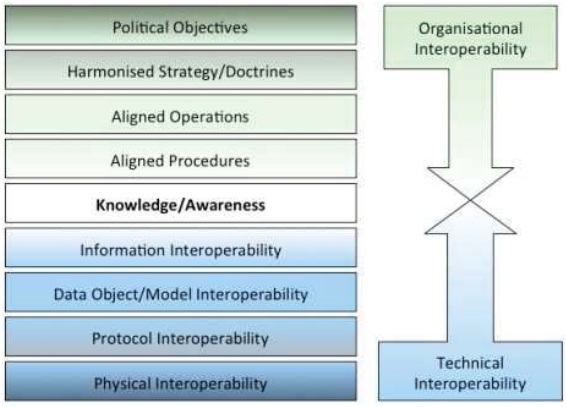


Fig. 3 Layers of interoperability according to ESENET.

2.2 Knowledge / Awareness Layer Requirements

Knowledge is seen as information which can be practically applied by a person within his or her specific context [9]. Turning information into knowledge often needs an informal sharing of views and ideas. Therefore, the basic requirement on the knowledge layer is to support this discussion process by providing a “*trading zone*” [4]. Pieces of information shared can – if required – be starting point for a discussion process.

2.3 Information Layer Requirements

Many organisations in the public safety domain are using their own, proprietary vocabulary for their communication. I.e. taxonomies and ontologies are very different and

[2] http://www.esenet.org/ Accessed 2015-06-11

it seems not likely that a common standard will be developed and adopted within a reasonable time. The basic requirement for the information interoperability layer is therefore to support a mapping between different, proprietary taxonomies [10]. At the same time existing ontologies (e.g. the tactical situation object TSO [11]) and best practises (e.g. the emergency relief items catalogue[3] of the IFRC) shall be considered.

2.4 Data Object / Model Layer Requirements

A number of well-known data exchange models is already available today. Relevant examples for domain specific models are the Emergency Data Exchange Language (EDXL)[4], including the Common Alerting Protocol (CAP)[5]; the U.S. National Information Exchange Model (NIEM)[6] or the Weather Exchange Information Model (WXXM)[7]. An example for a broadly used data model for geospatial information is the Geography Markup Language (GML)[8]. The basic requirement for the data object / model layer is to re-use these models and to provide interoperability including translation between specific models if required.

2.5 Protocol and Physical Layer Requirements

In order to fulfil the need for being able to build up ad-hoc, mission specific user-groups, the information distribution mechanisms must allow ad-hoc adding of additional partners. It must be possible to find services available within the information space (e.g. via a service registry). The specific situation of mission critical crisis and disaster relief actions requires off-line capabilities (i.e. local caching of information and automated re-synchronisation).

3 SOLUTION CONCEPTS

A number of projects within the public safety domain currently focus on solutions for a CIS. Therefore, it seems to be worthwhile looking into other domains with similar questions of collaboration. One of these domains is Air Traffic Management (ATM). Since airplanes are moving around the entire globe the necessity for developing standards and legal frameworks for information sharing has been there right from the beginning. This chapter gives an insight into solution concepts from both domains.

3.1 Solution Concepts from the Public Safety Domain

Within the public safety domain, the U.S. XChangeCore[9] programme and the ongoing European Research projects EPISECC [7], SecInCoRe[10], REDIRNET[11], SECTOR[12], IDIRA [6] and DRIVER[13] have been identified as relevant projects or initiatives, respectively. All these projects implement a Common Information Space (CIS). The CIS interconnects technical systems and applications of different organisations in order to support information sharing. The exchanged data needs to be converted since the different applications usually use owner-specific taxonomies, data formats, and protocols. In order to avoid the necessity of N-to-N conversions, the concepts are based on a set of standard protocols, data formats and taxonomies. This allows implementing N-to-1-to-N conversion models based on application specific adaptors which depend on the individual external application itself as shown in Fig. 4.

[3] http://procurement.ifrc.org/catalogue/ Accessed 2015-06-11
[4] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency Accessed 2015-06-11
[5] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html Accessed 2015-06-11
[6] www.niem.gov Accessed 2015-06-11
[7] http://www.wxxm.aero Accessed 2015-06-11
[8] http://www.opengeospatial.org/standards/gml Accessed 2015-06-11
[9] http://www.xchangecore.org/ Accessed 2015-06-11
[10] http://www.secincore.eu/ Accessed 2015-06-11
[11] http://www.redirnet.eu/ Accessed 2015-06-11
[12] http://www.fp7-sector.eu/ Accessed 2015-06-11
[13] http://driver-project.eu/ Accessed 2015-06-11

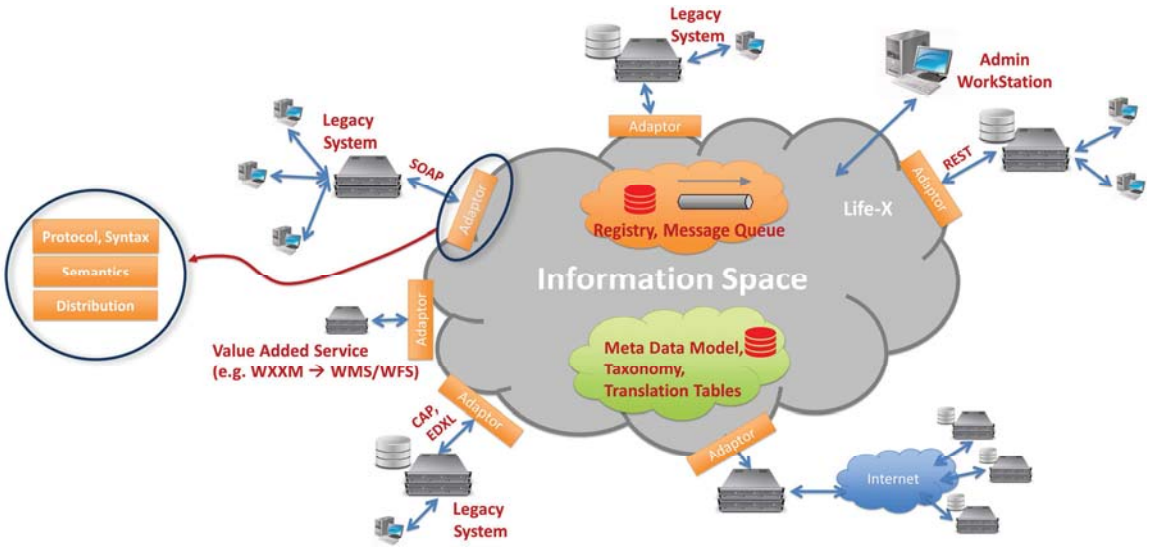


Fig. 4 Architecture of the Common Information Space (CIS)

The project C2-SENSE[14] additionally introduces profiles. Each profile defines with regard to a specific operational use which set of standards shall be used for communicating via the CIS. Referring to the knowledge/awareness layer, the project IDIRA [6] implemented a possibility to establish ad-hoc voice calls between a provider and a consumer of a certain piece of information using an application called IDIRA Webtalk. XChangeCore is based on a partially meshed network. XChangeCore servers allow clients to collaboratively assemble and share emergency management information using web services provided by their local XChangeCore server. Collaboration occurs between clients connected to one XChangeCore server transparently and between clients on different XChangeCore servers based on information sharing agreements. The Common Information Space is a data sharing platform but not a data repository. The ownership of the data stays with the applications. It doesn't provide any business logic. The validation, interpretation and processing of the transported data is part of the applications.

3.2 Solution Concepts from the Transportation Domain

Within the air traffic management domain, System Wide Information Management (SWIM) [12] including the ATM Information Reference Model (AIRM) [13], the Information Service Reference Model (ISRM) [14], and the SWIM Technical Infrastructure (SWIM-TI) [15] has been introduced. The concept of SWIM is a fundamental change of how information is managed along its full lifecycle, involving stakeholders from across the whole European ATM network. The list of stakeholders is divided into two main groups, civil and military. Under these you will find air navigation service providers, airport operators, airspace users, network managers and industry partners. SWIM is SESAR's[15] most important enabler for assuring that the right information will be available with a certain level of quality for a specific operation at the time needed [12]. It covers all ATM information, including aeronautical, flight, aerodrome, meteorological, air traffic flow, and surveillance. SWIM consists of standards, infrastructure, and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services.

The AIRM is used as a common reference and consists of an information- and logical data model capturing various domains [13]. The AIRM represents civil, military and

[14] http://c2-sense.eu/ Accessed 2015-06-11

[15] Single European Sky ATM Research, http://www.sesarju.eu/ Accessed 2015-06-12

hybrid information constructs relevant to ATM. The model ensures semantic interoperability within ATM and maybe will be used also on International Civil Aviation Organization (ICAO) level as ATM information standard worldwide. The ISRM describes information services needed by operational processes or operational services to fulfil their information needs [14]. The idea is to have a registry available from which the specific operational people can choose from. SWIM-TI is the technical enabler for the SWIM concept realization [15]. The main goal is to increase the common situational awareness by improving the ability to deliver the right information to the right people at the right time. SWIM-TI contributes to the services' solution aspects providing means supporting an effective and secure ATM-specific services provisioning and consumption among SWIM Enabled ATM systems. The SWIM-TI is a set of software components distributed over a network infrastructure providing functions and enabling collaboration among ATM systems. There are different profiles for different purposes available. With the commission implementing regulation No 716/2014[16] of the European Union, the legal aspects are defined for supporting the implementation of the European ATM Master Plan including SWIM in the context of the common pilot project.

4 COMPARISION AND DISCUSSION

Even though it looks as if there are nearly no overlaps between the Public Safety and Air Traffic Management Domain, the concepts presented are more alike than expected. This chapter compares and discusses the various concepts presented in section 3.1 and 3.2 in regards of similar approaches and standards used. Fig. 5 identifies the different interoperability layers of the discussed solution concepts. The semantic, syntactic, and technology interoperability layer can be found in the presented SWIM components as well (cf. section 3.2). The following sections handle those layers in detail.

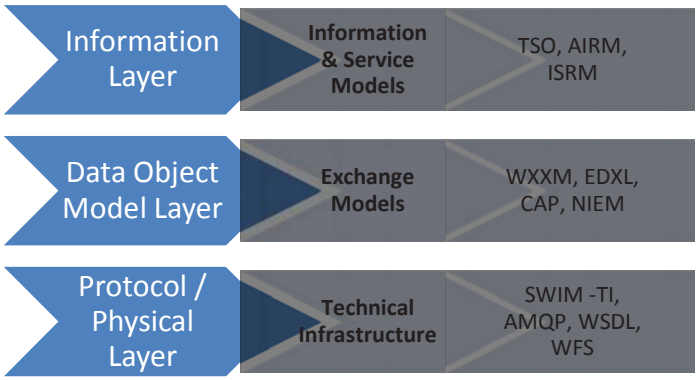


Fig. 5 Mapping the Interoperability Layers to Solution Concepts

4.1 Comparison of the Information Layer

All presented solution concepts contain a semantic layer which represents the operational knowledge of a specific domain. Within the transportation domain this layer was identified as one of the major fields of research for enhancing future interoperability and harmonization by introducing the information model AIRM and service model ISRM. In addition to the definition of business terms, also harmonized definitions for generic concepts such as geometries, temporality and identifiers are modelled. Future research programs like SESAR 2020 will further explore the semantic layer. Although a baseline has been found, future work on a common semantic reference model will be necessary within the public transport domain. In the public safety domain, this baseline has not yet been found and is currently within the scope of a number of research projects.

[16] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0716&from=EN Accessed 2015-06-11

4.2 Comparison of the Data Object / Model Layer

For each domain, a common information reference model needs to be aligned with the used exchange models and vice versa. Existing exchange models (e.g. WXXM, EDXL, CAP, and NIEM) are already used today to improve the digital communication between different stakeholders. This defines the Data Object / Model Layer. This proliferation of formats obviously increases the effort used in building a knowledge framework – inconsistent use of business terms and business rules would need to be resolved.

4.3 Comparison of the Protocol and Physical Layer

The architectural and messaging patterns described in the solution concepts are very similar (SOAP, Web Services, etc.). Each technical infrastructure uses adaptors (access points) and provides capabilities and functionalities that enable those adaptors and external service consumers/producers to participate in operation of services and information exchange. Adaptor components therefore specify service authentication and authorisation, data conversion, and other additional features. In the transportation domain different profiles support specific operational needs (e.g. near real-time transmission). In the public safety domain the solution of EPISECC and DRIVER is similar to XChangeCore except the network structure. The services are connected via adaptors to the CIS which allows the network configuration being independent from the connected application/services. C2Sense introduces a profile concept similar to the transportation domain.

5 CONCLUSION & OUTLOOK

What can we learn from the air traffic management domain for crisis management? One lessons learnt is that the challenges which the crisis management is currently facing can be mastered. Secondly, it is obvious, that the experiences cannot simply be transferred directly from the global air traffic management domain to the regionally fragmented, complex and highly dynamic crisis management domain. Taking this into account, the following learnings are proposed to be considered: A transformation from a product-centric paradigm to an information-centric paradigm is needed. The development of an information reference model (semantic layer) is necessary. Information sharing doctrines and procedures need to be introduced. Early development of applications providing a possibility to experience the user-benefits in reality will facilitate the transition. All of that should follow an iterative approach starting with a simple baseline. Existing data models should be re-used for finding the baseline where appropriate. Possible candidates are the relief items catalogue of the IFRC, the Tactical Situation Object or the Weather Information Exchange Model, but many others can be identified.

Within the European Union different strands of activity are driving the transformation forward:

Standardisation: The discourse about a concept of networked crisis and disaster management is being pushed forward by policy makers of DG Enterprise. A good example is the mandate 487[17] of the European Commission.

Focused R&D: Different research projects mentioned in this paper will contribute further by developing and demonstrating practical solutions: EPISECC, SecInCoRe, REDIRNET, SECTOR, IDIRA, and DRIVER.

Stakeholder involvement and awareness raising: Among other initiatives, the project ESENET conducts a number of workshops in different European member states and provides a structured possibility for online discussions.

[17] http://www.etsi.org/images/files/ECMandates/m487.pdf Accessed 2015-06-10

ACKNOWLEDGEMENTS

IDIRA, EPISECC, DRIVER, ESENET and SESAR are funded by the European Commission. SemNOTAM is funded by the Austrian Research Promotion Agency (FFG).

REFERENCES

[1] W. Treurniet and et al., "Governance of occasional multi-sector networks," in *Proceedings of the 11th International ISCRAM Conference*, University Park, Pennsylvania, USA, 2014, pp. 118 - 122.

[2] J. Morentz, "Unified Incident Command and Decision Support (UICDS): A Department of Homeland Security Initiative in Information Sharing," in *Conference on Technologies for Homeland Security*, Waltham, IEEE, 2008, pp. 321 - 326.

[3] V. Atluri and et al., "UICDS-based information sharing among emergency response application systems," in *Proceedings of the 12th Annual International Digital Government Research Conference*, New York, ACM, 2011, pp. 331-332.

[4] K. Boersma and et al., "Negotiating the 'Trading Zone'. Creating a Shared Information Infrastructure in the Dutch Public Safety Sector," *Journal of Homeland Security and Emergency Management,* vol. 9, no. 2, 2012.

[5] N. Selvaraj and B. Fields, "Developing a Framework of Common Information Space (CIS): Grounded Theory Analysis of Airport CIS," in *Collaboration and Technology*, Berlin Heidelberg, Springer, 2010, pp. 281-296.

[6] Fraunhofer, "IDIRA Interoperability of data and procedures in large-scale multinational disaster response actions - Final Report," 13 05 2015. [Online]. Available: http://www.idira.eu/. [Accessed 08 06 2015].

[7] e. a. Huebner, "Towards a Pan-European Information Space," in *Proceedings of the ISCRAM 2015 Conference - Kristiansand, May 24-27*, Kristiansand, Palen, Büscher, Comes & Hughes, eds., 2015.

[8] H. Kubicek and et al., "Layers of Interoperability," in *Organizational Interoperability in E-Government*, Berlin Heidelberg, Springer, 2011, pp. 85-96.

[9] J. Hey, "The data, information, knowledge, wisdom chain: the metaphorical link," *Intergovernmental Oceanographic Commission,* 2004.

[10] H. C. Siddharth Kaza, "Evaluating ontology mapping techniques: An experiment in public safety information sharing," *Decision Support Systems,* vol. 45, no. 4, 2008.

[11] D. R. Fedra Henriques, "OASIS Tactical Situation Object: a route to interoperability," in *SIGDOC '08 Proceedings of the 26th annual ACM international conference on Design of communication*, New York, ACM, 2008, pp. 269-270.

[12] P. Single European Sky ATM Research (SESAR) Programme, "SWIM conops, edition 00.04.05," SESAR Joint Undertaking, Brussels, 2014.

[13] P. Single European Sky ATM Research (SESAR) Programme, "AIRM Primer, edition 03.03.01," Sesar Joint Undertaking, Brussels, 2015.

[14] P. Single European Sky ATM Research (SESAR) Programme, "ISRM Primer, edition 00.05.00," SESAR Joint Undertaking, Brussels, 2014.

[15] P. Single European Sky ATM Research (SESAR) Programme, "SWIM TI definition, edition 00.02.00," SESAR Joint Undertaking, Brussels, 2014.

[16] F. Burgstaller, E. Gringinger, D. Steiner, M. Schrefl, S. Wilson and S. v. d. Stricht, "AIRM-based, Fine-grained Semantic Filtering of Notices to Airmen," in *Integrated Communications, Navigation and Surveillance Conference*, Washington, 2015.

ANALYSING ORGANISATIONAL, LEGAL, AND POLITICAL FRAMEWORK CONDITIONS TO SUPPORT THE IMPLEMENTATION OF NEW CRISIS MANAGEMENT SOLUTIONS

Maike Vollmer[1], Todor Tagarev[2] and Isabelle Frech[3]

[1] *maike.vollmer@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT, Dept Meta-Analyses and Planning Support, Appelsgarten 2, 53879 Euskirchen (Germany)

[2] *tagarev@gmail.com*
"IT for Security" Department & Centre for Security and Defence Management IICT - Bulgarian Academy of Sciences, Acad. G. Bonchev Str., Bl. 25-A, Sofia 1113 (Bulgaria)

[3] *isabelle.frech@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT, Dept Meta-Analyses and Planning Support, Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

New solutions, technical and non-technical, provide strong opportunities to improve crisis management, while successful operationalisation of new solutions essentially depends on framework conditions such as organisational, legal, and political aspects in the respective area. Within the FP7-project DRIVER, these framework conditions are addressed in a dedicated part. Next to the objective of receiving most realistic scenarios for the testing of new Crisis Management solutions, the analysis of framework conditions aims at developing evidence-based recommendations for different types of stakeholders. Intensive surveys of the European Member States, selected third countries, the United Nations and the European Union have been completed. In a next step, more pertinent organisational, legal, and political framework conditions regarding the applicability of DRIVER solutions will be focused.

Keywords: Crisis management; innovation; operationalisation; resilience; policy; legislation; organisation.

1 INTRODUCTION

Natural and man-made hazards, their variances and broad range of possible impacts on society, critical infrastructures, environment or economy, perpetually induce new challenges for crisis management. These challenges must be met by constant improvements and adaptations of the crisis management process, to ideally be able to cope with complex disasters in the best possible way at any time. New technical and non-technical solutions play a crucial role in this regard, providing strong opportunities for improving crisis management capabilities and thus societal resilience.

Whether new solutions are implemented in crisis management, if they actually strengthen resilience, as opposed to rather triggering negative secondary impacts or providing no real added-value, strongly depends on conditions such as relevant organisational, legal, and political framework conditions.

1.1 The EU-FP7 project DRIVER

The EU-FP7 project DRIVER (*"**Driv**ing Innovation in Crisis Management for **E**uropean **R**esilience",* running May 2014 – October 2018, with a budget of approx. € 45 million)

implements the Aftermath Crisis Management System-of-Systems Demonstration Programme funded under the 7th Framework Programme by the European Commission.

DRIVER aims at three main dimensions:

- The development of a pan-European test-bed, an assembly of virtually connected, distributed operational or training facilities dedicated to experimentation plus test-bed tools (modelling and simulation, data recording, data analysis), methods (experiment design, campaign planning, analysis, evaluation), people, and ideas enabling the testing and iterative refinement of new crisis management solutions.
- The development of a DRIVER Portfolio of Emerging Solutions that improves Crisis Management at Member State and EU level (solutions for civil resilience, for professional response, and methods or infrastructure for individual and organisational learning)
- The development of a more shared understanding of crisis management across Europe including all stakeholders in crisis management who are concerned by societal and technological innovation in crisis management.[1]

The DRIVER consortium consists of 36 organisations from 13 EU Member States and two associated countries. The project is coordinated by European IT services leader Atos with technical and scientific support from the Swedish Defence Research Agency (FOI) and the Fraunhofer Institute for Technological Trend Analysis (INT).

1.2 Part of DRIVER: Analysing organisational, legal, and political framework conditions

DRIVER follows an approach of campaigns of experiments, providing an iterative way towards operationalisation of innovative solutions in crisis management. For these experiments, an analysis of organisational, legal, and political framework conditions supports the development of different scenarios. Next to the objective of receiving most realistic scenarios, the analysis of framework conditions aims at developing respective evidence-based recommendations for different types of stakeholders based on the results of the experimental campaigns.

In accordance with the overall DRIVER concept, instead of focusing on specific conclusions only relevant for specific solutions, findings especially target methodological approaches for future actions to foster innovation processes.

2 METHODOLOGY

As a first step, a “high-level” analysis has been conducted, providing general overviews on crisis management organisational, legal, and political framework conditions in the EU Member States, selected third countries, and on EU- and UN-level. All studies followed the same template, ensuring comparability of the gathered information. An additional survey examined the evolution of civil-military coordination in crisis management.

The work has mainly been done by desk top research, based on publicly available information. In addition, information gaps have been filled by conducting interviews with relevant stakeholders [1, 2].

Following the DRIVER working definition of a crisis as “a major disaster (natural or man-made) that requires coordination between or assistance from other countries, i.e.

[1] See project website: http://driver-project.eu/

that exceeds the crisis management capacity of one nation or affects more than one country," excluding e.g. a "financial crisis" or war-like crises, bi- and multilateral cooperative linkages between nations have been focussed.

As the experiments in DRIVER are getting more and more complex, so does the need for more detailed information on framework conditions. Thus, in a second step, more pertinent framework topics will be identified, in collaboration with the project partners working on the experiments and their design. A respective feedback loop has already started. The confirmation of framework topics will be followed by a selection of countries to be analysed, and the actual analysis of the topics in these countries (plus EU- and UN-level).

In addition, assessments of DRIVER experiments are expected to reveal additional requirements of organisational, legal, and political framework conditions, which will, together with the analysis described above, feed into evidence-based recommendations with regard to the implementation of DRIVER solutions under different conditions.

Adaptations to enhance the compatibility of solutions with framework conditions can be made from different angles. Respectively, recommendations will be developed for different target groups – incident commanders, decision makers, policy makers, and legislators.

3 RESULTS

The "high-level" studies, conducted for EU Member States, selected third countries, and on EU- and UN-level, cover topics on *Organisation* (e.g. chains of command, cross-border operational cooperation), *Procedures* (e.g. Standing Operating Procedures, national crisis management plans), and *Capabilities* (e.g. human/ materiel resources). They further cover *Policy* (e.g. risk assessments, analytical support and R&D, financing, policy review cycle, approaches to resilience, information sharing and data protection) and *Legislation* (e.g. general crisis/ emergency/ disaster law, emergency rule, specific regional and local legal arrangements, regulations on the involvement of volunteers, international engagements of first responders). They also provide data on CM organisations' *procurement processes* to support the exploitation of DRIVER emerging solutions and the DRIVER test-bed. Besides general information, also first specific information needs for DRIVER solutions have been considered in the analysis [1, 2].

As already stated, innovation processes in Crisis Management, i.e. a successful operationalisation of new Crisis Management solutions, strongly depend on the ability to be integrated in the respective framework conditions.

Those conditions can considerably differ between different nations, as shown in some examples below.

3.1 Policy and Strategy focus

Comprehensive crisis management includes measures for prevention and risk reduction, preparedness and protection of critical assets, maintaining capabilities and readiness to react to emerging crises quickly and manage their consequences, as well as measures to enhance resilience.

The surveyed countries recognise the need to comprehensively address crisis management requirements. For example, the aspiring EU member Albania recently introduced a comprehensive approach towards disaster risk reduction and management, including prevention, preparedness, response and recovery [3].

Some of the surveyed countries clearly emphasise the importance of one or another phase of crisis management. Countries like Albania, Belgium and Croatia emphasise response tasks and capabilities [3, 4, 5]. The strategy focus in Finland, on the other hand, is on preparedness and prevention rather than on response and recovery as a result of its low risk profile in terms of natural and man-made-disasters [6]. The policy of Austria puts a premium on preparedness issues like education and training of key response personnel, the promotion of new response technologies like decision support systems, simulation tools and also on an improved organizational framework for cooperation and coordination in the response phase [7].

While in some countries the concept of resilience is virtually unknown (and the term does not even translate easily in the respective language, e.g. Albania, Bulgaria), other countries strongly emphasise the importance of increased resilience of communities and societies. Such examples are provided by the Czech Republic, the United Kingdom, and other among the surveyed countries [3, 8, 9, 10].

3.2 Centralised vs distributed crisis management

Practically all European countries implement distributed systems for crisis management. In practice, however, there are significant differences in views – and respective policies and budget allocation – on the role of the state versus the role of the local preparedness and response. Bulgaria, for example, still heavily relies on the centralised development of capabilities and financing from the state budget. The crisis management approach of Denmark, taken as an example to the contrary, assumes the local level to be better placed to tackle local crisis situations, than the national level, and relies heavily on the contribution of private organisations, volunteers and NGOs in Danish crisis management [8, 11].

3.3 Volunteer involvement

The involvement of volunteers in crisis management strongly differs in various EU Member States, which has already been shown in previous studies [12, 13]: In general, volunteering is strongly influenced by the history, politics and culture of a community and a country. There are countries with longstanding traditions and well developed voluntary sectors (e.g. Ireland, the Netherlands, UK) as well as countries with less developed voluntary sectors (e.g. Bulgaria, Greece, Romania). Also, volunteering has different weights on the political agenda (e.g. high in Austria, Germany; rather low in Bulgaria, Czech Republic), which lead to differences also in the level of volunteering. Moreover the general treatment, organisation and support of affiliated volunteers and voluntary agencies differ from country to country.

The studies at hand e.g. confirm (referring to [14]) that the “German civil security system officially and strongly relies on non-profit relief organisations and their volunteer staff. […] While most management tasks and everyday emergency services are carried out by professional staff, volunteers remain essential for more exceptional crisis management situations.” [14, 15]. Also the country study Austria confirms that "One characteristic of the Austrian Crisis and Disaster Management is the strong involvement of voluntary organizations which enable an easy access to a huge amount of human resources. Due to the fact, that there is no single organisation in Austria, which will be mainly responsible for the response to disasters, related duties will be organized by voluntary organisations” [7]. In contrast, in Bulgaria “the legal provisions for the use of volunteers and volunteer formations are fairly recent. In the short period of about three years in which they are in force, 162 formations were created, and FSCP (Fire Safety and Civil Protection) provides public access to the respective registry” [8].

3.4 Post-disaster assessment and Lessons Learned systems

First evaluations of the country surveys let assume that nearly every organization involved in Crisis Management reports and analyses the measures that have been taken during a disaster as well as during exercises and trainings, in many cases including international/ cross border experiences. Nevertheless, only few additional centralized (national) or inter-organisational Lessons Learned systems including central data bases of respective information and/or a central organization exist like in Ireland [16] or Finland, where investigation reports of all major accidents, regardless their nature, are prepared and include recommendations for improving systems, policies and processes [17, 6]. A major problem of these review processes is in many cases the lack of implementation of its findings. As a result, findings of review processes could often rather be seen as lessons identified than lessons learned, which hampers the innovation process.

4 OUTLOOK: WORK IN PROGRESS

The next (update) phase will focus on pertinent issues regarding the applicability of DRIVER solutions. In a two-way process, information with the teams designing, conducting, and analysing the results of DRIVER experiments will be exchanged. This exchange is planned to be organised along questions, such as:

1. How each proposed and demonstrated solution adds value to the European capacity to manage crises? Potential contributions may range from filling in an identified capability gap, to a more robust crisis management (i.e. increases of effectiveness), to increasing the efficiency of preparedness and response.
2. To what extent the solution could be adapted to framework conditions (i.e. legislation, procedures, organization, existing capabilities, and policy), that differ from the ones in which the experiment took place?
3. What are requirements in the framework conditions (which might differ among countries) that are necessary in order to implement the solution?
4. What additional contextual information is needed to better tailor the solution and design future experiments?

The expectation is that such rigorous and structured exchange, complemented by additional surveys and analysis, will provide a sound foundation for evidence-based recommendations to policy-makers and legislators, as well as to incident commanders, and other decision makers at the operational and tactical levels of crisis management.

From current status, three groups of recommendations are anticipated, addressing respectively the capacity for professional response; strengthening the involvement of societal actors and resilience, and enhancing the capacity to innovate and adapt crisis management policies to evolving risks and societal expectations, with each group covering four thematic issues.

4.1 Professional response

The professional response to crisis management will benefit significantly by enhanced situational awareness, efficient coordination, command and control, streamlined information management, and enhanced logistics.

In terms of awareness, DRIVER solutions will facilitate situational assessment and sense-making, with focus on damage and needs assessment, prediction of crisis evolution and raising alerts, and continuous risk mapping. Further, situation assessment will be complemented by information from airborne sensors, with the requisite mission planning for remotely piloted aerial systems (RPAS) and modelling and optimization in traffic management.

Recommendations on Coordination, Command and Control will focus on multinational/ cross-border, multiagency and, in particular, civil-military coordination. The supporting analysis, including analysis of results of experimentation, will cover the issues of resource allocation and tasking, information exchange and interoperability.

The focus in the examination of information management is on reporting lines for and exchange of operational situational information, elaboration of a common operational picture (COP), interoperability, crowd sourcing and sending information to the public.

In terms of logistics, the main interest is on modelling logistics processes in crisis management, optimization of transportation means, and cooperation with civil society logistics' stakeholders.

4.2 Resilience

Society can turn into an effective actor in crisis management and disaster response through advanced volunteer management, enhanced societal and community resilience, effective crisis communication, and timely and professional psycho-social support.

Recommendations in regard to volunteer management will focus on volunteer registration databases, ad hoc management of spontaneous volunteers in the field, and crowd tasking.

Societal and community resilience will be addressed by measuring community resilience and raising awareness on local levels, assessment of the resilience of local government and definition of respective action plans, organisation and mobilization of individuals and communities.

The analysis of crisis communication will focus on crisis resilience communication, measuring the impact of messages to the public and the elaboration of key messages to the public.

The focus in providing psycho-social support will be on training, in particular basic training for psychosocial first aid.

4.3 Innovation capacity

The capacity to innovate and adapt to changing circumstances is contingent on the rigour and professionalism of education and training, the capacity to identify and incorporate good practice, and the agility of crisis management organisations.

Recommendations related to education will focus on continuous learning, multinational and multiagency education, as well as the shared understanding of required crisis management competences.

Advances in training will emphasise multi-national and multi-agency training, serious gaming, and training of volunteers, as well as context and dilemma training and the development of educational packages for trainers.

The identification of good practice requires rigorous evaluation and drawing lessons from field experience, exercises, experiments, and demonstrations. Focus is on a lessons learned framework for cooperation, coordination and collaboration across borders, sectors and organisations.

The EU-wide capacity for innovation depends on organizational agility and adaptiveness that include, *inter alia*, continuous mapping of requirements to available capabilities and maintaining a European crisis management architecture.

5 CONCLUSION

Successful innovation processes in Crisis Management depend on various factors. One of the major issues in the implementation of new Crisis Management solutions, besides being thoroughly tested and societal as well as ethical acceptable, is their compatibility to existing framework conditions such as relevant organisational, legal, and political circumstances.

The FP7-project DRIVER faces these challenges to foster innovation in European Crisis Management by building a sustainable pan-european test-bed, and elaborating a Portfolio of emerging solutions.

To facilitate the later implementation of these emerging solutions, the existing Crisis Management organisational, procedural, legal, and political framework conditions are analysed respectively. An intensive survey of the European Member States, selected third countries, the UN and the EU as well as a study on the evolution of civil-military coordination in crisis management have already been completed. First examples of policy and strategy focus, centralised vs distributed crisis management, volunteer management, and post-disaster assessment have demonstrated differences between countries with respect to framework conditions, which have strong influence on a successful implementation of crisis management solutions.

As the experiments in DRIVER are getting more and more complex, so does the need for more detailed information on framework conditions. The results of these more realistic experiments will feed into the formulation of evidence-based recommendations for different target groups – incident commanders, decision makers, policy makers, and legislators. While not expecting to derive only clear and exclusive recommendations for action, pros and cons/ risks and opportunities for different alternatives of action will be elaborated and linked to different local backgrounds/ framework conditions, considering that enhanced adaption to framework conditions can be supported from both sides – from the solution as well as from the framework itself.

REFERENCES

[1] Frech, I.; Vollmer, M.; Tagarev, T. et al. (2014). FP7 project DRIVER - D82.11 - CM organisations & capabilities report.

[2] Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). *FP7 project DRIVER - D83.11 - CM policy & legislation report.*

[3] Tzvetkov, G.; Spassov, P.; Petkov, V.; Tagarev, T. (2014). *Albania. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[4] Birkman, L.; de Swart, Linette (2014). *Belgium. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[5] Jager, B. (2014). *Croatia. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[6] Frech, I.; Vollmer, M. (2014). *Finland. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[7] Jager, B.; Neubauer, G. (2014). *Austria. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[8] Tagarev, T.; Ivanova, P.; Ivanova, N. (2014). *Bulgaria. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[9] Eichner, F.; Jager, B. (2014). *Czech Republic. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[10] Hayes B., (2014). *United Kingdom. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[11] Birkman, L.; de Swart, Linette (2014). *Denmark. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[12] GHK (2010); Educational, Audio-visual & Culture Executive Agency (EAC-EA), Directorate General Education and Culture (DG EAC). *Volunteering in the European Union.*

[13] Stolk, D.; Beerens, R.; de Groeve, T.; Hap, B.; Kudrlova, M.; Kyriazanos, D.; Langinvainio, M.; van der Lee, M.; Missoweit, M.; Pastuszka, H.-M.; Pienemann, R.; van Rijk, R.; Segou, O.; Vollmer, M. (2012). *ACRIMAS – D5.1 Approaches and Solutions.* Available at http://www.acrimas.eu/ (10/06/15).

[14] Hegemann, H.; Bossong, R. (2013): Analysis of Civil Security Systems in Europe – ANVIL. Country Study: Germany.

[15] Vollmer, M.; Frech, I. (2014). *Germany. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[16] Comer M.; MacDonagh P.; Mackin M., (2014). *Ireland. Capabilities, Organisations, Policies, and Legislation (COPL) in crisis management and disaster response.* In: Tagarev, T.; Petkov, V.; Frech, I.; Vollmer, M. et al. (2014). FP7 project DRIVER - D83.11 - CM policy & legislation report.

[17] UNISDR, EC, OECD. Building resilience to disasters: Assessing the implementation of the Hyogo Framework for Action (2005-2015): *Peer review report Finland (2014)*

Acknowledgements

The research leading to these results has received funding from the European Community's 7th Framework Programme (FP7/2007-2013) under Grant Agreement n°607798. We thank the DRIVER project partners contributing to the described work. Only the authors' views are reflected, the Commission and the Project are not liable for any use that may be made of the information contained therein.

RESOLVING THE PRIVACY AND SECURITY TRADE-OFF – CONTRIBUTIONS FROM PARTICIPATORY INVOLVEMENT OF CITIZENS

Johann Čas
Jaro Krieger-Lamina

jcas@oeaw.ac.at
jaro.krieger-lamina@oeaw.ac.at
Austrian Academy of Sciences, Institute of Technology Assessment
Strohgasse 45/5, 1030 Vienna, Austria

Abstract

The alleged trade-off between privacy and security largely dominates security policy-making and the development and implementation of surveillance orientated security technologies. Accordingly, infringements of privacy are seen as an acceptable or even necessary cost of enhanced security, constituting a perception that reinforces the self-fulfilling prophecy character of the trade-off approach. The SurPRISE[1] project challenged this approach from different perspectives, attributing a core role to the attitudes and perceptions of citizens within its research activities. To this end, SurPRISE conducted in nine countries Citizen Summits and Citizen Meetings, involving about 2000 participants in total. This paper will focus on the policy relevant project results, comprising factors and criteria relevant for the evaluation of security technologies and recommendations for acceptable security measures and technologies. They synthesize theoretical models and considerations with empirical research and expert opinions with suggestions and recommendations provided by the participating citizens.

Keywords: Privacy, surveillance, security, technology assessment, participation of citizens.

1 INTRODUCTION

The objective of this paper is to summarise the policy relevant results of the SurPRISE project. They entail recommendations for security measures and technologies that respect human rights and European values and of factors and criteria influencing the acceptability of surveillance oriented security technologies (SOSTs).

One of the core aims of SurPRISE was to put into question the trade-off approach between privacy and security which largely dominates security policy-making and the development and implementation of surveillance orientated security technologies. SurPRISE challenged this approach from different perspectives: from a theoretical one, which was subsequently empirically tested in large-scale participatory events and from a practical one, investigating technical, regulatory and societal options to eliminate privacy and human rights infringements caused by surveillance technologies. SurPRISE applied a participatory approach, involving 2000 European citizens in the discourse of these issues in informed debates and asking them to develop their own suggestions and recommendations on how to maintain or increase security. For this participatory technology assessment an innovative method how to involve citizens in future decision making on security measures was developed and tested.

The next chapter outlines the two types of citizen involvement activities conducted by SurPRISE, Citizen Summits and Citizen Meetings. Chapter 3 presents 16 SurPRISE

[1] SurPRISE – "Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe" is a FP7 Security research project; it has received funding from the European Union under grant agreement No. 285492.

recommendations, one of the key outputs of the project. The fourth chapter summarises our empirical research on factors and criteria relevant for the acceptance and acceptability of SOSTs. Chapter 5 concludes this brief description of SurPRISE methods and results.

2 CITIZEN PARTICIPATION IN SURPRISE

The increasing role and use of SOSTs for a variety of purposes is a matter of societal concern, which is evident in a number of public discourses. Although citizens are directly affected by the security and surveillance measures employed in their countries and across Europe, their views and opinions on these issues are widely unknown. To narrow this gap, the SurPRISE project gave about 2000 residents of nine European countries the unique opportunity to express and discuss their perceptions regarding security technologies and their implications at twelve citizen summits and five citizen meetings. The summits [1] were organised in nine different countries in the first half of 2014 (in alphabetical order): Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom. The events were full-day public meetings where citizens gathered to have face-to-face discussions about surveillance-orientated security technologies. In addition to the citizen summits, in five countries[2] "Small-Scale Citizen Meetings" were arranged in summer 2014 with a total of about 200 participants.

2.1 The Citizen Summits

The SurPRISE Citizen Summit method is an innovative technology assessment exercise that gathers both qualitative and quantitative data on the basis of a precise and thorough research design. This method ensures that participants[3] not only have a chance to express preferences among a set of predetermined options, they also have an opportunity to voice their own views, ideas, knowledge and proposals during table discussion rounds. The SurPRISE citizen summits provided two types of outcome: (1) a deep scientific understanding of the rationale behind rejection or acceptance of SOSTs; and (2) recommendations for policy makers and stakeholders involved in decisions on, and the provision of, security related services and technologies, by providing guidance on how to increase the appropriateness and effectiveness of security measures embedded in complex social realities while respecting fundamental rights.

The summits featured the analysis of three different SOSTs (Smart CCTV, Deep Packet Inspection - DPI, and Smartphone Location Tracking - SLT). The use of specific SOSTs served two purposes: providing concrete examples for the discussions, as well as investigating the interrelations between perceived effectiveness and intrusiveness of SOSTs, and related concerns. Sets of pre-defined questions and statements clustered around different topics were complemented by discussion rounds relating to each thematic block.

Participants were seated at tables in groups of six to eight individuals, and each table discussion was facilitated by a moderator. The summits comprised alternating quantitative and qualitative phases. The surveys were linked to an electronic polling system that allowed participants to immediately answer the questions via keypads, and the results were presented for each individual question right after the polling. Prior to attending the summit, participants received an information brochure. At the event, before the discussion of individual SOSTs, movie clips were presented to the audience. The clips provided additional information to that contained in the brochures, and were designed to stimulate recall and

[2] Denmark, Hungary, Italy, Norway and Spain

[3] The recruitment for the SurPRISE Citizen Summits aimed at getting groups of citizens respectively residents who are, on the one hand, not professionals in the area of surveillance, privacy and security, and that, on the other hand, reflect the national demographics regarding age, gender, geographical zone (rural, urban and metropolitan), educational level, occupation and minorities.

discussion. The mix of written information (the brochure) and more thought-provoking visual information (the film clips) helped equalize participants' knowledge, thus facilitating discussions on relatively equal footing.

In total, three discussion rounds were conducted per summit. One round was devoted to each of the two SOSTs allocated to the different countries, focusing on the perceived benefits and risks in relation to the particular form of surveillance and with the objective of gaining more insights into the participant's views and reasoning. The purpose of the third and final discussion round served for participants to develop suggestions and recommendations targeted at policy makers at the national as well as the European level.

2.2 The Small-Scale Citizen Meetings

The main objectives of the deliberative research undertaken at the small-scale citizen meetings were to supplement the results of the large-scale citizen summits and to test the SurPRISE Decision Support System[4] (DSS). At the Citizen Meetings the societal context of two more SOSTs and further factors and criteria influencing trust and citizens' concerns about security challenges were investigated.

Besides the three technologies of Deep Packet Inspection (DPI), Smart CCTV and Smartphone Location Tracking that were also discussed during the large-scale citizen summits, two additional technologies were included in the assessment process: drones and biometrics. The 3-hour Citizen Meetings were preceded by a short introductory plenary session and consisted of two discussion rounds conducted in small groups:

3 THE SURPRISE RECOMMENDATIONS

The generation of the recommendations was based on several steps, involving a very large number of individuals with varied backgrounds. An essential contribution came from citizens participating in the Citizen Summits and Meetings. About 300 recommendations were developed by approximately 2000 residents from nine different European countries. These recommendations were integrated in and enriched by academic research and expertise within and external to SurPRISE. They were transformed[5] in various ways to become the output presented here in a more coherent form. The recommendations listed below are abridged versions; please see the SurPRISE Policy Paper [2] for the full versions, including background information and, where applicable, links to current policy initiatives at the European level.

The legal framework on data processing must meet the challenges of technological advances

The current data protection legal framework needs to be adapted and modernised to meet the specific challenges of the most recent tools and techniques, e.g. of (big) data processing performing data crawling, matching, linkage and analysis functions.

Enforcing data protection in Europe

The impending revision of the data protection legal framework on the EU-level and amendments of national law should provide for mechanisms to effectively enforce data subjects' rights, also when tackling national and public security.

[4] See D7.3 for a description of the Decision Support System tool developed by SurPRISE.

[5] SurPRISE, with all its diverse expertise on board, has done its best to fulfil diverse and partly conflicting demands in the finalization of the recommendations and to integrate the citizens' views when formulating its recommendations. In this context, we would like to thank the members of our advisory panel and the external experts for their advice and feedback. Specifically, we acknowledge the essential contributions of about 2000 European citizens, but take full responsibility for this set of recommendations.

Protect personal data in transit, notably on the Internet

Technical and legal solutions need to be adopted to protect data in transit, notably on the internet, and in particular data travelling outside the European Union and the Schengen area.

Strengthen agencies providing supervision, guidance and control

For the processing of personal data, particularly in the field of police and justice, harmonised guidelines on a high level of protection are necessary. This especially applies to the respective control instances as well as to their control standards. They should be enabled to include representatives of different knowledge areas and societal domains into their personnel structure.

It is recommended that existing local, national and European supervisory authorities are organised in such a way that governance is provided by them close to the European citizens and with effective means of enforcement even in cases of cross-border data transmissions.

All data protection supervisory authorities should be made better known to the citizens.

Implement proper safeguards

Untargeted mass surveillance circumvents existing legal safeguards. Any restriction of fundamental rights resulting from the use of surveillance technologies and derived personal data must be based on a stringent case-by-case examination of their permissibility, ensuring that any restriction of fundamental rights has a proper legal basis; these restrictions are compatible with a democratic society; any exercise of discretion by (administrative) authorities is foreseeable and constrained; these restrictions are reasonable, necessary and proportionate in achieving an identified and pressing aim; and they do not violate the core dimensions of privacy.

Limit the scope of data collection

Enable a more effective preservation of citizen's right to privacy by meaningful enforcement of the principles of purpose limitation and proportionality. This encompasses a genuine consideration of non- or less intrusive alternatives prior to the deployment of surveillance measures for security purposes. Develop, foster, and prioritise measures (including SOSTs) with a narrower scope of data collection, storage and use whenever they are suitable instead of focusing on forms of untargeted mass surveillance.

Increase accountability and prevent abuse

European states need to promote and pursue a sincere political reflection as to how to design and deploy technology for security purposes in compliance with fundamental rights. Stronger accountability and liability for misuse and abuse must be established in both the public as well as the private sector.

Organisational and technical measures should be implemented to prevent abuse and to make abuses detectable to supervisory agencies.

Regulate and limit the role of private and non-governmental actors in the provision of public and national security

Security should remain the responsibility of state actors. It should be clarified to which extent and in which way the private sector and non-governmental actors currently contribute to the pursuit of security and to which degree these contributions are necessary. Security functions may only be outsourced if the contributions of private actors are equally or better than public standards in both terms, compliance with fundamental rights and quality of services.

The ownership and control of data should always remain under European legislation; security related data must not be mixed with other private data.

Establish a privacy-orientated competitive market

Policy makers should provide regulatory acts and incentives to establish a European market where privacy constitutes a competitive advantage. To this effect two sets of measures should be adopted. First, incentives in the form of regulation should be implemented, e.g., obligatory Privacy by Design for public procurement. Second, asymmetric or missing information of citizens concerning means of data collection, storage and use should be corrected, e.g., by mandatory information of users of "free services" about the basis of business models of such offers.

Implement and improve transparency

Member states need to increase their efforts to implement and improve the transparency of policy decisions, of the work of security authorities as well as of corporations and companies, in particular if the privacy of the citizens is affected. Transparency must be supported actively as current arrangements are insufficient and must comprise more than existing rights to know.

Improve training and education of security authorities

There is a need for more training and education for the personnel of security authorities and stakeholders in various surveillance practices to improve their work in order to act in compliance with privacy and other fundamental rights. Stakeholders in surveillance practices refer to all parties who are involved in conducting surveillance practices such as governmental organisations, service providers (public and private), staff of (surveillance) technology producers and vendors, or consultancies advising security authorities.

Raise awareness on security and privacy

Governments should support all actors in the field of education to reach citizens and educate the population on how new information technologies, and in particular SOSTs work, and how citizens can protect their privacy and manage their digital data. Appropriate strategies should be developed and implemented for different knowledge levels, ages and social backgrounds.

Foster participation in decision making

Citizens need to be fully involved in the process of policy-making, at least at the local and national level. National and regional governments should open the debate on surveillance orientated security technologies to the public and find appropriate solutions for involving citizens directly in decision making.

Establish technology assessment and on-going evaluation

A Technology Assessment (TA) should be conducted from the earliest stage of developing security technologies. A vital part of technology assessment is looking for and evaluating different alternative solutions, be it technical, organizational or legal. Applied TA methods should provide a transparent and participative assessment of alternatives. The discussions of which technologies are permissible (and acceptable) should be mandatory and fully included in the procurement and decision-making processes.

An evaluation of surveillance-orientated security technologies should also embrace implementation and deployment. Therefore, it needs to be regularly repeated during use by an impartial and competent entity.

Request mandatory Privacy by Design and Privacy by Default

The integration, maintenance, and further development of Privacy by Design and Privacy by Default principles should become a mandatory requirement for the development and implementation of surveillance-orientated security technologies. It must be ensured that the realisation of PbD is effective, comprehensible, evaluable, and that it goes along with an effective Privacy Impact Assessment in advance.

Focus on root causes of insecurity

Economic and social policies should become an integral element of security strategies at the level of the European Union and its member states. Reducing economic inequalities and addressing the general problems of lacking social justice are of essential importance for other key dimensions of security. It is an indispensable contribution to the prevention of violent radicalisation, and also a precautionary measure against poverty related crime, terrorism and the loss of political and societal cohesion in Europe.

4 CRITERIA AND FACTORS DETERMINING THE ACCEPTABILITY OF SECURITY TECHNOLOGIES

In response to the oversimplifying trade-off approach, dominating not only political debates and decision making on security technologies but also informing and thus influencing empirical research on the acceptability of SOSTs, SurPRISE developed a comprehensive and complex model of factors and criteria influencing the assessment of security technologies by citizens. This model was empirically tested at the participatory events organised by SurPRISE. In this chapter the main findings on factors and criteria influencing the acceptability of SOSTs are briefly summarised.[6] It contains information of highest importance and relevance for policy makers, security agencies, security industry and citizens alike. In the context of SurPRISE, factors represent those elements that influence people's opinions, but that people usually do not explicitly state or that they recognize only partially. Criteria are argumentations consciously used by citizens to explain their position vis-à-vis the acceptability of SOSTs. Factors may be addressed by means of quantitative methods, while criteria can be better assessed qualitatively through table discussions and focus groups.

Institutional trustworthiness is a key factor determining the acceptability of SOSTs, and it shows that, besides what citizens may think or know about security technologies, the degree of trust that security agencies and political institutions enjoy is a crucial element that citizens do take into account when assessing the acceptability of security technologies. Interestingly, the perceived level of threat has a limited effect on the acceptability of SOSTs, whilst Social Proximity has a strong impact on acceptability, confirming that security technologies that operate blanket surveillance are considered significantly less acceptable than security technologies carefully focusing on specific targets. Both effectiveness and intrusiveness emerge as highly relevant factors in explaining the level of acceptability of SOSTs. Moreover, whilst much of the security technology discourses insists that security technologies need to be intrusive to be effective, citizens argue that the more a technology is considered intrusive, the less it might be considered to be effective. This results question the general idea that SOSTs need to be intrusive to be effective, and, consequently, radically questions the trade-off approach. Moreover, our analysis shows that the trade-off approach does not generally influence acceptability, except in the case of very controversial SOSTs, like DPI. Age is positively correlated with acceptability; a result that radically questions the general belief that the younger generation, due to their familiarity with ICTs and SOSTs, would be less concerned with privacy issues. Table 1 and Table 2 list the factors tested in the empirical model, Table 1 contains the factors that proved statistically significant, Table 2 those without statistical significance, i.e. influence on acceptability.

[6] See D2.4 - Key factors affecting public acceptance and acceptability of SOSTs for a full description of the theoretical foundations of this model, of the complex hypotheses and relationships mapped in the model, of the methods applied in the empirical testing, and of the detailed results of the empirical analyses.

Table 1: Factors influencing acceptability of SOSTs

1. **General attitudes towards technology**. A generally positive attitude towards the ability of technology to enhance security makes SOSTs more acceptable. Conversely, a generally critical or sceptical view makes SOSTs less acceptable.
2. **Institutional trustworthiness**. Trust in security agencies makes the use of a given SOST more acceptable. The opposite is also true: the use of a more acceptable SOST (CCTVs or SLT, in this case) helps security agencies to be perceived as more trustworthy.
3. **Social Proximity.** SOSTs targeting specific groups or profiles, usually presented as "suspects" or "criminals" are eventually more acceptable than SOSTs that operate on blanket surveillance.
4. **Perceived intrusiveness** has a negative influence on acceptability. The more a SOST is perceived as intrusive, the less it is considered acceptable.
5. **Perceived effectiveness** has a positive influence on acceptability. The more a SOST is perceived as effective, the more it is considered acceptable.
6. **Substantive privacy concern.** A higher concern for both information and physical privacy makes SOSTs less acceptable.
7. **Age**. Age is positively correlated with acceptability of SOSTs. Older participants are more likely to accept SOSTs than younger ones.

Table 2: Factors not influencing acceptability of SOSTs

1. **Perceived level of threat**. Contrary to expectations, a more intense perception of security threat would NOT make SOSTs more acceptable. Concerns for online security, though, do have a positive effect on acceptability: the more participants are worried about their safety online, the more willing they were to accept SOSTs.
2. **Spatial proximity**. The proximity of SOSTs located and/or operating close to the physical and virtual spaces usually frequented by the participants did not influence the acceptability of SOSTs. However, we found that it has an effect on Substantive Privacy Concerns, which decreases the likelihood of considering SOST acceptable.
3. **Temporal proximity.** The prospective of SOSTs being very influential in the future did not influence the acceptability of them. However, we found that it has an effect on SOST Perceived Intrusiveness and Substantive Privacy Concerns, which, in turn, decrease the likelihood of considering a SOST acceptable.
4. **Familiarity with SOSTs.** Contrary to expectations, a deeper familiarity with SOSTs does not influence the acceptability of them.
5. **Security/privacy balance**. Considering technologies as both intrusive and effective do not make these technologies, in general, more acceptable.
6. **Education.** The educational level does not influence acceptability of SOSTs.
7. **Income.** The income level does not influence acceptability of SOSTs.

The analysis of the qualitative data has identified a number of criteria influencing the acceptability of surveillance technologies.

SOSTs are regarded as more acceptable if:

- operating within a European regulatory framework and under the control of a European regulatory body.
- operating in a context where transparency about the procedures, information about both data protection rights and principles and about the purposes and the scopes of security actions as well as accountability of security operators is ensured at all times.

- operated only by public authorities and only for public benefits. The participation of private actors in security operations, such as when security agencies acquire banking data or Facebook data or when security functions are outsourced to private operators, therefore, must be strictly regulated.
- their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives.
- their operation can be regulated through an opt-in approach. Whenever this is not possible, their operation need to be communicated to targeted individuals.
- they allow monitored individuals to access, modify and delete data about themselves.
- they target less sensitive data and spaces, whenever possible, according to criteria and purposes known to the public.
- they do not operate blanket surveillance. After reasonable evidences are gathered, they address specific targets, in specific times and spaces and for specific purposes. Whilst their purposes may change, these changes need to be explicitly discussed and publicly approved.
- they incorporate Privacy-by-Design protocols and mechanisms.
- they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are not alternatives but complementary to human resources and social policies.

All these criteria are also addressed by the recommendations included in the previous chapter. They should be integrated in decision making on SOSTS as an additional checklist and initial opening of the evaluation process.

5 CONCLUSIONS

The growing focus on pre-emption and proactive measures, resulting in increasing investments in surveillance capabilities, was predominantly based on an assumed trade-off between security on the one hand, and liberty and privacy on the other hand. The use of SOSTs for mass surveillance purposes is obviously eroding liberties and values it pretends to defend, nevertheless related programs remain largely untouched and unchanged, despite clear conflicts with fundamental rights and lack of evidence for their effectiveness.

The results from the involvement of about 2000 citizens from nine European countries in participatory assessment activities of SOSTs conducted by the SurPRISE project, confirm the scepticism against the trade-off approach in general and, in particular, as a suitable guideline for decision-making related to security policy. The participants of the Citizen Summits and Citizen Meetings predominantly requested strict limitations and regulations with regard to the use of surveillance technologies. The participants requested a more comprehensive, holistic and long-term approach to security, demanding a stronger focus on root causes of insecurity, i.e. tackling the enormous economic and social injustices resulting from the persistent economic crisis in Europe. SOSTs should not replace but only be used in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. A stable socio-economic environment is an essential precautionary measure not only against minor crimes but also against increasing violent radicalisation on an individual as well as on a political system level. Listening to the voice of citizens would therefore reduce the need for surveillance to and thus also lessen resulting risks for privacy and related fundamental rights, fostering democratic and societal development in line with European values.

REFERENCES

[1] http://surprise-project.eu/events/citizen-summits/

[2] The SurPRISE Deliverable 6.13 Policy Paper as well as the other mentioned deliverables is available at http://surprise-project.eu/dissemination/research-results/.

EUROPEAN ATTITUDES TOWARDS INTERNET SECURITY AND PRIVACY

Sunil Patil[1], Dimitris Potoglou[2] and Neil Robinson[3]

[1] *spatil@rand.org*
RAND Europe, Westbrook Centre, Cambridge CB4 1YG, (UK)

[2] *potogloud@cardiff.ac.uk*
Cardiff University, Cardiff (UK)

[3]*neillydone@googlemail.com*
RAND Europe, Westbrook Centre, Cambridge CB4 1YG, (UK)

Abstract

This paper presents part of the empirical evidence gathered from a large-scale pan-European survey conducted in autumn 2013. The survey targeted 1,000 participants in the most populated countries and 750 participants in less populated countries (e.g. Cyprus, Malta), all Member States of the (then) EU27. Citizens' concerns and level of trust appear to vary significantly across Europe. We also observe high-level of concern and distrust of the online world and its potential threats across countries in Southern and Eastern Europe as opposed to Nordic countries. The results of this study also suggest citizens' high levels of concern and distrust overall, generally align between the virtual and real worlds. Countries whose citizens express high levels of distrust in institutions and more generally, also exhibit high levels of concerns and distrust with regard to internet surveillance, websites and public and personal security.

Keywords: Internet privacy, internet surveillance, security, PACT.

1 INTRODUCTION

Personal communication and financial transactions are increasingly moving to cyber space. Accordingly, individuals and institutions are facing a rise in online privacy threats such as identity theft and accidental or unauthorised disclosures [1]. The internet is also being exploited by radical elements of the society creating a range of state-level security issues. To mitigate or address these threats, cyber security and other law enforcement agencies are engaging in internet surveillance including mass surveillance thus further raising privacy concerns on behalf of the general public. Therefore, there is an ongoing debate regarding online privacy and citizen's privacy attitudes and their concerns over the use of the Internet. The latter is quite important as it is responsible for driving consumers' practices for adopting data protective measures and technologies and their consumption patterns and competition across e-businesses, among others [2]. As a result, a number of scales have been used to monitor and measure citizen's responses to Internet security and privacy.

This paper reports on results from a pan-European survey conducted in autumn 2013 as part of PACT ("Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action"), a three-year research project funded by the European Commission's 7th Framework Programme. The overall aim of PACT[1] was to understand public perceptions of security, privacy and surveillance across the (then) 27 European Union Member States (EU27). The survey involved three stated preference experiments each corresponding to the following real-life

[1] http://www.projectpact.eu/

contexts: 1) Travel on metro or train; 2) Choice of an Internet Service Provider and 3) Purchasing a device or service for storing health-related personal data. The focus of this paper is on information collected in the context of internet use.

The aim of this paper is to map European attitudes towards data privacy, security and surveillance over the internet. The key research question which these data aim to answer concerns to what extent attitudes to privacy, security and surveillance differ across European countries. An important wider purpose was to derive evidence that would allow other findings from the PACT project to account for any such variations in how such topics are considered.

Findings from this paper provide an important yet missing input relating to public perception in the debate on security and privacy. The pan-European data collected from over 26,000 respondents is an added strength of this paper. This paper analyses responses collected from a set of psychometric scales related to trust, distrust and concerns, which are combined to generate composite indices as explained in the following sections. Finally, the paper investigates if people who are distrustful in general are also more concerned about internet privacy and surveillance.

2 PARTICIPANTS AND METHODOLOGY

Respondents across EU27 participated either via an online survey or a face-to-face interview. Online surveys were conducted in 12 countries with comparatively higher internet penetration (greater than 80%) and face-to-face interviews took place across 13 countries with relatively lower internet penetration [3]. Data were collected from both internet and face-to-face surveys in Italy and Germany in order to examine potential survey-mode biases. Approximately, 1,000 respondents aged 18 and older were interviewed in each country except Luxembourg, Malta, and Cyprus where, due to smaller population sizes, about 750 responses were collected. The survey included questions related to trust in institutions, distrust, concerns over security, data privacy and surveillance of the internet. Given that the survey fieldwork was carried out just after revelations of mass surveillance in summer 2013, the responses provide a snapshot of public concerns across the EU27.

2.1 Trust attitudes

Respondents answered 11 questions used to identify their level of trust in: banks, data protection authorities, hospitals, large internet based companies such as Google or Facebook, multinational companies, private health insurance companies, the army, the courts of law, European Union, media and national government. Responses are provided for each institution and range on a Likert scale between ‘don't trust at all' to 'completely trust them'.

Using these responses, we compute the Institutional Trust Index [4], which reflects respondents' overall trust across all eleven institutions. The Index is computed using Westin's methodology for creating composite indices. In effect, the Institutional Trust Index classifies respondents into three groups according to the number of ‘trustful’ responses across all the eleven institutions where 'trustful' responses indicate either complete trust’ or ‘trust’ in the institutions: high (7 or more ‘trustful’ responses); medium (4-6 ‘trustful’ responses) and low institutional trust (less than 4 ‘trustful’ responses).

Four additional statements were used to compute Westin's Distrust Index [4]: (a) Technology has almost got out of control; (b) Government can generally be trusted to look after our interests; (c) The way one votes has no effect on what the government does; (d) In general business helps us more than it harms us. Responses were collected on a Likert-type scale ranging from 'Strongly Agree'' to ''Strongly Disagree'. Based on the number of ‘distrustful’ responses to the above statements, we

constructed four segments in the sample: high (3-4 distrustful responses); medium (2 distrustful responses); low (1 distrustful response) and no distrust (0 distrustful responses).

2.2 Data protection concern

We computed an overall Data Protection Index, which represents respondents' concern for data protection while browsing the internet. Respondents were classified into the following four groups depending on the number of 'concerned' responses: high (3 or more 'concerned' responses); medium (2 concerned responses); low (1 concerned' response); and no concern. The classification into the above categories was based on responses (not concerned at all to very concerned) to the following statements [5]:

- Your information such as age, gender, location shared with websites or companies which you don't use
- Your internet usage information (including details of items you searched or purchased) shared with websites or companies which you don't use (third-party)
- Your personal information is not handled in a legitimate way (for example, the personal information you provided when opening an account with a website is not deleted when you closed the account).
- I am concerned that too much personal information is collected and stored by internet websites or Internet Service Providers (responses coded as disagree strongly to agree strongly).

2.3 Public security concern

The survey also included psychometric scales on concerns related to: use of internet by terrorists for training and planning attacks; use of internet for creating panic and/or spreading hatred; use of internet to share and publish child pornography; use of internet to perpetrate organised crime [6]. Answers from these four questions were used to create an internet related Public Security Concern index. Each respondent was grouped in one of the four groups depending on the number of concerned responses using the same coding scheme as the Data Protection Concern Index.

2.4 Individual security concern

Aside from threats to public security, internet users may also experience threats to their own security/property. Accordingly, responses to the following four statements were used to create an Individual Security Concern Index using the same coding scheme as in Data Protection Concern Index. The statements included concerns related to [5]: a computer virus which harms [your] computer; harassment or threatening comments on internet; theft of financial data (such as credit card information) or identity theft and theft of personal information to be used for impersonating [you].

In addition to the above mentioned indices, we used responses to individual statements to capture how trust in websites and concern for internet surveillance varies across EU27.

Trust in websites was captured through the statements:

- Most internet websites are safe environments in which to exchange information with others
- Most internet websites are reliable environments in which to conduct business transactions

Respondents indicated concern for internet surveillance through the following statements:

- Your private conversations on the internet being monitored
- Your internet usage monitored by police department in a different country

3 RESULTS

Fig. 1 shows how the Institutional Trust Index (ITrust_Index) varies across the surveyed EU27 countries. Malta was the country with the highest institutional trust followed by Latvia, the Czech Republic and Slovakia. More than 25% of participants in these countries expressed high institutional trust when the EU27 average was about 15%. On the other hand, less than 10% of respondents in Portugal, UK, Austria, Ireland, France, Cyprus, Italy, Spain and Greece expressed high institutional trust.

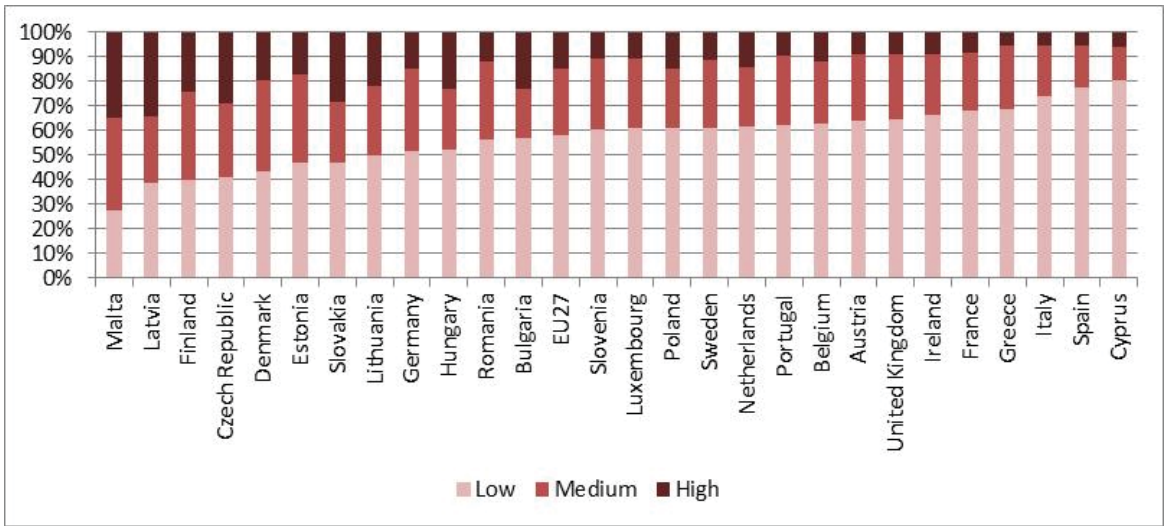


Fig. 1. Institutional trust across EU27

Using the segmentation process outlined in the previous section, Fig. 2 shows the variation of Westin's Distrust Index (DT2_Index) across the EU27 countries and the overall breakdown of 'high distrust', 'medium distrust', 'low distrust' and 'no distrust' across the EU27. More than 30% of respondents in Italy, Slovenia, Portugal, France and Spain are classified as 'high distrust' individuals whereas the overall proportion of high-distrust respondents across the EU27 was approximately 21%. The lowest proportions of respondents with high distrust appeared in Cyprus (9.3%), Denmark (10.3%), Sweden (12.8%) and the Czech Republic (12.8%).

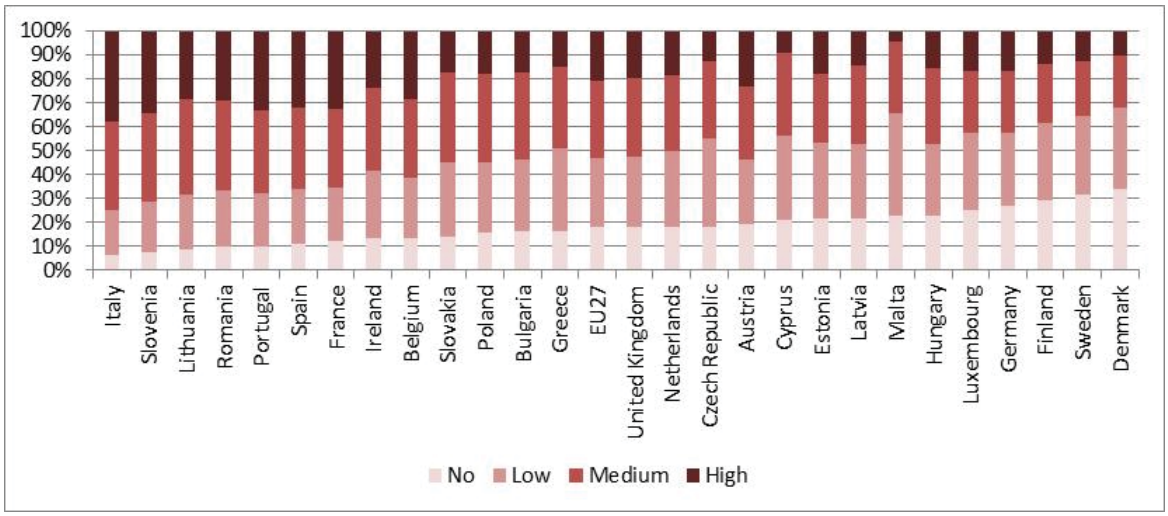


Fig. 2. Distrust across EU27

Fig. 3 shows the variation of the Data Protection Concern (DPC_Index) index across the EU27, which indicates how privacy-concerned respondents were when browsing the internet. Countries in southern and eastern Europe had the highest proportion of highly concerned respondents including Lithuania (83.4%), Spain (73.6%), Greece (73%) and Latvia (71.3%). The overall proportion of highly concerned individuals across the EU27 was at 52.4% that is a little more than half of respondents expressed high concerns with regard to their data protection.

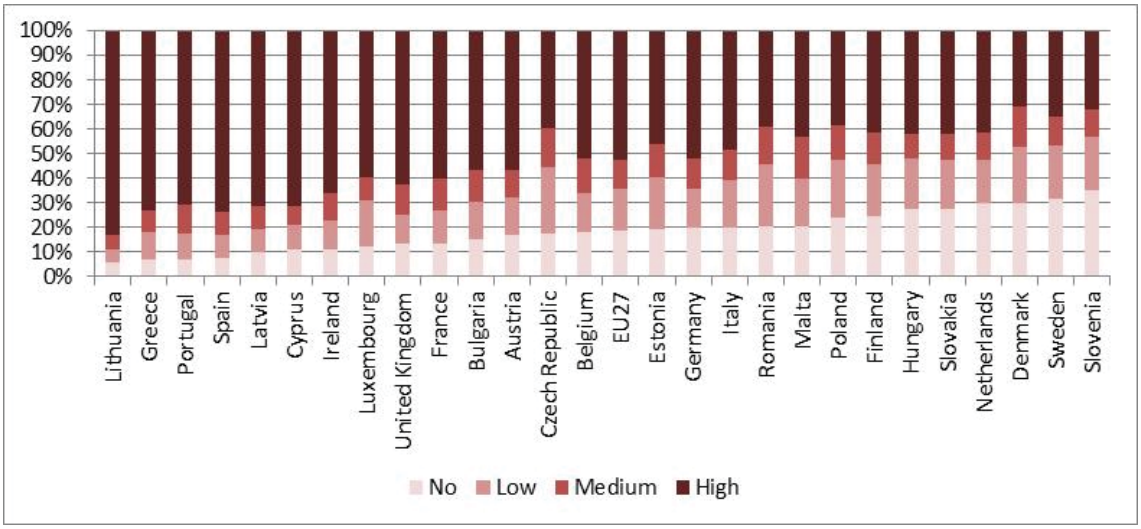


Fig. 3. Data protection concern across EU27

Using the responses on how the internet may be used to facilitate crime or spread hatred we constructed the Public Security Concern index (PSC_Index) described in the previous section. The proportion of high-, medium- , low- and no-concern respondents across countries and the EU27 overall is shown in Fig. 4. A similar pattern to the Data Protection Concern Index arises. Countries in Southern Europe (Portugal, Spain, Cyprus) and Eastern Europe (Lithuania, Latvia, Bulgaria, Romania) where the proportion of individuals that were highly concerned about public security was more than 54%. On the other hand, in Nordic countries (Denmark, Sweden, Finland, Denmark), Hungary, the Czech Republic and Poland lowest proportion of respondents expressed high public-security concern (less than 35% of respondents). The overall proportion of high-concerned respondents across the EU27 was approximately 48%.

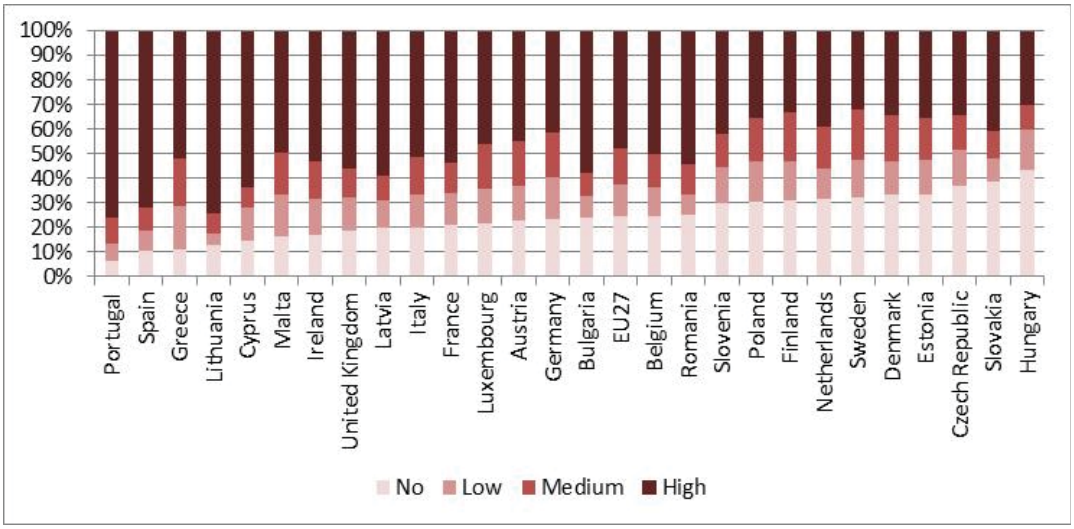


Fig. 4. Public security concern across EU27

The pattern of responses was fairly similar when looking at the distribution of the Individual Security Concern (ISC_Index) index in Fig. 5. Again, countries in Southern (Portugal, Cyprus, Spain, Greece) and Eastern Europe (Lithuania, Latvia, Bulgaria) had the highest proportions of highly concerned with regard to individual security. The proportions of respondents with high individual-security concern ranged between 36.3% (Bulgaria) and 71.4% (Lithuania). On the other hand, the lowest proportions of highly concerned respondents were observed in Sweden (7%) and Demark (7.4%). The overall proportion of highly concerned respondents with regard to individual security concern across the EU27 was approximately 28%.

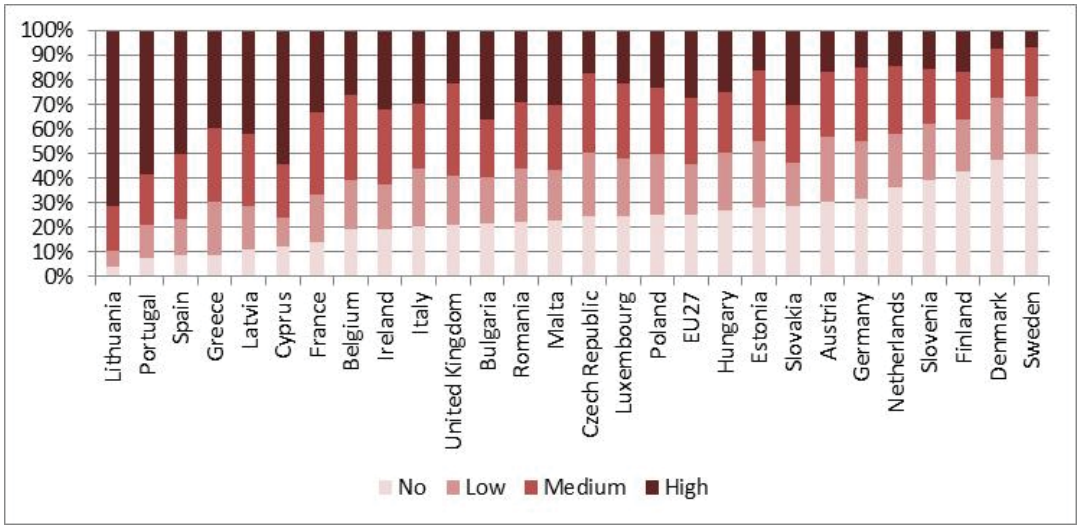


Fig. 5. Individual security concern across EU27

Further, we investigated potential associations between all the above mentioned indices. As show in Table1, a positive value indicates that if a respondent is classified as belonging to a high (trust/distrust/concern) group on one index, he/she is also likely to be classified as high on the other index. The results confirm that respondents with high institutional trust indicated low general distrust, low data protection, public security and individual security concerns.

Table 1. Spearman rank-order correlation coefficients*

	ITrust_Index	DT2_Index	DPC_Index	PSC_Index	ISC_Index
ITrust_Index	1				
DT2_Index	-0.2551	1			
DPC_Index	-0.0951	0.2167	1		
PSC_Index	-0.0345	0.1472	0.4124	1	
ISC_Index	-0.0574	0.1774	0.5016	0.5589	1

** p<0.001 across all coefficients*

Using the responses on trust in websites we observe that overall about 27% and 29% of respondents across EU27 think that most websites are safe and reliable respectively. Again the highest proportions of such respondents are observed in eastern Europe. With respect to internet surveillance, overall 55% of respondents across EU27 say they are concerned about their private conversations on the internet being monitored. Similarly, about 48% of respondents across EU27 say they are concerned about their internet usage being monitored by a police department in a different country. The highest proportions of respondents from Latvia, Portugal, Spain, Greece, Cyprus and Lithuania indicate concerns over internet surveillance. These findings likely present a snapshot of heightened concerns towards internet surveillance in the aftermath of revelations of secret mass surveillance programmes.

4 CONCLUSIONS

This paper presents part of the empirical evidence gathered from a large-scale pan-European survey conducted in autumn 2013. The survey targeted 1,000 participants in the most populated countries and 750 participants in less populated (e.g. Cyprus, Malta) member states of the (then) EU27. Its primary focus is on the use of the internet and its potential threats to privacy and personal information. Particular attention is also given to Europeans' levels of trust and concern at the institutional (e.g. banks and public services) level and more general distrust. By developing a number of composite indices derived through a set of attitudinal scales we measure Europeans' level of trust in websites, their concerns about data protection and internet surveillance, public and individual security on the internet.

It is evident that citizens' concerns and level of trust significantly vary across Europe. The high-level of concern about and distrust of the online world and its potential threats observed across countries in southern and eastern Europe as opposed to Nordic countries is particularly noteworthy.

The results of the present study also suggest citizens' high levels of concern and distrust overall generally align between the virtual and real worlds. Countries whose citizens express high levels of distrust in institutions and more generally, also exhibit high levels of concerns and distrust with regard to internet surveillance, websites, public and personal security. For example, respondents in Cyprus (80.3%) and Spain (77.4%) expressed the lowest levels of *Institutional Trust* whereas respondents in Malta (34.7%) and Latvia (34.6%) expressed the highest levels. With regard to data protection, the highest levels of concern were observed in Lithuania (83.4%), Spain (73.6%) and Greece (73%) whereas remarkably high proportions of 'no concerns' were observed in Slovenia (34.9%), Sweden (31.6%), Denmark (29.7%) and the Netherlands (29.6%).

The present study builds upon subsequent research in which citizens' levels of concern and trust feed into a broader analytical framework to analyse their preferences for different levels of security and privacy when using the internet, and specifically their choice of Internet Service Provider. The evidence presented in this paper feeds into the overall understanding of citizens' concerns about institutions and practices on the internet It supports findings about attitudes to privacy described in, for example, the Flash Eurobarometer polling on awareness of data protection authorities, in addition to other research on trust in European institutions more generally [7]. It helps inform the debate on privacy and security in the online world and provides useful information to service providers and policy-decision makers regarding the current state of trust and concern of European citizens which may help when designing privacy and security enhanced technologies, with the aim of them both being socially desirable and in line with European values.

Limitations of this study include possible sources of error due to survey nonresponse, question wording and question order. In addition, the results can also be affected by interviewer bias in face-to-face surveys. Further, the analysis presented here does not utilise weighting by demographic control data and being a snapshot including time, reflect attitudes which may be driven by news and current affairs such as the revelations surrounding surveillance by intelligence agencies. Other limitations concerned the innovative nature of the methodology (described separately in another paper) as it applied to the nuanced domain of privacy.

Finally, given the nuances of this subject, great care was taken to consider how different terms might be interpreted by citizens in different countries. Nonetheless with such a complex and at times emotive topic, the research design was confronted with a number of conceptual challenges including the meaning of privacy.

REFERENCES

[1] The Guardian (2013a) Edward Snowden's leaks are misguided – they risk exposing us to cyber-attacks http://www.theguardian.com/commentisfree/2013/sep/26/edward-snowden-leaks-misguided-cyber-attacks, [Accessed: 14/08/2014].

[2] Pribusch, S. (2013) Guide to measuring privacy concern: Review of survey and observational instruments, International Journal of Human-Computer Studues, 71, pp. 1133-1143.

[3] Johnson, A. & Lucica, E. (2013) Sampling Report, Project PACT Deliverable: D3.2, http://www.projectpact.eu/deliverables/wp3-fieldwork/d3.2, [Accessed: 02/08/2014].

[4] Kumaraguru, P. & Cranor, L.F. (2005) Privacy indexes: A survey of Westin's Studies CMU-ISRI-5-138, Institute for Software Research International, Carnegie Mellon University, Pittsburgh.

[5] Dinev, T. & Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. Information System Research, 17, pp. 61-80.

[6] Buchanan, T., Paine, C., Joinson, A.N. & Reips, U.-D. (2007) Development of Measures of Online Privacy Concern and Protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58, pp. 157-165.

[7] Special Eurobarometer 359 (2011) Attitudes on Data Protection and Electronic Identity in the European Unon, Survey co-odinated by DG Communication and conducted by TNS Opinion and Social http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [Accessed: 29/06/2014].

ACKNOWLEDGEMENTS

The PACT project, including the empirical work reported in this paper, has been funded by the "European Commission's 7th Framework Programme: Security" under grant agreement no 285635. The authors also wish to thank the PACT consortium members for their contributions to the study conception and survey design. We are also grateful to Catherine Saunders, RAND Europe, for her comments on the paper.

THE COMPLEXITY OF SECURITY DIMENSIONS: A COMPARISON OF THE NORTH-WEST AND SOUTH-EAST EUROPEAN REGIONS

Ksenia Chmutina[1], Milos Jovanovic[2], Lee Bosher[3], Andrew Dainty[4] and Joachim Burbiel[5]

[1] *k.chmutina@lboro.ac.uk*
Loughborough University, School of Civil and Building Engineer, Loughborough, LE11 3TU (UK)

[2]*milos.jovanovic@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT, Appelsgarten 2, 53879 Euskirchen (Germany)

[3]*l.bosher@lboro.ac.uk*
Loughborough University, School of Civil and Building Engineer, Loughborough, LE11 3TU (UK)

[4]*a.r.j.dainty@lboro.ac.uk*
Loughborough University, School of Civil and Building Engineer, Loughborough, LE11 3TU (UK)

[5] *joachim.burbiel@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT, Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

Prone to multiple interpretations, 'security' is becoming a multiple and hence, nebulous concept. Security can be associated with national security and the State's military power; notions of the individual safety; or human values and fundamental rights issues. This is clearly demonstrated in Europe with various member states using various concepts of security, making them event and space specific. Using two case study regions, this paper demonstrates the increasing complexity of the concept of security, as prominent security discourses and their impacts and consequences fall across more than one category of security dimensions. A large number of actors involved in, and affected by, security issues makes it harder to identify security dimensions. The political, economic, environmental and other security dimensions are interconnected and form a complex system of inter- and intra- dependent networks. Understanding these complexities will aid policy makers in formulating measures that influence an evolving European concept of security.

Keywords: security dimensions, European Union, case study.

1 INTRODUCTION

'Security' is a complex concept that is becoming nebulous, as it is prone to multiple interpretations both across and within different societies and cultures, domains of human activity, academic disciplines and so on. Security can be associated with the national security of states mainly buttressed by military power; at the same time, it is inextricably tied up with notions of the safety of individuals grounded in the fulfilment of basic Maslowian needs; and for yet others human values and fundamental rights issues are crucial elements of security. This is clearly demonstrated in Europe: despite

being under one political umbrella - the European Union - various European member states adopt various concepts of security, making them event and space specific.

The aim of this paper is to demonstrate the complexity of the concept of security using two European case study regions: North-West Europe (NWE) and South-East Europe (SEE) provide a sense of the complex interconnectivity of the debates that have shaped / are shaping the security discourse, as well as the disconnected dimensions that could be considered under this nebulous and politically charged term.

The approach to security employed in this paper (discussed in Section 2) and its perception are in many aspects similar to the capability approach to social problems as theorised by Sen [1] and later expanded [2]. Where the capability approach defines a certain set of functioning and opportunity freedom, the case study regions discussed in this paper look at different types of security perceptions in different fields (e.g. territorial security as opposed to physical security). The capability approach thus represents one possibility to complement this approach by looking at possibilities to improve people's capabilities in order to heighten their security.

2 METHODOLOGY

Based on the methodology developed for the EvoCS project,[1] this paper employs a combination of quantitative and qualitative methods and datasets that have been combined to identify the dimensions of security over time for the two discussed regions. Whilst four regions have been analysed during the project, only two will be discussed in this paper:

- North-Western EU (United Kingdom, Netherlands, France)
- South-Eastern Europe (Serbia, Bulgaria, Turkey).

These regions have been chosen due to their historical differences and the roles they are playing in the EU: the NWE region is seen as the core (financial and political), whereas the SEE region is a relatively new member of the EU with some of the countries still not being a part of the Union. In addition, the threats and challenges these regions are facing differ quite dramatically, which emphasises the challenge the EU is facing in developing a singular security strategy.

A comprehensive coding of approximately 2,300 relevant documents was also conducted using an analytical framework [3].

A concept of security consists of five dimensions: the *core values* which refer to the different aspects of life that actors seek to secure including physical safety and security, territorial integrity and security, environmental and ecological security, social stability and security, cultural identity and security, political stability and security, economic prosperity and security and information and cyber security*;* the types of *security challenges* that affect these core values which can be either risks, threats or hazards*;* the *levels* at which security needs to be protected which may include the local, subnational, international, transnational and global level; the *actors* that are involved including – but not limited to – national or local government, the private sector, civil society or the individual citizen; and the *ethical and human rights issues* which manifest themselves in this process.

Different beholders prioritise different core values and perceive different security challenges; they prefer these to be addressed by different actors at different levels, and consider different ethical and human rights issues to be a problem. In order to assess these differences empirically, the research process was divided into two stages.

[1] More information about the Evolving Concept of Security (EvoCS) project can be found at: http://www.evocs-project.eu/

In the first stage, currently prevailing security concepts in their respective countries across six principal security discourses (government, parliament, academia, media, the private sector and the NGO sector) were assessed. For each discourse in each country, a similar set of documents was retrieved based on a set of predefined criteria and a set of detailed retrieval instructions. The documents were then manually coded; this process relied on a uniform coding scheme in order to elicit various concepts of security. The results were then recorded in a centrally managed online data repository to which all country team researchers had access.

In stage two the findings were further analysed through a series of workshops held around Europe in early 2015 and desk-based research. The principal purpose was to get a more granular understanding based on in-depth qualitative analysis of the findings unearthed in stage one. The evolution of countries' and regions' concepts of security over the past decade was also described qualitatively to get a better grip on the recent historical context in which it emerged.

3 CASE STUDIES

3.1 North-Western Europe region

In the period after the Second World War, NWE region has been relatively stable from the political and economic perspectives. Nevertheless, a number of threats (such as terrorism and natural hazards) have been affecting the region. NWE region plays a key role in EU security policy due to the historic and financial role of the countries that compose this region. In particular, the main roles are played by the UK, France and Germany: they can still rely on their own political weight to influence developments and are less dependent on multilateral institutions; they are part of several institutional frameworks (e.g. NATO) in which they can operate, with the EU being just one these frameworks; they are involved in shaping policies on various levels and across a much wider range than other states. At the same time, the region has differences within itself which can affect the future of the EU security: France has a desire to play a leading role in the EU, whereas the UK is not sure whether it really belongs in the union at all and whether or not to remain in it. The role of the Netherlands however should not be underestimated as it is an important player in developing cooperation within the region.

Physical safety and security is by far the most salient core value in the NWE region, with social stability and security (in particular in France, where the issue of immigration is very prominent), information and cyber security, and economic prosperity and security also being widely discussed. The two latter core values are extremely intertwined, particularly when it comes to the context of cyber-crime. Within the most prominent core values, the most salient threats for the NWE region are cybercrime and terrorism. Other threats that are discussed in the NWE's popular discourse include immigration (including illegal immigration), natural hazards, climate change, and energy and food supply.

The UK, France and the Netherlands security strategies were written in approximately the same time in the late 2000s as they – and a region as a whole – were trying to redefine their approach to national security in light of changes in NATO and expansion of the EU. The national security strategies of the region share a similar way of adopting a risk-based 'all hazards' and 'all of society' approach as the new security direction. One of the most prominent similarities is the focus on the same security issues. Terrorism is a regional issue which, however, is mainly discussed at a national level; the discourse of terrorism includes not the terrorist attack but also the issues of radicalisation and polarisation. Supply-related threats (particularly energy supply) provide another good example: despite searching for new energy sources (e.g. fracking) and investing in renewable energy sources (e.g. solar and wind in Germany),

the NWE region is highly dependent on the fossil fuels supply from politically unstable regions (such as Russia). The main focus of the security discourse is on the national level, with national actors playing the most prominent role across the region. At the same time, general public which is perceived as the main object of threats hardly plays any role in this discourse.

There are however some differences in the way security issues are addressed. For example, the Netherlands is very outward looking, with large focus on the international state (it has even implemented an International Security Strategy [5]). Both national and international strategies overlap, but it is the only country that explicitly states the role that international affairs play in its security discourse. At the same time France and the UK acknowledge the role of the international actors yet mainly discuss the issues at a national level. Another example is the perception of the roles within the EU: the UK sees EU as mainly a trade partner (as many of its security deals are with the USA), whereas the Netherlands and France are more reliant on the EU in terms of security cooperation. The 2008 Financial crisis is admitted as a security issue in the region, however the discussion of its implications for the security in the UK is largely absent, whereas in Netherlands and France it further reinforced the inward shift, with socio-economic dimensions (such as unemployment; health; security of the elderly; and pensions) attaining greater salience.

The roles NWE region countries play in the EU is another interesting aspect that can influence the future developments in the security on the EU level. NWE is the largest (in terms of the population and the wealth) in the EU. Whilst all three analysed countries acknowledge that the EU is critical for their security and prosperity, their roles within the EU security agenda differ. The EU acts as a bloc with all 28 member states discussing issues and unanimously making decisions, but many argue that behind the scenes lies a tacit agreement that the Big Three - France, Germany, and the UK- take the lead on foreign policy, including security matters. UK and France continue to play important roles in the EU security (particularly in NATO), but they are also very protective of their sovereignty [6]. The Netherlands on the other hand prioritises integration with EU to also pursue defence cooperation within Europe, both multilaterally and bilaterally [7].

Overall, the NWE region shares similarities as well as having very specific differences, however security is at the top of the agenda in the region, which is demonstrated by the existence of the National Security Strategies in analysed countries as well as specific security strategies for particular threats.

3.2 South-Eastern Europe region

The SEE region constitutes an area that stands out in a number of striking ways. Not all countries in this region are part of the EU (e.g. Albania or Macedonia), some of them are in NATO (Bulgaria), while some have declared neutrality (Serbia). In the western part of SEE - the territory of former Yugoslavia - the worst military conflicts after World War II took place, with ethnic tensions still taking place (e.g. Macedonia in early 2015). Serbia was a major party during the Yugoslav civil war, therefore Serbian society was embedded in the broader context of socialist Yugoslavia, and in the last two decades have been having to adjust to a new political and economic system. It does not have NATO or EU membership but is a candidate country for the latter, and has strong ties with Russia. Serbia has an ongoing territorial conflict with one of its (former[2]) provinces: Kosovo and Metohia. Serbia's direct neighbour - Bulgaria - is an EU, and a NATO member. Bulgaria also has traditional ties with Russia and was part of the Eastern bloc, which is why Bulgaria still struggles with economic and societal transformation

[2] Kosovo has been recognized by over 100 states. However, for EvoCS, Kosovo was treated as an internal province of Serbia in accordance with UNSCR 1244 and to include Kosovo in the national case study.

processes. The Republic of Turkey has been a candidate country for the EU for almost a decade and is a NATO member. Its population is mostly Muslim; it has a common border with crisis-stricken states like Syria or Iraq. Along with similar security discourses as in the other countries of the region, Turkey faces a couple of unique internal (e.g. the Gulen movement) and external (e.g. groups fighting in the Syrian civil war) challenges. Together, these three national case studies represent a good sample of the diversity of the security discourse in SEE. Each of these countries has a number of unique security challenges and some that are common to all of them.

In recent history, the countries of SEE have been part of three different blocs, i.e. the western and eastern bloc and the movement of non-aligned countries. All this changed with the end of the Cold War, when countries such as Bulgaria or Romania started the transformation of their societies and economies towards the West. Such history was clearly reflected in the coding results.

Case study countries from this region have different foci. Physical safety and security is an often discussed core value in Serbia and in Turkey (where territorial integrity and security is also salient), but it is less prominent in Bulgaria, which mainly focuses on political stability and security. What the three studied countries do have in common is the fact that the environmental and ecological security and information and cyber security are the least salient.

SWE is also diverse in the security challenges the countries face, even though certain common issues can be identified. For instance, Serbia still observes the conflict with Kosovo and Metohia as an important security issue, although its focus has changed. While it was (and to a certain but much weaker degree still is) an issue of territorial integrity and security, current discussions concentrate on the situation of the Serbian community in Kosovo and their well-being [8]. Turkey faces a similar issue with its Kurdish minority (which has also weakened in recent years due to an on-going peace process). Serbia and Bulgaria are both struggling with the integration of their Roma communities, even though both countries have adopted national strategies for this [9].

There are also aspects that all three of the studied countries have in common: the security discourse predominantly takes place on a national level; and the main addressor of the security discourse in all three countries is the national government. In Bulgaria, the case is particularly interesting, since, according to the EvoCS coding findings, the addressor is the national government, while, according to [10] the people of Bulgaria in general seem to distrust their governing bodies (such trends can often be found in other countries of the region).

Similarly to NWE, security is an important aspect in the SEE public discourse and is addressed in the various national security strategies. In Serbia, the security challenges found in the coding exercise are mostly addressed in the national security strategy, while in Bulgaria the findings from the Bulgarian governmental annual report on Defence and Armed Forces are quite different from the findings of the project [11]. But one also has to keep in mind that the region is very different from NWE in many aspects like its historical background, salience of different core values and the existence of other security challenges [12].

4 DISCUSSION

The security policies of the European Union need to be effective (in protecting our societies), efficient (in the way these policies are executed), representative (for the security interests of different societies in the Union), in compliance with the EU legal and fundamental rights framework, and perceived as legitimate (by its citizens), and reflect national concerns and priorities as well as European ones. These are revealed in the four dimensions through which security is discussed in this paper (the first dimension - core values - is presented across the remaining four dimensions).

4.1 Actors

A variety of actors are involved in the popular discourse of security in NWE and SEE, however the most prominent addressor in both regions is national government, with its role being particularly noticeable when it comes to addressing the issues relevant to physical security and safety. The role of the private sector as an addressor increases dramatically in the context of cybersecurity, which is not surprising as they are perceived to also be an object of this threat. The actors which are addressed on the security issues are also diverse. Again, national government plays the largest role as an addressee, however the private sector – particularly in the case of cybersecurity in NWE - is also perceived to be an actor that should listen to what addressors have to say. In both regions, foreign government acts as an addressee in the context of terrorism: this may be explained by the efforts of all six governments to find the root of the terrorism problem and reduce its impacts. Whilst being by far the largest object of the majority of the threats in the both regions, general public at the same time they play a very little role (if any) as addressors or addressee.

Overall in both regions, national governments and parliament have the largest say and are the largest recipients of the information. In the NWE however whilst mostly talking to themselves, governments are also trying to connect with the private sector, which is a core of a region's economies. At the same time there is very little contact with local and regional governments, which are in charge of implementing security-related policies on the ground. Similarly, the general public who is perceived to be the largest object of threats is hardly being communicated to, thus it is unclear whether the general public should fully rely on governments' decisions when it comes to security matters.

4.2 Sources

Physical safety and security - the most salient core value in both regions - is discussed in most of the sources all sources, with government, parliament and newspaper publications covering this core value most. The exception is academic publications, which only seldom discuss physical safety and security in both regions (and when it does it solely focuses on terrorism (UK) and Kosovo war (Serbia)). Economic prosperity and security is also discussed in all the sources (except for academia in SEE), and in particular by private sector in NWE.

Terrorism and cyber-crime get wide coverage by a diverse set of sources in the NWE, with the national government publications playing the largest role when it comes to the discussion of terrorism. Newspapers also largely cover terrorism: this could be explained by the fact that terrorism-related stories attract more audience attention, as a terrorist attack would potentially have a large impact. Parliament and government publications have a more balanced coverage focusing on both issues, however slightly more attention is paid to terrorism. There is a sense that the issue of cyber-crime is being left to private businesses to resolve on its own, with only very few guidance from the government. NGOs are not discussing the most salient threats in the region; their main focus is on food supply, social stability and climate change, which is not surprising: as NGOs often address the importance of these issues. SWE differs slightly: main security challenges discussed are organised crime and corruption, but challenges such as violence against women, natural hazards, traffic security and a major influx of refugees (Serbia and Turkey) or the integration of the Roma minority and control of the security intelligence services (Serbia and Bulgaria) are also covered. Government policy documents and parliamentary debates tend to discuss all core values, sources from the private sector focus on economic prosperity and security, and the NGOs (among other core values) on social stability and security.

4.3 Levels

The main level at which security is discussed in both regions is national, however the discussed threats differ: such, at the national level the NWE region mainly focuses on terrorism and cyber-crime (with these issues also being touched upon at an international level), whereas in SWE it is organized crime and corruption. Global level is very rarely a part of the security discourse in the context of the analysed threats. In both regions, larger attention is paid to security at the national level. With an exception of Serbia which focuses on subnational level in the context of on-going Kosovo conflict, it is surprising that very little discussion is taking place at subnational and local levels, as some of the most salient threats (such as terrorism, cyber-crime or natural hazards) could have a large impact on a local scale. In addition, the main object of these threats being general public and private sector, both operating at local level, are thus largely ignored.

Different publications focus on different levels when it comes to specific threats. For example, government publications cover various levels, and whilst national level is prominent in the NWE region, both terrorism and cyber-crime are discussed in the context of international and transnational levels, but hardly touch upon local level. In SEE, some of the local discussions tend to focus on traffic security issues (for instance in Serbia). But this is probably due to a law being passed in the period under scrutiny.

4.4 Human rights and ethical issues

When it comes to the most salient threats discussed here, human rights and ethical issues are not very often touched upon. NWE region demonstrates some concern (although human rights are seen as a 'mentioned' rather than 'main' topic, as has already been discussed in the UK profile), but only briefly related to these issues when it comes to terrorism and cyber-crime, mainly in NGO reports, parliament publications and newspaper. Overall in the NWE region human rights are most prominently discussed under the physical safety and security and social stability and security core values. In SEE, human rights and ethical issues are discussed more often, with issues like discriminations against minorities, women and/or the lesbian, gay, bisexual and transgender community or the rights of refugees found in the security discourse.

5 CONCLUSION

This paper demonstrated a kaleidoscopic, but at the same time comprehensive, overview of the key elements of security perceptions in two regions, which at first glance seem very different.

Indeed, the historical situation and political context in which these regions have developed impact the perception of security. The NWE region, whilst addressing the traditional areas of security, is also shifting its focus on newly emerging threats such as cybercrime and terrorism, as well as encouraging the securitisation of threats that have not been covered by the security discourse previously (e.g. climate change). In the SEE region, the security discourse is dominated by more "traditional" security challenges like organised crime and corruption on the one hand and on historical problems that are still important like the Kosovo conflict in Serbia, the relations with Russia in Bulgaria or the internal threats (e.g. the Gulen movement) in Turkey. The difference between the regions lies in the historical context: ethnic struggles are mostly (with an exception of the Northern Ireland) a thing of the past in NWE, and the security discussions have moved onwards to modern "non-traditional" challenges.

However two regions also have quite a lot in common. For instance, although the EU promotes cooperation among the member states as well as with third country partners, both regions – and the countries within the regions - whilst mentioning cooperation -

focus largely on their own efforts, capacities and capabilities in addressing various threats. The most prominent security discourse happens at the national level emphasising a strong focus on the internal situation and not so much on the regional or European. The roles various actors play in the security discourse – with the government being the most prominent actor – are also very similar.

In conclusion, the two European regions are in many ways surprisingly similar, considering the many specific historical and political differences between them. These findings are important because they will feed into the policymaking process by establishing the representativeness and legitimacy of European security policies and their ability to account for the geo-political contexts and stakeholder perspectives across which they must navigate. From a European point of view, this might be seen as an opportunity since future European Security Strategies can better address shared security problems of both EU and (possible future) non-EU members.

REFERENCES

[1] Sen, A (1979). *Equality of what?* In: MacMurrin, S (ed.) The Tanner lectures of human values. Cambridge University Press. UK.

[2] Comim, F, Qizilbash, M & Alkire, S (2008). *The Capability Approach – Concepts Measures and Applications*. Cambridge University Press. UK.

[3] Sweijs, T. et al. (2015). *Asessing Evolving Concepts of Security: Coding Handbook*. Deliverable 3.1. Available at: http://evocs-project.eu/deliverables (accessed 28/05/2015).

[4] BSA (2015). *EU Cybersecurity Maturity Dashboard*. Available at: http://cybersecurity.bsa.org/index.html (accessed 9/06/2015).

[5] Ministry of Foreign Affairs (2013). International Security Strategy. Available at: http://www.government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html (accessed 9/06/2015)

[6] Lehne, S. (2012). *The big three in European policy*. Carnegie Europe.

[7] Dickow, M. et al. (2013). *Deepening German-Netherlands Defence Cooperation for Europe's Security Needs.* Working Paper. Research Division EU External Relations.

[8] Jovanovic, M. et al. (2015). *Evolving Concept of Security. D8.1 – Report on the regional workshop.* Available at: http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3323306.pdf (accessed 09/06/2015)

[9] For the Serbian case (in Serbian Cyrillic): Vlada Srbije (2015). *Стратегија за унапређивање положаја Рома у Републици Србији.* Available at: http://www.srbija.gov.rs/extfile/sr/107688/strategija_romi0080_cyr.zip (accessed 09/06/2015)

[10] Ivan Krastev (2013). *In Mistrust We Trust: Can Democracy Survive When We Don't Trust Our Leaders?* (Kindle Single) (TED Books).

[11] Bulgarian Government (2014). *Government's Annual Report on Defence and Armed Forces.* Available in Bulgarian language at www.md.government.bg/bg/doc/drugi/20150327_Doklad_MO_2014.pdf (accessed 9/06/2015)

[12] Jovanovic, M. et al. (2015). EvoCS Deliverable 8.2. Available at: http://evocs-project.eu/deliverables (accessed 9/06/2015)

LEGAL CHALLENGES OF FIGHTING BOTNETS: A LAW ENFORCEMENT PERSPECTIVE

Karine e Silva[1]

[1] *k.k.esilva@uvt.nl*
PhD candidate, Tilburg University, Tilburg Institute for Law, Technology, and Society (TILT), Prof. Cobbenhagenlaan 221, 5037 DE Tilburg (The Netherlands)

Abstract

Strengthening enforcement of cybercrime law is not a simple question of more legislation. Botnet investigations often intrude in the private sphere of third parties, possibly implicating access to large amounts of data related to innocent individuals and unrelated to the investigated offence. In addition, prior to entering the network, law enforcement may not be able to anticipate where data are located, posing a threat to the sovereignty of foreign States. The challenge to ensure the rule of law while enabling effective law enforcement revolves a difficult equalize between privacy, public security, and jurisdictional rules, explored in this paper by a comparative analysis of the United States and Dutch legal systems.

Keywords: Botnets, Criminal Law, Cybercrime.

1 INTRODUCTION

This paper investigates the legal issues surrounding effective and adequate law enforcement actions against botnets[1] and the underlining questions that have hindered proper mitigation of such malicious infrastructures by police and judiciary in the United States (herein U.S.) and in the Netherlands. The issue of effectiveness and adequacy of law enforcement against cybercrime is genuine and troublesome. First, law enforcement is bounded by powers and measures provided by law. Here, botnets' dynamism and fast-pace infections have posed a serious challenge for lagging legislative processes, in which the reality of cybercrime and the existing powers of law enforcement are widely apart. Secondly, jurisdictional conflicts and insufficient international cooperation have frustrated effective law enforcement response. While botnets are characterised by borderless infections and controls, law enforcement actions are strictly circumscribed to territoriality and the uneven levels of legislation and resources hinder proper international collaboration. Overall, structural legal problems have given botnets a fair advantage in most jurisdictions.

1.1 Methodology and Goals

This paper uses the functional method for comparative legal analysis to identify the strengths and weaknesses of the U.S. and the Netherlands. As the lead of important international consortiums that disrupted Gameover Zeus, Coreflood, and ZeroAccess, the U.S. revels an approach to privacy that is largely different from EU Member States, together with broad law enforcement powers. In the EU, the Netherlands offers a sharp legal framework, with a tradition for privacy, and specialised police and courts dealing with cybercrime. By comparing the legal frameworks of these two major players, the legal analysis has the potential to result in legislative recommendations that may help advancing both national frameworks and support other countries strengthening the rule of law.

[1] Botnets are collections of machines, called zombies, infected by partially autonomous piece of advanced software (bots) which render functionality of the compromised system to the attacker(s), as they connect back to other infected machines or to central server(s) [1].

2 BACKGROUND

In both civil and common law countries, a criminal investigation often starts with a notice of a crime placed at law enforcement investigative agencies or by an ex officio procedure initiated by law enforcement, in face of evidence of a crime. Individual users, however, may face obstacles in this process. First, end users may not realize they have fallen victim of a cybercriminal. Some forms of criminal use of the Internet are subtle for individuals accustomed to physical forms of crime. Secondly, estimating the impact of cybercrime is not obvious. Especially when these attacks are not targeted at causing direct financial losses, or cause only minimal impact [2]. Without a clear understanding of the legal interests affected by cybercrime and its financial costs, victims have fewer incentives to report cybercrime. Moreover, companies have purposefully restrained from reporting cybercrime attacks for fear of reputational damages [3] and consumer claims.

There are numerous issues related to cybercrime investigation and prosecution, but the analysis conducted in this paper shall be restricted to three main issues closely related to botnets. These are the respect to privacy during an investigation, the scope of national jurisdiction, and international cooperation. Moreover, it is not the purpose of this paper to exhaust all legal implications of these three issues, but to provide an overview of the most relevant elements and a functional comparison of the status of botnet investigation in the U.S. and in the Netherlands. The functional method of comparative legal research enables an approximation between different legal systems. This is because the functionalist method is factual, looking at how legal systems respond to the same real life situation, rather than the theories and formalities behind the system.

2.1 Privacy

Even when cybercrime is reported, evidence may be scattered, with victims and attacks taking place in different parts of the world, turning investigation into a challenge for local authorities. This is certainly the case with most botnets. The widespread evidence of crime and botnet architecture poses a serious challenge to lawful collection of evidence, and how it can be balanced against privacy of victims. In this context, tools that intrude on the data flows of victims' networks in order to collect evidence about the remote perpetrator risk impinging on the rights to privacy and data protection of victims. For this reason, law enforcement must pay due attention to the requirements of privacy and the need for requesting court orders, when applicable, before attempting to collect information about botnets. Moreover, even if an investigation is conducted in compliance with the privacy laws of the national state, it may reach devices and networks of foreign victims, who are subject to different privacy regulation in their country. In order to avoid violation of privacy in the course of an investigation, it is paramount for law enforcement to work in cooperation with foreign authorities, and to foster research on the legitimacy of anti-botnet solutions, rather than focusing on their effectiveness.

2.2 Jurisdiction

The importance of cooperation against botnets has become a central element of botnet investigation and prosecution for the challenges it brings to the legal idea of jurisdiction. The escalation of botnets is seldom restricted to one country. From a legal perspective, this large-scale dissemination restricts the sphere of lawful actions that can be undertaken nationally, since authorities have their power limited to the territory of their State. Nevertheless, jurisdiction is a complex legal concept, which encompasses three subdivisions. Prescriptive jurisdiction refers to the power of a State to have jurisdiction over a criminal offence as defined in national law. Furthermore, adjudicative jurisdiction refers to the power of bringing a suspect to the court of the prosecuting State. Finally, enforcement jurisdiction refers to the power of subjecting a sentenced criminal to the penalty ruled by the court. This multifaceted understanding of jurisdiction explains why a perpetrator liable of an offence in a country may not be brought before that court or imprisoned in a country where he has been convicted for

a crime. Altogether, the limits of territoriality and jurisdiction have played an important role on the fight against cybercrime, contributing to legislative discussions on extraterritorial effects of national law, in the attempt to strengthen the powers of authorities beyond the national State and bypass dependency on mutual assistance. While it seems such overachieving extraterritoriality provisions would help expedite the lengthy mutual legal assistance treaties (MLATs) and letters rogatory,[2] it has also posed challenges of jurisdictional conflict, threatening State sovereignty and the guarantees of criminal procedure.

2.3 International Cooperation

If a criminal procedure ends with a court ruling against a criminal located outside the territory of that State, the judiciary still needs to find ways to enforce their ruling. This may be achieved by extradition, whereby a criminal is sent to the territory of the country where he has been convicted, or by recognition and enforcement of a foreign court ruling by the State where the criminal is located. The two countries object of this analysis, the U.S. and the Netherlands, have ratified the Council of Europe Convention on Cybercrime, which created rules for extradition of cybercriminals under Art. 24. However, when extradition[3] is not possible, a country may request a court ruling issued by its authorities to be recognised and enforced in a foreign State. In this case, the law of the foreign State will dictate the requirements and procedure for recognition and enforcement of the alien ruling, a procedure without legal certainty if there is no MLAT established between the countries.

Finally, it is important to mention Chapter III of the Council of Europe Convention on Cybercrime contains important measures to streamline mutual assistance in criminal matters, which is crucial for investigation of botnets, which involves data vulnerable to loss if not otherwise expeditiously secured. Besides provisions regulating various investigation powers to use mutual assistance, the establishment of a 24/7 network (Art. 35) was particularly important to enable prompt contacts between states. However, the current framework of international cooperation established at the level of the Council of Europe is insufficient to cover the multitude of States whose assistance is necessary. Lastly, the framework of the convention also fails in providing a specific procedure for urgent matters, which are often the case of botnets and the imminence of their attack, the reason why many States, including the U.S., have given preference to using MLATs instead.

3 BOTNET INVESTIGATIONS IN THE UNITED STATES

Cybercrime legislation in the U.S. dates from as early as 1984, when the criminal offences of unauthorized access and use of computer and computer networks were enacted, also known as hacking provisions [6]. The current provisions on cybercrime are a result of continuous changes on the Computer Fraud and Abuse Act, amending 18 U.S.C. §1030 [6]. The cybercrime provisions of the U.S. criminal code (Title 18 of the U.S.C.) result in one of the most fine-tuned cybercrime legislations in force, covering a wide range of offences and providing various legal measures to ensure prosecution of cybercrime and compensation for the damages caused by criminals. Botnets are designed for various purposes, entailing a two-stage criminal offence. First, the dissemination of the bot itself can be considered a hacking offence (18. U.S.C. §1030(a)(2)) or a malware offence (18. U.S.C. §1030(a)(5)), since bots gain unauthorised access to systems in order to compromise their autonomy. Later, since the widespread dissemination frequently serves an ultimate criminal purpose of

[2] In the U.S., MLATs are bilateral cooperation treaties available to prosecutors for foreign law enforcement cooperation and assistance in support of criminal investigations and proceedings. MLATs are considered relatively efficient, being the principal mechanism for assistance in criminal matters involving foreign requests for collecting evidence, search and seizure, serving judicial documents, etc. Letters rogatory are formal requests for judicial assistance made by a court in one country to a court in another country, primarily used by non-government actors without access to the MLATs. Letters rogatory are more time-consuming and less predictable than MLATs, as they depend on discretion of the requested court [4].

[3] "The practice of extradition enables one state to hand over to another state suspected or convicted criminals who have fled to the territory of the former. It is based upon bilateral treaty law and does not exist as an obligatin upon states in customary law" [5].

launching a large-scale attack, the botmaster(s) shall also be liable for the ultimate offence, which may coincide or not with the first.

Here it is important to highlight that, although Federal law already covers hacking, every U.S. state has passed legislation on hacking, and many on forms of aggravated hacking, in case the access results in copying or loss of data [3]. A similar approach is found in State law criminalising other types of cybercrime, albeit the limited application of these provisions, since cybercrime is almost inevitably a ubiquitous offence [3]. As a result, investigation and prosecution of such crimes is also a primarily responsibility of federal authorities, explaining the large influence of the FBI in the fight against botnets in the U.S. and abroad. After this short introduction on the U.S. cybercrime law, the elements of comparison shall be analysed.

3.1 Protection of Privacy

To understand the implications of botnet investigations on the privacy of victims and, arguably, of the suspects, it is important to comprehend how privacy has been regulated in the Fourth Amendment of the U.S. Constitution. This is particularly relevant when considering search and seizure in the course of an investigation, which under U.S. law can take place with and without a warranty. The two cases shall be analysed separately.

Search and seizures conducted without warranty must respect a person's reasonable expectation of privacy. When deciding whether individuals could have expectation of privacy over information stored in computers, U.S. courts decided this should be possible, using the analogy of a 'closed container', adopting the plain view doctrine [7] to computer data. In a simple metaphor, a warranty will be necessary if, under the same situation, law enforcement would be prohibited from opening a briefcase and examine its content. However, if the content is knowingly made publicly available, the expectation of privacy does not subsist, and no warranty is required. The same is valid if control over the protected information is offered to a third party, such as if data are turned over to another person, for instance, via electronic communications. During the transfer the Fourth Amendment remains applicable, but, once the recipient receives the item, the reasonable expectation of privacy ends [8]. As a result, law enforcement is allowed to examine the transferred data without a warranty once the transmission is concluded. This is to say that no warranty is required to obtain information transfer by the sender to banks, telephone operators, and other third parties, based on the Supreme Court rulings in *Katz* [9], *Jackson* [10] and *Smith* [11] [3]. By analogy, the same termination of privacy is applied to data transferred over any electronic means. Nevertheless, the Supreme Court recognises that in the case of emails and phone calls, the Fourth Amendment should cover the content of these communications [3], but not their traffic data. Finally, in *Kyllo* [12], the Supreme Court ruled that in cases where innovative technology is used to collect information about the home, the Fourth Amendment might apply. This is the case only if the technology deployed in not in general public use and if the collected information refers to the interior of the home of the suspect. *Kyllo*, however, is not applicable to electronic communications [8], whose signals are transmitted outside the home environment.

For all other cases, a warranty must be requested. This is achieved via an affidavit or application for a search warrant, in which the probable cause and the limits of the search must be made explicit by the requesting authority. When establishing the probable cause, the requesting party must assure there is evidence of crime in a private space, such as computer hardware, which requires the issuing of the warrant in light of the expectation of privacy. In addition, the warrant must be specific and limited, this is it has to fulfil the particularity and breadth criteria [13]. In short, the warrant must be specific enough to permit the executing officer to exercise reasonable, rational and informed discretion and judgment in selecting what should be seized [14]. In the course of a cybercrime investigation, it means the warrant must describe the devices (place) and the data (thing) to be taken from the device for the purpose of the investigation.

3.2 Scope of national jurisdiction

Under U.S. law, cybercrimes and, more specifically botnets, will almost inevitably call for the application of federal law [6]. To bring a claim before a U.S. court, however, it is necessary to demonstrate its jurisdictional competence over the subject matter and the defendant. Therefore, the provisions of 18 U.S.C. §1030 grant courts the competence to decide on cybercrime, given that connection to the Internet affects interstate commerce, but it is not sufficient to grant courts the competence to decide on the case if personal jurisdiction is not ascertained. The personal jurisdiction element, enshrined under de Due Process Clause of the Fourth Amendment, requires a party to have substantial systematic and continuous contacts with that forum. This criterion, also referred to as purpose availment, ensures that a court can exercise jurisdiction over a defendant where he purposefully directs his actions, and that a state can adjudicate crimes targeted at its territory [15]. Additionally, in Provident Nat'l Bank [16], the Supreme Court decided that a federal district court may assert personal jurisdiction over a non-resident of the state in which the court sits to the extent authorized by the law of that state. This provision was used in the takedown of Gameover Zeus [16], where law enforcement authorities started the claim against the offenders in the state of Pennsylvania. The reason for preferring to start a claim in Pennsylvania, when other states where an option, arguably lies on the fact that Pennsylvania provides for a long-arm statute with extraterritorial effects to non-nationals. By combining the rules of the Due Process Clause of the U.S. Constitution and the state law of Pennsylvania, law enforcement was capable of bringing a case against a non-national located in a foreign country before a U.S. federal court, which recognised jurisdiction over the case and ultimately ruled against the defendant.

3.3 International Cooperation

The U.S. has established a large network of cooperation for criminal matters that could be applicable to botnets and cybercrime at large, including participation in the EUROPOL Joint Cybercrime Action Taskforce (J-CAT) [18], and numerous MLATs. The U.S. has also ratified the Inter-American Convention on Mutual Legal Assistance of the Organization of American States, the United Nations Convention against Transnational Organized Crime, and the Council of Europe Convention on Cybercrime. The latter provides specific rules for mutual legal assistance between parties to the instrument. Given the numerous applicable instruments at hand, the U.S. has multiple options for cooperating with foreign States. For its leading economic position, it is easier for the U.S. to ensure other countries respect the commitments made based on the MLATs, guaranteeing a strong network for investigation and prosecution procedures initiated by its national authorities.

4 BOTNET INVESTIGATIONS IN THE NETHERLANDS

The Dutch Criminal Code and the Dutch Criminal Procedural Code are the main sources of legal provisions directly applicable to the criminalisation and investigation of botnets. Because a botnet develops in phases, it is possible to identify multiple criminal offences committed by the perpetrator from the dissemination until the attack phase. The very concept of bot exploitation is a hacking offence under Dutch criminal law, described as the intentional and unlawful intrusion into a computerized device or a part thereof (Art. 138ab of the Dutch Criminal Code, hereinafter DCC). Moreover, creating a bot also amounts to data interference (Art. 350a(1), DCC) and can also be qualified under Art. 350(3), DCC, for it disseminates data intended to damage computer systems. Distribution of malware is criminalised under Art. 350a(3), DCC, and DDoS attacks by Art. 138b, DCC. Overall, the DCC offers a broad range of criminal offences that are applicable to botnets, revealing the efforts of the national legislator in keeping pace with the evolution of cybercrime.

4.1 Protection of Privacy

The regulation of privacy in the Netherlands follows the Charter of the European Union in Human Rights and the European Convention on Human Rights, which have set the high-level norms for the concept and lawful limitations on the fundamental right to privacy. In contrast to the U.S. system, the civil law model of the Netherlands and the binding instruments regulating privacy have ensured a privacy-oriented legal system, which cannot be waived by claims of national security and criminal investigation without fulfilling strict legal requirements. Nevertheless, criminal investigation may impinge on the right to privacy, when necessary, adequate, and as regulated by national law. As a result, it is possible for law enforcement to make use of traditional investigation powers, such as data production orders (Arts. 126n, 126na, Dutch Criminal Procedure Code, herein DCPC). These can grant police the right to request the provider of a communications service to deliver identifying data such as name, address, postal code, birth date, etc., concerning a user of that service.

Specific powers to search and copy computer data (Articles 125i and following, DCPC) enable the police to search computers connected to devices on the place of the search, insofar as the people living or working in the searched location have lawful access to those systems. Currently, a new Computer Crime Bill (CC III) is in parliament. The CC III aims at expanding investigation powers of law enforcement to match them against the needs of cybercrime fighting. Among several important aspects highlighted in this bill, two proposed sets of investigation powers have direct application to botnets, namely the provisions on hack back into computers and the notice and takedown for disabling access to data. The first would give police a legitimate ground to engage into crawling and Sybil attacks, for instance. In addition, the power of disabling access to data could be used to order the takedown of servers and block malicious traffic. Discussions on the legitimacy of CC III and its impact on privacy have taken place among scholars and practitioners, as they seem unbalanced with the right to privacy and confidentiality of communications.

4.2 Scope of national jurisdiction

Art. 2 of the Dutch Criminal Code (DCC) establishes substantive national jurisdiction [19] over anyone guilty of any offence in the Netherlands. The DCC thus determines application of Dutch criminal law based on the territoriality principle [19]. The territoriality principle and the theory of locus delicti in itself are often insufficiently clear to determine whether a country has jurisdiction over cybercrime cases. The Dutch territoriality tradition allows national judges to take into account the place of the activity, the place of the instrument of the crime, the places of the constitutive consequences and even the ubiquity criterion in order to decide whether they have competence to decide on a case [20]. This all-embracing approach leads to a quasi-universal jurisdictional competence by Dutch authorities. Exploring the characteristics of Dutch jurisdictional powers is not the aim of this paper, but has direct influence on the topic at hand. In the Bredolab case [21], a largely studied botnet takedown in the Netherlands, the locus delicti points for Dutch jurisdiction on the matter, as victims, business and servers located in the Netherlands were affected by the malware, despite the extraterritorial elements of the crime.

Another noteworthy controversy associated with CC III is the possibility of extraterritorial application of hacking powers by the police. CC III would exceptionally enable national police to use hacking powers beyond Dutch territory, in cases when the location of the computer in unknown. Here, Art. 4 of the DCC was extended to legitimise cross-border investigations, possibly impinging on foreign sovereignty. However, the limits and circumstances of these cross-border investigations remain unclear and the legislator has failed in providing further details on how the CC III can be compatible with international law. Currently, there is legal uncertainty on the legitimacy of such far-reaching measures being enacted by the Dutch legislator.

4.3 International Cooperation

The international cooperation framework adopted by the Netherlands and applicable to the investigation of botnets include the Council of Europe Convention on Cybercrime and the European Arrest Warrant (EAW) regulation, based on the Council Framework Decision of 13 June 2002. Where the norms of the convention are the same applicable to the U.S., the EAW is has improved and simplified cooperation between EU Member States law enforcement only, and listed computer-related crime between the offences subject to the Framework Decision. The adoption of the EAW in 2002, which entered into force in 2004, implied faster and simpler surrender procedures with legal certainty, and the impossibility of EU Member States to refuse to extradite nationals to another Member State.

5 RESULTS AND CONCLUSION

This paper presented a legal perspective on investigation and prosecution of botnets in the U.S. and in the NL, highlighting the weaknesses and strengthens of both systems. While legislators and law enforcement authorities of the two countries are still working on better laws and procedures for effective response to botnets, the fundamental right to privacy and structural aspects of the legal system require further attention from both authorities. If, on the one hand, the U.S. system has revealed to be more flexible to the dynamics of botnets, on the other hand, this flexibility can be associated to the variable standards of privacy afforded by its legal order. The Dutch system preserves the European Union tradition of rigid norms of privacy, based on its cultural values. On the territorial scope of legislation, the U.S. has an ambitious set of extraterritorial provisions, which can and have been used to prosecute botmasters located outside the country. The Netherlands is currently under a heated discussion on the possibility of granting extraterritorial powers to law enforcement in the fight against cybercrime, which would be directly applicable to investigate and prosecute botnets.

Ideally, a legal system should have the flexibility and specificity of the U.S. system and the respect for fundamental rights offered by the Dutch framework. There is no reason why each country should not try to adjust their legislation in this direction. However, the focus on extraterritoriality growing in both jurisdictions presents a serious threat to the international legal order. Investigation of botnets without due account to the privacy of nationals and non-nationals must be stopped. Jurisdictional conflicts must be tackled at the international level, avoiding unilateral expansions of state powers in detriment to the sovereignty of foreign states and the rights of their citizens.

Moreover, both countries are part of the Council of Europe Convention on cybercrime, the first solid internationally binding instrument of its kind, but arguably an out-dated convention at this stage and evolution of cybercrime. Together with the rules on extradition and mutual legal assistance provided by the convention, countries have other bilateral and multilateral agreements in force to help expedite cybercrime investigations. This mosaic of rules on international cooperation, and the consequent lack of legal security and transparency, reveal the need for an integrated international approach on special forms of transnational crime, with a special focus on botnets and other large-scale forms of cybercrime.

REFERENCES

[1] Clark, K., Warnier, M., & Brazier, F. M. (2011). BotClouds - The Future of Cloud-based Botnets? *Proceedings of the 1st International Conference on Cloud Computing and Services Science (CLOSER 2011)*. Noordwijkerhout: SciTePress – Science and Technology Publications, pp. 597-603.

[2] de Hert, P., Fuster, G. G., & Koops, B.-J. (2006). Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision and the Council of Europe Convention. *International Review of Penal Law*, 3 (77), pp. 503-524.

[3] Brenner, S. W. (2012). *Cybercrime and the law: challenges, issues, and outcomes*. Boston: Northeastern University Press.

[4] Federal Judicial Center. (2014). *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*. International Litigation Guide. Washington: Federal Judicial Center.

[5] Shaw, M. (2010). *International Law*. Cambridge: Cambridge University Press, p. 686.

[6] Office of Legal Education. (2010). *Prosecuting Computer Crimes*. US Department of Justice, Computer Crime and Intellectual Property Section Criminal Division. Washington: Office of Legal Education.

[7] Romero, E. (1988). Fourth Amendment--Requiring Probable Cause for Searches and Seizures under the Plain View Doctrine, 78 *J. Crim. L. & Criminology*, pp.763-791.

[8] Office of Legal Education. (2010). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Computer Crime and Intellectual Property Section Criminal Division. Washington: Office of Legal Education.

[9] Katz v. United States, 389 U.S. 347.

[10] Ex parte Jackson, 96 U.S. 727.

[11] Smith v. Maryland, 442 U.S. 735.

[12] Kyllo v. United States, 533 U.S. 27.

[13] Regensburger, D. (2008). Bytes, BALCO, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in United States v. Comprehensive Drug Testing, Inc. *The Journal of Criminal Law and Criminology*, 97 (4), pp. 1155-1208.

[14] United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 57.

[15] Spencer, A. B. (2006). Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts. *University of Illinois Law Review*, 1, pp. 71-126.

[16] Provident Nat'l Bank v. California Federal Sav. & Loan Ass'n, 819 F.2d 434, 437 (3d Cir. 1987)

[17] United States v. Bogachev, U.S. District Court, Western District of Pennsylvania.

[18] EUROPOL, *Joint Cybercrime Action Task Force (J-CAT)* <https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat> accessed on 16 June 2015.

[19] Koops, B.J. (2010), Cybercrime Legislation in the Netherlands. *Electronic Journal of Comparative Law*, vol. 14 (3), pp. 1-33.

[20] De Hert, P. (2010) Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in cyberspace – whose sovereignty is at stake? In Brenner, S. & Koops, B.J. Cybercrime and Jurisdiction – A global survey, TMC Asser Press, The Hague, pp. 71-110.

[21] De Graaf, D., Shosha, A. F. and Gladyshev, P. (2012) Bredolab: shopping in the cybercrime underworld. *Digital Forensics and Cyber Crime*. 4th International Conference, ICDF2C 2012, Lafayette, IN, USA, October 25-26, 2012, Revised Selected Papers, pp. 302-313.

A MULTI-SENSOR TECHNOLOGY FOR IMPROVING SECURITY AT COMPLEX SCENARIOS WITH INCREASED RISK OF VIOLENCE

Frank Pagel[1], Jürgen Moßgraber[1], Carsten Decker[2] and Jan-Peter Germann[3]

[1] *{frank.pagel, juergen.mossgraber}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB)
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[2] *carsten.decker@polizei.bund.de*
Bundespolizei Direktion Bundesbereitschaftspolizei (German Federal Police),
Niedervellmarsche Straße 50, 34233 Fuldatal (Germany)

[3] *jan-peter.germann@polizei.bund.de*
Bundespolizeiabteilung Hünfeld (German Federal Police),
Molzbacher Straße 35, 36088 Hünfeld (Germany)

Abstract

Each weekend, about 3000 federal police officers and additional forces of the state polices secure the fan traffic to and from the stadiums. Sometimes, small groups among the fans are violent and cause dangerous situations for fans and travellers. It is the first obligation of the security forces to detect violent acts and to withdraw offenders. However, for convictions at Court a complete chain of evidence is required. Here, it must be strictly taken care of differentiating offenders from peaceful fans in the crowd. The research project *Muskat* aims at improving the security while respecting the citizens' privacy and fundamental rights. Therefore, a multi-sensor platform will be developed in order to support security forces in the field by tracking single offenders and generating Court proof evidence in a shorter time. This paper presents the activities of the *Muskat* project under technical, legal and ethical viewpoints.

Keywords: Multi-Sensor Cluster, Privacy-by-Design, Tracking, Law Enforcement, Person Retrieval, Information Control Center, Dense Crowds, Evidence Preservation

1 INTRODUCTION

Today, ensuring safety and protection for participants of large events is one of the major challenges of police forces and security agencies. For example, in 2012/2013 about 13 million people attended the matches of the German Bundesliga (first league) which requires more than 3000 officers of the state police alone each weekend in order to guarantee safe events. Unfortunately, small groups among the crowd are violent and cause dangerous situations for participants and unrelated persons, but also for the security personnel. It is the first obligation of the security forces to detect violent acts and to withdraw offenders. However, inflicting penalties for offenders is very difficult, as offenders are often hard to track in the crowd until there is an opportunity for an arrest. Furthermore, for convictions at Court and the preservation of evidence a complete video documentation of the offender from the commitment of the crime until the arrest is required. At the same time, the police need to strictly differentiate offenders and uninvolved people in the crowd, in order to avoid that people will be wrongly accused of being delinquent.

The research project *Muskat* funded by the German Ministry of Education and Research aims at improving the security while respecting the citizens' privacy and fundamental rights. For that purpose, *Muskat* aims at developing a flexible multi-sensor

platform that is supposed to support security forces in the field by tracking single offenders and generating Court proof evidence in a shorter time. A sensor cluster will consist of several static and mobile video cameras, extended by inertial and GPS sensors. Once an offender is tagged on the screen by a police officer, the person will be automatically tracked in the redundant camera network. Video exploitation algorithms for robust person tracking in crowds are explored and implemented. Also, new approaches are investigated that aim at automatically re-identify and retrieve selected offenders in the large amount of video material based on the sensor data in order to support security staff to generate evidence material in a shorter period of time.

Core of such a sensor cluster is the Information Control Center (ICC) which is responsible for the communication between the sensor nodes and the preparation and visualization of the information in a dynamic situation map. Furthermore, *Muskat* aims at developing an interface in order to enable units of the federal and the state police to share and exchange data for a seamless tracking during operation.

All technical developments are closely attended by legal research in order to guarantee a lawful system even from the beginning of the research. The *Muskat* philosophy intends to prosecute only single 'black sheep' instead of supervising the whole crowd: Situational security instead of mass surveillance.

In the following, the project's outline and its technical as well as legal implementation will be presented in detail.

2 THE MUSKAT PROJECT[1]

2.1 Project outline

The project *Muskat* ("Multisensorielle Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen") comprises four full partners, one subcontractor and two associated partners. The project started in 09/2014 with a duration of 3 years. While there are five technical work packages addressing the Information Control Center (ICC), the mobile sensor units, the communication modules, the image processing and the implementation of a demonstrator, the whole project is centered in the legal research in order to make sure at any time of the development that legal requirements are fulfilled. The project is accompanied by ethical studies.

Figure 1: Pictures from the measurement campaigns in 12/2014.

Beside legal guidelines, central output of the project will be a demonstrator, consisting of two sensor clusters. The technical components of the sensor cluster will be described in the next section. This demonstrator will not only be used to show the capability of each technical component, but especially the interaction between these components and their benefit for the security forces in service. Therefore, all end users in the project will perform extensive evaluation tests.

[1] http://www.iosb.fraunhofer.de/?MUSKAT (German version only)

In order to be able to develop algorithms and technologies that meet real scenario requirements, measurement campaigns were planned and executed by the end users where sensor data for the further research could be acquired (see **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Furthermore, one central research goal is the realization of a communication platform for information exchange between clusters of different forces (e.g. between forces of the state police and the federal police). Today, such interfaces do not exist. Hence, the improvement of the communication infrastructure alone would already lead to significant improvements in event management in complex and potentially violent scenarios

2.2 Project goals

Meeting legal and ethical requirements: A complete video documentation of the crime and the offender until her or his arrestment is the fundament for convictions at Court. It needs to be taken care in the system design that all operations are triggered manually by police officers for each individual case. An automatic video surveillance must be explicitly avoided. Person related data must only be acquired for the purpose of risk prevention or law enforcement. In addition, the system must follow the order of differentiation, e.g. minimize of the risk of getting unjustified into the focus of police forces.

Complete preservation of evidence by multi-sensor exploitation: By creating a redundant camera network consisting of mobile (handheld) and static overview cameras, documentation of offenders' tracks can be expected to be much more effective. This requires the investigation of new algorithmic approaches that explicitly consider the sensor configurations and positions in the cluster network. The preservation of evidence and law enforcement will additionally be supported by an offline exploitation of all video and sensor metadata material after the operation. It is one goal of the *Muskat* project to develop a semi-automatic and hence interactive video cutting system that – based on person retrieval algorithms and knowledge about sensor positions and time stamps – supports the selection of relevant video segments that are related to a specifically determined offender. This promising approach can speedup operational post-processing drastically.

Cooperative law enforcement: Due to insufficient existing communication infrastructures at German Federal and State Police, the handover of information between police units is often ineffective, slow or even incomplete. By creating a comprehensive situation visualization and a concept for secure information exchange, *Muskat* aims at closing this gap. The possibility to exchange offenders' profiles between clusters will enable the seamless tracking of offenders and lead to more precise, differentiated and effective law enforcement, which in turn positively influences the legal and ethical compliance of the overall system.

Enabling successful operations under challenging circumstances: There are several reasons that make the earlier described scenarios so challenging for image processing systems. Dense crowds do not allow a complete view of the body. Instead, one has to deal with occlusions, appearance changes, different lighting and weather conditions and high dynamics. In addition, such scenarios are not seldom characterized by uniform clothes of the participants or disturbances like smoke and pyrotechnics (see also Section 4).

2.3 Clusters: A multi-sensor network for effective law enforcement

A Muskat sensor cluster consists of three basic technical components: A mobile sensor unit, an overview unit and the information control center (see Figure 2).

Mobile video cameras are already in use in current operations of police forces. These cameras usually are used to document offenses and to track offenders in the crowd. In Muskat, these mobile sensor units will be extended by additional sensors in order to determine the position and orientation, and hence the geo-referenced field of view of the cameras. Furthermore, each sensor unit is equipped with a communication module that allows the transmission of sensor data to other units. In order to improve the tracking performance in dense crowds, the sensor cluster also consists of cameras that are installed at a height of approx. 3-5m and have a large field of view. It is assumed that (automatic) person tracking in such overview cameras can be done more reliably as with handheld cameras. Furthermore, each sensor cluster will be designed to be dynamically extendable by new sensors (e.g. when two clusters merge), or mobile sensor units can be converted to overview cameras. The core of such a sensor cluster is the information control center, which is described in more detail in the next section.

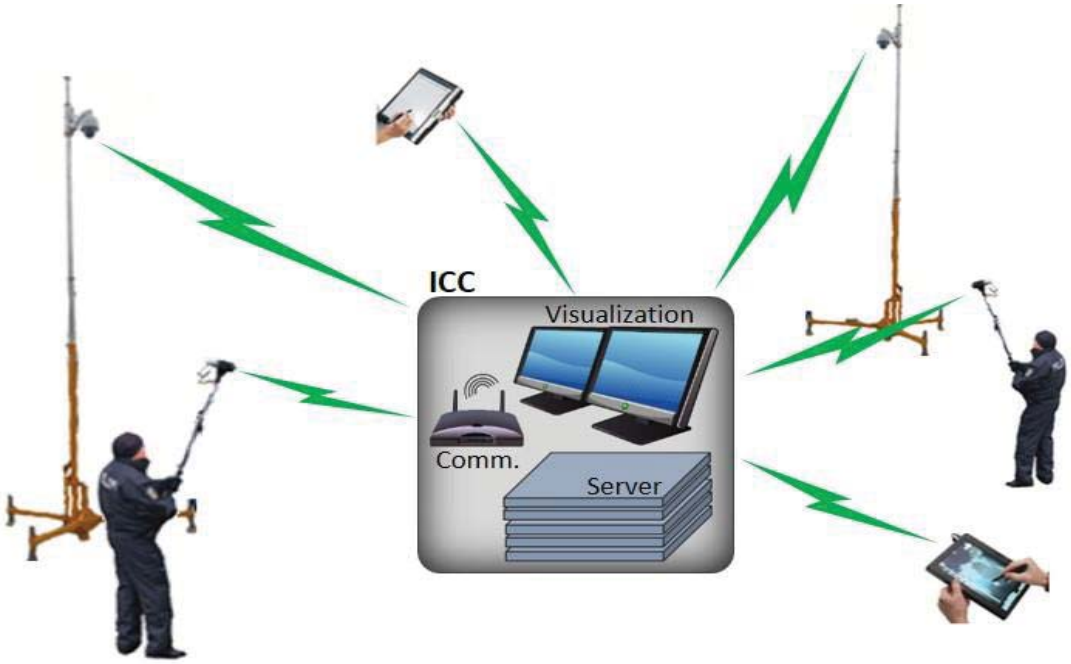


Figure 2: Cluster with handheld sensor units, overview cameras and an information control center, which can also be accessed by mobile devices (read-only).

3 INFORMATION CONTROL CENTER

The Information Control Center (ICC) is responsible for the communication between all sensor nodes (mobile cameras) and the preparation and visualization of the information in a dynamic situation map. Furthermore, necessary manual adjustments and entering of additional information can be done. The ICC stores all data, which is necessary for the preservation of evidence taking into account data privacy and compliance with German law (see section 5).

3.1 Usage during police operation

It provides a web based user interface both for desktop and mobile clients in order to enable units of the federal and the state police to share and exchange data for a seamless tracking during operation.

The current situation is modelled by facilitating an ontology (e.g. see [1]). This is a semantic abstraction of a “part of the world” or a usage domain in our case the combination of the different domains police, law, geo-data, time and the preservation of evidence. From these domains a specific *Muskat* ontology was created, which can fulfill the requirements of the project. Based on the information in the ontology the

visualization of the current situation is created (see Figure 3). On a map, the positions of cameras and tracked offenders are displayed.

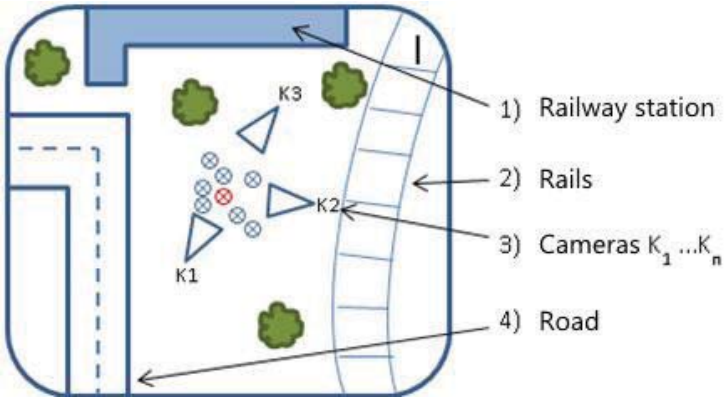


Figure 3: Schematic visualization of a current situation.

An important requirement of *Muskat* is to support the communication and interaction between the German Federal Police (Bundespolizei) and the police of the states (Landespolizei). The former is responsible for providing transportation security (railway) and the later secures the way to and from the stadium. Crimes, which already took place in the train or a railway station, are documented by the Bundespolizei and need to hand over to the Landespolizei to arrest the criminal in a situation where he or she is separated from the crowd (e.g. during entering the stadium). To support this, two ICCs can be connected and transfer the information about a crime.

3.2 Post-processing of police operations

After the police operation, the tracks of offenders and camera positions can be analyzed. With a timeline slider, one can scroll through the changing situation. This can be used for better documentation of a crime situation and provide further information for a trial (see Figure 4).

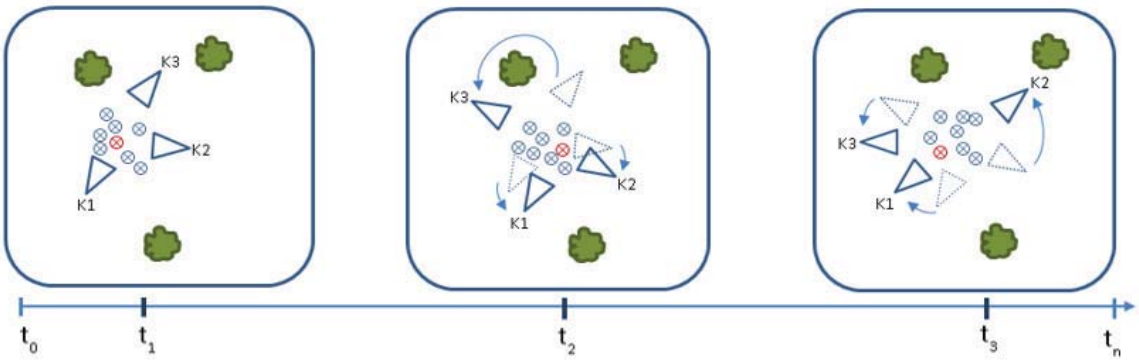


Figure 4: Example of a user interface for post-analyzing a police operation.

4 IMAGE EXPLOITATION

4.1 Tracking of multiple persons in dense crowds

Tracking offenders in the described scenarios is very challenging due to changing appearances and occlusions of the targets, as well as similar clothes and high dynamics among those in the crowd. Therefore, our research of new real-time tracking algorithms focuses on the capability of the tracker to adapt new appearances of target while being robust against high dynamics and short-term occlusions[2]. In this area,

[2] Long-term occlusions might require other algorithmic approaches like person retrieval approaches [xxx].

plenty of approaches already exist in literature [2]-[6], which has been tested, but none of them has proven to cover all requirements in our challenging scenarios. For that purpose, a tracker is being implemented which combines the capabilities of several state of the art trackers: An adaptive (hence learning multiple appearance models [2]), context-based (in particular considering ambient image features [4][5]) and motion-based [3] tracker (ACT)[3] (see Figure 5). Evaluation of ACT will be performed on standard benchmark data sets as well as on data from our own measurement campaigns.

Figure 5: Impressions from our tracking framework (ACT). From top left to bottom right: Tracking window; extracted descriptors in the target area (green), ambient supporting features (red) and distracting features with similar appearances as the object (blue); segmented motion fields; Hough voting space of the target's image position.

4.2 Person-handover between cameras in the sensor network

Each camera in the network is equipped with additional sensors that provide location and orientation in 3D space. We combine image-based person recognition methods with spatiotemporal metadata, in order to handover tracked offenders between cameras, in particular from handheld cameras to overview cameras, which have a more appropriate perspective for tracking purposes. Image-based approaches alone suffer from the significantly different perspectives of the cameras. This is where the metadata is used to narrow down the 3D and hence 2D search space in the respective camera images. Furthermore, we also aim at using image context, based upon the assumption that the relative alignment of significant features in the images (in particular well discriminable and hence easy to match) differ only by the perspective transformation given by the metadata.

4.3 Post-processing person retrieval

The research results of the tracking and person handover will be further used to implement an offline search engine for person retrieval. The purpose of this tool will be to speed up the generation of evidence material. It semi-automatically recognizes and tracks a specific offender in all data streams (including video and metadata) and cuts and stitches the related video files. However, a human operator will have to do all final decisions in order to avoid mismatches during the retrieval process.

[3] More details and results of the tracker itself will be published in the near future.

5 LEGAL AND ETHICAL CONSIDERATIONS

5.1 Legal research

Data security and privacy issues in the context of intelligent, static surveillance camera networks for preventive usage are being discussed in Germany for many years now (e.g. [7]-[10]). These existing works can be used as a basis for the legal research in *Muskat* concerning the combination of static and dynamic cameras in a common network. However, when it comes to the purpose of law enforcement, novel research needs to be done concerning the evidential requirements of the technical components. *Muskat* does not only address the exchange of particulars but also the usability of the captured and explored data at Court.

Concerning the tracking of single persons in a crowd, the fundamental right of self-determination over personal data is highly relevant. The legal research covers the question, how person-related data is used in the use cases. Furthermore, it will be investigated from a legal point of view to what extend measures of risk prevention and law enforcement, respectively, need to be distinguished. At the evidence stage, the Codes of Penal Procedure needs to be investigated with respect to the *Muskat* scenarios and its semi-automatically generated digital evidence. All legal analysis is accompanied by the preparation of proposals for the continuing development of the legal framework in Germany for the usage of a multi-sensor cluster during police operations for the purpose of effective and legal evidence preservation and law enforcement.

5.2 Ethical studies

Most considerations of video systems in public spaces for the purpose of crime prevention and investigations focus on locally static systems (e.g. [11]-[13]). In this context, questions arise about data protection, implications on public life and attending dangers for privacy. The *Muskat* system can be considered a mobile system, which intends preventive as well as investigative purposes and is bound to specific occurrences. These circumstances require new ethical approaches.

Based on the results of the *MuViT*[4] project the *Muskat* system will be analyzed according to two aspects. First, the technology is investigated under ethical viewpoints. This includes considerations of pre-assumptions, manifesting values and questions concerning the identifiability in the scenarios. Second, societal relevant issues are analyzed with respect to specific use case scenarios. Here, implied security issues and acceptability regarding social standards will be discussed and, based on that, alternative solutions will be developed.

6 CONCLUSIONS AND OUTLOOK

The *Muskat* project will end in September 2017. A first version of the demonstrator will be presented in early 2016, where all technical components will be integrated and the capability of each single component will be demonstrated. The second half of the project focuses at optimizing the components with respect to their interaction and usability, fulfilment of legal requirement and realization of a data exchange between two clusters. A final measurement campaign is planned in early 2017.

ACKNOWLEDGEMENT

The research project *Muskat* is funded by the German Ministry of Education and Research (BMBF).

[4] http://www.bmbf.de/pubRD/Projektumriss_MuViT.pdf (project description only available in German)

REFERENCES

[1] J. Moßgraber, M. Rospocher, *Ontology Management in a Service-oriented Architecture*, Int. Workshop on Web Semantics and Information Processing (WebS), 2012.

[2] Xu Jia, Huchuan Lu, Ming-Hsuan Yang, *Visual Tracking via Adaptive Structural Local Sparse Appearance Model*, In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012.

[3] S. Stalder, H. Grabner, and L. Van Gool, *Dynamic Objectness for Adaptive Tracking*, In Proceedings of the IEEE Asian Conference on Computer Vision (ACCV), 2012.

[4] H. Grabner, J. Matas, L. Van Gool, and P. Cattin, *Tracking the Invisible: Learning Where the Object Might be*, In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2010.

[5] T. B. Dinh, N. Vo, and G. Medioni, *Context Tracker: Exploring Supporters and Distracters in Unconstrained Environments*, In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2011.

[6] J. Metzler, D. Willersinn, *Robust tracking of people in crowds with covariance descriptors*, In SPIE Defense and Security 2009: Visual Information Processing XVIII. 2009.

[7] C. Post, *Polizeiliche Videoüberwachung an Kriminalitätsbrennpunkten: zugleich eine Untersuchung des § 15 a PolG NW*, Hamburg: Kovač, 2004.

[8] A. Roßnagel, G. Hornung, M. Desoi, *Gestufte Kontrolle bei Videoüberwachungsanlagen. Ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung*, DuD 2011, pp 694-701, 2011.

[9] C. Bier, I. Spiecker gen. Döhmann, *Intelligente Videoüberwachungstechnik: Schreckensszenario oder Gewinn für den Datenschutz?* CR 2012, pp 610-617.

[10] G. Hornung, M. Desoi, *"Smart Cameras" und automatische Verhaltensanalyse. Verfassungs- und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung*, Kommunikation & Recht 2011, pp 153-158, 2011.

[11] Haggerty, K. and Ericson, R., *The New Politics of Surveillance and Visibility*, Toronto: University of Toronto Press, 2006.

[12] Lyon, D. (ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, London and New York: Routledge, 2003.

[13] Norris, C. and Armstrong, G., *The Maximum Surveillance Society: The Rise of CCTV*, Oxford: Berg, 1999.

CAMERA TECHNOLOGY FOR BEHAVIOURAL PROFILING AT AMSTERDAM AIRPORT SCHIPHOL

G.J. Burghouts, J-M ten Hove, B. van den Broek, J. Baan, R. den Hollander, K. Schutte, E. Zwier[1] and R.J. Ebbelink, J.J.M. de Moel, R. van der Kamp, K. Weijers[2] and W. van 't Hooft[3]

[1] *eddy.zwier@tno.nl*
TNO, Intelligent Imaging, The Hague (The Netherlands)

[2] *r.vd.kamp@mindef.nl*
Royal Netherlands Marechaussee, Koningin Maxima Kazerne, Schiphol (The Netherlands)

[3] *wim@qubit.nl*
Qubit Visual Intelligence BV, The Hague (The Netherlands)

Abstract

At Amsterdam Airport Schiphol, innovative technology is developed to support automated predictive behavioural profiling of deviant behaviour from CCTV camera footage. The Royal Netherlands Marechaussee expects predictive behavioural profiling to become a valuable asset to performing its tasks in the near future.

Keywords: behaviour profiling, camera technology, tracking of people, action recognition, behaviour analysis

1 INTRODUCTION

A global trend is the increasingly widespread use of cameras to combat crime in areas under surveillance, such as airports, inner cities, shopping malls and public transport. Both government and the private security sector are investing heavily in surveillance and, as a consequence, cameras and surveillance control rooms are on the rise. An increase in the number of cameras, however, is not always accompanied by an increase in the number of staff watching incoming material. Additional images are distributed among existing staff and they have to view more and more footage. This prompts the question of how they can watch all the footage sufficiently closely and yet still guarantee security.

With social pressure to prevent incidents the focus has shifted from investigation, to caught in the act and towards prevention. This implies that the pressure to correctly predict incidents on the basis of deviant behaviour is also rising. Deviant behaviour is all behaviour that precedes and is related to undesirable activities such as fighting, terrorism, pick-pocketing and dealing. Thus, deviant behaviour refers not only to the incident itself but also to the behaviour that precedes the offence. This paper describes a software technology that automatically analyses and detects such behaviour in video. The use of our technology is expected to improve efficiency and effectiveness in the following ways:

- Many cameras can be monitored automatically. When deviant behaviour occurs, a signal can be given automatically to the camera operator or other security officers. This increases the opportunity for proactive intervention, which may prevent a possible offence.

– The video images are tagged automatically (time, date, camera number, location and type of deviant behaviour), which makes the analysis and retrieval of relevant video much easier and faster.

At Airport Amsterdam Schiphol, our objective is to recognise typical behaviour that occurs around luggage theft, to recognise unattended luggage and to recognise situations that occur when people suddenly collapse for example due to a heart attack or faint. These situations are relevant to the duties and tasks of the Royal Netherlands Marechaussee.

The state-of-the-art in behaviour recognition has not yet achieved to yield good performance for the subtle, complex behaviours such as theft in a complex environment like an airport. In complex environments, simple human actions such as running through an airport can be recognised with high accuracy by recent methods. Complex behaviours, such as baking a cake, which involves many constituent actions and several interactions with objects, can be recognised in simple environments, such as one person in a kitchen. The combination of a complex environment and complex behaviours is our aim. The recognition software has been developed using the existing security cameras currently already operational at the airport. Developments presented in this paper are inspired by numerous recordings of incidents. Experiments have been performed on recordings from red teaming events.

The basis of the innovation is a multidisciplinary approach which combines gamma and beta sciences, by integrating in-depth knowledge about human behaviour and state-of-the-art video technology respectively. The key innovation of the technology is that the software analyses the many subtle and complex facets of human behaviour: movement patterns, interactions between persons, involvement of objects, and interactions with the environment. The behaviour scientists have defined the various behavioural characteristics. The technologists have developed the algorithms to capture these characteristics in the video data. This software finds the specific patterns that can be associated with crime offenders, their victims, and their interplay.

The organisation of the paper is as follows. Section 2 discusses the state-of-the-art of video technology for behavioural profiling. Section 3 describes our approach for the automated recognition of crimes and incidents and presents the novel video technology. In Section 4 the performance of the technology is evaluated and several sample detections are shown. Section 5 summarizes the approach, technology and results.

2 STATE-OF-THE-ART

Three core research areas are relevant to the innovation that is discussed in this paper: tracking of people, action recognition, and behaviour analysis. Tracking recently gained in maturity with live demonstrations in realistic crowded environments. For action recognition and automatic behaviour recognition, we observe that the simple patterns, such as loiter detection, are emerging in many applications. Human action recognition obtains very high performance values in controlled environments and it is progressing towards more realistic environments. More advanced approaches, such as pickpocket recognition in a shopping mall and the detection of threats to trucks on a parking lot have been developed and the first systems have been presented in live demonstrations.

Commercially available software can detect persons and vehicles in video, as well as relatively simple actions such as: person passes line and person enters area. The presented technology represents a huge step forwards and makes it possible to recognise the subtle and complex human behaviours that are related to crimes.

The reason why we consider these behaviours complex, is because the behaviours vary significantly, they happen in the midst of many other people with normal behaviour which also varies significantly, the circumstances such as crowdedness are of influence and also these are changing continuously. Moreover, it is typically insufficient to recognise a single behaviour in order to recognise a crime. Many of the individual behavioural elements of a crime are in themselves not a definite cue. For instance, with luggage theft, the combination of victim and offender cues are distinctive. Individual elements such as a person standing still for some time may just as well be an offender on the lookout, or just somebody waiting for a friend or reading an email on a smartphone. The objective in this paper is to search for distinctive patterns in video streams to recognise crimes, by analysing various behavioural characteristics, combining them, and analysing the interplay between victim and offender.

3 AUTOMATED RECOGNITION OF CRIMES AND INCIDENTS

For our developments, we have first analysed the crimes and the incidents at Airport Amsterdam Schiphol, and which behavioural characteristics define them. The crimes and incidents under investigation are luggage theft, unattended luggage and people who suddenly collapse. After identifying the behavioural characteristics, the software has been tuned to search for them. It analyses the many subtle and complex elements of human behaviour: movement patterns, interactions between persons, involvement of objects, and interactions with the environment. The discriminative power of the software arises from the combination of various elements of behaviour.

Collapsing is a combination of slowed pace of walking and then falling down. Therefore, this is measured in the video stream by analysing both the person's trajectory and the pattern of downward motion which ends abruptly.

Leaving unattended luggage behind, may happen with or without intent. In both cases, there are behavioural cues before the moment of leaving the object behind. In both cases, the object is with the owner for a while, then placed by a person, who finally abandons it. Current commercial software aims to recognise unattended luggage by searching for significant changes in the scene, which may relate to left luggage, or by detecting particular shapes. These appearance cues are not sufficient, because there are many changes in the scene that are not related to unattended luggage, including moving people, banners, TV screens, clouds, sunlight, etc. Our software complements the appearance cues with the behavioural cues before, during and after the activity of leaving the luggage.

Theft of luggage involves a victim and an offender, and they have an interaction (of which the victim is often unaware). The offender needs to approach the victim, getting nearby, reaching for the object of interest, and taking it away. The victim is often relatively stationary while the offender takes the object. Our software searches for this interaction in three steps. First, we search for small pieces of visual evidence of potential offenders in one of the states of the theft. Second, in a similar way, we search for small pieces of visual evidence of potential victims. Third, we search for spatiotemporal combinations of these pieces of visual evidence, raising an alert only when sufficient behavioural characteristics of a theft have been observed.

4 REAL-TIME DETECTIONS AT THE AIRPORT

The software has been developed by means of actual recordings and red-teaming at the airport. The incidents are: theft, unattended luggage, and sudden collapse. During the red teaming experiments, each of the incidents was repeated 50 times, recorded by one camera at one of the most crowded locations at the airport. The experimental setup is a leave-one-incident-out cross-validation, where for each fold 49/50 is taken

from the background by randomly selected five-minute blocks. Several results are shown in the next subsections by means of snapshots. At the conference, we will show more results of the behavioural profiling software during the oral presentation. In addition, the performance will be indicated by means of true and false positive rates, at a selected operating point where the true positive rate is 50% or higher and false positives per hour are less than 10. This operating point is selected by setting a particular threshold. The user can adapt this threshold to increase or decrease the number of hits, if operating conditions require this. For instance, when intelligence indicates a high risk for any incident, this threshold may be lowered.

4.1 Theft

The true positive rate is 70%, at a false alarm rate of 10 per hour. Illustrations are shown in Figure 1. In Figure 1a, the left image shows the video frame and the probability and the right image shows the ground truth. Two theft incidents are correctly detected. First, a case on the left in the image, where the man with the brown jacket steals a bag. Second, a case on the right in the image, where the man with the bag pack steals a bag. In Figure 1b, two false positives are shown. First, the man with the green jacket who is airport personnel. He is taking a lost bag from the ground, which is accidentally interpreted as theft. Second, two men standing close to somebody with a luggage cart and loitering close to it, erroneously interpreted as theft.

Figure 1a. True positives of theft (examples).

Figure 1b. False positives of theft (examples).

4.2 Unattended luggage

The true positive rate is 50%, at a false alarm rate of 5 per hour. Illustrations are shown in Figure 2.

Figure 2a. True positives of unattended luggage (examples).

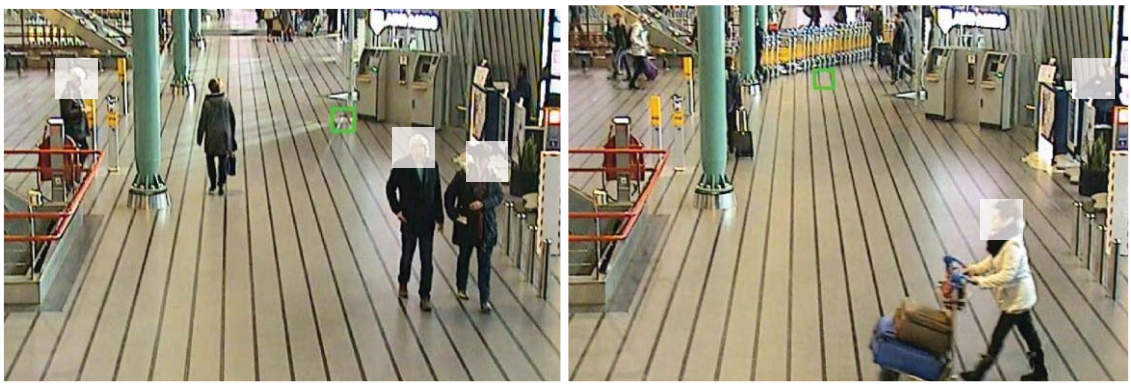


Figure 2b. False positives of unattended luggage (examples).

4.3 Sudden collapse

The true positive rate is 60%, at a false alarm rate of 8 per hour. Illustrations are shown in Figure 3.

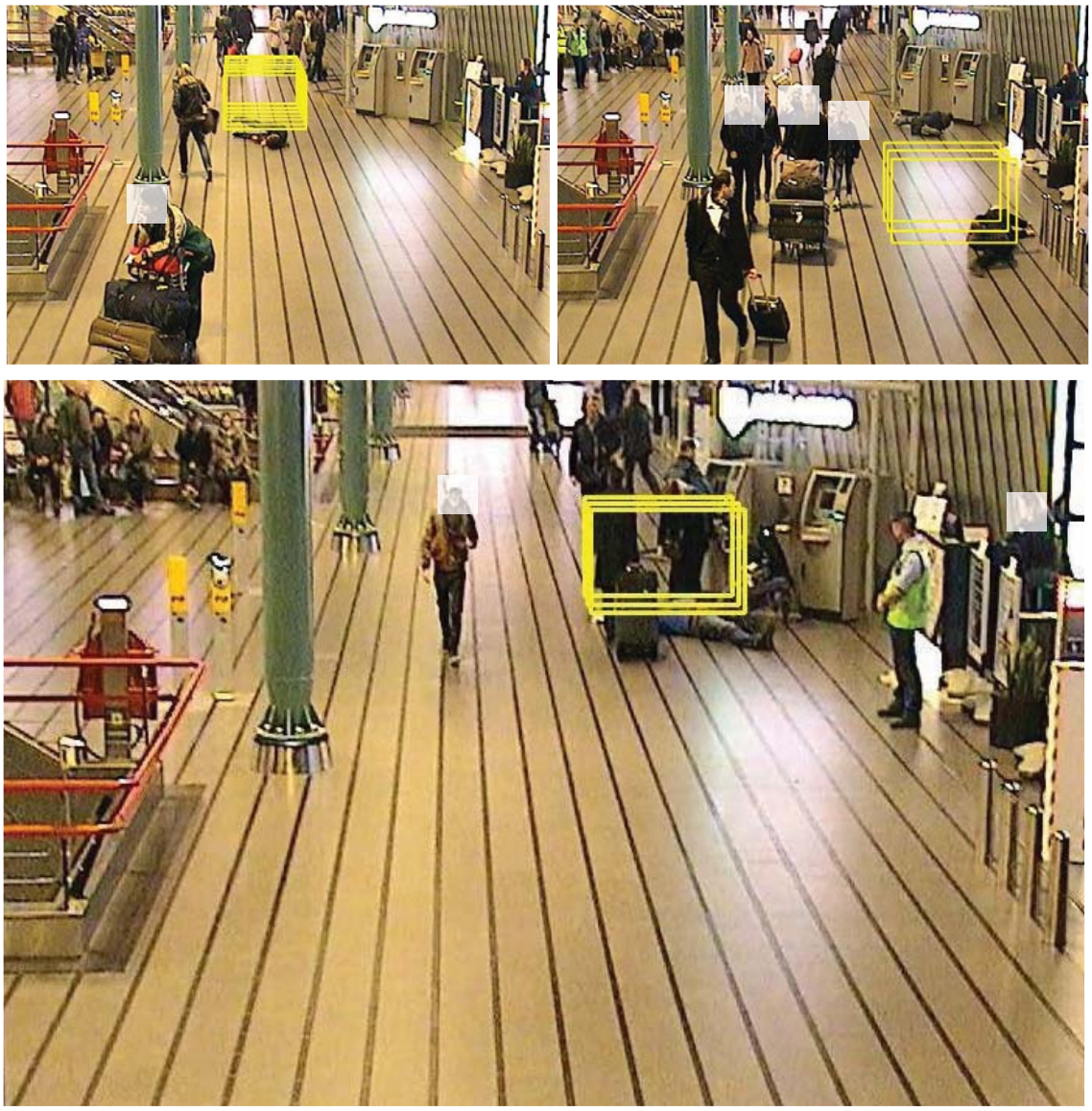


Figure 3a. True positives of collapse (examples).

Figure 3b. False positives of collapse (examples).

5 SUMMARY

The innovation presented in this paper, is that we developed behavioural profiling software to detect realistic incidents at the airport, including theft, unattended luggage, and sudden collapse. The software finds the specific patterns that can be associated with offenders and victims and their interplay. The presented technology will assist in the detection of objects and behaviour, i.e. no changes will be made to the approach, tasks and powers of security professionals. The operator in the control room monitoring the live streams from various camera positions will, where possible, be automatically alerted and referred to the specific footage of the actual occurring incidents. We project that this enables quicker response times for emergency services. This may increase life-saving capabilities and crime prevention.

ACKNOWLEDGEMENTS

The project, named HARVEST (Human Activity Recognition in VidEo STreams) is supported and co-funded by the Netherlands Ministry of Security and Justice's [Secure] through Innovation program.

KNOWLEDGE-BASED SITUATIONAL ANALYSIS OF UNUSUAL EVENTS IN PUBLIC PLACES

David Münch, Stefan Becker, Hilke Kieritz,
Wolfgang Hübner and Michael Arens

david.muench@iosb.fraunhofer.de

Fraunhofer Institute for Optronics, System Technologies and Image Exploitation IOSB,
Gutleuthausstraße 1, 76275 Ettlingen (Germany)

Abstract

Combining appropriate methods from computer vision and artificial intelligence enables further progress in smart video surveillance. In this work, an Interacting Multiple Model (IMM) filter is used for person tracking due to the fact that a single motion may not capture the complex dynamics from persons. In addition, context information from the IMM is used for controlling the background model to detect left luggage. The combination of this processing chain serves as input for the situation recognition in addition to person detection and tracking.

The computer vision components are integrated in the distributed Cognitive Vision System (dCVS) architecture, which is applied up to now to Traffic, Robotics, Smart Homes, and Video Surveillance. For this work, we cope with situations dealing with unusual events in public places.

Keywords: left luggage detection, video surveillance, situation recognition.

1 MOTIVATION

The combination of suitable methods from both computer vision and artificial intelligence enables further progress in smart video surveillance. Supporting the surveillance operator with significant cues of unusual events, such as left luggage, is a huge step towards more situational awareness.

Methods establishing situational awareness are dependent on lower level computer vision components providing the necessary raw input data such as person detection, person tracking, change detection, or object detection, see e.g. Figure 1.

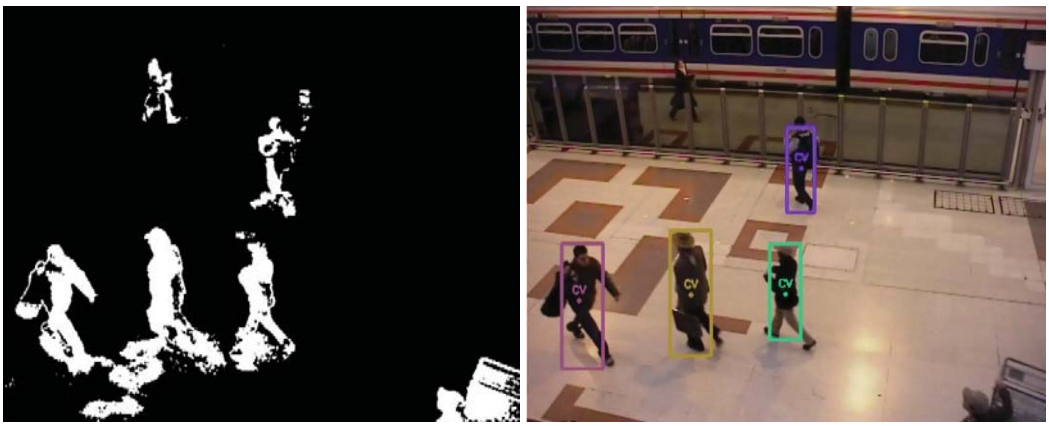


Fig. 1. Background subtraction (left) and person detection & tracking (right). All people are moving and are in a “constant velocity”-state.

In this paper, we integrate reliable computer vision components: person detection, person tracking, and left luggage detection with high-level semantic video understanding. The components are plugged into a distributed architecture to satisfy real practical needs in a working environment of video surveillance.

1.1 Related Work

The survey papers [1], [2], [3], [4], and [5] provide a broad overview about the recent field of situation recognition in video surveillance. The strategies to deal with the problem to extract meaningful semantic information from raw image sequences can be divided into different approaches. On the one hand, there are the direct approaches making use of massive machine learning support. They work in principal as a black box where the input image sequence is fed in, and without exactly knowing how these images are processed, the black box results the recognized situations. On one side, these methods work quite good in limited scenes, on the other side their success is mostly dependent on a huge amount of training data.

On the other hand, there are hierarchical approaches. They divide the problem into several layers in which different subproblems are addressed. Among them, there are statistical approaches [6] making use of graphical models and other probabilistic methods. It is a smart theory, in contrast to complex modelling and expensive inference. Syntactical approaches, such as formal grammars [7], are easier to model but less flexible for complex situations. Description-based approaches do not rely on training data; instead, they are based on expert knowledge and background knowledge. Their basis is mostly formal, such as higher order formal logic etc. Knowledge about spatial, temporal, and abstract properties is formulated and is available for inference during the process of recognizing situations [8], [12].

Fig. 2. Person detection & tracking: One challenge is to detect and track the corresponding height resolution of each person.

2 COMPUTER VISION COMPONENTS

In the following section, the computer vision components used in this work are explained.

2.1 Person detection

In any person centric scenario, a person detection method is a core component. As every other subsequent step is based on the person data, it has to provide robust, reliable, and coherent results. The person detection is based on [9], [10], and [11].

Person detection consists of three steps:

1. Pre-processing for generation and transformation of meaningful features.

   In our case, ten feature maps are generated, including colour maps, gradient, and gradient orientations.

2. Classification with a soft-cascade and sliding window multi-scale approach.

   For this work, the classifier instead of the image is scaled. This has two advantages: First, no recalculation of features, second, learning the classifier on different scales lets the classifier learn to deal with unpredictable artefacts at different scales.

3. Post-processing to identify the detected person with a non-maxima suppression.

Training of the person detection method is done with two disjoint data sets to avoid the problem of overfitting. One data set (training) is used for setting the parameters of the weak classifier and the other data set (validation) is used for defining the soft-cascade thresholds.

Figure 1 (right) and Figure 2 depict the result of person detection (and tracking). Challenges in the person detection step are different view angles of the person (Figure 1 (right)) and a large variance of the distance of persons to the camera and consequently their resolution in image space (Figure 2).

Directly from person detection (and tracking) simple events can be inferred. There are e.g. person pass-through, person counting, and intrusion detection.

2.2 Person Tracking & Left Luggage Detection

In recent years, many methods have been proposed for automatically detect abandoned objects in video surveillance. These methods not only differ in their desired application, but in addition, how such an event is defined. In this work, we use the approach of Becker et al. [13] for automatically detecting left luggage in surveillance scenarios. Similar to [14] a left luggage sets a split from a person as a prerequisite. One processing stage is the detection and tracking of persons in order to detect a drop-off event from a non-human, static object. One way for detecting a change of static

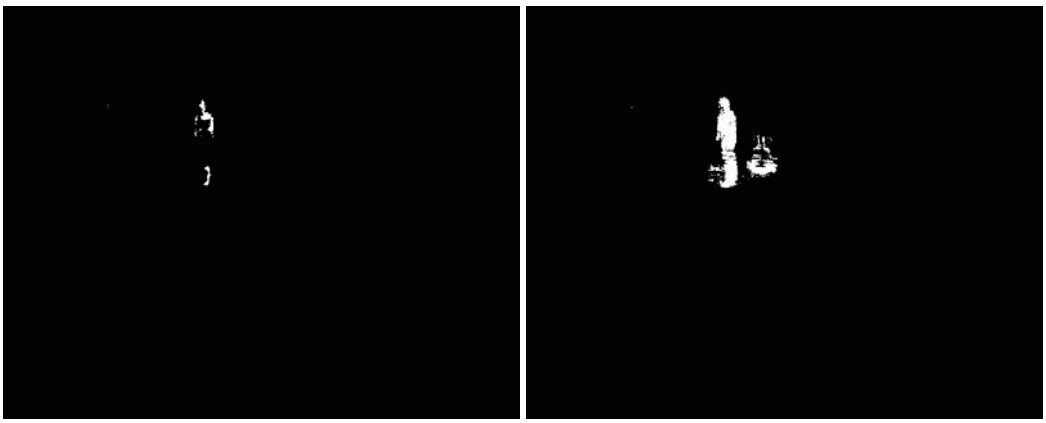


Fig. 3. Foreground masks obtained from the background subtraction algorithm with (right) and without context information (left).

object in the scene caused by such an event is to compare long-term and short-term background models with different learning rates. Instead of using such dual background models, the used approach relies on the state estimate of the dynamics of a tracked person for controlling the pixel-wise update probabilities of one non-parametric background model. The approach of Hofmann et al. [15] serves as basis for the background model. There, the background is modelled by a history of recently observed pixel values. Not only a dynamic controller controls the foreground decision, also the background update is based on a learned per-pixel state variable. As mentioned, here the background update is in addition combined with the person state estimate. This combination prevents that objects carried by person are too fast integrated in the background model. Hence, the per-pixel update probability depends on a measure of the pixel dynamics and on the person dynamics. In a region close to a person, the update probability is decreased, when the person is in a standing or loitering state. In contrast, the update probability is not changed in cases where the person is for example in a fast moving state.

Figure 3 shows an example image of a resulting foreground masks in case of a slowly moving or rather standing person with and without context information. On the left the original image is shown, in the middle the resulting foreground mask obtained with no tracking information is shown, and on the right with context information. When the tracking state is not used, the person and the carried object are almost fully integrated in the background model. Another major part of this processing pipeline consists of determining the context information for the used context aware pixel-based adaptive segmenter. In order to differ between persons that stand still, walk, or run is important to use several motion model to describe such varying characteristic and to consider that the motion model of a person can change over time. For modelling the different motion states of person and simultaneously better capture the complex dynamics of a person, an Interacting Multiple Model (IMM) filter [16] is used. IMM filter are a popular choice for estimating systems, whose model changes according to a finite-state, discrete-time Markov chain. IMM filter can also be used in situations, in which its parameters are estimated from a set of candidate models, and hence it can be also used as a method for model comparison [17]. In our experiments, we used a set of three different motion model. A constant position, a constant velocity, and a constant acceleration model. The IMM filter consists of three major steps: interaction (mixing), filtering, and combination. Under the assumption that a particular model is the right model at current time step, the initial conditions for this model is obtained by mixing the state estimates produced by all filters. Then a standard Kalman filtering is applied for each model. Followed by computing the weighted combination of all updated state estimates. This yields to the final state estimate and covariance in that particular time

Fig. 4. (Left) Sample input image. (Right) Example of detected abandoned object. (PETS2006 dataset; S1-T1).

step. The weights are chosen according to the probabilities of the models, which are computed in filtering step of the algorithm. For more details on the IMM Filter, we refer to the work of Bar-Shalom et al. [16] or Blom et al. [18]. The states of our IMM filter are the image space coordinates and the height of the person bounding box. In case that the constant position model is the best fitting model for a current time step. The current states is used to define a region of interest and conduce as context information for a background model. Further, the tracking id is assigned to this region. Hence, a unique assignment between possible left object and the responsible person is achieved. As mentioned above, a too fast integration of a standing person and his carried object in to the background model is avoided. When a person leaves its assigned region of interest, which is associated with a switching from a standing state to a walking or running state, the detected foreground pixels are used to trigger an alarm event. In our experiments, an alarm event is triggered when a person leaves its assigned region of interest for a defined time interval and the number of detected foreground pixels inside this region exceeds a threshold. Figure 4 shows exemplary the result of detected left luggage event in PETS2006 dataset [19]. The detected left luggage is highlighted with red. The tracked persons are marked with a bounding box.

3 ARTIFICIAL INTELLIGENCE MODULES

The computer vision components above are integrated in the distributed Cognitive Vision System (dCVS) architecture [12], which is applied up to now to Traffic, Robotics, Smart Homes, and Video Surveillance. The dCVS consists of different levels; in the Contextual Level (CL) reasoning, situational analysis, visualization, and evaluation is done. Expert knowledge encoded as Situation Graph Trees and Fuzzy Metric Temporal Logic is used as knowledge base. In between of the CL and the Quantitative Level (QL) a persistence layer cares about communication between the different computer vision modules from the QL and the CL. At the bottom in the Interactive Subsystem raw sensor data, such as video data from cameras, is processed and passed to the QL.

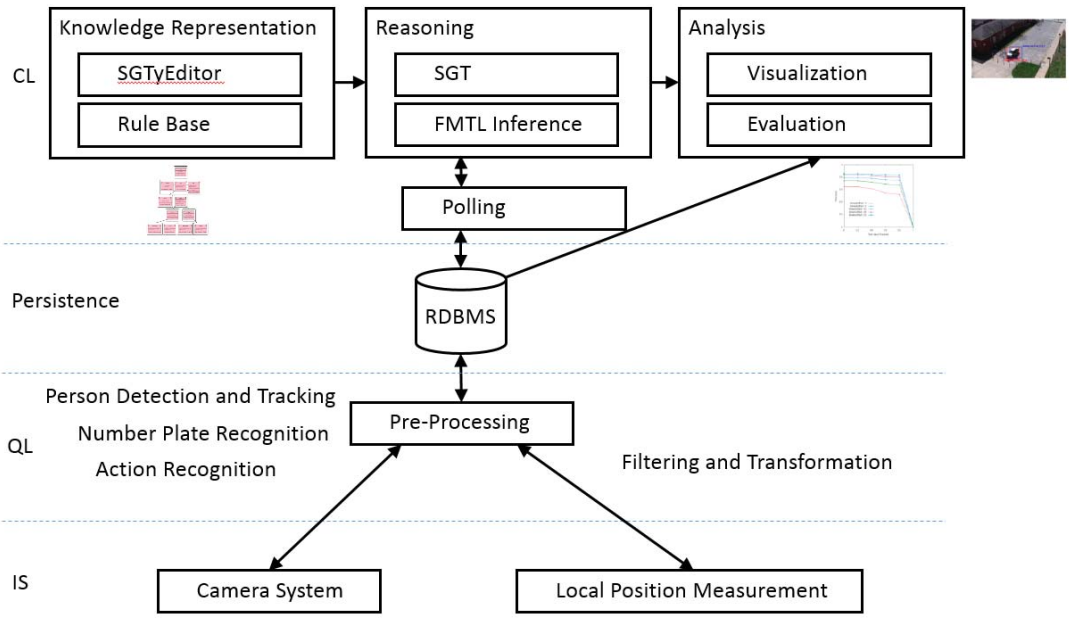


Fig. 2. Concrete instantiation of the dCVS.

Some simpler situations can be detected with the computer vision modules. These situations are usually single person/object related and based on the position and its

derivatives. Such situations are walking, running, pass-through, counting, intrusion detection, left luggage detection. Whereas using high-level semantic support, such as the dCVS, raises the capability to recognize much more complex situations. In the following, we will discuss the components of the dCVS and its consequences.

The dCVS is a modular architecture for (computer-vision-based) situation recognition. This property makes it universally applicable in any kind of surveillance task. E.g., any of the computer vision modules in the QL can be exchanged, added, or changed, such that the computer vision modules fit to the application at hand. In a practical environment (with an existing infrastructure), there is need for a consistent information basis for the situation recognition in CL. This is achieved with a persistence layer, where all results from QL are stored and subsequently passed to CL.

The logic based inference system in CL can use background knowledge in different kind of formats. On the one hand, there is basic knowledge “the physics of this world” which is provided as logical formulas. On the other hand, there is higher-level knowledge, which is provided via situation graph trees. In this structure, knowledge of the expected situations of the agents in an observed scene can be exhaustively modelled.

The combination of both allows inferring about the completely observed scene with all its persons and objects. At this point interactions and group situations can be detected because every single-person property can be put in context.

4 CONCLUSION

This work focuses on combining suitable computer vision components for high-level situation recognition. The contribution of this paper is the concrete set of computer vision modules into the dCVS architecture to deal with indoor surveillance scenarios. The computer vision modules in conjunction with the dCVS allow an exhaustive situational analysis for better supporting surveillance operators.

REFERENCES

[1] Turaga, P., R. Chellappa, V. S. Subrahmanian, and O. Udrea (2008). *Machine Recognition of Human Activities: A Survey*. IEEE Transactions on Circuits and Systems for Video Technology.

[2] Lavee, G., E. Rivlin, and M. Rudzsky (2009). *Understanding Video Events: A Survey of Methods for Automatic Interpretation of Semantic Occurrences in Video*. IEEE Transactions on System, Man, and Cybernetics, Part C: Applications and Reviews.

[3] Aggarwal, J. K. and M. S. Ryoo (2011). *Human Activity Analysis: A Review.* ACM Computing Surveys.

[4] Vishwakarma, S. and A. Agrawal (2012). *A survey on activity recognition and behavior understanding in video surveillance*. The Visual Computer.

[5] Ye, Juan, Simon Dobson, and Susan McKeever (2012). *Situation identification techniques in pervasive computing: A review*. Pervasive Mob. Comput.

[6] Fischer Y. and J. Beyerer (2012). *Defining dynamic Bayesian networks for probabilistic situation assessment.* Proceedings of the 15th International Conference on Information Fusion (FUSION).

[7] Aloimonos, Y., G. Guerra, and A. Ogale (2009). *The language of action: a new tool for human-centric interfaces*. In Human-Centric Interfaces for Ambient Intelligence.

[8] Ryoo, M. and J. Aggarwal (2009). *Semantic Representation and Recognition of Continued and Recursive Human Activities*. International Journal of Computer Vision.

[9] Dollár, Piotr, Serge Belongie, and Pietro Perona (2010). *The Fastest Pedestrian Detector in the West.* BMVC.

[10] Benenson, Rodrigo, et al (2013). *Seeking the strongest rigid detector*. Computer Vision and Pattern Recognition (CVPR).

[11] Kieritz, H., W. Hübner, and M. Arens (2013). *Learning transmodal person detectors from single spectral training sets.* SPIE 8901A Optics and Photonics for Counterterrorism, Crime Fighting and Defence.

[12] Münch D., A.-K. Grosselfinger, H. Kieritz, W. Hübner, M. Arens (2014). *Architecture for and Evaluation of Situational Analysis in the Real World*. Proc. of the 9th Future Security Research Conference, Berlin, Germany.

[13] Becker, S., D. Münch, H. Kieritz, W. Hübner, and M. Arens (2015). *Detection of abandoned objects based on interacting multiple models* Proc. SPIE Volume 9652 Optics and Photonics for Counterterrorism, Crime Fighting, and Defence.

[14] Ferrando, S., G. Gera, and C. Regazzoni (2006). *Classification of unattended and stolen objects in videosurveillance system.* International Conference on Advanced Video and Signal based Surveillance (AVSS).

[15] Hofmann, M., P. Tiefenbacher, and G. Rigoll (2012). *Background segmentation with feedback: The pixel-based adaptive segmenter.* Conference on Computer Vision and Pattern Recognition Workshops (CVPRW).

[16] Bar-Shalom, Y., T. Kirubarajan, and X.-R. Li (2002). *Estimation with Applications to Tracking and Navigation.* John Wiley & Sons, Inc., New York, NY, USA.

[17] Li, X. and V. Jilkov (2005). *Survey of maneuvering target tracking. part v. multiple-model methods*. IEEE Transactions on Aerospace and Electronic Systems.

[18] Blom, H. and Y. Bar-Shalom (1988). *The interacting multiple model algorithm for systems with markovian switching coefficients.* Transactions on Automatic Control.

[19] *PETS, International workshop on Performance Evaluation of Tracking and Surveillance*. (2006). (see http://www.cvg.rdg.ac.uk/PETS2006/index.html).

ACOUSTIC EVENT SOURCE LOCALIZATION SUPPORTING A VIDEO SURVEILLANCE SYSTEM

Peter Transfeld[1], Uwe Martens[2], Harald Binder[2], Thomas Schypior[2], and Tim Fingscheidt[1]

[1] *{transfeld, fingscheidt}@ifn.ing.tu-bs.de*
Institute for Communications Technology, Technische Universität Braunschweig, Schleinitzstr. 22, 38106 Braunschweig (Germany)

[2] *{uwe.martens, harald.binder, thomas.schypior }@artec.de*
artec technologies AG, Mühlenstr. 15-18, 49356 Diepholz (Germany)

Abstract

This contribution presents a robust approach to acoustic event source localization for surveillance under reverberant environmental conditions. In particular, we support the classical generalized cross-correlation algorithm with phase transform weighting (GCC-PHAT) and the steered response power (SRP) algorithm by a sound activity detection and an event onset detector. The proposed algorithmic framework including spatial minimum tracking and smoothing for the suppression of artifacts in the spatial likelihood function significantly outperforms respective reference frameworks, decreasing both the miss ratio by about 9% absolute, and the average angular estimation error by about 4°.

Keywords: acoustic event source localization, surveillance, reverberant environment, onset detection

1 INTRODUCTION

Acoustic source localization and acoustic speaker localization have been intensively investigated in the last years. In several aspects, the knowledge of the position of speakers or sound sources can be useful and is consequently employed within a wide range of applications. In teleconferencing and videoconferencing the speaker's position can be exploited by steering a microphone beamformer or automatically pointing a camera at him [1]. These two applications can be as well found in the field of smart rooms, where the room itself is aware of the people inside it [2]. As well, these techniques can be used for security aspects [3].

There are a considerable number of acoustic sound source localization methods. Most common is the estimation of the time difference of arrival (TDOA) between two microphone signals. A state-of-the-art TDOA estimation approach is the generalized cross-correlation (GCC) method, which is based on the cross-correlation between two microphone signals. Within this method several weighting factors can be employed, from which the phase transform (PHAT) [4] gives good results under reverberant conditions [5]. To improve the resulting position estimate, optionally, one can make use of the steered response power algorithm (SRP) [6]. Another option is to employ acoustic beamforming and exploit the directional pattern of a microphone array [7].

In reverberant environments the precision of the position estimate may severely be affected by sound reflections. Highest precision can be achieved in the moment once the direct sound arrives at the microphone, which requires then to detect the onset of an acoustic event. Onset detection is used in several research fields. Two typical application fields are musical analysis using phase- and energy-based onset detection [8], and auditory scene analysis, using onset detection for audio segmentation [9].

In our present work we recapitulate and rearrange the approach presented in our previous publications [10, 11] to obtain a framework suitable for acoustic event localization

with a *microphone array* in a far-field context. The technique is used for surveillance purposes, where the task is to estimate an event sound source location and then steer a camera to it. The acoustic event source localization presented in this paper shall augment respective image-based processing for higher robustness in bad visual conditions. As in this work the sound source has to be located in the far field, a further step is to change the geometry behind the computational framework to a *spherical coordinate* search space. In addition, we simplify the noise floor estimation in the computation of the total spatial likelihood function towards a *minimum statistics* approach. Furthermore the simple time-domain voice activity detection is replaced by a frequency-domain *sound activity detection* (SAD) and an *event onset detection* (EOD).
The organization of the paper is as follows: In Section 2 we briefly revisit the GCC-PHAT and SRP methods, present the employed algorithms, and the new search space. Section 3 details our new event onset detection, the spatial filtering and smoothing process. In Section 4 the evaluation methodology is presented and the results are analyzed. Section 5 then gives final conclusions.

2 BASELINE ALGORITHMIC APPROACHES

2.1 Signal Model

Given a room, and a rectangular microphone array with a camera placed in the array center. The position of the acoustic event sound source which shall be localized is assumed to be in the camera's field of view. The array consists of M microphones $\mu \in \mathcal{M} = \{1,2,\dots,M\}$, providing output signals $y(t)$. The microphones are equidistant and located at positions $\boldsymbol{r} = (r_{x\mu}, r_{y\mu}, r_{z\mu})^T$, respectively, with $()^T$ being the (vector) transpose. The array center is in the origin $\boldsymbol{r} = 0$. From a sound source position $\boldsymbol{r}_s$ a signal $s(t)$ is emitted and then convolved with the impulse response $h(t)$ of the room towards microphone μ. Environmental noise $n(t)$ is superimposed leading to the microphone signal

$$y_\mu(t) = h_\mu(t) * s(t) + n_\mu(t).$$

The time needed for an arbitrary sound wave to travel from a position $\boldsymbol{r}$ to the microphone $\boldsymbol{r}_\mu$ at a velocity of $c = 343m/s$ is

$$\tau_\mu = \tau_\mu(\boldsymbol{r}) = \frac{\|\boldsymbol{r}_\mu - \boldsymbol{r}\|}{c},$$

with $\|\cdot\|$ being the Euclidean norm. Neglecting reverberation for the moment and setting $\boldsymbol{r} = \boldsymbol{r}_s$, the microphone signal can be written as

$$y_\mu(t) = a_\mu \cdot s(t - \tau_\mu) + n_\mu(t),$$

whereby a_μ denotes an attenuation factor which is related to air absorption. The time difference of arrival (TDOA) between two microphones $\mu, \nu \in \mathcal{M}$ and an arbitrary position $\boldsymbol{r}$ can be written as

$$\tau_{\mu\nu}(\boldsymbol{r}) = \tau_\mu(\boldsymbol{r}) - \tau_\nu(\boldsymbol{r}) = \frac{1}{c}\left(\|\boldsymbol{r}_\mu - \boldsymbol{r}\| - \|\boldsymbol{r}_\nu - \boldsymbol{r}\|\right).$$

2.2 Far Field Assumption and Direction of Arrival

In this work we assume that the sound source position has a distance to the microphone array which is much larger than the array itself. In such case the sound source position is said to be in the far field of the array. Under this assumption the array is not able to resolve the distance $\|\boldsymbol{r}_s\|$ to the sound source [6], which generally leads to inaccurate localization results. The solution to this problem is to transfer the sound source position from a rectangular coordinate representation (depending on the distance $\|\boldsymbol{r}_s\|$), to a representation depending on the direction of arrival (DOA) of a sound wave to the origin. For a position $\boldsymbol{r} \in \mathbb{R}^3$ this is done by a spherical coordinate transformation. Neglecting the length $\|\boldsymbol{r}\|$, and defining $\mathcal{C}$ as the set of all possible vectors $\boldsymbol{\zeta}$,

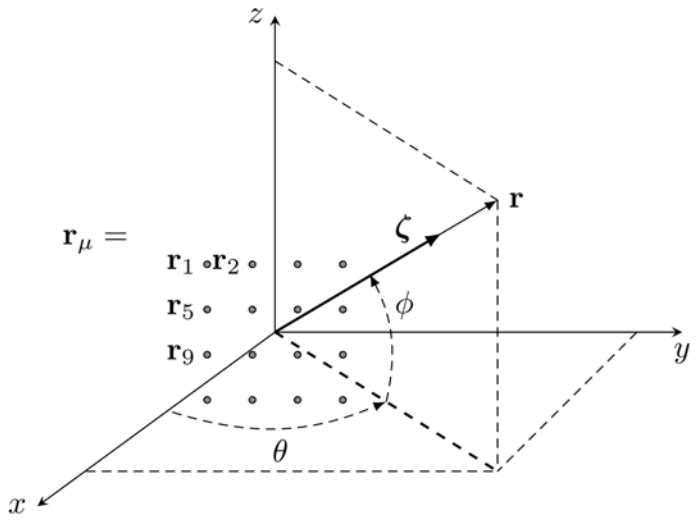


Fig. 1: Coordinate system and angles, $\boldsymbol{r_{x\mu} = 0}$

the azimuth angle $-\pi \leq \theta \leq \pi$, and elevation angle $-2\pi \leq \phi \leq 2\pi$, the so-called propagation vector is defined as

$$\boldsymbol{\zeta}(\theta,\phi) = \begin{pmatrix} \cos\phi\cos\theta \\ \cos\phi\sin\theta \\ \sin\phi \end{pmatrix} \in \mathcal{C} \text{ with } \|\boldsymbol{\zeta}(\theta,\phi)\| = 1.$$

The definition of the angels follows the standard geographic convention. All described angles, positions, and their orientation can be found in Fig. 1.
The angle dependent TDOA can now be written as

$$\tau_{\mu\nu}(\boldsymbol{\zeta}(\theta,\phi)) = \frac{1}{c}\left[(\boldsymbol{r}_\mu - \boldsymbol{r}_\nu)^T \cdot \boldsymbol{\zeta}(\theta,\phi)\right].$$

2.3 Generalized Cross Correlation – Phase Transform

There are several methods for the estimation of TDOA values. In this paper the generalized cross-correlation (GCC) method is used in combination with a phase transform (PHAT) weighting [4]. For a pair of microphones and their sampled signals $y_\mu(n)$ and $y_\nu(n)$ with the discrete time index n the cross-correlation function is derived by the following steps.
After applying a Hann window of length K to the microphone signals $y_\mu(n)$ and $y_\nu(n)$ for framing, the discrete Fourier transforms (DFTs) $Y_\mu(\ell,k)$ and $Y_\nu(\ell,k)$ with frequency bin k and frame index ℓ are computed (the frame index ℓ will be omitted in this paper).
The generalized cross-correlation (GCC) function of these two microphone signal spectra can be computed by the inverse DFT and the insertion of a complex-valued weighting factor $G_{\mu\nu}$ leading to [4]

$$\varphi_{\mu\nu}^{GCC}(\tau) = \frac{1}{K}\sum_{k=0}^{K-1} G_{\mu\nu}(k) Y_\mu(k) Y_\nu^*(k) e^{j2\pi\frac{k\tau}{K}},$$

with $()^*$ denoting the complex conjugate. The weighting factor $G_{\mu\nu}$ can be chosen in many ways [6]. As it gives good results in reverberant environments, in this work the PHAT weighting is employed [4] resulting in the GCC-PHAT function

$$\varphi_{\mu\nu}^{PHAT}(\tau) = \frac{1}{K}\sum_{k=0}^{K-1} G_{\mu\nu}^{PHAT}(\tau) Y_\mu(k) Y_\nu^*(k) e^{j2\pi\frac{k\tau}{K}} = \frac{1}{K}\sum_{k=0}^{K-1} \frac{Y_\mu(k)Y_\nu^*(k)e^{j2\pi\frac{k\tau}{K}}}{|Y_\mu(k)Y_\nu^*(k)|}. \quad (1)$$

The estimated TDOA between the two microphone signals $y_\mu(n)$ and $y_\nu(n)$ is typically taken as

$$\hat{\tau}_{\mu\nu} = \arg \max_{\tau\in\mathcal{T}} \varphi_{\mu\nu}^{PHAT}(\tau), \quad (2)$$

with the maximum being searched over an application-dependent search range $\mathcal{T} \subset \mathbb{R}$.

2.4 Steered Response Power

Due to sound reflections within the room, the GCC function (1) may have more than one local maximum. In this case the TDOA estimate in (2) can be inaccurate or even wrong. To overcome this problem in this paper the steered response power (SRP) [6] method is used, which is based on the variation of τ in (1). This variation corresponds to steering a beamformer over the search space and measuring the output power. Under the far-field assumption the search space $\mathcal{C} \subset \mathbb{R}^3$ is expressed in discretized angles to represent different directions of arrival (DOAs): The resulting search space is then given by $\mathcal{Q} = \mathcal{A} \times \mathcal{E} = \{(\theta, \phi) | \theta \in \mathcal{A}, \phi \in \mathcal{E}\} \subset \mathbb{R}^2$ with $\mathcal{A} = \{\theta_{min}, \dots \theta_{max}\}, \mathcal{E} = \{\phi_{min}, \dots \phi_{max}\}$ and $\times$ denoting the Cartesian product. Each pair of angles $(\theta, \phi) \in \mathcal{Q}$, corresponds to a specific $\tau_{\mu\nu}(\boldsymbol{\zeta}(\theta, \phi))$ for each microphone pair $(\mu, \nu) \in \mathcal{P} \subset \mathcal{M}^2$. The ranges of $\mathcal{A}$ and $\mathcal{E}$ need to be chosen task-dependent. Employing $\tau = \tau_{\mu\nu}(\boldsymbol{\zeta}(\theta, \phi))$ in (1), leads to a specific GCC function $\varphi_{\mu\nu}^{PHAT}(\boldsymbol{\zeta}(\theta, \phi))$. Expressed as a function of $\boldsymbol{\zeta}$ (and in this way of θ and ϕ), it can be interpreted as a spatial likelihood function (SLF)

$$S_{\mu\nu}(\boldsymbol{\zeta}) = \varphi_{\mu\nu}^{PHAT}\big(\tau_{\mu\nu}(\boldsymbol{\zeta})\big) = \frac{1}{K}\sum_{k=0}^{K-1} G_{\mu\nu}^{PHAT}(k) Y_\mu(k) Y_\nu^*(k) e^{j2\pi\frac{k\tau_{\mu\nu}(\zeta)}{K}} \quad (3)$$

for each pair of microphones (μ, ν). The resulting function should show a maximum value belonging to an explicit DOA $\boldsymbol{\zeta}$. Taking the sum of these SLFs over all microphone pairs (or at least more than one) gives a more precise DOA estimate, but on the other hand increases the computational complexity as (3) has to be computed for each microphone pair. The sum of the SLFs over all microphone pairs we will call the total spatial likelihood function (TSLF) which is expressed as

$$S_{\mathcal{P}}(\boldsymbol{\zeta}) = \frac{1}{|\mathcal{P}|}\sum_{(\mu,\nu)\in\mathcal{P}} S_{\mu\nu}(\boldsymbol{\zeta}). \quad (4)$$

3 PROPOSED ACOUSTIC EVENT LOCALIZATION

3.1 Sound Activity and Event Onset Detection

In the following the sound activity detection (SAD) and the event onset detection (EOD) are described, as they will be used later in the spatial filtering process (Section 3.2). Each frame ℓ of any microphone signal $y(n)$ is divided into subframes $\ell' \in \mathcal{L}' = \{1, \dots, L'\}$. A 3–state sound activity detector (SAD) in the DFT domain [12], with frequency bin $k' \in \{0, \dots, K'/2\}$ is employed to obtain a sound activity hypotheses for each frequency bin. Now for each subframe ℓ' (and channel μ) the decision $SAD_\mu(\ell')$ is made upon this sound activity hypotheses in that channel. We decide for $SAD_\mu(\ell') = 1$ if at least 60% of its frequency bins in the range [500 Hz, 5000 Hz] are classified by the 3–state SAD as sound active otherwise $SAD_\mu(\ell') = 0$.

The single decisions for each subframe ℓ' need to be joined to a decision for each frame ℓ. This is done by

$$SAD_\mu(\ell) = \begin{cases} 1, & if\ \sum_{\ell'\in\mathcal{L}'} SAD_\mu(\ell') \geq \delta_{\mathcal{L}'} \\ 0, & else. \end{cases}$$

Finally, the sound activity decisions $SAD_\mu(\ell)$ are joined to an overall sound activity decision

$$SAD(\ell) = \begin{cases} 1, & if\ \sum_{\mu\in\mathcal{M}} SAD_\mu(\ell) \geq \delta_{\mathcal{M}} \\ 0, & else. \end{cases}$$

Based upon the *subframe* sound activity decision $SAD_\mu(\ell')$, we propose an event onset detector (EOD). In a first step the subframe event onset decision

$$EOD_\mu(\ell') = \begin{cases} 1, & if\ \prod_{\lambda'\in\{\ell', \dots, \ell'+L_{min}-1\}} SAD_\mu(\lambda') = 1 \\ 0, & else. \end{cases}$$

is made. This operation requires a lookahead of $L_{min} - 1$ subframes and ensures that there are at least L_{min} consecutive future subframes marked as active sound. By this means the performance of the whole framework can be optimized, as single subframes marked as active sound are ignored and a minimum event length is ensured. Following

the hierarchy of the SAD, the event onset decisions for each subframe are joined to a frame-and channel-wise onset decision

$$EOD_\mu(\ell) = \begin{cases} 1, & if\ \sum_{\ell' \in \mathcal{L}'} EOD_\mu(\ell') \geq \delta_{\mathcal{L}'} \\ 0, & else. \end{cases}$$

For the further processing the channel-wise decisions are again joined to an overall event onset decision

$$EOD(\ell) = \begin{cases} 1, & if\ \sum_{\mu \in \mathcal{M}} EOD_\mu(\ell) \geq \delta_{\mathcal{M}} \\ 0, & else. \end{cases}$$

The parameters $\delta_{\mathcal{L}'}$, $\delta_{\mathcal{M}}$, and L_{min} have to be chosen dependent on the task.

3.2 Spatial Minimum Tracking, Smoothing, and Localization

Estimating the DOA by maximizing (4) w.r.t. $\boldsymbol{\zeta}$ may still be affected by acoustic disturbances. The reduction of these disturbances can be achieved in many ways. Within this work a Wiener-type filter is used to suppress spatial noise and reverberation. In case of sound absence ($SAD(\ell) = 0$), and using frame index ℓ, the noise floor (NF) of the SLF is simply estimated by (c.f. (4))

$$S_{NF,\ell}(\boldsymbol{\zeta}) = S_{\mathcal{P},\ell}(\boldsymbol{\zeta}).$$

In case of sound presence ($SAD(\ell) = 1$), potential speaker positions are deleted from the desired noise floor by applying the following spatial minimum tracking

$$S_{NF,\ell}(\boldsymbol{\zeta}) = \min\left(S_{\mathcal{P},\ell}(\boldsymbol{\zeta}), \frac{1}{|\mathcal{C}_{\boldsymbol{\zeta}}|} \sum_{\boldsymbol{\zeta}' \in \mathcal{C}_{\boldsymbol{\zeta}}} S_{\mathcal{P},\ell}(\boldsymbol{\zeta}')\right), \tag{5}$$

$\mathcal{C}_{\boldsymbol{\zeta}} = \{\boldsymbol{\zeta}(\theta', \phi') | \theta - \delta \leq \theta' \leq \theta - \delta, \phi - \delta \leq \phi' \leq \phi - \delta\}$ being the space of vectors $\boldsymbol{\zeta}(\theta', \phi')$ belonging to a squared vicinity of $\boldsymbol{\zeta}(\theta, \phi)$ in the 2D spherical coordinate space. Independent of the SAD decision, in both cases a (temporal) first-order IIR filter is employed

$$\tilde{S}_{NF,\ell}(\boldsymbol{\zeta}) = \beta_{NF} \cdot \tilde{S}_{NF,\ell-1}(\boldsymbol{\zeta}) + (1 - \beta_{NF}) \cdot \tilde{S}_{NF,\ell}(\boldsymbol{\zeta}),$$

with the initial value $\tilde{S}_{NF,0}(\boldsymbol{\zeta}) = 0$, and forgetting factor $\beta \in [0,1]$. In case of no detected event onset ($EOD(\ell) = 0$), processing for the current frame ℓ stops here.
If an event onset is detected ($EOD(\ell) = 1$), a spatial a *priori* SNR ($\xi_\ell(\boldsymbol{\zeta}) \geq 0$ cf. (5))

$$\xi_\ell(\boldsymbol{\zeta}) = \frac{S^2_{\mathcal{P},\ell}(\boldsymbol{\zeta}) - \tilde{S}^2_{NF,\ell}(\boldsymbol{\zeta})}{\tilde{S}^2_{NF,\ell}(\boldsymbol{\zeta})}$$

is calculated. This a priori SNR can now be used to compute a Wiener-type spatial weight and to obtain an enhanced SLF

$$S^{opt}_{\mathcal{P},\ell}(\boldsymbol{\zeta}) = S_{\mathcal{P},\ell}(\boldsymbol{\zeta}) \cdot \frac{\xi_\ell(\boldsymbol{\zeta})}{1 + \xi_\ell(\boldsymbol{\zeta})}.$$

Even the enhanced spatial likelihood function $S^{opt}_{\mathcal{P},\ell}(\boldsymbol{\zeta})$ may still show several local maxima, therefore, we propose to smooth it with a 2-dimensional Gaussian lowpass filter in the spherical coordinate system leading to the smoothed SLF

$$\bar{S}^{opt}_{\mathcal{P},\ell}(\theta, \phi) = \left(\frac{1}{2\pi\sigma^2} e^{-\frac{\theta^2+\phi^2}{2\sigma^2}}\right) * S^{opt}_{\mathcal{P},\ell}(\boldsymbol{\zeta}(\theta, \phi)),$$

with $*$ denoting the convolution operation. Finally, the estimated DOA in terms of θ and ϕ is given by

$$\hat{\boldsymbol{\zeta}} = \boldsymbol{\zeta}(\hat{\theta}, \hat{\phi}), with\ (\hat{\theta}, \hat{\phi}) = \arg \max_{(\theta,\phi) \in \mathcal{Q}} \bar{S}^{opt}_{\mathcal{P},\ell}(\theta, \phi),$$

and is estimated only in frames with $EOD(\ell) = 1$. As the search space $\mathcal{Q}$ is spanned by only two angles (θ, ϕ) we in fact end up with a 2-dimensional optimization.

4 EVALUATION SETUP AND RESULTS

4.1 Array Setup and Data Acquisition

For our experiments, a microphone array was placed in a medium size lecture hall. The array consists of $4 \times 4 = 16$ microphones, equidistantly arranged with 10 cm spacing,

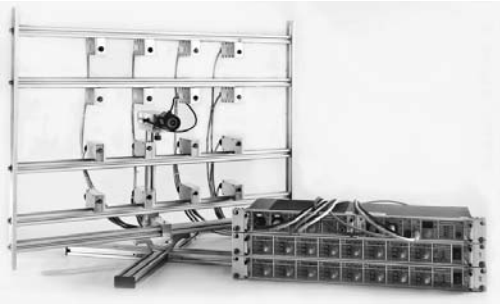


Fig. 2: Microfon array with camera and recording equipment

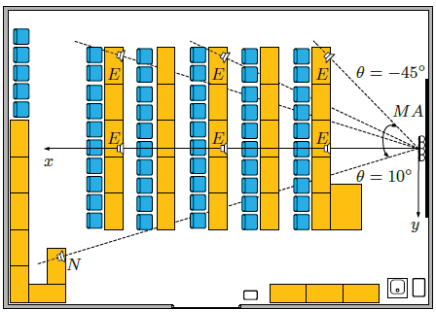


Fig. 3: Lecture hall with positions of the microphone array (MA), event sources (E) and the noise source (N)

with a camera being placed in the center (see Fig. 2). Two RME Octamic were used for amplification and sampling, connected to two RME Fireface working as audio interfaces to a computer. For optimal hardware performance the microphone signals were recorded at a sampling frequency of 48 kHz and later downsampled to 16 kHz for the experiments. At 6 room positions (see Fig. 3, symbols E) 10 files of 50 classes from the RWCPSSDRAE database [13] were played back by a broadband loudspeaker (Fostex Personal Monitor 6301B). The loudspeaker was positioned with the membrane facing the array. In addition two types of noise (babble noise (denoted as 'bab') and street noise (denoted as 'str')) were played back at a seventh position in the back of the room. The noise source (N) is positioned in the lower left corner and the microphone array (MA) on the right side. Note that the displayed x and y axes are consistent to Fig. 1. Since for all computations the coordinate system was placed in the array's origin, all angles in this section are given relative to the array's origin.

4.2 Algorithm Setup and Evaluation Methodology

For our evaluation the recorded acoustic events were split into three sets: development (20%), development-test (20%), and test (60%). In consequence, all results given in this paper are averaged over 6 positions × 6 files × 50 classes = 1800 different single acoustic events. To explore the influence of noise to the proposed algorithm, different signal-to-noise ratios (SNRs) where chosen and processed. Within this evaluation the searchspace $\mathcal{Q}$ is spanned by $\mathcal{A} = \{-55°, \ldots, 55°\}$ and $\mathcal{E} = \{-47°, \ldots, 46°\}$. The angle limits are determined by the optical specifications of the camera in the array's origin. As already mentioned the estimated sound source position shall be used to steer a second camera. Based on this the search space spacing is $1°$ both w.r.t. θ and ϕ.
For evaluation we use two common metrics, based on the Euclidean distance of the estimated $(\hat{\theta}, \hat{\phi})$ to the original DOA (θ, ϕ)in degrees

$$\Delta_{\mathrm{DOA}} = \sqrt{(\hat{\theta} - \theta)^2 + (\hat{\phi} - \phi)^2}.$$

At first for each test case the miss ratio (MR) is calculated, giving the percentage of position estimates where $\Delta_{DOA} > 3°$. Second the average estimation error (AEE) is calculated as the average over all Δ_{DOA}. All parameters were optimized on clean and 10dB SNR data, minimizing the miss ratio on the development-test dataset in each case, as in our use case it is most important to recognize an event within $\Delta_{DOA} \leq 3°$.
The baseline results are calculated by the framework from [10], modified for DOA estimation using the DOA search space and our frequency-domain sound activity detection, henceforth listed 'REF'. Our new framework is dubbed by 'EOD', including all functions as presented in Section 3: SAD, EOD, spatial minimum tracking, smoothing, and then localization. Both frameworks use the following parameters: GCC-PHAT-SRP framelength $K = 4096$ (no overlap), SAD/EOD framelength $K' = 512$ (overlap 256 samples) resulting in $L' = 16, \delta_{\mathcal{L}'} = 9, \delta_{\mathcal{M}} = 9, L_{min} = 3$, the vicinity of $\boldsymbol{\zeta}$ is given by $\delta = 3$, spatial noise floor smoothing constant $\beta_{NF} = 0.1$, smoothing filter standard

	SNR					
	0 dB	5 dB	10 dB	15 dB	20 dB	∞
REF-str	28.04	24.37	22.84	20.37	19.73	18.59
REF-bab	63.59	57.92	53.31	49.15	45.63	
EOD-str	**18.76**	**17.33**	**17.62**	**15.67**	**16.08**	**17.10**
EOD-bab	**59.17**	**53.55**	**49.04**	**45.26**	**41.21**	

Tab. 1: Miss ratio (MR) in percent, for the baseline framework REF and our new approach.

	SNR					
	0 dB	5 dB	10 dB	15 dB	20 dB	∞
REF-str	15.07	14.63	14.31	13.20	12.80	10.16
REF-bab	30.76	30.69	30.06	29.65	28.30	
EOD-str	**11.06**	**10.85**	**11.27**	**10.26**	**10.30**	**9.90**
EOD-bab	**30.75**	**30.51**	**29.50**	**28.88**	**26.58**	

Tab. 2: Average estimation error (AEE) of missed frames in degrees, for the baseline framework REF and our new approach.

deviation $\sigma = 3°$. Within the evaluation $M = 4$ microphones at the four corners of the array were used.

4.3 Evaluation Results and Discussion

At first have a look at the miss ratio (MR) in Tab. 1, a measure for the robustness of the localization algorithm. It is clearly visible that our new framework significantly decreases the miss ratio under noisy conditions, gaining about an absolute improvement of $3.6\% \ldots 9.3\%$ under street noise and $3.9\% \ldots 4.5\%$ under babble noise. Obviously the EOD framework clearly outperforms the REF framework in all SNR and in all noise conditions.

As the main goal of the proposed algorithm is to gain a high recognition rate of events and to localize them close to the original location, the miss ratio is the most important performance measure. Nevertheless, now have a look at the average estimation error (AEE) for missed frames in Tab. 2 for the evaluation of the precision of the proposed algorithm. Here the goal should be to lower this error as in this way all position estimates become more precise. Our new EOD framework significantly improves the AEE in both noise conditions, gaining up to $4°$ improvement under street noise at 0dB SNR.

Altogether we can summarize, that the proposed new EOD framework clearly outperforms the REF framework both in miss ratio and average estimation error. For street noise the new EOD approach performs approximately equal in the whole investigated SNR range.

5 CONCLUSION

In this paper we derived a framework for acoustic event source localization with a microphone array. A GCC-PHAT-SRP framework is supported by an frequency-domain sound activity detection and event onset detector. For the suppression of artifacts in the spatial likelihood function, spatial minimum tracking and smoothing are employed. The new framework clearly outperforms the baseline framework, by reducing the miss ratio up to 9% and increasing the overall precision under non-stationary noise and several signal to noise ratios.

REFERENCES

[1] H.Wang and P. Chu, “Voice Source Localization for Automatic Camera Pointing System in Videoconferencing,” in Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Munich, Germany, Apr. 1997, pp. 187–190.

[2] C. Busso et al., “Smart Room: Participant and Speaker Localization and Identification,” in Proc. Of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Philadelphia, PA, USA, Mar. 2005, pp. 1117–1120.

[3] A.R. Abu-El-Quran and R.A. Goubran, “Security-Monitoring using Microphone Arrays and Audio Classification,” in Proc. of IEEE Instrumentation and Measurement Technology Conference (IMTC), Ottawa, Canada, May 2005, vol. 2, pp. 1144– 1148.

[4] C. Knapp and G. Clifford Carter, “The Generalized Correlation Method for Estimation of Time Delay,” IEEE Trans. Acoustics, Speech, and Signal Processing, vol. 24, no. 4, pp. 320–327, Aug. 1976.

[5] C. Zhang et al., “Why Does PHAT Work Well in Low Noise, Reverberative Environments?,” in Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Las Vegas, NV, USA, Mar. 2008, pp. 2565–2568.

[6] J. H. DiBiase, A High-Accuracy, Low-Latency Technique for Talker Localization in Reverberant Environments Using Microphone Arrays, Ph.D. thesis, Brown University, Providence, RI, USA, May 2000.

[7] A. Ikeda et al., “2D Sound Source Localization in Azimuth and Elevation from Microphone Array by Using a Directional Pattern of Element,” in Proc. of. IEEE Sensors Conference, Atlanta, GA, USA, Oct. 2007, pp. 1213–1216.

[8] J.P. Bello et al., “On the Use of Phase and Energy for Musical Onset Detection in the Complex Domain,” IEEE Signal Processing Letters, vol. 11, no. 6, pp. 553–556, June 2004.

[9] G. Hu and Wang D.L., “Auditory Segmentation Based on Onset and Offset Analysis,” IEEE Transactions on Audio, Speech, and Language Processing, vol. 15, no. 2, pp. 396–405, Feb. 2007.

[10] F. Hummes, J. Qi, and T. Fingscheidt, “Robust Acoustic Speaker Localization With Distributed Microphones,” in Proc. of European Signal Processing Conference (EUSIPCO), Barcelona, Spain, Aug. 2011, pp. 240 – 244.

[11] P. Transfeld, U. Martens, H. Binder, T. Schypior, and T. Fingscheidt, “Acoustic Event Source Localization for Surveillance in Reverberant Environments Supported by an Event Onset Detection,” in Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Brisbane, Australia, Apr. 2015, pp. 2629–2623.

[12] B. Fodor and T. Fingscheidt, “Reference-Free SNR Measurement for Narrowband and Wideband Speech Signals in Car Noise,” in Proc. of 10th ITG Conference on Speech Communication, Braunschweig, Germany, Sept. 2012, pp. 199–202.

[13] S. Nakamura et al., “Sound Scene Data Collection in Real Acoustical Environments,” The Journal of the Acoustic Society of Japan, vol. 20, no. 3, pp. 225–231, May 1999.

A TRANSPARENT APPROACH FOR PRIORITISING SECURITY MEASURES

Tim Müller[1], Sascha Meng[2], Wolfgang Raskob[1], Marcus Wiens[2] and Frank Schultmann[2]

[1] *{tim.mueller, wolfgang.raskob}@kit.edu*
Karlsruhe Institute of Technology (KIT)
Institute for Nuclear and Energy Technologies (IKET)
Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany

[2] *{sascha.meng, marcus.wiens, frank.schultmann}@kit.edu*
Karlsruhe Institute of Technology (KIT)
Institute for Industrial Production (IIP)
Hertzstraße 16, 76187 Karlsruhe, Germany

Abstract

We describe a method to improve security through a more efficient prioritization of security measures. Our approach is able to determine a set of security measures tailored to a particular, well-defined attack scenario against a public rail transport system. However, there exist specific requirements and boundary conditions. Our approach combines two long-established decision-support methodologies: case-based reasoning (CBR) and multi-criteria decision analysis (MCDA). CBR makes use of prior events and expert knowledge, deriving a set of possible security measures. MCDA is applied to rearrange these sets on the preliminary list with respect to their suitability against particular attack scenarios. The latter enables the decision makers to take their personal preferences into account and to prioritize security measures in a transparent process. Putting all constraints and requirements in a structured form, the proposed approach enhances decision making quality in a very sensible domain and introduces transparency and traceability into the decision process.

Keywords: decision support, adversarial threats, MCDA, CBR

1 INTRODUCTION

Complexity of and interdependencies among (critical) infrastructures make it difficult to provide sufficient levels of security. At the same time, decision makers have never before had access to such vast amounts of information, which has turned out to be both a curse and a blessing for them. In contrast to what is assumed in most economic theory, real-world decision makers are neither infinitely sensitive nor perfectly rational; they have limited cognitive capacities and abilities—they are only boundedly rational (Conlisk, 1996). As a result, decision makers are frequently unable to make good (optimal) decisions without any additional support (Djamasbi, 2007). Decision support systems (DSS) help to identify, structure and process relevant information, to recognize and efficiently treat uncertainties, and to appreciate the existence and the implications of complexity in their decision making processes (Sojda, 2007). Using decision support tools for making decisions concerning security investments has been proven useful for various reasons: it enables the sustainable use of scarce resources, and it allows the consideration of technical, organizational, and social-political constraints.

Decision making, even when some form of DSS is applied, still remains a non-trivial task. There are often numerous parties (stakeholders) involved in the decision processes who perceive risks unevenly, and who also have different knowledge, experiences and preferences. Additionally, it is often necessary to consider a broad

range of uncertain decision variables. To provide good decisions under such circumstances it is important for the whole decision making process to be as transparent and comprehensible as possible. Among other means, multi-criteria decision analysis (MCDA) approaches seem to be appropriate tools for the given task. They remove "subjectivity" to some extent and make the decision process more understandable. However, simply using MCDA methods is not always sufficient, especially if the decision process is particularly complex and a suitable "starting point" for the MCDA is not obvious. It then might be useful to prefix other approaches to a MCDA method which are suitable to structure information and to provide the mentioned starting point. We therefore integrate case-based reasoning (CBR) in the decision making process. CBR proposes solutions for decision problems based on prior, historical experiences and expert knowledge. Because information about adversaries, their motives and abilities is usually scarce, similar historical decision problems as well as expert knowledge are used to supplement the knowledge data base of the CBR and to derive a course ranking of well-suited security measures. As CBR only takes similarities or similarity measures between attributes into account, it is not suited by itself to provide situational security measures. Hence, the course ranking requires refinement through the MCDA in return. The two methods complement each other in a meaningful way.

In this paper we present the results of our attempt to combine both approaches. Our research has been motivated by and is part of the research project *RIKOV*, which aims at improving security for German public rail transport systems.

2 THEORETICAL FOUNDATIONS

Decisions are based on information, and information is often only available in an unstructured state. Information may exist in different forms, and it is challenging to gather, process, and store it. Hence, decision makers frequently use DSS. DSS are computer-based systems which help decision makers to make good decisions in the face of uncertain or complex decision situations (Shim et al., 2002). DSS should be comprehensible, transparent, flexible and easy to use. All DSS have similar, basic components: a (knowledge) data base, a model or analytical measures to take account of the decision context, and a user interface. We use CBR and MCDA as analytical measures, to structure information and the decision makers' preferences.

CBR makes use of "well-known" cases, which consist of historical cases and expert knowledge. It is based on the paradigm that similar problems often have similar solutions (Beierle & Kern-Isberner, 2003) and in general mimics the behavior of a decision maker by referring to his knowledge and experiences in the past. Cases are mutually exclusive, and are made up of a problem and a respective solution for it. Cases help decision makers to understand and solve new or unknown problems and serve as indicators for possible solutions. The main advantage of CBR-systems is that decision makers can rely on existing and already structured knowledge. It entails that decision makers do not always have to acquire the knowledge necessary for solving a problem from scratch. If knowledge is stored in a structured manner (in a data base), it saves resources and improves the quality of the solutions (Stein et al., 2007). All CBR-systems are typically realized as cycles, with typically four steps: *retrieve* (a similar old case), *reuse* (the respective solution and adapt it if necessary), *revise* (if necessary the proposed solution after testing it), and *retain* (the problem and its solution as new case in the data base) (see, e.g., Aamodt & Plaza, 1994; Bergmann, Althoff, Minor, Reichle, & Bach, 2009; Kolodner, 1992). Difficulties which may occur when applying CBR are, for example, (1) that solutions for existing cases are not necessarily the best solutions, (2) that the modeler needs to find suitable similarity functions for comparing cases, (3) that solutions of similar cases need to be useable, and (4) that uncertainties are taken into consideration (Beierle & Kern-Isberner, 2003; Stein et al., 2007).

MCDA is concerned with decision situations in which the members of a group of decision makers have different, (partially) conflicting objectives. When applying MCDA, the decision makers' objectives are to find one or more "good" solutions with respect to their individual preferences and to structure the decision process, enabling them to make transparent, coherent decisions in complex decision situations (Belton & Stewart, 2002). There exist different approaches, and selecting an appropriate MCDA-approach is crucial because it affects the suggested solutions (Guitouni & Martel, 1998). MCDA-approaches, however, cannot make decisions perfectly "objective" and cannot free decision makers from making decisions (Belton & Stewart, 2002). All approaches have a similar underlying structure, including the following steps: *problem identification and structuring* (with respect to, e.g., goals, values, uncertainties), *model building* (including specifying alternatives and defining criteria), *searching for solutions* (including preference elicitation, information aggregation and sensitivity analysis), and *developing an action plan* (Belton & Stewart, 2002; Lin, Brauner, Münzberg, Meng, & Möhrle, 2013). MCDA-approaches are differentiated among multi objective decision making methods (MODM) and multi attribute decision making methods (MADM), which are further differentiated between classic approaches, outranking methods and fuzzy methods (Zimmermann & Gutsche, 1991). Although the Analytic Hierarchy Process (AHP) as a more sophisticated variant was available, we chose a classic MCDA-approach in our DSS for the sake of simplicity. It is assumed that the decision makers can assess the importance of their criteria directly on a cardinal scale (Saaty, 2008). Every criterion has assigned a weight which indicates its importance compared to all other criteria; the criteria are aggregated by calculating the weighted sum over all criteria.

3 DSS FOR PRIORITISING SECURITY MEASURES

We consider public rail transport systems. Decision makers (i.e., operators, authorities) have a great number of security measures available to protect these systems against external actions like a terrorist attack. But not all these measures can be implemented because of, i.e., financial, technical, legal, and socio-political constraints. Security measures are also only appropriate for certain types of attacks. It is, thus, important to define for all (possible) attack scenarios — possible combinations of perpetrator profiles, targets and weapons — a specific security measure or set of security measures. The objective of our DSS is to propose for a given attack scenario a set of security measures, which are well-suited in terms of certain criteria. In theory, such a set of security measures is optimal with respect to the used criteria. But in reality, decision makers are confronted with uncertainties and complexities and, thus, cannot simply realize these sets without further considerations.

Our DSS is based on a knowledge data base which currently contains more than 130 cases, based on an analysis of 88 historical attack scenarios (Neubecker, 2013) as well as scenarios generated in expert interviews. The data base also contains for each scenario the actual chosen set of security measures or the suggested set of security measures. A scenario together with its related solution is called a case (cf. section 2). Each case also contains dynamic scenario parameters such as costs etc. The result of the DSS is a list of security measures which are ordered with respect to their applicability for a certain scenario.

The DSS is a two-stage process. First, CBR is used to structure the knowledge of the decision makers and to preselect proper security measures for protecting public railway systems in Germany. Second, MCDA is applied to find the *best* security measures out of the preselected list by refining the list created through CBR with respect to certain criteria. The term *best* in this context refers to the preferences of the decision makers, which may vary significantly. Thus, applying MCDA does not only help finding good solutions, it also points out consequences of different preferences. Both stages,

realized as software, are enclosed by a control module which handles the input and output parameters, and which controls the process. The described process can be repeated for as many scenarios as necessary. The different results can afterwards be weighted and aggregated, to find an appropriate set of security measures which provides protection against many different attack scenarios.

3.1 Knowledge data base

The knowledge data base has a complex structure as shown in Figure 1. It mainly consists of scenarios definitions which are linked to appropriate security measures. The disadvantage of security measures and scenarios created by experts is that they contain an inherent subjective component. The problem with historic scenarios is that it is not known whether the chosen measures fit the criteria if no other similar cases exist. Within our DSS these uncertainties are not explicitly addressed because the process itself is independent of it. For our DSS we assume that the relevant security measures match the gold standard, which means that they are valid, tested and provide an acceptable solution for the given scenario.

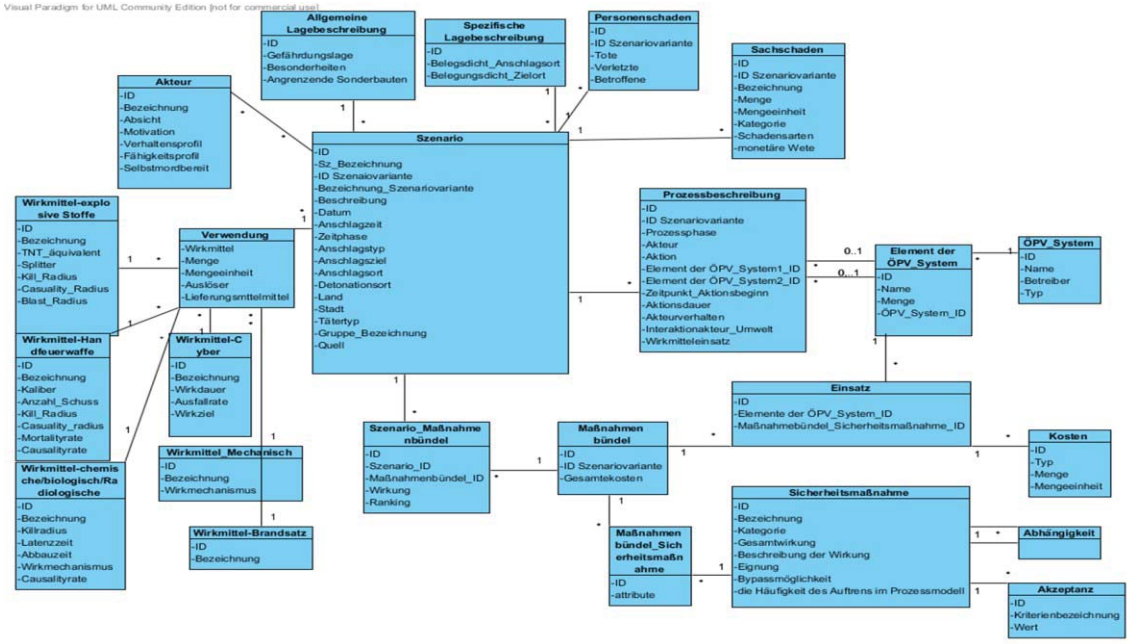


Figure 1: Structure of the knowledge database developed for the DSS.

As the DSS is part of a comprehensive software tool to address the needs of decision makers in public transportation, it was implemented as a package of independent modules programmed in Java, which are loosely coupled and can be embedded in an external application. The DSS receives the parameter required for executing in form of XML-files which have to be provided by the main application. When the control module is started, CBR is applied to all scenarios which are defined in the input file. For each scenario a CBR input file is generated, and CBR is executed resulting in one CBR output file for each input. To process the identified security measures in the MCDA module, specific parameters such as risk reduction or costs are required. The data of the CBR output together with the specific parameters are combined in an MCDA XML input file. The result of the MCDA is again an XML file. Finally, for each scenario a ranked list with sets of security measures in the form of an MCDA output file is generated. The sets are finally aggregated as a weighted sum resulting in a final ranked list, providing a set of suitable security measures. In principle, a large number of scenarios can be calculated at the same time, whereas processing power and storage capacities are limiting factors. It should be noted that evaluation by simulation may require time if done properly.

3.2 Process

At first, relevant cases are stored in the data base. A XML-data structure is created, which serves the DSS as input parameter and starts the control module. It analyses the XML-files and for each attack scenario of interest CBR is applied. The control module creates from an existing template the XML-data structure which serves as the input parameter for the CBR process.

3.2.1 CBR

In the template, the set of input attributes, their weights and the expected output attributes are predefined. The CBR calculates for all existing cases in the data base their similarity with the attack scenario of interest. Similarity of the attributes is calculated through similarity measures (Moehrle, 2012). For attributes with numeric domains the Euclid norm is usually applied. For enumerated domains, useful similarity measures are defined. The similarity of textual attributes is measured by textual similarity measures based on the model of (internet) search engines, e.g., *Solr* (Apache Software Foundation, 2015).

The CBR process results in a relative ranking of security measures based on the similarity of their attributes. It is highly abstract and not suited as a solution since similarity alone is not sufficient to derive security measures. Therefore, the result represents a rough solution which needs to be refined and adopted to the decision makers' individual preferences. The revise step of the CBR process necessarily requires the verification of the proposed solution. In RIKOV, three approaches are possible: expert surveys, simulations, and verification through decision rules and external knowledge. The verification is addressed in the discussion section of this paper.

3.2.2 MCDA

MCDA further prioritizes the list of security measures which has been identified through CBR. For this purpose, an attribute tree has been defined in RIKOV with the help of RIKOV project partners and project-external experts, which have been identified as being useful for prioritizing security measures (Figure 2). The values of the attributes result from the scenario itself, or are the result of dynamic calculations within RIKOV. Other values may be the result of expert appraisals or simulations.

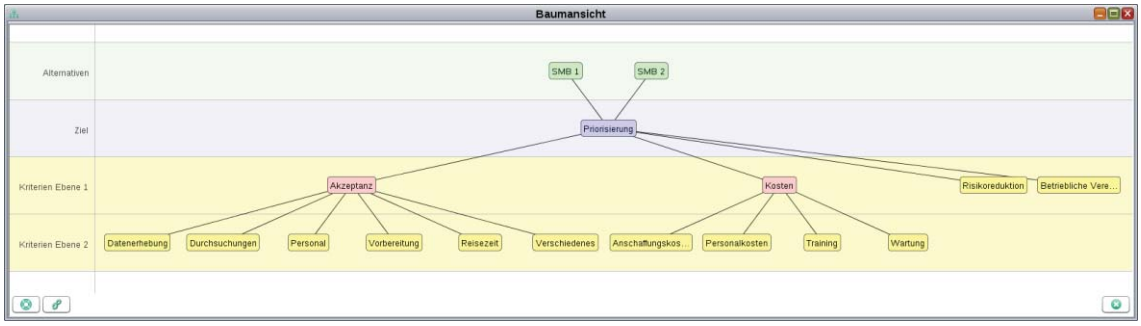


Figure 2: Attribute tree for referencing security measures by MCDA.

The values of the attributes are aggregated. The importance of each attribute is characterized through its weight. The weights have been defined within expert workshops by German operators of public rail transport systems and security authorities (other decision makers might use different weights or even different attributes). The weights applied, however, represent a consensus found in a transparent process. Whenever the group changes, a new consensus needs to be found.

3.2.3 Aggregation

For every scenario a list of ranked security measures and sets of security measures is identified. A value will be assigned to every solution indicating their relevance for that particular attack scenario. To find the solution which is best with respect to all analyzed scenarios, the results for each scenario are themselves aggregated again. This is combined with a subsequent second MCDA step which uses again the weighted sum approach (also other aggregation mechanism might be applied). The result is a final, ranked list of security measures best suited for all those considered in the assessment.

3.2.4 Decision Making

The generated list of ranked security measures has to be understood as a simple "suggestion of the DSS" how to spend resources on security. The DSS is not intended to replace human experts. The proposed (possibly suitable) security measures are supposed to be used by the decision makers as a new, valuable starting point. When evaluating certain security measures, decision makers need to make use of their individual knowledge and expertise, to extend or combine existing measures to derive a "new security concept for an existing attack scenario".

The final decision is then assigned to the investigated scenario as a new solution, and the whole data set is stored as a new case in the knowledge data base. Subsequently, if decision makers (i.e., users) realize that the solution for a certain scenario is not appropriate, the case may be deleted from the data base. To apply this novel DSS it is important to know the structure of the DSS and the selection approach of the security measures. The quality of the decision increases with the knowledge of the decision maker and the selection of proper similarity measures for scenario parameters.

4 DISCUSSION

The DSS we have presented in this paper is generic in its structure and thus can be applied to other fields if appropriately modified. However, developing a specific DSS is a difficult and complex task. First, decision makers need to identify appropriate attributes which can effectively describe the decision problem. Second, the decision makers are confronted with different types of uncertainties, which they very often cannot fully eliminate and thus need to live with. An additional problem in the context of security is that information is very often only sparsely available, if at all: e.g., certain attack scenarios may have never occurred or information about it is confidential. Also it is not possible to claim that a certain defense strategy is effective against a certain type of attack only for the reason it has not occurred as there may exist unknown circumstances that prevented the attack in the first place. Still the described DSS helps decision makers to structure available information and to show interdependencies.

Mastering CBR and MCDA as application requires several crucial steps: first of all the theoretic approach of CBR has to be adapted to a practical application, meaning that suitable attributes have to be defined which comprehensively describe the problem. Furthermore, suitable measures have to be defined to estimate the similarity between instances, which can be challenging especially for non-numeric attributes. Likewise for MCDA criteria that describe the problem comprehensively have to be identified. In contrast to CBR the process is slightly more subjective and depends on the members of the decision group. In addition, the weights of the criteria have to be defined and agreed upon in the decision group which on the other hand contributes to transparency. Last but not least, many different algorithms are available to normalize the criteria and to aggregate them, though it is possible to create a reasonably good DSS with default algorithms, e.g., using the weighted sum for aggregation. This is supported by the fact that in the end only the relative order of the ranked solutions is of interest. The whole design process is rather time consuming and tedious but in the end

also leads to a very stable DSS that can be applied quickly and efficiently to varying problems of the domain.

The DSS consisting of a sequence of CBR and MCDA requires several steps for evaluation or validation. For the CBR, as it is based on similarity between scenarios, the reason is obvious: though scenarios may be similar with respect to their attributes the suggested security measures nevertheless may not be transferable and thus require validation. This is performed in the revise step of the CBR. For the MCDA, as it is based on criteria normalization, weighting, and aggregation, we use some criteria that implicitly reflect the effectiveness of countermeasures. These values are generated by evaluating the security measures. Last but not least the DSS itself requires an evaluation. For the mentioned purposes three evaluation methods have been used in RIKOV: by experts, by rules, and by simulation. Clearly experts are not available for everyday use and can only be consulted under specific circumstances. Rule sets, derived from expert knowledge, are easy to apply and generally involve low computation costs, though they lack accuracy and flexibility. Still they are useful and provide an acceptable compromise in practice. Evaluation by repeated simulation with varying parameter sets is on one hand most flexible and very accurate if modelled properly, but on the other hand is rather complex and time consuming in practice. For RIKOV the simulation method was successfully tested using a commercial simulation software, but could not be embedded into the DSS demonstrator due to licensing issues. For this reason, rule sets are currently used in the DSS. In a commercial realization the simulation method would be preferable, assuming license fees and computation time issues are acceptable. In the near future the demonstrator of the RIKOV project will be finished and the described DSS will be embedded as part of it.

5 SUMMARY AND ACKNOWLEDGEMENTS

We presented an approach to combine CBR and MCDA into a DSS to transparently rank security measures, overcoming the drawbacks of both methods being used separately. For the CBR a knowledge data base and similarity functions have been established. For the MCDA the criteria and their weighting have been defined. For validation rule sets have been defined which have low computation costs and are an acceptable compromise. More accurate evaluation methods that involve more computation have been considered and tested, but have not yet been integrated.

The DSS will be evaluated as part of the RIKOV demonstration during an evaluation workshop by end of this year, evaluators being the RIKOV consortium and external experts of the public transportation operators. The structure of our approach is in itself generic and can easily be applied to other decision problems. Only the data structures are problem-specific and, thus, always need to be developed from scratch for every new decision problem. We have only used well-known approaches and algorithms, and flexibly designed interfaces. The data and data structures which we have used to analyze terrorist attacks against public rail transport systems have been identified in expert workshops within RIKOV.

The research presented in this paper has been supported by the BMBF. We also would like to thank all project partners in RIKOV for their support.

6 REFERENCES

Aamodt, A., & Plaza, E. (1994). Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches. *AI Communications*, *7*(1), 39–59.

Apache Software Foundation. (2015). *Apache Solr*. Retrieved from http://lucene.apache.org/solr/

Beierle, C., & Kern-Isberner, G. (2003). *Methoden wissensbasierter Systeme: Grundlagen, Algorithmen, Anwendungen* (2nd ed.). *Computational Intelligence*. Wiesbaden: Vieweg.

Belton, V., & Stewart, T. J. (2002). *Multiple Criteria Decision Analysis*. Boston: Springer US.

Bergmann, R., Althoff, K.-D., Minor, M., Reichle, M., & Bach, K. (2009). Case-Based Reasoning: Introduction and Recent Developments. *KI - Künstliche Intelligenz, German Journal on Artificial Intelligence - Organ des Fachbereiches "Künstliche Intelligenz" der Gesellschaft für Informatik e.V. (KI)*, *23*(1), 5–11.

Conlisk, J. (1996). Why Bounded Rationality? *Journal of Economic Literature*, *34*(2), 669–700.

Djamasbi, S. (2007). Does positive affect influence the effective usage of a Decision Support System. *Decision Support Systems*, *43*(4), 1707–1717.

Guitouni, A., & Martel, J.-M. (1998). Tentative guidelines to help choosing an appropriate MCDA method. *European Journal of Operational Research*, *109*(2), 501–521.

Kolodner, J. L. (1992). An introduction to case-based reasoning. *Artificial Intelligence Review*, *6*(1), 3–34.

Lin, L., Brauner, F., Münzberg, T., Meng, S., & Möhrle, S. (2013). Prioritization of security measures against terrorist threats to public rail transport systems using a scenario-based multi-criteria method and a knowledge database. In M. Lauster (Ed.), *Proceedings / 8th Future Security - Security Research Conference. Berlin, September 17 - 19, 2013* (pp. 195–204). Stuttgart: Fraunhofer-Verlag.

Moehrle, S. (2012). Generic self-learning decision support system for large-scale disasters. In L. Rothkrantz, J. Ristvej, & Z. Franco (Eds.), *ISCRAM 2012 conference proceedings book of papers. 9th International Conference on Information Systems for Crisis Response and Management* . Vancouver: Simon Fraser University. Retrieved from http://www.iscramlive.org/ISCRAM2012/proceedings/260.pdf

Neubecker, K. A. (2013). *Szenarien für RIKOV: Ein Katalog möglicher Szenarien*. RIKOV Zwischenbericht (unpublished). Neubiberg.

Saaty, T. L. (2008). Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy / network process. *RACSAM*, *102*(2), 251–318.

Shim, J. P., Warkentin, M., Courtney, J. F., Power, D. J., Sharda, R., & Carlsson, C. (2002). Past, present, and future of decision support technology. *Decision Support Systems*, *33*(2), 111–126.

Sojda, R. S. (2007). Empirical evaluation of decision support systems: Needs, definitions, potential methods, and an example pertaining to waterflow management. *Environmental Modelling & Software*, *22*(2), 269–277.

Stein, B., Sauermann, M., Kleine Büning, H., Kelbassa, H.-W., Reckmann, A.-a., & Tellmann, R. (2007). *Fallbasiertes Schließen - Case-Based Reasoning. Grundlagen und Anwendung für Konstruktions- und Entwurfsaufgaben* (Forschungsbericht). Universität Paderborn, Paderborn.

Zimmermann, H.-J., & Gutsche, L. (1991). *Multi-Criteria Analyse: Einführung in die Theorie der Entscheidungen bei Mehrfachzielsetzungen. Heidelberger Lehrtexte Wirtschaftswissenschaften*. Berlin: Springer-Verlag.

CONCEPTUAL FRAMEWORK FOR EVALUATION OF THE EFFECTIVENESS OF INTELLIGENT SECURITY MEASURES IN PUBLIC TRANSPORTATION THROUGH A MULTI-AGENT-SIMULATION DATA FARMING EXPERIMENT TO PREVENT TERRORIST ATTACKS

Holger Bracker[1], Florian Brauner[2], Daniel Kallfass[3], Andreas Lotter[2], Ompe Aime Mudimu[2] and Alex Lechleuthner[2]

[1] *holger.bracker@airbus.com*
Airbus Defence and Space GmbH, Communications, Intelligence and Security (CIS), Landshuter Str. 26, 85716 Unterschleißheim (Germany)

[2] *rikov@f09.fh-koeln.de*
Cologne University of Applied Sciences, Institute of Rescue Engineering and Civil Protection, Betzdorfer Str. 2, 50679 Cologne (Germany)

[3] *daniel.kallfass@airbus.com*
Airbus Defence and Space GmbH, Studies & Innovative Concepts Germany, Claude-Dornier-Straße, 88090 Immenstaad (Germany)

Abstract

Dealing with terrorist attacks is a major challenge - especially for critical infrastructure protection when hazards cannot be described in normative risk management systems, e.g., anthropogenic threats with low probability but high consequences.

Using the example of rail-bound public transportation, a multi-agent simulation of a terrorist attack on a fictitious train station provides a basis for evaluating the effectiveness of intelligent security measures. Using different scenario constellations, the challenge of assessing low terror event probabilities empirically or historically can be replaced by conducting simulation experiments for a wide bandwidth of possibilities and analysing this data for further risk management assessment. This process is called Data Farming: in this paper, it is applied to a specific case and the results obtained are discussed. It is shown that the proposed approach gives essential support to decision-makers who are in charge of shaping security systems according to the given requirements.

Furthermore, the conceptual framework includes an expert table-top-exercise and a realistic exercise in a real train station in Cologne. The outcome and the course of the exercise were captured numerically to compare it with the simulation results and used to calibrate the simulation model.

Keywords: multi-agent-simulation, real exercise, security measures, system design, RiKoV

1 INTRODUCTION

Terrorist attacks have become a growing danger in recent years, as they aim to harm as many people as possible. Frequently chosen targets among mass gatherings (sports, music etc.) are public transportation systems such as airports and train stations. Thus, there is an increasing need of methodologies and tools to assess existing, but also future security measures with respect to their ability to prevent such attacks.

A well-suited scenario-based approach to cope with this task is using an agent-based simulation. Once appropriate models for all relevant scenario elements are designed and implemented, simulation runs will create possible courses of action. By measuring the outcome of the simulation with appropriate performance indicators, it is then possible to assess these security measures in a quantitative manner.

The multi-agent approach has been successfully applied in various domains relevant to security, such as for airport security [1] [2], maritime security [3] and district security [4], to mention just a few. The domain of interest of this paper is public rail-bound transportation, with a focus on train stations.

2 MULTI-AGENT SYSTEMS

Multi-agent systems (MAS) consist of agents and an environment. The fact that each agent has a specific behaviour and interacts with other agents as well as the environment, can lead to unpredictable behaviour in a system. This is one of the strengths of the approach and may lead to insights that cannot be gathered otherwise. A further significant benefit of this approach is that the operational setting of the scenario can be modelled in a realistic manner. To allow as much flexibility as possible, the scenario and the main elements may be defined by parameters. The set of all parameter settings is called a scenario configuration. The outcome of the simulation may be measured by indicators, the so-called “measures of effectiveness” (MoEs). Typical indicators are the number of casualties or injured people, the time to achieve a certain goal, etc.

2.1 The Data Farming Approach

Data Farming [5] is an approach for conducting simulation-based experiments that creates huge data files (MoEs) for a large number of possible scenario configurations. It allows one to analyse statistically the configurations and identify specific configurations that the user is interested in. This offers the possibility to investigate the results for robustness and possible outliers. In our case, the scenario configuration will be concerned with the properties of the individual security measures as well as the composition of the overall security setting.

To get a complete picture of all possible configurations of interest, a permutation of all input parameters would be necessary, requiring a tremendous number of simulation runs. However, appropriate designs of experiments (DoE) improve the situation significantly by using intelligent sparse sampling of the input parameters with only a fraction of all possible combinations. Together with a High Performance Computing (HPC) platform, the time to create the simulation results for all desired parameter variations can be decreased to an acceptable time span.

3 THE SCENARIO

The scenario (“system”), which will be investigated in this paper, is a terrorist attack at a major train station. The basic elements of the scenario are the following: An attacker, a number of security measures (cameras, explosive detectors and police patrols), pedestrians and an environment.

3.1.1 Environment

The environment is a 3D geometry model, which represents a large train station in London. An additional navigation mesh allows realising realistic movements of humans by indicating obstacles or areas where it is not possible to walk (e.g., barriers or rails).

3.1.2 Sensors

Cameras and explosive detectors are sensors. Cameras allow identifying (by an operator) suspicious persons by their appearance and behaviour, whereas explosive detectors may detect explosives on the body of a suspicious person. Explosive detectors are not yet readily available on the market. A prototype in development is the HAMLeT (Hazardous Material Localisation and Person Tracking) system [6].

Depending on the sensor type, the probability of detection varies and needs to be set in the simulation environment.

The mode of operation of a sensor is as follows: Once the attacker remains sufficiently long in the area illuminated by the camera (modelled by a line-of-sight check taking into account occlusions), the sensor triggers, according to a given detection probability, an alarm, which again triggers a patrol to start moving towards the terrorists in order to arrest them. This is a shortcut to what happens in reality, where an operator in an operation centre supervises one or more monitors that display the images of different sensors. Once the operator detects a suspicious person, the patrol is sent to check this person for weapons or explosive substances.

3.1.3 Pedestrians

The pedestrians are modelled by agents, which are configured to exhibit arbitrary, but plausible routes when moving within the train station. They do not actively influence the course of the scenario, but can be harmed when too close to the explosion of a bomb. An injury model estimates the degree of severity in several categories. Thus, the approximate human damages caused may be measured.

3.1.4 Terrorist

The terrorist is an agent who is acting according to a plan: Moving to a platform area, where a train is about to arrive, with the intention of detonating a bomb there.

3.1.5 Patrol

The patrol is modelled by two security agents moving in formation (either in parallel or one behind the other). Their task is two-fold: They may detect the terrorist during their regular courses, approach and arrest him/her or approach and arrest him/her on order from above. Each security agent perceives the environment by a sensor modelling the human sight.

Figure 1: Scenario realization in a virtual 3D train station (source: AIRBUS DS)

3.1.6 Course of the scenario

On the way to the track platform, the terrorist risks entering areas that are illuminated by sensors. If this is the case and the terrorist stays sufficiently long in the sensor cone,

an alarm will trigger the patrol with a certain probability. The patrol will then try to arrest the terrorist but this is only possible if the patrol reaches the terrorist in time. The terrorist may also be spotted by the patrol directly. The outcome of the scenario is simply measured by a true or false flag indicating if the terrorist could successfully ignite the bomb or not.

4 RESEARCH QUESTIONS, EXPERIMENTAL DESIGN AND RESULT ANALYSIS

Research questions may be formulated on two levels: On an overall system level, it is interesting to know which security measures should be considered in the overall system. On a system element level, it is interesting to analyse how characteristics (parameters) of isolated security elements should be chosen in order to meet the given requirements. Obviously, both research questions go hand in hand.

In order to get insights on the ability of security measures to prevent terroristic attacks, we define the following tasks:

1. The security measures in question are explored individually and in combination with fixed detection probabilities
2. The security measures in question are explored in combination
3. The detection probabilities of each security measure are varied from 0 to 100%
4. For the future HAMLeT device, a requirement for the detection probability will be derived.

For each task, an appropriate experiment may be set up. However, it is also possible to create all data for tasks 1 to 3 in a single experiment. This is more efficient as only one experiment has to be set up.

The total number of simulation runs is estimated as follows: We consider three security measures, thus the number combinations is $2^3 = 8$. We sample the probabilities of detection for each security measure from 1% to 100% in 6 equidistant steps, thus the number of combinations is $6^3 = 216$. For each run, 200 replicates are carried out to eliminate stochastic influences (e.g., the randomly chosen path of the attacker or the current position of the walking patrol at the time the attacker enters the train station) which cannot be controlled. This results in 8*216*200 = 345,600 runs that are partly executed on a High Performance Computing (HPC) cluster.

After each simulation run, it is recorded whether the attack could successfully be prevented or not. In the following, we present the results of the four tasks and discuss them briefly.

4.1.1 Experiment #1

Based on each security measure the probability of attack prevention is measured through all simulation results. The results of this experiment are depicted in the following table.

Table 1: Results of probabilities in experiment #1 (source: AIRBUS DS)

Security measure	Probability of detection [%]	Probability of attack prevention [%]
No security measure	0%	0%
Patrol (consisting of 2 persons)	10% (per person)	14.5%
Cameras (10 in total)	2% (per camera)	3.5%
HAMLeT (2 in total)	95% (per system)	93.5%

The probabilities of preventing an attack is hereby not equal to the cumulated detection probability of all security measure instances (e.g., ten cameras) due to the fact that the patrol needs to arrest the attacker before he can trigger his bomb, and the cameras and patrols need to have line-of sight through the 3D environment with visual obstacles like walls to the moving attacker.

The results show that if no security measures are active, the attacker will not be prevented from performing the attack, thus the probability of prevention is zero. Although this is a trivial insight, it is a simple check for the plausibility of the model. The patrol and the cameras perform poorly with a probability of attack prevention of 14.5% and 3.5% respectively. Obviously, HAMLeT is the most effective security measure with a result of 93.5% that is due to a detection probability which is significantly higher than that of the other security measures.

4.1.2 Experiment #2

The second experiment illustrates the probabilities of attack prevention for the following combinations of security measures.

Table 2: Results of probabilities in Experiment #2 (source: AIRBUS DS)

Combination of security measures	Probability of attack prevention [%]
Patrol + cameras	19.5%
Patrol + HAMLeT	93.0%
Cameras + HAMLeT	94.5%
Patrol + cameras + HAMLeT	96.5%

The results shown in this table confirm one's intuition: HAMLeT is the dominating security measure and its capability to prevent attacks can only be slightly improved by adding additional security measures.

4.1.3 Experiment #3

The purpose of the third experiment is to show how the detection probability of an individual security measure influences the probability that the overall system is able to prevent an attack. For that purpose, the probability of detection is varied in six steps from 1% to 100%. The results are shown in Fig. 2 below.

From these results, the following conclusions can be drawn: although an attacker is detected by the patrol in all cases (probability of detection is 100%, see (a)), the probability of the system to prevent the attack is only 55%. The reason is that the patrol moves around the train station and does not always have the chance to get close to the attacker in order to detect and arrest him/her in time.

Cameras and HAMLeT correlate linearly (see (b) and (c)) that may be interpreted as an improvement possibility of the detection probability of a camera or HAMLeT in the future (e.g., through higher resolutions or better image recognition algorithms). This improvement will proportionally increase the probability of attack prevention. Cameras and HAMLeT may reach values close to 100%, but at least in the case of cameras, a 100% probability of detection is a theoretical value and very hard to achieve in reality.

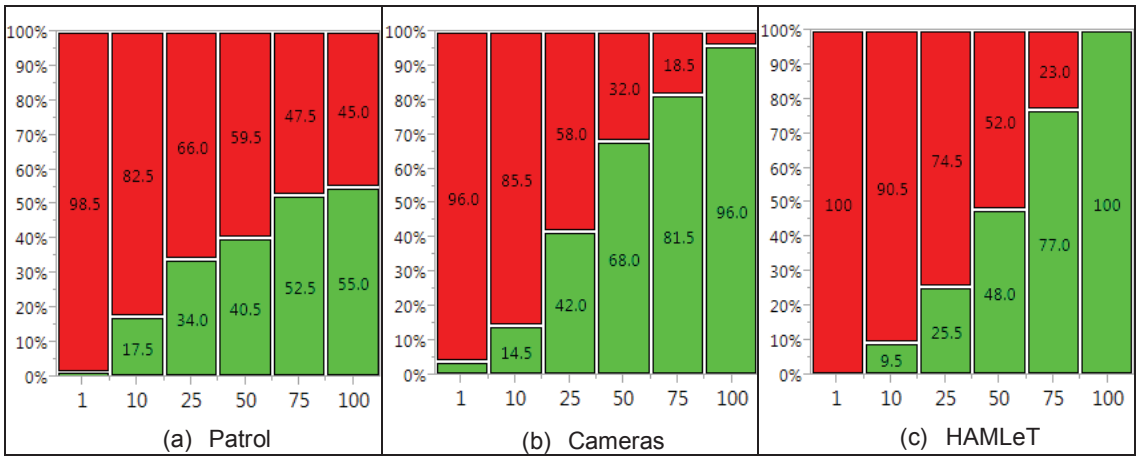


Figure 2: Bar chart - results of Experiment #3 (x = detection rate / y = part of prevented attacks) (source: AIRBUS DS)

4.1.4 Experiment #4

The purpose of this experiment is to explore how a new sensor device such as HAMLeT may improve a system composed of "conventional" security measures (cameras and patrol). Therefore, we keep fixed values of detection probabilities for the latter ones, and we vary the detection probabilities of HAMLeT from 0% to 100% in ten steps. The results are shown in the diagram in Fig. 3.

If the probability of prevention (y value in Fig. 3a) is set as a requirement, it is then possible to estimate a required probability of detection for the HAMLeT device.

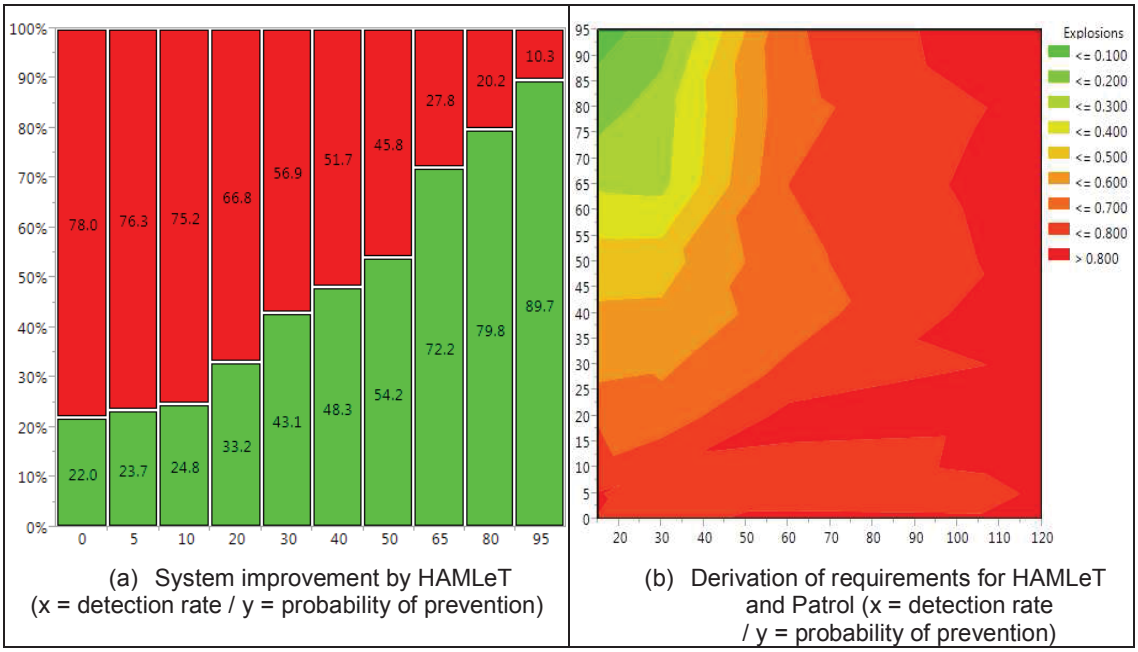


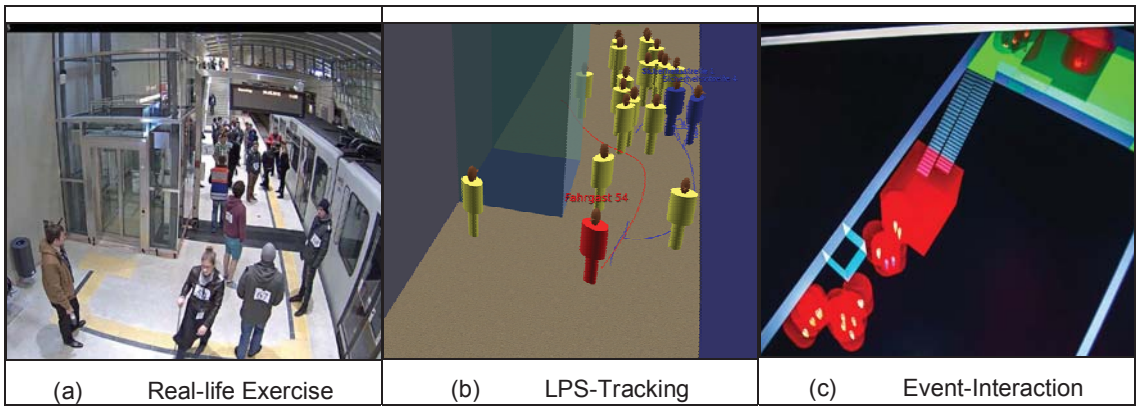
Figure 3: Results of Experiment #4 (source: AIRBUS DS)

The quality of the HAMLeT device, however, must not be seen isolated in terms of probability of detection. The quality of HAMLeT is also closely linked to the patrol that needs to appear in time to arrest the attacker. Stipulating that 70% or more of all attacks are to be prevented successfully, Fig. 3b shows that this can be achieved and that HAMLeT has a probability of detection of at least 65% if the patrol reacts within 60 seconds.

5 VALIDATION THROUGH REAL-LIFE EXERCISE

Multi-agent systems are simulations, which highly depend on the former pre-setting of definitions, e.g. customer/ terrorist or security measure behaviour [7]. Often, scientific values can be used to define such settings, but in many cases a lack of information requires using assumptions or iterative pre-tests. Expert interviews would improve these assumptions and therefore should be carried out more frequently [8].

Real-life exercises provide a good data basis for filling the gap of information, which is needed. In this case, we executed a real-life exercise in a subway train station with one hundred passengers and nine different security measures to collect data about customers' and security measures' behaviour. To capture and assess the exercise, ten experiments were executed and all participants were tracked in time and location via an ultra-wide-band local positioning system (LPS). The data delivers patterns of behaviour that can be compared with the pre-setting of MAS and also with the simulations results.



(a) Real-life Exercise (b) LPS-Tracking (c) Event-Interaction

Figure 4: Exemplary snapshot of real-life exercise and person tracking (source: CUAS)

In this example, the route of security patrols and a fictive attacker were evaluated according detection possibilities and possible bypassing actions in the so-called "modus operandi" of the attacker (see Fig. 4). The results influence the effectiveness of the security measure. The same analysis was executed with camera ranges.

Although real-life exercises are extensive and time-consuming, the combination with MAS enriches the results of simulations and provides important contributions to further simulation runs in general.

6 CONCLUSION

The presented agent-based simulation approach in conjunction with the Data Farming approach is well-suited to obtain insights on the performance of security measures in an operational context. As the interaction between physical devices, operational processes and local conditions quickly leads to unforeseeable consequences, this approach may support decision-makers in charge of designing security systems. The approach allows one to obtain insights into weaknesses and strength of existing systems, but also on how new devices would affect the system properties and how those need to be designed to meet a given overall system performance.

The comparison of MAS with real-life exercises allows validating the simulations with real patterns and enriches the simulations by strengthening the definitions of multi-agents for new simulation runs. In the future, we will focus on further combinations of simulations and real-life exercises in order to make simulations even more reliable as

well as applicable for end-users to support the decision-making process for designing security systems [9]. Two aspects will be in focus of the future research activities: Firstly, the interaction of security measures among each other with their positive and negative effects and secondly, the understanding of the detection probability and prevention probability complex.

ACKNOWLEDGEMENT

The presented work in progress is a result from our research within the project 'RiKoV'. The research presented in this paper is supported by the German Federal Ministry of Education and Research (BMBF). We would like to thank the BMBF as well as the 'RiKoV' project partners for the fruitful collaboration.

REFERENCES

[1] Zhang, Y. and Brown, D. E. (2013). *Police patrol districting method and simulation evaluation using agent-based model & GIS*. Security Informatics 2013, 2(7) doi:10.1186/2190-8532-2-7.

[2] Vaněk, O.; Jakob, M.; Hrstka, O.; Pěchouček, M. (2013). *Agent-based model of maritime traffic in piracy-affected waters*. Transportation Research Part C. Emerging Technologies 36, pp. 157-176.

[3] Meinberg, U.; Lorenz, C.; Huber, L.; Papproth, A.; Stegner, C and Hyka, R. (2010). *Agent-based Simulation of Security Related Logistic Processes on Airports*. 14th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando/ Florida, 29.06.-02.07.2010 http://www.iiis.org/CDs2010/CD2010SCI/SCI_2010/PapersPdf/SA804GA.pdf

[4] Weiss, W.E. (2008) *Dynamic Security: An agent-based model for airport defense*. In: Mason, S. J.; Hill, R. R.; Mönch, L.; Rose, O.; Jefferson, T.; Fowler, J. W. (eds.). Proceedings of the 2008 Winter Simulation Conference.

[5] Horne, G. and Meyer, T. (2004) Data Farming: Discovering Surprise. In: Ingalls, R, Rossetti, M.D., Smith, J. S. and Peters, B. A. (eds.) In: Proceedings of the 2004 Winter Simulation Conference, p. 171-180. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

[6] HAMLeT - EU project HAMLeT (PASR-2006). http://europa.eu/rapid/press-release_MEMO-06-375_en.htm

[7] Fonseca, S.P.; Griss, M.L. and Letsinger, R. (2002). *Agent Behavior Architectures - A MAS Framework Comparison.* In: Proceedings of AAMAS (Bologna, Italy) ACM Press, New York.

[8] Brauner, F.; Maertens, J.; Bracker, H.; Mudimu, O. A. and Lechleuthner, A. (2015). Determination of the effectiveness of security measures for low probability but high consequence events: A comparison of multi-agent-simulation & process modelling by experts. The 12th International Conference on Information Systems for Crisis Response and Management. In: L. Palen, M. Buscher, T. Comes, and A. Hughes (Eds.), ISSN: 2411-3387, ISBN: 978-82-7117-788-1.

[9] Lin, L.; Brauner, F.; Muenzberg, T.; Meng, S.; and Moehrle, S. (2013). Prioritization of security measures against terrorist threats to public rail transport systems using a scenario-based multi-criteria method and a knowledge database. 8th Future Security Conference, Berlin, Germany.

EXPLORING DATA ANALYSIS TECHNIQUES FOR THREAT ESTIMATION

Matthias Dehmer[1], Alex Lechleuthner[2], Ompe Aime Mudimu[2] , and Stefan Pickl[1]

[1] matthias.dehmer@unibw.de, stefan.pickl@unibw.de
Universität der Bundeswehr München, Fakultät für Informatik,
Institute for Theoretical Computer Science, Mathematics and
Operations Research
Department of Computer Science,
Neubiberg, (Germany)

UMIT, Department of Biomedical Computer Science,
Eduard Wallnöfer Zentrum 1
Hall in Tyrol (Austria)

[2] alex.lechleuthner@fh-koeln.de, ompe_aime.mudimu@fh-koeln.de
Faculty of Process Engineering, Energy and Mechanical Systems
Institute of Rescue Engineering and Civil Protection
Cologne University of Applied Sciences, Cologne, (Germany)

Abstract

This paper discusses data analysis techniques for threat estimation. We mainly survey existing methods from the area of transportation and threat analysis and also mention techniques which have been used in RIKOV.

Keywords: data analysis, security, threat, complex networks

1 INTRODUCTION – THREAT ESTIMATION

Terrorist threats, always together with criminal activities and vandalism, are dangerous and complicated for any kind of transportation system. Some characteristics such as accessibility, affordability, availability of public transportation make such a system vulnerable to terrorist attacks. Generally, public transportation has become one of the most preferred targets of terrorists and, therefore, it needs considerable attention when it comes to analyze the possibility of threat.

Towards estimation of threats, many different circumstances need to be considered, for instance, which kind of public transportation and terrorist attacks, the place where the terrorist attack will happen, how many innocent people there are in the attacked place, and so forth. Importantly Naşcu [1] pointed out that, whatever the situations are, the process of threat evaluation follows a procedure consisting of eight steps. The first step is the preparation stage of evaluation process. Information of possible terrorist attacks need to be known. The second step is the detection of the critical assets, based on the aforementioned information. The third step is the identification of these critical assets with greatest impact on people and system. The fourth step relates to the determination of threats to these key assets. The fifth step is developing alternative solution scenarios for the threats, based on aforesaid information. The sixth step is to reckon anticipated consequences of threats. The seventh step is not only to classify the hierarchy of vulnerable spots in public transportation but also to make some decisions on choosing the appropriate corresponding safety

measures. The eighth step is to audit the implementation of safety measures. We see that threat estimation is multifaceted.

This paper is mainly a survey of data analysis and visualization techniques for threat estimation in the area of public transportation. To perform the review, we put the emphasis on methodical aspects of such methods; this is important when designing new applications.

2 VISUALIZATION TECHNIQUES

Another possibility to solve the problem in the above mentioned area relates to visualize the possibility of threat. Until now, various visualization techniques have been widely used in public transportation. One of these visualization technologies is video surveillance that has been introduced in [2]. The video surveillance turns out to be important for transportation security. Actually, it has been extensively used in plenty of major cities around the world for monitoring airports, railway and subway stations, bus stations, sea ports, and so on. As the developments of video-capturing hardware, advances in thermal and infrared (IR) technology, computer networks, and algorithmic advances in computer vision and image processing, the video surveillance becomes more scalable and cheaper. The combination of these technologies could help to extract some useful and important information such as recognition of face and detection of intention from real-time video stream data provided by video surveillance. Therefore, this tool might be helpful for making decisions.

Also Zeng [2] introduced tracking and location technologies such as Global Positioning System (GPS) and Radio Frequency Identification (RFID), which can be used to monitor moving objects or key assets of interest. But such technologies still have their own information security vulnerabilities, so they have both opportunities and challenges to identify interesting and relative patterns from spatial data streams and to use these technologies in the area of public transportation security.

As we know, sensors play an irreplaceable important role in the area of visualization. In [3], Hallowell introduced lots of sensor technologies. These technologies under consideration mainly contain sonar, seismic, radar, video imaging, ASDE-X radar, microwave, and ground-based radars. They have been widely used not merely for detection of intrusion of perimeter and surveillance but also for detection of breach and control. Furthermore, Hallowell also introduced bulk sensors, which mainly include computed tomography, neutron interrogation, nuclear quadrupole resonance, X-ray diffraction, dual energy X-ray, millimeter wave, and X-ray backscatter imaging. These bulk sensors are often used for detection of explosives and weapons.

In [4], Wang introduced Geographic Information Systems (GIS), simulation models and computer visualizations. In order to integrate these three technologies into one system for supporting planning and decision-making in traffic, Wang developed a prototype traffic impact analysis system. In such integrated system, these three technologies contribute different features. Since there are many spatial relationships among entities, the aim of GIS is to provide some functions allowing users to check these relationships. Yet the simulation modeling deals with displaying dynamic relationships between causes and effects. Moreover, the goal of computer visualization is to represent data in an understandable way.

A more abstract approach to visualize the possibility of threat is based on using complex networks [14, 15]. For instance, so-called transportation networks [15] can be used to model, e.g., train networks and other network-based transportation systems. Such a network represents a relational structure that consists of vertices and edges. So, the structure of a network can be now analyzed in terms of specific properties, e.g., the network topology or local properties such as hubs of a network [15]. It is obvious that network visualization might be helpful to examine the possibility of threat towards a given network. However, network

visualization is far from trivial as it is not clear what kind of structural features should be emphasized. A powerful attempt in this direction is due to Tripathi et al. [16]

3 DATA ANALYSIS TECHNIQUES

Numerous data analysis methods have been developed for analyzing public transportation systems. In [5], Kastrinaki and Zervakis, et al. performed a survey on video processing techniques applied to traffic systems. Due to different input data, such as feature-driven data, area-driven data and model-based data, and different domains of processing, such as spatial/frame and temporal/video, the approaches of image-processing should also be distinguished. As demonstrated in [12], when a large number of cameras are connected to computers, the computers can automatically detect suspicious activities by applying complex vision-based algorithms.

In [10], Barai made a review on further applications of data mining to transportation engineering problems. The data mining could be used to extract the previously unknown and potentially useful information from a large amount of data. The author demonstrated the typical example of “Vehicle Crash Study” to illustrate the application of data mining to transportation engineering problems. Meanwhile, Barai emphasized the potential of applications of data mining in transportation engineering sector.

In [11], Bi and Omer, et al. proposed a method to model the probability of pedestrian detection as a function of distance and image metrics. This presented approach has three steps. First, based on combinations of image metrics, the authors developed some models of detection probability of one pedestrian. After that, another model was developed, which illustrates the relationship between the distance to a pedestrian and an image-based pedestrian size metric. Finally, a final model of detection probability as a function of distance and image metrics was developed by combining models of both the distance and the detection probability. In practice, these models cannot merely be used to predict pedestrian-detection performance with night-vision systems, but they are also capable of estimating the effectiveness and efficiency and support the development of night-vision systems.

In [13], Nishiuchi and Todoroki, et al. presented a method to evaluate transfer nodes based on smart card data. The proposed approach applied the Data Envelop Analysis (DEA) model to evaluate the efficiency of user transfers between transportation systems. The authors mainly discussed two types of DEA model, which are the Charnes, Cooper & Rhodes (CCR) model and the Banker, Charnes Cooper (BCC) model.

4 RISK ANALYSIS

In [6], Haimes and Kaplan, et al. developed the Risk Filtering, Ranking, and Management (RFRM) method for risk analysis. As pointed out by Kaplan and Garrick (1981), during the risk assessment process, there are three questions that need to be answered: what can go wrong? What is the likelihood of something wrong will happen? What are the consequences of these happened wrong things? The proposed RFRM approach consists of eight major phases.

Phase I is the identification of risk scenarios through Hierarchical Holographic Modeling (HHM). During this phase, most sources of risk are distinguished through the HHM approach into distinct categories of risk scenarios such as acts of terrorism, accidents and natural hazards. Actually, the risk scenarios are the descriptions of what can go wrong. The phase II is scenario filtering based on scope temporal domain, and level of decision making. In this phase, according to the interests and responsibilities of a risk manager, the sources of risk are filtered. This phase could reduce the number of risk sources significantly. The phase III is a bi-criteria filtering process and ranking using the ordinal version of U.S air force risk matrix. This kind of matrix denotes the severity of a scenario by combining the likelihood of a given scenario occurring and consequences of corresponding scenario if it occurs. The phase IV is

a multi-criteria evaluation. The aim of this phase is reflecting the ability of each scenario to respond to the three defensive properties including resilience, robustness and redundancy. Furthermore, the phase V relates to perform a quantitative ranking using the cardinal risk matrix. In this phase, the likelihood of each scenario is quantified by using Bayes Theorem and all the relevant evidence available. Moreover, the phase VI is risk management. The phase VII is safeguarding against missing critical items. In this phase, the performance of the selected scenario against these filtered-out scenarios will be checked. The final phase is operational feedback. The purpose of this phase is to update the strategies of scenario filtering and decision processes on the basis of the obtained experience and information.

In [8], Leventakis introduced a comprehensive Transportation Security Risk Assessment Framework. Based on a repetitive process of risk evaluation and assessment of severity, Leventakis defined a common Risk Analysis Framework for interconnected and heterogeneous transportation networks. Meanwhile the Risk Analysis Framework also takes the Likelihood of occurrence and the Consequences into account. The proposed method is not only analytic enough to include an exhaustive list of threats relating to transportation but also has an intrinsic framework to evaluate the propagation of risk to the interconnected transportation assets.

In [9], Willis firstly presents a definition of terrorism risk, which contains three components that are the threat to a target, the vulnerability of target to the threat, and the consequences should an attack be conducted on the target successfully. The authors conducted the risk analysis from these three perspectives of components of terrorism risk. In [9], Willis also discussed the uncertainty and value judgments in terrorism risk assessment. Moreover, the authors introduced two methods to estimate the terrorism risk in urban areas, that is, the simple risk indicators and event-based models. As examples, the authors addressed one of simple risk indicators Population-based Metrics, and one of event-based models the Risk Management Solutions (RMS) Terrorism Risk Model. These two comparative examples are made to illustrate the strengths and weaknesses of each method. Furthermore, the authors also discussed the performance of distinct estimates of terrorism risk.

In [17], Meyer-Nieberg et al. explored the vulnerability of public transportation. They introduced a three-model approach as an analysis tool for identifying critical points of passenger flows. The approach proposed combining approaches of different level of detail. Note that parts of this work have been demonstrated in RIKOV successfully.

5 CONCLUSIONS AND OUTLOOK

In this paper we briefly surveyed methods to analyze the possibility of threat in the area of public transportation. This relates to discuss visualization techniques for data sets and networks. Also, we explored data analysis techniques for this purpose. We have seen that threat analysis is far from trivial as it depends from various factors. Also, finding the right data analysis methods has been difficult as well.

In the future, we try to apply some of the mentioned in RIKOV as well. In particular, this relates to apply novel risk analysis methods to transportation networks. For this, we have to meet the challenge combining risk theory and graph theory properly.

6 ACKNOWLEDGMENT

We gratefully acknowledge financial support from the German Federal Ministry of Education and Research (BMBF) (project RiKoV, Grant No. 13N12304).

REFERENCES

[1] Naşcu, Ioan. "Terrorist Threats and Public Transportation." Theoretical and Empirical Researches in Urban Management (2009): 80-81.

[2] Zeng, Daniel, et al. "Protecting transportation infrastructure." Intelligent Systems, IEEE 22.5 (2007): 8-11.

[3] Hallowell, Susan F., and Paul Z. Jankowski. "Transportation security technologies research and development." Military Communications Conference, 2005. MILCOM 2005. IEEE, 2005.

[4] Wang, Xinhao. "Integrating GIS, simulation models, and visualization in traffic impact analysis." Computers, Environment and Urban Systems 29.4 (2005): 471-496.

[5] Kastrinaki, V., Michalis Zervakis, and Kostas Kalaitzakis. "A survey of video processing techniques for traffic applications." Image and vision computing 21.4 (2003): 359-381.

[6] Haimes, Yacov Y., Stan Kaplan, and James H. Lambert. "Risk filtering, ranking, and management framework using hierarchical holographic modeling." Risk Analysis 22.2 (2002): 383-397.

[7] Jones, Elizabeth V., et al. "Virgina's critical infrastructure protection study." Systems and Information Engineering Design Symposium, 2003 IEEE. IEEE, 2003.

[8] Leventakis, G., et al. "A Security Risk Analysis Framework for Interconnected Transportation Systems." Proceedings of the 8th International Conference on Information Systems for Crisis Response and Management, ISCRAM2011. 2011.

[9] Willis, Henry H., et al. Estimating terrorism risk. Rand Corporation, 2006.

[10] Barai, Sudhir Kumar. "Data mining applications in transportation engineering." Transport 18.5 (2003): 216-223.

[11] Bi, Luzheng, Omer Tsimhoni, and Yili Liu. "Using image-based metrics to model pedestrian detection performance with night-vision systems." Intelligent Transportation Systems, IEEE Transactions on 10.1 (2009): 155-164.

[12] Goldgof, Dmitry B., et al. Evaluation of Smart Video for Transit Event Detection. No. Report No. 2117-7807-00. 2009.

[13] Nishiuchi, Hiroaki, Tomoyuki Todoroki, and Yusuke Kishi. "A Fundamental Study on Evaluation of Public Transport Transfer Nodes by Data Envelop Analysis Approach Using Smart Card Data." Transportation Research Procedia 6 (2015): 391-401.

[14] Dehmer, Matthias, Emmert-Streib Frank. Quantitative Graph Theory. Theoretical Foundations and Applications, CRC Press, 2014

[15] Dehmer, Matthias, Emmert-Streib Frank, Mehler Alexander. Towards an Information Theory of Complex Networks: Statistical Methods and Applications, Birkhäuser Publishing, 2011

[16] Tripathi Shailesh, Dehmer, Matthias, Emmert-Streib Frank. NetBioV: An R package for visualizing large network data in biology and medicine, Bioinformatics, 2014

[17] Meyer-Nieberg Silja, Dehmer Matthias, Bracker Holger, Schneider Berhard, Assessing the Vulnerability of Dynamical Systems in Public Transportation, Proceedings of the 9th Future Security, Berlin, 247-252, 2014

ASPECTS OF QUANTITATIVE ANALYSIS OF TRANSPORTATION NETWORKS

Matthias Dehmer[1], Marian Sorin Nistor[2], Walter Schmitz[3], and Karl Adolf Neubecker[4]

[1] *matthias.dehmer@umit.at*
The Health and Life Sciences University (UMIT), Eduard Wallnöfer-Zentrum 1, A-6060 Hall in Tirol (Austria)

[2] *sorin.nistor@unibw.de,* [3] *fam.schmitz-walter@t-online.de,* [4] *adineubecker@web.de*
Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85577 Neubiberg (Germany)

Abstract

In this paper, we describe numerical results when applying quantitative graph theory to a set of transportation networks consisting of 34 large international subway networks. So far, the networks have been analyzed by using standard indices for characterizing networks. Therefore we here put the emphasis more on using statistical measures like entropy. Also we draw conclusions how these results can be used and compared with classical methods/measures for determining, e.g., the structural complexity of transportation networks.

Keywords: Transportation networks, quantitative graph theory, graph entropy, structural indices

1 INTRODUCTION

Quantitative graph analysis has been a major research field for various disciplines [1–3]. One important question in this field is examining whether a method/measure captures structural information properly. One specific way to tackle the problem would be through classical methods for determining the structural information content of a graph by partitioning groups of vertices to infer a proper probability distribution [4–7].Thereby, a graph entropy measure representing the structural information content of a graph can be determined using Shannon's entropy [8], but the probabilities need to be defined properly. This has been a challenging problem and surely depends on the underlying application domain.

Entropy-based methods have been used in research fields such mathematical chemistry, cybernetics, and computational physics, see [9–11]. For quantitative analysis of transport networks, specifically represented by subway networks, mostly standard indices have been used [12].

To determine the structural complexity of a graph, an information-theoretic approach of [13] has been used for this paper. This method avoids the problem of determining vertex partitions for defining the entropy of a graph by using a probability value for each vertex of the graph. Thus, the local vertex functionals, defined as positive mappings, have been used for quantifying the structural information based on a given probability distribution [14].

The main purpose of this paper is to analyze entropy measures on a set of international subway networks [12] by using an information-theoretic method and to compare the results with some other classical graph measures. This relates to determining the structural complexity of transportation networks. Discussing the numerical results of the entropies is the main contribution of this paper. In this sense, we first present all key

steps of our method applied to the mentioned networks. Then, we demonstrate the feasibility and usefulness of the method for this type of networks by analyzing the relationships between the graph entropies, starting from different information functionals, in comparison with other classical graph measures, e.g., Wiener index [15], and Randić index [16].

The structure of this paper is organized as follows: in Section 2, we introduce the method by presenting the key steps of determining the graph entropy measures concept of Dehmer [13], and we present the information functional to be used for computing the graph entropies. In Section 3, we summarize the numerical results to investigate the impact of different information functionals on the measured entropies and the connection with some other classical graph measures. The paper ends with a summary and conclusion in Section 4.

2 ENTROPY MEASURES BASED ON INFORMATION FUNCTIONALS

In this section, we present the information indices which are based on the full topological neighborhood of all vertices of the transportation network [14].For this, we use the method developed by Dehmer [13] for deriving graph entropy measures which are based on information functionals. An information functional is a mapping that quantifies structural information of a network[14]. The advantage of using this method is that the probability values are not determined for each subtracted partition, but for each vertex of the network.

We define $G = (N(G), E(G))$ as a finite and connected network. $N(G)$, and $E(G)$are called vertex and edge set of network G, with the diameter $\rho(G)$, and $\delta(v)$ the degree of vertex $v \epsilon N(G)$. For $|N(G)| < \infty$,$|E(G)| < \infty$, we can define $|N(G)| := N$, respectively $|E(G)| := E$. An information functional f that quantifies the structural information of $G$is defined [17] as:

$$I_f(G) := -\sum_{i=1}^{N} \frac{f(v_i)}{\sum_{j=1}^{N} f(v_j)} \log\left(\frac{f(v_i)}{\sum_{j=1}^{N} f(v_j)}\right), \quad (1)$$

where $I_f(G)$ is a family of graph entropy based on information functional. The distance between the entropy defined in equation (1) and the maximum entropy $(log\ (N))$ is defined [17] as:

$$I_f^{\lambda}(G) := \lambda\left(\log(N) + \sum_{i=1}^{N} \rho(v_i)\log(\rho(v_i))\right), \quad (2)$$

$$\rho(v_i) := \frac{f(v_i)}{\sum_{j=1}^{N} f(v_j)}\ , \quad (3)$$

where $\rho(v_i)$ are the vertex probabilities with$\lambda > 0$ as a scaling constant[17].

In this paper, we use the information functional $f^V(v_i)$[14] to capture the information structure of the complete neighborhood of each vertex on a transportation network by taking into account the number of vertices in the available j-spheres around a vertex. The j-sphere of a vertex v_i from a network $G$is defined [14] as:

$$S_j(v_i, G) := \{v \in N | d(v_i, v) = j, j \geq 1\}, \quad (4)$$

where $S_j(v_i, G)$ represents a set of vertices with distances j,$v_i \in N$.The information function using the j-spheres is defined [17] as:

$$f^V(v_i) := c_1|S_1(v_i, G)| + c_2|S_2(v_i, G)| + \cdots + c_{\rho(G)}|S_{\rho(G)}(v_i, G)|, \quad (5)$$

where $c_k > 0$, and based on [20] $c_1 > c_2 \ldots > c_{\rho(G)}$.

Another meaningful information functional to compute entropy measures on transportation networks is the information functional $f^C(v_i)$[13] that captures centrality

properties of each vertex in the network. The centrality of a vertex v_i from a network G is defined [13] as:

$$\beta^{L_{G(v_i,j)}}(v_i) = \frac{1}{\sum_{i=1}^{N} d(v,v_i)} \quad , \tag{6}$$

where $\beta^{L_{G(v_i,j)}}(v_i)$ expresses that we apply β to v_i regarding the local information graph $L_{G(v_i,j)}$,$d(v,v_i)$ represents the shortest distance between $v, v_i \in N$, and $j \geq 1$ [13]. The information function using vertex centrality is defined[17] as:

$$f^C(v_i) := c_1\, \beta^{L_{G(v_i,1)}}(v_i) + c_2 \beta^{L_{G(v_i,2)}}(v_i) + \cdots + c_{\rho(G)} \beta^{L_{G(v_i,\rho(G))}}(v_i), \tag{7}$$

where $c_k > 0$, and based on[20]$c_1 > c_2 \ldots > c_{\rho(G)}$.

3 RESULTS AND DISCUSSION

The aim of this section is to investigate the impact of the entropy measures based on the transportation networks. Additionally, we also interpret the connection with some other classical measures. For analyzing the numerical results, e.g., entropy measures, and classical graph measures, we present *Table 1* to examine the extremal behavior of the values.

The chosen data to analyze for this paper consist of 34 worldwide subway networks collected by [12] (data at http://derrible.people.uic.edu/pubs.html/). The Munich subway network that we found important [21] due to its size, it is complemented to the available ones.

The statistical analysis has been performed using the programming language R [18] (Release version 3.1.3). Whence, *QuACN* package[19] based on *graph* package [22] from the *Bioconductor* project [23] was of great help to this work.

To compute the two entropy measures, we first derive the two information indices mentioned in Section 2, based on equation (2). Therefore we define $f_{lin}^{V}(v_i)$ if the coefficients $c_1, c_2, \ldots, c_{\rho(G)}$satisfy the property [14]:

$$c_1 := \rho(G), c_2 := \rho(G) - 1, \ldots, c_{\rho(G)} := 1 \tag{8}$$

$I_{f,lin^V}^{\lambda}(G)$ represents the first information index based on information functional using j-spheres with coefficients linearly decreasing while the topological distance increases.

And we define $f_{lin}^{C}(v_i)$ if the coefficients $c_1, c_2, \ldots, c_{\rho(G)}$satisfy the property (8) [14]. $I_{f,lin^C}^{\lambda}(G)$ represents the second information measure for graphs based on information functional using vertex centrality with coefficients linearly decreasing.

To capture different properties of the network, we also use classical topological descriptors, e.g., the Wiener index $W(G)$[15], and the Randić connectivity index $R(G)$[16]. $W(G)$captures the structural branching in a graph based on the shortest distance between vertices, and is defined [15] as:

$$W(G) := \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} d(v_i, v_j). \tag{9}$$

$R(G)$ captures the connectivity structural information in a graph based on the degrees of the vertices, and is defined [16] as:

$$R(G) := \sum_{(v_i,v_j)\epsilon E}[\delta(v_i)\delta(v_j)]^{-\frac{1}{2}}. \tag{10}$$

Table 1. Numerical results when using graph entropy measures, and classical measures applied to 34 subway networks.

Subway network description		Entropy measures		Classical graph measures	
G	N	$I^{\lambda}_{f,lin^V}(G)$	$I^{\lambda}_{f,lin^C}(G)$	$R(G)$	$W(G)$
Rome	5	2.291691997	2.170951	2	16
Cairo	6	2.561797395	2.472710	2.642734	29
Marseille	6	2.561797395	2.472710	2.642734	29
Delhi	8	2.974937501	2.852587	3.25	58
Prague	9	3.137872401	3.008971	3.75	75
Athena	9	3.146511813	3.051286	3.976068	84
Brussel	9	3.148544446	3.048088	4.008760	82
Toronto	10	3.298967694	3.227638	4.574586	127
Lyon	10	3.303965134	3.191903	4.315384	103
Montreal	10	3.303965134	3.191903	4.315384	103
Lisbon	11	3.440603962	3.320138	4.654701	130
Bucharest	11	3.447166499	3.359155	4.943211	130
Buenos Aires	12	3.564289701	3.434701	4.791241	154
Singapore	12	3.566564099	3.462496	5.380768	173
Saint Petersburg	14	3.779984327	3.653563	6	230
Milan	14	3.790941813	3.677794	6.136751	264
Washington DC	17	4.067472188	3.951641	7.564219	424
Hong Kong	17	4.073472036	3.989126	7.685299	458
Stockholm	20	4.305959889	4.219484	8.945988	762
Boston	21	4.373901873	4.260488	9.163460	748
Shanghai	22	4.439564553	4.321836	9.753185	711
Chicago	25	4.627309812	4.527158	11.03558	1099
Barcelona	29	4.844750440	4.734342	13.16729	1434
Berlin	32	4.990214795	4.896278	14.21587	1807
Mexico City	35	5.122056244	5.040476	15.92196	2142
Osaka	36	5.157871724	5.063904	16.32995	2439
Moscow	41	5.344479241	5.234316	18.45853	3038
Madrid	48	5.576345430	5.504596	22.32704	4621
Tokyo	62	5.944948339	5.862996	28.62657	8002
Seoul	71	6.139360595	6.034646	33.43750	12716
New York	77	6.254533823	6.143715	35.69329	15435
Paris	78	6.276859237	6.188044	35.65673	14898
London	83	6.362360456	6.247954	38.35881	18828
Munich	96	6.569532362	6.489395	47.05044	46335

Notation:

G- subway network

N- number of vertices

$I^{\lambda}_{f,lin^V}(G)$- entropy measure based on information functional using the j-spheres

$I^{\lambda}_{f,lin^C}(G)$ - entropy measure based on information functional using vertex centrality

$R(G)$- Randić's connectivity index

$W(G)$ - Wiener index

From *Table 1* we observe that the two entropy measures capture the structural information uniquely compared with the other two classical measures. $I^{\lambda}_{f,lin^V}(G)$ encode the complete neighborhood of each vertex, and $I^{\lambda}_{f,lin^C}(G)$ encode the centrality of each vertex within the network.

To interpret the extremal entropy values which can be observed in *Table 1*, and based on equation (2), we note that the smaller the entropy value, the more symmetric the network is, see also [14]. In [14], Dehmer et al, found that the measures used capture symmetry in networks. Thus the quantities can be useful when exploring the structural organization of subway networks and other kinds of transportation networks. We see that the entropy values increase with expansion of the neighborhood of a vertex within the network.

We note that even if$I^{\lambda}_{f,lin^V}(G)$,$I^{\lambda}_{f,lin^C}(G)$ and $W(G)$ descriptors are generally based on distances in a network, the values are highly uncorrelated. $W(G)$ captures the branching structural information, and we can observe that the higher the value, the more cyclic the network is.

Another observation interpreting the values from *Table 1*, is regarding the $R(G)$ values. According to [16], $R(G)$ attains a minimal value for a path network, and a maximal value for a star network. Thus, the first networks in the table are more pathshaped, while the ones toward the bottom of the table are more star shaped.

4 SUMMARY AND CONCLUSION

In this paper, we analyzed entropy measures of transportation networks by using an information-theoretic method. In addition we compared the entropy measures with other known graph measures.

We found that some of the measures can be used as useful structural measures for quantifying features of the network topology. Solving the question what kind of network topology the network has is far from trivial as the structural interpretation of the measures used is often not clear. This was a first attempt to deal with this problem when using statistical graph measures like entropy. It is likely that these measures may be used in the context of threat estimation when it comes to transportation systems. This could be valuable in case these systems are represented by networks. So, in this sense we believe that the used apparatus can be proven useful within RIKOV when dealing with networks of public transportation systems.

ACKNOWLEDGEMENTS

Matthias Dehmer, Walter Schmitz and Karl Adolf Neubecker gratefully acknowledges financial support from the German Federal Ministry of Education and Research (BMBF) (project RiKoV, Grant No.13N12304).

The research leading to these results, carried out by Marian Sorin Nistor, was funded by the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme FP7/2007-2013/ under REA Grant Agreement Number 317382.

REFERENCES

[1] F. Harary, Graph theory, Addison-Wesley, Reading, MA, 1969.

[2] C. Berge, The theory of graphs, Courier Corporation, 2001.

[3] F. Emmert-Streib, M. Dehmer, Exploring statistical and population aspects of network complexity (2012).

[4] A. Mowshowitz, Entropy and the complexity of graphs: I. An index of the relative complexity of a graph, The Bulletin of mathematical biophysics 30 (1968) 175–204.

[5] A. Mowshowitz, Entropy and the complexity of graphs: II. The information content of digraphs and infinite graphs, The Bulletin of mathematical biophysics 30 (1968) 225–240.

[6] A. Mowshowitz, Entropy and the complexity of graphs: III. Graphs with prescribed information content, The Bulletin of mathematical biophysics 30 (1968) 387–414.

[7] A. Mowshowitz, Entropy and the complexity of graphs: IV. Entropy measures and graphical structure, The Bulletin of mathematical biophysics 30 (1968) 533–546.

[8] C.E. Shannon, The mathematical theory of communication. 1963, MD Comput 14 (1997) 306–317.

[9] D. Bonchev, Information-Theoretic Indices for Characterization of Chemical Structures (1983).

[10] W. Zurek, Complexity, entropy, and the physics of information (1990).

[11] A.L. Fradkov, Cybernetical physics, Springer, 2007.

[12] S. Derrible, Metros as Biological Systems: Complexity in Small Real-life Networks, Advances in Network Complexity (2013) 259–285.

[13] M. Dehmer, Information processing in complex networks: Graph entropy and information functionals, Applied Mathematics and Computation 201 (2008) 82–94.

[14] M. Dehmer, K. Varmuza, S. Borgert, F. Emmert-Streib, On entropy-based molecular descriptors: Statistical analysis of real and synthetic chemical structures, Journal of chemical information and modeling 49 (2009) 1655–1663.

[15] H. Wiener, Structural determination of paraffin boiling points, Journal of the American Chemical Society 69 (1947) 17–20.

[16] X. Li, Y. Shi, A survey on the Randic index, MATCH Commun. Math. Comput. Chem 59 (2008) 127–156.

[17] L.A.J. Mueller, M. Schutte, K.G. Kugler, M. Dehmer, QuACN: Quantitative Analyze of Complex Networks (2014).

[18] R Development Core Team, R: A Language and Environment for Statistical Computing, Vienna, Austria, 2008, available at http://www.R-project.org.

[19] L. Mueller, M. Schutte, K. Kugler, M. Dehmer, M.L. Mueller, Package ‘QuACN’ (2012).

[20] F. Emmert-Streib, M. Dehmer, Information theoretic measures of UHG graphs with low computational complexity, Applied Mathematics and Computation 190 (2007) 1783–1794.

[21] MVV-Muenchen, Netzpläne, 2015, available at http://www.mvv-muenchen.de/de/netz-bahnhoefe/netzplaene/index.html (accessed on March 31, 2015).

[22] R. Gentleman, E. Whalen, W. Huber, S. Falcon, et al., Package ‘graph’ (2011).

[23] R.C. Gentleman, V.J. Carey, D.M. Bates, B. Bolstad, et al., Bioconductor: open software development for computational biology and bioinformatics, Genome biology 5 (2004) R80.

CYBER THREATS: INTRODUCING A RISK MANAGEMENT FRAMEWORK FOR CYBER SECURITY IN CRITICAL INFRASTRUCTURE PROTECTION

Silja Meyer-Nieberg[1] and Martin Zsifkovits[2]

[1] *silja.meyer-nieberg@unibw.de*
Fakultät für Informatik, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85577 Neubiberg (Germany)

[2] *martin.zsifkovits@unibw.de*
Fakultät für Informatik, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85577 Neubiberg (Germany)

Abstract

This paper introduces a risk management framework for the area of critical infrastructure focusing on cyber threats. Cyber security concerns have gained more and more importance in recent time. Owing to the importance several risk management frameworks have been developed. They rely however on qualitative approaches. In contrast, the process developed here also considers quantitative approaches. It is highly adaptable and allows integrating methods from other frameworks.

Keywords: risk management process, cyber security, critical infrastructure protection.

1 INTRODUCTION

A first world state depends strongly on its infrastructure. Without communication networks, transportation, energy, state, industry, and society would soon cease to function. Over the years, the installations of the so-called critical infrastructures have become more and more interconnected: Communication via networked structures plays an increasingly important role. This affects especially industrial control systems which regulate and monitor the processes of the installations. While this increases the ease of control, it introduces new vulnerabilities towards cyber threats. As the recent years have shown, cyberattacks carried out with sophisticated tools like Stuxnet or more recently Regin represent growing challenges to many parts of [18,19]. Risk management and strategic foresight for the area of cybersecurity is thus of great importance [14].

A failure of a single industrial control system may cause serious damage if the singular first effect starts to spread and to cascade. Safeguarding installations against cyber threats is therefore an important challenge. This even more so since many actors with different skill sets may be involved - ranging from advanced persistent threats to hackers who use toolboxes distributed in the Internet [19]. The means of attacks may also take various forms: Here attacks may be physical as e.g. a manipulation of hardware, may stem from worms, viruses, or Trojan horses, or may be due to human factors as in social engineering [18, 19]. This makes an assessment of vulnerabilities and risks a complicated task. A structured risk management is therefore required. Due to the importance of critical infrastructure protection, several risk management processes have been introduced so far. Many existing risk frameworks focus on qualitative approaches, however, and thus on the judgement and agreement of human experts. In this paper, we argue that quantitative methods, as for example simulation-based analysis, optimization, network and graph analysis, and multi-criteria decision analysis are invaluable tools that can support human decision making in cyber security.

The risk management process introduced in this paper aims therefore at an integration of quantitative and qualitative operations research techniques. It focuses on the central phases of risk assessment, i.e., risk identification, analysis, and evaluation. Each phase itself consists of several steps and interweaves quantitative assessments and analyses with human judgement. Furthermore, visualization techniques are used so that options can be easily explored and examined. The paper introduces the process and contrasts it with the well-known frameworks OCTAVE and CORAS. It is shown that the new process can be seen as a template which may integrate qualitative procedures from other frameworks which it then augments by quantitative tools and techniques. This enables an easy adaptation of the risk management framework.

The remainder of the paper is structured as follows. First, the risk management process is described. Afterwards, details for the main steps of the risk assessment: risk identification, risk analysis, and risk evaluation are provided.

2 AN ADAPTABLE RISK MANAGEMENT PROCEESS

This section describes our framework which is based on the ISO 31000 Norm. Risk management is the means by which the policy maker keeps risks for humans and their livelihoods as low as possible, or at least within acceptable bounds. This leads to the question of where the level of acceptance can be set. “How safe is safe enough?” These aspects make the risk management process even more complex and lead to the need of comparisons and planning from a holistic perspective [7]. There is a standardized risk management process structure available, called ISO3100 norm. This generalized process guideline is a promising framework for such a structured process. According to the definition of the ISO31000 risk management process, it is structured as shown in Figure [9].

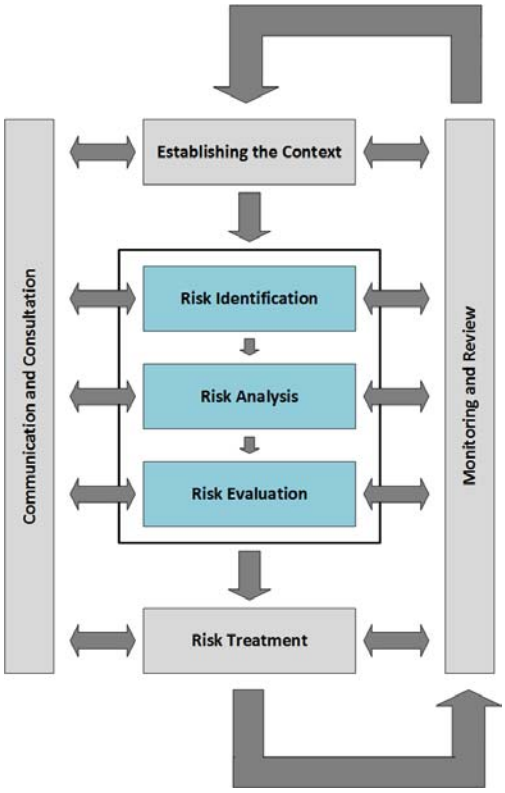


Figure 1: The ISO Risk Management Process [9]

“Establishing the Context”, “Communication and Consultation”, “Risk Treatment”, and “Monitoring and Review” are interactive tasks that need to be handled by the decision maker continuously. However, the core of the risk management process is the identification, analysis, and evaluation of risks. Therefore, we are suggesting a framework that supports the decision maker and guides through the management core process based on several existing tools that were individually developed. One has to note that the presented and recommended tools need to be selected, analysed, and evaluated for every case separately. Thus, the process needs adaption for each application that might be evaluated. However, the basic structure stays unchanged.

In general, the process is based on the primarily established context of interest and leads to concrete recommendations for responding to the risk. Thereby, in the first step also the time horizon of interest needs to be defined besides the thematic concept. The decision maker here needs to define, if the risk management support is needed on a strategic or an operational level. The risk management core process then brings together the overall context of the threat and concrete recommendations for the risk treatment on a case by case basis.

In the case of risk management in the area of cybersecurity, the process can be augmented by methods and approaches stemming from other dedicated risk management frameworks. Here, we consider CORAS [11] and OCTAVE [4]. CORAS is a framework that was developed in a European research project. It introduces a dedicated modelling language and a modelling tool which serve to record the information gained during the process. Its focus lies on qualitative methods using techniques like structured brainstorming. Furthermore, it introduces specialized diagram types to record and communicate the information gained [11].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) represents a process to assess information security risks, see e.g. [4]. It focuses on organizational risk and security practices using an asset-based approach. It has been developed at the Software Engineering Institute at the Carnegie Mellon University. The current implementation consists of four phases which are subdivided into eight steps. For each step, it provides a standardized approach, specific worksheet formats for documentation, and in some cases questionnaires.

Concerning our process, methods from the framework can support especially the early phases of the process, see [5] for more information. Here, e.g. the first steps of CORAS can be carried out in order to reach e.g. a shared understanding between decision makers and analysts. Furthermore, threat diagrams or risk profiles may be helpful in the construction of the catalogue of hazards. Interestingly, both frameworks often apply structured brain storming in workshops during their respective phases. This may be feasible if the risk management is carried out for a single installation or for a small organisation where it is easy to bring the analysts together. In general, however, the usage of collaboration systems may be more advisable.

In the following the steps of the risk management process developed are detailed using an example of a lignite power plant the SCADA control center of which is connected to the network of the enterprise and finally through a gateway with the internet.

3 RISK IDENTIFICATION: OF THREATS, ACTORS, AND MEANS

Risk identification consists of several steps. Figure 2 shows the main processes that our framework suggests. The initial phase (either with the help of quantitative or qualitative methods) which precedes the actual risk identification narrows the general context to the problem area itself. Here, we are concerned with the protection of the

power plant against cyber attacks. First of all, a clear, precise and shared understanding of the system is required. For this, the assets of the system must be identified. This phase can be carried out with methods stemming from OCTAVE or CORAS. For instance, CORAS differentiates between direct and indirect assets and conducts brainstorming and discussion meetings of decision makers and analysts [11]. Indirect assets are based on direct assets and may, for example, comprise public trust in the institution. In contrast, OCTAVE considers information assets for example the control software allowing the operation of the SCADA center, and container assets, e.g. the workstations used [4]. It must be decided on a case-by-case basis, which classification is more suited to the organisation.

Once the assets have been identified, the question arises which hazards threaten the installation. The frameworks CORAS and OCTAVE operate here mainly with qualitative approaches and rely on the knowledge of experts. These are highly relevant. To gain further information, we suggest conducting internet-based researches. Topic monitoring, for example, can be used to scan for information on new attack types and potential system vulnerabilities in the general open sources. In the context of a study founded by the Planungsamt der Bundeswehr a tool was developed that enables a high-level keyword-based internet search and provides insights into ongoing activities [21]. Additionally, specialized data bases can be taken into account: Several vendors of antivirus software or dedicated sites as the SANS Institute [17], the US Enterprise Information Security Office [22], or the German Alliance for Cybersecurity [8] may provide important information. The topic monitoring tool can be configured to focus on certain URLs and can be used for a monitoring of specialized sites.

At this point, a more detailed picture of the nature of the threats or hazards must be gained. In this paper, a threat in cyber war and cyber security is interpreted as a potential attack against a computer system or against a network. Attacks can be divided into several phases: a reconnaissance, the actual attack, and the exploit itself where the system access is used to steal data or to perform sabotage [19].

To continue the example, let us assume that recent reports indicated an increasing activity in searches for SCADA servers thus raising concerns. The analysts now require insights concerning potential actors and potential attack means. While the set of threats that is collected during risk identification is relatively large, the threats considered must be relevant to the organisation. Thus preliminary assessments are necessary. In addition, see also the next section, new vulnerabilities may be identified with the help of simulations, network-analyses, and further quantitative methods, see Fig. 2. In our fictional case, the gateway is judged to be potentially vulnerable towards denial-of-service attacks or distributed denial-of-service attacks. Since this kind of attacks do not require a high level of technical knowledge, highly sophisticated state sponsored actors as well as cyberterrorists may be involved. In addition it is revealed that the SCADA servers also use commercial off-the-shelf components that are vulnerable against a certain kind of worm recently reported to have been found in systems of other countries. Due to the necessary sophistication, only state sponsored actors could have designed the code.

Finally, the threats identified are collected in a database, the so-called catalogue of hazards. We suggest characterizing a hazard by the components: actors, target, means, phase, and threat class. Concerning the actors for example, we may distinguish between advanced persistent threats (ATPs), organized crime, hacktivists, insiders, and so-called script kiddies, see e.g. [18,19,20]. The danger they pose is highest in the case of ATPs which are often assumed to be state-sponsored actors. It is lowest for the script kiddies which may use tools found in the vast space of the internet to try to attack an installation. The means used by the actors are connected to the actor class and the attack phase. For example, the attack may be carried out by a denial of

service, a virus, a rootkit, or by a worm. At this point, the question arises how the dangers and risks posed by the threats are to be judged.

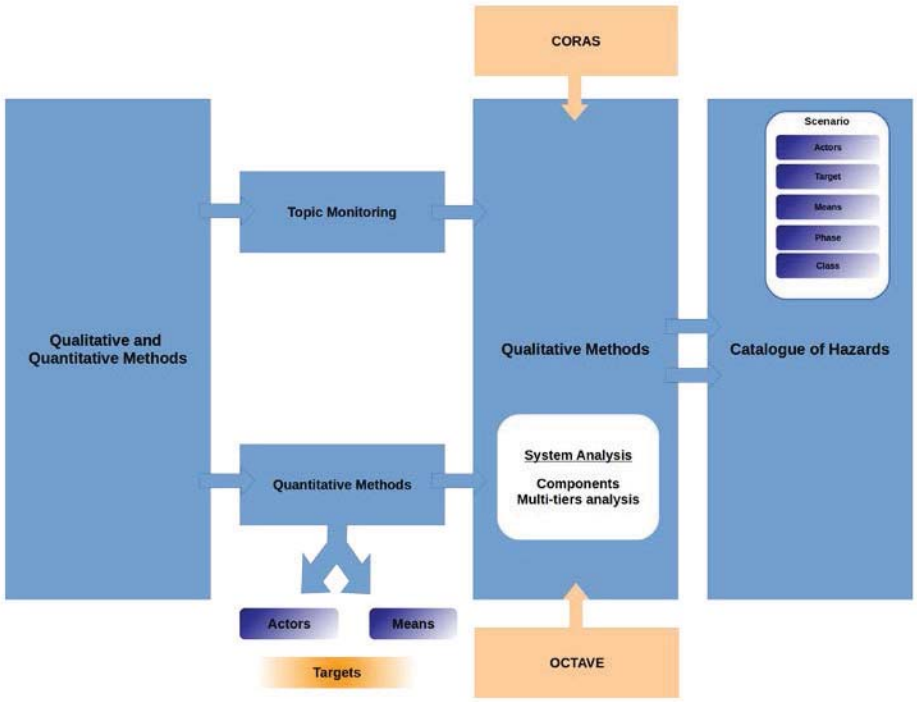


Figure 2: Risk identification for cyber security.

4 RISK ANALYSIS: IDENTIFYING RELEVANT SCENARIOS

The hazards collected must now be investigated in more detail. Concrete scenarios need to be derived and analysed. First, the group of scenarios should be thinned out. Here, a scenario rating tool may support the multi-criteria decision process. The scenario rating tool developed allows the analysts to state their estimation of likelihood and impact. The results are the visualized and classified so that the analysts and the decision makers can immediately see which scenarios may be serious. The diagrams also support arriving at a shared situational understanding. Afterwards, a collection of first-order threats or scenarios has been derived that require further attention.

In the next step, the interdependency and cumulative effects must be taken into account. To this end, we recommend a network-based approach since it appears well suited to the context of cyber security. Attack graphs [13] may play an important role. Attack graphs model the connections between different vulnerabilities and visualize potential attack paths. In addition, they can be used to design countermeasures since they also show the effects of blocking certain pathways. Often, they are built in a red teaming phase with one team assuming the role of the attacker. They also represent the transition towards the next phase of the risk assessment process, the risk evaluation.

It should be noted that automated red teaming or simulation based optimization may be applicable, see e.g. [15]. Since the computer systems and other installations are physical-technical systems, a simulation model can be built relatively easily. Several environments have already been developed [12]. After defining impact measures, the automated approaches search for combinations causing the largest damage and may thus provide new insights concerning the vulnerabilities of the system. When such vulnerabilities are detected, it is recommended to return to the risk identification phase

in order to judge whether the new hazard should be entered into the catalogue of hazards.

5 RISK EVALUATION: IMPACTS AND LIKELIHOODS

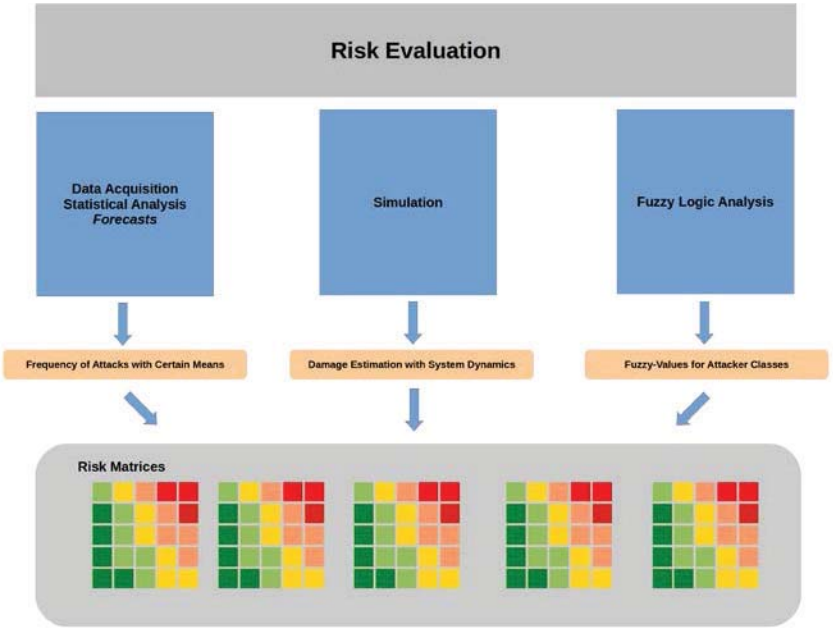


Figure 3: Risk evaluation.

During risk evaluation, our framework recommends the use of several techniques depending on the data that is available and to follow a combined approach if possible. Risk evaluation necessitates determining the impact and the likelihood of the scenarios. Therefore, two processes appear which can be conducted in parallel or sequentially. Both consider a qualitative phase where the analysts use a collaboration system or a shared meeting in order to obtain the final results.

Concerning the impacts, network analysis via attack graphs or other models may be used. Of special interest are system dynamics models or in general dynamical systems which can depict the interactions of the important components and their development over time with the help of computer-based simulations. Analysing the impacts on the direct assets may not require a full system dynamics simulation. However, these models can be built easily and can be used to ascertain how the indirect qualities are affected. A system dynamics model may e.g. show how the direct assets are connected to the primary purpose of the power plant of providing energy. With the help of a simulation model, quantitative data is collected concerning the detailed effects of certain hazards. Afterwards, a qualitative phase follows since human experts are required to judge the results and assess effects on finances and reputation. The impacts are then classified using a five-point scale. Having arrived at a matrix or table containing complete scenarios with the impact class, the question arises how which of the scenarios are likely to occur.

Since a scenario consists of several components (attacker, means, …), their likelihoods need to be determined and combined to derive the general estimate. It will be difficult to derive a probability model for the likelihood of certain attacker groups targeting the respective system. Thus, only fuzzy information grouped e.g. into very likely, likely, moderate, highly unlikely, is obtainable. Concerning the likelihood of a certain attack type or means, statistical data can be obtained is certain cases by falling

back on honeypots or honeynets [19, p. 144]. They mimic vulnerable systems attackers might be interested in.

In a short time experiment with a simulation of a SCADA system at the Universität der Bundeswehr München, three kinds of attacks were observed: denial of service (DoS), distributed denial of service (DDoS), and port scanning [6]. The last is used to gain more information and typically precedes the actual attack. In addition, an enterprise may have been monitoring port scans and have intrusion detection capabilities. This information may prove very valuable to access the frequency of certain attack types. This continuous data has then to be transformed into qualitative data and combined with the fuzzy information obtained beforehand. Again tables or matrices are obtained as the result.

Combining the different likelihoods for the threats and the impact classes leads to the risk evaluation matrices that our framework envisions as the final result of the risk assessment, see Figure 3 and also [23].

6 CONCLUSIONS

Cyber security and the protection of critical infrastructures represent important challenges today. Safeguarding the assets of an organisation requires detailed and repeated analyses of the structure and potential threats. To this end, a risk management process is developed based on the ISO 31000 norm. The focus of the risk management process lies on the central risk assessment, divided into the processes of risk identification, risk analysis, and risk evaluation. The process recommends the combination of qualitative and quantitative methods. This is in contrast to other frameworks in the area of cyber security which rely mainly on qualitative methods and on the judgement of human experts. While human judgement is absolutely essential and standardized methods of communication are required, quantitative methods as considered by our framework may provide new insights regarding potential threats and their impacts.

7 ACKNOWLEDGEMENTS

The support by the Planungsamt der Bundeswehr is gratefully acknowledged.

REFERENCES

[1] Bundesamt für Sicherheit in der Informationstechnik (2013). ICS-Security-Kompendium. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security kompendium pdf.pdf? blob=publicationFile, last accessed on 11/14/2014.

[2] Bundesministerium des Innern (2009). Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). URL: http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf, last accessed on 11/20/2014.

[3] Bundesministerium des Innern (2011). Cyber-Sicherheitsstrategie für Deutschland. Tech. rep., URL: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie node.html, last accessed on 10/15/2014.

[4] Caralli, R.A.; Stevens, J.F.; Young, L.R.; Wilson, W.R. (2007). Introducing OCTAVE allegro: Improving the information security risk assessment process. Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon

University, URL http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419, last accessed on 11/13/2014.

[5] Dehmer, M.; Meyer-Nieberg, S.; Mihelcic, G.; Pickl, S.; Zsifkovits, M. (2015). Collaborative Risk Management for National Security Concerns. Submitted.

[6] Douramanis, M. (2014). Risk assessment for cyber threats to networked critical infrastructure. Master's thesis, Universiteit Leiden/Universität der Bundeswehr München.

[7] Federal Office for Civil Protection (2014). Integrated Risk Management, Bern, Switzerland.

[8] German Alliance for Cybersecurity. URL: https://www.allianz-fuer-cybersicherheit.de (last accessed on 03.10.2014).#

[9] ISO31000 (2009). Risk Management – Guidelines for principles and implementation of risk management.

[10] Kushner, D. (2013). The real story of Stuxnet. IEEE Spectrum 50(3):48–53.

[11] Lund, M.S. et al. (2011). Model-Driven Risk Analysis, Springer.

[12] Liljenstam, M.; Liu, J.; Nicol, D.M.; Yuan, Y.; Yan, G.; Grier, C. (2006). Rinse: The real-time immersive network simulation environment for network security exercises (extended version). Simulation 82(1):43–59.

[13] Noel, S.; Jajodia, S; Wang, L.; Singhal, A. (2010). Measuring security risk of networks using attack graphs. International Journal of Next-Generation Computing 1(1):135–147.

[14] NYS Office of Cyber Security (2012). Cybersecurity: Risk management. URL http://www.dhses.ny.gov/ocs/local-government/documents/Risk-Management-Guide-2012.pdf, last accessed on 08/10/2014

[15] Pickl, S.; Meyer-Nieberg, S.; Wellbrink, J. (2012). Reducing complexity with evolutionary data farming. SCS Magazine (2), pp. 47-53.

[16] Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report 15(3):112–133.

[17] The SANS Institute. URL: http://www.sans.org/ (last accessed 04.10.2014).

[18] Schöhnbohm, A. (2011). Deutschlands Sicherheit: Cybercrime und Cyberwar. Monsenstein und Vannerdat.

[19] Shakarian, P.; Shakarian, J.; Ruef, A. (2013). Introduction to Cyber-Warfare. A Multidisciplinary Approach. Syngress. Elsevier.

[20] Singer, P.; Friedman, J. (2014). Cybersecurity and Cyberwar. Oxford University Press.

[21] Stutzki, J. (2014). Multilingual trend detection in the web,. In: Proceedings of the 4th Student Conference on Operational Research SCOR 2014, OASICS, vol 37, pp 16–24.

[22] US Enterprise Information Security Office. http://www.dhses.ny.gov/ocs/ (last accessed on 03.10.2014).

[23] Zsifkovits, M.; Pickl, S.; Meyer-Nieberg, S. (2014). Operations research for risk management in strategic foresight. Planet@Risk. Submitted.

DECISION-MAKING CRITERIA FOR CYBER SECURITY ADOPTION: INTERNET OF THINGS CYBERSECURITY ISSUES

Alexandra Lukavchenko[1], Alexander Wiesmaier[2], Hariharan Rajasekaran[2], Panayotis Kikiras[2]

[1] *lukavchenkoalexandra@gmail.com*
Graduate School of Management, St Petersburg State University, Volkhovsky per., 3, 199004 St Petersburg (Russia)

[2] *[awiesmaier | hrajasekaran | pkikiras]@agtinternational.com*
AGT International, Hilpertstraße 35, 64295 Darmstadt (Germany)

Abstract

We address the problem of decision-makers' lack of guidance in issues related to cybersecurity investment. We identify and prioritize factors that influence such decision, and introduce a high-level sequence of decision-making actions aiming to guide an executive in order to understand risks and make an informed cybersecurity investment decision. The study serves as a basis for the future comprehensive framework development, and would be particularly useful to the Internet of Things (IoT) industry executives, since due to its specific nature IoT is very much exposed to cyber-threats and due to the fact that IoT operations adoption is rapidly growing in areas in which security was not a consideration before.

Keywords: economics, cybersecurity, Internet of Things (IoT), information technology (IT), uncertainty, framework

1 INTRODUCTION

The number of cyber-attacks surged by 48% in 2014 [1] and will continue to do so [2]. McKinsey & Co. estimates the potential loss due to the delay in adopting security measures in domains such as cloud computing to be as much as US$1.4 trillion by 2020 [3]. In the Internet of Things (IoT) era, it is projected that by 2020 about 40.9 billion devices [4] are going to be activated and connected, thereby exposing organizations to growing cyber threats and increase the risks of critical infrastructure damage.

The analysis done by the research community revealed the lack of awareness among practitioners regarding cyber security: they do not have common understanding of its notion as well as awareness of how security (and unavailability of it) can affect all of their job functions and roles; neither do they have sufficient experience in dissecting the situation to identify necessary security relationships. [5]

Decision makers in an organization must be able to fully understand, evaluate and assess the risks and costs associated with data breaches and operational disruptions due to cyber-attacks. In turn, this should allow them to allocate appropriate resources to prevent such incidents and to be better prepared to deal with aftermaths of any cybersecurity breach. Cybersecurity becomes especially critical in IoT deployments. Given the enormous amount of data generated and collected, secure operations are extremely important.

The purpose of our paper is to enable company management to evaluate cybersecurity issues, when they are making investment decisions about IoT set up within their organization. First, we provide a holistic overview of decision-making criteria, including financial and wider economic points of analysis – such as insurance and impact of network externalities on a firm's protection level. Second, we prioritize them upon the

professional opinion of cyber security experts. These prioritized factors would serve as an initial study for the future decision-making framework development.

The rest of the paper is organized as follows. Section 2 presents our research approach, demonstrating how fuzzy Analytical Hierarchy Process (AHP) is used to incorporate uncertainty intrinsic to IT personnel's opinions regarding cybersecurity. Section 3 provides relevant economic challenges and incentives for cyber security adoption offered by the literature, as well as an overview of major existing frameworks on cyber security decision-making. Sections 4 and 5 then move to describe and discuss the results of the questionnaire responses' analysis, providing managerial implications on the subject. We conclude in section 6 and outline research limitations in section 7.

2 APPROACH

In order to achieve our goal – identify and prioritize cyber security investment consideration factors, – we first made an academic survey of economic challenges and incentives relevant for cyber security system adoption, and then summarized existing frameworks for cyber security decision-making. Based on the academic research, we derived factors that academia consider important for cyber security adoption decision-making. Then, we tested these factors with a questionnaire presented to experts with multiannual experience in cyber security area and exposure to the IoT industry. The pool of 13 experts, who responded to the survey, represents C-level security executives, heads of units and cyber security team leaders in large private and public organizations, including governments.

In order to incorporate uncertainties intrinsic to the decision-making process, the results of the survey are analyzed via fuzzy analytical hierarchy process (AHP) model.

The questionnaire consists of a set of pairwise comparisons aimed at identifying trade-offs between different factors while assessing a decision about cybersecurity adoption. We present respondents with a choice between two factors each time and evaluate the relative importance of each on the scale of 1-10 (1 being "equally important", 10 being "extremely more important"). We then input them in the pairwise comparison table model; calculate triangular fuzzy weights (incorporating respondent's uncertainty) through logarithmic least squares method; aggregate the matrices of comparisons of all respondents; and present final weights of factors based on fuzzy numbers.

As a result, the objectives and decision-making factors are prioritized based on the leveraged opinion of professionals in the field, and managerial implications are discussed.

3 LITERATURE SURVEY RESULTS

3.1 Identification of economic challenges and incentives which impact cybersecurity

We surveyed the economic models to find challenges and incentives, which affect the cybersecurity value added to the organization. A factor can often be both an incentive and challenge, depending on how it is treated in the organization. Later, we test these factors for cybersecurity decision-makers awareness and rank in order of importance from IT personnel's point of view.

The seven factors that influence the level of cybersecurity in a company and identified by our literature survey are grouped as follows:

1. Vulnerability of critical assets (CA), where CA are "systems and assets, whether physical or virtual, so vital that their incapacitation or destruction may have a debilitating impact on the security, economy, public health or environment of a [nation

and/or organization]". Vulnerabilities are defined as the internal risks faced by a company.[6, 7]
2. Benefit (cost of cyber damage avoided by adopting cybersecurity system) [8, 9]
3. Investment required for cybersecurity solution adoption [8, 9]
4. Nature of cyber-attacks as they become more sophisticated, "360-degree challenge" [10, 11, 12-14]
5. Stakeholders involved in decision-making, degree of alignment of their incentives and interconnectedness [15, 16].
6. Insurance provided by cybersecurity vendor in order to cover losses from cyber-attacks and data breaches by assigning premium based on a firm's information technology (IT) infrastructure and managerial processes [16, 17]
7. Microeconomic consequences: network externalities (both positive, which reduce the level of cybercrime, and negative, which may discourage from investment and result in customer lock-in, free riding etc.), asymmetry of information (poorly informed consumers and businesses may by mistake invest in mountebank solutions); discriminatory pricing (resulting from the lack of information available about cybersecurity market). [13, 14, 16]

Our next step is to survey existing frameworks to see which factors are accounted for in the state-of-the-art decision-making frameworks.

3.2 Cybersecurity decision-making frameworks overview

As decision-making process of cybersecurity adoption becomes both increasingly important and challenging, several frameworks were developed by academia and consulting companies. In framework development, it is important to remember that cybersecurity is very much a managerial issue, which directly influences economics of an organization, and tackle the problem holistically, from three angles: critical infrastructure, technology and organization [29]. Cyber risk and economic analyses must be adaptive in their approach and use the best combinations of methods and available information in this challenging and dynamic problem space.

The majority of existing frameworks either focus on purely financial factors, or provide the to-do list of how to execute the cybersecurity solution once the adoption decision is made. We review the state-of-the-art and investigate which factors they account for.

The key steps accounted for in the cybersecurity decision tree are:

1. Assets identification and prioritization by value and risk of compromise [17, 19]
2. Estimation of the costs being avoided by cybersecurity solution adoption [17, 18]
3. Estimation of costs required to implement control mechanisms [17]
4. Evaluation of the nature of the attack [20]
5. Evaluation of vendors' responsibility, which represents concern about organization stakeholders [21]

McKinsey & Co. [22] underlines the importance of the cybersecurity model to be business-driven and flexible. The research points out that "corporations are reorienting security architectures from devices and locations to roles and data".

We see that such important economic factors previously identified in the state-of-the-art, such as insurance and influence of network externalities, are not included in present frameworks. This gap requires us to include the abovementioned factors, which affect cybersecurity value added to the organization, in our questionnaire, and test it with decision-makers.

4 MANAGEMENT QUESTIONNAIRE RESULTS

We ranked factors that impact cybersecurity of the organization based on cybersecurity professionals' opinion, taking into account trade-offs the latter make when deciding.

Table 1 shows the aggregated fuzzy weights (accounting for respondents' uncertainty) for each factor, 1 being the most important, 7 – the least important:

Table 1 Aggregated fuzzy AHP results for all respondents

Rank	*Factors*	*Final Fuzzy weights*
1	Expected benefit (cost of avoided damage)	28.61%
2	Nature of the Attack	21.29%
3	Stakeholders involved	20.61%
4	Critical assets vulnerability	16.02%
5	Investment required	10.34%
6	Microeconomic consequences	2.23%
7	Insurance provided by vendor	0.90%

The factors thus represent the decision-making criteria, which an executive may consider in order to make a well-rounded decision. Table 2 presents the high-level sequence of actions an executive should take in order to discover intrinsic risks and understand whether to invest or not.

Table 2 Actions to take making a decision regarding cybersecurity adoption

Step #	*Action to be taken*
1	Evaluate the cost of avoided damage **Why**: understand if cybersecurity is necessary; if the cost of avoided damage is large enough, as defined by a firm, proceed to step 2. Recommended for all companies that possess IT infrastructure and Internet connectivity.
2	Define the nature of the attack **Why**: understand which type of cybersecurity solution is appropriate for the specific attack
3	Consider stakeholders involved: who would benefit more or less **Why**: identify hidden long-term costs & risks, company's politics to be aware of
4	Evaluate degree of critical assets vulnerability: to what extent a company's survival depends on cybersecurity solution **Why**: prioritize investments appropriately
5	Calculate the investment required **Why**: to budget and plan long-term
6.1	1. Assess nature of players on the cybersecurity solutions market 2. Assess the cybersecurity solution vendor's characteristics **Option 6.1.1: a dominant vendor with customer lock-in suspected** Non-prioritised list of optional steps to choose from: 1) Negotiate a customized solution providing the required cybersecurity protection level;

	2) Choose another, non-dominant player with same or higher solution quality offer; 3) Go with dominant vendor standard solution, but be aware of possible negative consequences, such as the lock-in and possible overpayment for the solution's procurement and service; 4) Do not invest at all, if you think you can free ride on other market players' investment, but be aware that the lack of cybersecurity puts your company at risk. **Why**: to mitigate risk: avoid lock-in, prevent free-riding, reduce cybercrime level **Option 6.1.2: customer lock-in not identified** 1) Invest in cybersecurity solution **Why**: this will reduce the level of cybercrime towards your firm and others
6.2	1. Be aware of the macroeconomic characteristics of the cybersecurity market 2. Gather as much information as possible before investing in the cybersecurity solution 3. Openly discuss the cybersecurity solutions with other firms **Why**: to be aware of the market risks and mitigate them: reduce information asymmetry and prevent discriminatory pricing
7	1. Consider improving IT infrastructure 2. Choose vendor with acceptable insurance premiums 3. But not over-rely on insurance, as may put the company at risk **Why**: to mitigate risk – potentially beneficial to a firm if infrastructure is good

From the factors' trade-off point of view, the ranking means that expected benefit (avoided costs) from cybersecurity will be the primary point of evaluation of the adoption decision, followed by stakeholders that would be affected, for example. Similarly, the nature of the attack to be prevented or resisted needs to be considered before the degree of critical assets vulnerability. Microeconomic consequences and insurance presence stay at the 6th and 7th places, as considered the factors of the lowest importance, or present in the decision-making process in the very end of the decision tree.

5 DISCUSSION

There are two major tendencies revealed by the study. First tendency is to consider non-monetary aspects, such as the nature of the attack, stakeholders and assets vulnerability, prior to the volume of investment required. This means that cybersecurity-savvy organizations turn to more long-term thinking regarding cybersecurity investments, as the above-mentioned factors rank higher than short-term financial considerations. This is relevant for the companies implementing IoT as well. Potentially, the investment required is deemed less important if a significant stakeholder is in danger. Similarly, the investment would be justified if a critical asset were under threat.

Second tendency is that economic factors such as purchase of cyber insurance and impact of microeconomic effects are considered to be the least important, or not present in the decision-making tree at all. The reasons for the low ranking of the latter factors may lie in the behavioral biases, and explain the hesitance to invest in cybersecurity.

First, the market players' tend to believe that their decision cannot change the status quo regarding asymmetry of information, or network externalities. This is derived from the

notion of a network externality: people think others will not invest, and get discouraged from investment themselves.

Second, it can be explained by the prospect theory's risk framing concept [23]. The hesitation to invest in cybersecurity represents the loss aversion in the so-called "mortality frame" – admittance of possible loss in case of investment due to low probability of cyber-attack. In this frame, more people tend to become risk-seekers and, thus, not invest in the cybersecurity solution. As losses (giving up the good) are felt much more strongly than gains (receiving the good) [23], these irrational biases are very powerful.

The main recommendation for cybersecurity executives is thus to include insurance and microeconomic issues in the decision-making process. There are 3 reasons for this. First, insurance would can become a positive incentive for cybersecurity solution adoption, and advantageous for the company overall. Second, a decision-maker should be aware of possible network externalities, which can have both positive and negative impact on cybersecurity of the organization: understanding of the externalities' implications can improve the level of protection or reduce the negative impact. Third, asymmetry of information and price discrimination challenges need to be accounted for to understand risks intrinsic to cybersecurity solution adoption. All in all, the consideration of the above points would increase IT professionals' market risks awareness and effectively contribute to the success of the cybersecurity investment, namely, providing an organization with a more secure cyber protection.

6 CONCLUSION AND SUGGESTIONS FOR FURTHER RESEARCH

In our paper we provide the holistic overview of decision-making criteria, including financial and wider economic points of analysis, and prioritize them upon the professional opinion of cybersecurity experts using the fuzzy AHP model. Our study introduces a high-level sequence of steps, which an executive may consider to follow in order to make a well-rounded decision about cybersecurity adoption, and serves as a basis for a comprehensive decision-making framework development in the future.

Based on our research results, we recommend decision-makers in the cybersecurity space to follow the steps described above, and, in particular, account for insurance and the microeconomic issues. This would help identify risks and take a more informed cybersecurity investment decision. Among the strengths of this approach are the flexibility, helicopter view and generic nature of the decision-making criteria. The study would be applicable to all industries where IT infrastructure is used, and especially the IoT industry – which is particularly vulnerable to cyber-attacks, and high costs can be incurred in case of damage resulting from such attacks.

Further research would be beneficial in order to, firstly, estimate risk probabilities and mitigation potential of a cybersecurity solution when it is adopted, and incorporate this information into the economic decision-making process. Secondly, estimate an optimal level of cyber insurance to be included in the cybersecurity solution package. Thirdly, develop an approach to challenge asymmetry of information, which negatively influences cybersecurity adoption. Fourthly, identify which network externalities to be aware of dealing with various types of stakeholders and prioritizing their interests.

7 LIMITATIONS

The following limitations to the research apply. First, the questionnaire does not provide for an overview of which factors are not used by cybersecurity professionals at all, rather the ranking of their relative importance in the cybersecurity executive mind set.

Second, low ranking of insurance and microeconomic factors may as well signal the marginal impact they have in general on the cybersecurity adoption decision compared to other factors from executives' point of view.

REFERENCES

[1] White, S. (2014). Global cyber-attacks up 48% in 2014. CGMA magazine, 08 Oct 2014.

[2] Lever, R. (2014). Cyberattacks Are Just Going To Get Worse From Here. Business Insider, 9 Dec 2014.

[3] Bailey, T. (2014). The rising strategic risks of cyberattacks. McKinsey Quaterly, May 2014.

[4] ABI. (2014). The Internet of Things will drive wireless connected devices to 40.9 Billion by 2020. ABI Internet of Everything Market Research, 20 Aug 2014.

[5] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cybersecurityrisk. Computers & Security 31, pp. 597-611.

[6] Clarke, R., & Knake, R. (2010). Cyber war: The next threat to national security and what to do about it. Toronto: Harper Collins Canada.

[7] Hiller, J., & Russell, R. (2013). The challenge and imperative of private sector cybersecurity:: An international comparison. Computer law & security review 29, pp. 236-245.

[8] Bauer, J. M., & van Eeten, M. (2009). Cybersecurity: stakeholder incentives, externalities and policy options. Telecommunications Policy, 33, pp. 706-719.

[9] Shackelfold, S. (2012). Should your firm invest in cyber risk insurance? Business Horizons 55, pp. 349-356.

[10] Henrie, M. (2013). CybersecurityRisk Management in the SCADA Critical Infrastructure Environment. Engineering Management Journal. Vol. 25 No. 2. Retrieved November 14, 2014,

[11] Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: economic & institutional considerations. Electron Commer Res, 13:41–69.

[12] Hendershot, S. (2014). Security Guards. PM Network, Sep 2014, Vol. 28, №9. Retrieved November 26, 2014 , from

[13] Anderson, R., & Moore, T. (2006). The Economics of Information Security: a survey and open questions. University of Cambridge , Computer Laboratory, Cambridge .

[14] Swartz, J. (2003). Firms' hacking-related insurance costs soar. USA Today. Retrieved from

[15] Kunreuther, H., & Heal, G. (2003). Interdependent security. Journal of Risk and Uncertainty 26 (2-3), pp. 231–249.

[16] Akerlof, G. (1978). Market for "lemons": quality uncertainty and the market mechanism. Uncertainty in Economics, pp. 237-251.

[17] Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review, Fall 2002, Vol. 45, # 1.

[18] McKinsey & Company. (2014). Risk and responsibility in a hyperconnected world: Implications for enterprises. McKinsey Quarterly, Jan 2014.

[19] Spina, S. M., & Skees, J. D. (2013). Electric Utilities and the Cybersecurity Executive Order: Anticipating the Next Year. The Electricity Journal, Volume 26, Issue 3, pp. 61-71.

[20] Greenwald, J. (2013). Cybersecurity framework welcomed. Business Insurance, 11/4/2013, Volume 47, # 22.

[21] Saqib, A., Anwar, R. W., & Hussain, O. K. (2015). Cybersecurity for cyber physical systems: a trust-based approach. Journal of Theoretical and Applied Information Technology, Vol. 72, #2.

[22] McKinsey & Company. (2011). Meeting the cybersecurity challenge. McKinsey Quarterly, June 2011.

[23] Ackert, L., Deaves, R. (2010). Behavioural finance: psychology, decision-making, and markets. USA: South-Western Cengage Learning.

ParasiteEx: Disinfecting Parasitic Malware Platform-Independently

Thomas Barabosch, Adrian Dombeck and Elmar Gerhards-Padilla

{firstname.lastname}@fkie.fraunhofer.de
Fraunhofer FKIE, Friedrich-Ebert-Allee 144, 53113 Bonn (Germany)

Abstract

Throughout the last years many malware families have emerged that inject their malicious payload in legitimate processes and operate without the need of their own process space. This parasitic behaviour allows malware, for example, to operate covertly or to intercept critical information. While there have been several scientific approaches for detecting and preventing this behaviour, the systematic disinfection of this kind of parasitic malware has been shunned so far.

In this paper, we present a novel approach for disinfecting parasitic malware platform-independently. Our approach – called ParasiteEx – detects such parasitic malware signature-based and cleans up the infected process spaces. ParasiteEx relies on concepts found in all current multitasking operating systems such as threads and memory pages. Based on these concepts, our approach disinfects process spaces. This fact ensures that ParasiteEx is easily portable.

In experiments with benign and malicious programs, we show that ParasiteEx has high success rates with no false positives. ParasiteEx is able to clean infected processes on Windows as well as Linux. To the best of our knowledge, we are the first to present a platform-independent approach for disinfecting parasitic malware.

Keywords: Computer Security; Malware; Dynamic Analysis; Local Disinfection; Host-Based Code Injection Attacks

1 INTRODUCTION

Cyber criminals employ malicious software (malware) for a wide range of operations, e.g. spamming, fraud or sabotage. The antivirus industry and cyber criminals are competing in an ongoing arms race. Malware uses several techniques for evading antivirus products. One especially popular technique is the Host-Based Code Injection Attack (HBCIA). A wide range of malware types such as banking Trojans like ZeusP2P, cyber weapons like Stuxnet or Ransomware like Cryptolocker use HBCIAs. HBCIAs allow malware to intercept critical information, operate secretly or escalate privileges [5]. The basic principle of a HBCIA is copying code from an attacker process into a victim process. Subsequently, the code is executed within the context of the victim process. The attacker and the victim process run on the same system during a HBCIA.

Several publications have focused on the detection and prevention of HBCIAs (e.g. [5], [6], [7]). However, the disinfection has been shunned so far. Several problems like system instability can arise during a disinfection of a process space. Reinstalling the system is therefore considered the safest way. However, this is not always possible. An example would be a control system that cannot be shutdown immediately [10]. In such a case it would be very valuable to disinfect the system during its runtime.

In this paper, we present ParasiteEx. ParasiteEx is a platform-independent approach for process disinfection. It relies only on concepts found in every multitasking operating system. These concepts include processes, threads and memory regions. Thus, our approach is easily portable to different platforms. ParasiteEx scans all running

processes for memory regions belonging to HBCIA-employing malware. The scanning engine uses a signature-based approach. In case ParasiteEx has detected an infected memory region in a process space, it halts the execution of the process temporarily. Then ParasiteEx determines the corresponding malicious threads and terminates them. ParasiteEx proceeds to free the infected region and it also cleans all hooks pointing to this infected region. Finally, ParasiteEx resumes the cleaned process.

We implemented a prototype of ParasiteEx for Windows XP and Ubuntu 13.10. In our evaluation, we tested this prototype with fifteen current malware families and hundreds of benign programs. The evaluation shows the feasibility of our approach. Our approach disinfected twelve of fifteen malware families successfully. No false positives were observed.

2 HOST-BASED CODE INJECTION ATTACKS

Host-Based Code Injection Attacks (HBCIA) are a popular technique employed by current malware. The motivations for using this technique are manifold. They include covert operation, interception of critical information or privilege escalation [11].

The copying of code from an attacker entity into a victim entity and subsequently the execution of this code is termed Code Injection. If this happens without the intention of the original author of the program then we call this a Code Injection Attack. While the victim entity is typically a process space, the attacker entity can be a process space or a kernel module [11].

There exist two variants of a Code Injection (Attack). Firstly, the attacker and the victim reside on different systems. This is called a Remote Code Injection (Attack). Remote Code Injection Attacks were very popular with network worms in the early 2000s [11]. Secondly, the attacker and the victim reside on the same system. This is called a Host-Based Code Injection (Attack). HBCIAs have become very popular throughout the last years. In particular this is related to the rise of banking Trojans. In this paper, we will only cover the second variant of Code Injection Attacks.

Figure 1 A malware dropper injects code into an office program sketches a HBCIA. In this figure a malware dropper injects code into an office program. We assume that the attacker and the victim are both user space processes. This figure is split into two parts. The first part sketches the moment of the injection. The right side depicts an attacker process (a malware dropper). The left side depicts a victim process (an office program). The attacker process runs a malware dropper as its main program. One thread is running in this process space (symbolized by the arrow). The dropper holds a pointer to a payload that is going to be injected into the victim. The victim process runs an office program with one thread. In addition, it has loaded several system libraries like kernel32.

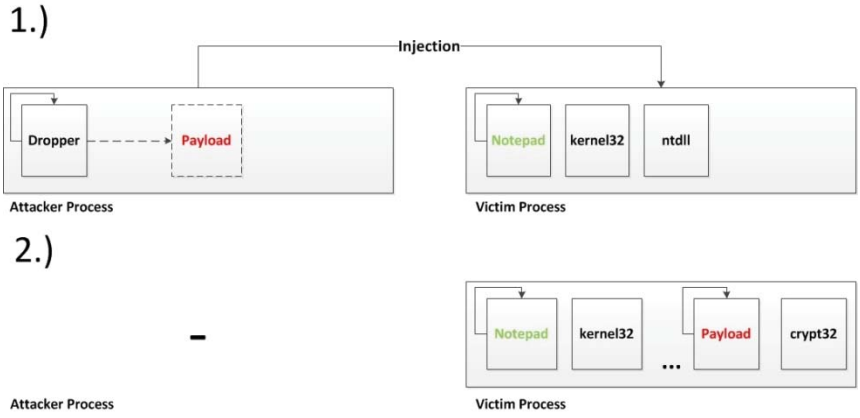


Figure 1 A malware dropper injects code into an office program

In the second part of this figure the HBCIA has already been carried out. The attacker process does not exist anymore. The payload is now running within the context of the victim process. It has got its own thread running concurrently to the victim process' original program. Additionally, it has loaded new system libraries like crypt32 for carrying out its malicious operation. The payload blends into the behavior of the benign victim process. HBCIAs break therefore with the common belief that only one program is responsible for the behavior of a process space.

3 PARASITEEX

ParasiteEx is an approach for disinfecting processes from parasitic malware that employs HBCIAs.

3.1 Methodology

In this section, we will discuss the methodology of ParasiteEx. **Figure 2 Disinfection algorithm of ParasiteEx** sketches the disinfection algorithm of our approach. ParasiteEx enumerates all running processes. It accesses each process and applies its disinfection algorithm to it.

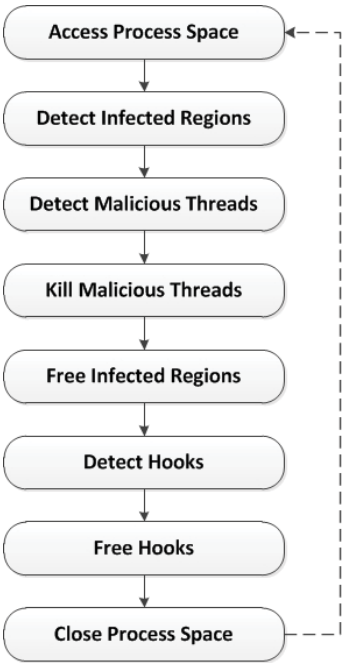


Figure 2 Disinfection algorithm of ParasiteEx

At first ParasiteEx detects infected regions. We define an infected region as a series of memory pages. ParasiteEx scans all pages of a process space for a set of predefined string signatures. Once a signature matches a memory page, this memory page and all its preceding and proceeding memory pages are considered as infected region. Given the set of infected regions for a process space, ParasiteEx determines all malicious threads. If the start address of a thread originates in an infected region, then this is termed malicious thread. These malicious threads are suspended and killed afterwards. Subsequently, ParasiteEx frees the corresponding infected regions.

Once it has freed the infected regions, ParasiteEx detects hooks within the process space. ParasiteEx does this by scanning system libraries of the process space for jumps to infected regions. In case ParasiteEx detects a hook in a system library, it replaces this system library with a clean copy. Finally, the process space is closed properly.

The following sections discuss the detection of the infection, the removal of malicious artifacts and the removal of hooks in detail.

3.1.1 Infection Detection

In this section, we describe how ParasiteEx detects infected regions and their corresponding malicious threads. There are two crucial parts needed for a HBCIA [5]: executable code and an execution context. They correspond to infected regions and malicious threads in our case.

We assume that a set of good signatures already does exist. So far signatures have to be created manually. Future work focuses on the integration of automatic signature generation. Previous work does already exist (e.g. [4]).

ParasiteEx scans all memory pages of a process space and applies its set of signatures to them. In case a signature matches a string in a memory page, the whole region surrounding this memory page is assumed to be infected. If a malware family splits its code over several infected regions then a signature for each of these regions is needed.

In case ParasiteEx has detected infected regions in a process space, it proceeds to determine associated malicious threads. We assume a thread as malicious, if and only if its start address originates in an infected region. ParasiteEx enumerates all threads of the process space (suspended or running). It determines for each thread its start address. Then it checks, whether this start address lays in an infected region or not. If it does so then this thread is marked as malicious.

3.1.2 Removal of Malicious Artifacts

If ParasiteEx has detected infected regions and malicious threads within a process space then it removes these malicious artifacts. Firstly, ParasiteEx suspends and kills all threads that are tagged as malicious. Then it frees the infected regions.

3.1.3 Removal of Hooks

Next ParasiteEx detects and removes hooks. To this means, ParasiteEx scans the process space for jumps that cross memory regions. These jumps form the set of hook candidates. For each hook candidate, ParasiteEx checks if it jumps into an infected region. These jumps are considered as hooks.

In case hooks have been found, ParasiteEx removes them. It achieves this by overwriting the hooked module with a clean copy of it. ParasiteEx maintains a database of system libraries. It chooses the right version of the system library and overwrites its hooked copy.

4 PROTOTYPE IMPLEMENTATION

We implemented ParasiteEx for two different operating systems: Microsoft Windows XP SP2 and Ubuntu Linux 13.10. ParasiteEx's architecture is split in two layers. The first layer is the operating system abstraction layer (OSAL). It abstracts from the underlying operating system and offers the second layer a set of functions for dealing with memory regions, threads or processes. The second layer is the logic layer. It implements the logic of ParasiteEx by using the functions offered by the OSAL.

We implemented ParasiteEx as a user space program, i.e. it runs in its own process space. Malware can therefore infect ParasiteEx as well. We chose to implement the prototype as a user space program because it allowed us a faster prototyping. Though, we recommend a productive implementation that does not reside in user space. Please note that this shortcoming does not apply to the underlying approach in general.

On Windows the OSAL relies on functionality provided by the Win32 API such as memory management functions (e.g. VirtualProtectEx), process enumeration (e.g. CreateToolhelp32Snapshot) or process and thread functions (e.g. TerminateThread). In addition, we had to use some internal functions (e.g. NT* such as NtResumeProcess for resuming processes). On Linux the OSAL uses /proc for determining process information and accessing memory pages. It also relies on ptrace in order to manipulate processes.

5 EVALUATION

In this section, we evaluate ParasiteEx's prototype implementation on Windows and Linux.

5.1 Dataset

The data set consists of fifteen representatives of prevalent malware families such as Bebloh, Hanthie, Poison or ZeusP2P. These representatives target two different operating systems. Fourteen malware families target the Microsoft Windows NT platform and one malware family targets Linux. We only have to consider one representative of each family, since HBCIAs are a malware family feature [5]. We also added benign programs to the data set, which were taken from Windows' system directory. In total, 334 benign programs were added.

5.2 Methodology

We conduct the evaluation of ParasiteEx using virtual machines (VMs) for Microsoft Windows XP SP2 or Ubuntu Linux 13.10. The operating systems are virtualized with VirtualBox 4.3.14. Both virtual machines (VMs) are hardened against commonly known VM detections.

Before we conducted the evaluation, we crafted manually signatures for the malicious binaries. For each sample of the data set we repeat programmatically the following: at first, we start the VM. Subsequently the sample is executed. We grant each sample two minutes for initialization. After two minutes, ParasiteEx is executed. Once ParasiteEx has finished the disinfection, we check the VM for signs of infection. Additionally, we verify the functionality of the VM by creating a file with a text editor.

5.3 Results & Discussion

Table 1 Summary of the results summarizes the results of the evaluation for Windows malware. ParasiteEx cleaned successfully the system in eleven cases. None of the benign samples was falsely assumed to be malicious. This means that the signatures were created with care. However, we do not consider the disinfection successful in three cases. These three cases are Napolar, Sality and Sirefef.

ParasiteEx is not able to detect the start address of Napolar's malicious threads. Napolar's threads have a start address of zero. This is probably an anti-reverse engineering technique. ParasiteEx reports therefore only the detection and no disinfection is carried out. The underlying problem is that the prototype implementation relies on information provided by user space libraries. In the cases of Sality and Sirefef, ParasiteEx could clean all infected processes except one. We assume that this is due to the fact that both families also come with a rootkit component that might interfere from kernel mode.

We also conducted a disinfection of a Linux malware. This malware – called Hanthie – was the first banking Trojan for Linux first detected in 2013. Hanthie targeted mainly Ubuntu 13.10. We therefore used this version in our experiment. At first Hanthie was started in the VM. After two minutes, ParasiteEx was executed. ParasiteEx detected

the infection and disinfected successfully all infected processes. The VM stayed stable and functional afterwards.

Malware family	Processes Checked	Processes w/o infection	Processes successfully cleaned	Processes not able to clean	Memory regions cleaned	Malicious threads killed	Malicious processes killed	Hooks removed
Bebloh	22	21	1	0	3	1	0	1
Conficker	22	20	2	0	3	6	0	11
Dorkbot	24	23	1	0	0	1	1	0
EyeStye	23	4	19	0	27	63	0	396
Napolar	23	22	1	0	1	0	0	0
Poison	20	19	1	0	1	0	0	0
Redyms	22	0	22	0	23	21	0	33
Sality	23	14	8	1	17	41	0	1
Sazoora	22	21	1	0	1	0	0	0
Sirefef	22	19	2	1	2	2	0	2
Trxa	23	14	9	0	18	12	0	30
Vawtrak	23	21	2	0	1	1	1	0
Zbot	23	14	9	0	9	9	0	140
ZeusP2P	23	13	10	0	9	9	1	277

Table 1 Summary of the results for Windows malware

The results of the evaluation show that disinfection of HBCIA-employing malware is possible. ParasiteEx succeeds in disinfecting process spaces infected by HBCIA-employing malware on Windows and Linux. However, there are still problems that have to be solved. A major problem is system instability due to poor hook removal. If the malware is intertwined with the original program, then removing the malware from the process space leads to system instability. An example would be a malware that steals bytes from the original program. Only malware families that are well understood should be automatically disinfected. Furthermore, the prototype implementation relies on information provided by user space libraries. Such information can easily be faked. Future work will address these shortcomings.

6 RELATED WORK

Host-Based Code Injection Attacks are discussed in detail in [11]. There has been a lot of work on detection and prevention of Code Injections Attacks. This is especially the case for Remote Code Injection Attacks (e.g. [6], [7]). These works are based on instruction-set randomization. Each process space has its own set of instructions. Hence, injected code does not run in other process spaces. However, this demands considerable adjustments of the operating system as well as the hardware. There are also publications that cover the detection of Host-Based Code Injection Attacks (e.g. [5], [8]). While the authors of [5] present a dynamic approach for HBCIA detection by employing a process honeypot, the authors of [8] propose a static approach for

forensically detecting HBCIAs in memory dumps by hashing executable areas and comparing them to a database.

Leder et al. [9] present Conciller. Conciller terminates the Conficker worm. Their approach scans all process spaces for Conficker and terminates its threads without touching the process. While their work is closely related to ours, it lacks the full disinfection of an infected process as well as the genericity.

7 CONCLUSION & FUTURE WORK

ParasiteEx is a novel approach for disinfecting infected process spaces that are infected by HBCIA-employing parasitic malware. It relies only on concepts such as memory pages, threads or hooks that are universally in the realm of current multitasking operating systems.

We implemented a prototype of ParasiteEx for Windows and Linux. Our experiments with fifteen HBCIA-employing malware families show that our approach is feasible. The prototype disinfects processes on two different platforms successfully with very high success rates. However, there are still cases in which the disinfection was not 100% successfully.

Future work will focus on improving the hook detection, the removal engine and minimizing the risk of system instabilities. We will also move ParasiteEx out of the user space in order to improve its tamper resistance.

REFERENCES

[1] G Data Software, "Security Blog," 17 December 2013. [Online]. Available: https://blog.gdatasoftware.com/blog/article/bebloh-a-well-known-banking-trojan-with-noteworthy-innovations.html. [Accessed 25 May 2015].

[2] Bennett, J. T., N. Moran and N. Villeneuve, "Poison Ivy: Assessing Damage," 2013.

[3] Vínsula, Inc., "Analysis of CryptoLocker Racketeer spread through fake Energy Australia email bills," 10 June 2014. [Online]. Available: http://vinsula.com/2014/06/10/analysis-of-cryptolocker-racketeer/. [Accessed 25 May 2015].

[4] K. Griffin, S. Schneider, X. Hu and T. Chiueh, "Automatic Generation of String Signatures for Malware Detection," in Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2009.

[5] T. Barabosch, S. Eschweiler and E. Gehards-Padilla, "Bee Master: Detecting Host-Based Code Injection Attacks," in Detection of Intrusions and Malware, and Vulnerability Assessment, Springer International Publishing, 2014.

[6] G. S. Kc, A. D. Keromytis and V. Prevelakis, "Countering code-injection attacks with instruction-set randomization," in Proceedings of the 10th ACM conference on Computer and communications security, ACM, 2003.

[7] A. Papadogiannakis, L. Loutsis, V. Papaefstathiou and S. Ioannidis, "ASIST: architectural support for instruction set randomization," in Proceedings of the 2013

ACM SIGSAC conference on Computer & communications security, ACM, 2013.

[8] A. White, B. Schatz and E. Foo, "Integrity verification of user space code," in Digital Investigation 10, Elsevier, 2013.

[9] F. Leder and T. Werner, "Know Your Enemy: Containing Conficker - To Tame A Malware," 2009.

[10] B. Zhu, A. Joseph and S. Sastry, “A Taxonomy of Cyber Attacks on SCADA Systems“, IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011

[11] T.Barabosch and E. Gerhards-Padilla, “Host-Based Code Injection Attacks: A popular technique used by malware“, MALWARE, 2014

EXPLOSIVE MATERIAL DETECTION THROUGH ANALYSIS OF INFRARED AND RAMAN SPECTRUMS CAPTURED BY A PORTABLE SENSOR

Hichem El Mokni[1], Josef Heinskill[2] and Marek Schikora[3]

[1] *hichem.elmokni@fkie.fraunhofer.de*

[2] *josef.heinskill@fkie.fraunhofer.de*

[3] *marek.schikora@fkie.fraunhofer.de*

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE
Fraunhoferstraße 20 | 53343 Wachtberg

Abstract

This paper presents the progress made in developing a semi-automated method for analysis and evaluation of infrared and RAMAN spectrums for explosive material detection, as part of the Vesper [Plus] project [5]. The method is based on a spectrum database of a set of explosive materials, and having a spectrum of an unknown sample, tries to determine the eventual mixture (with rough percentages) of explosive materials composing the sample. The evaluation algorithm is composed of two phases. The first phase extracts the most probable candidates in the spectrums database which matches peak by peak the sample spectrum to evaluate. The second phase removes the non-relevant candidates of the first phase using an innovative approach based on a particle filter. Each peak of the sample spectrum and spectrum candidates is treated solely to generate all possible mixtures corresponding to it in a multidimensional mixture space (one dimension for each candidate, where the ordinate corresponds to its percentage in the sample). The generated mixtures are used as measurements to update the repartition of particles in the multidimensional mixture space. The step by step update introduces a relationship between the peaks not used in the first phase. It is shown that by correctly tuning the parameters of the particle filter it is possible to get the correct explosive materials composition of the unknown sample.

Keywords: spectroscopy, Infrared, Raman, explosive material, particle filter.

1 INTRODUCTION

Spectroscopy results from the interaction between the analysed material and electromagnetic waves. It has virtually replaced the ancestral qualitative study of chemical compounds: it allows the determination of the structure on very small quantities of material, it implements non-destructive methods, and its precision is high in laboratory conditions. The advance made in developing portable devices for IR Spectroscopy will allow the use of this technology, not only by experts, but by police, customs and security crews, to identify any threat caused by any unknown material or luggage. For that purpose, a semi-automated and reliable method for spectrum analysis is needed to identify an eventual explosive material. The main procedure is illustrated in comparing the measured spectrum of an unknown material with a database of explosive materials spectrums. The proposed method tries to mimic the role of an expert in evaluating a noisy and inaccurate spectrum generated by the portable device (in contrast with the high spectrum precision in laboratory conditions).

2 FUNDAMENTALS

In this section we present a short review of Infrared and Raman spectroscopy, covering the historical background and the physical phenomena beyond, which will make the resulting spectrums more understandable.

2.1 Infrared spectroscopy

The infrared (IR) radiation was discovered in 1800 by Frederick Wilhelm Herschel. These radiation which are beyond the red wavelengths, are located between the region of the visible spectrum and radio waves. The infrared range extends from 0.8 micro meters to 1000 micro meters. It is arbitrarily divided into three categories, the near infrared (0.8 to 2.5 micro meters i.e. 12500-4000 cm^{-1}), the mid-infrared (2.5 to 25 micro meters i.e. 4000-400 cm^{-1}) and the far infrared (from 25 to 1000 micro meters or 400-10 cm^{-1}). In 1924 it was found that the energy of mid-infrared radiation coincided with the internal motions of the molecule. Thus, the relationship between the absorption of IR radiation by a molecule and its molecular structure was demonstrated. Although parts of the near and far infrared sparked some interest, using the mid IR spectroscopy remains the most suitable for the elucidation of the molecular composition of a compound [3].

Fig. 1 shows different vibrational movements of a molecule. The absorption of IR energy is possible only if the IR frequency is equal to the proper liaison frequency of the molecule. Infrared spectroscopy examines absorption and transmission of photons in the infrared energy range.

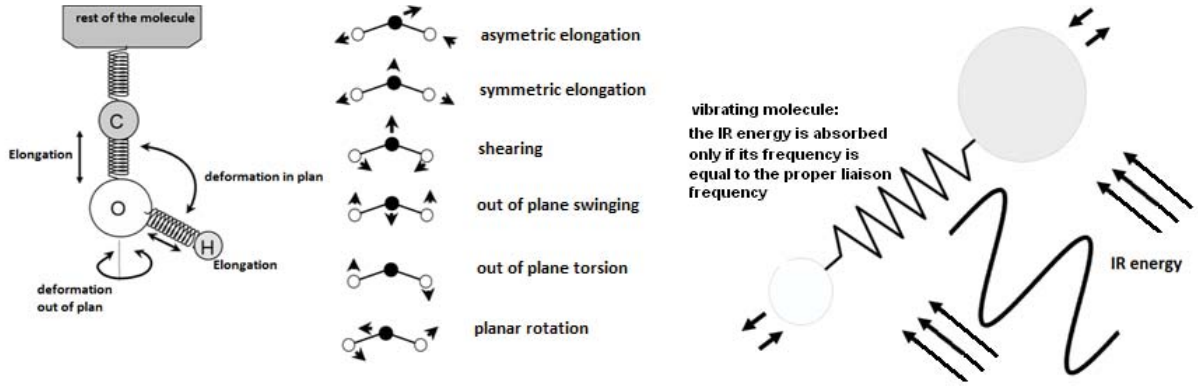


Fig 1: Infrared spectroscopy: vibrational movements of a molecule and IR absorption

2.2 RAMAN spectroscopy

Raman scattering (sometimes called the Raman Effect) was discovered by the Indian physicist C. V. Raman in 1928 [4]. Raman scattering has given rise to a number of important technologies, and foremost among these is Raman spectroscopy. Raman spectroscopy studies the vibrational transitions (movement wave number from 0 to 4000 cm^{-1}) from the process of inelastic scattering of light. The Raman Effect results from the interaction of photons of a monochromatic light source with the sample molecules. Approximately 1 in 10 000 photons are elastically scattered by molecules (free energy change). This diffusion is called Rayleigh diffusion, where the light does not gain or lose energy during the scattering (middle of the vibrational diagram in Fig. 2).

Occasionally one photon will be not elastically scattered (1 in 100 million) with a slight loss in energy (Raman scattering, left of the vibrational diagram in Fig. 2) corresponding to a vibrational transition. As it is intrinsically a very low process, intense light sources such as lasers are required. The amount of anti-Stokes scattering, where the scattered photon has more energy (right of the vibrational diagram in Fig. 2) is even lower. The shift due to the Raman Effect is determined by the spacing between the vibrational states and the ground states i.e. by the phonons of the system [4].

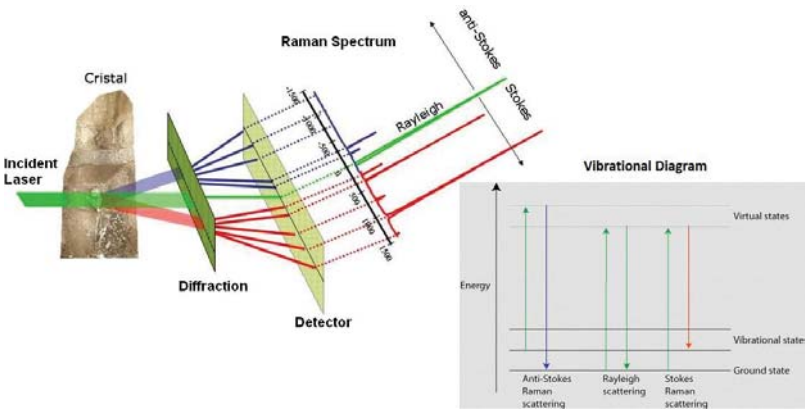


Fig 2: Raman spectroscopy *Copyright - © 2004 Philippe Gillet*

Raman spectroscopy is a complementary technique to infrared. They are based on the same natural origin: the vibration of bonds between atoms of a molecule that is permitted between the different levels of vibrational energy transitions. The different nature of the two processes of interaction at the origin of the Raman and infrared (absorption, reflection or transmission) make certain vibrations happen in infrared and others only in Raman (rule of mutual exclusion), others will happen in both, or neither in one nor in the other. Therefore, to construct a complete image of a vibrational molecule both techniques must be used.

3 USED METHOD

3.1 Problem presentation

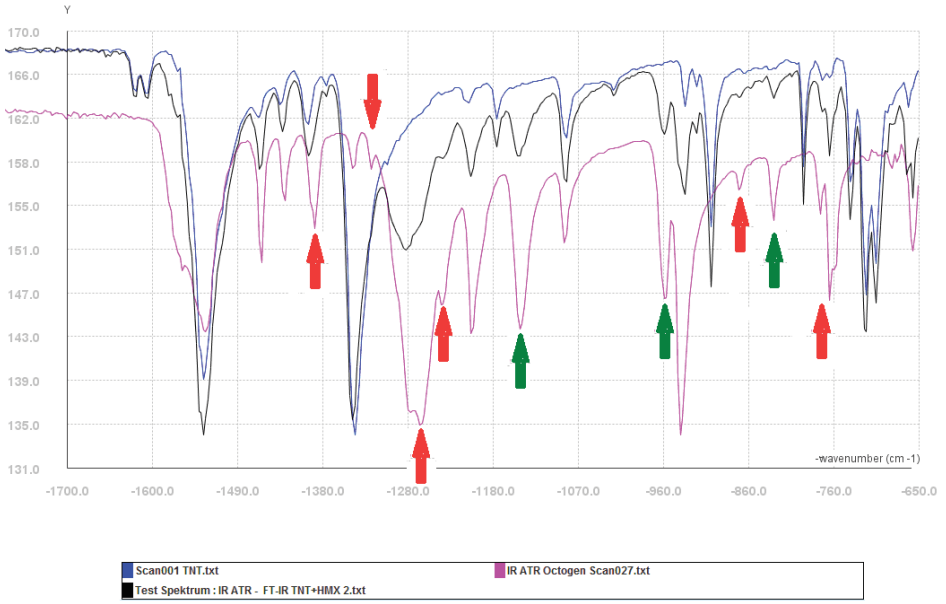


Fig 3: First example: TNT 80% + Octogen(HMX) 20%
Red arrow: a missed/displaced Octogen(HMX) peak in mixture
Green arrow: a characteristic present Octogen(HMX) peak in mixture

Through this first example we will try to illustrate the problem. Fig. 3 represents the IR-spectrums of TNT (blue), HMX-Octogen (purple) and a mixture of 80%TNT and 20% HMX (black), which are both explosive material. For each wavenumber (cm^{-1}) relative to a given Infrared wave frequency, the spectrum represents the amount of IR energy absorbed by the material (ordinates axis). The spectrum is truncated to the wavenumber interval from 650 cm^{-1} to 1700 cm^{-1} due to the high noise level outside this interval.

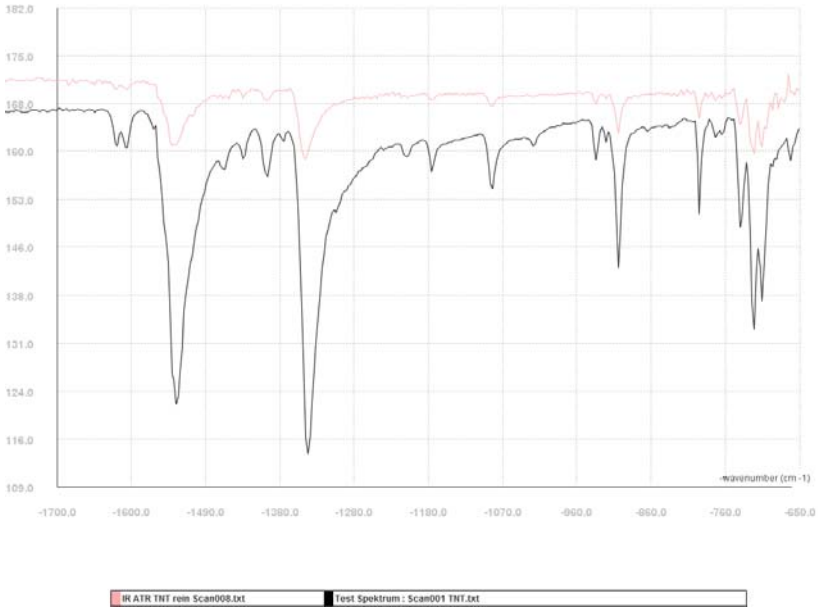


Fig 4: Stretching and vertical translation effect on two IR spectrums of TNT

Few remarks have to be highlighted. First, taking several measurements of a same material will not result in identical spectrums. A possible vertical translation (global shift in energy absorption) and a vertical stretching effect on the global spectrum shape are observed, as depicted in two spectrums of TNT in Fig. 4. This is due to several possible reasons: angle of arrival on the material of the IR energy, or heterogeneity of the material. Fig. 3 is actually an optimized visualization by bringing the spectrums on a common window. However, the peaks positions remain constant, and are considered as characteristic signals for comparing two spectrums. A strong peaks overlap is observable in this example, making it difficult to detect HMX which has fewer peaks than TNT. Moreover, characteristic peaks of HMX have disappeared or have been slightly displaced in the mixture spectrum (black), as presented by the red arrows. In fact, in those positions the TNT spectrum (blue) is characterised by a high slope, which causes the HMX peak (red arrow) to disappear in mixture or to be merged with the next too close TNT peak. The disproportion in the mixture (80% TNT and only 20% HMX) amplifies this effect. Nevertheless, three characteristic peaks of HMX are still present in the mixture spectrum, as shown by the green arrows. That is due to the fact that TNT spectrum (blue) has low slopes on those positions.

3.2 Peaks extraction

The first step in evaluating a spectrum is peaks extraction, applied on the corresponding text file generated by the spectroscopy sensor. The peaks extraction procedure is applied on all spectrums stored in the explosive materials spectrum data base. Peaks are looking downwards, so local minimums. The function takes the spectrum as input, and a threshold delta which indicates the minimum intensity of a peak. The peak intensity is the difference between the peak (local minimum) and next valley (next local maximum). Any peak intensity below the threshold delta is considered as noise, and so ignored. Fig. 5 shows the extracted peaks from a spectrum of TNT and HMX mixture.

Relying solely on peaks for finding the mixture of components of an unknown material is a limited procedure. Looking back to the spectrum of the mixture TNT80%-HMX20% in Fig. 3, HMX is distinguishable from TNT only with three peaks. Those three peaks are common for HMX and few other spectrums in our database. Besides, any of those peaks can disappear in another measurement due to noise, angle of view of the sensor to the material… A statistical approach, using a particle filter, is adopted to evaluate a spectrum as presented next.

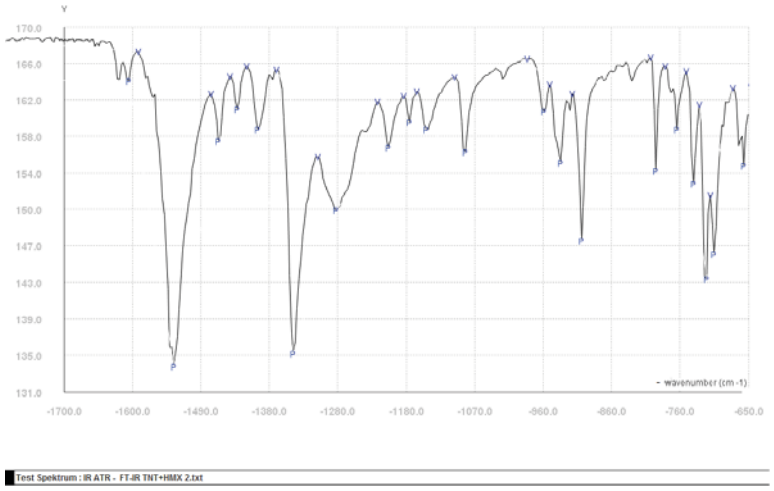


Fig 5: Peaks detection, P for peaks and V for valleys

3.3 Virtual sensor: possible mixtures as measurements

As revealed previously, an expert will focus on peaks to evaluate a spectrum and try to determine possible components. To mimic this behaviour, we will suppose a virtual sensor, which take a peak in a spectrum as input (position, intensity, shape) and generates all possible mixtures that may generate that peak. The maximum number of components in each mixture is set to three. The mixtures are chosen among the most probable components detected in the previous peaks extraction procedure (the first five classed components matching peak by peak the unknown spectrum to evaluate, but can be increased when working with larger database). At each filtering step we will take one peak of the unknown spectrum and generate the possible mixtures among the five candidate spectrums which will be passed as measurements to a sequential Monte Carlo intensity filter (SMC iFilter). The mixture (measurement) generation process for our virtual sensor will follow some heuristics. Let's denote the peaks of the unknown spectrum by $P_x^i, i = 1..nP_x$, and the peaks of a candidate spectrum k by $P_{c_k}^j, \mathrm{j} = 1..nP_{c_k}, k = 1..5$. A peak is characterized by its position (abscise), its intensity (ordinate) and the subset of spectrum points having abscise in peak's position $\pm PeakDelta$, which is set to 8 in our case. Let's proceed with one filtering step taking one peak P_x^i of the unknown spectrum. For each candidate spectrum CS_k we will check if it has a peak $P_{c_k}^j$ matching P_x^i. After superposing the two peaks (eliminating the vertical shift), a matching distance is computed: the sum of absolute point by point differences. The smaller the matching distance is, the closer the shapes of the two peaks are.

We have limited the possible affected percentage for each component in a mixture to a set of discrete values 99%, 75%, 50%, 25%, 12%, and 0%. Therefore, the set of all possible combinations of candidate spectrums CS_l, CS_m and CS_n is:

(99, 0, 0) | (75, 25, 0), (75, 0, 25), (75, 12, 12) | (50, 50, 0), (50, 0, 50), (50, 25, 25) |

(25, 75, 0), (25, 0, 75), (25, 25, 25) | (12, 12, 75), (12, 75, 12) |

(0, 0, 99), (0, 99, 0), (0, 75, 25), (0, 25, 75), (0, 50, 50)

where $l, m \text{ and } n \in \{1..5\}, \text{ and } \mathrm{l} \neq \mathrm{m} \neq \mathrm{n}$

Again, the mixture combinations are restricted to a maximum of three components, and chosen so that the percentages sum is close to 100%. Now we will use some heuristics to go through elimination within this set of all possible mixtures.

3.3.1 Heuristic 1

A matching distance between peaks P_x^i and $P_{c_k}^j$ below a given PEAKS_MATCH_THRESHOLD indicates that the shape of $P_{c_k}^j$, generated by candidate spectrum CS_k, is not affected by any

other component spectrum in the mixture. A peak is affected if another component spectrum in the mixture has a relatively high slope at that position (above a threshold) and a sufficient percentage. So we compute the slopes of the remaining four candidate spectrums at that position. If a candidate spectrum $CS_l, l \neq k$ has a high slope at this position, we eliminate all bi-components mixtures involving $CS_k$and $CS_l$with a percentage higher or equal to 50%. The same heuristic is also used to eliminate tri-components mixtures involving CS_k and two spectrums from remaining candidates having both high slopes at this position. Besides, for candidate spectrum CS_k that has generated this clear peak, we eliminate all mixtures involving CS_k with a percentage less or equal to 12%. Fig. 6.a illustrates an example where mixture peak (first peak) has a perfect match with TNT peak (last peak). Heuristic 1 excludes bi-mixtures between Semtex and TNT because Semtex has a high slope at this position, which if present will affect the shape of the peak.

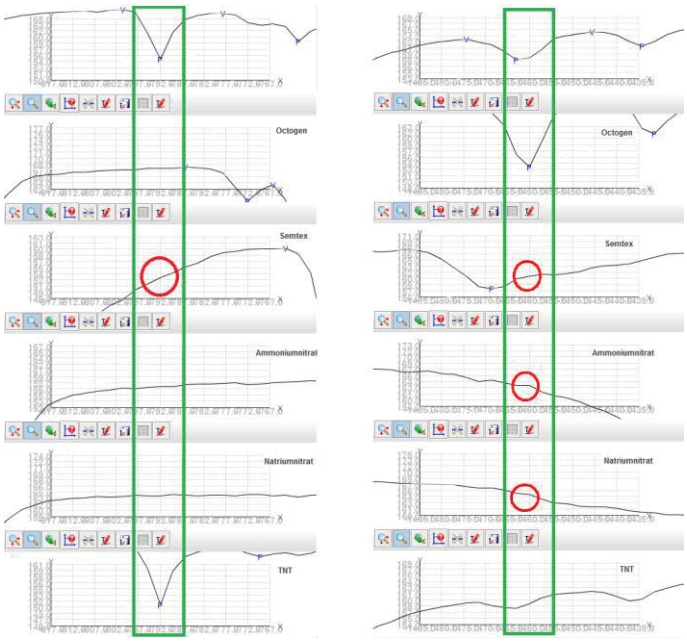


Fig. 6: (a) example for Heuristic 1 (b) example for Heuristic 2

3.3.2 *Heuristic 2*

A matching distance between peaks P^i and $P^j_{c_k}$ above a given PEAKS_NON_MATCH_THRESHOLD indicates that the shape of $P^j_{c_k}$, generated by candidate spectrum CS_k , is affected by at least one other component spectrum in the mixture. A peak is affected if another component spectrum in the mixture has a relatively high slope at that position (above a threshold) and a sufficient percentage. So we compute the slopes of the remaining four candidate spectrums at that position. If a candidate spectrum $CS_l, l \neq k$ has a low slope at this position, we eliminate all bi-components mixtures (75%, 25%) and (50%, 50%) involving CS_k and CS_l . The same heuristic is also used to eliminate tri-components mixtures involving CS_k and two spectrums from remaining candidates having both low slopes at this position. Besides, for candidate spectrum CS_k that has generated this affected peak, we eliminate the pure CS_k possibility with a percentage of 99%. Fig. 6.b illustrates an example where the mixture peak (first peak) is not matching the Octogen peak that has generated it: the shape is not matching and a shift to the left is visible. Semtex has a low slope at this position, which will not affect the shape of the peak if only mixed with Octogen, so bi-mixtures of Octogen and Semtex are discarded. Ammonium nitrate and Natrium nitrate have higher slopes, but the slope orientation is the inverse of peak shift orientation. The only component that can cause such a deviation of the Octogen peak is TNT. Thus all mixtures not including TNT are excluded.

3.3.3 Heuristic 3

After treating the peak P^i, we move to treat absent peaks between the position of peak P^i and the position of the previous peak P^{i-1}. We iterate through the candidate spectrums and for each spectrum CS_k that has missing peaks in that interval, we compute the slopes of remaining spectrums candidates at a missing peak, and keep only mixtures combinations that explain the absence of that peak: low percentage for CS_k with at least one spectrum with high slope at this position.

3.4 Sequential Monte Carlo Intensity Filter

The possible mixtures measurements generated by the virtual sensor looking at one peak at each step (based on the heuristics of previous section) are filtered by a SMC iFilter as presented in reference [2], which can be summarized in three main steps: the prediction phase, the correction phase and the resampling phase. The particle set corresponds to the multi-target state, where each target is a possible mixture combination of component percentages underlying the unknown spectrum to evaluate.

4 EVALUATION

Fig. 7 to the left presents an evaluation example of a mixture of 40% Ammonium nitrate, 30% TNT and 30% RDX. The superposed spectrums make a visual evaluation difficult, so our developed software offers the option to choose only one or more spectrums on the display window. The three components of the mixture with two other components, Eurodyn2000 and Seismogelit, were selected by the peaks matching procedure as spectrum candidates for the evaluated spectrum, and passed to the SMC iFilter. Fig. 7 to the right shows the output of the iFilter, each component with the evaluated percentage, where the Seismogelit component was excluded (percentage below 5%).

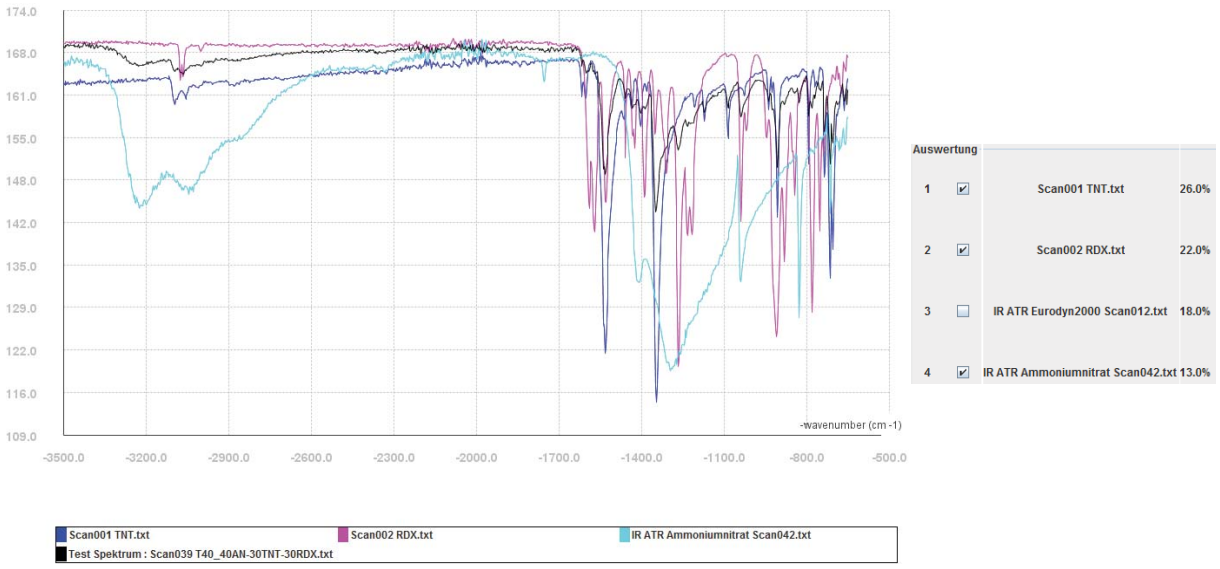


Fig 7: mixture and components spectrums (40% AN, 30%TNT, 30%RDX) and resulting evaluation

As an example for RAMAN spectrums evaluation, Fig. 8 presents an evaluation example of a mixture of 70% Ammonium nitrate, 15% TNT and 15%RDX. Here we can see that RDX was not detected, but we figured out that even visually there was no matching (RDX spectrum is not present on the figure). We think that the heterogeneity of the sample can cause a misdetection of one component. Besides a false detection of Eurodyn2000 is present, but a visual check of RAMAN spectrums cannot definitely discard its presence.

Fig 8: mixture and components spectrums (70% Ammonium nitrate, 15%TNT, 15% RDX) and Eurodyn2000 spectrum

5 CONCLUSION

We made the statement that some mixture spectrums weren't really reflecting the presence of all components. This may be due to the heterogeneity of the mixtures, which can explain gathering IR and RAMAN measurements of only few components in the mixture. Nevertheless, heterogeneity is a characteristic of amateur made explosives, targeted by our work. So detecting at least one explosive component in a mixture is satisfying the objectives of our work: we need to correctly launch a threat alarm of explosives presence, not to find the correct component percentages of the mixture. In over 90% of evaluated spectrums we were able to identify correctly at least one explosive component. We have to mention that our developed method is not intended to be full automated. It can limit the total number of possible evaluations and presents a convivial interface for a human evaluator who has to make the final decision. We think that a further closer work with an expert in spectroscopy can enhance the heuristics, leading to better final results. The complementarity aspect of IR and RAMAN spectroscopies needs also to be further investigated. This work can be also extended to detect other prohibited materials like drugs.

REFERENCES

[1] Chang, Chein-I ; Brumbley, Clark M. *A Kalman filtering approach to multispectral image classification and detection of changes in signature abundance.* IEEE T. Geoscience and Remote Sensing, 37 (1999), Nr. 1, S. 257-268

[2] M. Schikora, W. Koch, R. L. Streit, D. Cremers. *A Sequential Monte Carlo Method for Multi-Target Tracking with the Intensity Filter.* Chapter in Advances in Intelligent Signal Processing and Data Mining, Springer-Verlag Berlin Heidelberg, 2012.

[3] Chalmers, J.M., Edwards, H.G.M., Hargreaves, M.D. *Infrared and Raman Spectroscopy in Forensic Science.* John Wiley & Sons, 2012.

[4] University of Cambridge Teaching and Learning Packages. *Raman scattering.* http://www.doitpoms.ac.uk/tlplib/raman/raman_scattering.php

[5] E. Dalinger, H. El Mokni, J. Heinskill, D. Ley, G. Linkmann, F. Motz, O. Rassy, A. Wagner. *Verbesserung der Sicherheit von Personen in der Fährschifffahrt Plus (Vesper Plus).* Abschlussbericht Fraunhofer FKIE , FKZ: 13N11919, 2015.

SYNTHESIS AND TEST OF SUITABLE ADSORBERS FOR SELECTIVELY TRAPPING AND DETECTING EXPLOSIVES AND IMPROVISED EXPLOSIVES PRECURSORS FROM GASPHASE

Gudrun Bunte [1, 2], Jürgen Hürttlen[2], Moritz Heil[2], Max Rieger[2], Horst Krause[2]

[1] *gudrun.bunte@ict.fraunhofer.de*

[2] Fraunhofer Institute for Chemical Technology, ICT, 76327 Pfinztal (Germany)

Abstract

To counteract terrorists' threats posed by explosives and improvised explosives devices there are needs for reliable, rapid, highly sensitive and selective detection measures. Our approach is to develop molecularly imprinted polymers, MIPs, on the one hand as particulate substance selective sample enrichment materials to trap and enrich explosives traces from air. On the other hand we develop layered MIPs as selective sensor coating layers to be combined with different low cost sensor platforms (e.g. QCM, SAW, Gas-FET etc.) as portable, handheld sensor units or in fixed sensor networks capable to detect explosives, taggents or precursors from air. A relatively new work stream at ICT is also looking into the application of so called MOFs, metal organic frameworks as selective adsorber materials. MOF may be used as particulate materials or as layered coatings as well. In the current presentation a short overview will be given about the studied synthesis and coating technologies, the used characterisation techniques as well as the already achieved results.

Keywords: explosives trace detection, selective MIP, MOF, particulate adsorber, sensor coatings

1 INTRODUCTION AND OBJECTIVES

MIP and MOF adsorbers have a three-dimensional porous structure with high inner surface values and high adsorption capacities for specific target substances. Ideally MIP trap and enrich the targeted explosives and do not adsorb any other background substances typically present in the air (such as parfumes, fragances etc.), and these adsorbers enable the detection of explosives plumes even if they are present in the ppb-level or lower.

MIPs are pure organic materials which are synthesized in the presence of the later targeted explosive substance and like enzymes they possess substance selective adsorber sites after cleaning procedures have extracted the target molecules and the residual reaction agents. The effectiveness of the particulate MIP adsorption properties highly depend on the synthesis conditions (e.g. type of used monomers, organic solvent as porogen, emulsifier, UV-starter and cross-linker as well as their relative percentages in the formulation, temperature, time, stirrer conditions etc.). In the case of so called core-shell MIPs, cs-MIPs also a suitable material type of the inert core as well as a suitable linker procedure is needed to be able to synthesize a thin MIP layer onto the cores. Recent work was also directed to css-MIPs. These contain an inert core coated with a special very thin layer of a microwave heatable material and on the outer side the sensing MIP layer. Advantages of the cs- and css-MIPs will be the capability to use larger air volume flows through the packaging material and for css-MIPs also a faster desorption possibility of the trapped analyts into the detector device (e.g. MS).

If MIPs are used as sensing layer in low-cost sensor platforms such as QCMs, SAWs, Kelvin probes or Gas-FETs these need different layer thicknesses and sometimes different linker procedures depending on the sensor surface material (silica, gold, silver

etc.). Therefore we studied different coating technologies such as nanoplotting or spin coating combined with UV polymerization and newly also so-called grafting-from or RAFT synthesis approaches. In any cases the formulation configuration and the coating conditions must be specially and differently adapted to achieve layers of some µm or some nanometers.

MOFs are crystalline materials composed of metal ions or clusters (e. g. Zn, Cu, Fe) connected by organic linkers (e. g. terephthalate). Preliminary work on MOFs was done using some commercially available MOFs (e.g. MIL-53(Al) and ZIF-8) and testing their adsorption properties for precursors such as nitro methane.

2 EXMERIMENTAL

2.1 Synthesis of particulate and layered MIPs

Molecularly imprinted polymers are highly cross-linked, porous polymers which are synthesized in the presence of a template, namely the analyte to be detected later. When the template is removed, the MIPs have highly selective adsorption / binding sites for the targeted analytes. In case of nitro groups present in explosives such as TNT, DNT and in the taggent DMNB, a covalent template binding approach is not possible. Here a non-covalent approach via e.g. hydrogen bonds or van der Waals bindings was chosen. The synthesis of MIPs via suspension polymerization [6] was thoroughly tested in order to achieve the best conditions regarding type of porogenic solvent, amount of cross-linker, porogen and emulsifier as well as stirring conditions (speed, type of stirrer). Main objectives were to achieve regular particles with narrow particle size distributions, high specific surface areas and high adsorption capacities for the targeted analyte (TNT, DNT or DMNB). For reasons of comparison only methacrylic amide has been used as monomer for varying the before mentioned conditions.

In order to get more material out of one synthesis batch an upscaled synthesis reactor with two parallel 6 L autoclavs was planned, installed and tested. Also the necessary cleaning procedure was upscaled including soxhlet cleaning steps, vacuum oven handling and sc-CO_2 extraction as the last step. Using the best set of synthesis conditions afterwards also a variation of the monomer type was investigated, respectively, acrylamide (AA), methacrylic acid (MAA) and methacrylic amide (MAAM).

Because the synthesis of MIPs lead to particles with sizes of 20 to 40 µm also a second approach for synthesizing so called core-shell MIPs or cs-MIPs was tested and optimized in order to achieve particles with larger sizes yielding to an increased gas flow through the MIP packing in a standard glass tube used for air analysis. Different cores were tested (magnetite cores or SiO_2 cores) as well as different pre-preparation techniques for achieving a thin anchor layer on the cores before synthesizing the MIP layers onto the cores. Regarding both tested versions, thiol or acrylate anchors, the latter technique proceeded in a special fluidized bed reactor yielded to the best results.

For the synthesis of layered MIPs different coating technologies were studied over the years (spray coating, nanoplotting, spin-coating) in order to produce different layer thicknesses. Compared to particulate MIPs not a thermal radical starter but a UV light initiator of Irgacure type was used in combination with a special UV lamp. Especially for the spin-coating the synthesis mixture (type and amount of porogen solvent, emulsifier and cross-linker) had to be further adapted / improved in order to achieve good porous MIP layers with enhanced sorption properties for the targeted analyt compared to the non-imprinted NIP material. Depending on the type of sensor and the used surface material (silica, gold, silver, silicon) it was further necessary to test and develop a suitable pre-synthesis step for achieving first a thin anchor layer on the sensor surface on which the MIP layer was immobilized afterwards. Until now known gold is best preconditioned via a thiol anchor substance such as pentene thiol. Silica may be

preconditioned via grafting-from components such as TEOS, (tetraethyl-orthosilicate) and silicon may be anchored best via so-called RAFT (Reversible Addition–Fragmentation Chain Transfer) specific agents such as APTES ((3-aminopropyl)-triethoxysilan).

2.2 Characterisation and evaluation of sensing materials

Particulate MIPs and cs-MIPs synthesized so far were especially characterized for their internal surface areas and pore diameters (via BET) and their particle size distributions (laser diffraction spectrometry). The geometric structure and pore sizes were also scanned via raster electron microscopy. In case of layered MIPs also AFM images were used to determine the achieved pore structures. Achieved cleaning grades after synthesis were evaluated using special inhouse GC-MSD techniques using head-space or SPME-pre-sampling methods. [1/2]. For evaluating the selective adsorption properties of MIPs / cs-MIPs the materials were treated using homemade gas generators providing distinct low concentrations of targeted explosives (e.g. TNT, DNT or DMNB). The off-line-loaded samples afterwards were characterized again using SPME or HS-GC-MSD techniques. The imprinted material was tested against the non-imprinted correspondent (synthesized without using the target in the formulation). Best materials were also tested online using a special tandem adsorber/desorber device coupled to GC-TOF-MS [2].

Adsorption properties of synthesized / coated layered MIPs were studied using QCMs or Kelvin Probes as transducers together with our homemade gas generators [1/3].

In case of css-MIPs preliminary work was directed to find suitable microwave “coating materials” which enable preferable the highest heating rates per second. In that case until now different materials were until now coated on small plates or on glass beads testing different coating technologies. Reachable heating rates were tested using special techniques set-up in-house [4].

In case of MOFs so far a commercial gas generator was integrated in front of the TD-GC-TOF-MS system to evaluate the applicability of the gas generator as well as determining preliminary results regarding the adsorption properties of selected MOFs against small and highly volatile precursor components such as NM or NB [5].

3 SELECTED RESULTS AND DISUSSION

3.1 Particulate MIP adsorbers

A lot of work effort was directed to find out the best configuration of the MIP formulations and the best synthesis conditions. Fig. 1 exemplarily shows extremely different MIP particle types obtained via suspension polymerisation using chloroform, $CHCl_3$ or carbon tetrachloride, CCl_4. Using $CHCl_3$ as porogen solvent synthesis leads to spherical, porous polymers with mean particle sizes of about 20 to 40 µm and specific areas up to 400 m²/g. In case of CCl_4 the solubility and prearrangement of all ingredients of the MIP suspension mixture was rather poor, yielding to asymmetric irregular, hollow particles.

Best tested synthesis conditions using chloroform as porogenic solvent in combination with PEG4000 as emulsifier lead to uniformly layered core-shell MIP particles having sizes of about 230 µm and BET surface area values of about 240 to 270 m^2/g with a pore radius of 28 to 33 Å. As used for the full polymeric MIPs, the core-shell MIPs were synthesized using about 83 % of EGDMA, ethylene glycol dimethacrylate, as cross-linker.

During the BMBF financed project EXAKT we achieved an up-scaling of the synthesis process from lab-scale (glass ware, 10 g per batch) to a pre-technical scale yielding to

about 200 g per batch, including the necessary cleaning procedures after the synthesis step [2]. For this a special reactor with two parallel 6 L reactors was designed, installed, tested and successfully optimized. Moreover the synthesis formulation had to be further adapted, especially for the synthesis of cs-MIPs.

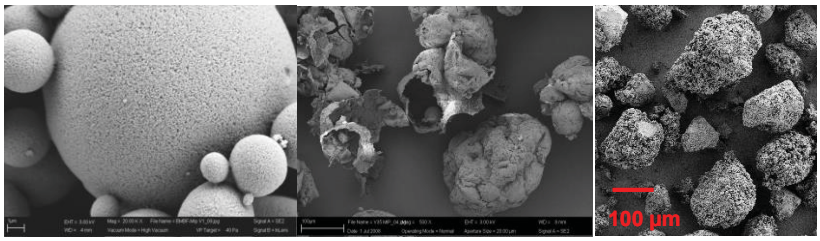


Fig. 1 SEM images of spherical, porous MIP particles using $CHCl_3$ (left) and hollow irregular MIP particles using CCl_4 as porogenic solvent (middle) and SEM of obtained core-shell MIP particles (right, $CHCl_3$ used)

Different core materials for cs-MIPs were tested (e.g. magnetite cores or SiO_2 cores). Silica cores showed the best results as they offer the most suitable linker procedure for depositing a thin adhesive layer to bind the MIPs onto the cores. The best suitable anchoring technique used an acrylate-based anchor applied in a special fluidized bed reactor.

For the explosives targets tested so far (TNT, DNT, DMNB) we were able to achieve MIPs and cs-MIPs showing enhanced, selective adsorption characteristics compared to their NIP correspondent. Best formulations slightly differ for full polymeric and core-shell adsorbents especially in the type of best pre-polymer (acrylamide, AA, methacrylic acid, MAA or and methacrylic amide, MAAM and in the type and amount of used emulsifier (PEG for MIPs and PVA for cs-MIPs in different amounts related to the used monomer).

Fig. 2 exemplarily shows the measured average MS-TOF-peak areas after online-treatment of TNT-imprinted cs-MIPs and cs-NIPs in a distinct TNT/nitrogen gas stream for a short adsorption step and following thermal desorption from the adsorbers into the TOF detector. Given peak area values are the mean values of 400 cycles of adsorption and desorption using the same filled trap. The cs-NIPs show no capacity for adsorption of TNT. Best imprint effect shows the AA-based cs-MIP followed by MAAM and MAA.

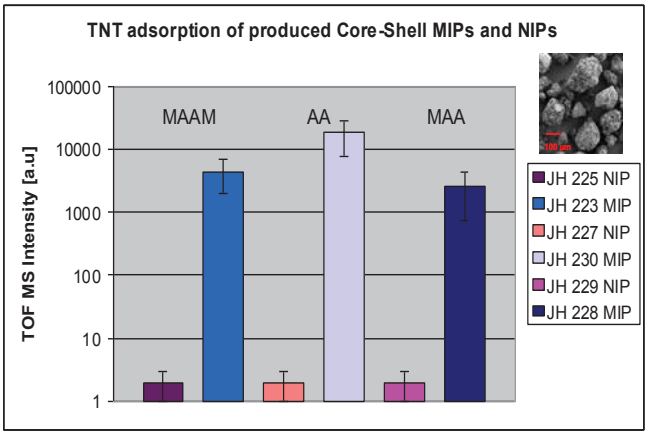


Fig. 2 Averaged measured TOF peak intensities after TNT adsorption on core-shell MIP and NIPs (online treatment for 8 min using TNT gas generator) and subsequent desorption from tandem desorber after 400 cycles

Adsorption tests of these TNT-imprinted cs-MIP materials using DNT or DMNB using homemade gas generators showed nearly no cross sensitivity to the other target analyst.

Some preliminary test measurements above realistic IED probes (Fig. 3) were made using a specially prepared radio IED equipped with a block of technical TNT in the rear of a radio, which was wrapped in a polymer foil. Used sampling time was 8 min using 20 ml/min flow speed. Using the best TNT imprinted cs-MIP as adsorption material in the TD-GC-TOF-MS-system, TNT was positively identified via airborne sampling near the radio. When replacing the TNT cs-MIP in the tandem adsorber with the best DNT imprinted cs-MIP, DNT could also be identified (typical component in technical grade TNT, 1 to 2 %). In case of Tenax only DNT was detected. Furthermore Tenax trapped a lot of different softeners and polymer foams from the radio. Compared to that, the produced cs-MIPs trapped very low number of components specific for the normal radio plume and in much lower amounts.

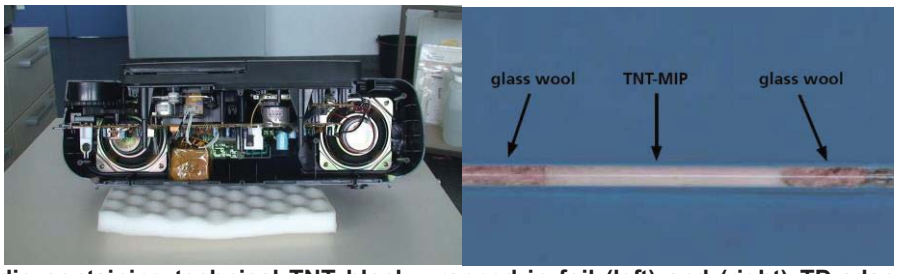


Fig. 3: Radio containing technical TNT block wrapped in foil (left) and (right) TD-adsorber tubes filled with TNT-specific MIP (before testing in the TD-GC-TOF-MS system)

Synthesis of TATP imprinted cs-MIPs is currently ongoing; until now not all cores are fully coated and the achieved particles partly grow to large (up to 1 mm, see Fig. 4). Improvements may be achieved using a new type of stirrer and/or altering the synthesis formulation (monomers, linker to cores, emulsifier potentially better related to TATP structure,…). Nevertheless sieved material with small sizes (230 µm) was cleaned via normal procedure and tested for the residual TATP amount using SPME-GC-MSD method. Only very few TATP was found. Therefore some first tests were made regarding the TATP adsorption properties of two different cs-MIPs and the related cs-NIPs. The material (200 mg) was packed in a GC-liner (i.d. 2 mm) with glass wool plugs (15 mg) in front and back position. In that case a special air-flow pump was used together with a small amount of TATP on a petri dish using different airflow values (20 ml/min, 100 ml/min and 500 ml/min for 15 min). Adsorbed / desorbable TATP was afterwards analysed via HS-GC-MSD. Only the measurements with high flow rate showed measurable TATP amounts in the MIP material, most was adsorbed by the glass wool in case of low flow values. Compared to the NIPs the imprinted materials showed slightly higher amounts of TATP. Further synthesis tests as well as enhanced adsorption test procedures will be worked on in the future.

Fig. 4: REM photo of TATP imprinted cs-MIPs and used sampling pump, GC liner and TATP source

3.2 css-MIPs and microwave adsorber / desorber

In order to fasten the desorption step (from some minutes to some seconds) ICT is working on a suitable microwave desorber element which could be installed for

example as inlet to the GC-TOF-MS-system (instead of the tandem desorber unit) used in the EXAKT project or to each other MS-system. Central element for such a unit would be the development of microwave heatable core-shell-shell-MIPs. These will consist of e.g. glass beads as inert cores with a first core of special material followed by a second shell consisting of a normal MIP-adsorber. Second, and more important effect of such css-MIPs would be the possibility of much larger flow streams per time through the adsorber package which might be very useful for e.g. sampling large containers potentially equipped with smuggled threatening materials. In any case larger flow volumes per time enhance the relative sensitivity of the adsorbing step. Targeted objectives are to test different microwave active materials, to test suitable coating technologies and conditions (fluidized bed reactor, pellet plant, ..) and to characterize the achievable heating rates and profiles. Initial work started with coating planar glass plates with different materials (e.g. magnetite, conductible soots, metal lacquers, ...) and activating them in a cylindrical micro wave emitter and measuring the achieved heating rates with an IR sensor. Best achieved heating rates were in the range of 80 °C per min (Fig. 5).

Fig. 5 Schematic view of the planar test set up (left), and photos of a test bead package and the initially used single mode micro wave plant (middle and right)

Later and current work is looking into the coating of glass beads and testing large amounts (package of some square centimeters with some centimeters height) for their heating profiles and the reproducibility of the layer dimensions. Currently the bead packages are tested in a multiple mode industry micro wave plant. Best material type found until now are some commercial iron carbonyl powders which may be coated onto glass beads using a fluidized bed reactor. The tested powders consist of mainly iron particles (different sizes) and small amounts of a polymer compound (different types). For the best iron powder tested until now a cylindrical bead package of 5 cm radius and 6 to 7 cm height is uniformly heatable up to 200 °C in only 6 seconds. Special x-ray CT measurements showed that uniform coating thicknesses in the range of 20 µm were realized (Fig. 6).

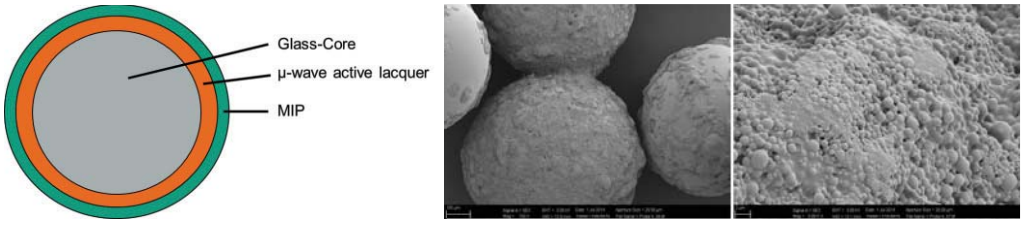


Fig. 6 Schematic view of css-MIPs (left) and REM pictures of glass beads coated with an iron carbonyl powder (left full bead and right a view of the near surface structure)

3.3 Particulate MOF as adsorbers for precursors

Preliminary results were achieved relating studying the adsorption properties of some commercially available MOFs. As a prerequisite for testing a commercial gas generator

based on the evaporation principle was coupled to the TD-GC-TOF-MS system mentioned earlier and a lot of pre-tests were done to measure the reproducibility of the produced gas concentrations and the actual amount using e.g. special IR gas cells as well as a quadrupole MS (Omnistar MS, Pfeiffer). Currently also gas sample bags are tested from which the gas is sampled via mass flow controllers to the inlet of the tandem desorber in order to achieve lower flow volumes compared to the commercial gas generator.

Fig. 7 Photo of the commercial evaporation based gas generator coupled to the entrance of the TD-GC-TOF-MS-system

For the commercial MOF MIL-53 first adsorption tests were done with nitro methane containing nitrogen gas. The MOF was pretreated in a vacuum oven over night at 100 °C and then filled into the cold traps of the tandem desorber. During recurrent adsorption and desorption cycles the peak intensity of NM was slowly reduced meaning the adsorbed / desorbed amount decreased over time. The material was analysed via x-ray diffraction where an altered diffraction spectra was measured. This may be due to a so called breathing of the MOF structure leading to smaller or larger pore sizes due to the adsorbed NM or the MIL-53 material degrades during the NM treatment. First tests with other commercial MOFs (ZIF-8 and HKUST-1) didn't show the before mentioned phenomenon.

3.4 Layered MIPs synthesized on QCMs and Kelvin probes

During the BMBF financed project NanoGasFET we intensified the development of new spin-coating based MIP synthesis conditions and MIP mixture. As sensor platforms gold coated QCMs and gold coated Kelvin probes were studied for the development of TNT and DMNB selective MIP coatings. The Kelvin probe setup was provided by Siemens, one partner of the BMBF financed NanoGasFET consortium. Best functioning MIP layers were afterwards also produced on SG-FETs, which were tested at Siemens. While QCMs lower their frequency proportionally to the mass load the sensor takes up, field effect transistors alter the work function read out if they adsorb a target (ΔU in mV). Moreover Kelvin substrates serve as test moduls for capacitive suspended gate field effect transistors, SG-FETs.

For an enhanced adhesion of the MIP layers on the gold surfaces the sensors were best pretreated with pentene thiol. The later MIP synthesis was best using Irgacure 819 as UV-starter and diglyme as porogen solvent together with TRIM (trimethylolpropane triacrylate) instead of EGDMA as the cross linker. As needed for the use in SG-FETs layer thicknesses were achieved scalable in the range of some hundred nanometers.

In case of DMNB the existing home made gas generator was upgraded with the option to alter the gas concentration used for sensor tests. Actually the concentration can be reproducibly varied between 6,92 ppm and 290 ppb. Furthermore a commercial water humidity gas generator was newly operated as well as gas generators for acetone and ethanol which were based on bubble flasks with mass flow controllers to study the

influence of potentially interfering substances. The Kelvin probe was installed into the GC oven of the gas generator.

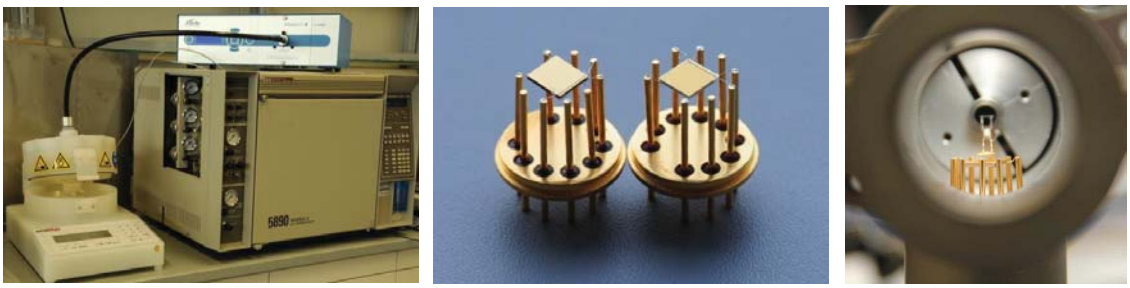


Fig. 8 Spin-coated with UV lamp and homemade vaporisation plant (left), in the middle two Kelvin probes, left without and right MIP coated and right phot shows a fully equipped Kelvin probe

Adsorption tests with DMNB and TNT showed enhanced adsorption for imprinted MIP layers compared to non-imprinted NIP layers with nearly no cross sensitivity to the second target compound. QCM based results in any case showed the same trends as the Kelvin probe measurements. As shown in table 1 MAAM showed the highest work function read out and ng-uptakes for TNT. In case of low DMNB concentration MAAM showed the highest rise in work function read out meaning highest sensitivity in time. Looking at the linearity of the measured work function read out values over increasing DMNB concentration MAA showed the best linearity making it the best suited MIP layer material for a later FET sensor. Interference tests with acetone and ethanol showed low influence while 4 % rel. humidity showed enhanced interference to the read out values. This might be compensated for in a real SG-FET sensor by appropriate measures.

Monomer	Kelvin-test [mV]	QCM TNT-uptake in ng
MAA	5	35
AA	6	24
MAAM	13	44

Tab. 1 Measured effect values for different MIP coatings on Kelvin probes and QCMs for TNT

Results e.g. achieved for TNT-imprinted Kelvin substrates show that current layered MIPs may be used as selective sensing layers in SG-FETs. Currently 10 ppb of TNT or lower are detected with low cross sensitivity to interfering substances [3].

REFERENCES

[1] G. Bunte, J.Hürttlen, H. Pontius, K. Hartlieb, H. Krause, *Gas phase detection of explosives such as 2,4,6-trinitrotoluene by molecularly imprinted polymers*, Analytica Chimica Acta 591 (2007) 49-56

[2] G. Bunte, J. Hürttlen, J. Deimling, G. Wolf, H. Kröber, M. Heil, H. Krause, *Substance selective molecularly imprinted adsorber materials for the rapid and sensitive detection of explosives vapour traces*, Proc. CD of 2nd European Conference on Detection of Explosives (2nd EUCDE), March 13, 2013 - March 15, 2013, Rome, Italy

[3] J. Hürttlen, G. Bunte, M. Heil, B. Hörr, A. Hirt, H. Krause, P. Jeanty, R. Pohle, S. Stegmeier, M. Fleischer, *Selective Layers based on Molecularly Imprinted Polymers for Work Function Readout,* Proc. CD of 2nd European Conference on Detection of Explosives (2nd EUCDE), March 13 - 15, 2013, Rome, Italy

[4] M. Heil, J. Hürttlen, G. Bunte, H. Krause, *Microwave heated beads as selective adsorbents for large volume sampling*, 45th Intern. Annual Conference: Energetic Materials – Particles, Processing, Applications, 24.-27. June 2014, Karlsruhe

[5] M. Rieger, M. Heil, Th. Altenburg, J. Hürttlen, F. Schnürer, G. Bunte, H. Krause, *Metal organic frameworks as selective preconcentrator materials for gas phase sensing*, Future Security – 8th Security Research Conference, Berlin, Sept.17 – 19, 2013

[6] W. F. Baitinger, P. R. Schleyer, T. Murty, L. Robinson, Tetrahedron, 1964, 20,1635-1637

LOCALISATION OF IED MANUFACTURING FACILITIES BY DETECTION OF EXPLOSIVES IN SEWAGE WATER

F. Schnürer[1], M. Heil, M. Rieger, A. Eberhardt, J. Aniol, H. Krause

[1] *frank.schnuerer@ict.fraunhofer.de*
Fraunhofer Institute for Chemical Technology ICT,
Joseph-von-Fraunhofer-Str. 7, 76327 Pfinztal (Germany)

Abstract

The objective of the EU-FP7 project EMPHASIS (Explosive Material Production (Hidden) Agile Search and Intelligence System) was to develop a system for detecting ongoing illicit production of explosives and improvised explosive devices (IEDs) in urban areas. The project started in 2011 and was finished in 2015.

The EMPHASIS system is composed of several different networked sensors. Strategically positioned area sensors, monitoring the vapour phase as well as static sensors, positioned in the sewer, monitoring the sewage for traces of explosives were used. Information from all sensors is transferred to and assessed in a command centre. Air and water monitoring sensors allow the narrowing of the area to be searched. Mobile sensors are then used to pinpoint the exact location of the bomb factory.

The consortium consisted of eight partners, research institutes (FOI, Fraunhofer ICT and IAF, TNO), industry (Morpho), SMEs (VIGO, Cascade) and an end user (Institut National de Police Scientifique).

This paper presents final results concerning the detection performance of the sensors in the sewer system.

Explosives, precursors to explosives and compounds from pyrotechnics can be disposed through the drain in the manufacturing of IEDs. Most of these compounds are present as ions when dissolved in (sewage) water leading to changes of the pH and the conductivity of the water.

Within EMPHASIS we analysed these properties with ion selective electrodes (ISEs). An ISE is a sensor which converts the activity of a specific ion dissolved in a solution into an electrical potential which can be measured by a voltmeter or pH meter. In EMPHASIS we used a bunch of ISEs with different selectivities in order to facilitate the detection of a variety of compounds.

This application was a new analytical challenge for these sensors. Related applications are known from research tasks such as tap water monitoring, analysis of contaminants of ground water and detection of sea mines by explosive traces. The established sensor techniques were applied in a new manner due to the complex matrix of sewage. The processing of this data with this highly variable background was a major challenge within in this project.

Furthermore, realistic simulations with CFD (computational fluid dynamics) were performed to determine realistic velocities of flow, concentrations, dispersion and expansion of threat substances in sewage.

INTRODUCTION

With just a few tools and easily accessible materials, such as chemical fertilizer, terrorists can manufacture bombs relatively easily, and it is not always possible for security forces to track down illicit workshops and thus prevent terrorist attacks. However, manufacturing a bomb leaves traces: Traces of the substances used adhere to door handles, while waste products enter the sewage system or are released via exhaust ducts.

The detection of IEDs in early stages faces several problems: One major difficulty is the broad variance of explosives and mixtures that can be used in terroristic attacks. Without knowledge concerning the type of explosive (or the presence of an explosive at all) it is very difficult to choose the appropriate detection method. While peroxides can be detected in the vapour phase, inorganic materials are hard to detect due to their low vapour pressure. Inorganic salts however can be seen in sewage and both – inorganic oxidizers as well as organic explosives – remain as trace residues on surfaces but are very hard to spot if not known where to look for. Furthermore, in large cities area surveillance is needed to get a starting point in order to pinpoint the specific location in which the IED is manufactured.

As yet no commercially-available technology can uncover illegal bomb manufacturing systematically and far enough in advance

CONCEPT OF EMPHASIS

The EU-funded project "EMPHASIS" has developed a sensor network which can detect such activities at an early stage and determine their precise location.

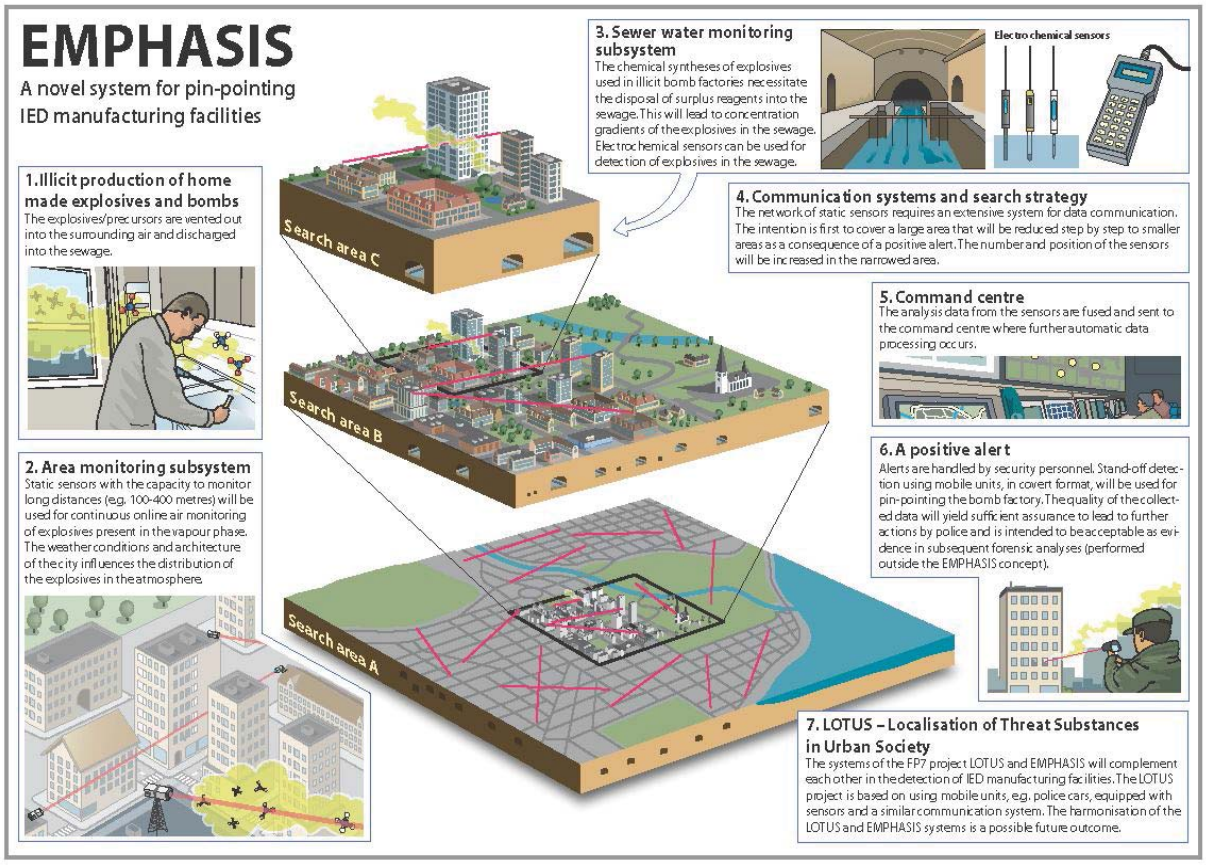


Fig. 1: EMPHASIS: A novel system for pin-pointing IED manufacturing facilities

To minimize the false alarm rate, different kinds of sensor technologies are used for the early and precise localization of illicit bomb manufacturing. The sensors are positioned in various locations, such as the roofs of high-rise buildings or in sewage ducts, depending on the respective technology, for the early detection of waste products released during the production of explosive charges and bombs. At the operating center, data from each sensor is collected and automatically evaluated. By this method a large area can be monitored by using different kinds of sensors, thus increasing the reliability of the entire system. When suspicious substances are detected, the system triggers an alarm. Using laser-based measurement technologies, the security forces can accurately localize the bomb manufacturing workshop from a distance.

While the stationary sensors for air and sewage and the mobile surface trace detection sensors are part of the EMPHASIS project, the mobile sensors from LOTUS can be used and linked up to the EMPHASIS network adding their mobile detection capability. LOTUS (www.lotusfp7.eu) was an EU project in which independent mobile sensors for cars was developed. These sensors are transmitting their data to the EMPHASIS command centre as well, completing the picture.

DETECTION SYSTEMS

The monitoring system consists of optical sensors covering larger areas mainly focussing on vapour traces. The techniques used are resonant Raman-scattering and IR-absorption respectively.

The resonant Raman-scattering uses laser light in the visible range (about 532nm) to get characteristic fingerprints in terms of a Stokes-shift. The Raman system developed by FOI can be capable of detecting vapour traces of explosives over distances up to several meters.

The IR-absorption sensor is provided by Cascade Technologies. The sensor is based on a tuneable QCL that conducts open-path measurements with a retro reflector.

Surface trace detection is also laser based using either IR backscattering or imaging Raman.

Imaging Raman is also provided by FOI, using lasers in the visible or UV-range to detect traces or bulks of explosive solids and liquids.

Fraunhofer IAF is responsible for IR backscattering sensors with quantum cascade lasers with a very high tuneable range up to 300 wavenumbers. By scanning over a large spectral area, sensitivity becomes greatly enhanced due to more accessible spectral features. Therefore it is possible to differentiate between different explosives and benign traces such as powders or pharmaceuticals. The use of an optical setup with a telescope enables the system to analyse over ranges up to 25m.

The sewage sensor system developed by Fraunhofer ICT combines several ion-selective as well as other electrodes to get a broad basis for data processing, thus enabling the system to create patterns to recognize traces of suspicious materials even in complex matrices such as sewage.

DETECTION OF EXPLOSIVES IN SEWAGE WATER

CFD modeling of the dispersion of solutes in sewage

To determine realistic velocities of flow, concentrations, dispersion and expansion of threat substances in sewage simulations with computational fluid dynamics (CFD) have been performed.

The calculations performed showed that CFD methods are applicable to produce quantitative results for downstream concentration profiles in sewage systems which allow conclusions on

relevant concentration ranges and on the spatial proximity of the discharge inflow point (high concentration reduction rate = inflow nearby).

In order to produce both quantitative and qualitative information further data are needed, e.g. exact channel geometry and type and amount of discharged solutes. Real effects like varying channel geometry due to deposits and inhomogeneous fluids have to be implemented by experimental validation.

The CFD calculations were able to provide realistic flow concentration profiles needed for the setup electrochemical sensor system architecture.

Electrochemical sensor system architecture

Ion selective electrodes are very sophisticated analytical techniques used in today's water trace analysis. However, in order to get best results it is necessary to prepare samples. This approach is unsuitable for long-term real-time monitoring of sewage water. Therefore statistical methods were developed to avoid complicated and time consuming recalibration of the electrodes.

The sewage monitoring subsystem consists of seven different ion-selective electrodes and a conductivity sensor.

These sensors feed their data to a read-out unit that provides the operator with the actual reading of each sensor. Since one ion-selective electrode, due to cross-interfering ions, is not able to certainly detect the substance it should be selective for, other electrodes are needed to create diversification.

The conductivity sensor detects changes of the conductivity of the waste water and therefore in its composition regarding ionic compounds such as salts and works as a trigger electrode. If a trigger signal is received an algorithm will analyse the signal of the different ion-selective electrodes at the corresponding time. Data analyses were performed with the software origin by OriginLab Corporation.

The electrodes translate a concentration gradient of specific ions between the waste water and an internal reference solution into a voltage which is recorded and sent to a computer. These voltage-signals are analysed in the computer and the signals of all electrodes create a pattern. Specific ions result in specific patterns which are used to perform pattern recognition to discriminate compounds of interest from those of common use.

Different backgrounds

The different substances have been tested in three major classes of background: de-ionised water, drinking water and artificial sewage water, the latter subsequently divided in two different "recipes". In order to gain first experience only de-ionised water has been used, followed by drinking water and finally sewage water in the evaluations. The results have shown not to be comparable to other backgrounds since the influence of the background is much stronger than anticipated. We also used two different artificial sewage waters as backgrounds. These artificial sewage waters contain mainly salts (such as e.g. $CaCl_2$) present in common sewage water within their allowed concentration range. One has been derived from German thresholds for sewage water (labelled ICT), the other refers to a DIN (German Institute of Standardisation) guideline. The main difference is the presence of peptone and whey in the DIN sewage water in order to simulate organic components. The result of this change in composition is a very strong change in detection capability (Fig. 2: Signal response for different substances depending on the sewage water composition). While the first background (black squares, labelled as ICT) responds to seven substances (all except #4), the second (red dots, labelled as DIN) containing peptone and whey responds only to two substances (6 and 7).

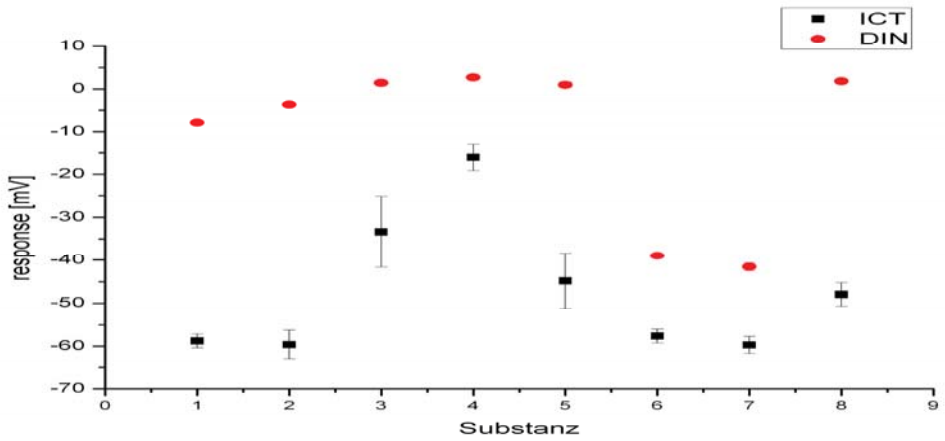


Fig. 2: Signal response for different substances depending on the sewage water composition (ICT, artificial sewage; DIN standard, artificial sewage).

Long term behaviour

In order to evaluate the long term stability of the electrodes a 500 hour measurements in a one single sample has been performed. The sample has been protected against excessive solvent evaporation leading to higher concentrations and the electrodes have been immersed all the time. However it is not possible to prevent evaporation completely which result in an increasing conductivity over time.
While a radical change of the sample is visible (Fig. 3: Electrodes in sewage after 240 hours (10 days)), this does not reflect the sensor readings to any significant amounts.

Fig. 3: Electrodes in sewage after 240 hours (10 days).

Concepts for hardening electrochemical sensors for sewer water applications

The influence of composition on sensor reading has already been mentioned. The relative stability of the readings regarding the macroscopic pollution of the sensors shows that there should be no immediate problem with electrode contamination. Nevertheless it must be considered that depositions on the electrodes can hinder or prevent diffusion to the electrode resulting in a decreased detection performance. Long-time storage and corresponding contamination do not substantially change detection capability, but if cleaning intervals are chosen too large it might be difficult to achieve complete cleaning in one cleaning cycle. We decided to use one cleaning cycle a week. The cleaning cycle must include a physical cleaning to remove all surface contamination.

Detection performance

The last step in the project was the trials at FOI test site in Sweden. The system was installed in a real world sewer system running autonomously. Environmental conditions were rain and heavy wind, so rain water and organic material such as leaves were brought into the sewer system.

Fig. 3: Test measurements in a sewage system.

During these trials different substances (e.g. NaCl) have been tested in different dilutions and amounts as well as different forms of applications (e.g. dissolving the substance in water with subsequent pouring into the sewer, spilling solid material into the sink with following slow dissolving by background water flow). We checked the detection of nitrates in general, discriminating between ammonium and potassium nitrate. This can be extended to other nitrates with possible non-identification of cations. Chlorates and perchlorates are possible too, since at least one electrode shows significant reaction to these ions. Benign substances can also be identified or neglected from our experience. We chose sodium chloride as the most common benign substance and were able to identify it without interference.
During the demonstration all test-substances could be easily detected and identified by electrode response electrode response.

Sewer system conclusions

Through the combination of various ISEs and the use of pattern detection analysis the most significant challenges have been solved, namely compensation for the changing background and the presence of interfering ions. Another challenge was the influence of long submersion times and lack of cleaning on the measurement performance of the ISEs. Despite significant contamination of the ISEs the measurements proved to be consistent over a period of several weeks, meaning that pattern recognition was still possible.
We have developed a setup for housing the electrodes and their readout devices in the sewer and established communication and data processing with the command centre using a router. Lab tests as well as field trials show the feasibility of detecting and identifying different substances over distances of at least 50 metres. Time resolution and sensitivity is sufficient to detect small amounts of suspicious materials. The method however has to be optimized to deal with lower threat quantities within changing compositions of real sewage.

CONCLUSIONS

The EMPHASIS project started in October 2011 and was finished in January 2015. At the end of September 2014, the suitability of the developed sensor network was demonstrated successfully at the testing grounds of the FOI (Swedish Defence Research Agency) near Grindsjön in Sweden.
The project demonstration showed that it is possible to detect precursors to explosives in scenarios relating to the illicit manufacturing of home-made explosives and IEDs. The developed system prototype represents today a backbone where further specific techniques that could be useful in other scenarios can be added on. This could then enhance the present capabilities.

ACKNOWLEDGEMENT

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No 261381.
EMPHASIS is a collaboration between:
FOI, TNO, Fraunhofer ICT, Fraunhofer IAF, Cascade Technologies, MORPHO, Institut National de Police Scientifique and VIGO.

STANDOFF TRACE DETECTION OF EXPLOSIVES WITH ACTIVE INFRARED HYPERSPECTRAL IMAGERY

F. Fuchs[1], S. Hugger, J.-P. Jarvis, Q. K. Yang, R. Ostendorf, Ch. Schilling, W. Bronner, R. Driad, R. Aidam, J. Wagner

[1] *frank.fuchs@iaf.fraunhofer.de*
Fraunhofer Institute for Applied Solid State Physics (IAF), Tullastrasse 72, 79108 Freiburg, (Germany)

Abstract

Broadband tunable external cavity quantum cascade lasers (EC-QCL) have emerged as attractive light sources for mid-infrared (MIR) “finger print” molecular spectroscopy for e.g. detection and identification of hazardous chemical compounds. The technique relies on active imaging with MIR laser illumination at various wavelengths while recording the diffusely backscattered radiation. Using a MIR EC-QCL with a tuning range from 7.5 µm to 9.5 µm, different explosives such as TNT, PETN and RDX residing on different background materials, such as painted metal sheets, cloth and polyamide, could be clearly detected and identified. For short stand-off detection distances (<3 m), residues of explosives at an amount of just a few 10 µg, i.e. traces corresponding to a single fingerprint, could be detected. For larger concentration of explosives, stand-off detection over distances of up to 20 m is feasible in real world conditions.

Keywords: Standoff detection, explosives, remote sensing, tunable infrared laser, quantum cascade laser, external cavity laser, hyperspectral image analysis.

1 INTRODUCTON

Broadband tunable external cavity quantum cascade lasers (EC-QCL) have emerged as attractive light sources for mid-infrared (MIR) “finger print” molecular spectroscopy for e.g. detection and identification of hazardous chemical compounds[1,2]. Compared to Fourier Transform Infrared (FTIR) spectrometers EC-QCL offer the advantage of a much higher spectral brightness, i.e. high output power within a narrow wavelength interval, as well as a collimated low-divergence output beam, enabling e.g. stand-off detection schemes.

Reliable stand-off detection of residues of explosives is still a challenging task[3,4,5]. Imaging MIR backscattering spectroscopy has been shown to be a promising technique for contactless detection of traces of explosives on various surfaces[6,7]. This technique relies on active imaging with MIR laser illumination at various wavelengths. Recording the backscattered light with a MIR camera at each illumination wavelength, the MIR backscattering spectrum can be extracted from the three-dimensional data set recorded for each point within the laser illuminated area. By applying appropriate image analysis algorithms to this hyper-spectral data set, chemically sensitive and selective images of the surface of almost any object can be generated. This way, residues of explosives can be clearly identified on the basis of characteristic finger print backscattering spectra and separated from the corresponding spectra of the underlying material. To achieve a high selectivity, a large spectral coverage is a key requirement. Using a MIR EC-QCL with a tuning range from 7.5 µm to 9.5 µm, different explosives such as TNT, PETN and RDX residing on different background materials, such as painted metal sheets, cloth and polyamide, could be clearly detected and identified. Very important for the practical use is the fact, that IR backscattering is eye-safe[7].

In the following sections the principle of operation is outlined. We discuss our understanding of backscattering signatures and the effect of polarization sensitive measurements. The technical setup of our system is very similar to the thermal resonant heating method[8]. However, we restrict ourselves in this report on measurements of backscattered laser radiation only. The system is described and results of outdoor trials are reported. We demonstrate that such capabilities can be used to detect illicit fabrication sites for the production of explosives and improvised explosive devices (IEDs). These trials were carried out as part of the FP7 projects EMPHASIS[9] and HYPERION[10] funded by the European Commission. These results clearly demonstrate the potential of QCL-based imaging backscattering spectroscopy for the detection of trace amounts of hazardous substances in relevant environments. There is further potential for increasing the detection range and/or field of view via up-scaling of the total power emitted by the illuminating laser system

2 INFRARED BACKSCATTERING SPECTROSCOPY

2.1 Principle of operation

In Figure 1 the basic measurement geometry is depicted. The laser radiation from a tunable laser source is directed to the object under investigation. The spot size of the laser is around 3 x 3 cm^2 and its wavelength can be tuned. This way an infrared measurement of the reflectance of the surface is realized for an arbitrary orientation. The diffusely backscattered laser light is collected with an infrared imager. The image recording is synchronized with the tuning of the laser. This process yields an image cube, where each image is associated to a specific illumination wavelength. This data cube is in the following referred to as '*hyperspectral image'.* The wavelength of the laser source is tuned in the range of the most significant spectral signatures. Spectroscopy in this "fingerprint" region enables identification of almost all chemical compounds composed by organic functional groups. The laser source of our standoff setup is able to scan across about 300 wavenumbers. We will show later that this feature in combination with active imaging enables identification of almost all explosives deposited on unknown surfaces.

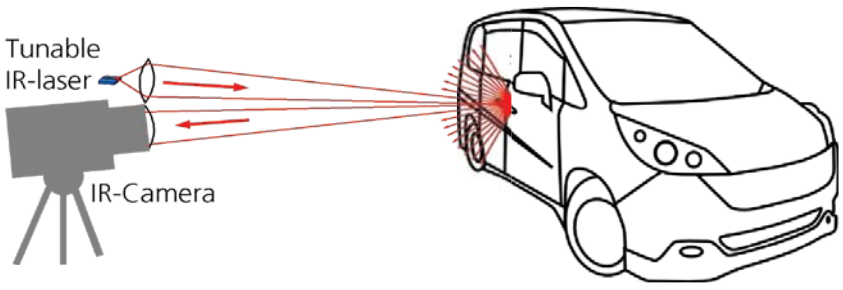


Figure 1 Principle of operation. The laser radiation from a tunable laser source is directed to the object under investigation. The wavelength of the laser can be tuned. The diffusely backscattered laser light is used for hyperspectral data analysis.

2.2 Spectral signatures and polarization dependence

Many real world samples show an angular dependent total backscattering intensity, which indicate, that the main contribution of the backscattering signal can be described in the framework of Mie scattering[3]. Many man-made objects have a surface showing a surprisingly high reflectivity for infrared radiation around a wavelength of 10 µm. If the target material is deposited on such a surface we typically observe a scattering behavior which can be quite well described by Mie theory[3]. Particles on a mirror-like surface behave similarly to a dielectric sphere (Mie scatterer), while the surface itself acts simply as a mirror, leading to an enhancement of the backscattering intensity.

In this section we show results on the polarization dependence of the back scattered signal. The laser radiation of the external cavity quantum cascade laser (EC-QCL) is directed close to normal incidence onto a scattering plate contaminated by traces of explosives. The diffusely backscattered light is collected by a teleoptics and focused on an infrared detector. A polarization filter is placed in front of the IR-detector. The backscattered radiation is then analyzed for different orientations of the polarizer. We define a polarization contrast by dividing the difference of the polarized components by the sum:

$$(p_{\parallel} - p_{\perp}) / (p_{\parallel} + p_{\perp})$$

Typical spectra of the polarization contrast (red) and the unpolarized backscattering intensity (blue) are shown below in Figure 2. Strong polarization effects are observed for all investigated samples. In Figure 2 we present measurements on four different materials (FOX7, TNT, PETN, RDX) deposited on painted car plate. Although the deposited concentration of the target material was only small, the effect of the depolarization is very strong.

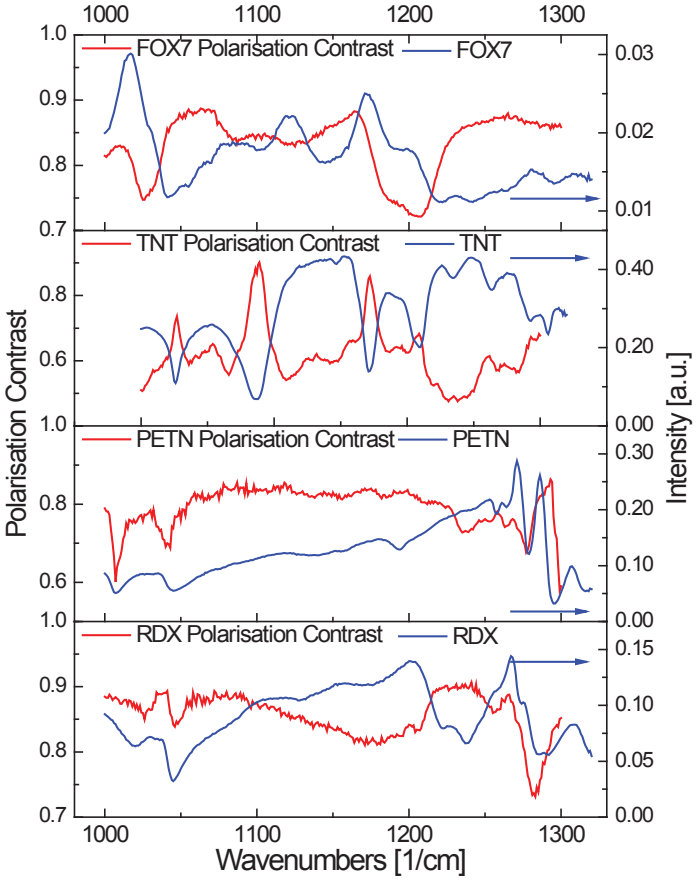


Figure 2 Polarization contrast (left scale, red) and unpolarized backscattering (right scale, blue) of traces of FOX7, TNT, PETN, RDX, deposited on painted car plate

A polarization contrast of typically around 30 % is found. We note, that the total signal level in the depolarized component $p_{\perp}$ is much weaker compared to the parallel component $p_{||}$ or the unpolarized measurement, respectively. This type of measurement is only possible for large backscattering signal levels. In the case of low scattering signal levels the depolarized component $p_{\perp}$ is obscured by other noise sources.

In the framework of Mie scattering theory for the signal scattered into forward as well as in backward direction no change of the polarization is expected. We explain the strong polarization dependence by multiple scattering of the laser radiation at the sample surface. With a certain density of particles on the target material the laser radiation undergoes multiple scattering, leading to the observed polarization effects. This interpretation could be experimentally confirmed by changing the direction of the incident laser beam to grazing incidence. Looking with that geometry, again we observe strong polarization effects.

In summary, for a scene where a high backscattering intensity is available, the polarization contrast can provide larger spectral signal modulation which leads to better detection sensitivity for material identification. If the signal strength becomes very weak - which is typically the case for large detection distances - the depolarization component is obscured by other noise sources. For this case, the conventional technique using the unpolarized backscattering spectrum yields the better result.

3 HYPERSPECTRAL IMAGE SENSOR AND DETECTION SYSTEM

3.1 The Hyperspectral Image Sensor

The imaging MIR backscattering spectroscopy system used in field trials for the detection of explosives as well as of precursors used for the fabrication of explosives is shown in Figure 3. The system consists of an EC-QCL based laser illumination unit[11], a large aperture optical telescope coupled to a high-performance cryogenically cooled MIR camera for collecting and detecting the diffusively backscattered MIR laser radiation, as well as a control and data processing unit. Co-linear with the MIR telescope also the visible image of the scene under investigation is recorded.

The IR camera offers a format of 384 x 288 pixels. For the measurements we used a subframe of 192 x 192 pixels and a frame rate of 388 Hz. Cutoff wavelength is 10.5 µm. The teleoptics operates with an entrance aperture of 12.5” diameter and f-number of ~ 3 with small field of view. A camera for the visible spectral range provides an image of the scene with larger field of view. The IR-detection image can be overlaid to the visible scene image. (see Figs. 6 and 7). System control is performed with a laptop. The complete electronics has been placed in a moveable and protected case for field test operation (Figure 3).

The laser illumination unit contains two EC-QCL modules equipped with QCL chips providing different, but overlapping tuning ranges. The output beams of the two EC-QCL modules were combined via a custom made dichroitic mirror. This way, a large overall wavelength span ranging from 7.36 µm to 10.14 µm (as defined by the full width at half maximum of the output power-vs.-wavelength tuning characteristic) is covered, corresponding to a total possible tuning range of 370 cm^{-1}. For the below experiments, the illumination wavelength was scanned between 7.63 µm (1310 cm^{-1}) and 10 µm (1000 cm^{-1}).

Figure 3 Stand-off detection system based on active imaging MIR backscattering spectroscopy ready for field tests in Grindsjön (FOI, Sweden).

The large telescope optics is required for measurements at distances from 10 m to 20 m. Laser and camera are operated synchronously, so that every second image the camera takes, the laser is switched off. The thermal image background can then be eliminated by subtracting two adjacent images from each other. By tuning the laser, over time, the system yields a stack of difference images, each associated to a specific illumination wavelength. This stack forms a hyperspectral image. Typical illumination areas at measurement distances of 20 m are around 10 cm^2.

3.2 Signal processing of imaging IR backscattering spectroscopy

Custom-made data analysis software allows to search for a defined set of substances with known backscattering spectra, while a-priori-knowledge of the background material is not required[12,13]. The target detection system's processing flow is shown in Figure 4. Target spectra and image data are combined to estimate the virtual dimension. In a two-step process, first, the background subspace is estimated. In the second step the target detection is applied. After application of threshold values the result is given as a detection image. The identified target material and other detection parameters and the image of the scene can be transferred to a central command center using a standardized protocol.

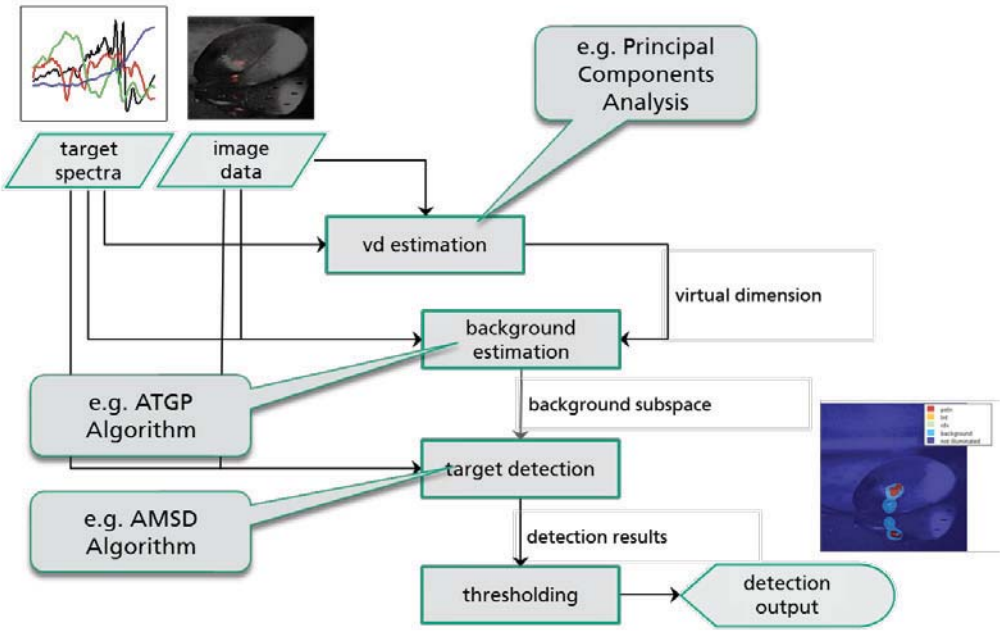


Figure 4 Scheme of the processing flow of the hyperspectral data.

4 RESULTS OF OUTDOOR MEASUREMENTS ON TRACE DETECTION

In the framework of the EU FP7 projects BONAS and EMPHASIS a demonstration campaign has been conducted during September 2014 at FOI test site in Sweden. Figure 3 shows the standoff setup during the demonstration campaign. Figure 5 shows the actual setting used in the outdoor field trial. The suspect car was parked at a distance of 13 m from the detection system. Residues of various precursor materials used for the production of explosives were placed at different locations at the outside and the interior of the car. During the campaign weather conditions lead to a humidity close to 100 % and most of the time medium to heavy rain fall.

Figure 5 MIR backscattering stand-off detection system pointing at suspect car parked at a distance of 13 m.

As a typical result, Figure 6 shows the chemically selective image of such a deliberately contaminated area, obtained via MIR backscattering spectroscopy, overlaid to the visible image. The time required for acquiring the full spectral set of MIR images was 30 s. The presence of residues of DNT located on the left rear tire of the car is unambiguously identified, in spite of the adverse weather conditions. These results clearly demonstrate the capability of EC-QCL based imaging MIR backscattering spectroscopy for detection of hazardous substances in relevant outdoor scenarios.

In the framework of the EU FP7 project HYPERION samples from a test explosion performed at the test site of FOI have been investigated with the present standoff IR system. For the test explosion Ammonium Nitride (AN) was used as dominant part of home-made explosives. Several test plates have been placed in the vicinity of the explosion center. Results are shown in Figure 7. It clearly shows the

spots of residues of AN, which did not fully react during the explosion. Detection distance of the measurement was 13 m. From these preliminary results we conclude, that for a post-blast scenario the standoff technique has the potential to determine the chemical composition of the explosive which has been used.

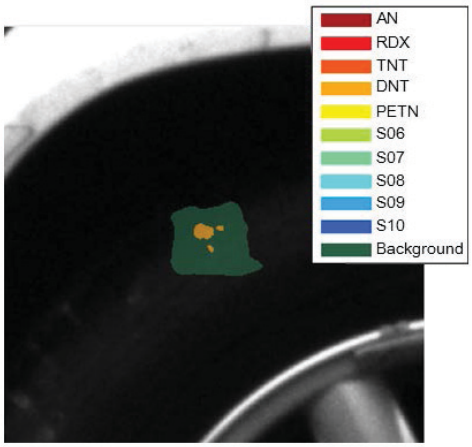


Figure 6 Traces of DNT, a precursor of TNT, detected by imaging MIR backscattering on the left rear tire of car parked 13 m away. The stand-off detection setup used is shown above in Figure 5.

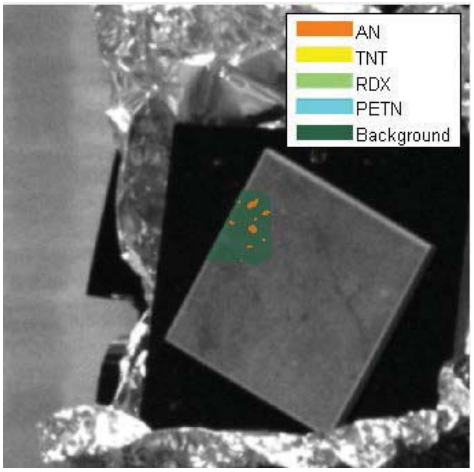


Figure 7 Substance detection map overlaid over visual image of a ceramic test plate. Several high confidence positive detections of AN traces were generated, while no false alarms occurred for competing substances.

5 SUMMARY AND OUTLOOK

Progress on infrared laser based standoff detection has been reported. The spectroscopy system comprises a tunable Quantum Cascade Laser (QCL) for active illumination and a high performance MCT camera for collecting the backscattered light. Spectral backscattering signatures for polarization sensitive detection have been investigated. The variation of the spectral signatures of the target materials under real world conditions has been investigated. The functionality of the eye-safe detection system has been validated outdoors in a relevant scenario. Trace detection of a large variety of explosive materials could be demonstrated. First measurements indicate potential for post-blast scenarios.

ACKNOWLEDGEMENTS

The results have been obtained within the collaborative projects IRLDEX, funded by the German Federal Ministry of Education and Research (contract number FKZ 13N4543), and the EU FP7 projects EMPHASIS[9] and HYPERION[10] (grant agreement numbers 261381 and 284585). We acknowledge the cooperation of H. Önnerud and H. Östmark from FOI in Sweden during these project activities. We acknowledge the work on polarization sensitive measurements of F. Zaum and thank K. Schwarz, U. Weinberg, and S. Liu for expert technical assistance.

REFERENCES

[1] Capasso, F., “High-performance midinfrared quantum cascade lasers,” Optical Engineering **49** (November), 111102 (2010).

[2] Faist, J., Quantum Cascade Lasers, University, Oxford University Press, Oxford (2013).

[3] Furstenberg, R., Kendziora, C., Papantonakis, M., Nguyen, V.., Andrew, R., “The challenge of changing signatures in infrared stand-off detection of trace explosives” Proc. SPIE **9073**, 90730M–1 (2014).

[4] Nordberg, M., Ceco, E., Wallin, S.., Östmark, H., “Detection limit of imaging Raman spectroscopy” SPIE Defense, Security, and Sensing, J. T. Broach and J. H. Holloway, Eds., 83571H, International Society for Optics and Photonics (2012).

[5] Moros, J., Lorenzo, J. a.., Laserna, J. J., “Standoff detection of explosives: Critical comparison for ensuing options on Raman spectroscopy-LIBS sensor fusion” Analytical and Bioanalytical Chemistry **400**, 3353–3365 (2011).

[6] Fuchs, F., Hugger, S., Kinzer, M., Aidam, R., Bronner, W., Lösch, R., Yang, Q., Degreif, K.., Schnürer, F., “Imaging standoff detection of explosives using widely tunable midinfrared quantum cascade lasers” Optical Engineering **49**(November), 111127 (2010).

[7] Fuchs, F., Hugger, S., Yang, Q., Jarvis, J.., Kinzer, M., Broadband-Tunable External-Cavity Quantum Cascade Lasers for Spectroscopy and Standoff Detection, Press Book, SPIE **PM238**, Press Book, M. Razeghi, L. Esaki, and K. von Klitzing, Eds., 645, WA, Bellingham (2013).

[8] Furstenberg, R., Kendziora, C. A., Stepnowski, J., Stepnowski, S. V., Rake, M., Papantonakis, M. R., Nguyen, V., Hubler, G. K.., McGill, R. A., “Stand-off detection of trace explosives via resonant infrared photothermal imaging” Applied Physics Letters **93** (22), 224103, AIP Publishing (2008).

[9] “http://www.foi.se/en/Customer--Partners/Projects/EMPHASIS/”.

[10] “http://www.foi.se/en/Customer--Partners/Projects/HYPERION/”.

[11] Wagner, J., Ostendorf, R., Grahmann, J., Merten, A., Hugger, S., Jarvis, J.-P., Fuchs, F., Boskovic, D.., Schenk, H., “Widely tunable quantum cascade lasers for spectroscopic sensing” SPIE **9370**, 937012 (2015).

[12] Jarvis, J., Fuchs, F., Hugger, S., Blattmann, V., Yang, Q., Ostendorf, R., Bronner, W., Driad, R., Aidam, R., et al., “Trace detection of explosive substances in hyperspectral imagery” Proc. 9th Security Research Conference Future Security, 241–247, Fraunhofer Verlag (2014).

[13] Jarvis, J., Fuchs, F., Hugger, S., Blattman, V., Yang, Q. K., Ostendorf, R., Bronner, W., Driad, R., Aidam, R., et al., “Hyperspectral Image Analysis for Standoff Detection of Explosives” Proceedings of the 8th Security Research Conference Future Security, M. Lauster, Ed., 205–214, Stuttgart: Fraunhofer Verlag, 2013, 505 pp, Berlin (2013).

UBICITY – CONQUERING CRISIS AND DISASTER MANAGEMENT CHALLENGES WITH BIG DATA ANALYTICS

Jasmin Pielorz, Christoph Ruggenthaler, Hermann Huber, Andrea Nowak

{firstname}.{lastname}@ait.ac.at
AIT Austrian Institute of Technology, Digital Safety and Security Department,
Donau-City-Straße 1, 1220 Vienna, Austria

Abstract

The growing community of users that are using their mobile devices to access the internet and share information are generating an unprecedented amount of data. With the systematic collection and analysis of these data streams new insights can be gained and business opportunities unlocked. However, in order to cope with large amounts of unstructured, distributed data in near-real time, new methodologies for data management and analysis are required. In order to tackle these challenges for the domain of crisis and disaster management, we propose a new platform for fast and scalable data storage and analysis called *Ubicity*[1]. The platform aims at extracting, collecting and indexing data from various sources. With the help of integrated powerful and flexible search interfaces, users can directly interact with massive data volumes, a variety of data structures and deal with the velocity of changing content such as social media streams.

Keywords: Crisis and Disaster Management, Big Data Analytics, Scalable Technology Platform

1 INTRODUCTION

Already in the early stage of the digital revolution, experts noted that with the increase in computational power the amount of produced data would soon exceed storage capacities. But it was not before the late 90s that John Mashey – a chief scientist at Silicon Graphics – coined the term Big Data to convey that the boundaries of computing keep advancing to an extend that requires attention [1]. Since then Big Data has advanced to one of the most commonly used buzzwords and many experts have attempted to come up with a concise definition. The one most widely used is probably the famous 3Vs the experts from Gartner came up with, stating that “Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization” [2].

1.1 Big Data Challenges in Crisis and Disaster Management

These three challenges also translate to the domain of crisis and disaster management (CDM). The enormous increase in the availability of public data (social media, forums, blogs, etc.) and the trend towards connecting ever more mobile devices and consumer electronics with central platforms are resulting in a growing pool of data that is of potential interest for detecting and predicting crisis situations. However, in comparison to other domains a key challenge of Big Data analytics for crisis management is the *spatio-temporal aspect* of the data. Data streams need to be clustered and analysed according to their geolocation and observation time in order to be put into the correct context. This requires among others the correct translation of the geo-referenced data into the same geographic coordinate system,

[1] More information about the Ubicity Platform can be found at http://ubicity.ait.ac.at

as well as a measure of proximity for the different observations in space, time and space-time before clustering them, which is all part of geographic data mining [3]. An additional challenge is the *heterogeneity of the data sources* in CDM. The data can be everything, from simple text messages as e.g. provided by Twitter, over sensor data measured with mobile devices (e.g. temperature, humidity or acceleration) to satellite images in different wavelengths and resolutions. In order to make use of them for geospatial knowledge retrieval, they need to be annotated and enriched with appropriate meta-data and stored into a database that supports schema free documents and flexible querying. Finally, one has to take into account the challenge of dealing with *uncertainty in the collected data*. Depending on the type of sensor used, e.g. one that was deployed and calibrated by an expert or low cost sensors used by untrained users, the observations have a different accuracy. This becomes even more challenging when humans are providing information during crisis situations. To validate their reported observations, e.g. of a collapsed bridge, it is either necessary to have this confirmed by others or to have a concept of trust that allows the crisis manager to distinguish between experienced first responders and ad-hoc volunteers [4].

1.2 Crisis Management Tools for Situational Awareness

Current approaches to making use of the vast amounts of available (open) data for CDM are typically limited to improving situational awareness for crisis managers or the general public. This can either be done passively by social media mining of already existing services such as Twitter, Flickr or Facebook. In this case, proper tools or platforms are required that allow users to systematically monitor and store data, as well as to relate them to specific geolocations and events [5]. Alternatively, an improved understanding of a crisis event can be achieved by engaging or crowdsourcing volunteers to provide the desired information. Here, the platform takes over the role of actively requesting users to provide information about a certain event such as the recent earthquake in Nepal or the snow storms at the US east coast in the last years. Only in a next step this information is then analysed and results are visualized. Typical examples of such platforms are Ushahidi or CrisisMappers.

In this paper, we introduce the Ubicity platform, which combines the best of both worlds in one scalable software platform. On the one hand it allows crisis managers to store, process and visualise heterogeneous data flows and sources, whereas on the other hand it can be used as a powerful crowdtasking application for managing spontaneous volunteers. While Section 2 gives an overview of the architecture and the implemented technologies, we detail in Section 3 the deployed and planned data analytics and visualisation tools. Respective use cases in crisis and disaster management are discussed in Section 4, which highlight current best practice approaches and state-of-the-art methodologies based on open source technologies. Finally, this paper summarizes the achieved results and gives an outlook on future work.

2 UBICITY ACHITECTURE OVERVIEW

As highlighted above, technical and societal changes in communication and collaboration are leading to several new challenges but also revealing promising methods of providing relief during crises and disasters. Especially, the enormous increase of publicly available open and social data combined with new concepts such as crowdtasking or -sourcing enable an unprecedented potential for professional organizations. With data analytics techniques tailored to the needs of the CDM domain and new media technologies, processes in the entire crisis management life-cycle can be improved.

2.1 Ubicity's Vision and Design Approach

The Ubicity approach aims to establish a unified platform, which is able to deal with this large amount of heterogeneous and fast changing data, distributed over multiple sources. Therefore, the overall Ubicity architecture has to be designed to cope with these challenges

by providing a scalable and distributed framework to enable distributed storage and processing applied to unstructured data enriched with geospatial metadata. Especially, in the advent of highly increasing geo-tagged information fragments, aggregation and analysis have to become more and more location aware [6]. Thus, the selection of appropriate storage, evaluation and visualization components and approaches has to be extended also to suitable geo-enabled technologies. Fig. **1** depicts the vision of the Ubicity platform and outlines the intended data source categories, analytics and visualization concepts.

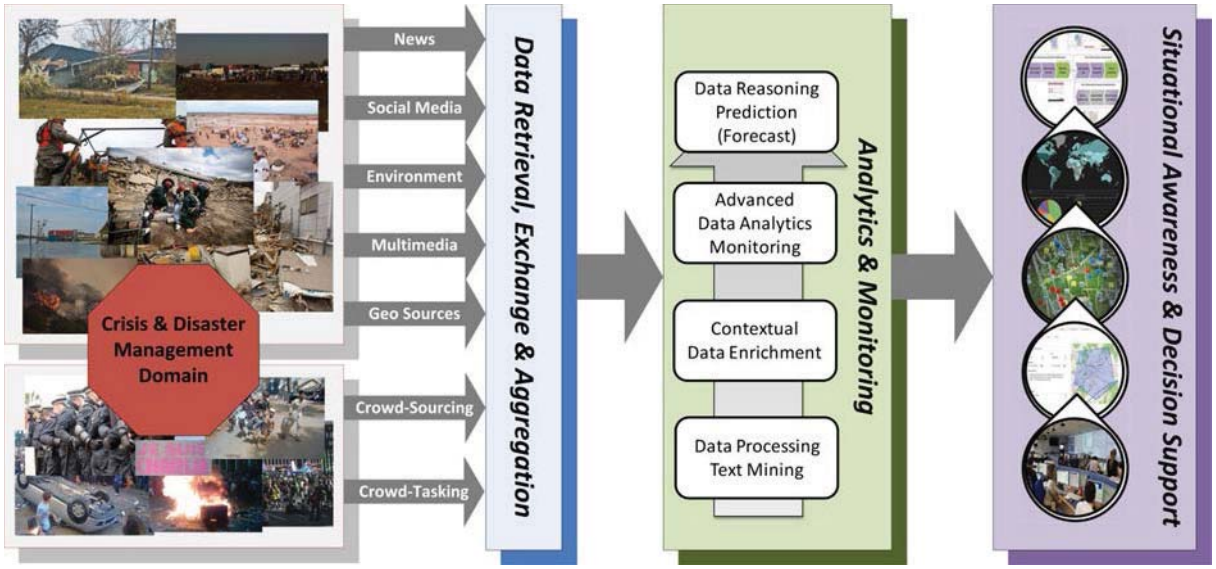


Fig. 1: Ubicity Big Picture and High-Level Architecture

Currently, Ubicity is deployed as a core component in several use and show cases within the CDM domain, where different facets of the holistic view are implemented and demonstrated separately. This approach allows the extension of the platform portfolio without the need of complex dependency management or any functional restriction of the created components.

2.2 Technical Architecture and Components

The Ubicity architecture is based on two main design principles: to support fast development of new functionality and to enable a flexible mechanism that blends various components together to a best-of-bread system.

As a consequence, the Ubicity core provides a light-weight plugin concept based on the Java Simple Plugin Framework (JSPF) to easily integrate and reuse existing components in diverse application setups [7]. Further, to enable a common information and data exchange flow between all plugins, the Event Driven Architecture (EDA) pattern is applied to all modules, where the Ubicity core encapsulates the base functionalities for publish and subscribe operations. The communication is based on de-facto standard protocols such as STOMP and WebSockets, which support a simple integration of third party and legacy systems. Moreover, the flexibility of the plugin framework enables the replacement of the internal message broker with an external ActiveMQ Apollo instance with its advanced functionality in terms of protocol support, authentication, authorization as well as scalability [8].

The data retrieval, exchange and aggregation layer handles the data ingest, pre-processing and storage functionality, where various sources such as Twitter, Flickr, Facebook or news portals are used to collect the information in real-time. To cope with the mostly schema free data and high update frequency, Ubicity uses different NoSQL backend technologies for data storage and basic aggregation as well as full text search operations. Especially to deal with

geo-enabled data from Twitter messages or GeoRSS feeds, Elasticsearch is used to store, index and search the entire data repository based on text fragments or geolocations. Elasticsearch itself supports a highly distributed and available deployment with the feature of schema free data indexing based on the JSON document format [9]. Additionally, the Couchbase Stack (Server, Sync Gateway and Mobile) is integrated in Ubicity to guarantee the flexibility to select the best storage technology for the supported use case. The document-oriented Couchbase stack facilitates efficient JSON data storage and (geospatial) search queries with added MapReduce functionality even on mobile devices [10].

Currently, the Ubicity platform is extended to support other NoSQL representatives such as graph databases. Additionally, to maintain interchangeability of the underlying storage layers, the Ubicity graph plugin uses the graph database abstraction framework Apache TinkerPop, which establishes a promising open source graph computing framework for JAVA with connector implementations for actual state-of-the-art projects such as Neo4J or TinkerGraph [11]. Moreover, the active development involves also the higher layers, i.e. analytics and visualization layers, where the main research and implementation effort is focused on efficient data processing and optimized representation of large amounts of geo-enriched data.

3 BIG DATA ANALYTICS AND VISUALISATION

The very fundamental element of every data analytics process is the presence of suitable data sets. In this regard the term suitable not only reflects validity, significance and relevance. It also alludes to technical suitability such as file formats, appropriate formatting and data structures. The first issue needs to be considered by analysts, whereas the latter can be handled easily with the support of proper data management tools. We noticed that dealing with different kinds of data requires considering various data representations that incorporate the corresponding characteristics of the considered types of data sets. Sensor data for instance is typically represented in a traditional table-based format, whereas relationships and network-like structures are usually represented as linked graphs. In order to handle the complexity of analysing large data sets from multiple sources an appropriate set of tools is required. We use Ubicity to solve exactly these kinds of problems, where the inhomogeneity of the data sets demands a high versatility. The ability to create data management plugins for arbitrary data stores enables us to solve the data representation issue. Ubicity's data routing mechanisms facilitate proper data exchange across multiple data stores. In the analytics process, proper data extraction mechanisms ensure interoperability with a variety of specialized programming languages and tool suites such as R or Python.

For basic aggregation and search queries, the built-in functionalities of the integrated NoSQL storage technologies are utilized. For instance, Elasticsearch has turned out to be one of the most important data stores. It can be used in two ways: either to directly index data in order to make it searchable for future analysis tasks or to index metadata of data sets in order to enable users to search for appropriate data sets and to retrieve corresponding volumes, formats, protocols or endpoints. Due to this, the comparison of multiple data sources and the exploration of the potential value for a specific analysis task have become much simpler than before. We also leveraged the power of Kibana, for basic visualization and monitoring of the indexed data in Elasticsearch. The web-based tool frontend offers a limited list of configurable widgets for displaying georeferenced data on maps, certain diagrams such as rings, bar charts or lists and corresponding filter mechanisms as depicted in Fig. 2. This is particularly useful for stream-based data acquisition to detect changes of the data stream properties (volume, quality, quantity, etc.) in near-real time. Amongst other applications and plugins, we also use the Kibana web interface application to visually verify that live data streams are behaving as expected and, in case they do not, to determine potential reasons for this.

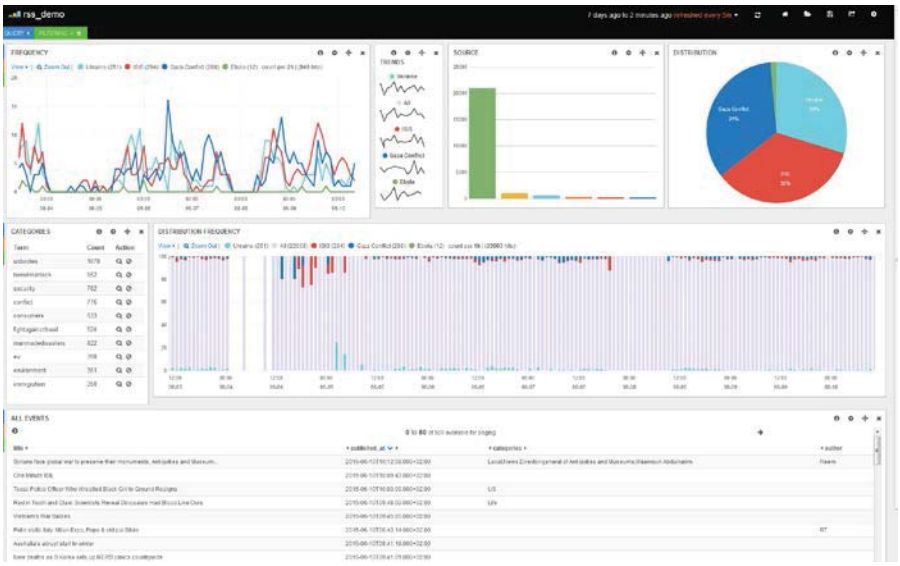


Fig. 2: Kibana frontend provides a basic visual representation of stored data in Elasticsearch

So far we only tackled the data management part of the analytics process. Apart from basic Kibana visualizations, Ubicity will be equipped with advanced analytics methodologies to analyse open source internet content, especially topic mining in large news corpora. Ubicity's stream-based data management approach and data routing across multiple modules offer a promising foundation. In a first step, we intend to conduct certain text mining operations such as named entity recognition and co-occurrence analyses. This is followed by re-indexing all findings in Elasticsearch and other data stores such as Titan or NEO4J. The iterative data processing approach enables us to refine our findings and implement self-learning analysis methodologies. In current scenarios we use third party tools such as the widespread programming languages R or Python to conduct each single step individually. Once they work seamlessly with the Ubicity platform, we intend to integrate them into the architecture. In this way, users will be facilitated to make use of a variety of techniques for data processing, analysis and visualization and to choose those that are suited best to solve domain specific problems. First tests revealed that both, R and Python, work well with the Ubicity platform, since they offer packages that support Elasticsearch and connectors to the Ubicity broker. While R offers a large variety of statistical and visualisation methods, which are continuously extended and improved by a large user community, Python provides better routines for parallel computing and multi-threading.

4 CRISIS AND DISASTER MANAGEMENT APPLICATIONS

In order to prove the applicability of the Ubicity platform, we tested it with real data in the scope of two relevant use cases in the CDM domain. In the following, we briefly describe them and discuss possible extensions and future work.

4.1 Crowdtasking of Volunteers

Crisis managers have to deal with two developments: (i) citizens are no longer interested in traditional memberships that bind them to first responder organizations and (ii) social media and new technologies play an increasing role in crisis communication. One way to take advantage of these developments is to involve spontaneous volunteers into the whole life-cycle of crisis management through *crowdtasking*. In contrast to the more known crowdsourcing, crowdtasking refers to assigning simple tasks to groups of volunteers that are selected due to their skill profile and geospatial location and are capable of executing the tasks at hand promptly.

The developed application is using the Ubicity platform with Couchbase Stack and Elasticsearch as data storage technologies. In this way, pre-registered volunteers are able to

use their mobile devices for interacting with the central management system [12]. At the same time, crisis managers are able to use the platform as a crowdtasking tool for selecting a specific group of volunteers according to their profile (e.g. language skills, physical abilities, etc.) and known geo-location, where Elasticsearch is utilised to handle (geo) data search and aggregation. Moreover, they are able to canalise communication e.g. to keep other volunteers updated about the current situation or to directly ask them to stay passive for the moment. In this way, crisis managers do not have to struggle with avalanches of volunteers on-site and are able to focus on more important tasks.

On a technical level, this is realized by using Ubicity as backend system, which is responsible for collection, storage and analysis of the volunteer responses. For the production of situation reports and monitoring of data streams, e.g. from social media, this platform has a generic interface that can be easily connected to different analysis or visualization tools. In order to support a continuous process of communication between crisis managers and volunteers, a web portal provides up-to-date information and allows volunteers to register at any time, as well as to download the mobile application.

4.2 Social Media Monitoring with Twitter

Social media platforms have been subject of various studies in the context of Big Data analytics. Due to its permissive data policy and its rich set of meta-data, Twitter is a very prominent and frequently used data source for such studies. One of the most intensively stressed use cases are market research and customer profiling. Social media data reflects people's interests, needs and opinions and is therefore a valuable foundation for all future commercial data analytics applications. On a much larger scale, social media data also reflects human behaviour. Being able to extract conclusions or to predict future trends from this behavioural data is a very promising field of research for the crisis and disaster management domain.

Ubicity has been used to collect 698 million geotagged tweets (261GB) during a three months period in order to examine the relation between societal events and the alternation of communication behaviour on twitter. We examined various scenarios in Egypt, Japan and the Ukraine and observed some indicators that stress our initial hypotheses [13]. We used Ubicity's geo query functionality to filter tweets according to their relevance for the considered scenario. Comparing the number of daily tweets in three different Ukrainian regions depicted diverging results. However, outstanding political events such as the annexation of the Crimean peninsula or the day when Ukrainian forces pushed into Lugansk led to a short time increase of tweets at respective days, while a substantial change of the overall communication behaviour within a three months period around these events was not observed. Even more surprisingly, we observed that the number of tweets per day on the Crimean peninsula constantly decreased in the reference period. Additionally, our analysis of twitter messages, both, from Ukraine and Egypt, indicated that the perception of political events is different in multiple geographical regions of the same country. Hence, social media data analysis is a promising technique for crisis managers to better understand the perception and reaction of citizens in case of large scale crisis events. In the near future, such analyses could provide valuable insight into public crisis communication and allow crisis managers to conduct impact assessments after certain crises.

Apart from the complexity that comes with human behaviour we examined instabilities in the twitter data stream. According to [14], the volume limitation of 1% in the public twitter stream seems to vary between 1% and 6%, but can even be above for short periods. Furthermore, we detected geographically related differences in the data stream by using a proxy server based in the US in front of the Ubicity backend. Based on those findings our current research activities focus on the normalization of public social media data streams in order to be able to obtain comparable and robust results, which are particularly important for the crisis and disaster management domain. Normalization and proper fragmentation of scattering data streams are still challenging and need to be a subject of future research activities.

5 CONCLUSIONS AND FUTURE WORK

The current trend of increasing social collaboration and the growing amount of available (open) data confirm the need of a generic software platform, which is able to handle heterogeneous data streams and formats. In particular, the rapidly growing amount of geo-enabled data sets requires novel analysis techniques such as location aware processing and evaluation. In this way, data streams can be clustered and analysed due to their geo-spatial properties, leading to new insights. By now, the development and application of Ubicity is focused on emerging crisis and disaster management challenges. In this domain publicly available information is still mainly unexploited, since it is considered as too complex and fast changing for traditional technologies and workflows. However, we already demonstrated in the early stages of developing Ubicity that with the right approach and technological concept, the handling of Big Data does not introduce higher barriers or uncertainties in comparison to traditional approaches. In the near future such platforms will be able to enhance the current CDM processes tremendously. With the planned integration of well-known programming languages such as R and Python, Ubicity will contribute to this development and its capabilities will provide crisis managers with a flexible platform that can be easily tailored to their demands.

REFERENCES

[1] Mashey, John R., Big Data and the Next Wave of InfraStress Problems, Solutions, Opportunities, [Online] http://static.usenix.org/event/usenix99/invited_talks/mashey.pdf [Accessed 12.6.2015]

[2] Laney, Douglas, The Importance of 'Big Data': A Definition, Gartner, 2012

[3] Miller, Harvey J. et al., Geographic data mining and knowledge discovery, CRC Press, 2009

[4] Havlik et al., Robust and Trusted Crowd-Sourcing and Crowd-Tasking In the Future Internet, Environmental Software Systems. Fostering Information Sharing, IFIP Advances in Information and Communication Technology, 2013

[5] Neubauer et al., Crowdtasking - A New Concept for Volunteer Management in Disaster Relief, ISESS Conference, 2013

[6] Lee et al., Geospatial Big Data: Challenges and Opportunities, Big Data Research 2, ISSN 2214-5796, 2015

[7] Java Simple Plugin Framework, [Online] https://code.google.com/p/jspf. [Accessed 12.06.2015]

[8] ActiveMQ Apollo, [Online] https://activemq.apache.org/apollo. [Accessed 12.06.2015]

[9] Elastic Elasticsearch, [Online] https://www.elastic.co/products/elasticsearch. [Accessed 12.06.2015]

[10] Couchbase, [Online] http://www.couchbase.com/nosql-databases/couchbase-server. [Accessed 12.06.2015]

[11] Apache TinkerPop, [Online] http://tinkerpop.incubator.apache.org. [Accessed 12.06.2015]

[12] Sebald et al., The RE-ACTA Crowdtasking Platform – For Crisis and Disaster Management in Austria, EMCSR Conference, 2014

[13] Neubauer et al., On the Volume of Geo-referenced Tweets and Their Relationship to Events Relevant for Migration Tracking, ISESS Conference, 2015

[14] F. Morstatter et al., Is the Sample Good Enough? Comparing Data from Twitter's Streaming API and Twitter's Firehose, in Proceedings of ICWSM, 2013

EXPERIMENTATION CAMPAIGNS FOR ASSESSING SECURITY SOLUTIONS: CASE STUDIES FROM FP7

Christian Carling and E. Anders Eriksson

christian.carling@foi.se
e.anders.eriksson@foi.se

Swedish Defence Research Agency
Gullfossgatan 6, 164 40 Stockholm (Sweden)

Abstract

We present our experiences from assessment work in a number of system-oriented security research projects (WIMAAS, SUPPORT, SEABILLA, and CONTAIN and SECUR-ED). Based on this, we discuss how the assessment method can be further developed to support more complex experimentation campaigns, comprising a mix of desk research, workshops, simple tests, experiments (including computer simulations) and demonstrations. We argue that such experimentation campaigns, with fully integrated assessment activities, provide a uniquely effective way to decide what solutions to adopt, or pursue further in security innovation.

Keywords: security; assessment; evaluation; experimentation; methods; stakeholders; workshops; innovation.

1 INTRODUDUCTION

This paper will summarise our experience of working with assessment of security solutions in a number of European security research projects. We are here only concerned with methodological aspects, with the aim to improve current methods. We will also comment on the design of demonstration activities and how it affected the assessment. To be clear, it is not a re-assessment of the solutions as such, neither is it a review of the projects' overall performance or impact.

The method we have used for assessment of solutions in the projects has evolved through use, with experience from one project being fed in to the work in later projects. They have therefore not been subjected to the same method and a balanced comparison is hard to do.

One problem when discussing methodological issues around these projects is that most of the material produced is not publicly available. Out of the five projects we will discuss, only one has a final assessment report that is public[1].

1.1 Problem background

In recent decades 'new mission oriented research' has emerged as embodied in the case of EU research programmes by the Societal Challenges pillar of Horizon 2020. Secure Societies is one of these challenges and arguably FP7-SEC can be seen as a precursor of this type this new type of mission oriented research. We would argue that our security based experience is of some relevance also for other societal missions. So

[1] We have decided to include references to all assessments reports in any case, in order to at least identify them.

societal challenges typically involve public goods or more generally problems with having the true beneficiaries pay the costs meaning that simple market solutions won't work. Therefore multiple stakeholder groups typically have a say as regards a proposed security innovation [1], [2].

More specific – not to say constitutive – for security is that we are dealing with a wide range of low probability event types. This property has direct implications for our subject. In, say, a normal industrial setting it is typically possible to assess a proposed novel solution by just asking a few experienced practitioners or by a benchmarking exercise with current practice. In security organisations the idea that there may be important scenarios for which a new solution is much worse than the incumbent is hard to disprove.

It is often said that the security sector is bad at adopting novelties. We have just sketched two reasons why this is to be expected. To be useful for security solutions assessment methods must be able to overcome the multi-stakeholder nature and the inevitable limitation of relevant operational experience germane for the security sector.

1.2 Terminology

Assessment is a vast field, both as a practice and as an academic discipline, Yet, or perhaps because of that, there is no strong consensus on terminology in the field. According to the Oxford English Dictionary, 'assess' means "to evaluate or estimate the nature, value or quality of something". In our usage, an assessment takes a broad perspective, aggregating results from many sources, seeking to draw general conclusions. An assessment will typically consider not only direct observations but also the possible effects of external factors. The key word is "estimate", reflecting the uncertainties that must be managed and the substantial degree of qualitative judgements involved.

By 'evaluation' we mean a well delimited analysis of the outcome of a single test, experiment or other exploratory event. It is performed according to a clear and well-defined process, using a pre-defined set of measures to summarise the outcome. A broad assessment may include a number of smaller, focused evaluations.

The work programme for FP7 Security [3] used the terms 'testing, validation and demonstration' for the type of activities that generate input to assessment. We introduce the term 'experimentation' to stand for the whole range of such activities. In our usage, 'demonstration' in the FP7 sense is then a type of experimentation, together with discovery and hypothesis testing experiments.

All the projects mentioned here have used different terms for the objects to be assessed: "tools", "systems", "technologies", "capacities", "system configurations". For simplicity, we will use the word 'solution' throughout, with the understanding that in research projects, these are all *potential* solutions, whose future value are to be assessed.

2 EXPERIMENTATION CAMPAIGNS AND ASSESSMENT

2.1 Rules for effective assessment

To properly address the requirements outlined in Section 1.1 the assessment procedure should be:

Impact-oriented

Focus on describing long term, high level impact of solutions, not detailed performance within specific situations.

Stakeholder-oriented

The assessment should include the perspectives of all major stakeholders, from the direct users of a solution to those directly or indirectly affected by its employment, including policy and law-makers and, in the end, the general public.

These two qualities, at least in our experience, can only be achieved if the assessment process is:

Scenario driven

The key assessment parameters – which missions to use in testing the solutions, which criteria to evaluate them, which weights to use in the overall assessment – should be driven by a set of scenarios. A more common alternative in many contexts would be to identify à priori a small set of performance measures. But in our experience this is seldom possible, and this intuition is supported by that the fact that a recent attempt to list relevant metrics for security solutions ended up with a hundred items.

2.2 Designing campaigns for assessment

Doing research on large-scale systems of systems, as the work programmes for FP7 states, requires a special methodology. It is not possible to assemble this kind of complex systems step by step, and then perform a single test in the end. The experimentation activities must be broken down into a sequence of manageable parts. In this, some activities can be performed in parallel, each focusing on a limited part of the system. Others need to be performed in sequence, the results of earlier experiments feeding into, thus affecting the planning for, later experiments. To be successful, this demands an approach that can be called campaigns of experimentation. This approach in turn rests upon two complementing principles: orchestration and adaptation. The first defines the detailed plan for the whole campaign: the overall objective must be broken down into manageable experiments; each experiment must be carefully designed in terms of scope and form; dependencies between experiments must be handled and conflicts resolved; activities must be properly sequenced and assigned to experiment facilities; each experiment must be evaluated and in the end, they must be aggregated into an overall assessment of the system as a whole.

Adaptation means that the experimentation plans must continually be reviewed, using the outcome from experiments to guide the objectives of later experiments. This adaptation must go beyond usual risk-limiting project management techniques, to actively look for opportunities for knowledge generation. This requires constantly looking for the areas with the largest potential for gaining new knowledge, or largest uncertainty that needs to be resolved to choose the best route forward, all with the aim to maximise learning throughout the work.

While we argue that the design of experimentation activities should follow from the assessment needs, this is not what we've seen in the selected projects. One can see four levels of connection between assessment and experimentation design:

1. Post-hoc assessment: assessment is completely separate from experimentation
2. Observation: ad-hoc data collection for assessment
3. Assessment directs data collection
4. Assessment directs experiment design

3 EXPERIENCE FROM FP7 SECURITY RESEARCH PROJECTS

In the following sections we will review our experience of assessment work in five projects. In time, they span the entire FP7 period, the first starting 2008, the last ending

in 2014. In one case the assessment was performed by a single partner, otherwise by teams consisting of up to 6 partners. In all, over 30 people from 12 organisations have participated in the assessments. Six of these were Research & Technology organisations, 2 were Industry partners and 4 were SMEs.

3.1 WIMAAS

WIMAAS was a Capability project (CP) in the first call of FP7-SECURITY, working on innovative concepts for airborne maritime surveillance. Key concepts explored were reduced crew solutions (e.g. tactical personnel on ground), optionally piloted vehicles (OPV) and RPAS. The project design had a clear system-of-systems perspective, with separate parts covering main systems (platforms, sensors, communications, data processing and fusion, tasking), a system-of-system architecture part developing promising configurations and a modelling and simulation part to generate data for the assessment. All studies worked within a common set of mission scenarios covering 6 different maritime surveillance missions: irregular migration, drug smuggling, terrorism, piracy, illegal fishing and search for weapons of mass destruction.

Using the categories of assessment design introduced above, WIMAAS was in category 3: the metrics for performance data to be generated by simulations was designed starting from the assessment needs, even though the influence was limited: in the end, some aspects of system effectiveness could not be addressed by the simulations, because of unsuitable parameter choices.

The Description of Work used the term “cost-benefit study”, but it was decided that a cost-effectiveness analysis would be more appropriate. Effectiveness was measured on the level of mission accomplishment, using a combination of measures, e.g. detection probabilities, endurance etc. A life cycle cost model was developed, to capture the difference in cost structure of the various system configurations. Obtaining sound estimates proved very hard and it is clear in hindsight that some of the estimates were based on very uncertain information.

In a systems-of-systems study, scenario discipline is critically important, to avoid sub-optimisation. This worked very well in WIMAAS: all separate system studies effectively worked within the selected mission scenarios, so results from each separate system studies could be combined and discusses in a meaningful way.

The effort for assessment-related activities were 8 person-months, about 3 % of the total of 284[2]. The partners involved were FOI (SE) and Dassault Aviation (FR). The report [5] is not publicly available.

3.2 SUPPORT

SUPPORT[3] was a capability project on main port security, with the aim to raise the current level of port security by integrating legacy port systems with new surveillance and information management solutions. If focused on physical protection of port facilities and surrounding areas. The solutions were mainly different sensors and detection systems. Some work on information fusion solutions was also demonstrated.

The final demonstrations were, in accordance with the project plan, rather limited. The design of the demonstration was of the first category (post-hoc, separate assessment). The only real record of how the demonstrated systems worked was collected by observation and interviews after the event.

[2] These numbers are taken from the projects’ Description of Work. Actual number of person-months used may differ.

[3] http://www.supportproject.info/

The assessment effort available was 14 person-months, less than 2 % of the total effort of 891. The demonstration was evaluated by FOI alone, with other parts of the final Cost-benefit analysis performed separately. The report [6] is not publicly available.

3.3 SEABILLA

SEABILLA[4] was an Integration project on sea border surveillance. The project design had a system-of-system character, in that the technical work covered all major parts of a European-wide sea border surveillance system, e.g. coastal radar chains with information processing systems; imaging satellites with ground stations and processing centres; and Remotely Piloted Aircraft systems (RPAS).

Computer simulations were run based on vignettes in three areas (the Atlantic outside west Africa, the English Channel and the Central Mediterranean), each simulation including several systems. The simulations were closely scripted and did not explore variations from the strict event sequences, so the generalisation to more generic use cases was difficult, based on reasoning more than data.

The simulations generated a lot of performance data for the technical analysis. For the overall assessment on the other hand, it was difficult to translate the data into relevant measures of operational effectiveness. In accordance with our system-of-system level experimentation approach, many systems were included in each simulation and some systems were tested in more than one vignette (e.g. RPAS and passive radar). This, and the ensuing analysis of the contribution of each system towards the overall effectiveness worked fairly well.

The assessment effort was 22 person-months, which was 2 % of the total effort of 1170. The assessment team consisted of FOI; Thales Communications and Security (FR); and JRC. Most reports from the SEABILLA project are public, including the assessment report [7], D46.1 Demonstration Evaluation and Project Synthesis.[5]

3.4 CONTAIN

CONTAIN[6] was an Integration project on container security. Sharing the overall approach and solution architecture with SUPPORT, it comprised a range of security solutions that could be grouped into three categories: monitoring solutions, e.g. detection systems and container tracking systems; situational awareness, e.g. information systems that gather and aggregate data; and decision support systems, e.g. information systems that help a user identify suspicious containers.

A singular feature of CONTAIN was that the project explicitly set out to find solutions that could simultaneously improve security as well as efficiency in the logistics chain[7]. Apart from setting a much higher requirement on solutions, it also forced an adaptation of the assessment framework, to ensure that these aspects could be described. The assessment effort was 20 PM out of 1090, which is just under 2 %. The team consisted of FOI, VTT (FI), Marlo (NO), BMT (UK) and Conceptivity (CH). The report [8] is not publicly available.

3.5 SECUR-ED

SECUR-ED[8] was one of the five large Phase II demonstration projects in FP7-SEC, on urban mass transport security. On-site tests and demonstrations were performed in the

[4] http://www.seabilla.eu/cms/

[5] It cannot however be retrieved from the SEABILLA web site.

[6] http://containproject.eu/

[7] That is on the system-of-system level, since no single system could be expected to deliver a substantial dual benefit.

[8] http://www.secur-ed.eu/

transport systems of four large cities (Madrid, Paris, Milan and Berlin) and six additional cities (Bucharest, Brussels, Lisbon, Izmir, Bilbao and Bergen).

Scenarios were specified, although not in any detail, already in the proposal phase. Some of the demonstrations used vignettes to script the demonstrated events. No variations were performed to see how plausible the depicted sequence of event would be, e.g. how often would a suspect person be reacquired by the video tracking system, after being lost from sight?

A large number of new solutions were explored in SECUR-ED: the initial technical work documented over 100 new concepts or potential solutions. 77 of those were tested in one of the demonstration cities and 11 of those were tested in more than one city.

The assessment was designed to look into results from all parts of the project, also evaluating solutions described at a conceptual level, and not brought into demonstrations. This led to a step-wise design for the assessment: in the first step, a very large number of solution ideas were evaluated according to a formal scheme, using only documents and interviews as sources. Second, all solutions that were implemented in tests and demonstrations were evaluated, followed by a final assessment stage, where a smaller number of particularly promising solutions were discussed in more detail, and in a wider context.

SECUR-ED had several activities drawing conclusions at the outcome from demonstrations from specific perspectives. The core assessment work comprised 50 PM out of 2421, which is 2 %. This was the largest assessment team of all these cases: FOI, Fraunhofer, JRC, TNO, University of Stavanger and UITP. Several reports from the assessment were produced [9], [10], [11], none of which are publicly available.

4 CONCLUSION FOR ASSESSMENT AND EXPERIMENTATION CAMPAIGN DESIGN

Many of the shortcomings we have seen in our work are direct consequences of the projects' design, where assessment has been a largely separate activity. In most cases it was possible, through intense proactive efforts, to compensate for this disconnect, but the overall conclusion must be that effective assessment requires a high level of integration with experimentation activities. This does not mean that there are no other concerns: to be credible, the assessment team must also have a clear independence, to avoid suspicion of bias or hidden agendas in the conclusions. This is a methodological issue that needs more discussion.

In terms of opportunities missed from the assessment perspective, the major recurring problem was the lack of systematic data collection within the testing and demonstration activities. Our solution was to collect the necessary material independently, mainly through interviews with people responsible for such tests and preparations. In the end, this did provide enough material to performs the assessments, but it is clearly not an optimal use of resources. This is the first and foremost lesson learned: systematic data collection must be an integral part of all experimentation activities, including pure demonstrations.

The second lesson is that possible synergies to maximise the knowledge gained from experimentation have not been realised. Better understanding of the knowledge objectives, leading to effective campaigns of experimentation, could increase the output of these projects to the long term security innovation process. This is the key observation behind the experimentation campaign approached adopted in the DRIVER project, one of the final demonstration projects within FP7-SEC.

All these projects have, just as similar future project should, worked with a very diverse set of solutions, of varying maturity. From a methodological point of view, it is very difficult to describe such a heterogeneous set of solutions in a common, well-defined framework: it is not possible to use the same metric to describe a training package for security personnel, as an experimental information fusion algorithm. The solution has been to work top down, starting from the broad assessment aspects, and to define a finer metrics within these only to the degree needed and possible. Our experience is is that this focus on higher-level and long term impact, multi-stakeholder perspective has worked well. Factors for success have been a broad collection of information to supplement the material coming directly from the experimentation events.

Another lesson concerns cost-benefit analysis (CBA), which (with variations in terminology) was an objective in all projects. Taking costs into consideration is a necessity but the character of these projects presents great methodological challenges. Considering benefits first, it is necessary to address the multi-stakeholder problem: for any proposed security solution, a great number of organisations and individuals, with different preferences and values will be affected, and must be considered separately. Furthermore, a pure CBA monetises also the benefits. In the security area, especially if personal integrity issues are involved, this can soon become contentious, making it hard to agree not only on a number but even on its sign: “your gain is my loss”. Weighing the different stakeholders preferences into a final value is a difficult exercise.

On costs, there are specific challenges, but most can be handled by established techniques. Once again, it is the difference in character and maturity of solutions that makes it difficult to produce comparable cost estimates. Since the CBE/CBA is used here only to identify especially promising solutions, it is enough to work with very rough order of magnitudes costs.

Table 1 below summarises some of the characteristics of the projects from the assessment perspective.

A general conclusion is that experimentation-based assessment of security solutions is as yet in its infancy. This is based primarily on the fact that the reported cases are so low in terms of the level of integration of Section 2.2: the experiments were not planned to enable assessment meaning that resources were wasted. Either the experiments were not assessed at all, or the cost for collecting by necessity far from perfect data post hoc was quite high. This said it should be underlined that not even in a world of fully mature security experimentation, all experiments would be level 4 in the ladder; doing field experiments in operational systems – as in SECUR-ED – the system owner always has veto rights.

Presumably the explanation for the low maturity of this activity is that experiments were designed as demos in established industries where experienced practitioners can relatively easily discern the benefits of a novel solution or where at least the proper metrics are well-understood and easy to collect.

Table 1 Summary of the assessment cases.

Project	Area	Type	Total PM	Assess-ment effort	Solutions tested	Assess-ment design category	Assessment data source		
							Sim	Lab	Field
WIMAAS	Airborne Maritime surveillance	CP	280	2,8 %	8	3	**X**		
SUPPORT	Port security	IP	900	1,5 %	4	1		x	**X**
SEABILLA	Maritime border control	IP	1170	1,8 %	13	2	**X**		x
CONTAIN	Container security	IP	1090	1,8 %	20	2		**X**	x
SECUR-ED	Urban mass transport	DP	2400	2,1 %	70	2	x	x	**X**

Explanation of the columns:
Type: Capability project (CP), Integration Project (IP), Demonstration project (DP)
Total PM: Project size in terms of total person-months
Assessment effort: size of the assessment effort, percentage of project size
Number of solutions: It is not trivial to decide what counts as a separate "solution". For WIMAAS, this is the number of system-of-system configurations included in the C/B analysis. For the others, it is the number of solutions included in major demonstration activities.
Assessment design category: Level of integration between assessment and experimentation activities in the project design, as defined in section 2.2.
Assessment data source: Type of source providing input to the assessment. "Sim" - computer simulation; "Lab" - tests in laboratory or office conditions, "Field" - tests performed in a realistic operational environment. A capital "X" means this was the main contribution to assessment, while a small "x signifies a minor, supplementary contribution to assessment.

REFERENCES

[1] ETTIS (2014), *D6.4 Report on Government intervention*

[2] Foray, D., Mowery, D.C., Nelson, R.R. (2012): *Public R&D and social challenges: What lessons from mission R&D programs?* Research Policy, 41(10), 1697-170

[3] European Commission (2012), *COM Work Programme 2013 Security*; European Commission COM(2011) 777

[4] Eriksson, E.A. and Carling, C. (2014): *Working with Security Systems-of-Systems*, Future Security 2014

[5] WIMAAS (2012), *D6.1 Cost-benefit analysis* (2012) [dissemination level RE]

[6] SUPPORT (2014), *D6.5 Evaluation - Cost-benefit Analysis - Recommendations* [RE]

[7] SEABILLA (2014), *D46.1 Demonstration evaluation and project synthesis* [PU]

[8] CONTAIN (2015) *D5.4 Evaluation - Cost-benefit Analysis - Recommendations* [RE]

[9] SECUR-ED (2013), *D54.1 Method for Assessing Capacities* [dissemination level CO]

[10] SECUR-ED (2014a), *D54.2 Benchmark of Capacities Considered in SECUR-ED* [CO]

[11] SECUR-ED (2014b), *D53.3 Improve the Risk Reduction System* [CO]

A QUANTITATIVE RISK MODEL FOR A UNIFORM DESCRIPTION OF SAFETY AND SECURITY

Jürgen Beyerer[1] and Jürgen Geisler[2]

[1] *juergen.beyerer@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)
and
Karlsruhe Institute of Technology KIT
Institute of Anthropomatics and Robotics
Adenauerring 4, 76131 Karlsruhe (Germany)

[2] *juergen.geisler@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies, and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

Abstract

A mathematical framework is presented that allows to describe quantitatively and in an integrative way the risk of safety and security constellations. Thereby, great importance is attached to a clear notation with a sound semantics.

Based on a role model with the three roles »source of danger«, »subject of protection« and »protector«, risk is modelled quantitatively using statistical decision and game theory. Uncertainties are modelled based of probability distributions, whereupon probability is interpreted in a Bayesian context as a degree of belief DoB.

The set D of sources of danger is endowed with a DoB-distribution describing the probability of occurrence. D is partitioned into subsets that describe dangers which are due to random causes, carelessness and intention.

A set of flanks of vulnerability F is assigned to each subject of protection. These flanks characterize different aspects of vulnerability concerning mechanical, physiological, informational, economical, reputational, psychological, ... vulnerability. The flanks of vulnerability are endowed with conditional DoBs that describe to which degree an incidence or an attack will be harmful. Additionally, each flank of vulnerability is endowed with a cost function that quantifies the costs which are charged to the subject of protection, if it is affected by a harmful incidence or attack.

With these ingredients the risk for the subject of protection can be quantified based on an ensemble functional with respect to all sources of danger and to all flanks of vulnerability. Depending of the respective subset of dangers such a functional is an expectation (case of random causes and carelessness) or a selection operation (case of intention), where in the latter case the attack will presumably take place at the weakest flank of vulnerability.

The calculated risk can be opposed to the cost of protection measures that are offered by the protector in order to foster an effective and economical invest decision.

From an attacker's point of view a utility function is formulated which a rational attacker presumably would use to evaluate his cost-benefit ratio in order to decide whether he attacks and which of his options he exercises.

The challenges of the approach are the determination of the cost functions and especially the estimation of the probabilities (DoBs) of the model.

The model can be used to simulate and evaluate the endangerment of subjects of protection quantitatively.

Keywords: Safety, Security, Risk, Bayesian Statistical Decision Theory, Game Theory, Degree of Belief, Role Model, Vulnerability, Flanks of Vulnerability

1 INTRODUCTION

Safety and security share a lot of commonalities. Nevertheless, measures and systems to provide and ensure safety and security are planned and implemented often independently by different experts. If both aspects were treated in an integrated manner, synergies could be realized and costs could be reduced.

If we want to ensure safety and security of such complex systems like critical infrastructures and socio-technical systems, many disciplines will be stakeholders: engineering, law, economics, humanities, social sciences etc.

Up to now, there is no established common formal language concerning safety and security and no common language across all involved disciplines. The aim of this paper is to propose a quantitative mathematical approach that could serve to describe and to analyze safety and security problems in a unified fashion and to plan and optimize dedicated measures and systems.

1.1 Related Work

The frameworks of statistical decision and game theory are mature and approved methodologies which have been applied to many different domains, foremost to economics [1]. In combination with attack trees, game theory has been already applied to model rational attackers [2]. Some aspects of the approach presented in this paper have been already proposed in a preliminary qualitative formulation in [3] and [4].

1.2 Safety and Security

The terms of safety and security only make sense in the face of some danger that is supposed to be able to cause damage. It emanates from some »source of danger« d, propagates over a certain »path of transmission« and has effect on a »subject of protection« s (see Fig. 1). The path of transmission is everything between d and s that is needed to transport the hazardous effect. It belongs neither to d nor to s.

In case of e.g. a radio-controlled explosive device this path comprises the radio link between trigger and device as well as the air between the device and the target that the bomb fragments have to pass. In case of a tsunami it is the water between the epicenter of an earthquake and the shore.

The danger hits the subject of protection s at some of its »flanks of vulnerability« F that can be of different quality (mechanical, chemical, psychological, financial, informational, ...). The flanks of vulnerability do belong to the subject of protection and are under its control.

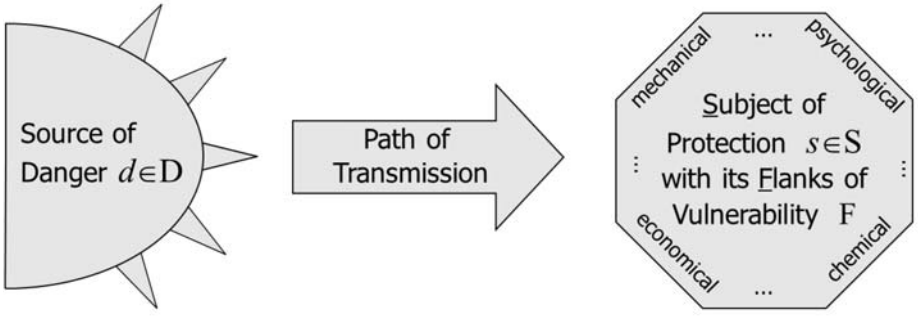


Fig. 1: Relation between a source of danger d and subject of protection s. D and S denote the sets of sources of danger and the set of subjects of protection, respectively.

The two examples mentioned above – explosive device and tsunami – illustrate two fundamental categories of dangers: willful and unintended. If a danger is willfully applied, we are in the domain of security. If it is unintended, we are in the domain of safety. A willful endangerment by human beings can be used on the one hand as a means to achieve some (material) goal, e.g. in the case of robbery. Or it can be executed as a purpose of itself, e.g. in the case of vandalism or amok. The source of unintended danger may on the one hand be human carelessness that may underestimate or even ignore damage. Or the origin may be a random event such as an unforeseeable technical fault or a natural event (e.g. an earthquake). Fig. 2 illustrates this categorization.

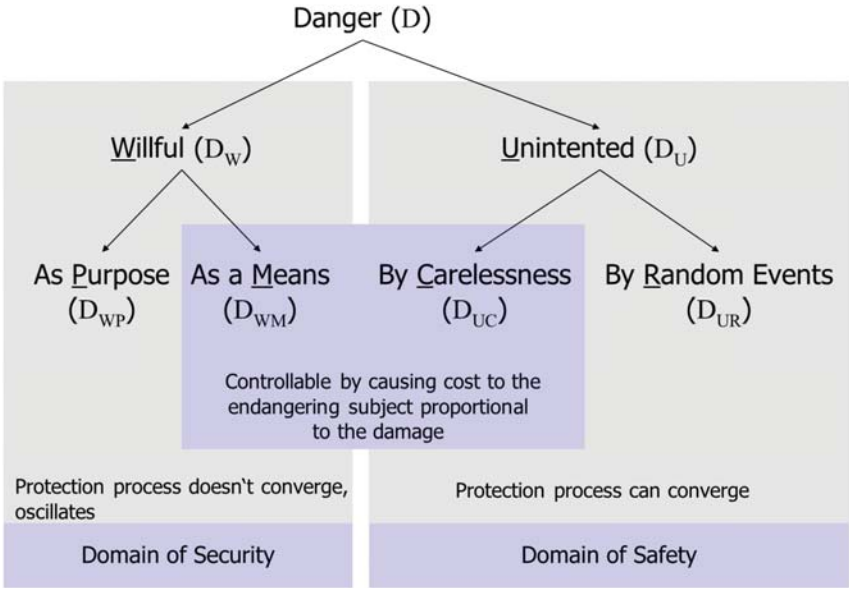


Fig. 2: Categorization of dangers with respect to safety and security. $d \in D_W$ are called "attackers" and $d \in D_U$ are called "causers". In the cases of an attacker $d \in D_{WM}$ or a causer $d \in D_{UC}$ the pertaining risk can be influenced by costs charged to d (penalties, money,…), so that d will be deterred from attacking or so that d is urged to act more carefully, respectively.

From a game theoretic point of view there is another interesting interpretation of safety and security [3]. With respect to safety the subject of protection s plays a game against nature. His opponent behaves like a random process. Based on a statistical analysis the distribution which characterizes the opponent can be learned and counter measures can be applied to reduce the risk. Especially if the distribution does not change with time, a stationary safety level can be attained with passive measures.

In contrast, regarding security, the adversary behaves intelligently. In this case, the subject of protection s plays against a strategically acting opponent who evades of being understood, who analyzes the weaknesses of s and who selfishly tries to maximize his benefit. Therefore, measures will be answered with counter measures and no stationarity will be achieved (see Fig. 2).

A further issue becomes clear from the discussion so far: an attacker who is a rationally acting agent does not randomly attack any of the flanks of vulnerability. Instead he will attack the flank which is must promising for him to achieve his goal. Relating to security, this directly leads to the following **minimum principle**: The weakest flank determines the degree of vulnerability.

Moreover, whether we are in the domain of security or of safety only depends on the source of danger d and does neither depend on the path of transmission nor on the

subject of protection s (see Fig. 1). E.g. if a fire was caused by an arsonist, we would have a security case. If however the fire was caused by an electric shortcut, we would assign it to safety. Relating to the path of transmission and to the subject of protection both cases need not to be distinguished, since both lead to the same consequences.

2 ROLE AND RISK MODEL

2.1 Roles

The goal of each measure to increase safety as well as to increase security is to prevent the subject of protection from harm caused by dangers. Therefore, we define a third role beneath the already introduced source of protection s and the source of danger d: The »protector« p. It is first of all a role, not necessarily an entity separate from s. When any s protects itself without any external help, p and s are coined by the same entity. With the introduction of p we can concentrate all measures of protection onto this role. That are (see Fig. 3): To detect and possibly neutralize the source of danger directly, to elongate the path of transmission in order to weaken the hazardous effect, to cover the subject of protection and to harden its flanks of vulnerability. A necessary precondition for the relation between the subject of protection and its protector is trust, in case of s and p are separate entities often confirmed by a contract.

To complete the relations between the three roles in Fig. 3 it should be made clear, that except for unintended danger by random events (see. Fig. 2) there is always some flow of value from s to d. That is expressed by the relation s »enriches« d.

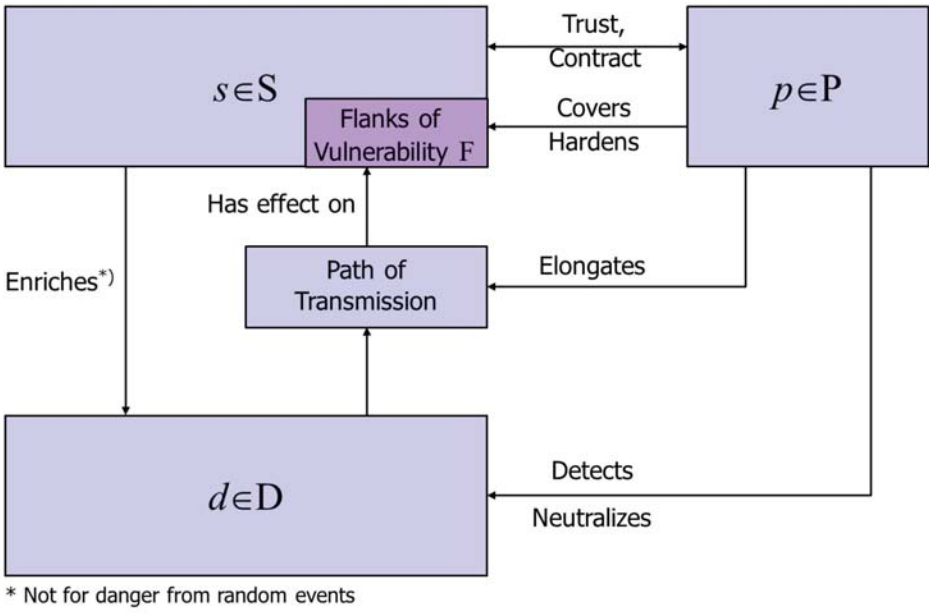


Fig. 3: Roles and relations between them. Note that the different roles can be played by different entities but coincidences are also possible. E.g. someone can be a danger for himself or someone can protect himself.

2.2 Formalization of Ingredients

In this section the entities, attributes and relations of the considerations above are formalized and quantified using the well-established approach of Bayesian statistical decision theory [1]. Probability is used in the broader sense as a degree of belief (DoB). This interpretation is a generalization of the classical frequentistic meaning of probability, which however is still compliant with the axioms of Kolmogorov [5], [6]. All

quantities relate to a time interval of length T, within which they are assumed to remain constant.

$\mathrm{S} = \mathrm{S}_{\text{Persons}} \cup \mathrm{S}_{\text{Objects}} \cup \mathrm{S}_{\text{Systems}} \cup \mathrm{S}_{\text{Legal Interests}}$ denotes the set of subjects of protection. These subjects $s \in \mathrm{S}$ have budgets $b(s)$ for safety and security measures and flanks of vulnerability $f \in \mathrm{F}_s$.

Dangers (attackers, causers) d are elements of the set of sources of danger $\mathrm{D} = \mathrm{D}_{\mathrm{WP}} \cup \mathrm{D}_{\mathrm{WM}} \cup \mathrm{D}_{\mathrm{UC}} \cup \mathrm{D}_{\mathrm{UR}}$, where the indices have the following meaning:

WP: Willful danger as a purpose (vandalism, amok, …)
WM: Willful danger as a means (burglary, robbery, …)
UC: Unintended danger due to carelessness or negligence (inattention, breach of duty)
UR: Unintended danger with random characteristic (technical failures, natural disasters)

We define two further subsets $\mathrm{D}_{\mathrm{U}} := \mathrm{D}_{\mathrm{UC}} \cup \mathrm{D}_{\mathrm{UR}}$ and $\mathrm{D}_{\mathrm{W}} := \mathrm{D}_{\mathrm{WP}} \cup \mathrm{D}_{\mathrm{WM}}$ that structure the dangers $\mathrm{D} = \mathrm{D}_{\mathrm{W}} \cup \mathrm{D}_{\mathrm{U}}$ into a willful and an unintended subcategory.

In the following $d \in \mathrm{D}_{\mathrm{W}}$ are called »attackers«. Attackers perpetrate attacks a which are pooled in the set of attacks A, $a \in \mathrm{A}$. An attacker has a budget $b(d)$ with which he finances the effort of an attack. The attacks a an attacker d is able to perform are summarized in the subset $\mathrm{A}_d \subseteq \mathrm{A}$.

Sources of danger $d \in \mathrm{D}_{\mathrm{U}}$ due to carelessness generate incidents i, which are pooled in set of incidents I, $i \in \mathrm{I}$. In the following $d \in \mathrm{D}_{\mathrm{U}}$ are called »causers«, because they cause incidents. The set of incidents referred to a causer $d \in \mathrm{D}_{\mathrm{U}}$ are summarized in the subset $\mathrm{I}_d \subseteq \mathrm{I}$.

If an attack or incident happens, the success (harm) of such an event is quantified by the degree of success $\beta \in [0,1]$.

An attack or an incident on s via flank f with success β costs s: $c(s, f, \beta) \in [0, \infty)$. Vulnerability with respect to attacks or incidents is modelled as a DoB-density. $p_{\mathrm{V}}(\beta | i, s, f)$ and $p_{\mathrm{V}}(\beta | a, s, f)$ describe the DoB-densities for the degree of success β, if a respectively i hits s via f .

Remark: In the case that the costs $c(s, f, \beta)$ are proportional to the success β, i.e. $c(s, f, \beta) = \beta \cdot c(s, f)$, costs and vulnerability can be factorized:

$\int_0^1 c(s, f, \beta) \cdot p_{\mathrm{V}}(\beta \mid i, s, f)\, \mathrm{d}\beta = c(s, f) \cdot v(s, f, i)$, where $v(i, s, f) := \mathrm{E}_{\beta | i, s, f}\{\beta\}$

$= \int_0^1 \beta \cdot p_{\mathrm{V}}(\beta \mid i, s, f)\, \mathrm{d}\beta$ is the mean success-DoB of an incident i.

Causers of danger due to carelessness $d \in \mathrm{D}_{\mathrm{UC}}$ are charged with costs $\kappa(s, f, \beta) \in [0, \kappa_{d\_\mathrm{Ruin}}]$. These costs correspond to a penalty for d for generating an incident $i \in \mathrm{I}_d$ hitting s via f with success β. The higher the costs for d the lower the probability of an incident generated by d should be (deterrent effect).

A protector $p \in \mathrm{P}$ provides safety and security measures $m(s,f) \in \mathrm{M}$ for the flank f of s. M denotes the set of available and $\mathrm{M}^* \subseteq \mathrm{M}$ the set of implemented measures. A measure m costs s the amount $c(m(s,f))$. Of course, s can only effort measures according to his budget. This introduces the constraint $\sum_{m \in \mathrm{M}^*} c(m(s,f)) \leq b(s)$.

Measures $m(s,f)$ should reduce vulnerability, i.e. the success of attacks and/or incidents, and/or the probability of occurrence of attacks and/or of incidents. However, $m(s,f)$ is modeled such that it does not reduce $c(s,f,\beta)$.

The following quantities are to be understood from the attacker's point of view. $g(s,f,\beta)$ denotes the gain due to an attack on s via f with success β. $p_{\mathrm{Success}}(\beta \mid a,s,f)$ is the DoB-density for success β, if a hits s via f. $c_{\mathrm{Effort}}(a,s,f)$ describes the costs due to the effort for executing an attack a on s via f. $c_{\mathrm{Penalty}}(s,f,\beta)$ denotes the monetary equivalent to a penalty for an attack on s via f with success β.

And finally, $\Pr(\mathrm{Penalty} \mid s,f,\beta) = 1 - \Pr(\neg \mathrm{Penalty} \mid s,f,\beta)$ denotes the DoB for a punishment of an attack on s via f with success β.

2.3 Quantification of Risk

The total risk R_{s_total} of a subject of protection s from the point of view of s can be expressed as: $R_{s\_\mathrm{total}} := \underbrace{R_s}_{\text{Model}} + \underbrace{R_0}_{\text{Outside modelling scope}}$, where R_S denotes the describable part of the risk and R_0 denotes that part of the risk, which cannot be modelled. Hopefully, measures m reducing the modelled part of the risk R_s should not increase R_0 for more than this reduction, i.e.: $\Delta R_{s\_\mathrm{absolut}}(m) := R_{s\_\mathrm{absolut}}(\text{without } m) - R_{s\_\mathrm{absolut}}(\text{with } m) \geq 0$ with $\Delta R_s(m) := R_s(\text{without } m) - R_s(\text{with } m) > 0$.

The risk R_s of s from the point of view of s can be expressed as:

$$R_s = \sum_{d \in \mathrm{D_U}} \sum_{i \in \mathrm{I}_d} \sum_{f \in \mathrm{F}_s} \int_0^1 c(s,f,\beta) \cdot p_{\mathrm{V}}(\beta \mid i,s,f)\, \mathrm{d}\beta \cdot \Pr_{\mathrm{U}}(i \mid s,f)$$
$$+ \sum_{d \in \mathrm{D_W}} \sum_{a \in \mathrm{A}_d} \int_0^1 c(s,\tilde{f},\beta) \cdot p_{\mathrm{V}}(\beta \mid a,s,\tilde{f})\, \mathrm{d}\beta \cdot \Pr_{\mathrm{W}}(a \mid s,\tilde{f}) + \sum_{m \in \mathrm{M}^*} c(m(s,f))$$

$\Pr_{\mathrm{U}}(i \mid s,f)$ denotes the probability of occurrence (DoB) of an incident caused by d on s via f. $\Pr_{\mathrm{W}}(a \mid s,f)$ is the probability of occurrence (DoB) of an attack of d on s via f.

The first summand of R_s corresponds with the risk relating to safety, the second quantifies the risk relating to security and the third addend numeralizes the costs of deployed measures m. Thus, R_s unites the rating of safety and security and also considers the efforts for reducing the risk.

Compared to statistical decision theory [1], additionally to the classical risk factors probability and cost, with p_{V}, which models the vulnerability, a third factor comes into play. This is in accordance with the approaches in [7] and [8] whereas we formulate this third factor as a conditional DoB-density, so that compliance with probability theory

is preserved. E.g. $p_{\mathrm{V}}(\beta \mid i,s,f)\cdot \Pr_{\mathrm{U}}(i \mid s,f)$ is equal to the joint DoB-density $p(i,\beta \mid s,f)$ for the occurrence of an incident i with success β given s, f.

Only if an attacker coincidentally has motivation, power and occasion, he will undertake an attack. Therefore, $\Pr_{\mathrm{W}}(a \mid s,f)$ is modelled with a product of three DoB factors: $\Pr_{\mathrm{W}} = \Pr_{\mathrm{Motivation}}\cdot \Pr_{\mathrm{Power}}\cdot \Pr_{\mathrm{Occasion}}$.

$\tilde{f} := \arg\max_{f\in \mathrm{F}_s}\{\max_{a\in \mathrm{A}_d}\{U_d(a,s,f)\}\}$ is the most beneficial flank of vulnerability of s from the viewpoint of the attacker d.

To quantify the awaited benefit for the attacker d perpetrating an attack a on s via f, the utility $U_d(a,s,f)\in[U_{\min,\,d}\,,\,U_{\max,\,d}]$ is modelled as:

$$U_d(a,s,f) := \int_0^1 g(s,f,\beta)\cdot p_{\mathrm{Success}}(\beta \mid a,s,f)\,\mathrm{d}\beta \; - c_{\mathrm{Effort}}(a,s,f) - \int_0^1 c_{\mathrm{Penalty}}(s,f,\beta)\cdot \Pr(\mathrm{Penalty} \mid s,f,\beta)\cdot p_{\mathrm{Success}}(\beta \mid a,s,f)\,\mathrm{d}\beta$$

$$U_d(a,s,f) = \int_0^1 \left[g(s,f,\beta) - c_{\mathrm{Penalty}}(s,f,\beta)\Pr(\mathrm{Penalty} \mid s,f,\beta)\right] p_{\mathrm{Success}}(\beta \mid a,s,f)\,\mathrm{d}\beta - c_{\mathrm{Effort}}(a,s,f)$$

whereupon $c_{\mathrm{Effort}}(a,s,f)\le b(d)$ holds. Obviously, it is straight forward to apply the risk modelling approach also to sets S of subjects s of protection who are endangered by D. In this case, the risk simply can be calculated by summing over S: $R_{\mathrm{S}} = \sum_{s\in \mathrm{S}} R_s$.

2.4 Introduction of Temporal Dynamics

Up to now, all quantifies have been treated as they were constants relating to a time interval of duration T. In order to cover real world problems, it is necessary to equip the approach with a time dependency. If, for example, a measure m is implemented to improve the security level of s, this will influence the behavior of an intelligent opponent d. Within a longer time period T this would couple the different quantities implicitly and would make the interplay between s and d obscure.

A straight forward approach is to model all quantities as time series. An upper index $k\in\mathbb{N}_0$ denotes the discrete instant of time. Additionally, a transition operator Φ^k is introduced that maps the relevant quantities from time step k to k+1.

$$\left(b^k(s), m^k, \ldots, p_V^k, \Pr_{\mathrm{U}}^k, \Pr_{\mathrm{W}}^k, R_s^k, U_d^k\right) \xrightarrow[\Phi^k]{} \left(b^{k+1}(s), m^{k+1}, \ldots, p_V^{k+1}, \Pr_{\mathrm{U}}^{k+1}, \Pr_{\mathrm{W}}^{k+1}, R_s^{k+1}, U_d^{k+1}\right)$$

It is assumed that the time discretization is fine enough to keep pace with the dynamics of the modelled system, so that all quantities can be assumed to remain constant within a time step k.

For example, the influence of a security measure m^k implemented at time k on $b\,(s), p_V, \Pr_{\mathrm{W}}, R_s$ and U_d is modelled by the change from $b^k(s), p_V^k, \Pr_{\mathrm{W}}^k, R_s^k$ and U_d^k to $b^{k+1}(s), p_V^{k+1}, \Pr_{\mathrm{W}}^{k+1}, R_s^{k+1}$ and U_d^{k+1} accomplished by the transition operator Φ^k.

3 CONCLUSIONS, CHALLENGES, AND SUMMARY

Based on a role concept we have introduced a mathematical framework that allows to model the risk of a subject of protection with respect to safety as well as with respect to

security in a unified manner. The roles and quantities have clear semantics, which is a helpful prerequisite to determine the model parameters quantitatively, if the framework is applied to real problems. Nevertheless, in practice it is very challenging to estimate the involved quantities with sufficient precision. Especially the estimation the different probabilities is far from trivial. If attacks or incidents occur very seldomly, frequently there is not enough data available to perform a standard statistical analysis. The only way out is to adopt the wider interpretation of probabilities as degrees of belief (DoB). Within the Bayesian statistics this is the usual semantics of probability. It allows in the extreme case to use probabilities to express subjective beliefs of an agent [5], as long as the syntactic rules for the calculation with probabilities, i.e. Kolmogorov's axioms, are not violated.

The quantitative formulation of the risk of the subjects of protection and of the utility of attackers should allow to run simulations, e.g. Monte Carlo or agent based simulations, in order to compute the risk numerically and to generate plausible event sequences according to a simulated game between instances of the introduced roles.

Future work will be focused on methods to estimate the parameters of the model and to apply the approach to real world safety and security tasks. Furthermore, we strive for an UML-based conceptualization of all terms of the model according to the ideas proposed in [9] and [10]. The further development of the modelling approach will be especially pursued within the working group "*Themennetzwerk Sicherheit*" of the German National Academy of Science and Engineering *acatech*.

REFERENCES

[1] Berger, J.O.: *Statistical Decision Theory and Bayesian Analysis*. Springer (1993).

[2] Buldas, A.; Laud, P.; Priisalu, J.; Saarepera, M.; Willemson, J.: *Rational Choice of Security Measures via Multi-Parameter Attack Trees*. In: Critical Infrastructures Security, Lecture Notes in Computer Science Vol. 4347, pp. 235-248, Springer (2006).

[3] Beyerer, J.; Geisler, J.; Dahlem, A.; Winzer, P.: *Sicherheit: Systemanalyse und -design*. In: Winzer, P.; Schnieder, E.; Bach, F. (Hrsg.): Sicherheitsforschung – Chancen und Perspektiven. pp. 39-72, Springer (2009).

[4] Beyerer, J.: *Sicherheitstechnik, Sicherheitssysteme und Sicherheitsforschung – Aktuelle Herausforderungen*. In: Stober, R.: Sicherheitsgewerbe und Sicherheitstechnik – Von der Personalisierung zur Technisierung – 9. Hamburger Sicherheitsgewerberechtstag, pp. 1-10. Carl Heymanns Verlag (2009).

[5] Bernardo, J.M.; Smith, A.F.M.: *Bayesian Theory*. Wiley (1994).

[6] Beyerer, J.: *Verfahren zur quantitativen statistischen Bewertung von Zusatzwissen in der Meßtechnik*. VDI Fortschritt-Berichte, Reihe 8, Nr. 783, VDI Verlag, Düsseldorf (1999).

[7] Baker, G.: *A Vulnerability Assessment Methodology for Critical Infrastructure Sites*. DHS Symposium: R&D Partnerships in Homeland Security. Boston (2005).

[8] Broder, J.F.; Tucker, E.: *Risk Analysis and the Security Survey*. 4th ed. Waltham, MA, USA : Butterworth-Heinemann (2012).

[9] Schnieder, E.; Schnieder, L.: *Verkehrssicherheit – Maße und Modelle, Methoden und Maßnahmen für den Straßen- und Schienenverkehr*. Springer (2013).

[10] Schnieder, E.; Schnieder, L.: *Präzisierung des Normativen Sicherheitsbegriffs durch Formalisierte Begriffsbildung*. In: Winzer, P.; Schnieder, E.; Bach, F. (Hrsg.): Sicherheitsforschung – Chancen und Perspektiven. pp. 73-115, Springer (2009).

IMPROVING THE BORDER CONTROL PROCESS BY QUEUE LENGTH OPTIMIZATION

Gunther Grasemann[1], Mathias Anneken[1] and Elisabeth Peinsipp-Byma[1]

[1] *{gunther.grasemann, mathias.anneken, elisabeth.peinsipp-byma}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

Abstract

The increasing amount of travelers crossing the EU borders and illegal border crossing with sophisticated spoofing methods forces the authorities to implement new solutions for the control process. In order to achieve higher control rates and to increase security and objectivity in the process, the borders have been supported by automated border control systems (ABC). One important aspect in the usage of ABC systems is the more complex queuing process.

Therefore, one objective of the EU funded project FastPass is the queue length optimization. By provision of a special distribution model, the optimal constellation of the queues can be calculated. The model describes the processes in their respective implementation. Two operation modes of the system have been realized. The first one is a calculation of probable process scenarios. The second operation mode is the simulation of the process with visualization and interaction components.

1 INTRODUCTION

The automation of passport control processes delivers effectivity, objectivity and an increase in security. However, this works only if the capacity utilization is suitable for the respective application. That means there are different facilities for passport control, automatic and conventional, Schengen and Non-Schengen.

The optimization task is the optimal distribution of the passengers between the available lines. The objectives are maximal speed, security and comfort for the passengers and the control staff.

There are three types of lines (cp. Fig. 1), the conventional line with human controls, an automatic line for passengers from the European Union and one for other passengers. Actually, it is not known before the control process itself, whether a passenger is allowed to use an e-gate and also not if he is willing to do so. Only the probabilities for each person for being allowed to use and wanting to use an e-gate can be estimated. Then a first estimation can be derived about how many lines should be open and how long they will probably be. Thus, there is a first constellation like in Fig. 1: The distribution of the N passengers of a plane can be combined to the vector

$$D = (T_1, T_2, A_1, A_2).$$

If the duration of a single control process is known as D_C for the conventional gate and as D_E for the electronic gate, the complete control time will be given by the following equation:

$$T_{tot} = max\ (D_C \times T_1, D_C \times T_2, D_E \times A_1, D_E \times A_2)$$

This value can be minimized by changing the distribution and thus the number of passengers for the single gates.

Values to be optimized:

Symbol	Specification	Min/Max
T_{tot}	Total time for the control of the plane	Min
T_{max}	Maximum time for a single passenger	Min
N_{BG}	Number of border guards required in total	Min
N_{Gat}	Number of gates required in total	Min

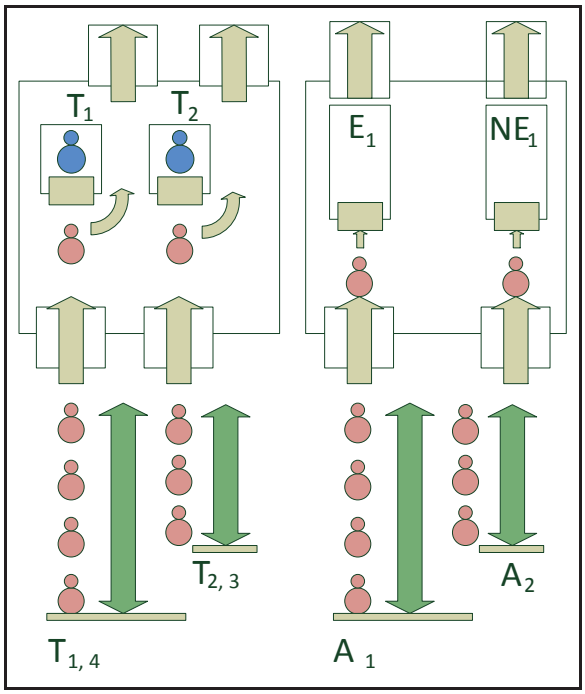


Figure 1: Optimization Scenario

2 METHODICAL APPROACH AND ALGORITHMS

For the modelling and optimization, there are several suitable techniques:

- Markov Chains
- Bayes Optimization
- Linear and non-linear Optimization (Simplex-Algorithm, „Transportation Problem“)
- Operations Research

In addition, a task oriented classification of the travelers is required. Therefore, an assumed set of requirements for the starting constellation of the complete system out of the entire set of information has to be calculated (prediction) and the available measurements have to be taken into consideration for the actual adaptation of the system (indication).

Input parameters at the airport are:

- Information about the scheduled flights, (time of arrival, origin, etc.)
- Estimated information about passengers' properties in the planes (number, classification, distribution)
- Dependencies from time of day, day of the week, actual events

The next block is the set of actual available sensor information:

- Information from the e-gates (as allowed due to data protection)
- Information from the observation from the border guards
- Information from the video sensors (queue length, number of persons, classification properties, images)

Approaches for the modelling of transportation and movement processes are proposed in [4], pp. 41 ff., and in [2]. The modelling and estimation of queue length is described in [5] and [11].

Knowledge has to be generated by use of data mining techniques from observation and experience. The knowledge has to be modelled and stored in a suitable database from which it can be retrieved simply by the front-end modules. The observations and their results have to be visualized by data reduction and aggregation of the most important properties for the prognosis (cp. Fig. 2 and 3).

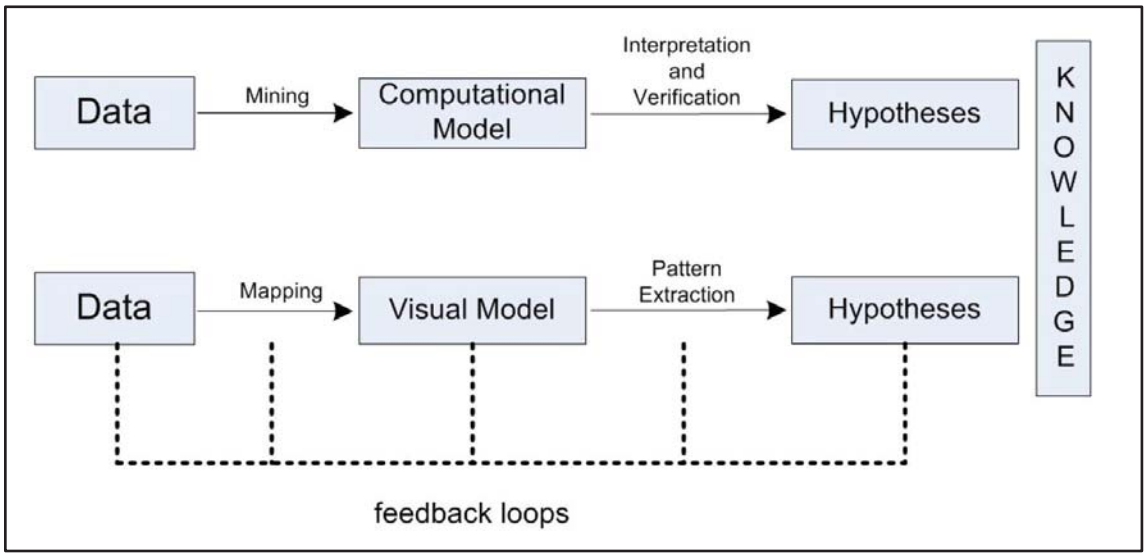


Figure 2: Knowledge generation with traditional data mining and information visualization analytic processes (from [3])

The first step can be realized by a multi-function approach to calculate an initial distribution of passengers' classification properties to be expected by a specific flight.

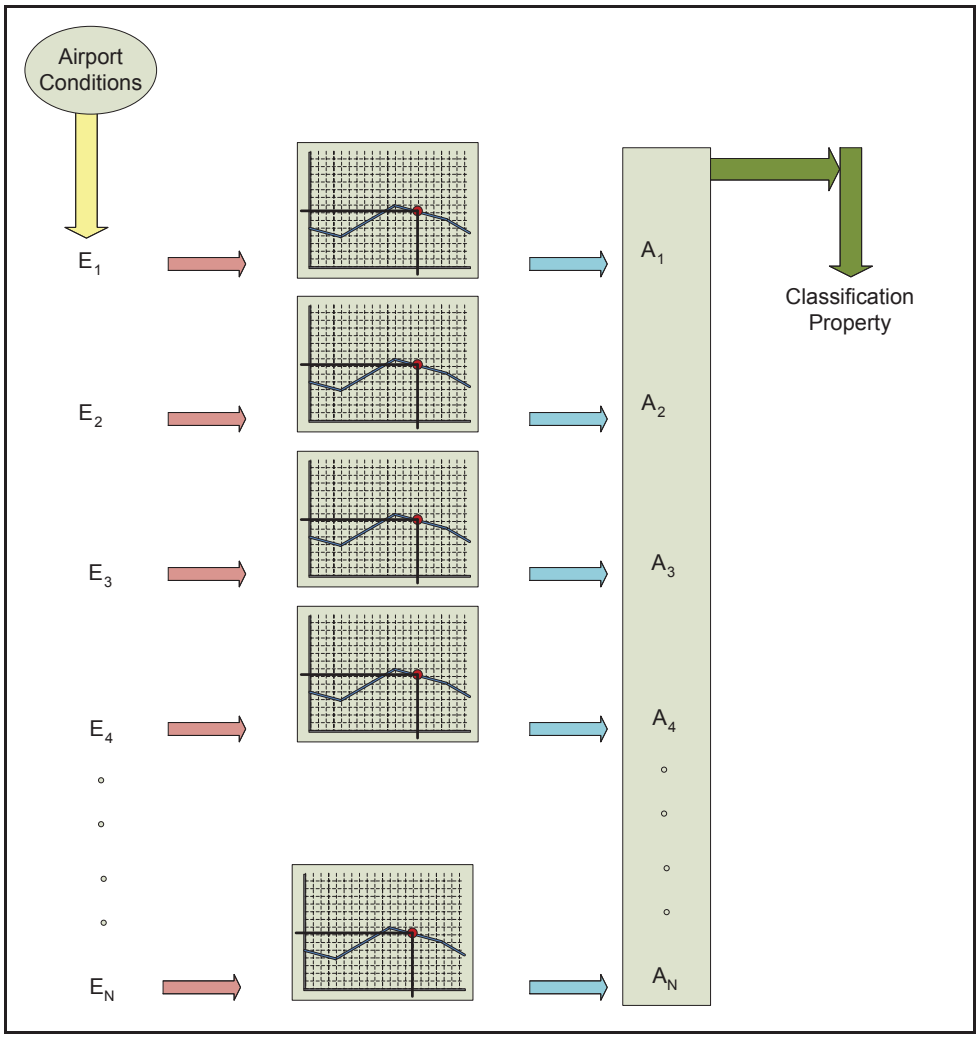


Figure 3: Summarize Classification Property

3 SOFTWARE ARCHITECTURE

For the software architecture, a distributed client server model is provided together with a web service model which is adapted to the standard from the OGC like SOS, WMS or WFS protocol. The techniques are described in [6], [7] and [8]. Some principal ideas are presented in [9].

The center of this approach is the application software in the control room for the border guards; they are responsible for the realization for actual constellations. Several automatic and interactive components serve them to achieve the best actual constellation for the complete control system.

The control room software communicates with the control component of the AIT[1] video subsystem as a client. The AIT systems provide all required and necessary information.

For that, it collects all video streams and calculates the respective values like queue length and number of travelers. In addition, it requests optimizing values from the IOSB subsystem. This system gets prepared values as well as raw images for further analysis steps for the classification.

[1] AIT = Austrian Institute of Technology, FastPass Coordinator

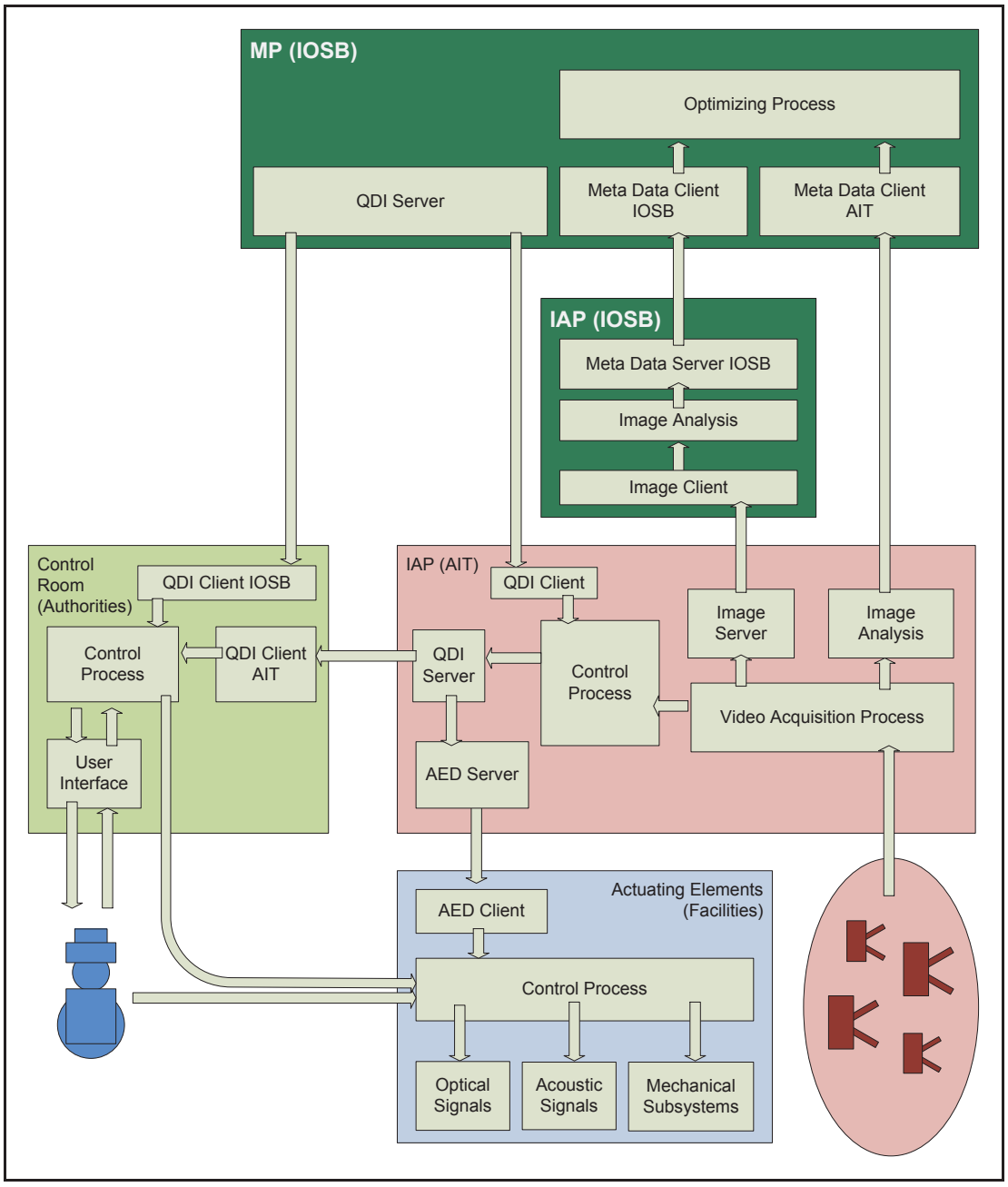


Figure 4: Block Diagram Software Architecture

The core of the system is the control block in the AIT application (cp. Fig. 4). Normally, it will be asked by the control room software to generate an actual constellation of the gate system that should be optimal in the meaning of all regarded parameters. In this case, the AIT system is a server for the control room. As a client, the AIT software requests the modeling process (MP) to send the optimal configuration. MP has to collect information from the AIT subsystem and the IOSB subsystem to collect all information for the optimizing process. The results are sent to the AIT system, which sends them to the actuating devices and to the control room.

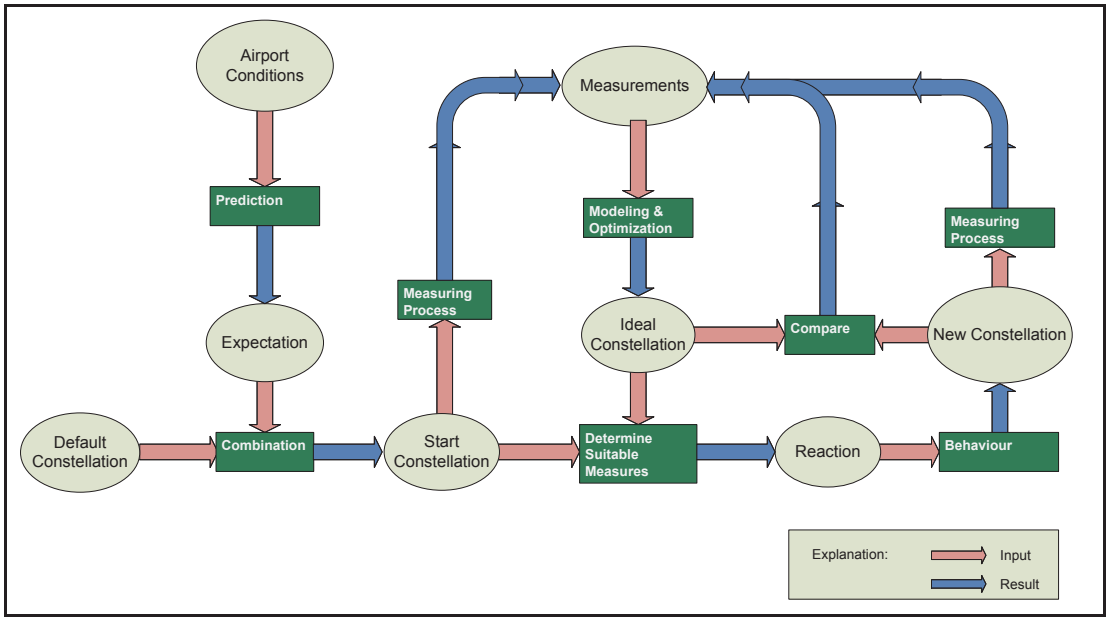


Figure 5: Process Flow Diagram

The process flow diagram (Fig. 5) shows the dependencies in the single steps: based on the airport information, a prediction is calculated to have an expected set of passengers in each group which delivers the start constellation of the system. In the process, all observed and measured values are calculated by the modelling process to achieve an optimal configuration which might be realized or approximated by means of signature or advices. This can be measured again and the control loop can be closed keeping the new constellation as close to the ideal one as possible.

The communication and interoperability between the flow optimization modules and the surrounding software components is implemented with a web service architecture concept based on the respective standards ([1], [10]). This enables a structured and task oriented approach, comprehensive modularity and thus the possibility to think and work in modules, independent implementations and different tool and working environments like languages, operating systems, development systems a. f. m. (cp. [9]).

4 CONCLUSION

For the control process, automated systems lead to higher effectiveness and more security. The more complex constellation of the gates needs an optimized control of the queues. That is realized by video surveillance, automatic length estimation and the optimization of the queuing process.

ACKNOWLEDGEMENTS

The work for this conference paper has been supported by the FastPass project. The research leading to these results has received funding from the European Union Seventh Framework Program (FP7/2007-2013) under grant agreement n° 312583. This publication only reflects the authors' view and the European Union is not liable for any use that may be made of the information contained therein.

REFERENCES

[1] Beaujardiere, J.
Open Geospatial Consortium Inc., Web Map Server Implementation Specification, Project document: OGC 06-042, http://www.opengeospatial.org/standards/wms

[2] Dodge, S., Weibel, R. & Lautenschütz, A.-K.
Towards a Taxonomy of Movement Patterns
Information Visualization. Information Visualization (2008) 7, 240–252.
doi:10.1057/palgrave.ivs.9500182.

[3] Keim, D. et al.
Mastering the Information Age Solving Problems with Visual Analytics
ISBN 978-3-905673-77-7, http://diglib.eg.org

[4] Koole, G.
Optimization of Business Processes: An Introduction to Applied Stochastic Modeling
Department of Mathematics, VU University Amsterdam, March 30, 2010

[5] Liu, H. X. et al.
Real-time queue length estimation for congested signalized intersections
Transportation Research Part C 17 (2009), 412-427

[6] ISO/TC 211 plenary
Resolution 252 ISO/TC 211 / Open GIS Consortium, Inc. co-ordination group
www.isotc211.org/opendoc/211n1451/211n1451.pdf

[7] ISO/TC 211 Vienna, Austria, 1999-03-04/05
Resolution 95 - Terms of reference for the ISO/TC 211 / OGC co-ordination group (TOCG)
www.isotc211.org/Resolutions/resolutn.htm

[8] Na, A., Priest, M.
Open Geospatial Consortium Inc., Sensor Observation Service, Project document: OGC 06-009r6
http://www.opengeospatial.org/standards/sos

[9] Vester, F.
Die Kunst vernetzt zu denken - Ideen und Werkzeuge für einen neuen Umgang mit Komplexität
München: Deutscher Taschenbuch Verlag, 2002.

[10] Vretanos, P. A.
Open Geospatial Consortium Inc. Web Feature Service Implementation Specification
Project document: OGC 04-094, http://www.opengeospatial.org/standards/wfs

[11] Wu, N.
Estimation of queue lengths and their per centiles at signalized intersections
Proceedings of the Third International Symposium on Highway Capacity, Copenhagen, Denmark, (1998)

DETECTION, RECOGNITION AND COUNTER MEASURES AGAINST UNWANTED UAVS

Igor Tchouchenkov, Florian Segor, Matthias Kollmann, Rainer Schönbein[1]
Thomas Bierhoff[2] and Mark Herbold[3]

[1]*{igor.tchouchenkov, florian.segor, matthias.kollmann, rainer.schoenbein}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, SystemTechnologies and Image Exploitation (IOSB), Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[2] *thomas.bierhoff@atos.net*
Atos IT Solutions and Services, Heinz-Nixdorf-Ring 1, 33102 Paderborn (Germany)

[3]*mark.herbold@atos.net*
Atos Nederland B.V, Papendorpseweg 93, 3528 BJ Utrecht (Netherlands)

Abstract

Small Unmanned Aerial Vehicles (UAVs) are getting better, cheaper and more accessible. As a result, they become more and more used in new areas of application. A side effect of this development an increasing number of more or less hazardous incidents with these systems can be noticed. Not only illegal activities as spying and drug transportation, but also disturbance or even simple mishaps which can happen with any technical system can lead to dangerous situations.

In this paper a concept of new Low Altitude Air Surveillance Control (LASC) system is described, which can be utilized to keep urban air space controlled and safe.

The LASC concept is based on multi-sensor detection, localization, tracking and classification or identification of small UAVs integrated in a scalable system providing interactive threat and risk assessment as well as selection possibilities for adequate counter measures.

Keywords: UAV, air, surveillance, counter measure, multi-sensor, distributed system.

1 SITUATIONAL OVERVIEW AND PRESENT PROBLEMS

Unmanned aerial vehicles are an emerging technology with a great potential to disruptively change our lives. They have by far exceed the capabilities of the niche products of radio controlled aircraft models with their ability in terms of payloads, flight duration and range, self-stabilizing and auto pilot capabilities, automated collision protection and video transmission capabilities. Leveraged with new technologies (e. g. high capacity battery packs, low energy consuming motors, diverse sensors and matchbox sized high computing power) small UAVs have started exceeding the toy and entertainment domain while entering more and more real business and scientific applications (e. g. surveillance, reconnaissance and rescue mission support, video production, logistics and delivery, biology, archaeology, etc.) [1], [2], [3]. This development has in parallel been boosted by a constantly rising commercial market for UAVs providing broad accessibility and diversity at a low cost scale.

Furthermore, with the broad availability and low cost aspect of UAVs, a common and unforeseeable use of this technology is expected in the private sector.

As always, each technology comes along with drawbacks and potential for abuse and this is in particular true for UAVs. With their inherent risk of crashing, causing damage

and harm to people, each application has to be assessed seriously in terms of security issues and constraints.

This will in turn demand for new laws, rules and enforcement technologies [4], [5] to keep the low altitude air space controlled and safe. To enforce regulations and timely and efficiently react to violations and emerging security risks, new technologies are required to detect and interfere with these systems.

To find efficient solutions and to provide a future-proof holistic system design a joint project between AToS SE and Fraunhofer IOSB has been set up and the concept for a Low Altitude Air Surveillance Control (LASC) system for control of small UAVs has been developed using multi-sensorial data utilization and background knowledge to assess and evaluate risks and provide situation dependent adequate counter measures.

2 ONGOING RESEARCH AND POSSIBLE SOLUTIONS

A boost of interest for solutions to detect and interfere with small aircrafts has originated from the increase in dangerous or unlawful UAV activities that could be observed recently. On the one hand it concerns the research and development of new sensor concepts which generally admit the detection and location of such systems as far as their payload and, on the other hand, also the search for suitable counter measures because small aircraft cannot be efficiently countered with conventional (e.g. military) systems not only in urban areas, but also in most other cases.

2.1 Detection of small UAVs

A simple but efficient detection and identification technology would be a standardized IFF system deployed in all UAVs. A transponder integrated into the electronics of the UAV collects the current GPS position, altitude, heading, speed and broadcasts the information periodically (or on demand) together with a unique identification number on a specific radio channel. But the standard IFF system is not usable on small UAVs.

Video based airspace surveillance is a promising approach but it comes with challenging requirements – especially for urban areas. The air space must be observed in all directions mostly without any fixed point and working distance to detect a small UAV in a video feed. Existing commercial systems use mostly easy change detection [6] and can often generate false alarms. Fraunhofer IOSB has done comprehensive research on robust computer vision algorithms allowing the detection and primary classification of different flying objects within the range of the sensor in real time [7].

Air space surveillance solutions are available within the visible spectrum of light as well as the infrared spectrum range, allowing the tracking by heat emissions with less sensitivity to weather conditions and poor visibilities.

Sound pattern emitted by UAVs are also representing a promising supplementary source for detection and even classification. Engines and rotors of UAVs are producing characteristic sound emissions, which can be caught by directional microphones [6]. Deploying digital signal processing with matched digital filters adjusted to the characteristic sound frequency spectrum, a UAV sound signal can be unveiled. Its direction is given by the alignment of the directional microphone and can be supported by distance estimation by the signal strength or triangulation. By this, the location of a potential UAV can be determined and based on level of compliance with the characteristic sound spectrum, a UAV classification can be sometimes provided, but the payload cannot be analyzed on this way.

Radar technology is always tailored to its application scene (e.g. detection range, size of object, material, etc.). It shows the advantage of being insensitive to environmental conditions (poor visibility, no light at nighttime, rain, fog, etc.) which makes it applicable

in almost any environmental situation. Long range air surveillance radar operating at 1 to 2GHz (L-Band) for long range (<400km) and large objects (>10m) are not suitable for the LASC system as UAV's small size, its low EM-wave reflecting composite material and low flying altitudes are not providing sufficient radar cross sections to get detectable reflection signals.

More suitable radar technologies are found in the K- and Ka-Band operating with frequencies between 20 and 40 GHz as far as in the W-Band between 60 to 120 GHz. But the detection and recognition of small UAVs with radar are still a topic of research. Applied in urban areas, reflection by infrastructures and building are representing the major challenge for development of appropriate radar surveillance sensor systems.

Passive electromagnetic radiation based detection procedures for UAV are promisingly and partially already in application [8]. The Achilles' verse of every remote controlled UAV is its up-/downlink to the ground control station. Control commands are sent with specific communication technologies from there to the UAV and sensor data like position, system state and in particular video signals are sent back. If the typical frequency bands are scanned, characteristic communication can be identified showing transmission activities with reasonable signal strength. Based on the detected radio transmissions, a rough identification of the drone's type can be retrieved. In conjunction with triangulation capabilities of a cooperating sensor network, the position and heading of a UAV can be determined as well.

If no continuous control- and signal transmission is used as the UAV is autonomously following a preprogrammed GPS or image based flight path, the detection of control- and sensor signals will most likely fail. In this case, more sophisticated technologies needs to be applied to detect electromagnetic background radiation of the UAV emitted by its electronic equipment.

2.2 Counter measures against small UAVs

Possible counter measures against small UAVs can be divided into two categories: "soft" and "hard" measures.

Possible "soft" measures include first of all jamming of remote control link and GPS spoofing. There are already first counter-UAV systems using jamming [9]. The problem of these measures is that the behavior of diverse UAVs can be very different. By jamming some UAVs try to fly near to their start position, but other UAVs can land immediately. Without knowing the behavior, jamming can bring even more problems as a flying unwanted UAV itself – for example if the UAV lands on an unsuitable place or if other important communication systems are unavailable because of the jamming.

GPS spoofing is often efficient [10], but it can be overtaken by remote control of UAV, and fast shifting of GPS position can also force UAV to immediately landing. Afterwards, the spoofing can disturb other important systems, so that it should be used with directed antennas only.

More efficient, but also much more challenging solution is a control overtaking. By success, the UAV of interest can be landed on suitable place. For some WIFI controlled UAV there are usable solutions [11]. Unfortunately, most UAV don't use usual WIFI, and there are a lot of remote control types. By digital control links UAV and remote control unit are matched while configuration, so the hacking is very challenging.

"Hard" interception technologies are based on physical touchdown enforcement with different physical effects and levels of collateral endangerment [12]. These technologies are representing the "last line" of defense and shall only be deployed if any other defense line has failed and collateral damages impacts are evaluated definitively less than the threat itself (explosive or chemical payload).

3 LOW ALTITUDE AIR SURVEILLANCE AND CONTROL CONCEPT

The major functional objective of a LASC system is the surveillance of the today uncontrolled air space below ca. 500m within urban areas. The space beyond the 500m is already been in control by conventional air traffic control mostly based on long-range radar technologies. In order to guarantee seamless information exchange (e.g. some UAVs may enter the high altitude air space and endanger the air traffic), LASC system must be integrated into conventional air traffic control.

The common workflow of LASC is depicted in Figure 1. The LASC system starts with a continuous monitoring of the air space with multiple sensors. Once a sensor detects a flying object, the system will try to locate it (e.g. by triangulation of sensor signals) and ensure tracking by orchestrating multiple sensors. Once the location and tracking is established, the back end IT system of LASC needs to carry out the classification and if applicable the identification of the detected object. Once this is executed, the LASC backend system starts the evaluation of the drone's authorization to fly through the current air space corridor. If no authorization is given, system will prepare reaction options considering the estimated threat classification and risk assessment (disturbing, illegal or endangering). The system provides decision support to a human operator who is in charge of initiating the counter measures. All this activities will be automated to a high degree in order to guarantee a real time execution of the process and to enable high scalability in terms of multiple events.

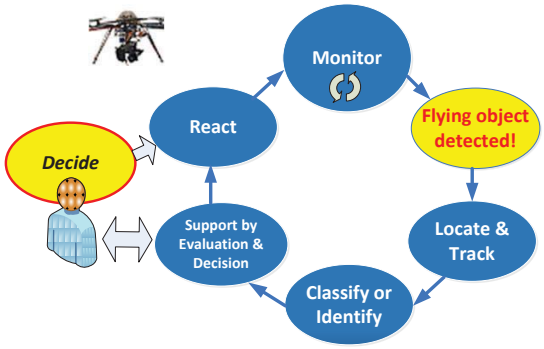


Figure 1: Common workflow of the LASC system

3.1 Flight Activity Monitoring

Distributed LASC system can contain both mobile and stationary LASC sub-systems to monitor flight operations in the low altitude air space (<500m) within a pre-defined area (10m-5km). Depending on the application scheme, the area of the air surveillance is scalable by adding further sensor- and counter measure devices to the LASC systems or new sub-systems. This modular approach will provide a broad field of application ranging from a single building to an entire suburb air surveillance, turning LASC into a flexible and highly adaptable solution. Monitoring flight operations covers detection, identification and tracking. Therefore, a multimodal sensor network based on the technology stack recapitalized in chapter 2.1, must cover a certain part of the controlled air space providing day- and night time operations and coping with bad visibility conditions. The next step after UAV detection is its identification based on sensor signal evaluation or by IFF signals broadcasted by the UAV. Once identified, the LASC system needs to reconcile the information with a LASC based central UAV flight register to see if the UAV's flight is already registered and further information is given covering payload, mission, flight path, destination and operator. If the UAV is registered, its flight register record must be updated by time stamp, current position, altitude and speed for consistent tracking. If there is no suitable UAV record found in

the LASC registration, a new one must be created with all available information (e.g. time stamp, current position, altitude and speed). In order to approve UAV flight authorization, its position needs to be mapped to pre-defined air space corridors, which will show permanent or temporarily valid restrictions or prohibitions. This is essential as different UAVs may have different air space transit rights (e.g. police drone may enter the corridor while an unregistered one may not). The last step of monitoring flight operations is represented by continuous tracking and updating the LASC register's records. Once a UAV is leaving the observation windows of a sensor or a LASC system, it might enter another one. The hand-over of such tracking must be supported by a LASC intelligence, which provides analysing and predictions of flight path and identification of potential sensors, which might detect the UAV soon.

3.2 Air Space Regulation Enforcement

The second objective of the LASC system is the downstream air space regulation enforcement for unauthorized UAV. Therefore, the violation of the air space must be unveiled, which must trigger a threat and risk analysis to determine appropriate reaction and counter measures possibilities. Based on the classification of risks and the availability of interception capabilities in reach, a decision support must provide human operators with suitable enforcement and interception solutions. As the interception is always related to potential collateral risks, it always needs to be initiated, monitored and controlled by a human operator. Therefore, the operator needs access to the sensor network (e.g. video/IR camera) of the LASC system to leverage assessment of the situation and to gain a reliable decision base. Furthermore, he needs GIS support for geo-referenced situational awareness (e.g. show locations of and distances to critical infrastructures in reach). All this needs to be integrated into the command and control center of the LASC system.

The major challenge of the LASC interception operation is the avoidance of collateral damage. Military interception solutions for low-altitude flying objects (e.g. shells or rocket defence systems) are not acceptable in urban areas. The new ways of soft interception techniques as introduced in chapter 2.2 need to be researched and integrated into the LASC solution. Another challenge is the ability of UAVs to takeoff almost everywhere. In case of an abuse, the UAV might take off near its destination reducing reaction time drastically down to seconds. Therefore, most LASC system functionalities must be automated by computer-based support, delivering alerts and decision support to the operator within seconds.

3.3 LASC System Design

The general system design and major building blocks for a full-blown LASC system providing comprehensive monitoring, intelligence and interception functionalities are depicted in Figure 2. Subsequently the functions of the building blocks and their interaction are introduced in order to provide a general picture about the LASC architecture and its mode of operation.

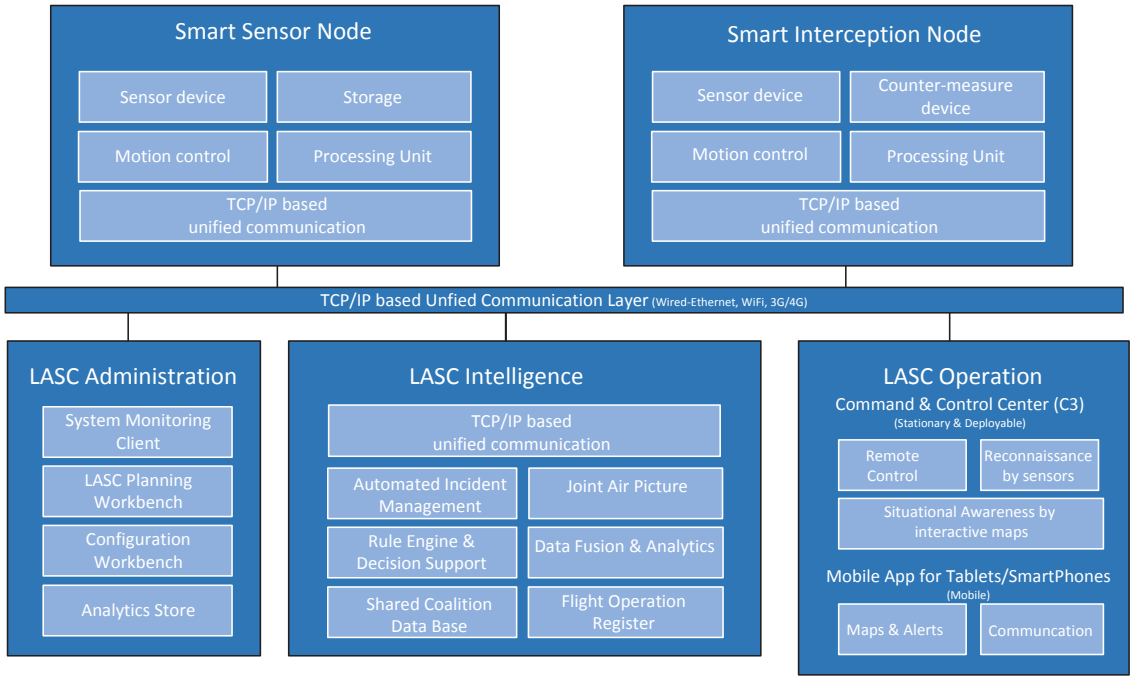


Figure 2: System concept with major building blocks

A field device of the LASC system covers the distributed network of smart sensor and interception nodes. The appropriate choice of the technology is strongly depending on the application and the environmental constraints (free space and the line of sight above roof tops, or covered and thus with a limited line of sight within urban canyons). So deploying various sensors and interception technologies in a multimodal approach must be considered because different technologies are cooperating and extending their capabilities among each other during a parallel operation.

Smart sensor nodes are distributed on appropriate places across the observed area and equipped with data storage and processing units to pre-process sensor raw data using specific algorithms and embedded system technology. This will decrease the data volume to be transmitted into a ground station by far, as only derived smart data in terms of an event needs to be transmitted. The derived information, analyzed data and detected events are provided via web services hosted in the sensor node and end-to-end secured (SSL, VPN) TCP/IP based communication channels. In addition, remote control and diagnose of the sensors is also enabled through the web services.

Smart interception nodes are distributed across the observed area, placed stationary on buildings, infrastructures, balloons or on vehicles (e.g. cars, drones, etc.) to provide deployable interception capabilities. Similar to the sensor nodes also mobile interception nodes can be used. The interception nodes are based on the same subcomponents as the sensor nodes except that the data storage is replaced by a counter measure device. The sensor device, deployed in the interception node, in conjunction with an embedded processing unit will enable automatic interception process preparation and support (e.g. semi-automated aiming and motion control).

Beside the field devices, the LASC system will contain three further major building blocks covering the domains administration, intelligence and operation.

The LASC administration block covers all kind of tools to configure, monitor and maintain the LASC system infrastructure and its components. It comes along with automated system monitoring and observation clients, which enable the survey of the operational state of sensor and interception nodes, allows load balancing of the

intelligence platform and even supports the configuration of the intelligence itself (e.g. setup of analytics chains). Another part of the LASC administration is the LASC planning workbench, which provides simulation-based design support for arranging the sensor- and interception node network across a defined area in order to achieve a certain degree of air surveillance performance.

The LASC intelligence is the core block of the entire system. Its major task is the data fusion of streams from the sensor network and appropriate fast data analytics and complex event processing to provide a joint air picture (JAP) of the observed area in real time. The JAP represents the georeferenced description of all detected and tracked UAVs including all restricted and/or prohibited air corridors. Utilizing a shared coalition database and the flight operation register, the LASC tries to identify a detected UAV automatically. If this fails, the LASC intelligence provides all available information (mainly video streams) for manual identification by a human operator using decision support tools. Once an air space violation is unveiled, an automated incident management provides several options for the operator to react appropriately to the incident. This incident manager utilizes a rule engine including pre-defined decision trees, risk assessments and potentially applicable counter measure nodes in reach. Once the LASC intelligence platform is deployed on virtualized server infrastructure, its service-orientated architecture provides the performance to handle tremendous amount of sensors (>1000), process their data in real time and provide all kind of information's to multiple authorized operation.

The last building block presents the operation clients of the LASC system, which can be distinguished into stationary/deployable command and control centers (C3) and mobile apps supporting mobile access to the LASC intelligence information system. It can be developed e.g. based on AMFIS ground control station [13]. All clients are connecting to the LASC intelligence platform via secured end-to-end encrypted (VPN, SSL) TCP/IP based communication channels and utilize its web service provision to access data and control. The C3 clients are based on rich internet or desktop applications that provide interactive maps visualizing the joint air picture to support situational awareness. Once an incident is detected, alerts are shown and the feature icon of the detected incident is highlighted to focus the operator's attention. The operator can request decision support from the LASC intelligence and real time video streams from optical sensors in the reach. All counter measure activities can be initiated and controlled by the C3 client software and are sent via the LASC intelligence control proxy to the selected interception node.

For mobile solutions (e.g. police man equipped with tablet, smartphone) client apps running on smart phones and tablets are provided to inform the operator about incidents in the near environment and/or transmit instruction for further action (e.g. evacuation).

4 CONCLUSION AND FUTURE WORK

The LASC system concept includes multi-sensor detection, localization, tracking and classification or identification of small UAVs integrated in a scalable distributed system. Beneath the detection, the classification of threats and the safe identification and separation of legal UAVs is a challenging task. Not only the current position and the type of a suspicious UAV must be recognized to assess the risk – much more important in these cases is the payload. A selection of suitable "hard" and "soft" counter measures for different situations and threats is based on comprehensive predictive analysis of danger of UAV and its payload. Preferred are "soft" countermeasures like communication based mission distortion and interruption. LASC system provides fast interactive threat and risk assessment as well as selection possibilities for adequate counter measures supported by user-friendly interface.

The scalable architecture of the distributed LASC system has open interfaces wherever it is possible and includes data analysis and fusion modules, coalition shared database as well as interactive visualization and decision support components. The LASC system must be integrated into conventional air traffic control to prevent possible incidents because of intersecting air spaces.

The system concept was developed in a joint project between AToS SE and Fraunhofer IOSB. In the next steps major components of LASC as well as system framework will be developed and tested in different situations.

REFERENCES

[1] Vasagar, J. (2014). *DHL to use 'paracelcopter' drones for delivery.* Finanical Time http://www.ft.com/cms/s/0/c00bd8e2-44ad-11e4-bce8-00144feabdc0.html#axzz3RtVgsK6d

[2] Wikipedia, *Amazon Prime Air* (2013). http://en.wikipedia.org/wiki/Amazon_Prime_Air

[3] Molina, P., Eulalia, M. et. al. (2012). *Drones to the Rescue*. InsideGNSS Journal, pp. 37-47.

[4] Lardinois F. (2015). *FAA proposed rules to open sky to some commercial drones*. TechCrunch. http://techcrunch.com/2015/02/15/proposed-faa-rules-will-open-the-sky-for-some-commercial-drones-but-delivery-drones-remain-grounded/

[5] Federal Aviation Administration (2015). *Overview of small UAS Notice of Proposed Rulemaking.* http://www.faa.gov/regulations_policies/rulemaking/media/021515_suas_summary.pdf

[6] DeDrone (2015). *Multi-Sensor-System zur Erkennung von Drohnen*. http://www.dedrone.com/de/dronetracker/drohnen-alarm-system

[7] Fraunhofer IOSB. *Experimental setup for object recognition and tracking*. http://www.iosb.fraunhofer.de/servlet/is/24431/

[8] DDC LLC (2015). *The Basic Drone Detection System*. http://www.ddcountermeasures.com/products.html

[9] Unmanned System Technology (2015). *New Anti-UAV Defence System Successfully Detects, Tracks, & Disrupts UAVs*. http://www.unmannedsystemstechnology.com/2015/06/new-anti-uav-defence-system-successfully-detects-tracks-disrupts-uavs/

[10] The University of Texas at Austin (2015). *Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV*. http://www.ae.utexas.edu/news/features/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav

[11] Pleban, J.-S., Band, R. and Creutzburg, R. (2014). *Hacking and securing the AR.Drone 2.0 quadcopter - Investigations for improving the security of a toy.* In Proc. SPIE 9030, Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications.

[12] Tchouchenkov, I., Segor, F., Schönbein, R. (2012). *Einsatzmöglichkeiten und Abwehr kleiner unbemannter Fluggeräte*. POLIZEI-heute, Nr. 3.

[13] Bürkle, A., Segor, F., Kollmann, M. and Schönbein, R. (2011). *Universal Ground Control Station for Heterogeneous Sensors*. In Journal On Advances in Telecommunications, IARIA, Volume 3, Numbers 3 & 4, pp. 152–161.

CARONTE

CREATING AN AGENDA FOR RESEARCH ON TRANSPORTATION SECURITY

Joachim Kochsiek[1] and Maximilian Schellert[2]

[1] Dipl.-Ing. Dipl.-Wirt.-Ing. (FH) Joachim Kochsiek

Joachim.Kochsiek@iml.fraunhofer.de

Fraunhofer Institute for Material Flow and Logistics

Joseph-von-Fraunhofer-Straße 2-4

44227 Dortmund (Germany)

[2] Maximilian Schellert M.Sc.

Maximilian.Schellert@iml.Fraunhofer.de

Fraunhofer Institute for Material Flow and Logistics

Joseph-von-Fraunhofer-Straße 2-4

44227 Dortmund (Germany)

Abstract

A security project to investigate future research priorities for protecting Europe's land transport sector.

The Project CARONTE is one of the last FP7 projects and is supported by DG Migration and Home Affairs. It aims to create a future research agenda on land transportation security. For the agenda the partners identify relevant existing and upcoming gaps and threats to the land transportation sector. Needs for future research and policies will base on the identified gaps and requirements by authorities and the transport industry together with consideration of already existing research projects (active, finalised or planned). It will define agendas for still missing solutions or research fields, considering the important ethical, social and legal aspects of security measures for acceptance and to assure freedom. Main target is to assure or increase security respecting the needs of easy and affordable transport.

Keywords: Security, Research, Agenda, H2020, Land Transportation, Road, Rail, Inland Waterway, Interfaces

1 THE CURRENT SITUATION

Europe and the whole world is threatened by terrorism and crime, although the number and severeness of attacks differs very much from country to country. The AON Terrorism & Political Violence Risk Map [1] of terrorism indeed shows for some Member states of the European Union a relevance of terrorism. The recent incidences in France (attack on the editorial department of Charlie Hebdo and a cyber-attack on France TVMonde) and Copenhagen (bomb attack in a café) and also a couple of threats for bombings in Germany show the relevance. Sooner, the 2004 terrorist

attacks against Madrid's train station and the 2005 ones against London's buses claimed the lives of 191 and 52 innocent civilians, respectively. In Russia frequently Underground systems are targets of attackers. Although not all the described incidences affect transport directly they show the relevance of terrorism on the one hand and indirect consequences on transportation on the other hand. Passenger transport in Paris got very complicated due to traffic interrupts and police blocks after the Charlie Hebdo attack.

Also Criminals consider the transport sector and its components to be an easy target. For example, theft of high value and high risk products moving through supply chains costs businesses about €9 billion a year in Europe [2] and TAPA (Transported Asset Protection Association) frequently reports about rising cargo theft, increasing organisation of crime with better information about interesting (value) freight and increasing violence against truck drivers [3]. According to conversation with the German Federal Police, the most important activities from their respect in land transportation are the increasing violence in passenger rail transport and the protection of critical infrastructures.

2 THE CURRENT ACTIVITIES

The European commission has published a large number of policies tackling security in the past years. The basis is the European Agenda on Security which was first published in 2010 [4] and recently updated on 28. April 2015 [5]. It mentions activities on Cyber, CBRNE, counter radicalism and recruitment, counter organised crime, resilience among others. For many details of security activities special policies are also published, namely

- EU approach to the detection and mitigation of CBRN-E risks [6]
- An open and secure Europe: making it happen (covers migration) [7]
- Customs Risk Management and Security of the supply chain [8]
- Cyber Security Strategy and Proposal for Directive to ensure a high common level of NIS [9]
- A European program for Critical Infrastructure protection [10]
- Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response [11]

In these policies a large number of activities are set and tracked by the EU. In the Seventh Framework Research Program and the HORIZON 2020 program a large number of research projects are introduced and realized tackling the contents of the policies. Currently the CARONTE partners are analysing these activities to deduce relevant future activities or already covered needs. The research projects cover risk assessment, protection measures for infrastructure, vehicles etc. detection methods for dangerous materials, human beings or drugs, processes for securing of assets, sites, transport, cyber- or ICT-security measures among others.

A search on the CORDIS pages in the FP7 projects has shown more than 140 project where the key words "security" together with transport, passenger or freight can be found (including CARONTE). In H2020 already 15 projects are active contain these keywords. After the 9/11 incidences more than 400 regulations and initiatives for trans-atlantic shipments were introduces like ISPS, modified customs code , AEO, CSI, C TAPT,... The 100% scanning of containers which are shipped to the US was postponed from Mid 2012 to 2014 but is not yet active. Many experts do not see any use of this obligation. The private initiative TAPA, founded by shippers and forwarders who have been tackled by crime is efficient, setting up binding regulations for forwarders in the

respective transport-contracts for example for safeguarding transhipment sites or warehouses or by defining processes and standards to protect vehicles and to control.

3 THE EXISTING AND EMERGING RISKS

Identifying existing and especially emerging risks is not easy and even dangerous. Looking at terrorism which is always surprising (remember 9/11), we must consider that even a low likelihood of an incidence can cause urgent consequences on life, society, economy and so for.

The CARONTE project came to more general statements, after having a couple of approaches assessment and collecting relevant information from extern experts and among the partners.

General:

- Currently, Islamic terrorism in Europe, especially from Al-Qaida, is low, but experts think that this is a preparation period for an unexpected larger strike
- Daily business for the logistics and freight sector is cargo theft or smuggling and (sometimes) industrial espionage.
- Rising violence
    - in cargo theft
    - in attacks on passengers (for theft / robbery but also violence against minorities, foreigners or weak persons)
- When attacking land transport, terrorists mostly targeted metro systems, commuter railways or buses to raise a lot of attention and to cause a large number of fatalities
- Bombing and armed assault are largely preferred by terrorists, followed by sabotage and arson.
- Cyber-attacks are a new instrument used often by economic criminals, saboteurs or hostile nations but are seen as a future mean also for terrorists (as recently shown). It is conceivable that cyber-attacks are used by foreign countries to hurt an infrastructure.

Especially looking at Cyber-Security the partners come to following statements:

- Cyber-crime is a rising problem and could especially affect critical infrastructures such as energy supply or the ICT-Systems
- Cyber-attacks occur on two fronts:
    - the sometimes very old ICT-systems with a design not respecting current and (urgently) needed ICT-Security
    - failures in software codes which are expected to be 1-25 in 1,000 columns and which can be gates for cyber attacks
- Rising dependency on ICT-Systems and radio transmission makes land transport and society more vulnerable, especially if the functioning of the transport system is dependent on central control systems like rail or transport hubs.
- The interconnection of systems makes the transport sector more and more vulnerable. In particular, a lack of information flow can stop goods supply and can cause follow-up problems such as lack of food, energy or medical supplies
- Humans are a special aspects in Cyber-Security

- Personal awareness
- Personal training and knowledge
- Complexity of IT-Security which leads to
- Most users are not experts of IT and IT-Security but are often forced to learn many details in dealing with the systems next to their core business
- Access to networks with mobile devices (private or company owned) which are not controlled by security experts

⇨ Many sources of uncertainty often accidentally

Indeed there are also some findings and facts which should be taken in mind which compensate or relative the security threats:

- In most parts of Europe, land transport networks are very dense, so bypassing of weak points when they are interrupted of attacks is often possible
- The public transport companies and authorities have made large efforts to improve the security, especially in terms of the secure feeling of passengers using different methods (e.g. CCTV, security guards, “friendly”, smooth design of stations, places or vehicles)
- Terrorist attacks have not been reported in the supply chains in Europe
- Dirty bombs have not been reported (although this threat is discussed very often).

4 THE WAY FORWARD IN CARONTE

Currently (June 2015), the partners are finalizing the gap and requirement analyses and have already begun to define “visions” or development directions for the future research agenda. The visions or development directions are currently very free and wide and are based on the experiences of the partners’ background and the interims experiences from the CARONTE project. Later these visions will be adjusted to the gap and requirements and already existing results from research and existing policies.

The work will be finalized in February 2015 and we will have a final conference in Brussels also in that month. Up to the Future Security Conference some more interims results will be ready to be presented.

REFERENCES

[1] 2015 Terrorism & Political Violence Risk Map, http://www.aon.com/terrorismmap/Aon-TPV-Map-Country-Risk-Ratings-2015.pdf (last visit 2. June 2015)

[2] (DVZ) Deutsche Verkehrszeitung, 16.11.2012

[3] TAPA Association http://www.tapaemea.com/ (last visit 17. October 2014)

[4] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU Internal Security Strategy in

Action: Five steps towards a more secure Europe; COM(2010) 673 final, Brussels, 22.11.2010

[5] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EU ROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - The European Agenda on Security; COM(2015) 185 final Strasbourg, 28.4.2015

[6] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - on a new EU approach to the detection and mitigation of CBRN-E risks; COM(2014) 247 final, Brussels, 5.5.2014

[7] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - An open and secure Europe: making it happen; Brussels, COM(2014) 154 final, Brussels 11.3.2014

[8] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE - on Customs Risk Management and Security of the Supply Chain; COM(2012) 793 final, Brussels, 8.1.2013

[9] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace; JOIN(2013) 1 final, Brussels, 7.2.2013

[10] COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection; COM(2006) 786, final Brussels, 12.12.2006

[11] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response; COM(2013) 941 final, Brussels, 15.1.2014

GENERATION DEPENDENCE OF COMMUNICATION DEVICE VULNERABILITY TO INTENTIONAL ELECTROMAGNETIC INTERFERENCE (IEMI)

Ch. Adami [1], M. Joester [2], T. Pusch [3], M. Suhrke [4], A. Taenzer [5]

[1] christian.adami@int.fraunhofer.de
[2] michael.joester@int.fraunhofer.de
[3] thorsten.pusch@int.fraunhofer.de
[4] michael.suhrke@int.fraunhofer.de
[5] hans-joachim.taenzer@int.fraunhofer.de
Fraunhofer Institute for Technological Trend Analysis INT, Dept Nuclear and Electromagnetic Effects, Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

Smartphones and tablet computers got impressively popular thanks to their intuitive multi-touch and gestures control and fast-to-catch graphical information presentation. These features make such devices attractive for usage as man-machine interface of Supervisory Control and Data Acquisition (SCADA) in critical infrastructures (CI). As a disadvantage, they are becoming potential targets of IEMI compromising their functionality to support illegal activities ranging from criminal to terroristic attacks. Tests of GSM mobile phones in the past already have shown a high vulnerability against High Power Electromagnetics (HPEM). Present-day technology offers additional frequency bands for wireless communication, a GPS receiver, a large set of integrated sensors and sophisticated touch-sensitive displays with increasing resolution. Radio frequency (RF) immunity tests with smart phones and tablet computers representing the state of the art in mobile computing technology of 2011-2014 give a picture of generation dependent vulnerability as well as general RF susceptibility related to design concepts and coupling paths. The tests show that IEMI can disturb smart phones and tablets in a broad frequency range. New functionality also opens new coupling paths for IEMI leading to higher vulnerability of the devices.

Keywords: IEMI, HPEM, CI, smartphones, tablet computers, vulnerability.

1 INTRODUCTION

Until 2007 wireless connections in mobile communication and mobile computing were separated into two worlds, the worldwide GSM network and local Wi-Fi networks. The GSM network provided telephony, Short Message Service (SMS) and a down-graded internet access with the Wireless Application Protocol (WAP). Mobile computing was defined by laptops accessing a LAN or the internet via a Wi-Fi link.

Smartphones with touch screens eliminating mechanical keys became possible when the computing power of a single-chip computer (System on a Chip, SoC), in combination with lithium-ion batteries, was sufficient for graphical user interface (GUI) with acceptable battery life. Motion sensors, video cameras and a GPS module round off the concept of using environment parameters and position for personalized and location-based information processing. Another class of device, the tablet, combines smartphone development with developments in laptops and notebooks.

To meet the demand for exchanging larger data volumes, radio modules for fast Wi-Fi and the mobile communications standard 4G and also as fall-back alternatives for the predecessors 3G and 2G networks have been installed in smartphones and tablets. For wireless near-field applications such as audio transmission and identification for

cashless payments, Bluetooth and NFC (Near Field Communication) modules are often integrated as well.

In an industrial setting, process parameters can be monitored and controlled with mobile computers, e.g. on a production line which means that tablets and smartphones become part of CI. The benefits of processing situational and personal data have been recognized also in the defence area, examples being the use of civil equipment in the U.S. Army programme “Nett Warrior”, and a military smartphone for networking between soldiers which is being developed on the basis of a civil series device.

In many deployment scenarios, maintaining the device function is highly important, even security-critical. Studying susceptibility to potential interference therefore deserves high priority. Looking more closely at the technology of touch screens, it is possible to presume susceptibility to IEMI. At many frequencies, radio modules inherently allow energy into the electronics via antennas. By blocking data exchange, interference sources on the reception frequencies could therefore seriously limit the functionality required of the tablet or smartphone. There is also the possibility of permanent damage to the radio modules or the remaining electronics.

To investigate this suspected IEMI vulnerability more closely, Fraunhofer INT asked how different generations of smartphones and tablets behave when irradiated with high-power radio frequency (RF) signals with field strengths up to three decades above those prescribed in the tests for electromagnetic compatibility (EMC) that such devices have to pass prior to market launch. Investigated were entry-level and mid-priced devices. Tests were carried out in Fraunhofer INT’s TEM waveguide. The tested frequency range covered many frequency ranges of the radio modules installed.

Vulnerability of IT systems including wired networks to IEMI has been investigated in depth previously (see e. g. [1-3]). There are less investigations on mobile and wireless devices [4-6].

In a first test run we selected smartphones and tablets from generations 2012 and 2013 [7]. They were compared both to tests of GSM mobile phones from 2001 [4] and to a second test run with smartphones and tablets from generation 2013/2014. The devices are described in Section 2 together with the test setup. Results are discussed in Section 3. We conclude that the IEMI vulnerability of mobile devices increases also due to increasing their complexity and their qualification to be used for control of CI should be assessed thoroughly.

2 DEVICE SELECTION AND RF IMMUNITY TEST DEFINITION

Smart handheld devices are a young technology started in 2007, but all electronic and mechanical parts show impressive improvement steps within roughly 12 months periods. So it is fair to compare devices manufactured in year distances and to expect distinguishable RF immunity performance differences related to the technical development. As there are test results available of older GSM phones from manufacturing years between 1997 and 2001 [4], these results have been integrated into the present study of generation dependence of vulnerability against IEMI.

2.1 GSM phones of manufacturing years between 1997 and 2000

Table 1 gives an overview of the devices tested during a test campaign with nine GSM phones between 2000 and 2001 [4]. The selected phones, introduced between 1997 and 2000 by four different manufacturers, are equipped with single GSM band receivers up to three GSM bands. New GSM data services have been integrated with the upcoming General Packet Radio Service (GPRS) at that time in year 2000.

Table 1: Selected GSM phones of generation 1997-2001

GSM Phone	#1	#2	#3	#4	#5	#6	#7	#8	#9
Manufacturer	A	A	B	C	C	A	A	D	B
Introduction	1997	1997	1998/99	1999	2000	2000	2000	2000	2000
GSM band	900	900	900, 1800	900, 1800	900, 1800	900, 1800	900, 1800	900, 1800	900, 1800, 1900
Fax/Data	▲	▲	▲	▲	▲	▲	▲		▲
SMS	▲	▲	▲	▲	▲	▲	▲	▲	▲
WAP-Browser					▲		▲		▲

2.2 Entry level and mid-price smart phones of manufacturing years 2012 and 2013

Ten years later the spectrum of available mobile communication devices is much broader as many manufacturers supply the market with model upgrades while the predecessor model is still sold from stock. Table 2 shows the test devices selected for testing entry-level and mid-price smart phones [7]. The now always-present four bands GSM service functionality of the phones is accompanied by many other services like Global Positioning System (GPS), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE), Wi-Fi in two frequency ranges, Bluetooth, Near Field Communication (NFC), and even FM radio. The entry-level smart phones are made of older SoCs and displays compared to the mid-price smart phones.

The enriched functionality of the smart devices moved from pure telephony to mobile computing, multimedia and text-based chat communication with permanent connection to the internet.

Table 2: Selected entry level and mid-price smart phones of generation 2012 and 2013

Smart Device	Phone #1	Phone #2	Phone #6	Phone #7	Phone #8
Manufacturer	E	F	G	H	E
Introduction	2012	2012	2013	2013	2012
GSM band	850, 900, 1800, 1900	850, 900, 1800, 1900	850, 900, 1800, 1900	850, 900, 1800, 1900	850,900, 1800, 1900
UMTS band	900, 2100	900, 2100	850, 900, 1900, 2100	850, 900, 1900, 2100	850, 900, 1900, 2100
LTE band	-	-	-	-	-
Wi-Fi	2.4 GHz	2.4 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz
Bluetooth	▲	▲	▲	▲	▲
GPS	▲	▲	▲	▲	▲
Display	TFT 3,2” 240x320	TFT 3,14” 240x320	TFT 4,6” 1280x720	TFT 4,2” 1280x768	AMOLED 4,8” 1280x720

All smart phones and tablets have a capacitive multi-touch sensitive display and a mechanical home button besides a mechanical on/off switch and a volume control via mechanical switches. Some devices are equipped with NFC or FM radio transmitter modules. The frequencies used by these services are outside the test frequency range and therefore neglected in the feature tables.

2.3 Mid-price tablets of manufacturing years 2013 and 2014

In a third test run tablet PCs were in focus of investigation. Tablets combine the mobile computing philosophy of laptop computers with the amenities of touch control and multimedia capabilities of mobile SoCs and high-resolution displays. This kind of devices is the main candidate to be integrated into critical infrastructure.

Several 7” and 10” tablets of manufacturing years 2013 and 2014 have been tested together [7]. One 10” tablet was introduced in 2011, but with technology of estimated 2013 generation. The 2014 generation has been equipped with mobile network capabilities beside Wi-Fi as an additional feature.

Table 3: Selected tablet PCs of generations 2013 and 2014

Smart Device	Tablet #1 10”	Tablet #2 10”	Tablet #3 7”	Tablet #4 7”	Tablet #14 10”	Tablet #15 7”	Tablet #16 10”	Tablet #20 10”
Manu-facturer	E	I	I	I	J	K	I	L
Intro-duction	2013	2013	2013	2013	2014	2014	2014	2011
GSM band	-	-	-	-	850, 900, 1800, 1900	850, 900, 1800, 1900	850, 900, 1800, 1900	850, 900, 1800, 1900
UMTS band	-	-	-	-	900, 1700, 1900, 2100	850, 900, 1900, 2100	850, 900, 1900, 2100	850, 900, 1900, 2100
LTE band	-	-	-	-	700, 800, 850, 900, 1700, 1900, 2100, 2600	800, 1800, 2100, 2600	800, 900, 1800, 2100, 2600	-
WiFi	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz	2.4 GHz	2.4 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz
Bluetooth	▲	▲	▲	▲	▲	▲	▲	▲
GPS	▲ + GLONASS	▲	▲	▲	▲ + GLONASS	▲ + GLONASS	▲ + GLONASS	▲
Display	TFT 10,1” 1280x800	IPS 10,1” 1920x1200	IPS 10,1” 1280x800	IPS 10,1” 1280x800	TFT 10,1” 1280x800	IPS 10,1” 1920x1200	IPS 10,1” 1280x800	IPS 10,1” 1280x800

2.4 RF immunity test definition

All devices have been tested in the frequency range between 150 MHz and 3425 MHz in an open TEM waveguide using pulse modulated RF. The RF is switched active 1 µs with a pulse repetition frequency of 1000 Hz. The pulsed field increased within a time of 20 s from approximately 100 V/m to a maximum value in a saw-tooth like ramp. In case of failure occurrence during the field ramp, the field was switched off manually already at this threshold.

During the test runs with the simple GSM phones the displays of the phones were observed with a video camera. Any changes in display quality and readability as well as unexpected notifications have been considered as failures. After each test run the network connectivity was tested to evaluate the communication transmitter functionality.

In smart devices much more functionality is active. To observe these devices with a video camera during the test runs, either a video app played a video file in an endless loop, or the built-in slide show function of the picture gallery app in endless loop was activated. Alternatively a messenger app was opened in test input mode, showing the virtual keyboard waiting for text input. Any changes in application functionality, e.g. video interruptions and random text input as well as display quality degradation have been considered as failures. As possible, the screen saver function was disabled or set

to the maximum possible time. After each test run the network connectivity of smart phones was checked.

3 TEST RESULTS

All results in the test frequency range between 150 MHz and 3425 MHz were plotted in result charts, normalized to arbitrary units. The following diagrams keep the same scaling to allow a comparison of the results. The red solid line in the charts reflects the maximum field strength reached by the RF test site during the test run.

3.1 Test results of generation 1997-2000 GSM phones

Fig. 1 summarizes the test results of the GSM phones. The observed failures were mainly related to the LCD, changing to black or completely losing contrast. Permanent firmware hang-ups and latch-up with high current consumption were observed as well. Beside the phones 4, 6, which were damaged with the very first test frequencies, even other phones were damaged during the tests and, for example, lost the sensitivity for the GSM communication frequency permanently. The test frequency ranges of these devices acquired successfully before damage are marked with bars in the lower part of the diagram with the same device related colour as the result symbols. The red solid line indicates the maximum field strength reached by the RF test site during the test runs. The dashed dark blue line is the average failure threshold of all tested phones for a set of frequency ranges, the GSM ranges 700 MHz – 1000 MHz and 1700 MHz – 2000 MHz , and the non-GSM ranges 150 MHz – 700 MHz, 1000 MHz – 1700 MHz, and 2000 MHz – 3425 MHz. In the GSM ranges front-door coupling through the antenna is expected, in the other frequency ranges back-door coupling into the circuitry via metal structures. In addition, the GSM bands are shadowed for better identification in Fig. 1.

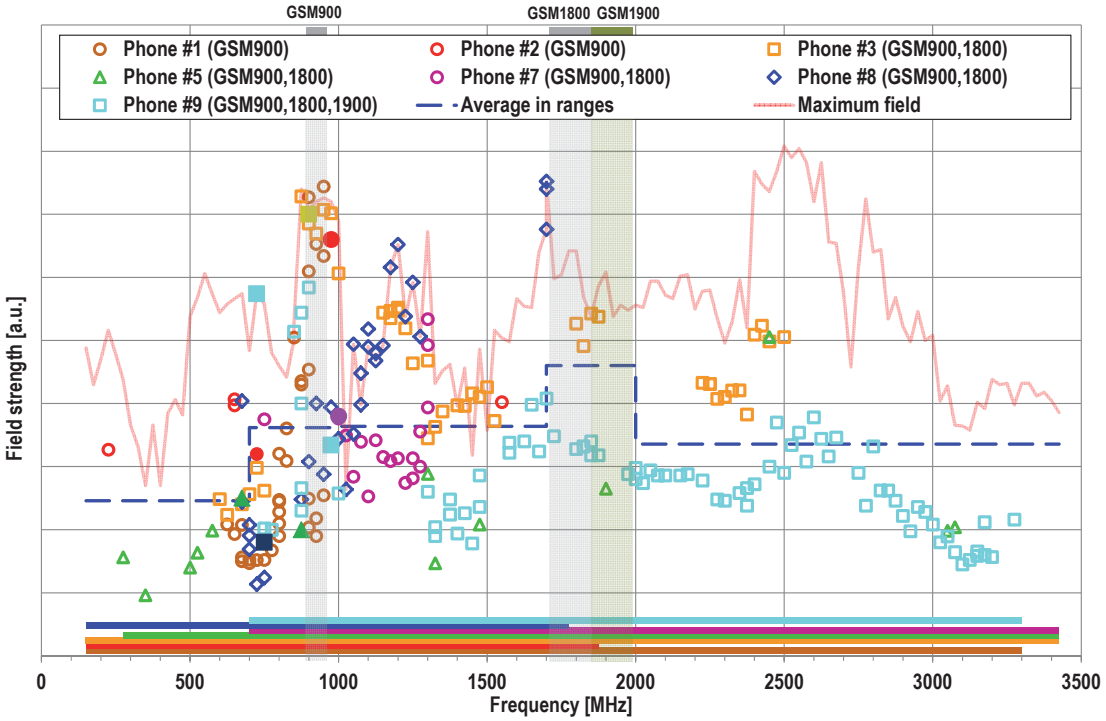


Fig. 1: Test result diagram of generation GSM phones 1997-2001

Phones 2, 4, 5, 6, 7, and 9 were damaged during the tests, marked with a filled symbol at the related frequency and field strength in Fig. 1. Phones 2, 5, and 9 are marked as damaged two times each, because a spare device has been tested. Obviously most of

the phones were damaged in the frequency range 700 MHz and 1000 MHz, this might be related to front door coupling via the antenna. One manufacturer is represented by cycle symbols in different colours for different phone models and a cluster of failures can be found in the lower frequency range. The squares, representing GSM phones of another manufacturer, show a spread failure occurrence in the whole frequency range. It might be a hint for an immunity performance related to the design of the phone.

3.2 Test results of generation 2012 and 2013 smart phones

The smart devices have been tested in combinations in the TEM waveguide like shown in Fig. 2. Each device executed an app playing a video or waiting for key strokes on the virtual keyboard on the screen.

Fig. 2: (a) Smart devices placed in test position in the TEM waveguide and (b) random touch activation by RF during test runs.

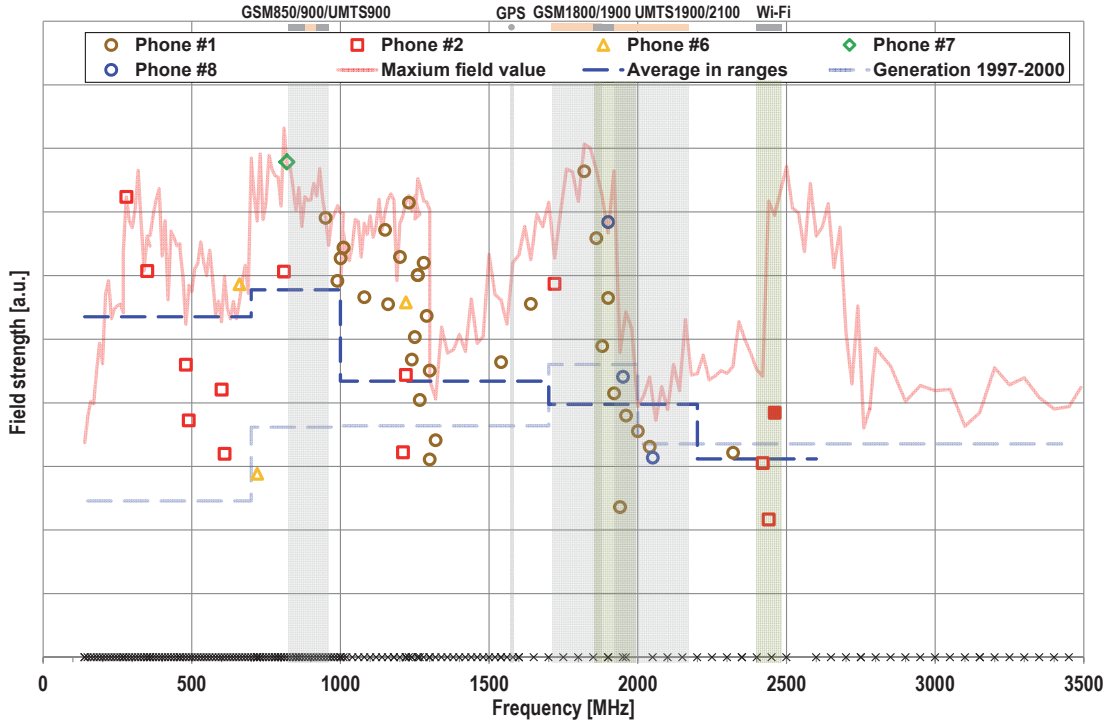


Fig. 3: Test result diagram of entry level and mid-price smart phones 2012-2013.

Again the test frequency range from 150 MHz to 3425 MHz has been plotted in a chart shown in Fig. 3. The observed failures can be grouped to two failure pictures related to the smart phone generation. The entry-level smart phones 1 and 2 stopped the video application via touch commands or got random text entries like as in the observation screenshot in Fig. 2. No other kind of failures occurred with these phones. The mid-price smart phones showed display quality degradation like lost synchronisation or

black display. The dashed blue line is the average failure threshold of all tested phones for a similar set of frequency ranges as in the GSM phone test. To compare these levels, the result of the GSM phones is plotted in light blue in the same chart.

In average the smart phones tested here are obviously less susceptible in the frequency range up to 1700 MHz. In the Wi-Fi range phone 1 and 2 showed failures, maybe by front door coupling, in the upper frequency range no smart phone failed. Just one smart phone, smart phone 2 has been damaged, marked with a filled red square at 2460 MHz. The Wi-Fi transmitter broke by irradiating RF within the unit's operating frequency range.

3.3 Test results of 2013 and 2014 tablet PCs

The 7" and 10" tablets are physically larger than the smart phones. Hence the tests have been performed in another test position within the TEM waveguide. The reachable maximum field levels are smaller by a factor of 2 to 3. Looking at the results of the tablet tests in Fig. 4, all tablet PCs are more susceptible than the smart phones tested in the previous test run. The dashed dark blue line indicates the average fault level of all tablet PCs, the medium light blue line the average failure level of the smart phones. In the frequency range below 1700 MHz the tablets are similarly susceptible as the GSM phones, marked with the lightest blue line. In the upper frequency range two of the tablets are even more susceptible, the cluster of failures for tablets 15 and 16 around Wi-Fi and LTE2600 frequencies denotes a possible front-door coupling. There is another failure cluster in GSM/LTE frequency range around 1800 MHz with the same possible reason.

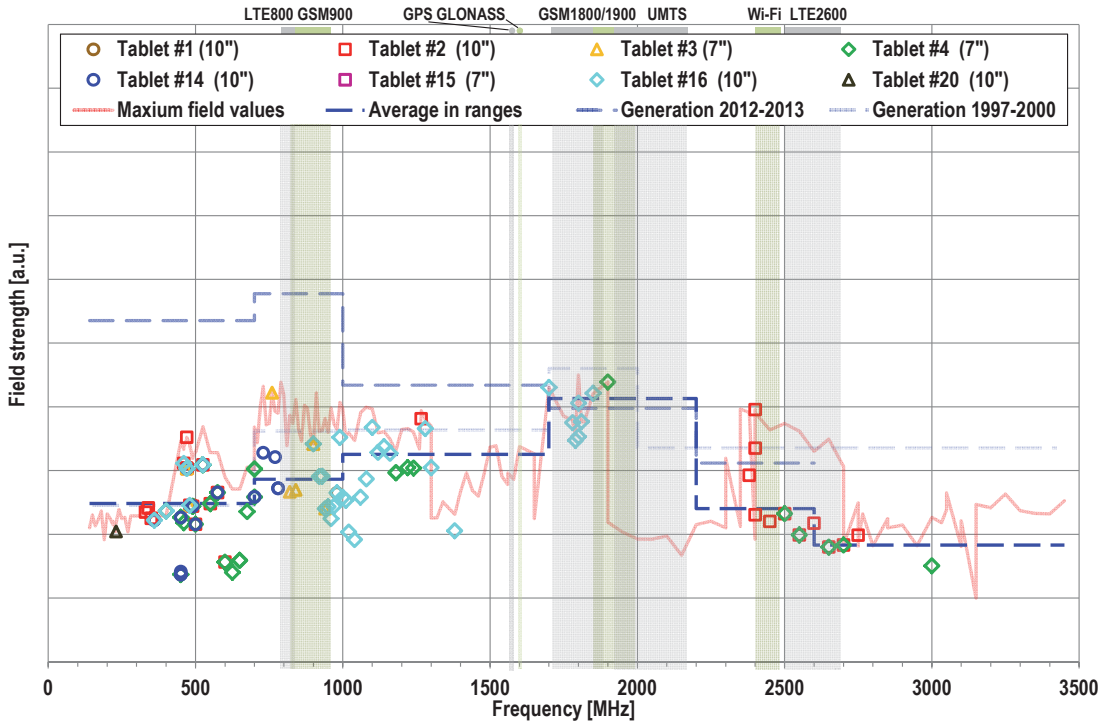


Fig. 4: Test result diagram of tablet PCs, market introduction 2013 and 2014.

The dimensions of the tablets could be related to resonance frequencies of the housings. For 11" tables a half wavelength would correspond to a range from 480 MHz to 850 MHz, for 7" tablets to a range from 650 MHz to 1300 MHz. One can see that a main failure cluster for 10" tablets can be found in the range from 400 MHz to 900 MHz, a tendency for failure clustering in case of the 7" tablets in a slightly higher frequency range.

4 CONCLUSION

With the simplification, that any failure leading to degraded functionality in the intended usage is not acceptable for an operator, we saw two tendencies of smart device susceptibility compared to the simple GSM phones. The tested smart phones with 3.5" to 4.5" display size got less susceptible below 1 GHz, but with growing device size represented with 7" and 10" tablet PCs and additional communication frequencies this advantage got more than compensated towards a worse RF immunity. Fairly spoken, the devices got much more complex and more functions have been considered in the immunity performance evaluation during testing. With every development step of smart devices more frequency bands have been implemented into the devices and therefore RF in plenty of frequency ranges can reach the electronics via antennas as front-door coupling. Many of the tested GSM phones got damaged permanently, but only one smart device has been damaged. This might be related to the miniaturization of electronic units and integration of additional protection circuitries into Integrated Circuits (ICs). Tablets are clearly more susceptible than the smaller smart phones. Looking to the results of the tablet tests, there seems to be a correlation of RF to the size of the devices as expected for back-door coupling. During RF exposure, we observed random touch entries and it might be impossible to control a touch screen device in that situation. Due to the lack of keypads with mechanical keys, a CI operator would not be able to use the device anymore. As we have found quite different susceptibilities of the tested devices, a solution would be at least to identify robust devices by IEMI tests and to use them in security-critical scenarios if they cannot be avoided at all.

REFERENCES

[1] Hoad, R., Lambourne, A., Wraight, A. (2006). *HPEM and HEMP susceptibility assessments of computer equipment*. EMC Zurich 2006. 17th International Zurich Symposium on Electromagnetic Compatibility, pp. 168-171.

[2] Braun, Chr., Clemens, P., Schmidt, H.-U., Suhrke, M., Taenzer, H.-J. (2009). *Susceptibility of Network Components to Pulsed Medium Power Microwave Fields*. EMC Zurich 2009. 20th International Zurich Symposium on Electromagnetic Compatibility, pp. 73-76.

[3] Kreitlow, M., Garbe, H., Sabath, F. (2014). *Influence of software effects on the susceptibility of Ethernet connections*. 2014 IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 544-548.

[4] Braun, Ch., Schmidt, H.U. (2002). *Effects of microwave irradiation on modern Telecom devices - failure thresholds of five mobile phones*. AMEREM 2002, June 3-7, 2002, Annapolis, Maryland, USA. Book of Abstracts, p. 9.

[5] Braun, Chr., Clemens, P., Schmidt, H.-U., Taenzer, H.-J. (2006). *Störfestigkeits-Untersuchungen von WLAN-Funkübertragungssystemen*. Elektromagnetische Verträglichkeit EMV 2006. pp. 471-480.

[6] Klunder, C., ter Haseborg, J.L. (2010). *Effects of high-power and transient disturbances on wireless communication systems operating inside the 2.4 GHz ISM band*. 2010 International Symposium on Electromagnetic Compatibility - EMC Europe, pp. 359-363.

[7] Adami, Ch., Joester, M., Suhrke, M., Taenzer, H.J. (2014). *HPEM Tests of Communication Devices*. AMEREM 2014, July 27-31, 2014, Albuquerque, New Mexico, USA. Book of Abstracts, p. 39.

ROBUST DETECTION OF THREATS HIDDEN UNDERNEATH HUMAN CLOTHING IN A GIVEN PASSIVE MILLIMETER-WAVE SCREENING SCENARIO

Satish Madhogaria[1] and Marek Schikora[2]

[1] *satish.madhogaria@fkie.fraunhofer.de*
Fraunhofer FKIE, Dept of Sensor Data and Information Fusion, Fraunhofer Str. 20, 53343 Wachtberg (Germany)

[2] *marek.schikora@fkie.fraunhofer.de*
Fraunhofer FKIE, Dept of Sensor Data and Information Fusion, Fraunhofer Str. 20, 53343 Wachtberg (Germany)

Abstract

Automatic detection of hidden threats is gradually becoming a huge research topic for border security, especially - with several millimeter wave technologies already available, which are capable of scanning people keeping privacy and safety of the people in check. In this paper, we present a novel approach towards the detection of hidden threats from the sequence of images generated by a passive mm-wave imager operating at 94 GHz. The solution shown here is a two-step process. In the first step, we identify threat locations in individual frames. This requires extracting connected components and filtering by analysing blob properties to extract blobs which could represent a threat object. The threat locations are appropriately projected onto a fixed-size template. In the second step, a clustering algorithm is applied to determine the region which consists of highest concentration of threat locations returned by the previous step. The approach presented here shows good results on real millimetre-wave test sequences.

Keywords: Threat detection, millimetre-wave imaging, object detection, etc.

1 INTRODUCTION

Image classification is a computation procedure that sorts pixels or regions of an image into groups according to their similarity. There have been many image classification tasks [1-3] which could assist in safety and surveillance systems. Border security is a relatively new area where automated classification and detection of objects in images can play a substantial role by providing automated means to the security personnel. Current focus is on developing an imager, capable of showing dangerous threats hidden under clothing [4-7]. In this context, the TeraSCREEN project [8] aims at developing an innovative security screening system that combines multi-frequency, multi-mode images produced from active and passive subsystems. These subsystems will scan the subjects and return spatial and spectral information, thus allowing for automatic threat (hidden object underneath clothes) recognition. This also calls for a reliable automatic threat recognition algorithm that is capable of locating and classifying threatening objects in images returned by the active and passive subsystems. In this paper, we present a novel approach for automatic threat detection in 94 GHz TeraSCREEN passive millimeter-wave (mmw) images. Most of the previous work [9,10] describes a segmentation-based approach for threat detection in mmw images. Besides being partially supervised, such methods are difficult to apply in the images dealt in this paper. Figure 1 shows examples of frames considered in our preliminary test run. All these frames consist of a human subject carrying two PVC tubes

containing sulfur and fluoride on the chest. The image-acquisition technique is in close resemblance to the one described in the paper [7] with the difference that the images are acquired in real time using an array of receivers (16 in this preliminary case). This scenario is more realistic compared to the previous work, where frame rates are far from real-time, i.e., the scene has to be static for several seconds. In this work, the subject merely walks by at normal speed in a given space. Ultimately, we aim to develop a screening method which is easier to be installed and operated in real environments. Therefore, mmw-wave images shown here differ from the ones presented in [6, 9, 10]. The acquired preliminary images have low resolution with a high noise level (later images have been significantly improved and will be presented in a future paper. Evaluation data sets from these images were not available at the time of writing this article.). The primary aim, here, is to detect and localize a threat hidden on the body in real-time. Because of small size of the images (16 x 100) and high noise level, many of the standard image processing algorithms cannot be applied. From the frames shown in Figure 1, two immediately noticeable hindrances can be drawn: First, due to limited pixels, details about the threat, for example - size and shape are not visible. Second, variations within the single data set make it harder to rely on just one frame to give the correct result. Therefore, our primary aim here is to develop a robust algorithm which is able to locate the threat hidden on the body by observing the results from all frames in a single run. Our detection process is completely unsupervised. The images are 16 x 100 pixels showing a subject with or without threat.

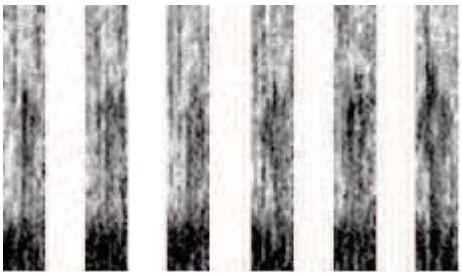


Figure 1: Shows images from a single run. All contain the same subject carrying the same threat. Still, there are visible differences which make it even harder to rely on the detection from a single frame. From these images, only in the 4th, 5th and 6th one, we can say that there is a threat, while in the first 3 images the threat is not so prominent.

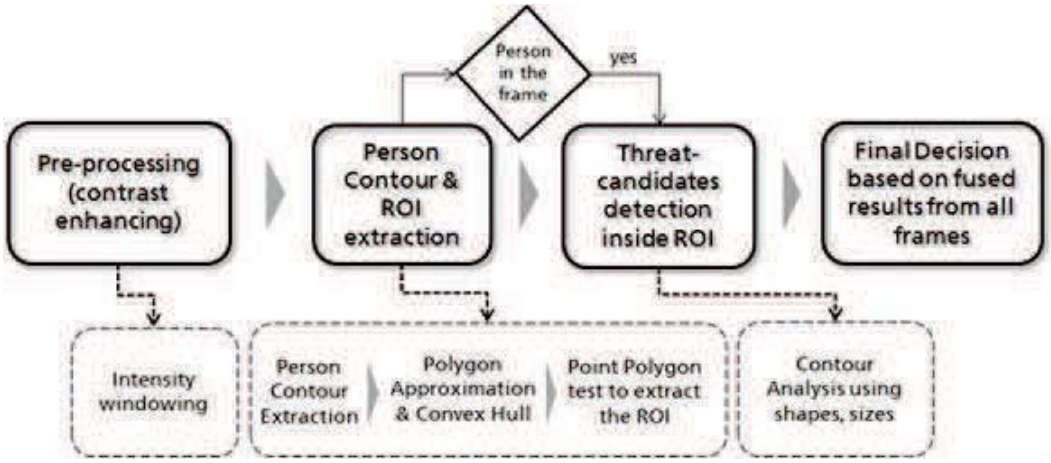


Figure 2: Workflow of the proposed algorithm to detect threats in mmw images

The paper is organized as follows: in the following section we discuss four principal steps, essential to solving the task of threat detection: pre-processing, region-of-interest (ROI) extraction, threat extraction in each frame and finally intelligent fusion of results from all frames. We discuss the problems incurred in each step and propose a solution. Next, we show some results and discuss the performance of the algorithm on a given data set.

2 DETECTION ALGORITHM

Figure 2 shows the flowchart of the detection algorithm proposed in this paper. The algorithm proposed here is a two-step process. In the first step, threat locations are detected in individual frames. This requires contrast enhancing, extracting connected components and finally, filtering by analysing blob properties to extract all blobs which could represent a threat object. In the second step, an appropriate clustering algorithm is applied to determine the region which consists of highest concentration of threat locations returned by previous step.

2.1 Step 1: Threat detection in each frame

Identifying threat locations in individual frames is achieved by following 3 steps: Contrast enhancing, Region of Interest (ROI) extraction and finally threat candidates detection inside the ROI.

2.1.1 Pre-Processing:

In the given images, the subject of interest is small and sometimes blurred. It makes sense to apply a contrast enhancing technique which could help to enhance the object of interest. To do that, one of the simplest ways is to focus only on the intensity range of the image which contains the features of interest. This can be accomplished by windowing the image. Piece-wise linear transformation T is applied to the intensity levels of the input image *f* at all points *(x, y)* that are inside the user-defined intensity interval *(I1,I2)*, where I1, I2 € (0,255). Values below this interval are mapped to a constant *c1* and values above this interval are mapped to another constant *c2*.

$$g(x,\ y)\ =\ T\ [f(x,y)] \tag{1}$$

where *g* is the output image and *g(x, y)* and *f(x, y)* denotes the intensity of *g* and *f* at any given location *(x, y)* of the image respectively. The overall transformation T can be defined as follows:

$$T = \begin{cases} If\ f(x,y) < I1; & g(x,y) = c1 \\ If\ (f(x,y) > I1\ and\ f(x,y) < I2; & g(x,y) = f(x,y) \\ If\ f(x,y) > I2; & g(x,y) = c2 \end{cases} \tag{2}$$

where *c1* and *c2* are constant intensity values. Figure 3 shows the contrast enhanced images (bottom row) corresponding to the input images shown in the top row.

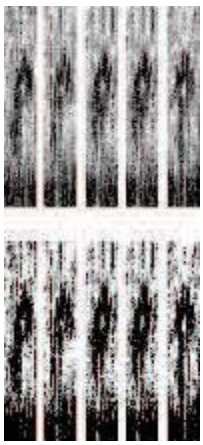
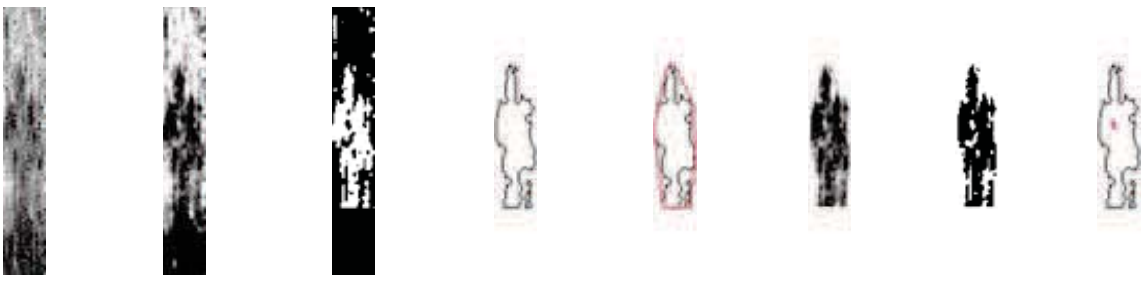


Figure 3: The top row shows the input images and the bottom row shows contrast-enhanced images.

2.1.2 ROI extraction:

Before applying the threat extraction, the search region can be reduced with appropriate region-of-interest (ROI) extraction. The region of interest in our case is the subject present in the frame and the objective is to search for candidate threats within the subject boundary. This step is essential to remove background noise, which reduces a considerable amount of false detections. ROI extraction involves human-like contour extraction, convex hull (of the human-like contour) computation and finally extraction of all points that lie inside the convex hull. Human-like contour can be extracted using these 4 steps: 1) Convert the image into binary form. In our case, inverse binary operation is suitable for extracting human-like contour. 2) Clean up the binary image. 3) Extract connected components (or blobs). 4) Filter by analyzing blob properties. For now, we keep it to "area" since we do not have much consistent information in the given preliminary images. To search for the threat contours, we take the convex hull of human-like contour as the region of interest. This is done in order not to miss the threats because of an error in extracting human-like contours near the boundaries or splitting of human-like contour into two. Figure 4 (c) - (e) shows an example output for ROI extraction.



(a) Input (b) Contrast-enhanced (c) Inverse Binary (d) Person contour (e) Convex Hull (f) Region of Interest (g) Binary of ROI (h) Threat candidate

Figure 4: The figure shows each step involved in the process of extracting a threat in each frame.

2.1.3 Candidate threat extraction:

Within the region of interest generated from the previous step, candidate threats are extracted from ROI by separating contours based on the shape and size of the contours. The process of threat contour extraction is similar to the human-like blob extraction. During the blobs filtering process, we check therefore area of the blobs as well as the convexity of blobs to be declared as a candidate threat. Figure 4 (h) shows the extracted "candidate threat" from the binary ROI.

2.1 Step 2: Fusion of results from a given sequence

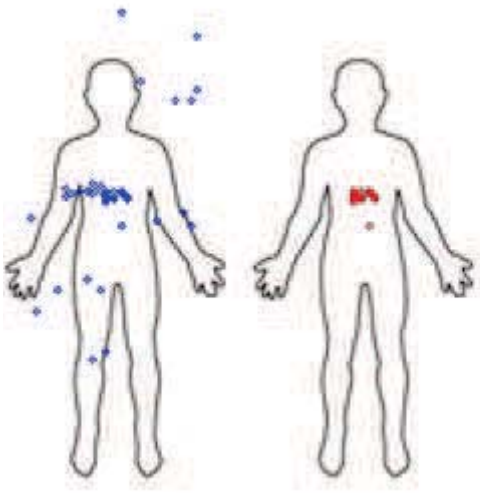
Due to the low quality of the given images, the candidate threat extraction process results in a lot of false detections. To further enhance the robustness of the system, we propose to use the outputs from all frames in a single sequence and fuse them in order to produce a reliable result. The centroids of all candidates are given as an input to a clustering method, which can return the most concentrated region in the fused image. In the proposed TeraSCREEN security system, for one single run, there could be 25-100 frames with a person in it, which could generate about 40-120 points (all true and false candidate threats). We want to find out a specific region, where most of these points are concentrated. For this purpose, we use the ART-2A clustering method [11]. The ART-2A clustering algorithm is well suited for our task for one primary reason, i.e., it does not require any previous knowledge on the number of clusters present in the data. This helps us to keep the detection process as unsupervised. The parameters of this clustering algorithm are automatically adjusted based on the input image size. Figure 5 shows the projected centroids of candidate threats on a template image and the resulting cluster (containing highest number of points). In Table 1, we can see the outputs generated by the ART-2A clustering method. It divides 60 candidate threats into 14 clusters and the largest cluster (with cluster-id 14) consists of 21 points, much higher than the second best cluster (Cluster1 with 6 points). Therefore, the region around the largest cluster can safely be termed as the probable location of threat. Furthermore, to determine whether the largest cluster can represent threat location, parameters that could influence the decision are used to create a number, that we call a validity factor. In our case, we take the ratio of number of points in the largest cluster, n, to the total number of candidate threats, N, as the validity factor and threshold this value to determine whether the largest cluster region, R(L) is the region of threat as shown in the equation below:

$$VF = \frac{n}{N}, \quad R(L) = \begin{cases} threat, & if\ VF \geq \eta \\ no\ threat, & otherwise \end{cases} \tag{3}$$

where η is the threshold, that determines whether the given largest cluster can be called the “region of threat”.

3 RESULTS

Here, we discuss the performance of the algorithm on 94 GHz mmw images in TeraSCREEN conops, where a person walks by at a normal speed and the frames are acquired in real time. Because of the low resolution and low image quality in the preliminary setup, instead of relying on the output from one frame, we perform cluster analysis on outputs from all frames in a given sequence. The algorithm takes the result from all frames in a sequence and gives a final decision on whether the subject is carrying a threatening object, and if so, the location of the threat. In this conops, for a single run, the number of frames with a person in it can vary from 25 to 100. Figure 6 shows some more results from the preliminary data set. This data set consisted of more than 100 images, out of which 22 frames had person in it carrying a threat on the chest. 33 candidate threats were extracted in the first step from all frames. The centroids of these candidate threats are then projected on a template image for cluster analysis. The ART-2A clustering algorithm returned 15 clusters out of which the largest cluster contained 9 points. The "largest cluster" is further analyzed to determine whether it belongs to a region of threat. Equation (3) gives us the final decision from the algorithm. In Figure 6(d), we can see that the points from the largest cluster correctly predict a threat on the chest of the person. We have evaluated 12 such sequences, where 8 of them had person carrying a threat and 4 were clean. We could correctly identify threats in 7 of them. The overall success rate was 75 %.

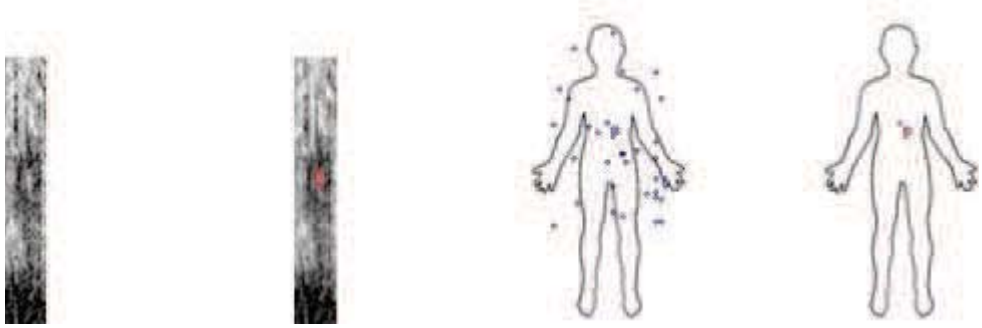


(a) (b)

Figure 5: (a) shows the projected centroids of "candidate threats" on a prototype display while (b) shows the points in the best cluster region after applying ART-2A clustering algorithm and selecting the cluster with the highest number of points

Cluster ID	No of Points
Cluster 0	2
Cluster 1	6
Cluster 2	1
Cluster 3	3
Cluster 4	4
Cluster 5	3
Cluster 6	3
Cluster 7	2
Cluster 8	1
Cluster 9	1
Cluster 10	1
Cluster 11	5
Cluster 12	2
Cluster 13	5
Cluster 14	21

Tabel 1: This table shows output of the ART-2A clustering algorithm. The points displayed in the figure on the left side are the points from cluster 14 (21 points). From the figure and the table we can see that the clustering algorithm can easily separate the threat area.



(a) Input Image

(b) Detected Threat Contour in a given frame

(c) Centroids of threat candidates from all frames

(d) Most compact clus--ter out of all clusters re-turned by ART

Figure 6: Shows the detected threat in a frame and the overall detection region from one single run. The most compact cluster shows the location of a hidden threat on the body. The data set consisted of 115 frames with 22 frames containing the subject. The algorithm returns 33 candidate threats which are then analyzed to extract the most compact cluster.

4 CONCLUSIONS

The algorithm presented in this paper is able to detect the location of a threat hidden underneath a person's clothing. The algorithm is primarily developed to work for low resolution images acquired from the 94 GHz passive subsystem, capable of generating images in real time. The preliminary images are 16 x 100 pixels with high noise. Most of the standard image processing algorithms are di cult to apply in such small images. In this work we have presented an approach, which takes advantage of results obtained from all frames in a sequence and eliminates false detections by cluster analysis of the detections from individual frames. From the results presented here, we can see the potential of the algorithm in correctly identifying the location of the threat hidden underneath human clothing in real millimeter-wave test sequences.

5 ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312496.

Disclaimer

REFERENCES

[1] S. Madhogaria, M. Schikora and W. Koch (2013). *Using whole and part-based hog filters in succession to detect cars in aerial images.* VISAPP (1), pp. 681-686.

[2] S. Madhogaria, P. M. Baggenstoss, M. Schikora, W. Koch, and D. Cremers (2015). *Car detection by fusion of hog and causal mrf.* IEEE transactions on AES 51, pp. 575-590.

[3] X. Zhengyu, J. Limin, Q. Yong, and W. Li (2012). *Research on moving object detection method of high-speed rail-way transport hub video surveillance.* International Symposium on ISISE, pp. 315-318.

[4] H. Stanko, D. Notel, A. Wahlen, J. Huck, F. Kloppel, R. Sommer, M. Hägelen, and H. Essen (2008). *Active and passive mm-wave imaging for concealed weapon detection and surveillance.* International conference on Infrared, Millimeter and Terahertz Waves, pp. 1-2.

[5] H. mei Chen, S. Lee, R. Rao, M.-A. Slamani, and P. Varshney (2005). *Imaging for concealed weapon detection: a tutorial overview of development in imaging sensors and processing.* IEEE signal processing magazine 22, pp. 52-61.

[6] N. E. Alexander, C. Callejero Andrs, and R. Gonzalo (2008). *Multispectral mm-wave imaging: materials and images.* SPIE 6948, pp/ 694803-694803-10.

[7] N. Alexander, C. Callejero, F. Fiore, I. Gmez, R. Gonzalo, I. Enrquez de Luna, I. Ederra, and I. Palacios (2009). *Suicide bomber detection.* SPIE 7309, pp. 7309D-73090D-12.

[8] N. E. Alexander, B. Alderman, F. Allona, P. Frijlink, R. Gonzalo, M. Hägelen, A. Ibez, V. Krozer, M. L. Langford, E. Limiti, D. Platt, M. Schikora, H. Wang, and M. A. Weber (2014). *TeraSCREEN: Multi-frequency multi-mode terahertz screening for border checks.* SPIE 9078, pp. 907802-907802-12.

[9] O. Martinez, L. Ferraz, X. Binefa, I. Gomez, and C. Dorronsoro (2010). *Concealed object detection and segmentation over millimetric waves images.* IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 31-37.

[10] X. Shen, C. Dietlein, E. Grossman, Z. Popovic, and F. Meyer (2008). *Detection and segmentation of concealed objects in terahertz images.* IEEE transactions on Image Processing. Pp. 2465-2475.

[11] G. A. Carpenter, S. Grossberg, and D. B. Rosen (1991). *ART-2A: An adaptive resonance algorithm for rapid category learning and recognition.* Neural Network 4, pp. 493-504.

3D MIMO IMAGING AT 360 GHZ FOR SECURITY SCREENING

Stefan A. Lang [1,*], Reinhold Herschel [*], Sandra Nowok [*],
Rüdiger Zimmermann [*], Nils Pohl [*]

[1] *stefan.lang@fhr.fraunhofer.de*
[*] Fraunhofer Institute for High Frequency Physics and Radar Techniques,
Fraunhoferstrasse 20, 53343 Wachtberg (Germany)

Abstract

Passenger screening at airports is a topic of continuous relevance to the research community. This is of special bearing when talking about systems which utilize millimeter waves. There are several different passenger screening systems currently in the process of admission for installation. Unfortunately, they generally do not possess the possibility of moving passenger screening in combination with high resolution images. This topic is still unsolved for millimeter wave scanners as well as for X-ray based scanners. The presented work deals with an active Terahertz system which is based on an Multiple Input Multiple Output (MIMO) approach in order to achieve the necessary high frame rate for moving passenger screening and is embedded in the EU FP7 project “TeraSCREEN”. The aim of the project is to develop an imaging system which combines active and passive modules at different frequencies. All gained information from the different modules is combined in a common image processing unit to automatically look for potential threats in the detected images.

Keywords: Terahertz, Imaging, Security Screening, MIMO, FMCW, Radar, Active.

1 INTRODUCTION

In contrast to X-ray scanners like in [1], millimeter wave and Terahertz scanners are using non ionizing radiation and also possess the advantage of very fast imaging with high dynamic range, which is crucial for the screening of moving passengers. Millimeter wave and Terahertz scanners are based on a wide spectrum of technologies like [2],[3]. There are also existing systems which are utilizing multi-antenna CSAR imaging [4],[5],[6] as well as systems which are based on a massive implementation of coherent transmitters and receivers – the so called Multiple Input Multiple Output (MIMO) systems like [7],[8] and many others like the present paper. In [9] an overview of currently researched or already available security screening systems is shown.

This paper deals with an active imaging system based on an MIMO approach operating at 360 GHz and is organized in four parts. First, the general concept and system design will be presented as an overview, including an explanation of the beam steering in elevation and a description of the used high frequency component chain. The second part consists of a description of the imaging algorithm. As the last part, a preliminary system operating at 90 GHz is shown, which is used to verify the overall system concept. The paper closes with a conclusion.

2 SYSTEM CONCEPT AND DESIGN

A crucial part of this comprehensive system is an active MIMO system at 360 GHz, which will be the main focus of this paper. The MIMO system consists of 16 transmitter and 16 receiver antennas within one single array. Using an FMCW bandwidth of 30 GHz, a range resolution of 5 mm is obtained. With the 16x16 MIMO system 256 different azimuth bins can be distinguished, leading to an azimuth resolution of 0.078° in a single linescan. In Fig. 1 the system concept is shown. More details about the system concept can be seen in [10].

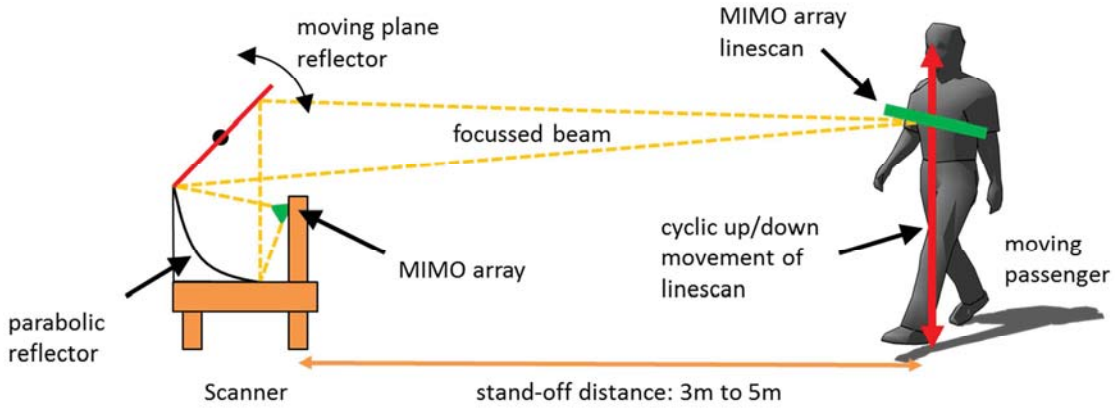


Fig. 1: Overall system concept for measurement of moving passengers

The above-mentioned parameters refer to the imaging of a passenger at a standoff distance of about 3 to 5 meters. In combination with the high frame rate of 4 Hz, this system enables high resolution 3D imaging of passengers passing by.

2.1 Beam steering approach

To obtain a resolution (or size of the linescan) in elevation of 0.15°, a focusing elliptical mirror is used. The MIMO array is mounted above this mirror and its beam is directed to it. The beam is then reflected to another mirror and afterwards reflected to (or from) the screened passenger. In order to move the linescan over the passengers' body, an electromechanical beam steering is used. The chirp rate of the high frequency system enables a fast measurement within 60µsec and therefore allows for 130 different elevation angles. The person's movement in this short amount of time is neglectable for the image reconstruction process. The beam steering setup can be seen in Fig. 2.

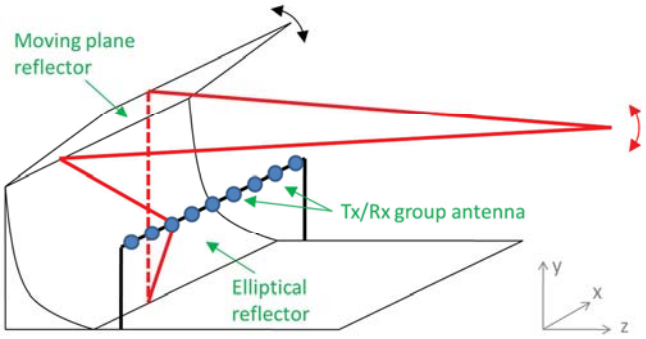


Fig. 2: Beam steering setup with MIMO array (Tx/Rx group antenna), parabolic reflector and an electromechanical steered moving plane reflector

The moving plane reflector is periodically moved with 4 Hz, to obtain 4 images per second. For this purpose, a closed-loop drive and control circuit with continuous comparison of nominal and actual values of servo drives and trigger signal was built. More details about the MIMO array can also be seen in [10].

2.2 High frequency component chain

The active high frequency part of the system is based on a Direct Digital Synthesis (DDS) element operating at a frequency of 10 GHz providing an FMCW bandwidth of

833 MHz. After this it is again upconverted in frequency by two frequency triplers to obtain 90 GHz. At this stage, the FMCW bandwidth already amounts to 7.5 GHz. The next stages are two separate multipliers, each providing a multiplication factor of 2. The final signal to be transmitted is achieved at this stage of the chain and provided to the transmitting antennas. In order to gain the necessary MIMO channel assignment, an electronic switch is implemented at 90 GHz, which provides time-multiplexing functionality. Of course there are also filters and power amplifiers present in the described chain to achieve a clean transmitted signal with an output power of about 1 mW.

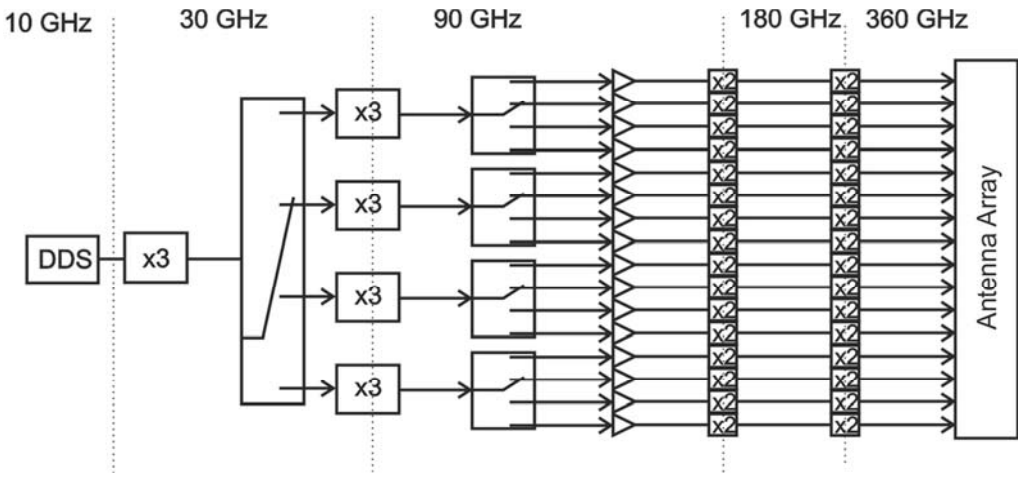


Fig. 3: High frequency component chain for the transmitter channels

However, the receiver's high frequency component chain is a little different from the transmitting one: there is no need for a switching matrix because all receiver channels are being sampled in parallel and the multiplier from 180 to 360 GHz is not needed due to a second harmonic mixer. Some of these components are built by partners in the consortium, whereas Fraunhofer FHR is responsible for building the complete system and bringing all components together. The components developed and manufactured by our partners are (all other components are being developed at Fraunhofer FHR): DDS and 90 GHz tripler by Goethe University Frankfurt (Germany); 90 to 180 GHz and 180 to 360 GHz multiplier as well as subharmonic mixer by STFC (UK); MIMO antenna design by Fraunhofer FHR and manufacturing by Anteral (Spain).

3 IMAGING ALGORITHM

The framework for measuring moving persons and gaining interpretable images out of this measurement makes it necessary to implement a very fast but also high image quality image reconstruction algorithm. These framework parameters can be covered with an implementation of the Range Doppler Imaging (RDI) algorithm. It provides both of the needed aspects by utilizing a Fast Fourier Transformation (FFT) in Range as well as in Cross-Range. In order to be able to use FFTs for both directions, several operations have to be applied to the raw measurement data. The complete RDI image reconstruction procedure is shown in Fig. 4.

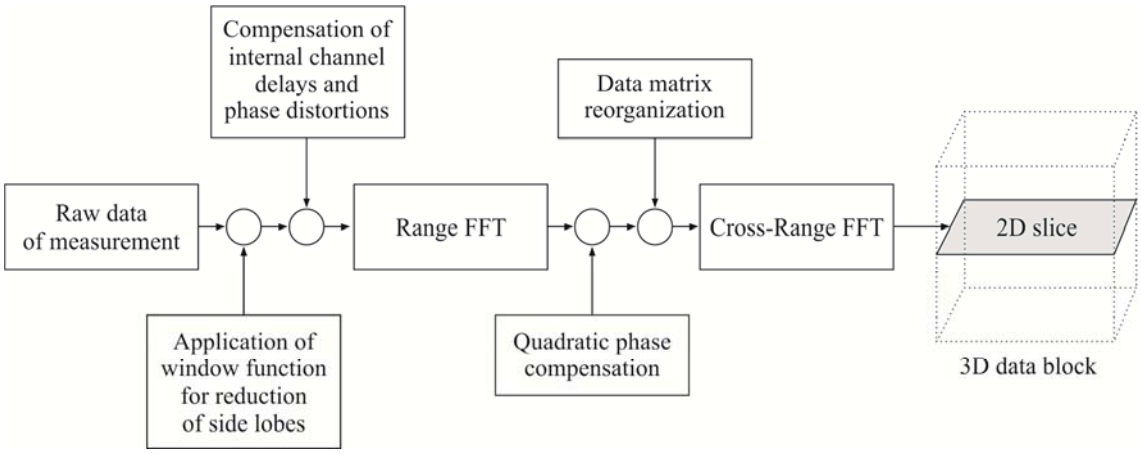


Fig. 4: Processing steps of the RDI imaging algorithm for one distinct slice

With this procedure, a single 2D slice can be reconstructed, whereas one dimension of the slice is the measurement depth and the other dimension represents the Cross-Range. Both dimensions then represent a single slice over the scanned person's body – for example representing the 3D contour of the person and possible hidden threats on the chest. In order to achieve a complete 3D volume, these slices have to be stacked together into a 3D data block, as shown in Fig. 5.

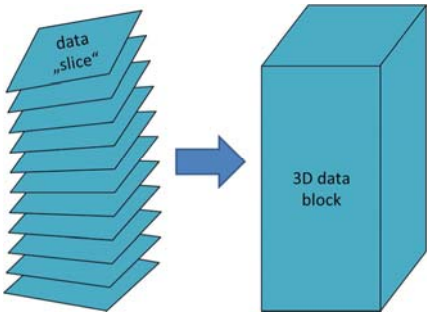


Fig. 5: Generation of 3D volume by adding all reconstructed slices into a 3D data block

The person is then completely included in this (or covered with this) 3D volume. Due to well-known features of the 3D volume, automatic threat detection algorithms can be applied to the reconstructed volume and hidden threats directly identified.

4 MIMO IMAGING DEMONSTRATOR AT 90 GHZ

In order to prove the feasibility of the MMO imaging procedure with the shown measurement setup already at the current state of the project, a demonstrator at 90 GHz was built. This imaging system is currently driven by a DDS developed at Fraunhofer FHR, which will be substituted by the DDS from Goethe University for the real 360 GHz system. This DDS is operating at 1.25 GHz and provides the fundamental FMCW chirp signal with an initial bandwidth of 111 MHz. The signal is then multiplied by 24 to achieve 30 GHz and is afterwards multiplied by a factor of 3 to achieve the 90 GHz output with an FMCW bandwidth of 7.5 GHz. Due to ongoing development of the electronic switch, only one transmitting channel but four receiving channels were set up. The block diagram of the 90 GHz is shown in Fig. 6.

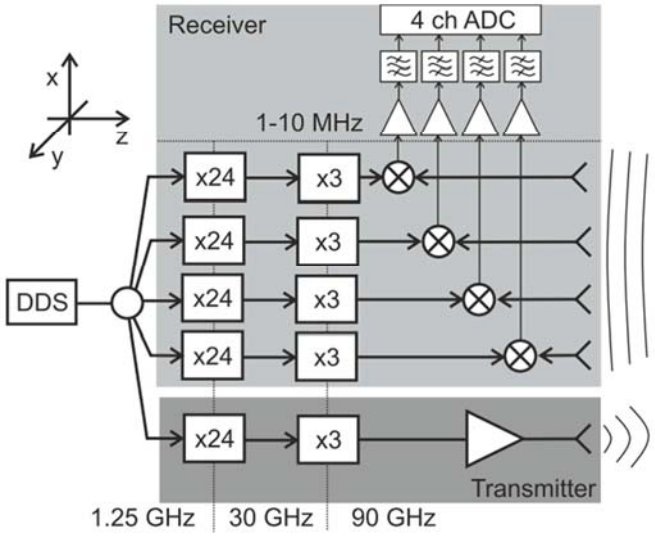


Fig. 6: Block diagram of the 90 GHz MIMO transceiver

In this case, both high frequency component chains are identical except for the power amplifier in the transmit case and the mixer in the receive case. With this system, calibration procedures were developed, implemented and tested as well as first images produced. Fig. 7 shows first exemplary results, which are obtained with the 90 GHz demonstrator system.

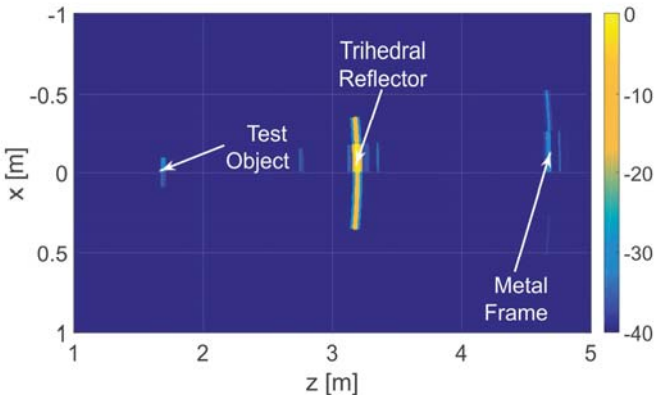


Fig. 7: Exemplary imaging results of the 90 GHz demonstrator tests showing the detected reflectivity in dB

Due to the reduced number of transmitters and receivers, the resolution of the demonstrator is very limited compared to that aimed for with the 360 GHz system. In the case of this demonstrator approach, the resolution was not the main driving force behind the development process. For this process, the main focus has been on the clarification of the overall MIMO imaging framework which is based on many high frequency components and therefore, directly depending on the performance of these components.

For the tests, a single corner reflector was placed in the scene. This reflector can clearly be seen in the reconstructed images. A metal rod of 10mm thickness was used as a visible target in the radar image at a distance z=1.7m. A metal frame standing behind the test setup can also be observed at approximately 4.7m. With these results, the developed characterization and calibration procedures could be verified and will also be implemented in the targeted 360 GHz system. Therefore, the experimental set up of the preliminary imaging demonstrator has to be viewed as a success.

5 CONCLUSION

The presented paper discussed a new way of security screening, which provides the possibility to measure moving persons. Especially in security relevant areas, where a high throughput of persons is necessary, such a system is beneficial for a reduction of time needed for the screening process. It is shown that the ongoing research on this system is advancing to the next stage and a demonstrator at a lower frequency – already comprising many of the developed high frequency components for the 360 GHz system – was built. The feasibility of MIMO imaging at lower frequencies by using the same imaging approach as for the targeted final system and a verification of the characterization and calibration procedures was shown.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312496. We also want to thank Manfred Hägelen, Paul Warok, Gunnar Briese and Sven Heinen as well as all partners of the TeraSCREEN consortium for their support.

Disclaimer

REFERENCES

[1] A.-S. Lalleman, G. Ferrand, B. Rosse, I. Thfoin, R. Wrobel, J. Tabary, N. B. Pierron, F. Mougel, C. Paulus, L. Verger (2011). *A dual X-ray backscatter system for detecting explosives: Image and discrimination of a suspicious content*. IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC). doi: 10.1109/NSSMIC.2011.6154503

[2] David M. Sheen, Douglas L. McMakin, Jeffrey Barber, Thomas E. Hall, Ronald H. Severtsen (2008). *Active Imaging at 350 GHz for security applications.* Proc. of SPIE Vol. 6948, 69480M. doi: 10.1117/12.778011.

[3] Frank Gumbmann, Phat Tran, Amir Cenanovic, Sebastian Methfessel (2009). Millimeter-wave imaging concepts: Synthetic Aperture Radar (SAR) and Digital Beam Forming (DBF). Frequenz, Vol. 63, 5-6.

[4] Sebastian Hantscher, Beverly Schlenther, Manfred Hägelen, Stefan A. Lang (2012). *Security Pre-screening of Moving Persons Using a Rotating Multichannel W-Band Radar*. IEEE Transactions on Microwave Theory and Techniques, Vol. 60, NO.3.

[5] Stefan A. Lang, Manfred Hägelen, Joachim Ender, Sebastian Hantscher, Helmut Essen (2011). *A new approach for fast Security Scanning with Millimetre-Waves: SARGATE*. Proc. of SPIE 8022. 802208. doi: 10.1117/12.883355.

[6] Stefan A. Lang, Manfred Hägelen, Joachim Ender, Sebastian Hantscher, Helmut Essen (2012). *Optical 3D assisted CSAR for security screening at a constant passenger flow*. 9th European Conference on Synthetic Aperture Radar (EUSAR). Nürnberg.

[7] Sherif Sayed Ahmed, Andreas Schiessl, Lorenz-Peter Schmidt (2011). *A Novel Fully Electronic Active Real-Time Imager Based on a Planar Multistatic Sparse Array*. IEEE Transactions on Microwave Theory and Techniques, Vol. 59, No. 12, December 2011.

[8] Jochen Moll, Philipp Schöps, Viktor Krozer (2012). Towards Three-Dimensional Millimeter-Wave Radra With Bistatic Fast-Factorized Back-Projection Algorithm – Potential and Limitations. IEEE Transactions on Terahertz Science and Technology, Vol. 2, No. 4, July 2012.

[9] Michael C. Kemp (2006). *Millimetre Wave and Terahertz Technology for the Detection of Concealed Threats – A Review.* Optics and Photonics for Counter-Terrorism and Crime Fighting II. Edited by Clon Lewis, Gari P. Owen. Proc. of SPIE, Vol. 6402, 64020D.

[10] Manfred Hägelen, Sandra Nowok, Daniel Nöthen, Stefan A. Lang (2014). An Active Personal Screening Method at 360 GHz, based on an FMCW-MIMO approach - a TeraSCREEN subsystem. 10th Future Security. Berlin.

EXTENDING SECURITY PERIMETER AND PROTECTING CROWDED PLACES WITH HUMAN SECURITY RADAR

Andrey Kuznetsov, Dmitrii Vakhtin, Valery Averyanov, Alexey Evsenin, Igor Gorshkov, Pavel Iurmanov , Grigory Labzovsky, Viktor Meshcheryakov, Marina Mokhova, Semen Semenov, Igor Vorobev, Stanislav Vorobyev, Viktor Vorobev, Evgenii Zarubkin and David Kellermann

kuznetsov@apstecsystems.com
Apstec Systems, Kesk-Sõjamäe tn 2, 11415, Tallinn (Estonia)

Abstract

The Human Security Radar (HSR) system based on active centimeter-range radio waves is described. On-going tests with actual people flows are discussed.

HSR can automatically identify in a crowd people carrying threat dielectric and/or metallic objects under clothes or in backpacks. HSR operates remotely, covertly and in real time without slowing down the people flow. Coordinates of the located potentially suspicious person and hazardous objects on its body are sent to a higher-level security system, or can be optionally superimposed on an ordinary video image.

HSR is a flexible multi-threat detection system that can be set up to simultaneously detect dielectrics (e.g. explosives), metallic objects (weapons, shrapnel), as well as radioactive and nuclear materials.

Keywords: multi-threat detection; standoff; automatic; dielectrics; metals; radioactive and nuclear materials; real-time; crowded places; centimeter-range radar.

1 INTRODUCTION

Current security-related detection equipment is usually limited to specific types of threats, and/or makes inspection process time consuming, labor-intensive, and plagued with privacy issues. Therefore, such equipment is typically used only at the perimeter of most sensitive areas, such as airports, where it tends to create waiting lines that interfere with normal operations and themselves can be targets of terrorist attacks. Unsurprisingly, such systems affecting the normal flow of people have little impact on protecting mass transport systems, crowded areas or public venues.

Human Security Radar (HSR) [1] is intended to be an automatic non-intrusive “early-warning” system that can move the security perimeter away from the protected venue by detecting in real time a wide number of threats without interfering with normal flow of people.

HSR is a multi-threat detection system that can identify in a crowd people carrying on their bodies dielectric objects (explosives, pyrotechnics, etc.), metals (e. g. weapons), as well as radioactive sources (with an optional gamma-spectroscopy module).

HSR is based on active centimeter-range radio waves, which offer the following advantages:

- Different ways of analyzing the same data allow detection of both dielectric (e. g. organic explosives) and metallic (guns, shrapnel) objects.
- Sufficient spatial resolution to detect objects with dimensions of few centimeters, while retaining possibility of automatic off-line real-time digital image processing.
- No privacy issues due to non-imaging standoff mode of operation.

- Avoiding operator's fatigue, since security personnel are only notified about the alarms and don't need to constantly monitor images or video stream.
- Better that shorter wavelengths penetration through wet clothes.
- Safety for people and equipment, the emitted power being many times less than that of a mobile phone.

HSR can be used either as a standalone multi-threat detection system, or as an “early-warning” components of a multi-layered security arrangement, where it can reduce the load on slower systems by preselecting targets from the crowd.

Fig. 1: Left: actual installation of the HSR in portal configuration in Tartu, Estonia. Right: possible configuration for all-round inspection.

HSR can be configured as a wide portal, as a long-range “flat panel”, or as a combination of modules for all-round inspection (Fig. 1).

2 HSR AS A MULTI THREAT DETECTION SYSTEM

2.1 Principles of operation

HSR operates by emitting centimeter range microwaves, which are reflected by the body and objects on it. Human body is a near-perfect reflector of radio waves in the used frequency range, and is “seen” by the system as a single reflecting surface. The system was described in some detail in [1].

HSR operates in K_u-band frequency range in stepped frequency change mode, when a narrow frequencies are emitted one at a time sequentially by elements of a square (16×16 elements) antenna array. This helps to avoid interference with neighboring equipment, and provides clean signals at the receiving antennae. Several receivers (Vivaldi- or horn-type) are used in locations depending on the configuration of the system. The number of emitting antenna arrays also depends on the system configuration.

The measured complex field is then processed by high-speed Graphics Processing Units (GPU) to reconstruct the 3D distribution of scatterers in front of the system. Depending on the orientation of the receivers, both co- and cross-polarized scattered field components can be obtained. The 3D distribution of scatterers is automatically analyzed to detect “anomalies”, which may correspond to objects on human body. These anomalies are then resolved by threat-specific algorithms described below.

The spatial resolution of the system depends on the distance, and is of the order of few centimeters, which eliminates some of the privacy concerns.

HSR currently works at about 15 frame per second, which leads to essentially real-time operation, so that the passing people do not have to stop or even slow down. Multiple targets are analyzed simultaneously.

2.2 Standoff detection of dielectric objects

HSR detects dielectric objects on body by using the fact, that incident radio waves are reflected both from the first (clothes-dielectric) and the second (dielectric-body) surfaces, while the body surface around the dielectric provides a single-surface reference (Fig. 2, also see [1]). Due to lower propagation speed of electromagnetic waves in dielectrics, the back surface (dielectric-body) appears to be pressed into the surrounding body. The dielectric constant ε of the object can be determined as:

$$\varepsilon = (D / d)^2,$$

where d is the actual thickness and D is the total apparent distance between front and back surfaces (i. e. actual thickness plus apparent concavity). Dimensions, area, volume and shape of the object can also be estimated.

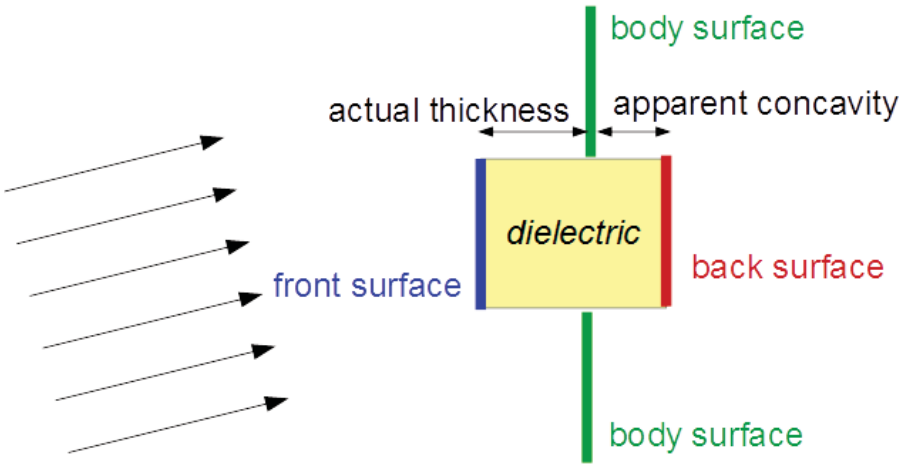


Fig. 2: Detection and characterization of dielectrics.

Dielectric constant, which is directly related to the density of the dielectric, is a rather specific characteristic of explosive, as was measured by us in direct experiments with C-4, Semtex10, AN, ANFO, and TNT. While this specificity is not perfect, it turns to be good enough to distinguish between organic explosives and non-threat dielectric objects that can be carried on body under clothing: wallets, phones or other gadgets, medical appliances, etc.

In the portal configuration additional information is obtained when the person walks at normal speed between the two sides of the portal (“transmission mode”). Any dense dielectric object would cause the increase of the apparent path traveled by the radio wave. This can be used to detect dielectrics carried, for example, in a backpack, which cannot be seen by the system that views a person only from one side (“reflection mode”).

The complex field calculated by GPUs is then analyzed to detect places with two reflecting surfaces one behind another (Fig. 2). Parameters of the found anomaly (volume, thickness, dielectric constant, shape, etc.) are then automatically determined, and integrated over the period of time when the target person is within the inspected zone of the system. The built-in tracking capability allows one to follow many anomalies simultaneously in real time and to select the best views of each anomaly with most

reliable parameters. These parameters are then used to automatically resolve the anomaly using decision-making algorithms based on “fuzzy” logic, which can do without an extensive “library” of threats. The result is a simple “alarm/no alarm” type of answer, plus the information about the nature of the threat (dielectric/metal/both) and its location on the body.

There are no images to look at, which drastically reduces requirements for the security personnel qualification, operator's fatigue, and privacy concerns.

Detection of dielectrics has been implemented in several prototype HSR systems. Tests and trials of these systems' ability to detect dielectric threat objects have been conducted, using both real explosives: C-4, Semtex10, AN, ANFO, and TNT and benign simulants with properties close to those of real explosives: PVC, wax, salt, etc. The results have been reported in [1].

2.3 Standoff metal detection

Metal detection with HSR is currently at an advanced R&D stage. It is based on the known effect of the increased cross-polarized component of the scattered field in presence of metals (see, e.g. page 33 of [2]).

Co-polarized amplitudes used in metal detection come from the same 3D distribution of the field that is used in detection of dielectrics (see above). Cross-polarized amplitudes are obtained by analyzing the subset of the data from receivers that are rotated by 90 degrees (see left part of Fig. 3).

Relation between co- and cross-polarized amplitudes is analyzed for each part of the body separately with specificity allowed by the systems' position resolution.

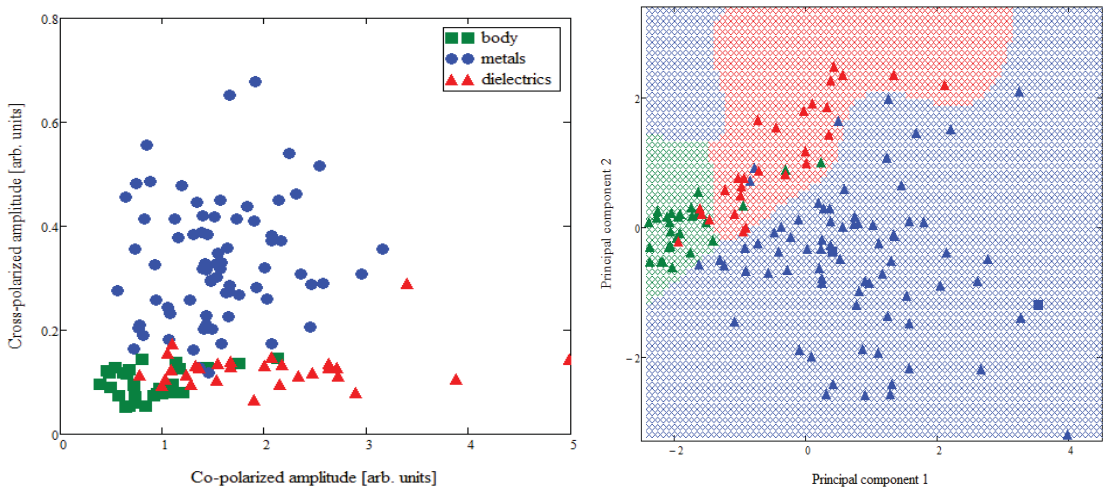


Fig. 3: Left: Cross-polarized vs. co-polarized amplitudes for body without objects, metals on body (shrapnel and a gun), and dielectric on body (wax).
Right: discrimination between body without objects (green), metals (blue) and dielectrics (red) obtained by using SVN algorithm with PCA data preprocessing.

The data analysis in case of metal detection consists in determining, to which of the “clusters” (body, metals, dielectrics) the given experimental point belongs. Unlike the case of dielectrics, in which compiling a library of “typical” threats is problematic, in metal detection the recognition algorithm can be “trained” to recognize main types of interesting anomalies by experimentally measuring response of the system to shrapnel, guns, knives, keys, mobile phones etc.

An appropriate classification algorithm can be used, such as support vector machines, Bayes classifier, neural networks, gradient boosted trees, K-nearest values, etc. Multi-dimensional data may be pre-processed, e.g. by Principal Component Analysis (PCA).

Example of training of the support vector machine (SVM) model on 131 measurements with a square (16×16 elements) transmitting antenna array and a pair of horn-type receivers rotated by 90 degreed relative to each other is shown on Fig. 3.

Coloured symbols correspond to the training data points (the data have been standardized), while coloured background areas show the results of training the model. A mismatch between symbol colour and the background colour indicates classification error. The above result was obtained for a single data frame. Results from consecutive frames can be integrated to further improve the classification (at present the system is operating at ~15 frames per second).

Preliminary results on polarization method indicate that HSR would be able to detect concealed metallic objects, such as guns or shrapnel, in real time from distance of several meters. Work is currently under way to integrate metal detection seamlessly into HSR's data analysis procedures.

2.4 Standoff detection of radioactive and nuclear materials

Another possible addition the HSR that makes it a multi-threat detection system, is a spectroscopic radiation portal, which can be based, for example, on APSTEC's gamma-ray spectrometer (GS) similar to those used in APSTES's smartSENNA system [3]. In portal configuration, two GSs can be placed inside the protective plastic cases of the HSR, one at each side and at about 1 meter from the floor. Alternatively, a single GS be placed above the portal (suitable for narrow portals). There are no additional power or shielding requirements. Preliminary tests with GSs indicate that they can successfully identify most common radioactive sources in real time (i.e within the time needed for a person to pass through the portal zone), while suppressing false alarms coming from naturally occurring radioactivity (NORM) and medical isotopes.

2.5 Reporting alarms

The main idea in reporting alarms from HSR is not to bother the security personnel with constantly updated “no threat” status, but to report only if an alarm has actually been detected. The alarm information includes time, type, position/coordinates on the body, and an optional photograph of the suspect.

The current reporting system is implemented as a separate “Integrator” component, which runs either on the data analysis computer or on a remote machine, and collects information from one or several HSR systems. The internal tracking module allows the Integrator to correlate alarms from several HSR systems, as well as from different subsystems of a single HSR system (dielectrics, metals, radioactive materials).

After receiving the alarm information, the Integrator forms a report and sends it to one or several user interfaces. The level of the detail can be anything from just a buzzer signal to full tracking information for a higher-level system with images of the suspect person.

Fig. 4 shows an example of a detailed user interface running on a desktop or laptop computer. The interface has no buttons to press or menus to scroll through, other than a narrow alarm database band at the bottom of the screen, which the operator can examine at any time to check on the past alarms.

Fig. 4: Example of a detailed user interface with information about an alarm. Red square indicates a suspicious person, yellow square shows the location of the threat object on the person. Thumbnails on the bottom of the screen represent the history of alarms.

2.6 On-going tests

HSR is currently tested at an industrial facility in Tartu, Estonia, where it is used to screen the employees passing through a corridor while performing their day-to-day duties (Fig. 5). The system is in portal configuration with two transmitting antenna arrays at each side.

Fig. 5: Installation of the HSR at an industrial facility in Tartu, Estonia.

The main goal of the test is to study the false alarm rate of the HSR, its long-term stability and 24/7 operational capabilities.

A total of about 1000 people are passing through the system during working hours in both directions every day, performing their daily duties. The passing people are automatically counted, and alarms are written to a database. The detection probability is periodically checked by asking people to carry a simulant.

The statistics and false alarms and their details (location on body, situation that caused them, etc.) from this small-scale real-life test will be used to tune the data analysis for situations that require different balance between the detection probability and false alarms rate.

3 CONCLUSIONS

Human Security Radar (HSR) is a fully automatic standoff multi-threat detection system that can detect threat objects carried by people under clothes or in backpacks.

The ability of the system to detect dielectric objects using K_u-band radio waves has been confirmed in tests with real explosives and with simulants [1].

The metal detection capability based on the analysis of co- and cross-polarized amplitudes of the scattered radio waves is at an advance R&D stage.

The system may be additionally equipped with a gamma-spectroscopy module, which will turn it into a spectroscopic radiation portal.

The data analysis and data integration component of the HSR allows operation in an imaging or non-imaging mode. In the latter case the security personnel are only notified of the alarms, and don't need to constantly process any images.

The non-imaging capability and full automation of the data analysis removes some privacy concerns.

HSR can be used either as a standalone multi-sensor, or as an “early warning” component of a broader security system, in which it will preselect targets for in-depth inspection from a crowd without affecting the people flow. This may help to reduce the adverse effect of security measures on normal operation of the venue, and help to extend the security perimeter to places, such as mass transit systems.

4 REFERENCES

[1] Valery Averianov et al., “Automatic Standoff Detection of Threats in Crowded Areas” // in Proc. of the 9th Future Security Research Conference, Berlin, September 16-18, 2014, Klaus Thoma, Ivo Haring, Tobias Leismann (Eds.), pp.319-326 (2014).

[2] Boris Y. Kapilevich, Stuart W. Harmer, Nicholas J. Bowring. “Non-Imaging Microwave and Millimetre-Wave Sensors for Concealed Object Detection.” CRC Press, ISBN-13:978-1-4665-7719-0, eBook-PDF, (2015).

[3] Andrey Kuznetsov et al., “Device for Detection of Explosives, Nuclear and Other Hazardous Materials in Luggage and Cargo Containers”. CP 1194, “International Conference on Applications of Nuclear Techniques”, Crete, Greece, 14-20 June 2009, edited by K.Bharuth-Ram, pp.13-23. 2009 American Institute of Physics 978-0-7354-0731-2/09. ISBN 978-0-7354-0731-2 ISSN 0094-243X

MEASURING RESILIENCE - THE BENEFITS OF AN EMPIRICAL STUDY OF POWER OUTAGES BY MEDIA DATA

Thomas Münzberg[1], Marcus Wiens[2], Wolfgang Raskob[3], and Frank Schultmann[4]

[1] *thomas.muenzberg@kit.edu* [3] *wolfgang.raskob@kit.edu*
Karlsruhe Institute of Technology (KIT), Institute for Nuclear and Energy Technologies (IKET), Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen (Germany)

[2] *marcus.wiens@kit.edu,* [4] *frank.schultmann@kit.edu*
Karlsruhe Institute of Technology (KIT), Institute for Industrial Production (IIP), Hertzstraße 16, 76187 Karlsruhe (Germany)

Abstract

So far there are no empirical studies about power outage impacts. It is unclear at which level of a Power Outage Magnitude (POM), which is defined by the duration and the number of affected people, an interaction of emergency and disaster management authorities is requested by the affected people. To enhance the understanding and to provide evidence-based recommendations, we analyse a dataset that stores characteristic parameters of experienced power outages. The data provide insight into the impacts, magnitudes, causes, and undertaken response activities. The dataset is derived from the content of investigated media articles that report currently experienced power outages. The basic idea of an empirical study of power outages by media data is introduced in this paper. The result of a pilot implementation using 234 incidents is demonstrated and its benefit is discussed.

Keywords: Power Outages, Power Outage Magnitude, Data Analysis, Business Continuity Management, Disaster Management

1 INTRODUCTION

The German electricity system is increasingly stressed by the integration of new utilities and the ongoing transformation process towards more renewable and low-carbon energy generation [1]. As a consequence, the risk of power outages with their potential adverse impacts on the population and on the economy are progressively discussed in society, by critical infrastructure (CI) providers, and disaster management authorities.

Power outages differ in duration, number of affected people and the amount of assets at risk. In particular, in cases of short power outages, the management of consequences is left to the freedom of the individual without relying on official assistance. However, little is known about the tipping point that defines the critical level of a power outage magnitude that requires a response of official emergency and disaster management authorities. To enhance the understanding of response actions and to facilitate the development of contingency plans for business continuity and disaster management, we analyse a dataset on power outage incidents extracted from media articles. For this pilot study, we restrict the analysis on power outages that occurred in Germany in four months in the year 2013. The generated dataset is statistically evaluated with respect to key properties of power outages that are relevant for emergency and disaster management. Based on the results first conclusions can be drawn with respect to the response of emergency and disaster management authorities and electricity utilities. The paper introduces the basic ideas and the benefits of this approach and discusses directions for our forthcoming research.

This paper is structured as follows: In the first section we introduce the motivation for investigating media data of power outages. The data collection and compiling process is described in the second section. In section three we discuss the data quality of media articles based on a conducted pilot study. The data is exemplarily analysed in section four to demonstrate ways for analyzing and to discuss its benefit. We finish the paper with a discussion and show perspectives for our forthcoming research.

2 MOTIVATION AND OBJECTIVES

In the context of electricity system reliability evaluations, there are some indices that are based on statistical data and provide information about duration, the starting and ending time of power outages. Also the number of affected people and the causes of the power outage are considered. In Germany, this data is collected and analysed by the regulatory authorities and associations of the electricity utilities referring to the German Energy Act ('Energiewirtschaftsgesetz'). Some utility associations also collect such information with the help of their member utilities. The annual results of the analysis are published [2]. However, the raw data is not publicly available due to the legitimate interests of the utility providers. This makes it nearly impossible to conduct an advanced analysis for the purposes of disaster management planning.

Information about further impacts on the performance of CIs and interactions of disaster management authorities is not gathered. To make use of the reporting system within the German Energy Act, a change in the legal regulation would be necessary. Collecting and reporting this information would most probably imply a disproportionate effort and expenses for the electricity utilities and could even lead to higher prices for the customers. This might be a reason, why the impacts of power outages on vital services and productions, and the requested response actions of emergency and disaster management authorities and organizations are not systematically collected, stored, and analyzed. However, there are some studies about causes and impacts of major power outages that lasted long for days and affected a large number of people (e.g. [3]). There are also some studies that analyzed general impacts (e.g. [4]), and impacts specific to a CI sector like health (e.g. [5]). Beside this isolated information, there is still a lack of empirical data and analysis which could significantly enhance the understanding of power outage effect absorptions and of supply restoration. By now, a statistical evaluation on these issues is still missing.

Based on empirical insights of the consequences of power outages, local emergency and disaster management authorities could define protection target level or a operation criterion such as at which point in time of a power outage they should activate further resources to manage the potential impacts in their area of responsibility. This critical point in time represents a tipping point during a power outage in which advanced assistance of emergency and disaster management authorities is requested. Until this point in time, all affected people and CI operators rely on their self-helping and coping capacity resources [6]. By being able to define such a tipping point, it is also possible to scale different intensities of an incident. This is well known in the management of other hazardous incidents like floods (e.g. flood alarm levels), severe weather situations (e.g. wind warning scale), epidemics or pandemics (e.g. pandemic alert phases).

In the context of power outages, an evidence-based reference scenario could help to state protection target levels that should be reached by prepared and implemented response resources [7]. It would also be interesting to know, if there is a significant dependence between response measures taken and the duration and number of affected people.

3 IMPLEMENTING MEDIA DATA ON POWER OUTAGES

3.1 Power outage reports in media articles

Power outages are of great interest for a society. Reporters inform and critically review causes and characterizing impacts of an experienced power outage as well as undertaken response activities. The articles are often written and published directly after the power outage, in some cases also during the incident. This fast response is of course a source for uncertainties. Basically, journalists are committed to carefully double-proof each information they publish regarding reliability, plausibility, and correctness [8]. Due to these journalistic principles, we assume that key published information about the power outage character is reliable, although some uncertainty and bias of the journalistic description cannot entirely be ruled out.

3.2 Systematic investigation, collection and storing of media articles

The key idea is to use media reports for collecting characterizing parameters of power outages. In 2012 we started the research on investigating all media articles that are

- available online,
- in German language,
- published in daily or weakly press,
- reflect issues of a power outage from a retro-perspective, and
- focussed on regional news.

The most crucial aspect in this data collecting process is the detection of the media articles. To ensure a systematic search for news, the current awareness service of Google-Alerts is used. Google-Alerts automatically searches for new documents, articles and websites that match with predefined criteria. The results of the search are summarized and provided to the user periodically. We used Google-Alert and defined search for news that include the German word for a power outage (‘Stromausfall’). It is this word that most probably should be used when reporting a power outage. In this way, new contributions with this word on pages that are ranked by Google are detected by the Google News Crawler in the moment of its online publication. However, this process is criticized due to its lack of transparency. For the customer, it is not clear what sources are reviewed. This concern is also critically reflected in the discussion.

For the pilot implementation a small set of samples is used. Articles from August, September, October, and November 2013 were investigated in which 234 power outage incidents were described.

A very similar approach appeared in the end of 2013 with the Blackout Tracker by EATON Germany [9]. The Blackout Tracker also uses media articles to assess grid reliability. There is no description available how EATON designed the data collecting process. For the period under consideration, we compared our results with the results of EATON. Seven incidents are described by the dataset of EATON that are missing in our dataset. However, there are 174 out of 234 cases that were not represented in the data set of EATON but described by our dataset.

3.3 Data compiling based on media articles

A brief initial content assessment of the investigated media articles was necessary to identify information that characterise the corresponding power outages. To do so, we defined six information parameters that are used to describe power outages by the media. The parameters are listed in Table 1. The table also expresses how often the parameters are used in the detected incidents.

For each incident the information for the parameters is stored in a dataset. This dataset allows further statistical evaluations and comparisons of the power outage incidents. The information availability differs depending on the investigated media articles. It is not always possible to find details for each parameter. In these cases, the parameters are left empty and neglected.

Table 1: Overview of the information parameters and number of incidents for which information is available

Parameters		Number of incidents	Percentage
a	Date and day of the week of the beginning of the power outage	234	100
b	Starting and ending time or duration	186	80
c	Affected municipalities and the city or district in which the municipalities are situated	234	100
d	Number of affected costumers and further affected assets	72	30
e	Deployed emergency response measures (excluding those implemented by responsible grid providers)	14	6
f	(Root) causes	199	85

As far as it was reported in press, information about deployed emergency response measures is collected. Measures under consideration are for instance

- Activation of voluntary fire and rescue stations to receive emergency calls at neighbourhood level,
- Implementation of mobile emergency power units,
- Medical treatments of, for instance, elderly people or people who rely on dialysis centres,
- Supply of CI operators with fuel,
- Supply of the population with information, food, and beverages, and
- Evacuations of for instance hospitals, dialysis centres or nursing homes.

Responses for helping people who were stuck in elevators can be neglected. This and measures that are implemented by responsible grid providers are excluded in parameter e. Cases in which redundant hardware was activated to restore supply are archived.

Table 1 shows, that only in 30 per cent of all incidents information is available for the number of affected people. There are also various ways how the number of affected people is reported. This may lead to some uncertainties and inaccuracies.

In 83 incidents (35 per cent of all incidents), information about the number of affected people is available in the media articles. In eleven of these incidents (5 per cent of all incidents), it is not possible to evaluate this information. In these cases, the reporters used terms like “a street” or “a neighbourhood” that does not provide clear numbers of affected people.

Only in 12 incidents a clear number was provided (5 per cent of all incidents). In all other incidents, the reporters use the terms “number of households” (39 incidents, 17 per cent of all incidents) and “number of customers” (21 incidents, 9 per cent of all incidents). We assume that each customer represents a household. Thus the number of affected people can be easily estimated by the statistical average number of people living in a German household provided by the German statistic departments of the federation and the federal states. For 2011, the average number of people living in a German household is 2.02 [10].

Of course, this simplification induces some uncertainties because also industrial customers could be named as customers. For a better consideration of affected

industrial customers, more detailed information is necessary like the missing electricity load (KWh) or the resulting monetary loss (EUR). As far as no such kind of information is available there is no solution for this problem.

Based on the availability of information for each parameter, the power outages can be distinguished into six Information Value Categories (IVC)(see Table 2).

Table 2: Information availability by Information Value Categories (IVC)

Information Value Category (IVC)	Parameters for which information is available	Number of incidents	Percentage of all incidents
1	a	234	100
2	a, b	186	80
3	a, b, c	186	80
4	a, b, c, d	66	28
5	a, b, c, d, e	7	3
6	a, b, c, d, e, f	7	3

Emergency response activities were reported for 14 incidents (6 per cent), but only in 7 cases (3 per cent) all information for the parameters a, b, c, d, and f is available.

It is interesting to see that only 28 per cent of all investigated power outages information for the parameter a, b, c, and d is available in the media articles. This may reflect the high uncertainty in the direct aftermath of such an incident in which the reports are written. The missing information about the number of affected people is a key factor for this result.

Although the availability of information does not allow interpretation of the power outage itself, the information quality expresses how well media reports power outages.

4 APPROACHES FOR AN EMPIRICAL STUDY OF POWER OUTAGES

Evidence-based insights on power outages can be won on the basis of the compiled dataset of power outage characterizing parameters. We look at the set of 234 incidents and highlight tendencies regarding the time of power outage occurrences, magnitudes, and response interactions This set is of course too small for identifying significances and evidences, however it allows to display some ways for a study and to discuss the benefit.

Fig. 1 shows the number of incidents that happened in the months under consideration of August, September, October, and November 2013. Most incidents started on a Monday (42 incidents), on Thursday (39 incidents) and on Friday (40 incidents). Fig. 2 shows the number of incidents per day of the week.

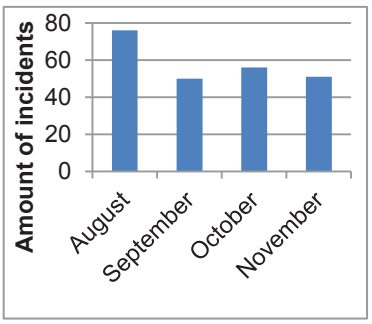


Fig. 1: Monthly incidents

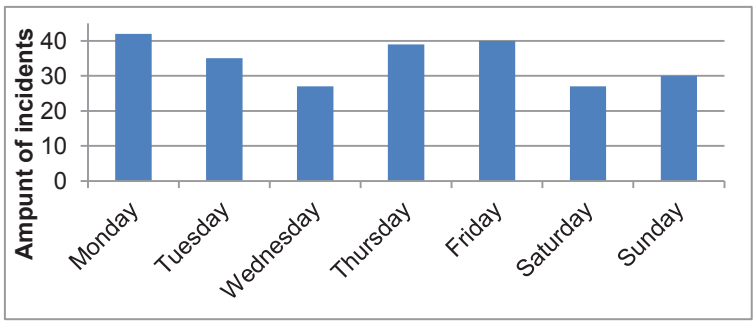


Fig. 2: Numbers of incidents on different days of a week

The power outage started at different times of day. Fig. 2 displays how many power outages started at different times of a day. Most of the detected incidents for which the

starting time is known (n=163) started between 12 a.m. and 1 p.m. (14 incidents), 7 p.m. and 8 p.m. (13 incidents), and 5 p.m. and 8 p.m. (12 incidents).

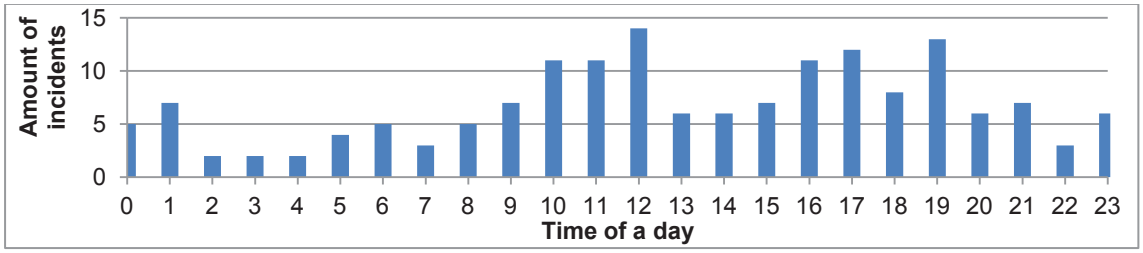


Fig. 3: amount of power outages that started at different times of day

The duration and the number of affected people are the main parameters to characterize a power outage. We define the product of both parameters as the Power Outage Magnitude (POM) which describes the intensity of a power outage. The POM can be calculated for all incidents of the information value category 4 (n=66) (Fig. 4).

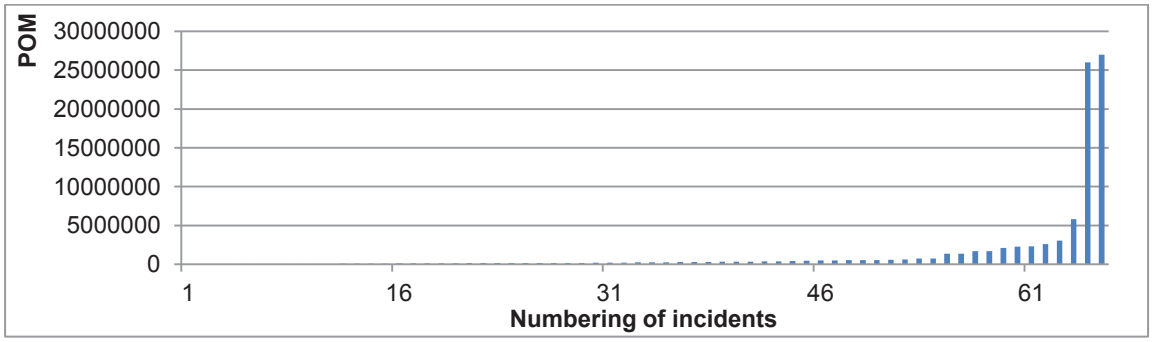


Fig. 4: Statistical representation of the Power Outage Magnitudes (POMs) for 66 investigated incidents

The incident's POM can also be displayed in a diagram (Fig. 5). In Fig. 5 we visualized those incidents in which further emergency response activities were deployed by the emergency and disaster management authorities and reported in media (see yellow dots, n=7).

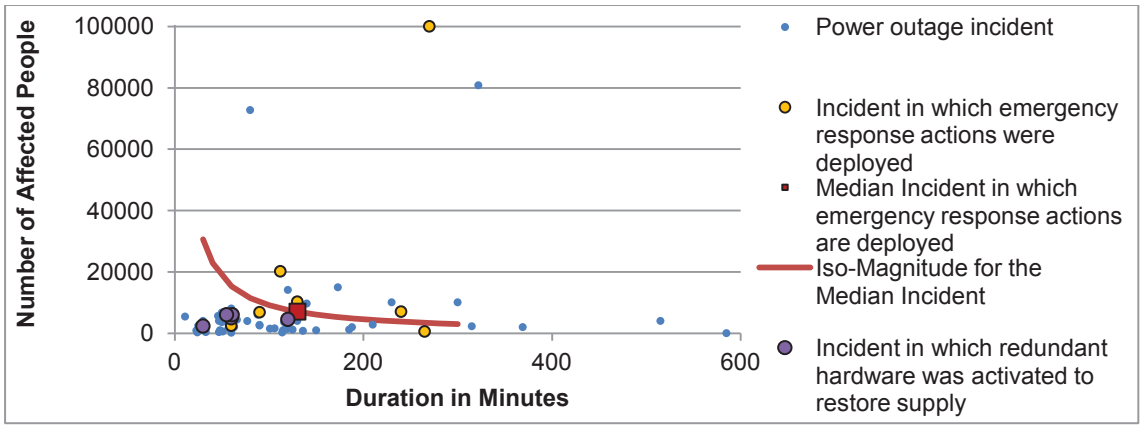


Fig. 5: Power outage incident characterized by POM. The incidents in which emergency response actions were deployed (n=7) and in which redundant hardware was activated to restore supply are marked (n=5). Also the Median Incident and the Iso-Magnitude are displayed.

The POM-calculation could also be the basis for further analysis to derive normative theories about the tipping point for the necessity of emergency response actions.

Such finding might be possible by using regressions with a larger dataset. Another way could be to describe a Median Incident derived from the median duration and a median

number of affected people of those incidents in which emergency actions were deployed (see the red square). This point expression can also be expanded to a line expression. This Iso-Magnitude displays a constant POM for incidents that have different durations (see the red graph).

A theory could state that such lines are understood as tipping points at which interventions seem to be necessary for incidents that have a higher magnitude. We exemplarily reviewed the starting point of incidents that have a higher POM than the Iso-Magnitude and for which no emergency actions were reported. However the number of incidents taken into account is small, it interesting to see that in six of the seven cases the power outage happened in the late evening or night times (7.55 p.m., 5.00 a.m., 11.15 p.m., 12.52 a.m., 7.30 p.m., 8.00 p.m., 4.55 p.m.). This may express a less relevance for blackouts that start at evening or night time. The effect could be caused by reduced activities and dropped electricity demands at this time. It would be interesting if this effect could also be recognized in larger datasets.

Another indicator for a tipping point could refer to grid-based mechanisms that support fast restorations of electricity disruptions. The German grid is for instance designed with redundancies (n-1-principle). If there is a failure in one device like a power line, a redundant hardware like a second power line is available and can be activated to keep a region supplied with electricity. As far as these mechanisms enable a fast recovery, an interaction of emergency and disaster management authorities might be not required. The analysis of articles showed five cases in which the supply was restored by using a redundant hardware. The relationships among the values could be estimated by a further regression analysis.

The demonstration of study approaches based on the incidents investigated in the pilot study showed promising ways to enhance the insights on power outages and the response to their impacts. However, the number of samples is much too small to identify significant findings.

5 DISCUSSION AND ONGOING RESEARCH

The paper demonstrated how media articles about power outages are detected, and what parameters could be compiled and stored in a dataset. 234 incidents were investigated, reviewed and analyzed in the pilot study of power outages by media data. This dataset allowed different studies which were exemplarily conducted and discussed. The result showed promising approaches for enhanced and evidence-based insights of power outages and of the emergency responses. Since this is an ongoing research, some aspects are of great interest for the ongoing research.

At the moment Google-Alert is used to investigate new media articles. Although the results are much better than the EATON-approach [9], it is unclear how well the used detection process identifies relevant media articles. To double check the results and if necessary to increase the detection rate, further current awareness services and other tools as well as messages in social media could be used in parallel in the future. For the future we assume that more articles are published online through continuing digitisation of journals and newspapers.

Not every power outage is reported in the media. It would be interesting to know how many incidents are reported and investigated compared to those automatically reported to the regulatory authorities by the grid operators.

At the moment, there are only a few incidents and reports that can be categorised in higher IVCs. The main reason for this is missing information about the number of affected people. If more reports would include this, a significant higher quality for the evaluation could be reached.

Although the number of samples used in the pilot is too small for significant findings, it was demonstrated there promising approaches to enrich the understanding of power outages and to identify evidence-based reference scenarios for disaster management planning. Currently, we are compiling media reports about power outages in 2014. The review of articles for incidents that happened in a whole year will result in a larger dataset and probably will allow significant empirical findings.

ACKNOWLEDGEMENT

This research herein is associated to the portfolio project "Security Research" of the Helmholtz Association and embedded to our research in the Centre for Disaster Management and Risk Reduction Technology (CEDIM). We are grateful for the technical and financial support of both institutions.

REFERENCES

[1] Hayn, M., Bertsch, V., and Fichtner, W. (2014). *Electricity load profiles in Europe: The importance of household segmentation*. Energy Research & Social Science 3, 30-45.

[2] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (2013). *Versorgungsqualität - SAIDI-Wert 2006-2013*. URL:http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/Stromnetze/Versorgungsqualit%C3%A4t/Versorgungsqualit%C3%A4t-node.html [06/10/2015].

[3] Union for the Co-Ordination of Transmission of Electricity (2007). *Final Report System Disturbance on 4 November 2006*. URL:https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf [06/10/2015].

[4] Hiete, M., Merz, M., Trinks, C., Grambs, W., and Thiede, T. (2010). *Krisenmanagement Stromausfall, Krisenmanagement bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg*. Stuttgart, 2010.

[5] Klinger, C., Landeg, O., Murray, V. (2014). *Power Outages, Extreme Events and Health: a Systematic Review of the Literature from 2011-2012*. PLOS Currents Disasters.

[6] Münzberg, T., Wiens, M., and Schultmann, F. (2015). The *Effect of Coping Capacity Depletion on Critical Infrastructure Resilience*. Proceedings of the 12th ISCRAM Conference, L. Palen, M. Buscher, T. Comes, and A. Hughes, eds.

[7] Münzberg, T., Wiens, M., and Schultmann, F. (2014). *Dynamic-Spatial Vulnerability Assessments: A Methodical Review for Decision Support in Emergency Planning For Power Outages*. Procedia Engineering 78, 78-87, 2014.

[8] Deutscher Presserat (2001). *Publizistische Grundsätze (Pressekodex)*. Richtlinien für die publizistische Arbeit, URL:http://www.presserat.de [06/10/2015].

[9] EATON Germany (2015). Blackout Tracker, *Jahresreport 2014 Deutschland, Österreich, Schweiz*. URL http://powerquality.eaton.com/Deutschland/About-Us/DE-blackouttracker-form.asp [06/10/2015].

[10] Statistische Ämter des Bundes und der Länder (2015). *Gebiet und Bevölkerung – Haushalte*. URL:http://www.statistik-portal.de/statistik-portal/de_jb01_jahrtab4.asp [06/10/2015].

TOWARDS A BETTER UNDERSTANDING OF CYBER CIVIC RESILIENCE (CCR)

Beatrix Wepner[1] and Misse Wester[2]

[1] *beatrix.wepner@ait.ac.at*
Innovation Systems Department; Research, Technology & Innovation Policy;
AIT Austrian Institute of Technology GmbH, Donau-City-Str. 1; A-1220 Vienna, Austria

[2] *misse.wester@foi.se*
FOI, Swedish Defence Research Agency, SE-164 90 Stockholm

Abstract

Today's society is characterized by an increased reliance on cyber services. This creates advantages for the citizens in terms of ease and availability of services, but also increases the vulnerability as more and more services are not possible to perform outside the cyber realm. The reliance on cyber services can both increase a cyber civic resilience, as the virtual society can provide an alternative to the physical one.

However, it can also be argued that an increased dependence on cyber services decreases resilience as the available alternatives diminish. If the whole of cyber space would fail, the consequences for our society would be paramount. Priority-setting processes cannot only rely on technical developments but must also take into account the respective views of different stakeholders. This is why social rationales for priority-setting in the domain of cyber security must be considered as well as technological advances.

The awareness among citizens and service providers of possible pitfalls of being a cyber-citizen needs to be increased. In order to understand what factors contribute to the strengthening or weakening of cyber resilience, we propose that the following areas need to be better understood:

- Social aspect, including trust and trusted group;
- A better understanding of the mechanisms behind cyber citizens' self-organization in the virtual domain;
- The role of privately owned networks and online platform and the consequences this has for privacy concern;
- and finally political and legal aspects.

The identification of Cyber Civic Resilience (CCR) as a major area for future research highlights the recognition of the growing importance of the citizen as a major source and agent of (cyber-)security.

The concept of CCR thus serves as a novel way of framing significant future research needs in relation to societal security. In this contribution, these aspects will be developed in length and their relation to the resilience of the cyber civic society will be discussed. Future policy recommendations were developed in these aspects within the EU funded ETTIS Project and will be outlined briefly.

Keywords: Cyber Civic Security; resilience; privacy; responsibility; awareness; citizens

1 BACKGROUND ON CCR IN THE CONTEXT OF SECURITY RESERACH

In order to create a common understanding for this field, it is important to clarify how we define Cyber, Civic and Resilience. As such, these definitions have no ambition to be exhaustive and exclusive, but rather serve as a starting position for further developments in the field.

'Cyber' will be used to denote anything involving computers or computer networks (i.e. the Internet) and services used in this context. Examples of this can be simple information sharing via the Internet, the use of social media, on-line transactions, as well as more elaborate forms of government initiated e-Governance and e-Government services.

'Civic' in this context will refer to a citizen perspective. This excludes states, business and organized networks, such as criminal or terrorist networks, but will relate to all services or applications that relate to citizens – in our capacity as creators or users of cyber services. The perspective is from a user-oriented, lay perspective with the main focus on civil usages.

'Resilience' is often used to describe the strength or ability of something to return to its original or better state after a disruption. For our purposes 'Resilience' will be used to focus on the capacity of citizens to use cyber services in times of insecurity, but also to use cyber services in a way that will strengthen resilience. This includes, but is not exclusive to, sound uses of cyber services without becoming overly reliant of these services. It also means that cyberspace can be a tool in increasing civil society's resilience after e.g. a disaster.

Figure 1 can be used to better understand how cyber space can be organized, what actors are present in the different 'communities' and also identify areas in which resilience can be strengthened or weakened.

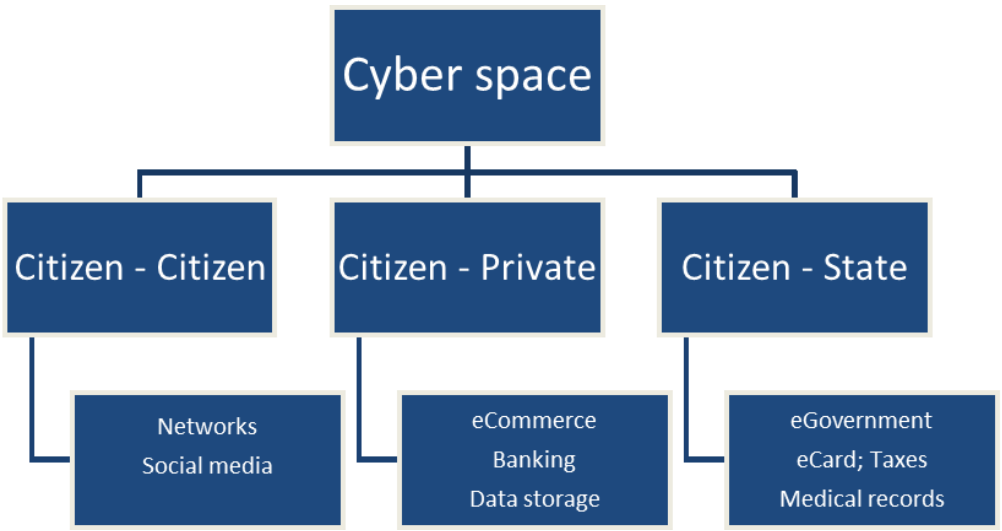


Figure 1: Defining cyber space and interactions

In this EU funded ETTIS Project security challenges were clustered and new thematic and structural options and priorities were worked out and formulated in order to stress future needs in research and policy. The project first of all delivered a range of rather specific threats, and secondly an overview of overarching security needs in four domains under study, Cyber Civic Resilience being one of them.

This material has been used to develop the security issues in a series of technical meetings. Future "solutions" to these security challenges, or "research-based opportunities for tackling security challenges", can be of two different kinds:

- Thematic ("What?")
- Structural ("How?")

The distinction between thematic and structural research-based opportunities is important, because a key argument of ETTIS is that not only different thematic agendas are needed in the future, but also new structures and processes in our research and innovation systems in order to enable the proper handling of these novel thematic agendas.

Once these thematic and structural research-based opportunities have been identified and assessed the shift towards the more political aspect of prioritization from the perspective of different stakeholders was addressed ultimately pointing also to new types of policy instruments that may be needed for realizing the new agendas (Figure 2).

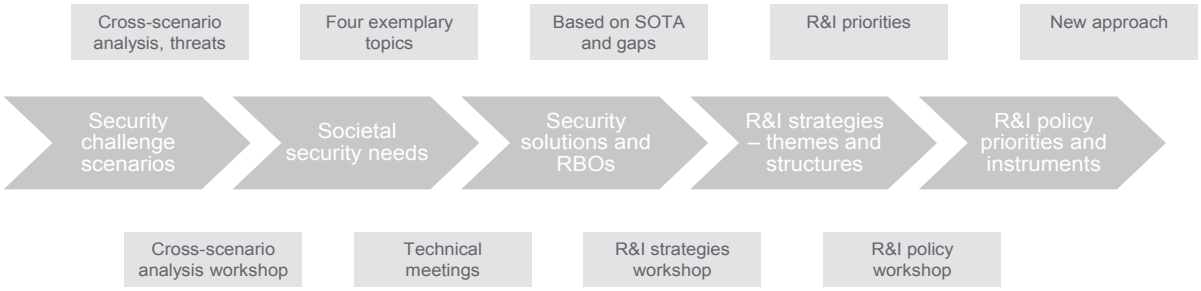


Figure 2: ETTIS work flow from Security Challenge Scenarios to R&I Priorities & Instruments

2 RESEARCH AREAS FOR CHALLENGE-DRIVEN RESEARCH ON CCR

Some of the identified research challenges and research based opportunities related to cyber civic resilience and related disruptive events in regard to cyber and society will be discussed as examples in this paper. The research based opportunities were in some parts very generic and in other parts on a very granular and thematic level. The examples of research areas portray a great variety of challenges in relation to CCR. Besides the importance of the reference object for security taken we can notice the importance of social aspects and need for legal regulations as well as for creation of awareness of the rights and obligations of cyber citizens, a summary is depicted in Box 1. A subsequent step is hence to reconsider how the governing of R&I ought to be done regarding challenge-driven research.

Box 1: Cyber Civic Resilience – Overview of examples of research areas

Technological research
- Security of big data and cloud computing;
- Cyber service technologies and civic resilience;

Research on social behaviour
- The emergence of trust and trusted groups;
- Awareness and behaviour with regard to possible attacks;
- Citizens‘ self-organisation as a means to enhance resilience and the formation of norms;
- Cyberbullying as a social phenomenon;

Economics of cyber security
- The resilience of e-commerce;
- The hidden costs of cyber services;
- The role of privately owned networks/platforms for the provision of cyber services;
- Business models and the transparency of data use.

Political and legal aspects of CCR
- New forms of cyber policy;
- The militarisation of cyber space;
- Cyber rights and obligations: informed cyber citizenships;
- International regimes of cyber governance, regulation and standards.

Cyber education and skills
- Citizens’ awareness of cyber-security;
- Understanding digital literacy;
- Dealing with a societal backlash in cyberspace.

2.1 Social aspects

When it comes to social attributes being considered in the cyber world a lot of aspects have been neglected in the past while others like mobbing have earned a lot of attention. High consideration should be paid to research in trust and trusted groups in order to consider how trust can be built through mere technical means and not personal contact. On the other side of this stands the need to create awareness of possible attacks and threats that would diminish trust in the cyber world, giving hints for possible system weaknesses in ICT.

Vital issues of discussion are privacy and trust. Protecting individual privacy has been a topic for discussion since the introduction of the camera and is continued in the cyber domain today. Attempting to find one definition for each term is in itself a research project, so it might suffice here to say that privacy can be interpreted as an individuals' right to be left alone and unaffected by the larger society outside (and this includes everything from states to spouses). This does not mean that the state is solely responsible for protecting the citizens' privacy; it also places responsibilities on the citizen not to divulge sensitive information about herself in various public or private forums. Alongside with this comes the question to what extend would the state allow total privacy or would want the individual to reveal information about herself thus gaining insight and control.

Trust in the civic cyber domain means on one side that users can trust other users to be the person (or person) he or she claims to be on the other side trust can also be seen as the security of the integrity of the systems, i.e. functional trust. Trust in this context needs to be both pragmatic and formalized. However, it can be stated again that the reliability and trustworthiness of the systems need to find a balance between realistic expectations of what services cyber citizens want to have access to and what is technically feasible. Furthermore the role of states and private companies, and how they perceive the issue of trust needs to be considered. Users develop new ways of using technologies or technical applications in ways that developers did not intend or foresee, so developing systems that can be trusted even if unpredicted usages occur, is important. This means that unintended uses of a specific technology should be acknowledged and adjustments made to accommodate the needs of the users. This calls for a broader involvement of end-users into the design phase integrating the needs and preferences of the users in developing services. In this way, ad-hoc solutions to fit user needs can be reduced and perhaps in doing so security and resilience of systems can be increased.

2.2 Mechanisms behind cyber citizens' self-organization

Humans have always found ways to organize themselves despite the absence of formal structures. In the process of self-organization, negotiations take place. Since the cyber citizen is free from possible physical restraints (like time, space, permeation or fluidity) the citizen is in some ways free to interact with others regardless of the physical distances or barriers between them. Reaching out to others in the cyber domain might be easier than approaching them in other contexts. This means that new forms of interaction between different actors can be achieved in the cyber domain, which was previously not possible. As result cyber activities are increasing in sophistication, where digital groups and networks cut across geographical boundaries and sovereignties, operate instantaneity and anonymously, and constantly reconfigure their structure. The question arising is if the use of internet and the cyber realm increases the individual´s vulnerability or resilience as self-organization becomes easier across boundaries, time and space.

Therefore linked to the specific functions of cyber services is the need to better understand the mechanisms behind cyber citizens' self-organization in the virtual domain. There is research to suggest that there are emergent norms that develop in interactions between cyber citizens, but in order to adapt the cyber world to the specific needs of the citizens therein this must be better understood and met. Citizens could also play a more active and permanent role in cyber resilience but it is still unclear how and in what way. At this point in

time, most citizens do not play an active role in cyber civic resilience. Mostly their role is issue-specific (i.e., response to a major crisis) and often mediated through other organizations (third sector type of organizations, public authorities and private companies). In terms of strengthening resilience, the role of cyber communication between different groups in times of crisis should be investigated as well as the role of individual citizens.

2.3 The role of privately owned networks

Privately owned networks play a major role in social function nowadays. This role of privately owned networks and online platforms needs to be considered in more depth. For example, many private services such as social media or commercial applications, might serve a public function. In the case of a failure in the service, public functions might suffer. This calls for a broader approach where the social functions of various services needs to be better understood and what role these play for civic resilience and security. By looking at services for this perspective, patterns of how services are used can become clearer and the consequences of failure can be better predicted and managed.

2.4 Political and legal aspects

Political and legal aspects need to address a variety of topics considering the cyber civic society and its resilience. The misuse issues increase along with the use of internet and possibilities therein. The risks created in the cyber domain is to some extent the responsibility of the citizen to manage, but is in other ways out of the citizens' control. No matter how one considers it the major issue is to increase awareness of cyber citizens, i.e. users of the internet, to the risks and potential threats.

Alongside with blurring or non-existing boundaries within the cyber space the need for new definition of legal aspects, responsibilities and protection arises. Not only prosecution in case of criminal acts but also protection of rights, individuals and data within the cyber space need to be taken care of and responsibility for these aspects has to be taken on. New data regulations as well as legal regulation across borders or prosecution across borders are to be developed and become operative and effective. Hand in hand with these considerations comes the debate on arising expenses and reimbursement and the balance of funding.

International and national regulations, security standards and guidelines should not stop or slow down the positive impact of cyberspace (e.g., economic growth and technological development) or reduce the trend toward resilience. There is the danger that an exaggerated concern with security could reduce the generativity of the Internet – the ability to put information technology to many different, initially unforeseen uses that have been identified as central to the development of the online economy. Stakeholders need to find the right balance between regulation, security, flexibility, cost–benefit considerations, resilience and openness of cyberspace. The direct and indirect impact of cyber measures on individual rights (i.e. privacy) and key societal values (i.e. trust, solidarity, inclusiveness, etc.) also has to be carefully assessed. For instance the controversial discussion on universal identification, which could apparently solve the issue of attribution, has polarized the debate between those who believe that international or national agencies could provide Internet identity credentials, based on other identification systems (e.g. passports, national identity cards, driver's licenses, etc.), and those who assert that attempting to build such a system is futile, and will only give criminals and hackers new ways to hide while hindering fundamental rights. Public concerns related to the fact that exaggerated fears over cyber security might cause governments to take excessive measures, and that these measures could lead to increased online surveillance, censorship, and the removal of the potential for legitimate anonymity stress the importance to take into consideration security and individual rights trade off when devising responses for building cyber resilience.

It might be beneficial to remember that cyber citizens make use but are also constrained by the options that are available to them. This means that research aimed at understanding and

promoting issues such as trust, risk avoidance and safe cyber behaviour is not enough. Cyber rights and obligations, that should be met by cyber citizens, are not very well defined, unstructured or following any borders. The balance between sound cyber behaviour, e.g. in order to protect one's privacy, and the lack of alternatives to some public cyber functions, such as having medical records stored electronically despite security risks, is not one that will be achieved by targeting the cyber citizens alone. Instead, research should be directed at investigating if and to what extent developers of technical solutions or services perceive the expectations and needs of the users. By focusing research on developers it will be possible to harmonize the developers' ideas with actual needs of the cyber citizens.

New forms of cyber policy need to be established. For instance, several countries have, or are considering, giving their militaries a role in the defence of cyberspace. There is a danger that the Internet could become increasingly militarized, with negative implications for its civilian use. Therefore careful thought is needed about the conceptual models of cyber security and cyber resilience that are used to attribute responsibility to organizational and potentially to individual actors. Militarization of cyberspace needs to be critically assessed. This includes but it is not limited to research on what constitutes cyber rights and cyber citizenship, both for individual and organizations, but also how more adaptive and innovative regulatory approaches could be developed to quickly respond to fast-moving technological developments without hampering innovation and the generative impact of cyberspace. Predictive research in order to foresee vulnerabilities may be one step towards IC technology assessment and the proper application of a technology and directions for behaviour of users.

2.5 Further aspects

Technological aspects: The obvious investigation, research and development of new and safer encryption methodologies or sensors and automatic identification of behavioural patterns are some of the possible technical strategies to increase resilience in the cyber world. Technical considerations that were thought of importance during the workshops include big data research and secure cloud computing. However, especially considering civic resilience in the cyber world, it needs to be investigated how resilience in the citizen-private and citizen- state interactions can be maintained if the Internet is disturbed or collapses completely. These include, but are not limited to, gaining a better overview of how cyber services contribute to or weaken civic resilience. Topics here might include the availability of non-cyber alternatives to cyber services; consideration of open or closed cyberspaces, investigating the awareness of the limitations of the technology among users and developers; alternative or unintended usages of technology. Technological aspects were not considered to be the most important matter in cyber civic resilience, but the focus was more on social aspects. Complete dependency on the internet (e-banking, e-commerce, e-government etc.) may create a societal backlash just to state an example for the strong linkage between social and technical aspects.

Education is as in other fields a support function for cyber civic resilience. Research needs to be conducted on digital literacy and illiteracy. As mentioned before civil society could start rejecting the use of the internet and interconnected services thus causing society to rethink the offers run over and dependency on the internet (e-banking, e-commerce, e-government etc.) creating a societal backlash. Education must go towards a direction to create cyber intelligence and awareness of possible online loss of privacy in the civil cyber society. A healthy civil society sphere may provide solutions and strategies for civil empowerment in the cyber world.

Economic aspects especially in regard to the ever-present and still expanding e-commerce are a wide field for research. From the civil perspective besides e-commerce, there are often hidden costs connected to cyber services. Personal information is collected and stored in ways that are not transparent to users, and the option to not use specific services without prevailing personal data is limited. The risks that face cyber citizens are created by the opportunities and constraints of the technical infrastructure.

3 REQUIREMENTS FOR A CHALLENGE-DRIVEN RESEARCH ON CCR

This section presents a list of 'requirements', which were identified as particularly relevant for CCR. This list originated from group work at another workshop with participants from the ETTIS-consortium and external experts on cyber security.

- Use a comprehensive cyber civil society approach
- Include the needs of those affected
- Include both long-term and short-term perspectives
- Include a global geographical area of concern
- Importance of inter- and trans-disciplinary research
- Information, awareness and trust in society
- Ethical and legal considerations

The portfolio of research projects in the field of CCR should aim to balance the mix of long-term and short-term time perspectives, as technical projects may have a short term perspective, while social aspects need to be considered in a longer time horizon. Creation of awareness and education of cyber citizens also need to be addressed in a long-term perspective in order to establish a secure civic cyber society in the future. The scope of cooperation in the CCR field has to be on a wide geographical basis, as the cyber world does not stop within boundaries, including multi-stakeholder from various countries, regions and educational levels.

3.1 How these requirements could play out in the different phases for CCR

3.1.1 Phase I: Structuring of challenges

The first phase is to identify, elaborate, assess and finally select challenges that the R&I program should respond to. Since this phase strongly relates to the agenda setting it also shapes the subsequent steps, which makes it particularly important to have a wide scope, and be careful of concepts and utilizing well-defined terminology.

A successful R&I strategy for an area like CCR must recognize that many solutions are non-technological in nature, trans- and multidisciplinary research approaching the security topic in a comprehensive way is therefore necessary. They may involve new technologies, but in essence they are about social awareness and change and take ethical considerations into account. What is key to this model is the locus of innovation. It does not take place in a specific technical lab, but in the midst of society itself. The R&I infrastructure for social innovation thus consists of a much broader spectrum of organizations than in traditional research, the needs of those affects have to be taken into account: in addition to conventional research institutes, civil society organizations involved in transdisciplinary social research (i.e. more bottom-up in the sense of engaging ordinary citizens), but also intermediary organizations (such as traffic red cross, i.e. organization of a more top-down nature) and SMEs (e.g. app developers).

3.1.2 Phase II: Development and assessment of options

Phase II is the development of challenges into main overarching themes for the research, specific calls for different areas and funding of proposals. The result can be seen as the development of a portfolio of options that can inform subsequent steps.

Since the area of CCR can be considered a novel field, the most relevant previous research needs to be collected from a number of related fields. The knowledge-base in the field of CCR has a strong focus on technical aspects, such as developing the best hard and software, but the focus will need to return to the 'civic' aspect and select the portfolio of options accordingly. Individual projects may include a comprehensive cyber civil society

approach, but with a strong focus on trans- and interdisciplinary research, merging social, technological and other facets. Individual projects could focus on specific countries or geographical regions, but need to strongly consider the needs of those affected, like different social and educational backgrounds in various countries.

3.1.3 Phase III: Implementation of research

Actual research projects can have a limited focus in terms of approach to security, time-perspective, geographical region, and need not be inter- or trans-disciplinary, but should in CCR be addressed differently. In phase III, the implementation of research, it is necessary to identify the best solutions to address the CCR challenges, irrespectively whether they came from one or another scientific subject. Consequently inter- and transdisciplinary research can contribute to find relevant and effective solutions for CCR. Eventual 'solutions' identified in research should be analyzed for potential side-effects, taking into account the wider needs of the actors.

The additional ethical considerations caused by potential policy-implications should be anticipated in the research. In general, research needs to be aware of the requirements identified above in order to be able to position the research in a wider policy context. In CCR education, awareness and trust in society is always a necessary add-on to each implemented solution. Thus in the implementation phase, each implementation action should consider whether additional education and awareness activities could improve the impact.

3.1.4 Phase IV: Evaluation and monitoring

Research programs, research calls and individual research projects should ideally be evaluated in relation to all the requirements identified above. However up to now H2020 research projects are hardly ever evaluated against their relevance, efficiency and effectivity. It might be argued that in industrial research, this is not necessary, as the companies and the market are an indicator for the evaluation.

However in challenge driven research, monitoring and evaluation against relevance, efficiency and effectivity to address social challenges is inevitable. Given the specific comprehensive approach to cyber civil society, an evaluation of success and impact is necessary to support iterative learning. Ethical and legal considerations, as well as considerations about trust and privacy in society can be used to evaluate research results and monitor their impact to society. Given the fact, that CCR has a short term component and a long term component, an evaluation and monitoring against expected long term effects can support the effectiveness of the research impacts.

REFERENCES

[1] Sofaer, Abraham D., and Goodman, Seymour E. (2001). "Cyber crime and Security. The Transnational Dimension", in The Transnational Dimensions of Cyber crime and Terrorism, Hoover Institute, Stanford, CA, 1-34.

[2] Winslett, M., Yu, T., Seamons, K. E., Hess, A., Jacobson, J., Jarvis, R., Yu, L. (2002). Negotiating trust in the Web. Internet Computing, IEEE, 6(6), 30–37.

[3] Colesca, S. E. (2009). Understanding trust in e-government. Inzinerine Ekonomika–Engineering Economics, 3, 7–15.

[4] Lyon, D., Ball, K., & Haggerty, K. (2012). Routledge handbook of surveillance studies. Routledge.

[5] Eriksson, M. (2012). On-line strategic crisis communication: In search of a descriptive model approach. International Journal of Strategic Communication, 6(4), 309–327.

[6] Reports and Deliverables from the EU funded, collaborative research project "European Security Trends and Threats In Society (ETTIS)"; http://ettis-project.eu

WAKE-UP TRANSCEIVERS FOR MONITORING CRITICAL INFRASTRUCTURE – A PROTOTYPE OVERCOMING DUTY CYCLING IN WIRELESS SENSOR NETWORKS

T. Kumberg[1], R. Tannhaeuser[1], L. Zimmermann[1], M. Schink[1], C. Schindelhauer[2] and L.M. Reindl[1]

[1]*timo.kumberg@imtek.uni-freiburg.de*
[1]University of Freiburg Department of Microsystems Engineering – IMTEK Laboratory for Electrical Instrumentation, Georges-Koehler-Allee 106, 79110 Freiburg (Germany)

[2]*schindel@informatik.uni-freiburg.de*
[2]University of Freiburg – Computer Networks and Telematics, Georges-Koehler-Allee 51, 79110 Freiburg (Germany)

Abstract

We present a powerful, but nevertheless low power and flexible, wireless sensor node utilizing a wake-up transceiver. The sensor node is equipped with several kinds of sensors, such as temperature, pressure and acceleration to monitor critical infrastructure. In sleep state, the node consumes only around 9 µW. We present a wake-up multi-hop routing protocol that supports the use of wake-up receivers in combination with long-range communication radios. The wireless sensor nodes and the routing protocol are tested at a large-scale highway bridge in south-west Germany, where a prototype network was installed in June 2015. A gateway node equipped with a Global System for Mobile Communications (GSM) modem transferred the network data to a remote server located at the University of Freiburg.

Keywords: Monitoring of critical infrastructure, Wireless Sensor Network, Wake-up transceiver, wake-up multi-hop routing protocol.

1 INTRODUCTION

Structural Health Monitoring (SHM) of critical infrastructure such as bridges is necessary in order to evaluate structural performance and to detect anomalies or threats originating from damages or deteriorations at early stages. SHM can provide real-time information to evaluate structural behaviour, estimate remaining life time, to assist in bridge maintenance planning, to verify the construction design and to deliver important data in case of disasters or extreme events [1, 2]. SHM is often realized with the help of Wireless Sensor Networks (WSNs), as they are cheap and easy to install on existing structures [1, 3]. They consist of wirelessly connected sensor nodes which are self- or battery-powered small units.

For long-term monitoring, sensor nodes are unattended over longer periods of time, since they are placed in remote areas where replacing of batteries is not feasible. Therefore, long node lifetimes are desired and the power consumption of WSNs has to be minimized. A possible way to save energy is an energy efficient communication protocol such as the on-demand communication approach [4]. Here, wireless sensor nodes have no synchronized listening and sleeping phases, but listen permanently in a low energy stand-by state and wake up to full functionality only after receiving a wake-up call or triggered by a sensor. An advantage of the on-demand communication approach is the low latency: since there exist no scheduled sleeping phases, messages can be sent immediately. For example, if a sensor detected a critical signal, this message may be transmitted to the gateway without further delay as would be the case when long and uninterruptable sleeping phases are implemented.

Wardhana et al. [5] analyses the reasons of bridge failures in the United States between the years 1989 and 2000. They analyse more than 500 failures of bridges, which had an average age of 52.5 years. Their analysis shows that the failures mostly took place during service life time and that 83% of the failures were triggered by an external event, like floods, earthquakes, fires, hurricanes, overloads and impacts of vehicles. This means, that continuous monitoring of bridges can be used to early detect such events or at least their impact which could be critical to the infrastructure. Taking this into account, on demand communication protocols can potentially save precious time by quickly broadcasting sensor data of triggering events. At the same time, on demand communication protocols can save energy by performing low duty cycling and asynchronous measurements.

Another advantage of wake-up transceivers, which support on demand communication, is their enhanced robustness because no clocks need to be synchronized. So, the embedded software may be reset at any time, e.g. if a fatal error state occurs. New nodes can easily be integrated into an existing network which is running in low duty cycle periods. Additionally, pulling data from the network or demanding extra measurements can be done easily – a great advantage during bridge maintenances. But the on-demand communication approach also poses new challenges, as sending of a wake-up signal can be more expensive than sending of a communication message [6]. Another challenge arises from the lower sensitivity of the wake-up receiver compared to the sensitivity of the communication radio, which requires several wake-up messages to reach a sensor node in communication range [6]. Therefore, protocols have to be used that are able to cope with these challenges.

Here, we present a powerful but flexible wireless sensor node utilizing the wake-up transceiver. The node is equipped with different kinds of sensors, such as temperature, pressure and acceleration to be used for SHM. We present a WSN installed on a large-scale highway bridge in south-west Germany and introduce a static wake-up multi-hop routing protocol. A Global System for Mobile Communications (GSM) gateway node is used to transfer the network data to a remote server.

2 RELATED WORK

Several WSN have been introduced for SHM of bridges which usually consist of sensor nodes that acquire process and transmit data. Lynch and Loh [3] give a comprehensive overview of wireless sensor node prototypes for SHM in academic and commercial context available during the years 1998 – 2005. In their work [3], they emphasize on the lower cost of installing a wireless monitoring system compared to tethered systems. They also reviewed available operational systems (OS), radio transceivers and data processing techniques to be used for SHM systems. In [7] Lynch et al. present a WSN consisting of 14 nodes to measure the acceleration response of the Geumdang Bridge.

Kim et al. present in [8] a WSN deployed on the Golden Gate Bridge consisting of 64 nodes that measured ambient vibrations, and a base station that was a Laptop. Due to the large size of the Golden Gate Bridge the network included a 46 hops multi-hop route. Similar to this work, Whelan et al. [9], Bocca et al. [10] and Sim et al. [11] present a WSN consisting of several nodes that were connected by a single-hop star-type network to a base station (microcontroller notebook).

Kurata et al. [12] presented a WSN on the New Carquinez Suspension Bridge in California based on the Narada wireless sensing units which feature a 2.4 GHz IEEE 802.15.4 radio standard. The Narada node, equipped with 5-AA batteries, had a lifetime of 40-45 hrs which could be extended by 60 % by using sleep modes. The sensor nodes send their data to a Narada server base station using single-hop links. The more powerful base station consisted of a low-power computer running a Linux OS

and was equipped with a third generation (3G) modem to deliver the data to a remote database server.

Chae et al. [13] successfully monitor the Yonjong Bridge with a WSN consisting of 45 nodes and a gateway station. The gateway includes a commercially available communication module to upload data to a remote server. The monitoring test provides three months of continuous data with 90 % transmission rate. Communication was based on commercial ZigBee modules but the authors did not provide figures on energy consumption of the modules. The installation includes dynamic (accelerometer and strain gauge) and static (wind and temperature) sensors which were connected as star- or mesh type network, respectively. The data are sent per single-hop to the gateway. To cover longer distances between node and gateway, directional antennas are used.

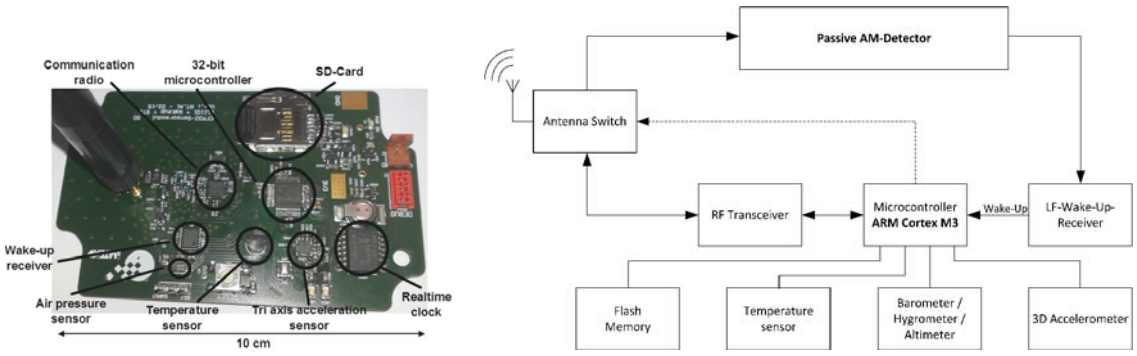
Hu et al. [14] designs a WSN to monitor the Zhengdian Highway Bridge based on nodes, which uses a MSP430 microcontroller and a CC2420 radio. The nodes are running TinyOS, which uses MintRout to send data over multi-hops to a base station. Including an energy storage of 6750 mAh, a node is able to monitor continuously for around 168 hours, or when choosing a sampling period of 1 hour/day, lifetime can be extended to 168 days. The base station is connected via a USB connector to a powerful host computer.

In contrast to the studies above, we present a SHM system based on ultra-low-power wake-up sensor nodes, which supports the use of flexible and asynchronous measurement cycles ranging from seconds to hours and days. In sleep mode they consume only around 9 µW energy and due to their flexibility, their lifetime can be enhanced without losing precious time in case of important events, compared to fixed duty cycling measurements. The base station, equipped with a GSM modem, submits data to a remote server. A wake-up multi-hop network protocol is presented, which supports the use of the introduced sensor nodes.

3 SENSOR NODES AND BASE STATION

The wireless nodes used in this work are based on the sensor node introduced in [15]. Featuring a wake-up transceiver, the nodes combine the advantages of fast communication, a small antenna and low current consumption. The microcontroller utilized on the boards is a powerful 32 bit EFM32 Gecko from SiliconLabs that has many in-build features like SPI, I^2C and a 12 Bit ADC just to name some of them. It provides up to 128 kB RAM and several low power states to reduce energy consumption. As long-range communication radio we use the CC1101 with a current consumption of 30 mA when transmitting at 10 dBm output power at 868 MHz. Its sensitivity lays around -104 dBm. The 125 kHz wake-up receiver (AS3932) from ams has a current consumption of around 3 µA in listening mode and, in combination with the passive modulation path, the board has a wake-up sensitivity around -50 dBm [15]. The sensor nodes are additionally equipped with a high precision realtime clock (PCF2129T) that has an accuracy of +-3ppm. To store data from sensors and from the network each board has a MicroSD card that provides several GB of storage. To minimize power consumption, a circuit was developed that can be used to switch the SD-Card completely OFF by the microcontroller. Fig. 1 (a) shows the sensor node including a temperature sensor (DS18B20), a three axis acceleration sensor (LIS3DSH) and a precision altimeter/pressure sensor (MPL3115A2). In wake-up listening mode the board has a current consumption of around 9 µW. Fig. 1 (b) shows the schematic of the sensor board with its different blocks. The antenna is connected by a switch either to the main radio or to the wake-up receiver. The wake-up signal is obtained from the 868 MHz signal via the passive AM-Detector that consists of the matching network, a rectifier and a low pass filter. In case the wake-up receiver detects

a valid input signal it triggers an interrupt in the microcontroller that toggles the antenna switch to the main radio. In this state, the sensor node is ready to receive and transmit communication messages.



(a) (b)

Fig. 1: The sensor node (a) and its schematics with the different block (b)

The relay nodes are similar to the sensor nodes except they lack the sensors on board. The base station is also similar to a sensor node but it is additionally equipped with a Global System for Mobile Communications (GSM) modem to transfer data to a remote server. To save energy, the GSM modem can be switched OFF when no communication to the internet is taking place.

4 WAKE-UP MULTI-HOP ROUTING PROTOCOL

Since to our knowledge no communications protocols for WSNs have been published, which support the use of wake-up transceivers, a new communication protocol needs to be developed. It should support both: wake-up receivers and long-range communication radios. Since the range of the wake-up receivers is small compared to that of the main radio, data and wake-up transmission is realized by a multi-hop routing protocol that supports sending of wake-up messages and data. The protocol stack consists of several layers. The lowest layer is responsible for the waking up of neighbouring nodes. The second layer handles single-hop message transmissions and the top layer routs messages and forwards wake-up signals along multiple hops, if the destination is not a direct neighbour.

As mentioned above, the sensitivity of the wake-up receiver is lower than that of the communication radio and data can be sent over longer distances than wake-up messages. The routing protocol as depicted in Fig. 2 makes use of this behaviour: by building a chain of woken nodes and transferring data to the most suitable receiver, nodes in between can be skipped during data communication. In Fig. 2 node 13 sends for example a wake-up signal to node 12, which forwards the wake-up to node 11 and so on, until a defined maximum number of forwards, or the destination is reached. Data can then be sent directly from node 13 to one of the woken nodes 10, 11 or 12.

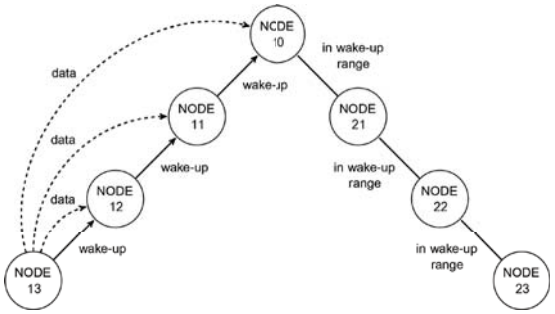


Fig. 2: Schematic of the wake-up multi-hop routing protocol developed in this work

Fig. 3 shows the sequence diagrams of the routing protocol for the different cases of (a) sending data to a direct neighbour, (b) sending data to a two-hop distant neighbour and (c) sending data to a three-hop neighbour. Decision, to which node data will be sent, is done at the node that started communication by sending a routing request (REQ). The node evaluates the request acknowledges (REQ_ACK) received from the participating nodes (nodes B, C and D). Further nodes are called by forwarding the routing request (FWD_REQ). Implemented parameters to support the decision are: available data slots at the receiving node and hop distance from the starting node. It is possible to include further parameters like link quality, receiver signal strength or remaining energy to increase the stability of the network.

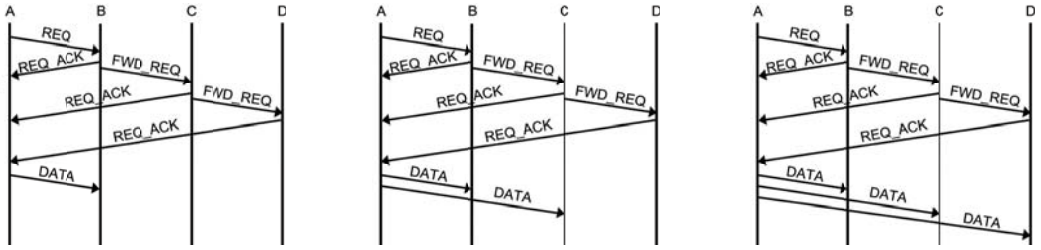


Figure 3: Sequence diagram of the routing protocol for the three different cases of communication to next neighbour (a), two hops neighbour (b) and three hops neighbour (c)

Once the communication link to a node is established, up to 64 data packets consisting of up to 256 bytes size each (max. 16 kB) can be transmitted. After transmission, the link gets closed and the participating nodes fall back to sleep, again. The same routing scheme is repeated until all data reached their destination.

The embedded software is implemented as a state machine as depicted in Fig. 4. At the beginning, a sensor node is in SLEEP state in which it consumes only minimal energy. A low-energy timer transfers the node from sleep either to start a sensor measurement (state MEAS), or to check if there is data available in the memory that is not yet sent (state STORE).

In case there are already prepared data slots available, for example from a previously aborted sending, the sleep state will be left and data transfer is initiated by sending a wake-up signal (state SEND WAKE-UP). After a measurement, sensor data is stored in a ringbuffer on the microSD card and data packets are prepared and moved into one of up to 64 available data slots. If there are no free slots available the data is kept in memory to be processed later.

After successful filling the message queue, sending of data is initiated with a wake-up signal (state SEND WAKE-UP). Successfully waking of the neighbour node, is indicated by a wake-up acknowledge and a routing request is sent (state SEND R_REQ) containing destination ID, number of data packets and max number of wake-up hops. Then, the node listens for route request acknowledgments sent by the woken nodes (state WAIT R_ACK). If at least one node that answers has a free slot available, the node starts to send all possible data packets (state SEND DATA). After successful sending, or if any error occurs, the node exits its current state and goes back to sleep. The state machine of the receiver is similar to that of the transmitter.

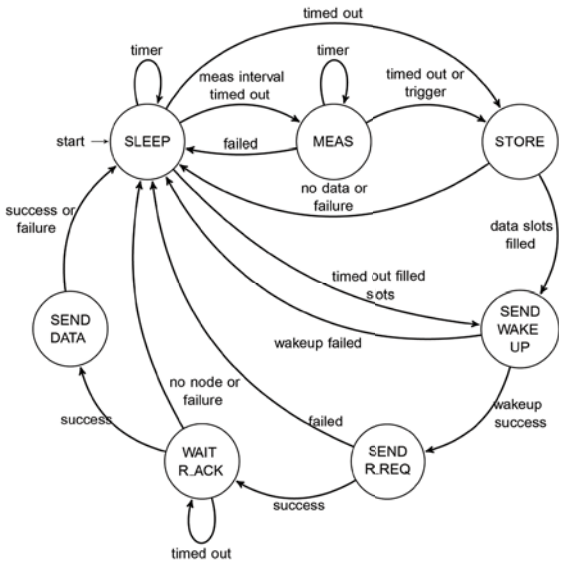
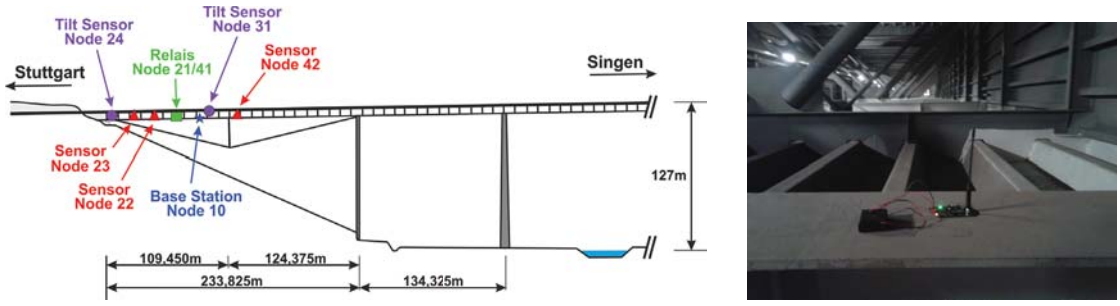


Fig. 4: State machine of a sensor node for data transmission

5 DEPLOYMENT AT THE WEITINGER NECKARTAL BRIDGE

Fig. 5 (a) shows the deployment of the prototype WSN at the Weitinger Neckartal Bridge installed in June 2015. The purpose of this prototype wake-up multi-hop WSN was to examine the communication inside the box girder of the bridge and to prepare a long-term measurement with additional sensor nodes. To realize these goals, the preliminary network consisted of a base station (node-10), a relay node (node-21/41), three sensor nodes (node-42, node-22 and node-23) and two sensor nodes equipped with a very accurate tilt sensor developed by project partner Northrop Grumman LITEF GmbH. The sensor nodes were equipped with temperature, pressure and acceleration sensors as introduced in Section 3. All nodes were placed inside the box girder of the bridge in the middle of various steel girders as can be seen for example in Fig. 5 (b) which shows node-42 deployed near the middle of girder 022.



(a) (b)

Fig. 5: Nodes deployment inside box girder (a) and a picture of deployed node-42 (b)

To cover the distances between the deployed sensor nodes and the base station, relay nodes were used to receive and forward wake-up messages according to the routing protocol introduced in Section 4. Fig. 6 (a) shows the topology of the wake-up network, where each node is able to wake its direct neighbour. Node-24 for example, is in a four hop wake-up distance to the base station, whereas node-42 is in a two hop wake-up distance to the base station. Fig. 6 (b) shows the topology of the network in case all nodes are active. Due to the longer communication range (compared to the wake-up range), additional paths between nodes can be established and the communication hop distance from nodes-24 and -42 to the base station shrink to one hop, in this example.

Fig. 6: Wake-up network topology (a) and communication network topology (b)

6 RESULTS

The prototype setup was installed in June 2015 at the Weitinger Neckartal Bridge, as introduced in Section 5. Node-31 was sending via a single hop link to the base station, and the others nodes used a multi-hop connection as introduced in Section 5. The base station successfully transmitted the sensor data to the server in Freiburg. Since there were many steel girders in the surroundings of the sensor nodes, we experienced communication problems when at high data rate of 500 kBit per second. After reducing the data rate to 38.4 kBit per second, a stable connection could be established. The test setup was running for several hours on this day, as can be seen in Fig. 7. Fig. 7 (a) shows the temperature readings of nodes-22 and -42 for around 12 hours and Fig. 7 (b) shows the air pressure measured at node-42 during the same period.

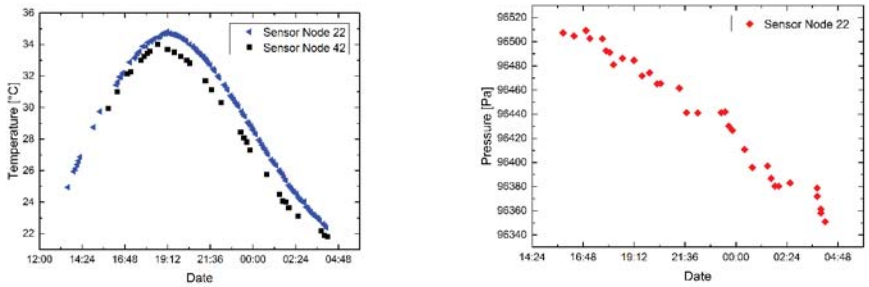


Fig. 7: Temperature at nodes-22 and -42 (left) and pressure at node-22 (right)

7 OUTLOOK AND CONCLUSIONS

In this paper, we introduce low power wireless sensor nodes with integrated wake-up transceiver. Due to their powerful microprocessor the nodes are very flexible and can be equipped with all kinds of sensors for structural health monitoring. In combination with wake-up receivers, the nodes have very low power consumption and support different features, such as asynchronous measurements, distribution of important detections with low latency, or pulling of data from the network at any time. Further on, we introduce a static routing protocol that supports wake-up receivers and combines them with the advantages of long-range communication radios. A prototype sensor network consisting of several sensor nodes, a base station and a remote server has been installed and tested at the Weitinger Neckartal Bridge in south-west Germany. The prototype WSN utilizes the wake-up multi-hop routing protocol as introduced in this work, and was successfully running for several hours, transmitting sensor data to the remote server at the University of Freiburg. In the next steps, we will realize a long-term monitoring network and develop a dynamic routing protocol to enable easy integration of additional nodes into an existing network.

8 ACKNOWLEDGEMENTS

We gratefully acknowledge financial support from the BMBF (13N11746) and BaSt (FE 88.0126/2012).

REFERENCES

[1] Ko, J. M., & Ni, Y. Q. (2005). Technology developments in structural health monitoring of large-scale bridges. Engineering structures, 27(12), 1715-1725.

[2] Chang, P. C., Flatau, A., & Liu, S. C. (2003). Review paper: health monitoring of civil infrastructure. Structural health monitoring, 2(3), 257-267.

[3] Lynch, J. P., & Loh, K. J. (2006). A summary review of wireless sensors and sensor networks for structural health monitoring. Shock and Vibration Digest, 38(2), 91-130.

[4] Al Ameen, M., Islam, S. M., & Kwak, K. (2010). Energy saving mechanisms for MAC protocols in wireless sensor networks. International Journal of Distributed Sensor Networks, 2010.

[5] Wardhana, K., & Hadipriono, F. C. (2003). Analysis of recent bridge failures in the United States. Journal of Performance of Constructed Facilities, 17(3), 144-150.

[6] Bannoura, A., Ortolf, C., Reindl, L., & Schindelhauer, C. (2015). The wake up dominating set problem. Theoretical Computer Science.

[7] Lynch, J. P., Wang, Y., Loh, K. J., Yi, J. H., & Yun, C. B. (2006). Performance monitoring of the Geumdang Bridge using a dense network of high-resolution wireless sensors. Smart Materials and Structures, 15(6), 1561.

[8] Kim, S., Pakzad, S., Culler, D., Demmel, J., Fenves, G., Glaser, S., & Turon, M. (2007, April). Health monitoring of civil infrastructures using wireless sensor networks. In Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on (pp. 254-263). IEEE.

[9] Whelan, M. J., Gangone, M. V., & Janoyan, K. D. (2009). Highway bridge assessment using an adaptive real-time wireless sensor network. Sensors Journal, IEEE, 9(11), 1405-1413.

[10] Bocca, M., Eriksson, L. M., Mahmood, A., Jäntti, R., & Kullaa, J. (2011). A synchronized wireless sensor network for experimental modal analysis in structural health monitoring. Computer-Aided Civil and Infrastructure Engineering, 26(7), 483-499.

[11] Sim, S. H., Li, J., Jo, H., Park, J. W., Cho, S., Spencer Jr, B. F., & Jung, H. J. (2014). A wireless smart sensor network for automated monitoring of cable tension. Smart Materials and Structures, 23(2), 025006.

[12] Kurata, M., Kim, J., Zhang, Y., Lynch, J. P., Van der Linden, G. W., Jacob, V., ... & Sheng, L. H. (2011, March). Long-term assessment of an autonomous wireless structural health monitoring system at the new Carquinez Suspension Bridge. In SPIE Smart Structures and Materials+ Nondestructive Evaluation and Health Monitoring (pp. 798312-798312). International Society for Optics and Photonics.

[13] Chae, M. J., Yoo, H. S., Kim, J. Y., & Cho, M. Y. (2012). Development of a wireless sensor network system for suspension bridge health monitoring. Automation in Construction, 21, 237-252.

[14] Hu, X., Wang, B., & Ji, H. (2013). A wireless sensor network-based structural health monitoring system for highway bridges. Computer-Aided Civil and Infrastructure Engineering, 28(3), 193-209.

[15] Gamm, G. U., Kostic, M., Sippel, M., & Reindl, L. M. (2012). Low–power sensor node with addressable wake–up on–demand capability. International Journal of Sensor Networks, 11(1), 48-56.

REALTIME DETECTION AND MITIGATION OF CBRN RELATED CONTAMINATION EVENTS OF DRINKING WATER

Thomas Bernard[1], Jürgen Moßgraber[1], Anna Elinge Madar[2], Aharon Rosenberg[3], Jochen Deuerlein[4], Helena Lucas[5], Karim Boudergui[6], Dag Ilver[7], Eyal Brill[8] and Nirit Ulitzur[9]

[1] *{thomas.bernard, juergen.mossgraber}@iosb.fraunhofer.de*
Fraunhofer IOSB, Fraunhoferstr. 1, 76131 Karlsruhe (Germany)
[2] *ellinge@arttic.eu*
ARTTIC, Rue du Dessous des Berges 58A, 75013 Paris (France)
[2] *Aharon.Rosenberg@hagihon.co.il*
Hagihon Ltd., HEBRON ROAD 101, 91100 Jerusalem (Israel)
[4] *deuerlein@3sconsult.de*
3S Consult GmbH, Albtalstrasse 13, 76137 Karlsruhe (Germany)
[5] *h.lucas@aguasdoalgarve.pt*
Aguas do Algarve SA, Faro (Portugal)
[6] *karim.boudergui@cea.fr*
CEA-LIST, Gif-sur-Yvette 91191 (France)
[7] *Dag.Ilver@acreo.se*
ACREO AB, Arvid Hedvalls Backe 4, Gothenburg SE-400 14 (Sweden)
[8] *admin@decisionmakers.biz*
Decision Makers Ltd., 19/8 Ayalon Street, 60850 SHOAM (Israel)
[9] *nirit@biomonitech.com*
BioMonitech Ltd., Golomb Street 3, 530612 Qiryat Tivon (Israel)

Abstract

The security of drinking water is increasingly recognized as a major challenge for municipalities and water utilities. The safety and or security of drinking water can be threatened by natural disasters, accidents or malevolent attacks. In the event of a contamination water spreads rapidly and hence extensively before the problem is detected. Contaminated drinking water can induce major epidemics, disrupt economic life and create mass panic. A first generation of software packages and sensors has been developed for managing drinking water safety and security and in particular for detecting incidents, such as the Guardian Blue from Hach Lange, Canary from EPA. They allow for an overall management of water security including the systematic collection and interpretation of information by online sensors. However this first generation of tools suffers from a range of serious shortcomings: (1) Real-time detection and alarm capabilities are non-existing or insufficient; (2) current limitations of propagation models make the effective situational assessment of potentially contaminated zones very difficult; (3) so far no generic approach for the online-calibration of the hydraulic and transport model exists; (4) Models for response, mitigation and recovery that are almost inexistent for real world systems at present; (5) the set of available CBRN sensors, which can be used to detect contamination threats to water drinking quality, is very limited. The European FP7 project SAFEWATER (10/2013 - 12/2016) aims at developing a comprehensive event detection and event management solution for drinking water security management and mitigation against major deliberate, accidental or natural CBRN related contaminations.

Keywords: Decision Support System, Drinking Water Networks, CBRN Sensors, Real-time Detection, Event Management, Online Simulation

1 MOTIVATION AND OBJECTIVES

The security of drinking water is increasingly recognized as a major challenge for municipalities and water utilities. The safety and or security of drinking water can be threatened by natural disasters, accidents or malevolent attacks. In the event of a contamination water spreads rapidly and hence extensively before the problem is detected. Contaminated drinking water can induce major epidemics, disrupt economic life and create mass panic. A first generation of software packages and sensors has been developed for managing drinking water safety and security and in particular for detecting incidents, such as the Guardian Blue from Hach Lange, Canary from EPA. They allow for an overall management of water security including the systematic collection and interpretation of information by online sensors. However this first generation of tools suffers from a range of serious shortcomings:

(1) Real-time detection and alarm capabilities are non-existing or insufficient;

(2) current limitations of propagation models make the effective situational assessment of potentially contaminated zones very difficult;

(3) so far no generic approach for the online-calibration of the hydraulic and transport model exists;

(4) Models for response, mitigation and recovery that are almost inexistent for real world systems at present;

(5) the set of available CBRN sensors, which can be used to detect contamination threats to water drinking quality, is very limited.

The European FP7 project SAFEWATER (10/2013 - 12/2016) aims at developing a comprehensive event detection and event management solution for drinking water security management and mitigation against major deliberate, accidental or natural CBRN related contaminations and in particular:

• to improve the detection capacities available for event detection by developing new cost-effective C, B, and RN sensors to be used in conjunction with existing sensors, benchmarking their capacities, and analysing their optimal placement location in the utilities network; in particular SAFEWATER will develop and validate an innovative concept with a broad network of low-cost sensors – “domestic sensors” (complementary to a set of sensors in strategic locations)

• to develop a technology platform able to: capture and analyze the data collected by the sensors and from other information systems, signal the level of alert, and give a full overview of the crisis to the responders by means of online look-ahead simulations to efficiently manage potential crises

The proposed comprehensive SAFEWATER solution, comprising enhanced near-real-time sensors, an advanced Decision Support System, on-line hydraulic propagation models and an all-encompassing Event Management System will be tested against several true-to-life usage cases (e.g. contamination of a municipal storage tank, contamination of a major water trunk line, contamination of a local supply line) using several families on contaminants such as organic compounds, toxic waste, and radioactive material. Trials and measurements of individual components of the system as well as the complete entire system are performed in special hydraulic test networks set up in three different water Utilities.

Applying the SAFEWATER system or even components thereof will enhance a Water Utility's ability to rapidly detect a contamination event, analyze its repercussions using real-time hydraulic models, mitigate the damage using simulation tools and swift operating procedures, and deal more effectively with the event using a comprehensive event management tool.

2 OVERVIEW ABOUT THE SAFEWATER SYSTEM

Fig. 1 provides an overview about the structure of the Structure SAFEWATER system. Key module is the *Event Management System* (EMS) which handles incoming events and provides decision support in case of a crisis (but also for routine operations). The *Event Detection System* (EDS) detects so far unknown constellations of water quality parameters. These events may be a hint on a contamination in the drinking water network, or due to a so far unknown operational effect. In case of an event it is important to provide decision support about the best mitigation measures (e.g. opening/closing of valves). In the SAFEWATER system the hydraulic and quality state of the network is simulated in real-time. In case of an event online response tools can predict the spread of the contamination and calculate optimal measures to minimize the impact of the contamination. The simulators can also be used in an offline context in order to train the operational staff. Furthermore, the simulators are used in order to train the event detection system. Within the SAFEWATER project also enhanced CBRN sensors are developed which provide the ability for an early detection of CBRN contaminations.

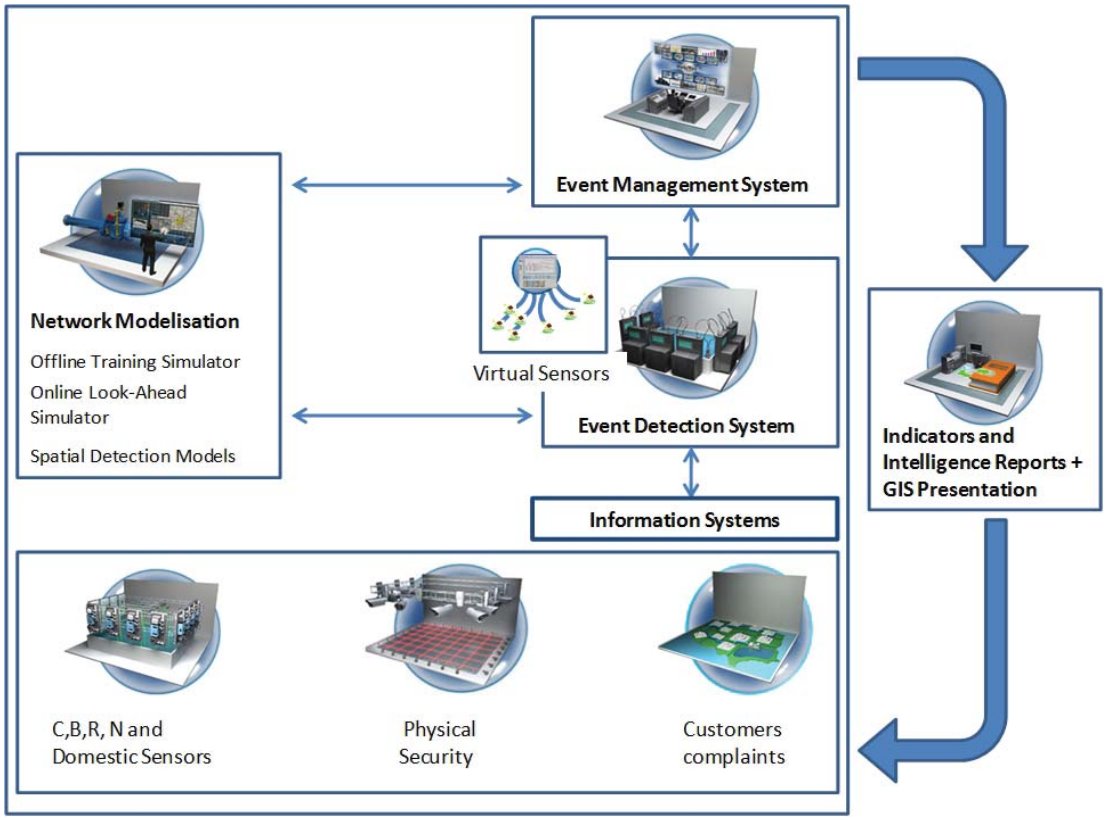


Fig. 1: Structure of the SAFEWATER system

3 EVENT MANAGEMENT SYSTEM

The Event Management System (EMS) provides a web-based user interface to manage contamination events. The EMS provides notifications about automatically detected events, allows manual introduction of new events and related information, and supports situational awareness. To provide such functionalities, the EMS relies on the Event Detection System (EDS) for the actual detection of events, and on the Simulators for estimating the evolution of the contamination spread, as well as the location of the contamination source. Additionally, a Workflow Engine enables the orchestration of the interactions among components according to pre-defined

processes specified using *Business Process Model and Notation* (BPMN[1]). Communication among the system components is achieved by means of a *Message oriented Middleware* (MoM), which permits loose coupling and provides flexibility regarding the distribution of the executing components (see).

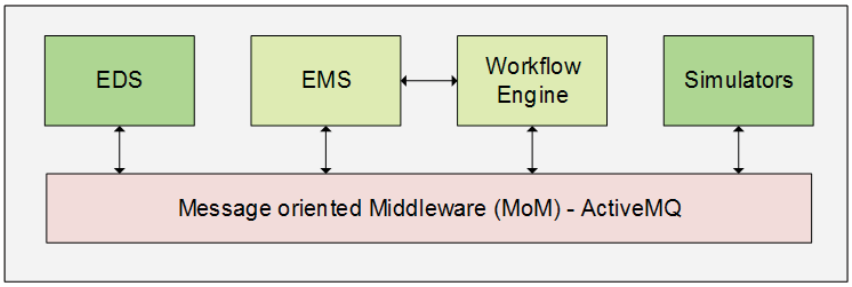


Fig. 2: The main components of the system decoupled via a Message oriented Middleware (MoM)

A simple detection and response scenario includes the following steps:

(1) The EDS monitors the network using SCADA data and detects an event.

(2) The EDS issues a notification about the event.

(3) The event is visualized in the EMS.

(4) A response workflow is started.

(5) As part of the response flow a simulation gets executed.

(6) The results of the simulation are displayed in the EMS.

While currently not implemented, the process execution mechanism provided by the workflow engine enables the extension of the system to accommodate complex scenarios. Those scenarios may involve the utilization of communication mechanisms such as e-mail or SMS, and interaction with other systems, such as an ERP or an intrusion detection system (as a complementary event generation source).

The EMS is able to visualize detected events both in table form, with search and sorting options, and on a map. In the latter case, an indicator is placed using the coordinates provided by the EDS (see Fig. 3). To support the event management process, information about the events can be extended through online forms.

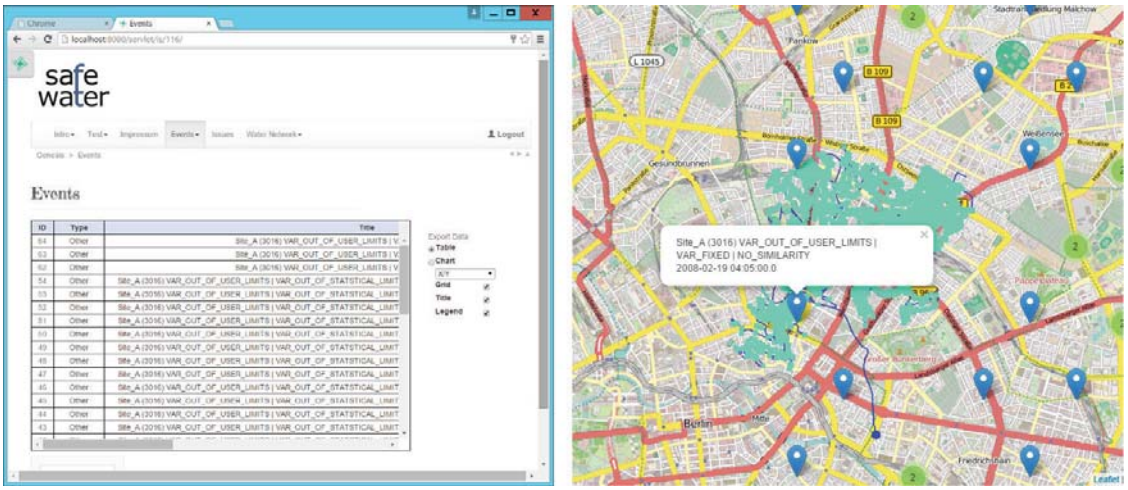


Fig. 3 Events can be visualized in table form and on a map.

[1] http://www.omg.org/spec/BPMN/2.0/

As indicated in the example steps listed above, upon detection of an event a workflow is started that will trigger the execution of the Simulators. When a contamination event occurs, a simulation to predict the contamination spread in the network during the following hours is executed. The results of the simulation are graphically displayed on a representation of the network with its parts colored according to the values generated during the simulation.

Besides the look-ahead simulation, other kinds of simulation are also available, which are also accessible through the EMS interface. The data provided by the SCADA system and the sensors can be used to feed an analysis algorithm that will try to estimate the location of the contamination source. Additionally, it is possible to explore what-if scenarios using different configuration options of the Simulators. The details regarding the EDS and the Simulators can be respectively found in sections 3 and 4.

4 EVENT DETECTION SYSTEM

The *Event Detection System* (EDS) is a software platform based on machine learning technology which enables to detect that there is an issue with the water quality. The need to detect pending problems in water system arises from the need to minimize damage cause by unexpected abnormal events. The logic behind this methodology is presented by the following table.

Common good - most	Common bad-change
Rare good	Rare bad

Horizontal axis shows two options. Common occurrences and Rare occurrences. The vertical axis displays a good occurrence versus a bad occurrence. The interaction between the two dimensions yields four basic occurrences.

- Common-Good: This is the case most of the time.
- Common-Bad: This indicates that this part of the system should be replaced.
- Rare-Good: Occurrences in this category require classification.
- Rare-Bad: This indicates that something is wrong in the system.

In many cases, detecting occurrences may be difficult since the system is asked to find something that hasn't yet happened in the past. Such a challenge addressed by utilizing an Unsupervised Machine Learning methodology (UML). The heart of UML is to learn the normal behavior of the systems and to detect when the system deviates from normal behavior.

The EDS uses several methods to generate an indication that something is wrong: (1) Violation of single variables limits, (2) Appearance of rare combination(s), (3) Similarity to Bad past situation(s), (4) Violation of Rules. Each type of indication may be based on one or several *Detectors*. A Detector is an algorithm trained to detect specific abnormality in data. An example of a Detector is an algorithm to detect that a variable is out of its statistical limits. Such a Detector "learns" the statistical limits of each variable and when actual data violates these limits (after delay time) the EDS generates alert.

It is the user's choice as to which Detectors to activate. The default option is that they are all activated. Once activated a Detector may be calibrated. When several Detectors simultaneously alert an event message is generated. An event needs to be classified by the user. Over time, the EDS learns from the classification of events and improves its alerting policy. The EDS and the EMS communicate via the MoM of the system.

5 OFFLINE AND ONLINE SIMULATORS

Since many years powerful simulation tools are available for the offline simulation of the hydraulic behavior of water distribution networks and the dynamics of water quality parameters. An example is the open source toolkit EPANET resp. EPANET-MSX for enhanced water quality simulations. These simulators can be used for the analysis of different contamination scenarios in order to get a better understanding of the water network behavior. However, the usage of these platforms for decision support of water utilities is still a challenge as the calibration of the models is not an easy task (mainly due to the lack of detailed water consumption data). Furthermore, the accuracy of water quality models is limited as in most packages the models are very simplified, e.g. assuming complete mixing of concentrations at junctions. One aim of the SAFEWATER project is the enhancement of existing simulation platforms (EPANET-MSX and SIR-3S) in order to improve the accuracy of the water quality models by a more realistic mixing model. Furthermore, the topology of the models is simplified by the technique of graph decomposition. Due to that, without any loss of accuracy, the model size is reduced considerably (typically more than 50%).

In recent years, simulations are also performed in (near) real time ("online simulation"). Such online hydraulic and water quality simulators support the online identification of contaminant sources in real time. They can also provide an estimation of the contamination severity and the impact of mitigation and recovery measures by means of look-ahead calculations. For application of network simulations as operative tool in the framework of a security management system, offline data are insufficient. Online Simulation models are important tools for network monitoring as well as mitigation and response to a contamination event. In case of a contamination the effective response to the event can save health or even lives of thousands of people. A basic requirement for that is to have a good estimate for the current and future situation, notably the spread of contamination. Therefore it is important that all water quality and transport calculations are based on a very accurate hydraulic model. This is possible only by using a well calibrated online simulation model. Besides the estimation of the future affected areas, also response actions such as source identification and determination of isolation valves for preventing the further spread of contamination are based on the results of the online simulation model.

In contrast to the offline simulators where the boundary conditions of the model define a certain scenario that represents the network behavior of the past or a situation that never has been happen in the real system the online simulation model aims at reflecting the actual operational state of the system as accurate as possible. For that purpose the hydraulic simulation engine is connected to the SCADA system of the utility. Dependent on the desired degree of integration this connection can be realized within the IT-infrastructure of the Process Control System (PCS) or outside the firewall of the PCS. In the latter case the process data are transferred in certain time intervals from the PCS to a database whereas full integration means that the simulation software runs within the PCS.

Online simulation is aimed to provide a complete overview of the actual state of a drinking water distribution system for both network hydraulics, as well as water quality, at any place and with a minimal time delay (including time for data transfer and processing as well as calculation). As measurements exist only at selected locations they can deliver only a local snapshot of the current system state. The simulation model by using the measurements as boundary conditions fills the gap between these locations and enables drawing a comprehensive picture about the current state of the entire system. The model is constantly updated and ideally fits with the real physical system by automatically updating the key model parameters (boundary conditions). It provides the basis for all higher functions such as source identification, propagation, severity, impact, as well as customized views on the system. In other words, online

simulation supports fast and appropriate response, in addition to monitoring the current state of the system.

In SAFEWATER online simulation models are implemented for designated pilot zones of the water supply systems of the three end users involved in the project. One model includes a domestic zone of an urban water supply system that serves around 50.000 people. The second model consists of a subsection of a large regional water supplier that delivers water to municipalities and their local water suppliers. The third systems incudes a combined transport and distribution system with two water works and storage facilities with dynamic network operations.

For modelling purposes the online data of the PCS are subdivided into two groups. The group of actuators includes operational states and measurements that are transferred to the simulator directly as boundary conditions of the simulation model. Examples are valve states, operational states (on/off) or speed of pumps, water level in reservoirs or set values of control devices. The second group consists of so called sensors. In the online model sensors include redundant information from measurements in the field that are used for the comparison of measurements and calculation results The difference plays an important role as indicator for the quality (matching with reality) and calibration state of the simulation model.

In order to make the online simulations capable of being integrated within different client software special tools and interfaces have to be developed. The data integration component implements a number of plugins, for instance, generic online data interface for connecting with any SCADA system and the simulator plugin that runs the simulations. In addition, multiple external calculation or visualization tools can be updated and operated using the central component.

Summarized, within the SAFEWATER project enhanced simulators of the hydraulic und water quality state of large drinking water networks will be developed. The simulation results are presented within the general and user friendly Event Management System (EMS) in order to make them available not only for experts that are experienced in using hydraulic simulation models but also for decision makers and technical staff of the utility.

6 INNOVATIVE CBRN SENSORS

The work on CBRN sensors deals with development and adaptation of sensors for water contamination. The sensors will be evaluated together with water utilities at two different stages during the SAFEWATER project. The rationality for this developmental work is to provide the event management system/event detection system with useful data of a kind that is not available using “off-the-shelf” sensors presently on the market.

The radioactive threats are covered by partner CEA using a technology based on plastic scintillators. To manage the challenge of beta radiation detection, and possibly also Alpha radiation, CEA has designed a new plastic scintillator light collection system and developed associated high velocity electronics and data processing algorithms. The first release of the system was built and is now under evaluation for detection of Beta radiation. A novel approach is used where the scintillator is implemented as scintillating optical fibers, to come close to the bulk of the water, in order to increase the area detection. The scintillating fibers will convert the radiation into light that will travel through each optical fiber to finally be detected by the PMT (Photon Multiplier Tube, see Fig. 4).

For detection of chemical contaminants in drinking water, partner Biomonitech is developing a compact bacteria-based chemical online sensor. This technology is based on measuring rapid changes in light emitted by natural marine luminescent bacteria upon exposure to low concentrations of a broad range of chemicals that affect their

metabolism. Biomonitech has developed assay buffers that make the bacteria sensitive to certain groups of chemicals to monitor either metallic (cationic heavy metals and metalloids) or other (mainly) organic chemicals.

For detection of *E. coli* bacteria in drinking water, partner Acreo has adapted an earlier concept for an antibody-based sensor. This sensor system use antibody-mediated fluorescent labelling of *Escherichia coli,* followed by counting of bacteria using a small in-house developed flow cytometer in combination with fast data analysis (Fig. 5). The whole system for fluorescent tagging of *E. coli* and detection in the flow cytometer has been integrated in a unit that is directed from a laptop PC and will be able to detect bacterial contamination reasonably fast. This will give new possibilities for quick response when integrated in the event management system/event detection system.

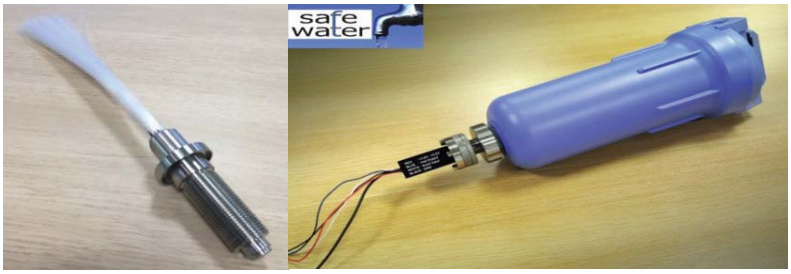


Fig. 4: left panel, scintillating optical fibre bundle. Right panel, scintillator bundle mounted with PMT in flow cell for water analyses.

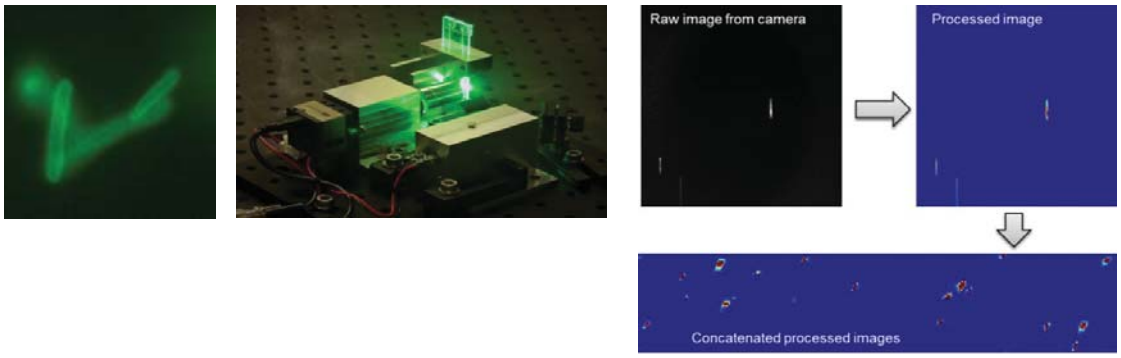


Fig. 5: Left panel; antibody mediated fluorescent labelling of E. coli. Middle panel, the video based flow cytometer. Right panel; Main steps in the video processing algorithm. Raw images from camera are filtered and the processed images are concatenated into a linogram where the particles (= bacteria) are counted.

7 SUMMARY AND OUTLOOK

The proposed comprehensive SAFEWATER solution, comprising enhanced near-real-time sensors, an advanced Decision Support System, on-line hydraulic propagation models and an all-encompassing Event Management System will be tested against several true-to-life usage cases (e.g. contamination of a municipal storage tank, contamination of a major water trunk line, contamination of a local supply line) using several families on contaminants such as organic compounds, toxic waste, and radioactive material. Trials and measurements of individual components of the system as well as the complete entire system are performed in special hydraulic test networks set up in three different water Utilities. First results are expected by the end of 2015.

Acknowledgements

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 312764.

SAWSOC: SITUATION AWARE SECURITY OPERATIONS CENTER

Giuseppe La Posta[1] and Claudio Porretti [2]

[1] *giuseppe.laposta@selex-es.com*
SELEX ES, LoB Cyber Security & ICT Solutions, Via Laurentina 760, 00143 Rome (Italy)

[2] *claudio.porretti@selex-es.com*
SELEX ES, LoB Cyber Security & ICT Solutions, Via Laurentina 760, 00143 Rome (Italy)

Abstract

Security monitoring is a number one priority, since it is the pre-requisite for allowing system operation to continue also in the presence of attacks. A security monitoring facility produces three categories of outputs: 1) Alarms – Notifications of attacks that must be handled; 2) Remediation/Reaction triggers – Events that are sent to the personnel/machinery in charge of performing actions/procedures aiming at countering and/or mitigating the effects of attacks; 3) Actionable Evidence – Unforgeable electronic evidence of attacks. A plethora of technologies exists but they very much lack integration. While recently some achievements have been made a further advancements in the convergence of physical and logical security technologies are very much needed. SAWSOC proposes a novel approach and a conceptual architecture for real-time security monitoring of complex networked systems. The approach is to collect information at several architectural levels and to implement, and validate techniques for achieving effective correlation of the diverse information flows.

Keywords: Logical security, physical security, correlation, real time, situation awareness, critical infrastructure, innovation, research projects.

1 INTRODUCTION

Security has become one of the major topics in contemporary societies. While facing new security risks and challenges like e.g. international terrorism, crime, climate change and economic crises, an increased concern for security can generally be observed among many European populations. Increasingly, attempts are made to 'produce' security in a primarily technological way. Technologies for implementing security services in the physical and in the electronic domain are both stable and mature, but they have been developed independently of each other. Security Operations Center (SOC) technology has improved significantly, but SOC solutions have typically been developed using vertical approaches, i.e. based on custom specific needs. Other key security technologies (such as: Video Surveillance, Forensic support and Building Automation) have also made dramatic improvements, but there is still a limited capability of performing complex correlation on security relevant data. The fragmentation of security approaches is perceived by citizens with confusion, disorientation, and fear. This discomfort is also amplified by the still too high rate of false alarms.

Convergence of security technologies could be very useful to increase control and monitoring functions in infrastructures like electric power grid, where attackers could manipulate either the power applications or physical system [2] [3]. In many other environments, convergence of security technologies could be useful for incrementing the infrastructure security and the awareness of security by users [4]. Such convergence, over the past few years, has been possible thanks to the reusing and merging of various technologies to create new and improved products and services, but mainly thanks to the development of internet and thanks to the global acceptance of IP protocol [1].

SAWSOC aims at bringing a significant advancement in the convergence of physical and logical security, meaning effective cooperation (i.e. a coordinated and results-oriented effort

to work together) among previously disjointed functions. SAWSOC enhanced awareness capabilities will allow accurate, timely and trustworthy detection and diagnosis of attacks, which ultimately will result in the achievement of two goals of paramount importance and precisely:

1. guaranteeing the protection of citizens and assets;
2. reducing the perception of fragmentation of security approaches, thus improving citizen's perception of security.

2 PROJECT OBJECTIVES

SAWSOC objective is to identify, implement, and validate techniques for achieving the convergence of physical and cyber security solutions (see Fig. 1).

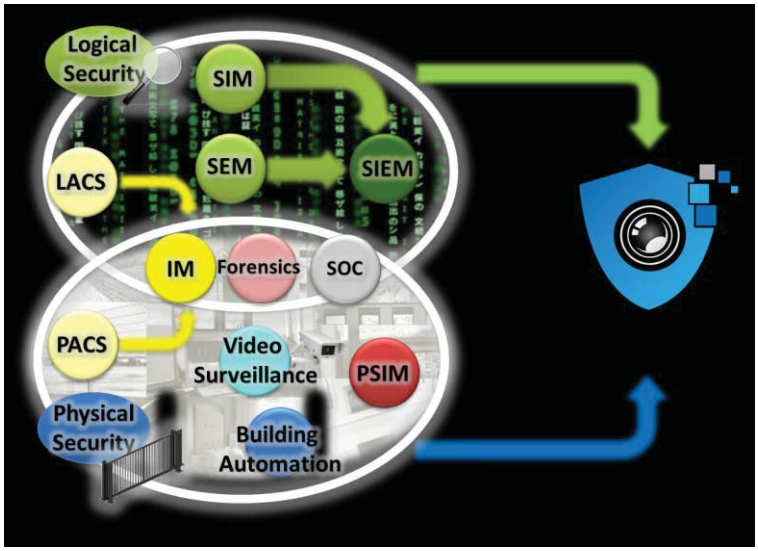


Figure 1: convergence of physical and cyber security solutions

More in detail, the project aims at:

- Advancing the state of the art of some of the key physical and logical security technologies;
- Developing techniques for correlating physical and logical security services, to achieve a consistent view and to be able to produce an irrefutable record of who did what, where, and when;
- Implementing those techniques in a Situation AWare Security Operations Center (SAWSOC) i.e. an integrated platform for providing sophisticated security services combining in a modular way diverse information from multiple data sources;
- Demonstrating and validating the proposed techniques and the framework by performing a thorough experimental campaign with respect to three substantial case studies.

3 CURRENT ACHIEVEMENTS

The main phases of the project are: use case analysis, technology review and gap analysis, components implementation, platform implementation, demo & validation.

During the first year of the project, the three use cases provided by the end users have been analysed, different key technologies have been identified for: (1) identity and credential management; (2) digital forensics for advanced interpretation of data; (3) video surveillance approaches for delivering information about visually observable events; (4) correlation of

physical and cyber threats patterns exploiting data from heterogeneous devices and information systems. Legal aspects and privacy concerns have been properly analysed for each of the mentioned technologies. Societal aspects and implications have also been addressed as part of project activities.

3.1 Use case analysis

SAWSOC design has been driven by three real use cases that were carefully selected with two objectives: capturing the diversity of the requirements and improving the perception of security by citizens. Such use cases collectively form an experimental test-bed perfectly suited for driving the design as well as for validating the development of a platform such as SAWSOC.

The first use case, namely MIARCI (Maintenance Impacts and Attack Recognition on Critical Infrastructures), is provided by ENAV, the Italian air traffic control provider. Such use case involves the management of a Critical Infrastructure (CI) for air traffic control. The objective is to use the SAWSOC platform for improving data integration and correlation capabilities of the system which is currently being used by the company for monitoring the security - both physical and logical - of the infrastructure. The most challenging requirement of this use case is the ability to clearly distinguish between a maintenance operation and a malicious attack

The second use case is called EPDCI (Energy Production and Distribution Critical Infrastructure). It is provided by IEC, the largest electric utility in Israel. The objective here is to use the SAWSOC platform for timely detection of attacks aiming at disrupting energy production and/or distribution and/or at damaging the infrastructure.

SAWSOC will correlate logical and physical information to support the decision making process on which dependable operation of the energy CI relies, particularly in the presence of sophisticated attacks.

The third use case is called CES&S (Crowded Events Safety & Security) and it is provided by Comarch, the Polish SME in charge of security management at the Cracovia stadium. The use case deals with the protection of people attending an event at the stadium. SAWSOC will provide important security features, such as early identification of abnormal behaviour and improved detection of unauthorized access. This use case directly involves people thus providing concrete evidence of the improved security level to the general public.

3.2 Gap analysis

A thorough technology review update has been carried out, with respect to the key technologies the SAWSOC platform relies on, namely: Security Information and Event Management (SIEM), Digital forensics, Video Surveillance, Security Operation Center (SOC), Physical Security Information Management (PSIM), Building Automation, and Identity Management. The study highlighted that currently available products are still far from achieving real convergence between physical and logical security. A gap analysis of physical and logical security technologies has been conducted in order to identify missing features concerning current security technologies. When performing the gap analysis, particular attention has been paid to technologies, such as video surveillance systems, SIEM (Security Information and Event Management) systems, and Identity Management systems, that will play a crucial role in the SAWSOC use cases. A synthetic summary of the main results is presented hereafter.

Video Surveillance Systems - some of the physical security features needed for SAWSOC are sufficiently provided by current commercial products. For other functionalities there are products and methods available, but unfortunately the detected events cannot be provided automatically and immediately on detection time for other processes in order to be correlated with other events. Finally, for some functionalities solutions are available but the reliability level of the detected events is low. At the end of such analysis, the project idea is to build

SAWSOC components on top of basic functionalities provided by current systems, and to derive more complex events from them by using brand-new features developed within SAWSOC, in order to provide a richer input to be correlated with logical security information.

SIEM Systems - gap analysis of SIEM systems has led to the conclusion that generally SIEM applications are too complex, they take a long time to deploy and they are too expensive with high installation costs; furthermore SIEM systems create a lot of data noise and are not cloud friendly. Complexity of SIEM systems could be dealt with data analytics and CEP (Complex Event Processing) [5] to reduce the overhead on Security Operation Centre analysts that deal with a huge amount of data and alerts.

Identity Management Systems - Technology gap analysis indicated that, from the Identity and Credential Management Systems (IDCMS) perspective, there are two high-level requirements that are common to the MARCI, EPCDI and CES&S use case scenarios. These are: to trust each device that has access to Critical Infrastructures (CIs) and to trust each person that has access to the trusted devices.

3.3 SAWSOC platform

The architecture of the SAWSOC platform has been designed through a collaborative process during which both general and use case specific requirements have been taken into account. A high level view of the SAWSOC architecture is presented in Fig. 2.

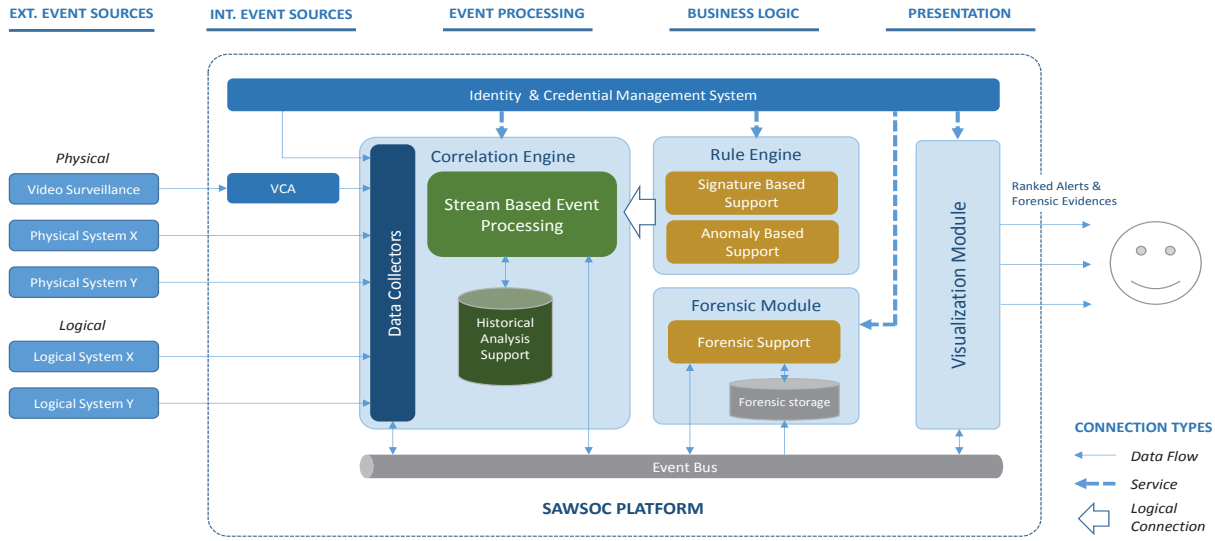


Figure 2: SAWSOC platform

The VCA component receives the inputs from video surveillance and fuses the lower level results from video surveillance physical sensors (e.g. cameras) into higher level concepts and events. For example, raw computer vision results, such as person detections, are collected and fused to person tracks, applying computer vision algorithms; or some change detection with the presence and absence of people is fused to perform some manipulation detection at an infrastructure device. Data streams provided by computer vision, according to the SAWSOC platform requirements that meets the Use Cases needs, are Person Detection, Person Tracking, Action Recognition, Context Analysis and Scene Analysis.

The Identity & Credential Management System (IDCMS) provides credentials for user authentication, device authentication and event signing in the SAWSOC platform. Specifically it provides the credentials for event signing at the Correlation Engine; credentials for user authentication (users/devices) on the Correlation Engine; credentials for user authentication on the Visualization Module. Additionally, auditing information (credentials used by the systems that created logs) can be retrieved from the IDCMS to the Forensic Module

The Correlation Engine is the component in charge of the event diagnosis process. It operates by correlating a huge amount of security relevant events/information from the physical and the electronic domain in real-time, through Complex Event Processing (CEP) techniques and stream processing computing technologies. The attack diagnosis process is driven by correlation rules that aggregate the parameters of attack symptoms, such as the attack type, the target component and the temporal proximity. Alerts are generated only when the correlation among such symptoms indicates a potential attack, thus exhibiting low false positive rates and improved detection capability.

The Rule Engine component provides the logical rules to be followed by the Correlation Engine. The Rule Engine includes two main components, Signature Based Support and Anomaly Based Support. They are complementary and in the approach taken for SAWSOC platform, they cooperate to detect all possible breaches to the systems being protected. The Anomaly Based module supports the Signature Based one, giving instruments to operators so that they can be able to detect and define new rules for the Signature Based module. The Anomaly Based module works in two steps: 1) Get events to create a behaviour model, 2) Process incoming events passing them to the behaviour model created before and deciding on whether such events are those expected or not.

The Forensic module provides a set of services that enable the end user (Security Operation Center operator) to trace from an event to the log data from which it was identified. The module will ensure that the events and their associated logs are stored in a forensically sound manner. It will support processes that ensure, to the greatest extent possible, that the event data will be acceptable as evidence.

The Visualization Module implements the User Interfaces of the SAWSOC platform, provides the Risk Monitor List visualization feature prototype and implements the Action Engine Interface in order to enable initiating actions in connected systems.

A first version of the main components, implementing the basic functionalities, is already available. A demo of those components was given at the first project workshop, which was held in Genova on the 10th December 2014 in conjunction with the Security Research Conference.

3.4 Citizens' perception of security

According to the Eurobarometer’s [6], security technology seems to have a rather bad reputation compared to other technologies. Contradictory findings from other studies signify ambiguous attitudes of citizens towards security technology and thus indicate the need for socio-scientific research on the various determinants for the acceptance of different security technologies.

The recognition of technology as rather one part of a comprehensive strategy to provide and ensure civil security instead of being a “cure-all” [7] is an achievement of humanities’ and socio-scientific research. Their diagnosis of coexisting objective risk assessments and subjective risk perceptions principally leads to the question, in what way technical measures for increased objective security impact on the actual perception of (in-)security. Appropriateness of technological interventions and a comprehensible balance between security and freedom play an important role [8].

An analysis of the relationship between security technologies and citizens feelings of (in)security has been carried out. The analysis started from a state of the art literature review on citizen’s feelings of (in)security, their acceptance of security measures and how both of the two are commonly measured in empirical research.

On this basis, an evaluation design for assessing citizens’ perceptions of convergent security technologies has been proposed.

4 CONCLUSIONS

The SAWSOC FP7 project started in November 2013 to implement and validate techniques for achieving the convergence of physical and logical security technologies.

After 15 months, at the end of the first period, the project is running according to the planned timeline. The use cases have been analysed, the requirements have been identified, the architecture has been designed, and a first version of the main components is already available.

The final result will be a prototype able to demonstrate the improvement that can be achieved in the field of real-time security monitoring of complex networked systems through effective convergence of physical and logical security technologies.

REFERENCES

[1] B.T. Contos, W.P. Crowell, C. DeRodef, D. Dunkel, E. Cole, “Physical and Logical Security Convergence”, published by Syngress Publishing.

[2] L. Coppolino, S. D’Antonio, L. Romano, “Exposing vulnerabilities in electric power grids: An experimental approach”, international journal of critical infrastructure protection 7 (2014) 51–60.

[3] Aditya Ashok, Adam Hahn, Manimaran Govindarasu, “Cyber-physical security of Wide-Area Monitoring, Protection and Control in a smart grid environment”, Journal of Advanced Research (2014) 5, 481–489.

[4] S. Baker, S. Waterman, and G. Ivanov, “In the crossfire: Critical infrastructure in the age of cyber war”, McAfee, 2009.

[5] Intelligent M2M: Complex event processing for machine-to-machine communication, Ralf Bruns, Jürgen Dunkel, Henrik Masbruch, Sebastian Stipkovic

[6] European Commission (2005): Social Values, Science and Technology. Special Eurobarometer 225. Online: http://ec.europa.eu/public_opinion/archives/ebs/ebs_225_report_en.pdf.

[7] Ammicht Quinn, Regina; Vagenborg, Michael; Rampp, Benjamin; Wolkenstein, Andreas F.X. (2014): Ethik und Sicherheitstechnik. Eine Handreichung. In: Ammicht Quinn, Regina [Hg.]: Sicherheitsethik. Wiesbaden: Springer VS: 277-296

[8] Albrecht, Hans-Jörg (2011): Neue Bedrohungen? Wandel von Sicherheit und Sicherheitserwartungen. In: Peter Zoche, Stefan Kaufmann und Rita Haverkamp (Hg.): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld: transcript: 111–127.

RISK-BASED RESILIENCE QUANTIFICATION AND IMPROVEMENT FOR URBAN AREAS

Kai Fischer[1], Ivo Häring, Werner Riedel

[1] *kai.fischer@emi.fraunhofer.de*
Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut
Am Klingelberg 1, 79588 Efringen-Kirchen, Germany

Abstract

The growing urbanisation, continuity or even increase of old and formation of new threats and the increasing complexity of critical infrastructures underlines the need for more robust and sustainable cities. To achieve this aim, the quantitative assessment of the resilience of cities is used to identify weak spots in urban environments allowing for systematic and cost-conscious resilience improvements.

In this paper, a comprehensive approach is presented to determine for buildings, infrastructure and public places cost-efficient security measures that are most suitable to increase the resilience of urban environments. In a first step susceptibility and vulnerability quantities are analysed and combined to various risk quantities to locally identify weak spots with respect to likely threats. In a second step a well-informed set of mitigation measures is applied and the same resilience quantities are computed again. The third step consists of a comparison of the resilience quantities resulting in a cost-benefit analysis for the applied measures. The resilience improvement is quantified with respect to performance targets including the well-being of persons, infrastructure availability, effects on the environment and physical damage of buildings and infrastructure. Forth, the counter measures leading to the most efficient resiliency improvement are selected.

The resilience assessment and improvement scheme is realized with a software-based solution including a user-friendly 3D visualization. The presented case study results focus but are not limited to physical measures. They show how to select tailored, efficient and affordable resilience improvement measures. The research of this project is funded within the EU-project EDEN.

Keywords: urban planning, resilience quantification, weak spot identification, cost-benefit analysis, selection of security measures, physical protection, application software, urban threats, sustainability

1 INTRODUCTION

Security and safety relevant issues become an increasingly important factor in modern urban planning. Different facts prove this statement: For the first time in history in 2008 the physical degree of urbanization reached a value of 50 per cent and has a rising trend [1]. This concentration of population increases associated security issues. A growing population density in cities and their agglomerations has a pronounced effect on the vulnerability to hazardous events [2]. A further argument for considering safety and security measures is based on the formation of new threats. Urban areas comprise the most critical infrastructure of the society and specify significantly their respective resiliencies [3]. According to Branscomb [3] cities are increasingly vulnerable to natural

disasters (e.g. hurricanes, flood, earthquake, and tsunamis), technogenic disasters (resulting from human error and failing infrastructure, e.g. power failure) and terrorism.

In summary, a rising urbanization and the formation and increase of new threats lead to the need of risk quantification to develop urban areas which are less vulnerable, more resilient and sustainable. This need is also underlined by the real estate industry: “The climate change has become impossible to avoid. New challenges are adaption and coping with new external threats” [4].

In comparison to existing city planning frameworks [6] the new comprehensive approach [7] [8] [9] contributes to shaping and designing the built environment, to transform a city or quarter in a more resilient state with respect to man-made and natural hazards, including a wide range of measures from physical to societal. Furthermore, the integrative assessment scheme is expected to increase knowledge, provide resources, foster emerging institutions, allow for informed decision making, enhance good governance and grant local autonomy.

In this paper, a new comprehensive approach for resilience quantification of urban areas is presented. The approach is aligned to and quantifies single indicators of the resilience cycle, see sections 2.1 to 2.4. The evaluation of expected losses (risks) brings in the terms susceptibility (frequency, probability) and vulnerability (consequences, damage). An exemplary evaluation of terroristic threats is applied using the commercial software VITRUV [5]. Results of the resilience analyses steps are visualized in a three-dimensional environment.

Section 2 introduces and discusses the resilience quantities provided for resilience management. Section 3 shows the cost-efficiency assessment of resilience enhancement measures applied in different resilience management phases. Finally, section 4 concludes this publication.

2 RESILIENCE OF URBAN ENVIRONMENTS

The expected loss for hazardous events is often evaluated with the use of similar parameters, independent of the field of research. In this context, terms like vulnerability, sensitivity, resilience, adaptation, adaptive capacity, risk and hazard or threat are frequently used. However, their relationship and discrimination is often unclear. The same terms may have different meanings when used in different contexts, e.g. social sciences or climate change research [10]. The aim of theses assessments, independent of the discipline is mostly a quantification of the expected damage in the categories of lives, injured persons, damage property or disrupted economic activity.

To quantify the resilience of urban environments the present work employs the resilience/ catastrophe management cycle of Figure 1. This threat event management approach evolves in time. The dynamic concept is used to quantify resilience and covers the following five phases and corresponding indicators or measures:

(1) Indicators for Preparation, arrangement for possible threats knowing the context (see section 2.1)
(2) Indicators for Prevention of hazardous events, reduction of frequency (see section 2.2)
(3) Indicators for Protection, decrease of damage/ impacts in case of events (see section 2.3)
(4) Indicators for Response, maintenance of essential functionalities, immediate crisis management
(5) Indicators for Recovery, bouncing back quickly (see section 2.4)

Figure 1: Five indicators of the resilience cycle [11].

The presented resilience assessment framework uses a quantification of the vulnerability (consequence in case of occurrence) to generate a relation between hazard and damage, as shown in the left diagram of Figure 2. The type of damage is related to the performance targets comprising the provision of basic services or basic security and safety, e.g. low numbers of affected people, monetary or structural damage. Hence, the vulnerability is used to quantify the discontinuity in the performance-time relation, as shown in the right diagram of Figure 2. The recovery process in Figure 2 is presented as a linear increase between the time of the disruptive event and the end time of recovery. Possible resilience enhancement measures can increase the level of performance during recovery. The subsequent sections show, how the presented weak spot analysis contributes to the indicators of the resilience cycle of Figure 1.

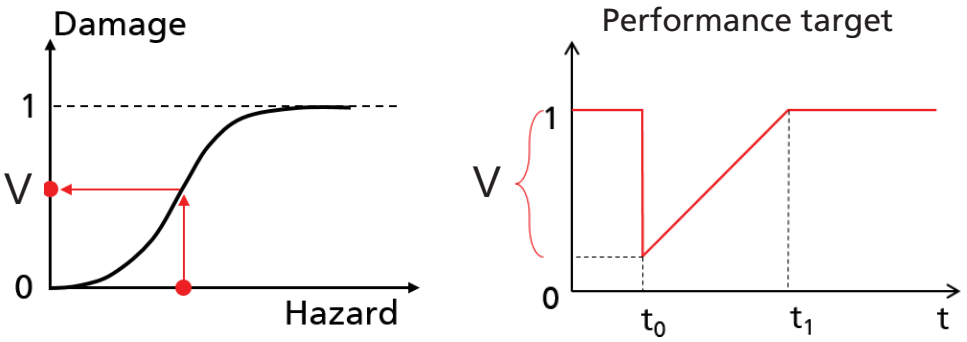


Figure 2: Relation of hazard and damage (left) for the quantification of damage (vulnerability, expected loss in case of event), which is used to quantify the resilience performance-time relation (right), i.e. a time-dependent resilience curve.

2.1 Preparation: Knowing the urban environment and context

3D digital representations of an urban area are used for a detailed and quantitative assessment concerning terroristic threats in a city. With a list of ten pre-defined building types, an arbitrary urban surrounding is approximated. As basis for the susceptibility, vulnerability and risk assessment, each urban object includes decisive attributes. For buildings, these parameters are: name, position, orientation, dimension, number of floors, floor height, construction type, material, building quality, building costs per area [€/m²], usage, building category, the person density, and access controls.

Beside the name, position and dimension, traffic infrastructure elements have some further attributes: route or rail type (e.g. highway or pedestrian area), traffic density and portion of trucks, pedestrians' density, rebuilding costs, information about rails, timetable cycle, and people per vehicle.

The use of these attributes allows a realistic approximation of urban areas. This city model can be applied for further investigation of unexpected hazardous events concerning their probability of occurrence and the expected losses, as well as modelling recovery. **Fehler! Verweisquelle konnte nicht gefunden werden.**

2.2 Prevention of hazardous events: Reduction of susceptibility / frequency of events

Insights of a quantitative susceptibility approach give information on likely events (event analysis), in particular it assesses the effects of counter measures on the frequency of threat events. The region, the urban object type, the threat type and the intensity of the threat are essential parameters to assess the frequency of events for the susceptibility quantification of a considered environment. Figure 3 shows exemplarily the calculated susceptibility for different threat positions in an urban environment. The coloured elements visualize the results of an areal threat density function, which depends on the forgoing mentioned parameters. The results use historical data of Western Europe [12]. Based on the object type of an embassy, positions around building no. 9 in the left picture result in relatively high susceptibility concerning terroristic threats. The right picture shows a changed usage of building no. 9 and the overall result has a lower criticality. This shows that based on the prevention measure local susceptibility, successful prevention measures can be selected. The susceptibility relates to the average time before events.

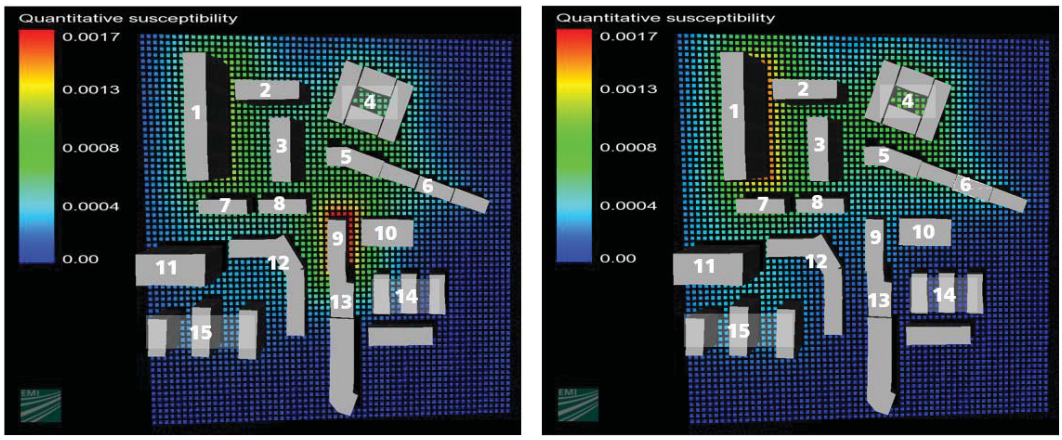


Figure 3: Region, object and threat dependent quantitative susceptibility using historical data of an industrialized society. Frequency of occurrence at possible event positions in the urban environment. The conversion for building no. 9 from embassy (left) to SME (right) reduces the local and overall absolute susceptibility. Building usage: (1) Corporation, (2,3) Finance/ trading, (4) Agency, (5,6,7,11,15) SME, (8) Supply/ disposal, (9, left) Embassy (9, right) SME, (10) Retail/ service, (12) Nursing, hospital, (13) Religion, (14, 15) Residential.

2.3 Protection: Vulnerability/Damage reduction in case of events

Based on the assessed susceptibility approach the left picture of Figure 4 shows the averaged vulnerability. In this assessment, the expected consequences are evaluated for each threat position shown in Figure 3. Every result is weighted with the threat intensity and position dependent susceptibility assuming that a threat event occurs within the urban area. Therefore, the approach gives the information of the expected losses (what-if risk), if a single threat scenario occurs allowing for all threat types and positions in the considered urban environment. The presented result shows the average progressive collapse of urban objects due to possible terroristic explosive events using physical engineering models of [13]. The approach emphasises neighbouring effects to critical objects resulting for some buildings results in a high vulnerability despite low susceptibilities.

In the right picture of Figure 4, the prevention measure of roadblocks is exemplary applied. This measure decreases the what-if susceptibility (frequency) of events with a large quantity of explosive, like vehicle bombing scenarios. The prevention of certain scenarios decreases the overall susceptibility as well as vulnerability, i.e. it contributes to prevention and protection.

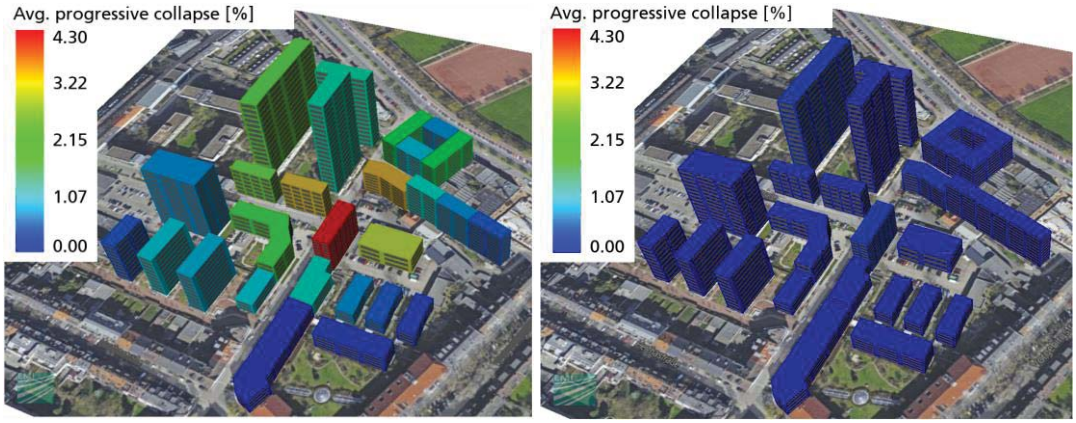


Figure 4: Comparison of the expected initial damage (left) and the weighted vulnerability with realization of access control (right). This prevention measure decreases the susceptibility of events with higher threat intensity.

Section 2.2 presented measures for prevention as well as the last text paragraph. However, there are use-cases, where a conversion of usage or an application of access control (e.g. physical access control using bollards) is not possible. The need of supply or escape routes avoid such a type of measure, for example. Hence, protection or response measures have to be considered to increase a certain level of resilience. The left picture of Figure 5 shows the initial situation of weighted vulnerability as basis for comparison. The right picture of Figure 5 presents the expected losses using an increasing robustness of selected objects. In this example innovative materials, like Ductile Concrete [14] or masonry retrofit [15] are applied to load bearing elements to enhance the resistance behaviour due to blast loading. A direct comparison of the two situations in Figure 5 emphasises the degree of damage reduction for the selected objects.

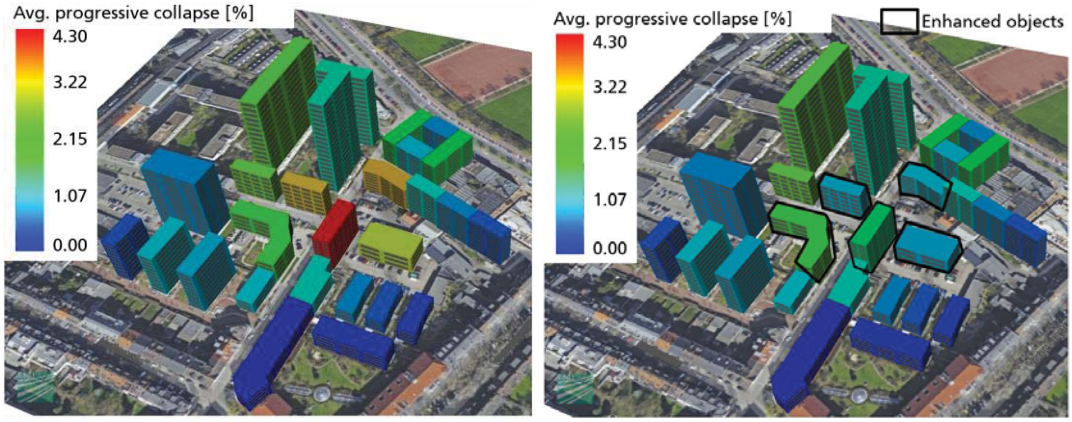
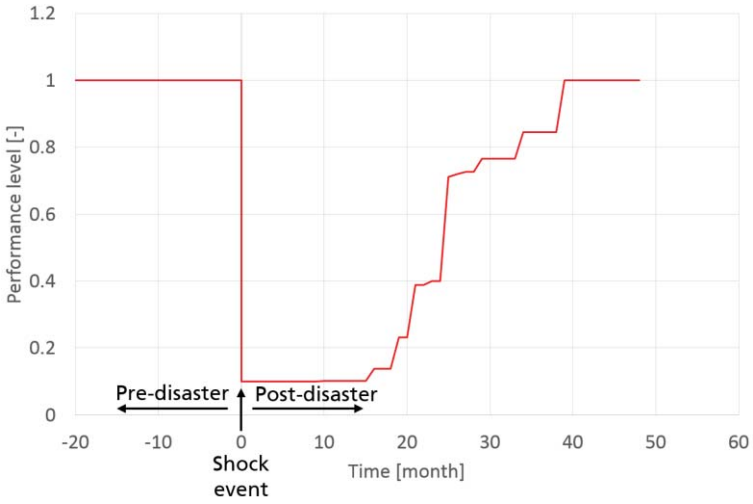


Figure 5: Comparison of the expected initial vulnerability (left) and the vulnerability with physical security enhanced objects (right). This protection measure decreases the vulnerability of selected buildings by increasing their robustness. The disruptive initial loss/ damage is reduced.

2.4 Recovery after threat occurrence

With respect to the presented resilience cycle in Figure 1, the last indicator describes the recovery process of a system. Based on the pre-defined construction types, each building relates to a planning and construction time. These time specifications in combination with a defined standard progress of reconstruction are applied to quantify the generalized performance-time relation of the right diagram in Figure 2. The recovery process in Figure 6 results from the summation of single urban objects and their corresponding planning and construction times. Finally, the integration of this curve in relation to the overall time span can give a further measure for the resilience of an investigated urban area. Based on the availability of resources or the rapidity after a

shock event, the time of recovery decreases, which has a positive effect on the measure of resilience [16].



,

Figure 6: Time-dependent resilience curve: reconstruction progress time history after disruptive event. Assessed performance-time relation of an urban environment after the occurrence of a hazardous event.

3 COMPARISON OF RESILIENCE INDICATORS

Based on the definition of urban objects and the corresponding parameters, see section 2.1, the comparison of the overall what-if (a threat event occurs) vulnerability is used to measure the effectiveness of a resilience improvement measure. The left diagram of Figure 7 shows exemplarily the degree of damage reduction for the measures prevention ("bollards"), protection ("enhanced structures") and preparedness ("changed usage"). Finally, the evaluation of monetary damage (right diagram of Figure 7) is a building block for the cost-benefit analysis of single resilience enhancement measures. Therefore, the approach gives a broad transparency for decision makers.

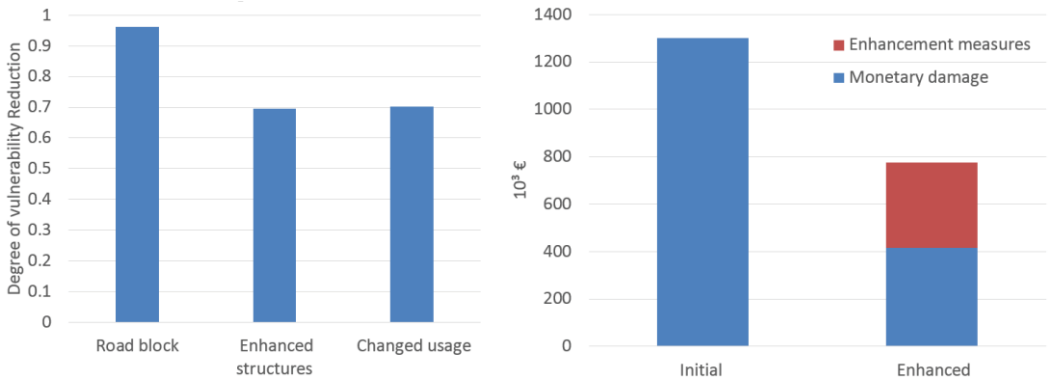


Figure 7: Comparison of different resilience indicators as input for cost-benefit analysis. The left hand side shows the costs of all enhancement measures. In case of an event, the measures will result in less overall costs, even without pricing any effects on humans, the society and economy.

4 CONCLUSIONS

This paper presents a quantitative resilience assessment scheme for the evaluation of urban areas with respect to disruptive man-made hazards. It defines up to serval measures for resilience for the resilience management phases prevention (local and overall absolute and what-if susceptibility), protection (local what-if vulnerability, overall what-if vulnerability) and recovery (reconstruction recovery resilience curve).

Furthermore, it quantifies which information is necessary to be prepared, in particular which attributes of buildings and infrastructure suffice to conduct resilience analysis. All but the response phase are covered. However, also for the latter quantitative resilience measures can be provided [17].

In the presented approach physically designed representative urban object types are used to approximate an arbitrary environment. Historical data of hazardous events derive the frequency in dependency of the region and the urban object type. The empirical frequency determines the quantitative susceptibilities. Besides using the empirical data, the local susceptibility is derived with a multidimensional surface area density function that includes further information on threat locations considering the configuration of the urban environment, e.g. the location of building entrances.

The basis for the quantitative vulnerability estimation builds the implementation of established physical and engineering models to overcome poor statistical consequence data. The pre-defined building types are considered for the approximation of a given surrounding and allow an evaluation of personal, structural, and monetary damage. In comparison to existing risk assessment schemes, the presented approach takes multiple positions and multiple intensity quantities of possible threats into account. Weak spots of urban surroundings can be easily detected and build the basis for decision makers to apply possible resilience enhancement measures.

In relation to the resilience cycle, this comprehensive approach can quantify the effectiveness of a single resilience measure using the resilience indicators. The approach shows in which resilience phase or phase the measure will be most effective, in particular whether the time-dependent recovery resilience curve improves.

Furthermore, this approach creates a basis for the cost-benefit analysis of single measures, in particular since it does not aim at pricing the loss of lifetimes. The new comprehensive resilience assessment is integrated in a suite of computerized tools and is readily available for security considerations in urban planning. Hence, this approach give contributions to generate more robust, resilient and sustainable cities.

5 ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Commission's 7th Framework Programme under grant agreement no. 313077. The contributions of all EDEN consortium members are gratefully acknowledged.

REFERENCES

[1] United Nations, "World Urbanization Prospects, the 2011 Revision," 2011. [Online]. Available: http://esa.un.org/unpd/wup/. [Accessed 19 01 2015].

[2] J. Cross, "Megacities and small towns: different perspective on hazard vulnerability," *Environmental Hazards 3,* pp. 63-80, 2001.

[3] L. Branscomb, "Sustainable cities: Safety and Security," *Technology in Society 28,* pp. 225-234, 2006.

[4] Bundesinstitut für Bau-, Stadt- & Raumforschung, "ImmoRisk - Risikoabschätuzung der zukünfitgen Klimafolgen in der Immobilien- & Wohnungswirtschaft," Berlin, 2011.

[5] Fraunhofer EMI, “VITRUV - Vulnerability Identification Tools for Resilience Enhancements of Urban Environments,” 2014. [Online]. Available: http://www.vitruv-tool.eu/. [Accessed 19 05 2015].

[6] Y. Jabareen, “Planning the resilient city: Concepts and strategies for coping with climate change and environmental risk,” *Cities 31,* pp. 220-229, 2013.

[7] M. Voss, I. Häring, K. Fischer, W. Riedel and U. Siebold, “Susceptibility and vulnerability of urban buildings and infrastructure against terroristic threats from qualitative and quantitative risk analysis,” in *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference (PSAM & ESREL)*, Helsinki, Finland, 2012.

[8] K. Fischer, W. Riedel and I. Häring, “Vulnerability identification and resilience enhancements of urban environments,” *Communications in Computer and Information Science 318,* pp. 176-179, 2012.

[9] K. Fischer, A. Klomfass and I. Häring, “An engineering approach for risk, resilience and vulnerability assessment of urban areas,” *5th International Conference on Design and Analysis of Protective Structures, Singapore,* 2015.

[10] N. Brooks, “Vulnerabiltiy, risk and adaptation: A conceptual framework (Working Paper 38),” Tyndall Centre for Climate Change Research, Norwich, UK, 2003.

[11] K. Thoma, “Resilien-Tech - "Resilience-by-Design": Strategie für die technologischen Zukunftsthemen,” acatech, Deutsche Akademie der Wissenschaften, Berlin, 2014.

[12] K. Fischer, U. Siebold, G. Vogelbacher, I. Häring and W. Riedel, “Empirical analysis of security critical events in urban areas,” *Bautechnik 91(4),* pp. 262-273, 2014.

[13] I. Müllers, K. Fischer, A. Nawabi and W. Riedel, “Design against Explosions and Subsequent Progressive Collapse,” *submitted to Structural Engineering International,* 2015.

[14] A. Stolz, K. Fischer, C. Roller and S. Hauser, “Dynamic bearing capacity of ductile concrete plates under blast loading,” *International Journal of Impact Engineering 69,* pp. 25-38, 2014.

[15] W. Riedel, K. Fischer, C. Kranzer, J. Erskine, R. Cleave and D. Hadden, “Modeling and validation of a wal-window retrofit system under blast loading,” *Engineering Structures 37,* pp. 235-245, 2012.

[16] M. Bruneau and A. Reinhorn, “Exploring the Concept of Seismic Reslience for Acute Care Facilities,” *Earthquake Spectra 23(1),* 41-62 2007.

[17] W. Riedel, K. Fischer, A. Stolz, I. Häring und M. Bachmann, „Modeling the vulnerability of urban areas against explosion scenarios,“ in *3rd International Conference on Protective Structures*, Newcastle, Australia, 2015.

ASSESSING PASSENGER FLOWS AND SECURITY MEASURE IMPLEMENTATIONS IN PUBLIC TRANSPORTATION SYSTEMS

Silja Meyer-Nieberg[1], Martin Zsifkovits[2] , Stefan Pickl[3], and Florian Brauner[4]

[1]*silja.meyer-nieberg@unibw.de*
Universitaet der Bundeswehr Muenchen, Werner-Heisenberg-Weg 39, 85579 Neubiberg (Germany)

[2] *martin.zsifkovits@unibw.de*
Universitaet der Bundeswehr Muenchen, Werner-Heisenberg-Weg 39, 85579 Neubiberg (Germany)

[3]*stefan.pick@unibw.de*
Universitaet der Bundeswehr Muenchen, Werner-Heisenberg-Weg 39, 85579 Neubiberg (Germany)

[4] *florian.brauner@fh-koeln.de*
Cologne University of Applied Sciences (CUAS), Institute of Rescue Engineering and Civil Protection, Betzdorfer Str. 2, 50679 Cologne (Germany)

Abstract

Critical infrastructures are essential for the functioning of state and society. Therefore, the prevention of any business interruption is of great importance. In this research-in-progress paper, we focus on the assessment of security measures and structural conditions in public transportation systems and how they influence the passenger flows in such a system. The approach presented in this paper combines real-life observations with computer experiments to strengthen prospective simulations tools for decision-makers. Using the example of major train stations, first analysis results are presented, where high peaks of passenger density will possibly occur and why. Therefore, a simulation model was created, which includes a 3D visualization component to provide decision-makers with comfortable means to visualize results.

The results will be compared and extended by data of a real-life exercise in a train station for validation and verification.

Keywords: RiKoV, simulation, real-life exercise, public transportation

1 INTRODUCTION

Critical infrastructures are essential for the preservation of state and society. Therefore, their protection is a primary task and a challenge for all stakeholders today. Public transportation systems are critical infrastructures according the classification of the German Federal Ministry of the Interior [3]. That means any disturbance of these structures leads to serious consequences of the public security or community. Especially, the rail-bound public transportation system is difficult to protect against man-made threats such as terrorism because it is often characterized as an open system with many entrances and high vulnerabilities [4]. To prevent disturbances providers, operators and authorities spend high efforts in risk and crisis management. Therefore, the project RiKoV [13] (funded by the German Federal Ministry of Education and Research) focuses on rail-bound public transport by considering costs and effects of security measures against terrorist threats. Here, the question arises, how the effects of certain measures can be assessed. Since real data is scarce, statistical analyses cannot be conducted.

The problem becomes even more pronounced if new technology shall be taken into consideration where only technical data and characteristics are obtainable. This does not allow the estimation of the impacts caused by the installation and integration into security concepts. Furthermore, additional factors have to be taken into account, which in the case of train stations concern among others station layout and structure and interactions of measures with passenger flows. Aside from identifying the interactions, it is important to analyse the flows w.r.t. common patterns and accumulation points with high passenger densities since they may represent e.g. critical areas for surveillance and tracking.

The everyday crowd behavior can be discerned by monitoring and analysing passenger crowds in a station. While this results in valuable data concerning the general behaviour, it cannot be used to test and assess the effects of security measures. For this assessment simulations (computer-based) and exercises (real life data) are required. Both have their strengths and weaknesses. Real-life exercises are time-consuming and expensive. In addition, they do not allow implementing and testing the same range of options that are available in a computer experiment. Their advantage is that they work directly with human actors not requiring a model.

The approach presented in this paper combines real-life observations with computer experiments. It aims at developing a partly automated prototype that allows carrying out simulation-based analyses of security measures. As a first step, real-life passenger flows from several stations are analysed in order to identify general behavioural patterns. This paper reports first results from two exemplary train stations in Munich and Cologne. Based on the patterns identified, a simulation model is developed for passenger crowd behaviour in railway stations. We propose to model the passengers as agents with stochastic components. The resulting model can be parametrized with real-life data and can therefore be adapted to new stations and used for simulation-based analyses.

In any analysis, the communication of the results is important. For this, visualization is a valuable tool. Therefore, the simulation model is augmented by a 3D visualization component, which provides decision-makers with a comfortable means to visualize and to relive representative simulation runs.

The paper is structured as follows: First, an introduction to the study focus is provided. The real-life experiments are described and analysed in the following section, before their combination with computer-based simulation analyses is discussed. The paper proposes to use data farming experiments in combination with agent-based models and provides a first analysis for the main station in Munich.

2 REAL-LIFE EXPERIMENTS

Real-life exercises provide the possibility to gain data for comparison with computer-based simulations (CBS) with real-life data e.g. pattern behavior. In addition exercise data provide the possibility to configure the setting of CBS at the beginning of the simulation to foster the reliability of results.

In May 2015, the Cologne University of Applied Sciences (CUAS) executed two exercises to collect data for risk and crisis management actions.

2.1 Context of Real-Life Exercise (Scenario description)

A fictitious terror scenario of a bomb attack in a public subway station was chosen to measure the effectiveness of different security measures as well as their effects on passenger flows in the station. Decision-makers, who are responsible for the implementation of security measures, are highly interested in a proof-of-concept of

security measures, especially, when security measure cause a serious impact on the customers e.g. negative influence on passenger flow.

Therefore, CUAS set up an exercise environment in a subway station having three levels (ground floor, intermediate level and train platform) and the different security measures (CCTV, security patrols, metal detectors, foot scanner, luggage scanner, fluid scanner, explosive scanner). In an operation status, hundred passengers were divided into different start groups passing the security measures. While the performance of different settings in the security measures are measured according their real performance, the passenger traffic is captured using a sensor grid of a local positioning system.

2.2 Data Aggregation Methodology

The local positioning system uses an ultra-wideband wireless measurement grid that tracks tags in location and time in a 3D visualization environment [18]. The time and location data of each passenger allows detecting high density spots caused by waiting times or structural conditions (e.g. stairs, platform, etc.).

It allows visualizing the behaviour of certain passenger groups e.g. a fictive terrorist related to security patrols or other security measures such as CCTV in a real environment. The technical security measures have an own documentation system, storing the results of their check/analysis in a server database. Using ntp (network time protocol), the data is fused in a common knowledge database.

2.3 Knowledge database

The knowledge database integrates all data of the security measures, the local positioning system, passenger descriptions as well as semi-quantitative and qualitative data by observers in one database. The database allows providing a central link to answer several research questions. In this case, exemplary the crowd behavior was chosen to run analysis.

At this research-in-progress step, just a broad overview can be given about first results. The analysis of passenger flows in the subway station showed a highly dependency of passenger flows according guidance systems and structural narrowness. Security measures that require additional time for clearances of alarms lead to increased passenger densities. The experiments showed that e.g. the detection rate and sensitivity setting of security measures highly influence the passenger flows. Once the passenger has passed the different security measures and has entered the secured area, a high passenger flow can be realized.

3 FROM REAL-LIFE EXERCISES TO COMPUTER-BASED SIMULATIONS

This section changes the focus to computer-based simulations and the analysis of the resulting system. First, a short introduction into simulation experiments is provided. Afterwards, existing approaches concerning crowd simulation are discussed, before the model developed is described.

3.1 Combining Experiments and Visualization

Real-life experiments can be augmented by computer-based simulations. Both approaches have their strengths and their weaknesses. It should be noted that both have to be interpreted as models of the true, unobserved situation. Since real-life experiments follow scripts and rules and since people are aware that they are observed, distortions have to be expected. However, they are conducted in real-life without the necessity of building executable models of persons and their interactions. Switching to computer-based simulations will result in a further abstraction and

simplification. Nevertheless, computer-based analyses allow conducting more experiments and to consider scenarios that cannot be investigated in real-life due to costs, security, and time required. For these reasons, a combination of both experiment types appears as a suitable means to address the research questions arising in RiKoV. Furthermore, the real life experiments and data stemming from further data collections, can be used to determine the influence factors of the model and of course for its verification and validation.

We will see below that the analysis of the agent-based models utilized in this paper is not an easy task and usually requires methods from statistics and data mining. While the results can be visualized and the effects observed can be traced back to the respective influence factors, it is not always easy to understand the interactions. Providing an opportunity to re-enact and to experience exemplary runs in a 3D simulation, may improve the acceptance of the results by the decision maker. Our analysis approach rests on three columns: real-life data/experiments, computer-based analyses with the help of agent-based models, and computer-based visualization. Due to space restrictions, the latter is not described in this paper.

3.1.1 Simulation-Based Analysis

Computer-based simulations require executable models pertaining to the scenario that shall be analysed. Here, we shortly sketch the approach followed in Data Farming [2], a relatively new approach similar to the better known Design and Analysis of Simulation Experiments (DASE) [9] and the Design and Analysis of Computer Experiments (DACE) [14]. In all cases, first a concise description of the purpose and the extent of the analysis is required since the model developed must be tailored to the situation and to the research question. Furthermore, performance measures have to be introduced in order to judge the outcome of the experiments. In this paper, agent-based systems or models are applied. Agent-based models (ABMs) are concerned with the behaviour of autonomous agents, depicting the actions and interactions between them and the environment [11]. They are used to analyse the (collective) behaviour of the modelled system.

Unfortunately, no generally accepted definition of the term agent exists [17, p.21]. In this paper, the following definition is used: “An agent is a computer system that is situated in some environment, and that is capable of autonomous action in this environment in order to meet its delegated objectives” [17, p.21]. Agents may thus interact with each other and with the environment. Since this paper is concerned with individual passenger behaviour, an agent-based model appears as an appropriate choice. The model and the description of the basic scenario provide the foundation for the analysis. It should be noted that the analysis of agent-based models is not easy due to stochastic influences and on the interactions on the individual level. This necessitates an experimental analysis in nearly all cases.

Before starting the analysis the intervals for the values of the influence factors have to be defined. The simulation runs are used to provide insights on the interactions between these parameters and on their influence on the performance measures. Once, the permissible ranges have been set, the question remains how to combine the parameter values in order to cover the search space on the one hand and to operate with a permissible number of experiments on the other hand. For this, experimental designs as e.g. nearly orthogonal Latin hypercube designs [7] may be used. It should be noted that for one parameter combination, several simulation runs have to be carried out since the model is usually stochastic. For this reason, data farming is often conducted on computing clusters.

The simulation runs result in vast amounts of data which need to be analysed. Here, methods from statistics (histograms, box-plots, regression analysis, classification and regression trees) and data mining (support vector machines, neural networks) can be

applied, see [5] for an overview. Data farming is often iterative since new experiments with different parameter settings may be required if interesting effects are observed. In addition, the simulation runs may reveal the need to re-address certain aspects of the model or may lead to new research questions. Before introducing the agent-based model that was used in the analysis, a brief overview of existing approaches in literature is provided.

3.2 Simulating Crowd Behavior

The simulation of pedestrian behavior has gained considerable interest in the last decades. The ability to simulate the behavior and motion of crowds is not only cheaper but also less dangerous than real experiments. This holds especially for extreme scenarios. Results are of interest for various institutions and companies, such as constructors of buildings, airplanes and ships; operators of large public constructions or mass events; or providers of public transport systems. Such system models allow for simulating evacuation scenarios in advance, discover possible existing problems and optimize plans [10]. Furthermore, the simulation of passengers' behavior in public transport systems compared to abnormal behavior is of great interest for identifying possible terroristic threats. Due to the increase in computational power over the last years, simulations of huge crowds are much more feasible today. However, the most critical part in such models is the parameterization of actors. Despite many people assume human behavior to be very irregular and not predictable, which may be true for extremely complex situations, it is possible to make some general rules for movement. Since a pedestrian is used to a given situation, he reacts rather automatically and determined by his experience [6]. Therefore, findings from real life experiments are very promising for a realistic parameterization.

In order to achieve complex behavior one often chooses a stochastic description instead of a deterministic one [15]. In complex situations even a minor change of the environment or minor events could lead to very different behavior which could only hardly be described by a deterministic approach. The stochastic approach takes into account that one usually does not have full knowledge about the system and its dynamics. Furthermore, average processes are described and questions about the probability of a certain event can be answered [15]. It is not necessary for a reliable simulation to know how a certain pedestrian acts, i.e. whether he/she turns left at the next possibility or not. It is sufficient to know what percentage of pedestrians turn left. Most models use a microscopic approach which models the individual behavior of a pedestrian. All the macroscopic behavior is a result of the interactions among the pedestrians.

3.3 Pedestrian Flows: An Agent-Based Model for Passenger Flows for the Example of the Munich Central Station

Two stations are considered in our ongoing research project: the subway station in Cologne where real-life data is obtained with the help of experiments and the central station of Munich. The stations considered augment each other: While the station in Cologne offered the chance to observe the effects of security measures on passenger flows directly in experiments, this opportunity does not exist in Munich. Here, the analysis can only be conducted with the help of computer simulations. However, the central station in Munich allows collecting data providing insight in the normal operation of a large train station. Keeping in mind the different types of the stations, findings can be transferred and be used as inputs for the baseline scenarios and analyses and for investigating the effects of security measure installations. As a first step, the agent-based model called Pedestrian-Flows is developed and parametrized for analysing the situation in the central station of Munich.

Munich is currently the second largest train station in Germany with estimated 350,000 passengers served by 240 long distance trains and over 500 short distance trains [7]. It is one of the main traffic hubs in the city itself, connecting to suburban trains and underground trains as well as to bus and tram lines. The terminal station with over 30 tracks consists of three distinct parts: the central platforms dedicated mainly to the long distance travel and two separate stations for regional lines. Figure 2 shows the layout of the station. The two smaller stations are in the upper left and right parts of the figure. All platforms are accessible from the main hall where shops and restaurants are also located. The station has three main entries which connect to the main hall and the ticket hall. As the figure shows, there are several shops, restaurants, and vending machines where people may cluster.

Figure 1: Munich central station. Figure taken from [12].

Furthermore, since two main entrances directly open into the main hall and since the hall must be passed by arriving passengers from long-distance-trains to leave or to change trains, pockets with higher population densities are expected. The question remains however, whether they are transient and dissolve in a short time or whether they persist. This is one of the research questions that shall be addressed in this paper. Of great interest are the effects of security installations on the passenger flows. Before these can be analysed, however, attention has to be paid to the interaction of the "normal" station layout with the passenger flows. This investigation is important since it helps to differentiate the effects due to the security measures from the effects stemming from the original structure. In addition, the analysis of several baseline scenarios provides insights where security installations may be located.

For the analysis, an agent-based model was designed to investigate where accumulation points occur. The agents enter the train station in one of the entries or by train, may stop at one or more of the shops, restaurants or ticket vending machines and may leave the station again via the exits or by boarding a train. Arriving trains provide large influxes of passengers the system has to cope with. Since a collision avoidance routine is implemented, larger densities of agents slow down the flow of passengers. The behaviour of the agents is determined by their type. Currently, the groups of commuters, tourists, and non-local business travellers are distinguished. The model, however, is easily adaptable to accommodate further groups. The agent type determines among others the destinations and the spawn points and of course the probabilities for stopping on their way to their destination. Not only the agents, but also the arriving trains and their types influence the simulation. Therefore, additional influence factors are taken into account.

In order to derive the permissible intervals for the influence factors, a data collection was conducted in the spring of 2015 resulting in data from 966 persons. The analysis is still ongoing and will be used for further data farming experiments. First results show that some station entrances are preferred with only a few passengers using the entries of the regional stations. Furthermore, a significant percentage between 30 to 55 % of passengers uses the station as a pass-through or visits the shops without boarding the trains. The data collected further indicates that most persons approach their destination directly whereas around one third of the passengers makes between one and three stops on their way.

The agent-based model was implemented with NetLogo [16] developed by Uri Wilensky in 1999. While it has originally been aimed at students, it has emerged as a serious research tool today. In the following, some examples from the first data farming experiments are provided [1]. The analysis investigates the effects of eleven parameters including the percentages of the different groups, the occupancy rate of incoming trains, and the distribution of the passenger types on the incoming regional trains. Using a nearly orthogonal Latin hypercube design [8], 33 combinations or data points are taken into account. For each data point, 30 simulation runs were conducted on a machine with 24 Intel Xeon X5690 CPUs with a maximal speed of 3466 MHz on six cores. A run of a single experiment took approximately two hours.

As performance measures, the passenger pass-through rates per time step, the waiting times caused by the traffic, and a coarse-grained spatial distribution of the passengers were considered. The experiments showed that e.g. the entrances to the regional stations, which are relatively narrow represent bottlenecks for the passenger flows. In contrast, the main hall of the central station provides an easy access to the tracks and trains. However, the hall is passed by many agents resulting in relatively high passenger densities. This is in contrast to the Cologne main station, which was also taken into account to provide an example of a pass-through station. Here, the effects of a clear separation between platforms and market hall can be observed.

4 CONCLUSIONS AND OUTLOOK

This paper gave an overview on ongoing research in the context of the project RiKoV, which is concerned with estimating the risks due to terrorist attacks and the costs and effects of security measures. Among others, security measures will interfere with the flow of crowds in the station. Furthermore, existing pockets of high passenger densities should be identified beforehand. To this end, the paper proposes combining real-life exercises with simulation-based analyses and reports first results from Cologne and Munich.

In the future, we will focus on a sensitivity analysis of the security measures setting and their influence on the passenger flows, to archive the right balance between security and satisfying customer flows in public transportation systems. The results will lead into guidelines for decision-makers for future security designs.

5 ACKNOWLEDGMENTS

The support by the German Federal Ministry of Education and Research is gratefully acknowledged.

REFERENCES

[1] Biskupski, K.; Luther, S. and Hauschild, D. (2015). *Datafarming mit Multiagentensystemen am Beispiel des öffentlichen Personennahverkehrs*. Bachelor Thesis, Universität der Bundeswehr München, 2015.

[2] Brandstein, A. G. and Horne, G. A. (1998*). Data Farming: A Meta-technique for Research in the 21st Century*. Maneuver warfare science 1988 US Marine Corps Combat Development Command Publication.

[3] Bundesministerium des Innern (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)* Last accessed on 11.06.2015. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html

[4] Brauner, F.; Baumgarten, C.; Kornmayer, T.; Bentler, C.; Mudimu, O. A. and Lechleuthner, A. (2014). *A Methodology for a vulnerability analysis of public transportation systems in context of terrorist attacks.* In: Thoma, K.; Häring, I.; Leismann, T. (Eds.): 9th Future Security, Security Research Conference; Sept. 16-18, 2014 in Berlin, Germany; Fraunhofer Verlag, Stuttgart; ISBN 978-3-8396-0778-7; pg. 271-277.

[5] Hastie, T.; Tibshirani, R.; and Friedman, J. (2001). *The Elements of Statistical Learning*, Springer.

[6] Helbing, D.; Molnar, P. (1995). *Social force model for pedestrian dynamics*. Physical review E 51(5), 4282. http://arxiv.org/pdf/cond-mat/9805244. Accessed 8 February 2015

[7] Hauptbahnhof München (2015), URL: http://www.muenchen.de/verkehr/orte/120302.html. Last accessed on 11.06.2015.

[8] Joshua, A. (2006). *Extending Orthogonal and Nearly Orthogonal Latin Hypercube Designs for Computer Simulation and Experimentating*. PhD Thesis, NPS Monterey, 2006

[9] Kleijnen, J. (2008). *Design and Analysis of Simulation Experiments*. Springer.

[10] Kretz, T. (2007). *Pedestrian Traffic - Simulation and Experiments*. Dissertation, Universität Duisburg-Essen. http://duepublico.uni-duisburg-essen.de/servlets/DerivateServlet/Derivate-16251/Kretz_dis.pdf (2007). Accessed 8 February 2015

[11] Macal, C. M. and North, M. J. (2010). *Tutorial on agent-based modelling and simulation*. Journal of Simulation 4(3):151–162.

[12] München Hauptbahnhof. URL: http://www.bahnhof.de/bahnhof-de/Muenchen_Hbf.html. Last accessed on 11.06.2015.

[13] Pickl, S.; Raskob, W.; Lechleuthner, A.; Laible, W.; Schmitz, W. et al. (2011). Common Proposal for joint research project: *RIKOV Risiken und Kosten der terroristischen Bedrohungen des schienengebundenen ÖPV: Eine Planungslösung für die ökonomische und organisatorische Optimierung präventiver und abwehrender Maßnahmen*. BMBF Projekt Förderlinie - Sicherheitsökonomie und Sicherheitsarchitektur.

[14] Santner, T. J., Williams, B.J., and Notz, W. I. (2003). *The Design and Analysis of Computer Experiments*. Springer Series in Statistics Springer.

[15] Schadschneider, A. (2002). *Cellular automaton approach to pedestrian dynamics-theory*. In: Pedestrian and evacuation dynamics, pp. 76–85.

[16] Wilensky, U. (1999). *NetLogo*. Last accessed on 31.07.2014. URL: http://ccl.northwestern.edu/netlogo/.

[17] Woolbridge, M. (2009). *An Introduction to Multiagent Systems*. John Wiley and Sons, 2nd edition.

[18] Ubisense AG. (2007). *Ubisense Precise Real-time Location – System Overview*. Last accessed on 11.06.2015. URL: http://www.ubisense.net

EXPEDIA - A NEW EU PROJECT AIMING TO REDUCE THREATS FROM HOMEMADE EXPLOSIVES

Thomas Keicher[1], Sven Hafner[1], Horst Krause[1],Henric Östmark[2], Malin Kölhed[2], Patrik Krumlinde[2]

[1] *thomas.keicher@ict.fraunhofer.de*
Fraunhofer-Institut für Chemische Technologie (ICT), Joseph-von-Fraunhofer-Str. 7, 76327 Pfinztal (Germany)

[2] *malin.kolhed@foi.se*
Totalförsvarets Forskningsinstitut (FOI), Swedish Defence Research Agency, Grinsjön, SE-147 25 Tumba (Sweden)

Abstract

Under the acronym EXPEDIA, which stands for **EX**plosives **P**r**E**cursor **D**efeat by **I**nhibitor **A**dditives a European consortium of eight nations is working to reduce threats from homemade primary and main charge explosives. This paper will present the aims of this project and how the results could reduce threats from homemade explosives (HME).

EXPEDIA will work on inhibiting additives that should prevent the transformation of precursors that are available as everyday chemicals to the public, into explosives. EXPEDIA will also investigate garage chemistry and will explore possible routes for HME manufacture. This project also will contribute with knowledge to identify different precursors and recognize garage laboratories for HMEs. This knowledge will be included in a European guide for first responders as an unclassified document. This guide will include scientifically assured, up to date information about the hazards of homemade explosives and safe handling once discovered in the field.

Keywords: Homemade explosives, improvised explosives, garage chemistry, inhibiting additive.

1. CONCEPT AND OBJECTIVES

Several basic household chemicals which are readily available and easily accessible can, in the hands of terrorists, be transformed to homemade explosives (HMEs). These chemicals are referred to as precursors and although the issue of the misuse of precursors is currently being addressed in previously and currently funded FP7 projects, the list of investigated precursors within these projects is far from complete and the threat from new substances is growing due to the accelerated information exchange on the internet. The objectives of the EXPEDIA project are to inhibit some frequently used explosive precursors and to increase the knowledge about “garage chemistry”. The inhibition studies of these precursors will be closely linked to feasibility and implementation cost evaluations as well as to toxicology investigations. The solutions should be environmentally friendly and economically defendable in order to be able to be implemented in large scale industrial processes. The garage chemistry studies are aimed to increase the understanding of how terrorists create HMEs and how easily it is performed, what chemicals they start from, where they find them in the open market, what basic equipment is required and to identify new threats. As one outcome of these studies, EXPEDIA will create a European guide for first responders with basic instructions on how to interpret findings on a crime scene when suspected bomb factories have been encountered.

In order for European legislators to take the correct decisions in the fight against terrorism, access to accurate data and in-depth understanding of the characteristics of HMEs and

various formulations thereof is of crucial importance. EXPEDIA will communicate generated information about HMEs directly to these groups via appropriate channels. Understanding the terrorist perspective and time line in HME production and preparation for an attack will give direct input to both first responders and European legislators.

2. WHAT IS "GARAGE-CHEMISTRY" AND WHY IS EXPEDIA EXPLORING IT?

"Garage chemistry" refers to chemistry performed outside a professional laboratory or a commercial factory. In many cases the garage chemist is an enthusiast who likes to experiment with chemicals, but in other cases the performed chemistry is illicit manufacturing of drugs and/or explosives. Some precursor substances can be found commercially available in pure form, whereas the majority is diluted or present in for example pastes or solid formulations. Therefore the garage chemist needs to purify or physically manipulate products in order to obtain a substance with the desired properties and sometimes even precursors need to be synthesized from very basic chemicals. Advanced chemical equipment and apparatus are probably not found in a home laboratory; instead the equipment is simple and homemade. This makes analysis of chemicals difficult to perform and properties like purity are most probably lacking and can only be roughly estimated. In case of explosives the purity is essential for stability, sensitivity and performance and accidents unfortunately occur due to incorrect handling or storage. Knowledge of recipes and possible equipment together with knowledge of sensitivity and stability of homemade explosives are essential for developing inhibitors for the manipulation of precursors and to advice first responders properly. When a bomb-attack has occurred the forensic investigation can show what type of explosives has been used in the attack. However, how they were produced is much harder to determine. This is one of the reasons why EXPEDIA need to explore possible routes for HME manufacturing. The main reason, however, is attributed to the fact that an HME can be prepared in many ways and it is a necessity to make the inhibition at a stage where as much of the routes can prevent the HME to be prepared. Detailed chemical understanding of specific parts of the synthesis of HMEs is extremely important for assessing where the effort provides the highest possible efficiency in the inhibition.

The objectives of EXPEDIA in this topic are:

• Inhibition of commercially available precursors to prevent synthesis of HMEs

• Creation of a European guide for first responders with basic instructions on how to interpret findings on a crime scene when suspected bomb factories have been encountered

• To provide scientifically evaluated information regarding homemade explosives and "garage chemistry" to European legislators

• To organize workshops for presenting and discussing the results reached, aimed at the European Commission Services, legislative and inspection bodies and law enforcement agencies and their precursor industries, as well as governmental end users and first responders and get their input on the structure and content of the European first responders guide

3. INITIATOR SYSTEM AND MAIN CHARGES

The main charge in bombs often consists of an explosive that is high in energy but low in sensitivity and therefore is difficult to initiate. A primary explosive on the other hand is low in energy but high in sensitivity, which means that it is easy to trigger but will not necessarily initiate the main charge due to its relatively low energy content. In such cases a booster charge is used and acts as a bridge between the primary and the main charge. There are examples of main charges and boosters consisting of primary explosives but this exposes the bomb maker to considerable risks both during manufacturing and during transport of the

bomb due to the sensitive nature of the explosive. Following Fig. 1 shows the different parts of a bomb and the functional sequence. The focus of EXPEDIA will be on both main charges and initiator systems.

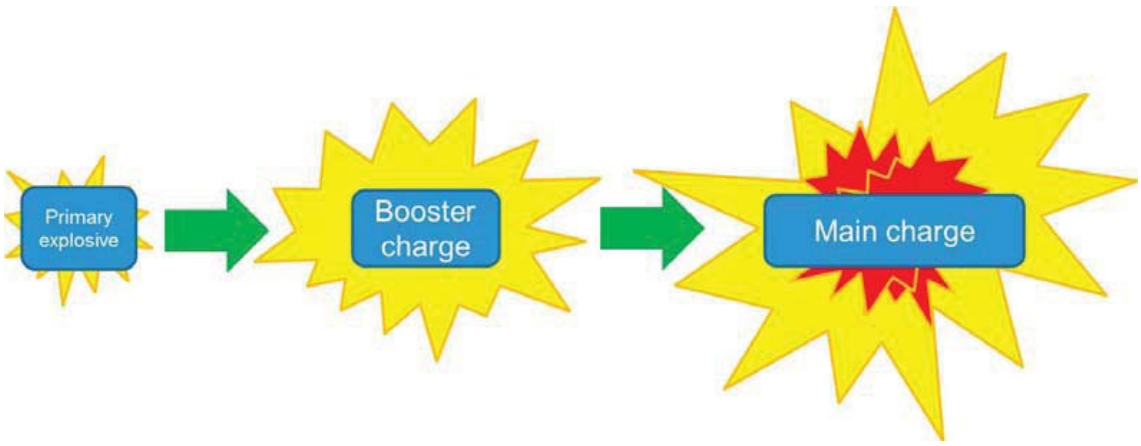


Figure 1: The different explosive parts of a bomb.

3.1 Initiator system and primary explosives

Improvised primary explosives are essential to build blasting caps/detonators for initiation of secondary explosives to detonation. There can be found varying recipes and synthesis instructions for this type of explosives. However, not all of them work in practice.

The objectives of EXPEDIA in this topic are:

• Collection of syntheses descriptions for improvised primary explosives from open literature sources like internet forums, news groups and terrorist handbooks

• Evaluation of the recipes with commercial available precursors with special focus on Hexamethylene triperoxide diamine (HMTD) and Diazodinitrophenol (DDNP)

• Evaluation of the equipment and the synthesis skills, which is necessary to build functional initiators

• Characterization of HMTD and DDNP (purity, sensitivity, life time and detonation properties)

• Evaluation of the specific characteristics of garage chemistry to provide new opportunities for detection of bomb factories and provide essential information for first responders to recognize bomb factories for initiator production including instructions how to deal with the threats.

• Investigate ways to inhibit hexamine to prevent the synthesis of HMTD from day-to-day chemicals

3.2 Main charge and secondary explosives

The targets are main charges made from home-made acids, perchlorates, nitromethane, fertilizers and hydrogen peroxide. Access to chemical precursors, garage chemistry procedures and equipment will be evaluated.

The objectives of EXPEDIA in this topic are:

• Collection and experimental evaluation of recipes leading to home-made acids from commercial sources and synthesis of known explosives from these acids

• Synthesis of homemade perchlorates/chlorates and measuring the explosive power of compositions using these ingredients

• Evaluation if pure nitromethane (NM) can be easily separated from commercial products and testing reactivity of compositions from this homemade NM. Studies to find additives for NM containing products to prevent possibilities for separation of NM

• Extraction of urea or ammonium nitrate from common fertilizers and measuring the explosive properties of compositions from it (e.g.: nitrate/fuel). Studies to find additives for fertilizers to prevent possibilities for extraction of urea or ammonium nitrate

• Thermal characterisation and study of decomposition kinetics, mechanism, and stability of selected hydrogen peroxide (HP) based explosive formulations. Explosive characteristics will be also studied

4. PROJECT CONSORTIUM MEMBERS

The project consortium members are:

- TOTALFORSVARETS FORSKNINGSINSTITUT / FOI (Sweden) - Coordinator of the project
- NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK / TNO (Netherlands)
- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES / CEA (France)
- FRAUNHOFER-INSTITUTE / ICT (Germany)
- YARA INTERNATIONAL ASA / YARA (Norway)
- ANGUS CHEMIE GMBH / DOW (Germany)
- ESBIT-COMPAGNIE GMBH / ESBIT (Germany)
- KCEM AB / KCEM (Sweden)
- NATIONAL BUREAU OF INVESTIGATION / NBI (Finland)
- WOJSKOWY INSTYTUT HIGIENY I EPIDEMIOLOGII / WIHIE (Poland)
- BRODARSKI INSTITUT DOO* / BI (Croatia)
- BUNDESKRIMINALAMT / BKA (Germany)

The research performed in this project has received funding from the European Union's Seventh Framework Program for research, technological development and demonstration under Grant Agreement No.604987.

METAL ORGANIC FRAMEWORKS AS SELECTIVE PRECONCENTRATOR MATERIAL FOR GAS-PHASE SENSING

Max Rieger[1], Moritz Heil[2], Jürgen Hürttlen[2], Frank Schnürer[2], Gudrun Bunte[2] and Horst Krause[2]

[1] max.rieger@ict.fraunhofer.de, +49 721 / 4640-348
Fraunhofer Institute for Chemical Technology ICT, Joseph-von-Fraunhoferstraße 7, D-76327 Pfinztal, Germany

[2] *Fraunhofer Institute for Chemical Technology ICT, Joseph-von-Fraunhoferstraße 7, D-76327 Pfinztal, Germany*

Extended abstract

Introduction

The trace-amount detection in ambient air, e.g. low volatile organic compounds (LVOCs), explosives and its precursors, faces two major challenges: low concentrations of the target compounds in the sub-ppm region (sensitivity), as well as the increasing number of interfering substances in these low-concentration regions (selectivity). Combined these factors hamper the effectiveness and reliability of common analytical methods. Both problems demand a pre-filter or selective preconcentrator featuring a strongly substance dependent adsorption-, diffusion- and desorption-behavior e.g. a raised Henry-constant as compared to interfering substances.[1-3]

Metal Organic Frameworks (MOFs) are a promising new substance class of highly porous materials with extraordinary properties. They are comprised of metal- or metal-cluster-cations ("nodes") and multidentate anionic or neutral organic molecules ("linkers").[4] The resulting 3-dimensional crystalline network exhibits pores and their interconnecting channels with spatial and chemical uniformity. Pore sizes reaching from 4 Å to almost 98 Å have been reported.[5] By varying the linkers, nodes and their molar ratios, it is possible to synthesize a tremendous amount of distinct structures. Recently published computational investigations suggest their usage as sensing- or preconcentrator-material for small molecules such as xylenes, phosphonates and trinitrotoluene (TNT).[6-9]

Materials and Methods

We modified a gas-chromatographic system in order to investigate MOFs for their sorption characteristics in terms of different analytes in a carrier-gas (see Figure 1). For this purpose, vapors of different analytes are injected into a stream of carrier-gas.[10] This gas stream is then conducted through a packed bed of MOF material. Analyte concentrations in the gas stream are online-monitored using a thermionic-ionization (TID) and photoionization detector (PID) at the exhaust of the packed bed, while the gas flow is measured using a mass-flow meter.
Via analyzing the retention- or breakthrough-times of different analytes with respect to different adsorbents it is possible to state analyte-sorbent affinities and gas-sorbent partition coefficients.[10]
For preliminary testing runs, widely known MOFs such as HKUST-1 (Cu_3BTC_2), MIL-53(Al) or ZIF-8 are examined. They are compared to state-of-the-art adsorbents like Tenax TA ® or molecular sieves.
Packed beds were realized using GC liners (ca. 1/4" outer diameter) while attaching 1/32" connecting capillaries to their ends using Swagelok reducing unions. The powder packing was fixed using MARKES ® regular quartz wool. Initially, different bed geometries were

explored by using GC liners with varying inner diameters. 1mm inner diameter became the column geometry of choice as an elongate shape is feasible with less adsorbent mass.

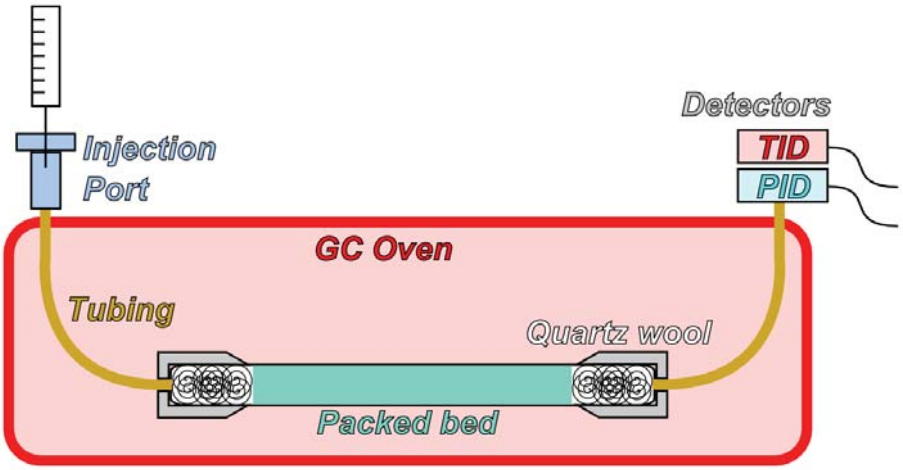


Figure 1: Schematic showing experimental Set-up. Vapor samples of analytes are injected via a syringe, conducted through a packed bed of sorbent via a carrier gas flow. Its concentration is continuously monitored after passing the bed.

Having $D_{0,9}$ particle-sizes of about 20-30 µm, the pressure drop along a packed bed of MOFs can be estimated using the Kozeny–Carman equations. In case of a 5 mm long and 1 mm thick packed bed this pressure drop is around 2 bars. The carrier gas flow vs. gauge pressure exhibits almost linear behavior from 0,5 to 3,0 bar, resulting in flows of 5 to almost 50 ml/min.(Figure 1).

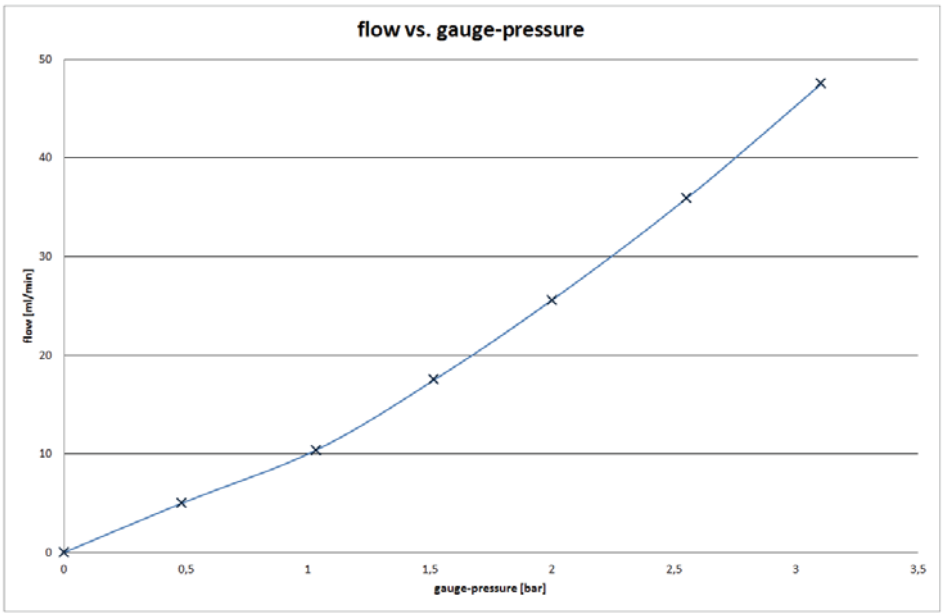


Figure 2: capillary flow (ml/min) vs. gauge pressure (bar) of a 10 mg packed bed with MOF adsorbent. Column diameter 1 mm, column length ca. 5 mm.

Breakthrough volumes were calculated by analyzing retention times of injected analyte-peaks. The amount of gaseous volume injected does not influence the temporal location of the corresponding peaks in the chromatogram. The retention time of the peaks at 10% or 100% value was considered and multiplied by the gas flow of the carrier gas. Breakthrough-volumes show high reproducibility and standard errors of below 1% in a MOF-analyte series during multiple injections.

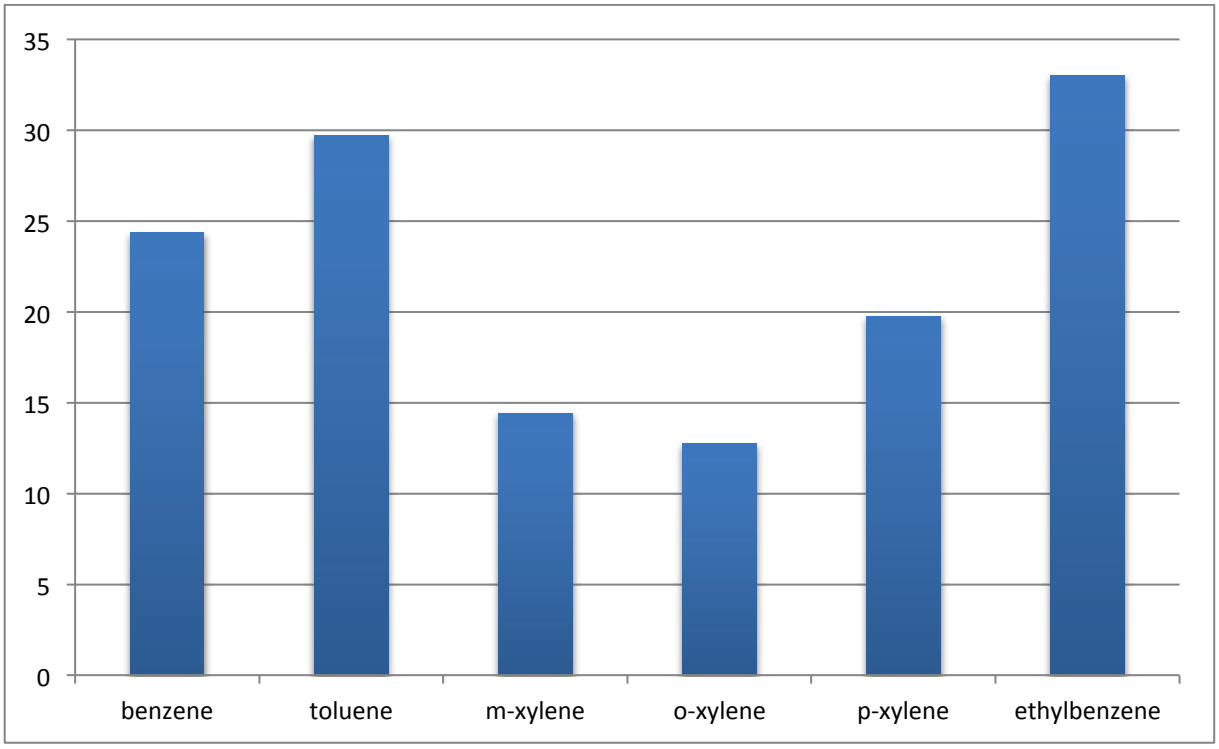


Table 1: Breakthrough volumes (in liters of nitrogen per g of sorbent) of different BTEX components on metal-organic framework HKUST-1 (Cu_3BTC_2).

Breakthrough volumes directly correspond to gas/sorbent partition coefficients and directly reflect the interaction of guest molecules (analytes) and sorbent material. This is mainly influenced by:

- Spatial descriptors
  - Pore system of sorbent
  - Molecular shape of guest molecule
- Polar interactions of sorbent and guest molecule
- Van der Waals interactions

Using multivariate data analysis like principal component analysis (PCA), it is possible to correlate sorbent and analyte descriptors to a range of experimentally derived breakthrough volumes.

Breakthrough volumes may be used in order to determine the safe sample volume and the purge-time as well as desorption temperature and desorption gas volume when using the sorbent material for purge-and-trap or thermal desorption analysis.

Acknowledgement

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No 604311
www.sensindoor.eu

References

[1] Senesac, L.; Thundat, T. G. (2008). *Nanosensors for trace explosive detection.* Materials Today, 11, 28–36.

[2] Ni, Z.; Jerrell, J. P.; Cadwallader, K. R.; Masel, R. I. (2007). *Metal-organic frameworks as adsorbents for trapping and preconcentration of organic phosphonates.* Analytical Chemistry, 79, 1290–1293.

[3] Xiong, R.; Odbadrakh, K.; Michalkova, A.; Luna, J. P.; Petrova, T.; Keffer, D. J.; Nicholson, D. M.; Fuentes-Cabrera, M. a.; Lewis, J. P.; Leszczynski, J. (2010). *Evaluation of functionalized isoreticular metal organic frameworks (IRMOFs) as smart nanoporous preconcentrators of RDX. Sensors and Actuators B: Chemical, 148, 459–468.*

[4] Rowsell, J. L. C.; Yaghi, O. M. (2004). *Metal–organic frameworks: a new class of porous materials.* Microporous and Mesoporous Materials, 73, 3–14.

[5] Deng, H.; Grunder, S.; Cordova, K. E.; Valente, C.; Furukawa, H.; Hmadeh, M.; Gandara, F.; Whalley, a. C.; Liu, Z.; Asahina, S.; Kazumori, H.; O'Keeffe, M.; Terasaki, O.; Stoddart, J. F.; Yaghi, O. M. (2012). *Large-Pore Apertures in a Series of Metal-Organic Frameworks.* Science, 336, 1018–1023.

[6] Greathouse, J. A.; Ockwig, N. W.; Criscenti, L. J.; Guilinger, T. R.; Pohl, P.; Allendorf, M. D. (2010). *Computational screening of metal-organic frameworks for large-molecule chemical sensing.* Physical Chemistry Chemical Physics : PCCP, 12, 12621–12629.

[7] Asha, K. S., Bhattacharyya, K. & Mandal, S. *Discriminative detection of nitro aromatic explosives by a luminescent metal–organic framework.* J. Mater. Chem. C 2, 10073–10081 (2014).

[8] Lan, A. et al. *A luminescent microporous metal-organic framework for the fast and reversible detection of high explosives.* Angew. Chem. Int. Ed. Engl. 48, 2334–8 (2009).

[9] Yamagiwa, H. et al. *Detection of Volatile Organic Compounds by Weight-Detectable Sensors coated with Metal-Organic Frameworks.* Sci. Rep. 4, 6247 (2014).

[10] Schneider, M., & Goss, K. U. (2009). *Systematic investigation of the sorption properties of tenax TA, chromosorb 106, porapak n, and carbopak f*. Analytical Chemistry, 81(8), 3017–3021. doi:10.1021/ac802686p

FACE- AND APPEARANCE-BASED PERSON IDENTIFICATION FOR FORENSIC ANALYSIS OF SURVEILLANCE VIDEOS

Christian Herrmann[1], Jürgen Metzler[2], Dieter Willersinn[3] and Jürgen Beyerer[4]

[1]*christian.herrmann@iosb.fraunhofer.de,* [2]*juergen.metzler@iosb.fraunhofer.de,*
[3]*dieter.willersinn@iosb.fraunhofer.de,* [4]*juergen.beyerer@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

1 INTRODUCTION

The increasing availability of surveillance cameras is both an opportunity and a challenge for forensic crime investigation. For serious crimes, video footage offers a widely accepted opportunity to identify criminals and reconstruct the events to find further offenders. Because this is often a highly manual task, automated video analysis methods are welcome to efficiently handle the growing amounts of video data. The research project MisPel (Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten) funded by the German Ministry of Education and Research addressed this field by creating and combining several automated video analysis tools into a demonstration system. A forensic analysis system is always controlled by a human operator who selects which data are to be analyzed and what kind of analysis should be performed. Here, the focus will be on one specific part: the identification of persons to find all occurrences of an offender in the video data. Assuming that an offender has caught the operator's attention, the aim is to assist the operator by finding further occurrences of this particular person in the relevant video data. This contribution focuses on the technical part of the data extraction.

2 FACE RECOGNITION

The first of the two presented methods to search for persons is via face recognition. This method usually works by extracting several features from a detected face which are consequently used for the comparison to further face representations. As result a ranked list of face matches is created showing the best match at the top. The major challenge when analyzing surveillance videos is their quality. Large capture distances lead to low resolution, movement of a person to motion blur, small data connections to severe compression artifacts and bad illumination to noise in the captured image (compare Fig. 1). By adjusting the collected features and fusing the sequential information of consecutive frames of the videos, some of the effects can be compensated [1]. Further benefits for low resolution data are possible by super-resolution including an extension to non-frontal head poses which are the usual case in surveillance data [2]. As a rule of thumb, one can say that a minimum face size of about 20-30 pixels is required to successfully perform face recognition. If the face size drops below that range, it is already the detection of the faces in the video that struggles significantly. An experiment with the widely used Viola-Jones-based face detector [3] shows that when trying to detect faces again on a lower resolution, that were detectable on a high resolution of 100 pixels, the performance degrades heavily below 20 pixels as is shown by Table 1. This indicates that the images need to have a certain quality and resolution to enable successful face recognition. Despite the possibilities to enhance low quality face recognition, there still exist a lot of surveillance data, where this approach is infeasible. Not only if faces are too small, but also if a person is only visible from behind or the face is occluded.

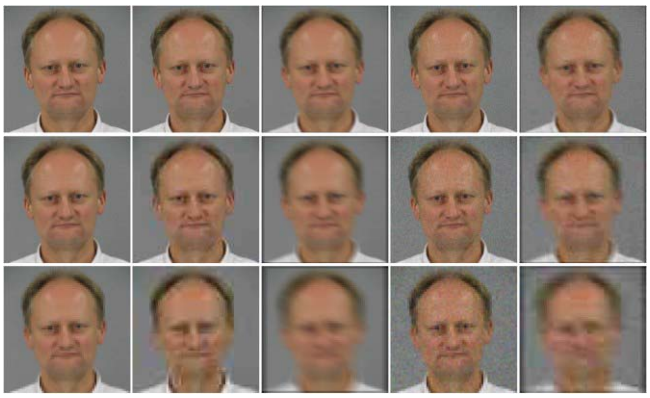


Fig. 1. Different effects that degrade the face quality. From left to right: resolution, compression artifacts, motion blur, noise and a combination of all. Severity of effect increases from top to bottom.

Table 1. Face detection rate depending on face resolution

face size (in pixels)	detection rate
100	100 %
30	98 %
25	95 %
20	90 %
15	72 %
12	35 %

3 APPEARANCE-BASED PERSON RE-IDENTIFICATION

Compared to face recognition, appearance-based person re-identification by the body relies mostly on the patterns and colors of a person's clothes. Because these cover a larger area on a person's body than a face does, this strategy is more suitable for lower image resolutions. However, a person can easily change the appearance, for example, by changing clothes, so this method might fail in crime investigations involving video data from several different days. Appearance-based person re-identification in cameras has become an intensive research topic in recent years [4]. Given an image region of a person (probe), the objective is to re-identify it in further video data (gallery). The result is a ranking of all comparisons sorted by their similarities which enables a human operator to quickly re-identify persons between video clips. The system chart in Fig. 2 shows an overview of the entire identification approach including the appearance-based person re-identification that is based on the work in [5] and [6].

Here, persons are represented by covariance descriptors that were introduced by Porikli et al. ([7]). They represent an image region by a covariance matrix of image features which is a natural way of fusing multiple features and, as shown in [7] and [8], there are several advantages of using covariance descriptors: they are invariant to mean changes, e.g. invariant to identical shifting of color values, insensitive to noise, support scale invariant features and offer an efficient fusion of multiple features. Furthermore, an evaluation of several tracking methods showed that the covariance descriptors-based tracking is the most appropriate one for crowd and riot scenarios [10] which encouraged us to use them for appearance-based re-identification ([5],[6]).

Let R_1 be an image region. First, for each pixel inside R_1 features are computed. Here, we use the x- and y-coordinates of the image pixels and the color values R, G and B. Then, d-dimensional feature vectors are constructed – one for each pixel inside R_1. Let $\{f_i\}_{i=1\dots n}$ be a set of feature vectors of the W-width and H-height rectangular R_1 and $f_i = (x, y, R(x,y), G(x,y), B(x,y))^T$ a feature vector at the pixel with the coordinates (x, y) and color values $R(x,y), G(x,y), B(x,y)$. Then the covariance, using the mean-vector μ_{R_1} of $\{f_i\}_{i=1\dots n}$, is $Cov_{R_1} = \frac{1}{WH}\sum_{i=1}^{WH}(f_i - \mu_{R_1})(f_i - \mu_{R_1})^T$. An efficient way to compute the covariance matrices for image regions of arbitrary size can be found in [10]. In order to compare two covariance descriptors, a non-Euclidean metric is required since covariance matrices do not reside in a vector space. The set of positive definite symmetric matrices can be formulated as a Riemannian manifold as described in [11]. With their proposed Riemannian metric, the (geodesic) distance between two given covariance matrices $\sum_1$ and $\sum_2$ is $d(\sum_1, \sum_2) = \sqrt{< log_{\sum_1}(\sum_2), log_{\sum_1}(\sum_2) >_{\sum_1}}$, where

$log_{\sum_1}(\sum_2) = \sum_1^{\frac{1}{2}} \log(\sum_1^{-\frac{1}{2}} \sum_2 \sum_1^{-\frac{1}{2}}) \sum_1^{\frac{1}{2}}$. The Riemannian metric is used for the person matching that is based on the output of a person tracker. As first step of the re-identification process, for each image region in the sequence of the person of interest (probe) a covariance descriptor is calculated as described above. Then, they are matched with the covariance descriptors of the gallery, resulting in a ranking of the gallery sequences.

4 COMBINATION

Based on the respective characteristics, the domain of appearance-based re-identification is the short time analysis, while face recognition helps for an analysis involving larger time periods. Combining both methods offers a broader scope of possible applications for the automated analysis.

Each method creates a ranking of the further occurrences of the person of interest. Both rankings might partially overlap in some results if both methods are able to detect the same occurrence. Due to information about timestamp and image location, they can easily be matched and fused. This prevents that the operator has to watch the same result twice.

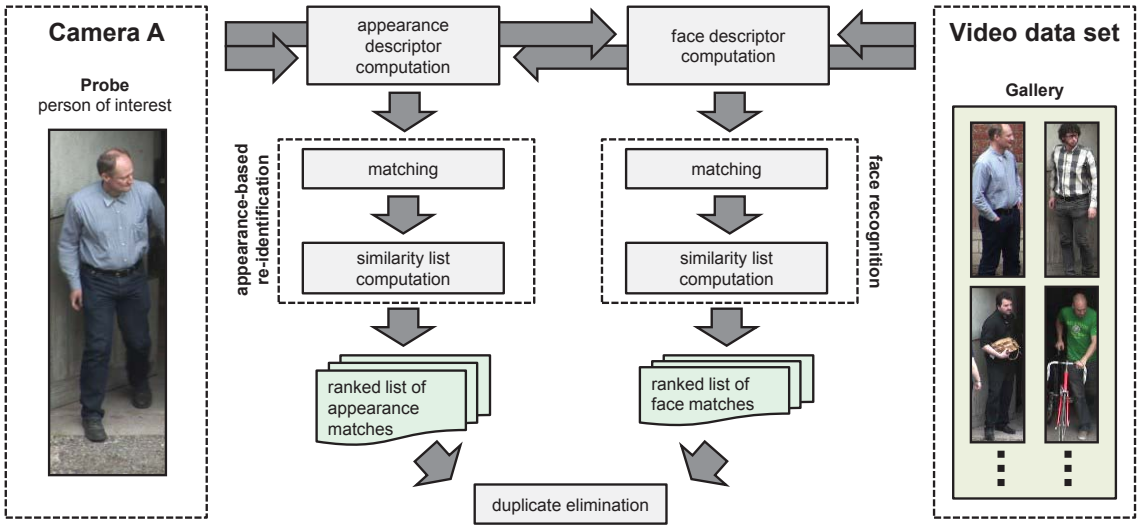


Fig. 2. System chart of the combined system.

5 RESULTS AND CONCLUSION

Applying the strategy to a set of surveillance videos leads to the results shown by Fig. 3. Using an example query person, the appearance-based and face-based searches lead to two different rankings. After finding the duplicates, one can see the benefits of the method combination. The best appearance-based match was missed by the face matching, because the person is only visible from behind. On the other hand, the face recognition finds two further occurrences that were impossible to detect for the appearance-based strategy because of different clothing and occlusion of the body. The results show that the pursued combination strategy leads to beneficial results compared to using each method alone.

ACKNOWLEDGEMENT

This work was partially supported by the German Federal Ministry of Education and Research (BMBF) as part of the MisPel program under grant no. 13N12062 and 13N12063.

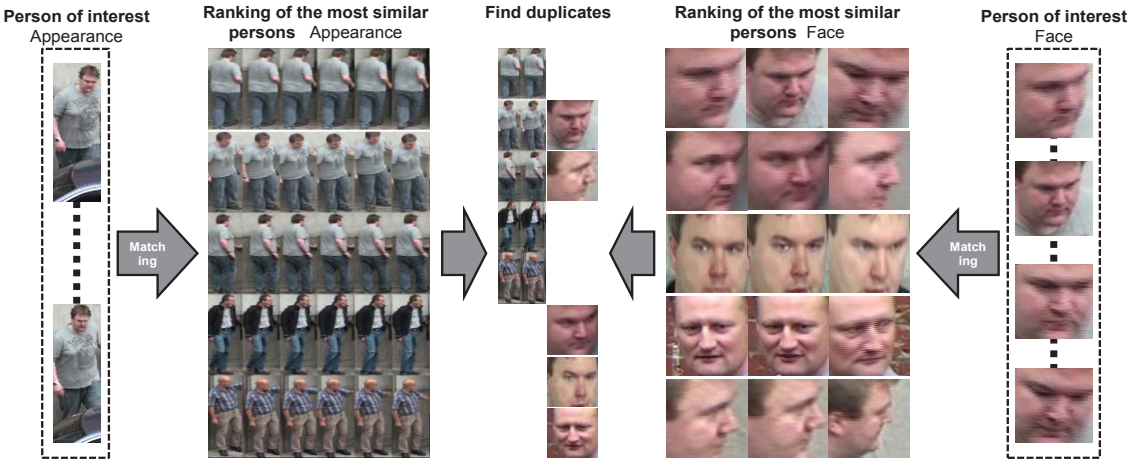


Fig. 3. Matching results including individual and fused rankings of the video sequences, each starting with the gallery sequence that is most similar to the probe.

REFERENCES

[1] Herrmann, C. (2013). *Extending a local matching face recognition approach to low-resolution video*. In Advanced Video and Signal Based Surveillance, pp.460-465.

[2] Qu, C.; Herrmann C.; Monari, E.; Schuchert, T. and Beyerer J. (2015). *3D vs. 2D: On the Importance of Registration for Hallucinating Faces under Unconstrained Poses*. In Computer and Robot Vision.

[3] Viola, P. and Jones, M. (2001). *Rapid Object Detection Using a Boosted Cascade of Simple Features*. In Computer Vision and Pattern Recognition.

[4] Bedagkar-Gala, A. and Shah, S. K. (2014). *A survey of approaches and trends in person re-identification,* ELSEVIER Journal, Image and Vision Computing, vol. 32, pp. 270-286.

[5] Metzler, J. (2012). *Appearance-based re-identification of humans in low-resolution videos using means of covariance descriptors*. In Advanced Video and Signal Based Surveillance, pp. 191-196.

[6] Metzler, J. (2012). *Two-stage appearance-based re-identification of humans in low-resolution videos*. In Workshop on Information Forensics and Security, pp. 19-24.

[7] Tuzel, O.; Porikli, F. and Meer, P. (2006). *Region covariance: A fast descriptor for detection and classification*. In European Conference on Computer Vision, vol. 2, pp. 589-600.

[8] Porikli, F.; Tuzel, O. and Meer, P. (2005). *Covariance Tracking using Model* Update Based on Means on Riemannian Manifolds. In Computer Vision and Pattern Recognition, vol. 1, pp. 728-735.

[9] Hübner, Y.; Metzler, J.; Dürr B.; Jäger U.; Willersinn D. (2008). *Assessment and optimization of methods for tracking people in riot control scenarios*. In Proc. SPIE 7114, pp. 191-196.

[10] Porikli, F. and Tuzel, O. (2006). *Fast Construction of Covariance Matrices for* Arbitrary Size Image Windows. In International Conference on Image Processing, pp. 1581-1584.

[11] Pennec, X.; Fillard, P. and Ayache, N. (2006). *A Riemannian Framework for Tensor Computing*. International Journal of Computer Vision, vol. 66, pp. 41-66.

CAIRGOLUTION – REAL TIME TRANSPARENCY OF THE AIR FREIGHT SUPPLY CHAIN

Tobias Seidler[1], Konstantinos Tigkos[2]

[1]tobias.seidler@scs.fraunhofer.de
Fraunhofer Center for Applied Research on Supply Chain Services SCS, Nordostpark 93, 90411 Nürnberg, Germany
[2]konstantinos.tigkos@iis.fraunhofer.de
Fraunhofer Development Center for X-ray Technology (EZRT), Flugplatzstraße 75, 90768 Fürth (Germany)

Abstract

Consistent monitoring of goods and load carriers is a key prerequisite for secure end-to-end transport processes. Manipulation and theft of unit load devices (ULDs) and their contents are looming risks throughout the global air cargo supply chain. To this point there are no viable and consistent solutions embedded in air freight supply chains that help to increase civil and process-related safety. The research objective of "CairGoLution" is the realization of a control system, able to recognize integrity violations on containers.

Keywords: air cargo, security, sensor technology, uld, containers, supply chain, transparency, smart objects

1. Background

Mexico, Brazil, South Africa, the United States and Russia are the countries most at risk for freight theft globally. But also in Europe Belgium, Italy, France and Germany continue to be the focal point of cargo crime. In 2012 the cargo theft incidents increased by almost a quarter [1]. Consistent monitoring of goods and load carriers is a key requirement for secure transport processes from shipper to customer. Manipulation and theft of unit load devices (ULDs) and their contents are risks that are looming throughout the global air cargo supply chain. A ULD is a palett or containers used to load freight for its air transportation. Every year, the estimated total cost of theft and of damages to ULDs is about $300 million, excluding flight delays and cancellations due to their unavailability [2]. Unsigned hazardous substances or unauthorized accesses violate the integrity of the ULD. To this point there are no viable and consistent solutions embedded in air freight supply chains that help to increase civil and process-related safety. The research objective of “CairGoLution” is the realization of a control system, able to recognize integrity violations on containers. Furthermore the system should send out alerts to administrators, if any integrity violations occur during the air cargo transport process.

2. Identifying integrity violations

The service of “CairGoLution” aims for real time identification of integrity violations. On top of that, the service supports the reduction of damages in the aftermath through the possibility to locate the potential dangerous air freight. The following cases of usage have to be achieved in order to enable the service:

- Identification of integrity violations through X-ray signature comparison [3]
- Identification of integrity violations through smart seals
- Identification of theft
- Collection and visualization of environmental and localization data

The technical system behind the service is based on the following components and their functions (Table 1).

Component	Function
Telematic-Box (TCU)	• Data collection of enviromental and localization information • Data transfer to the backend • Communication with the Smart Seal and the Unblock Beacon
Energy Harvesting	• Enlarge the time between external battery charges of the TCU by converting ambient energy into electrical energy
Smart Seal	• Monitor the lock state of an container • Data transfer to the TCU
Unblock Beacon	• Enable the transmitting activities of the TCU • Indicate areas, in which the TCU may transmit without any restrictions
Backend	• Central controlling point of the “CairGoLution” system • Identification of integrity violations • Send out security alerts
Frontend	• Provide the interface between the Backend and various (human) users
X-ray	• Provide additional control over the container integrity • X-ray data obtained at a scan site will be stored at the backend

Table 1: CairGoLution components and functions

The interaction of the components is detailed in Figure 1. The fundamental assumption in “CairGoLution” rests on the use of containers in the air freight supply chain from the shipper to the customer. That case is supported by the IATA ULD Care program [4]. This includes container transports on different means of transportation, e. g. trucks and air planes. The main risks in that supply chain are looming during the precarrige and oncarriage. Consistent container data collection and transfer of the backend decreases the risk of integrity violations. Therefore the service enables real time transparency of the air freight supply chain except for the period of time the container is located in an aircraft’s storage space. However, the risks of theft and manipulation in that timespan are expected to be negligible.

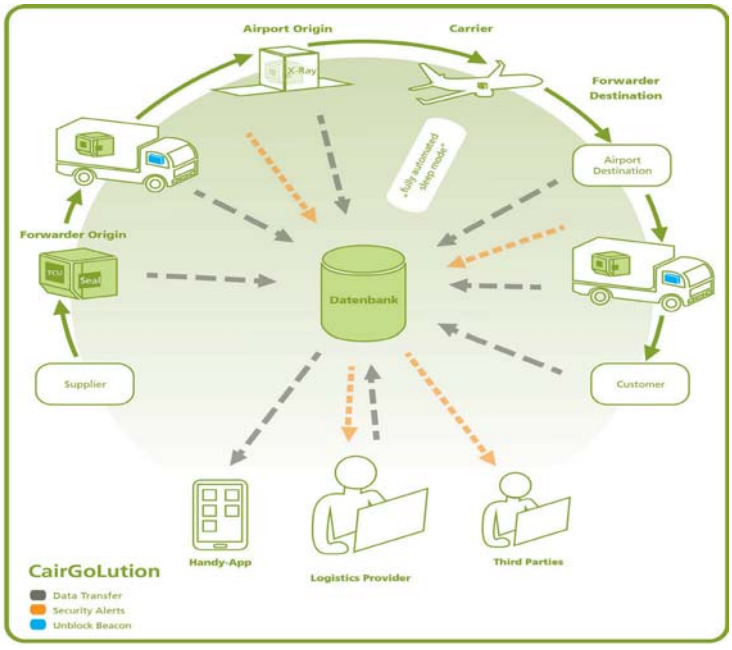


Figure 1: CairGoLution air freight supply chain

3. Challenges

The key challenge realizing the research objective comes with the restrictions connected to data transfer. While there are few to no restrictions concerning road, rail or naval transport, air cargo works different. During the main run in air cargo transport processes, the container is mostly located in the aircraft's storage space. Radio-based technology solutions have to be deactivated in that phase. Therefore, the partners in this research project are working on a reliable solution to automatically and in time turn on and off the wireless radio-based technology. As a consequence the intended solution is capable of tracking containers from the shipper to the customer. Our goal is to provide a flight suitable and approved demonstrator by the end of 2015. Currently the partners are realizing the necessary software and hardware components.

Another challenge arises with the process-related infrastructure of the current air freight supply chain. To identify possible integrity violations of the container using the X-ray signature comparison, two scans are required. To diminish the risks of threats these scans must be processed before the container will be moved into the airplane. To this date, container capable X-ray scanners are rare and not included in the standard operations process in air freight supply chains.

4. Current status

First test results for the automatic flight mode detection of the TCU show favorable results. There are two criteria for the recognition of flight mode. Position and dynamic of the container are the core features for the flight mode. The Unblock Beacon marks legitimate areas, e. g. trucks or warehouses for the data transfer of the TCU. The Unblock Beacon is based on Fraunhofer s-net® technology. The Beacon is not allowed to be carried in airplanes. Table 2 shows the relation between data transfer and container status in different scenarios. The dynamic of the container will be analyzed by means of sensor fusion in the TCU. Basically container movement is connected with the fact that the container is inside the airplane. Therefore the TCU is passive. When there is a Beacon available e. g. during the precarriage and oncarriage, data transfer is required.

Scenario	Status container	Beacon available	Data transfer
Transport (Land)	Movement	Yes	Active
Transport (Flight)	Movement	No	Passive
Warehouse	Idle	Yes	Active
Idle/Theft	Idle	No	Active
Theft	Movement	No	Passive

Table 2: Scenarios vs. data transfer

In case of container theft the data transfer will be triggered when the status switches from movement to idle.

Using smart sensors the system recognizes unauthorized accesses on the container and generates alerts for authorities and corresponding administrations. In addition to this Fraunhofer EZRT develops a method based on X-ray technology to compare container signatures. The automatic comparison is supposed to precisely identify possible manipulations of the container content during the transport. Hence alerts due to integrity violations will be forwarded. The interaction of software and hardware components is embedded in a service for logistic and express service providers and airlines.

Initial global tests with a data logger mounted on containers have shown that a precise movement pattern can be identified during takeoff and landing of airplanes. As a consequence of that and in combination with different sensors it is possible to discern if the container is inside an airplane. Additional global movement data enables the possibilities, in addition to increased safety, to achieve economic potentials using containers.

5. Outlook

The “CairGoLution” service provides a security solution for air freight containers. In reality an immense amount of freight is moved with pallets surrounded by nets. The technical solution doesn’t suit for these carriers. As a consequence of that future research projects need to develop pertinent devices.

The output of “CairGoLution” is an important step towards secure and transparent air freight supply chains. The ongoing digitalization, economical technologies and more tolerance for data transfer will create pillars to close the gap between physical and virtual environment in air freight.

This project is funded by the German Federal Ministry of Education and Science BMBF, Grant Number 13N12654.

6. Literature

[1| Freightwatch International: „2013 Global Cargo Theft Threat Assessement“. Internet: https://www.naed.org/NAEDDocs/Research/Legal%20Issues/FreightWatch%202013%20Global%20Cargo%20Theft%20Threat%20Assesment%20Full_0.pdf (last access 22.05.2015)

[2] IATA: Unit Load Devices (ULD). Internet: http://www.iata.org/whatwedo/cargo/unit-load-devices/Pages/index.aspx (last access 22.05.2015)

[3] Tigkos, K. et al. (2015): Development of X-ray signature comparison to increase air freight security. 10th Future Security Conference.

[4] IATA: ULD CARE. Internet http://www.uldcare.com/about-us.html (last access 01.06.2015)

TOWARDS A MOBILE CONTEXT-SENSITIVE FRAMEWORK FOR INTEROPERABILITY AND IMPROVED SITUATIONAL AWARENESS IN CRISIS AND EMERGENCY MANAGEMENT

Ravi Coote, Kellyn Rein, Markus Esch, Ulrich Schade

{ravi.coote, kellyn.rein, markus.esch, ulrich.schade}@fkie.fraunhofer.de

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE,
Dept. Information Technology for Command and Control,
Fraunhofer Str. 20, 53343 Wachtberg (Germany)

Abstract

We present ongoing work towards a framework that enables not only users like first responders from emergency organizations but also citizens who, for example, reside in a natural disaster prone area to send geo-localized key information from the crisis site such as the number of injured persons, the type of injury or the degree of urgency. This geo-referenced information will be fed into the crisis network and will thus be instantaneously distributed to all relevant levels of the crisis management automatically, utilizing a data distribution mechanism for crisis management messages.

Keywords: Situational Awareness, Crisis Management, Wearable Computing, Self-Organized Citizens, Crisis Management Language CML

1 INTRODUCTION

As a result of various natural disasters such as severe earthquakes, hurricanes and floods in the last few years, several technical hurdles to efficient multi-agency crisis and emergency management have been identified. These hurdles include barriers to coordination such as a lack of shared situational awareness, but also barriers to communication such as disruptions in communication systems, asynchronous (delayed) communication, and lack of common understanding. Further developments in information technology are expected to overcome these technical barriers.[1]

The rest of the paper is structured as follows. In Section 2 we review several studies and research projects that have been conducted in the last few years tackling one or more of the technical obstacles. In Section 3 we identify several key capabilities and then sketch a framework that realizes our vision of mobile multi-agency collaboration and self-organization of civilians for crisis management in the field. In Section 4 we briefly state our conclusions and outline possible future work.

2 REVIEW OF FRAMEWORKS AND PLATFORMS FOR CRISIS MANAGEMENT NEAR THE FIELD

Several works and studies related to crisis management and emergency management have been published, mostly focusing on a subset of technical aspects. In the work of Bahnik [1], the focus was on using an unmanned aerial vehicle (UAV) carrying an on-board camera system as central mobile data collector. Such an UAV provides a real-

[1] In some cases technical requirements differ and one needs to distinguish between crisis and emergency management. The terms “emergency” and “crisis” may apply to the same situation or occurrence. The words, however, denote a different combination of time-span and extent which may depend upon who and what is at stake in a specific situation or occurrence. From a time perspective, an emergency is a serious situation or occurrence that happens unexpectedly and demands immediate action, because of a potential threat to life or the environment. With respect to time, the terms crisis and disaster denote a significantly longer period of time than an emergency (see [6]).

time aerial video stream of the area of operation to all rescue agencies involved in the operation. The system was successfully tested in a firefighting scenario.

The overall objective of the Lage Project [2] was to create a collective understanding of events, structures and processes used on the higher levels of operation. To this end, a common operational picture was generated utilizing a linked information pool and integrated processes, taking into account all connected systems, by implementing a holistic concept for organizational, semantic and technical interoperability. The scenario was an assault at an inner-city big event (*World Cup* and *Love Parade*) with mass casualties with an involvement of a German main railway station.

3 PROPOSED FRAMEWORK AND CAPABILITIES

Here we envision a software-based framework especially for the purpose of crisis and emergency management that incorporates communication with commercial off-the-shelf (COTS) devices such as modern mobile computers and Android-based smart phones. As such, it enables interoperability across multiple agencies including, for example, search and rescue organizations, technical assistance agencies and fire brigades. In addition to first responders from emergency organizations citizens who may, for example, live in a natural disaster prone area are able to provide authorities with valuable geo-localized key information from the crisis site such as the number of injured persons, types of injuries incurred, and degree of seriousness of those injuries. Using the proposed framework, geo-referenced information will be added into the crisis network and will instantaneously and automatically distributed to all relevant levels of the crisis management via crisis management messages.

Depending on the severity of the crisis – for example, “high” in the case of a major earthquake – local communication infrastructures are likely to fail. In such a scenario, the framework also supports a novel level of self-organization of citizens who are located in the area affected by the natural disaster by creating temporary smart phone-based networks that are independent of the local communication infrastructure. Thus, self-organized citizens will be able to build a “citizen volunteer group”. During the course of the crisis, multiple volunteer groups can be built and can become a valuable resource for efficiently managing and conquering the crisis.

In order to realize our vision of crisis and emergency management on the level of mobile/wearable computing, we have identified several (already existing) technologies which we describe below and which will be integrated into the framework.

Outdoor and Indoor Localization

The exact position of all players (e.g., firefighters) and also volunteer citizens should be available at all levels of operation. Generally satellite-based localization technologies (such as Global Positioning System, GPS) are widely used for the determination of positions. However, the reliability of this technique can vary heavily with respect to update rates, precision and signal sensitivity. Even more seriously, in indoor environments GPS-based localization fails, unless extremely high-sensitivity GPS sensors are used. Nevertheless, in the case of short term emergency management, such as firefighting or rescue operations, the ability to locate emergency workers, through one means or another, within buildings is crucial [3]. One option for the localization of forces within buildings is inertial navigation which is an autonomous/GPS-independent technique. Although the development of smaller and less expensive inertial sensors has made major progress in recent years, the hurdle to effective use in applications such as we propose is *sensor drift*. Sensor drift is a cumulative measurement error which occurs over time and affects the accuracy of the location; the longer the measurement time, the greater the offset from true position. One possible solution to tackle this hurdle is the use of advanced filtering methods

proposed by Haid [4]. Another approach for autonomous/GPS-independent indoor localization is the integration of RFID-sensors into the localization strategy proposed by Guerrieri et al. [5].

Interoperability and the C2 Lexical Grammar (C2LG)

In cases of severe crises, a multi-agency scenario is formed, which may consist of medical services, technical assistance agencies, police, fire fighters and others. Multi-agency collaboration is causing interoperability problems, ranging from syntactical interoperability, to semantical interoperability to conceptional interoperability [6].

The C2 Lexical Grammar (C2LG) is a formal grammar that is used to generate expressions of military communication (orders, requests and reports). The resulting formal language, that is, the set of all expressions that can be generated using the C2LG, is called Battle Management Language (BML). Since C2LG is a formal grammar, the expressions generated can be analysed (parsed and interpreted) by computer systems. Originally, C2LG used a lexicon of terms well defined in the field of military operations to generate standardized, unambiguous, human- and machine-readable expressions to express the “5 Ws” (Who, What, Where, When, and Why) [7] [8]. The formal language can be used to exchange expressions between the C2 systems of allied forces or to exchange messages between C2 systems and simulation systems in order to use the simulation systems for decision support or training, as well as for enhanced situation awareness [9]. During the past few years, work has begun to expand C2LG into the domain of crisis and emergency management, as the interagency C2 incompatibility exists not only between coalition partners in the military domain but also between emergency services in crisis and emergency management.

Message Distribution Service

Automatic distribution of information is crucial for situational awareness on all levels of operation. The publish/subscribe model for sending and receiving data, reports, and directives among connected systems is an approach to keep information up to date for all operational partners and their systems. A publish/subscribe service enables information to be automatically distributed within the network even when the network provisionally integrates volunteer citizens. As a result, it makes the information known by the volunteer citizens available to the operation centres of fire brigades and police forces as well as to other official crisis managers.

The publish/subscribe model is well-established in distributed systems. According to this pattern, messages and information are categorized by topic or content. Information consumers (subscribers) are able to subscribe to categories of interest. Information providers (publishers) send messages not directly to receivers, messages are published to categories, instead. A middleware (e.g., Data Distribution Service [10]) makes sure that all subscribers of a category receive the information provided. Depending on the middleware the information distribution can either be done by a centralized broker or in a fully decentralized way. The publish/subscribe pattern fits well for situational awareness applications since it ensures that operational nodes receive all relevant information.

4 CONCLUSIONS AND POSSIBLE FUTURE WORK

We have identified several key capabilities to bring our vision of a framework for mobile and interoperable multi-agency communication and self-organization of citizens in crisis and emergency management into being.

Next, we will develop a base system and deploy it on several wearable devices which together will constitute an outdoor test lab for field exercises and studies involving fire brigades, police, and technical assistance agencies. We believe these practical studies

will reveal valuable insights in the future challenges of applying information technology in the scope of crisis and emergency management.

5 REFERENCES

[1] P. Bahnik, M. Gerke, I. Masar, F. Jelenciak and V. Beyer, "Collaborative data-exchange architecture for crisis management using an UAV as a mobile sensor platform", *International Conference on Process Control (PC),* 2013.

[2] Federal Ministry of Education and Research, "LAGE: Integration vorhandener Informationssysteme für ein gemeinsames Krisenmanagement", 28 January 2014. [Online]. Available: http://www.bmbf.de/de/22397.php.

[3] M. Puyol, M. Frassl and P. Robertson, "Collaborative Mapping for Pedestrian Navigation in Security Applications", *Future Security - Communications in Computer and Information Science,* 2012.

[4] M. Haid, Verbesserung der referenzlosen inertialen Objektverfolgung zur Low-cost Indoor-Navigation durch Anwendung der Kalman-Filterung, Fraunhofer TEG, 2005.

[5] J. Guerrieri, M. H. Francis, P. Wilson, T. Kos and L. Miller, "RFID-assisted indoor localization and communication for first responders", *First European Conference on Antennas and Propagation, EuCAP,* 2006.

[6] P. M. Gustavsson, J. J. Garcia, J. Wemmerg and M. Norstedt-Larsson, "Expanding the Management Language Smorgasbord-Towards Standardization of Crisis Management Language (CML)".

[7] U. Schade, M. R. Hieb , M. Frey and K. Rein, "Command and Control Lexical Grammar (C2LG) Specification", Fraunhofer Instituite FKIE, Wachtberg, Germany, 2012.

[8] U. Schade und M. R. Hieb, „Battle Management Language“, in *Verteilte Führungsinformationssysteme*, Heidelberg, Springer, 2009, pp. 235-245.

[9] U. Schade und K. Rein, „Battle Management Language as a “Lingua Franca” for situation awareness“, *IEEE CogSIMA,* March 2012.

[10] Object Management Group, *Data Distribution Service (DDS),* 2015.

[11] United Nations, "UNISDR Terminology on Disaster Risk Reduction - International Strategy for Disaster Reduction ISDR", [Online]. Available: http://unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf. [Accessed 5 July 2015].

AN ADAPTIVE DATA-CENTRIC INFRASTRUCTURE FOR BIG DATA TYPE COLLECTION APPLICATIONS IN RESTRICTED ENVIRONMENTS

Sandro Leuchter

sandro.leuchter@ieee.org
Rhine-Waal University of Applied Sciences, Faculty of Communication and Environment, Friedrich-Heinrich-Allee 25, 47475 Kamp-Lintfort (Germany)

Abstract

Communication in distributed security related human-machine systems is often implemented with the help of communication middleware. We present extensions to the OMG Data Distribution Service standard for near real time communication middleware that help to cope with varying bandwidth, reachability, and prioritization in mobile Internet connections. A cloud computing example related to data acquisition for big data processing is presented as case study for this infrastructure.

Keywords: middleware, infrastructure, cloud computing, Internet-of-Things

1 INTRODUCTION

This contribution describes an adaptive infrastructure that is currently developed in the context of smart city applications as a prototype on laboratory scale. It adapts its quality of service parameterization, features of the network, and the runtime platform according to current demands of operational load, integrity, and functional capability of the system. This makes it possible to collect and process large amounts of data in a distributed way.

Many security-related applications need to collect data from sensors and need to send commands to actuators. They can be also seen as distributed human-machine systems with an inherent need to enable communication between their elements. In the context of Internet-of-things projects different middleware systems are discussed to enable sensor/actuator/decision element integration (e.g. in disaster and risk management [1]). They have been developed with the enhancement of the integration capability in mind. But often security related applications also need to work in restricted environments. Such restrictions arise from the dynamic and critical nature of those systems (e.g. demand for prioritization, real time behaviour, and guaranteed bandwidth for absolutely necessary messages).

2 ARCHITECTURE

Indirect communication based on the Publish-Subscribe pattern is a widely applied middleware paradigm. It has been found to be effective for near real time communication in many technical environments. Decoupling of producer and consumer nodes using this pattern makes it possible that communication partners do not need to know about each other except for a common data model (see fig. 1). In particular no function call interface co-ordination is necessary and late binding at run time is also possible. Thus service oriented architectures with pluggable nodes from different vendors can be easily built with this middleware approach. This system integration technique is also known as “data-centric”.

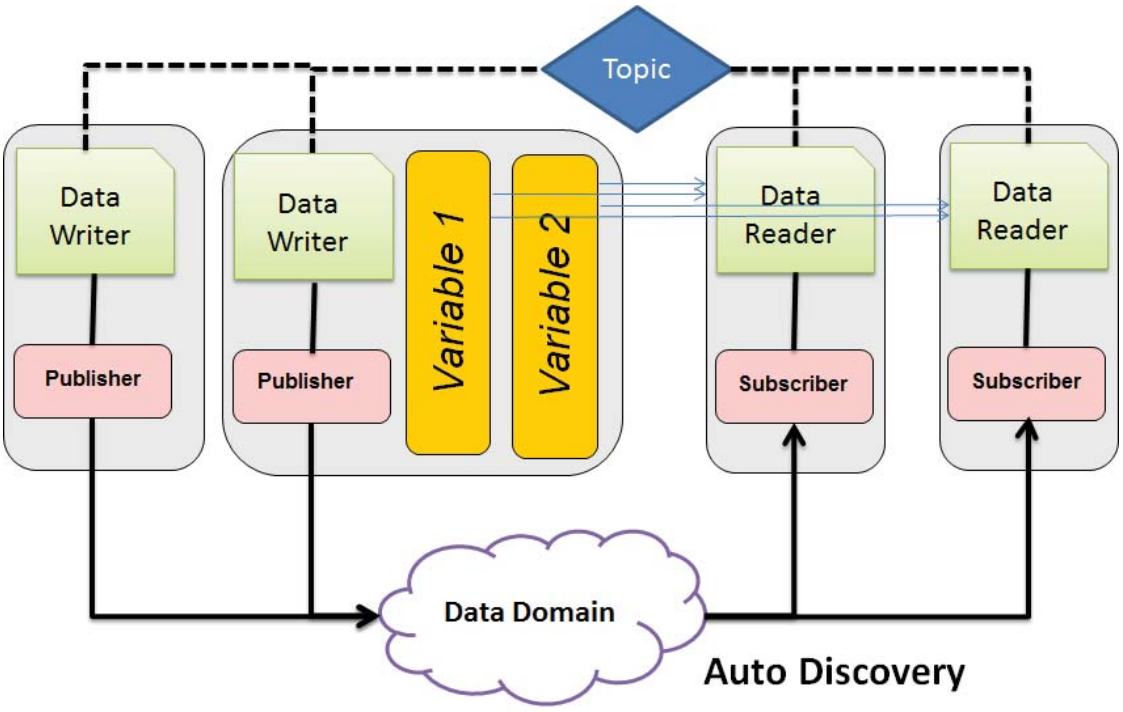


Figure 1: Publish/Subscribe architectural approach as in OMG DDS

Data-centricity also means that information elements can be subsequently derived by autonomously working nodes as in multi-agent systems for distributed problem solving. Our middleware is an intelligent infrastructure using this mechanism.

We add consumers called **sensors** to the architecture that observe the operation regarding different aspects. Each sensor publishes its observations as aggregated items that are understood by components in other parts of the network.

Controller components then use these observations to change middleware parameters in order to adjust the system to the current operational load. One example is to turn off resource consuming add-ons such as logging or persistence. In extreme cases reliable messaging could also be downgraded to best effort in order to save bandwidth. The deployment of the runtime platform and the (SDN enabled) network topology may also be adapted.

On top of the Connext middleware suite by RTI this framework is being developed. It consists of components that work as producers and consumers of the common data model and at the same time adapt the quality of service parameterization of the Connext infrastructure and the network structure through OpenFlow.

3 EVALUATION

The development of the framework takes place in the context of a smart city application. The framework is used to connect public transport vehicles to a distributed OpenStack installation at two sites of the university (see fig. 2) in order to collect sensor data for different big data type applications. The network is using a cellular connection for mobile Internet (depending on availability using GPRS, EDGE, UMTS, or LTE). Thus bandwidth varies greatly.

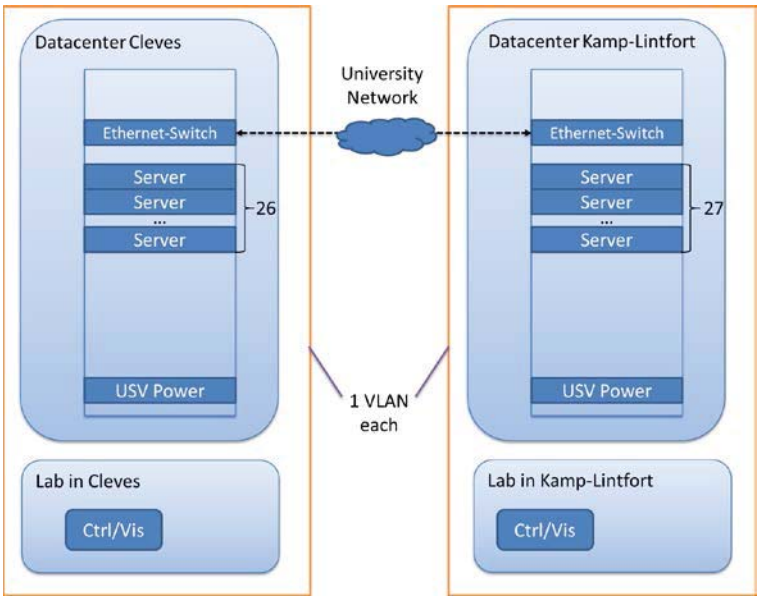


Figure 2: Cloud computing environment infrastructure for experimental development

The infrastructure framework runs on top of OpenStack (see fig. 3). The state of the middleware, the network and the cloud infrastructure is visualized on a control/visualization host ("Ctrl/Vis" in fig. 2) in a laboratory.

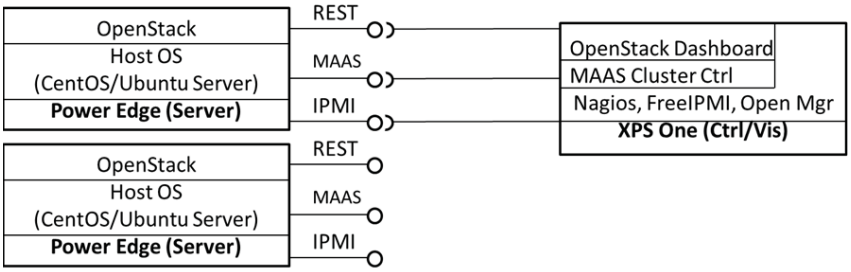


Figure 3: Communication interfaces in the cloud computing infrastructure

4 CURRENT STATUS AND OUTLOOK

In the moment the main focus is on specification and implementation of the infrastructure framework. The smart city application is analysed for requirements and demands towards the infrastructure.

In later phases the smart city application itself will be the main point. Currently the plan is to implement big data like processing in an Apache Spark environment.

Complex event processing components could be introduced in the future in order to detect application specific patterns as a way to identify operational states.

REFERENCES

[1] Uslaender, T. (2015). The trend towards the Internet of Things: what does it help in Disaster and Risk Management? *GRF Davos Planet@Risk, Vol 3, No 1*, pp.140-145.

DEVELOPMENT OF X-RAY SIGNATURE COMPARISON TO INCREASE AIR FREIGHT SECURITY

Konstantinos Tigkos[1], Ulf Haßler[1], Frank Sukowski[1], Tobias Seidler[2] and Theobald Fuchs[1]

[1] *konstantinos.tigkos@iis.fraunhofer.de, ulf.hassler@iis.fraunhofer.de, frank.sukowski@iis.fraunhofer.de, theobald.fuchs@iis.fraunhofer.de*
Fraunhofer Development Center for X-ray Technology (EZRT), Flugplatzstraße 75, 90768 Fürth (Germany)

[2] *tobias.seidler@scs.fraunhofer.de*
Fraunhofer Center for Applied Research on Supply Chain Services SCS, Nordostpark 93, 90411 Nürnberg (Germany)

Abstract

Air freight plays an increasingly important role in global trade activities. World-wide air freight supply chains are affected by the risk that the Unit Load Devices (ULDs), typically containing the air cargo, are stolen or manipulated, which results in violation of the integrity of the shipment. Fraunhofer EZRT is working on the integration of X-ray scanning of ULDs in the air cargo supply chain by developing a method to reliably detect integrity violations of the shipment, involving as little human interaction as possible. The proposed approach is to define a “signature” which is derived from the X-ray scan and abstractly characterizes the contents of the ULD. By scanning the ULD at critical points within the supply chain, such signatures may be generated and compared with each other in order to automatically determine whether any changes in the contents of the ULD have occurred.

Keywords: air freight, cargo security, supply chain, ULD, x-ray imaging, image processing, image analysis, CairGoLution

1 INTRODUCTION

1.1 Project Background

Up to date, there is no viable and consistent solution that increases the civil and processual safety related to air freight transport. The goal of the research project CairGoLution is to provide a control system that identifies integrity violations during the air cargo process and triggers alarms if such a violation occurs. Core components of this system are an intelligent telematic unit, able to collect data about the location and status of the ULD and state of the art X-ray image analysis, able to automatically determine integrity violations within the supply chain.

1.2 New Concepts in X-ray Air Freight Inspection

Within CairGoLution, a new automatic cargo inspection concept is defined. According to the project goals, it is important to determine whether the contents of a shipment transported in an ULD container have been altered during transport, which would constitute an integrity violation of the shipment. In order to facilitate such an inspection by means of X-ray scanning, the ULD has to be scanned at different stages of the supply chain between which the risk of an integrity violation is high [1]. To avoid hindering the process throughput, this inspection should be as efficient and automated as possible.

2 MATERIALS AND METHODS

Reliably detecting an alteration of a shipment's contents is a challenging task. An integrity violation would occur when an item is added or removed from the shipment without authorization [1]. Detecting such a change may seem trivial in the ideal case where the only change in the X-ray scan occurs due to an item being added or removed. However, a number of practical factors complicate this detection. Due to differences in X-ray scanner components and design, two scans of the same shipment acquired with devices from different manufacturers may substantially differ in various properties. What is more, items are displaced in position and orientation during transport which results in differences between two X-ray scans of the same content, which do not correspond to an integrity violation. The proposed method is intended to achieve high manufacturer independency and invariance to content displacements.

2.1 Simulation Study

As the scanning of complete ULD containers has not yet been widely adopted in air freight supply chains, the possibility to produce large quantities of real test scans to serve as test data for the algorithm development was not given. Therefore, test data was generated by means of X-ray computer simulation. In order to produce realistic X-ray scans of a ULD container loaded with cargo and test objects, the analytic X-ray simulation software Scorpius X-Lab® developed by Fraunhofer EZRT was used. The test scans were generated by simulating the HI-SCAN 180180 scanner developed by Smiths Detection which is suited for scanning airfreight containers. The ULD container and enclosed test cargo, shown in Fig. 1, was simulated by using three dimensional CAD models and geometric primitives. Integrity violation was simulated by removing one item from the cargo. Random displacements and changes in the orientation of the container contents in various magnitudes have been simulated in different combinations.

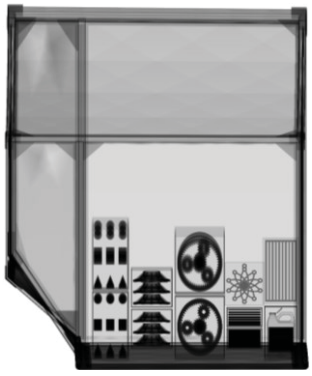


Fig. 1: Simulated ULD container with load.

2.2 X-ray Signature

The existing cargo inspection algorithms are fairly limited in number and functionality, primarily serving as support for the human operator. To the author's knowledge, methods for automatically detecting alterations in the cargo contents by means of X-ray image analysis are not yet established in a production environment. The proposed approach is to define a "signature" which is derived from the X-ray scan and abstractly characterizes the contents of the ULD. By scanning the ULD at different stages of the supply chain, such signatures may be generated and compared to each other in order to determine whether any changes which correspond to integrity violations have occurred. In this way, only the X-ray signature data, which is significantly smaller than the entire image, has to be stored and transmitted. Fig. 2 roughly depicts the image processing and analysis chain for deriving and comparing X-ray signatures.

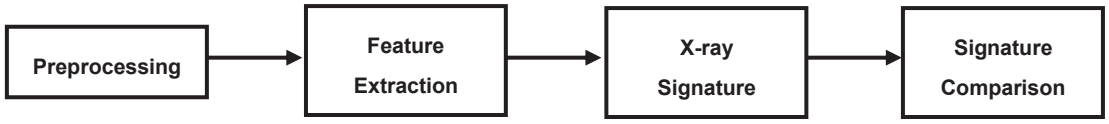


Fig. 2: Image processing and analysis chain for the generation and comparison of X-ray signatures.

A preprocessing step is necessary in order to normalize some basic image properties and reduce the noise so that manufacturer independence can be achieved and the X-ray signature stability is improved. Afterwards, the components that compose the X-ray signature are calculated. These components are image properties, or "features", which are calculated either globally on the entire image, or locally on image segments. The image segments are defined by a uniform partitioning of the image according to a rectangular grid. In the future, a method to segment the image into meaningful regions [2] may be employed if necessary to improve results. The combination of global and local features which express different image properties and achieve a certain degree of invariance to rotations and translations is necessary in order to achieve a reliable X-ray signature comparison. Table 1 categorizes different features which currently compose the X-ray signature or will be employed in the future in different classes.

After the X-ray signatures have been derived, they are compared in order to determine whether an integrity violation has occurred. Respective features are compared one by one according to a normalized distance metric. Currently the default metric is the Normalized Mean Square Error (NMSE) but other metrics may be employed if necessary. Finally, a score which reflects the total deviation between two X-ray signatures is computed. The contribution of each individual feature distance to the final score is determined by a weight which is defined after the experimental evaluation of the feature performance. If a feature performs reliably and is insensitive to content displacements it will contribute more to the final score. Consequently, the comparison between X-ray signatures which are sufficiently invariant to content displacements should yield a high final score when an integrity violation occurs and a low score when no violation occurred, regardless of the cargo displacements. Given a clear threshold between these two cases, a reliable decision can be made whether an integrity violation actually occurred.

Feature class	Typical features
Intensity	Intensity, Contrast, Gradient Features
Statistical	Histogram, Central Moments, Entropy [3], Correlation [3]
Geometrical	Extent, Eccentricity, Weighted Volume/Cut/Curvature [4]
Textural	Gabor Filter Banks [5], Tamura Features [6]
Spectral	Fourier Based Features
Material	Material Discrimination (in case of dual energy scans)

Table 1: Categorization and typical examples of features which currently compose the X-ray signature or will be employed in the future.

3 EXPERIMENTAL RESULTS

Experiments have been carried out on simulated data which was generated as described in section 2.1. At the moment the X-ray signature consists of 18 features

belonging to the intensity and statistical classes, as described in Table 1 and the X-ray signature amounts to approximately 550 KB. Table 2 shows the final signature deviation in percent for some test cases where the deviation was highest. There is a minimum threshold interval of 0.64% between cases with integrity violation and cases without, making it possible to detect potential violations without false alarms. However, the existing simulated test data is fairly simple and the threshold interval of 0.64% is fairly low which could lead to false alarms in more complicated scenarios.

Maximum Displacement	Signature Distance (%)	
	w. violation	w/o violation
Translation 5 cm	1.77	0.24
Translation 15 cm	1.53	0.89
Rotation 2°	2.23	0.33
Rotation 10°	2.35	0.61
Rot. 10° + Transl. 15 cm	2.29	0.81

Table 2: Signature distances for various test cases.

4 CONCLUSIONS AND FUTURE WORK

The first experimental results show the potential of the proposed method to detect integrity violations while at the same time displaying a fair degree of invariance to content displacement. Further experiments with more complicated test data may show the need to employ more features in order to improve the robustness of the X-ray signature. Additionally, real X-ray scans of a loaded ULD container will be carried out by Fraunhofer EZRT and detection limits will be concretely assessed. The proposed method may be applied to supply chains other than air freight with minimal adaptation.

This project is funded by the German Federal Ministry of Education and Science BMBF, Grant Number 13N12654.

REFERENCES

[1] Seidler, T. et al. (2015). *Cairgolution – Real time transparency of the air freight supply chain*. 10th Future Security Conference.

[2] Zhang, H., Fritts J., Goldman S. (2008). *Image segmentation evaluation: A survey of unsupervised methods*. Computer Vision and Image Understanding 110, pp. 260-280.

[3] Haralick, R.M. (1979). *Statistical and Structural Approaches to Texture*. Proceedings of the IEEE 67, pp. 786-804.

[4] Caselles, V., Kimmel, R., Sapiro, G., Sbert, C. (1997). *Minimal surfaces based object segmentation*. IEEE Transactions on PAMI 19(4), pp394–398.

[5] Kumar, A., Pang, G. (2002). *Defect detection in textured materials using gabor filters*. IEEE Transactions on Industry Applications 38 (2), pp. 425–440.

[6] Tamura, H. et al. (1978). *Textural Features Corresponding to Visual Perception*. IEEE Transactions on Systems, Man, and Cybernetcs, Vol. SMC-8, No. 6, pp. 460–472.

PRIVACY AWARE MODULAR VIDEO ANALYTICS

Martin Boyer[1] and Stephan Veigl[2]

[1] martin.boyer@ait.ac.at [2] stephan.veigl@ait.ac.at
AIT Austrian Institute of Technology GmbH, Safety & Security Department,
Donau-City-Straße 1, 1220 Vienna (Austria)

1 INTRODUCTION

Enforcing the right for privacy, justice and freedom of citizens in the development and operation of surveillance infrastructure is a challenging and complex task. The incorporation of modular video analytics in such surveillance systems raises the level of complexity even further. Nevertheless modular video analytics offer essential advantages when flexibility and/or scalability (performance) are required. In our work we show how a set of simple and individually harmless algorithmic modules can be exploited to extract sensitive personal information from surveillance video footage. Trying to solve this challenge exclusively by technical means (i.e. for individual components) is not reasonable and will not lead to a successful solution: The functionality of a combination of primitive algorithms can exceed the abilities of the sum of the parts by magnitudes. Moreover, it is not sufficient to strictly follow the privacy-by-design paradigm for each individual component in order to guarantee privacy preservation for the whole system. Therefore the solution has to be applied on a higher, comprehensive level considering the whole lifecycle of such systems, starting with the planning and design phase. Furthermore it also needs to assist the development and has to ensure that privacy aspects are reviewed continuously while the surveillance system is in operation or maintenance. We will present a solution being applied to a Connected Vision application (details in section 3) as an example of a distributed, modular computer vision analysis system.

2 GOALS

The goal of the PARIS (PrivAcy pReserving Infrastructure for Surveillance) project [1] is to define and demonstrate a methodological approach for the development and operation of privacy aware surveillance infrastructure. This novel approach shall ensure the right of citizens for privacy, justice and freedom and take into account the evolving nature of such rights (e.g. aspects that are acceptable today might not be acceptable in the future), the social and anthropological nature of such rights (e.g. perception of these rights varies) and constantly changing technology. The methodological approach will be based on:

1. A theoretical framework concept – further called SALT (Socio-ethicAl / Legal / Technological) – to balance surveillance and privacy/data protection and fully integrate the concept of accountability.
2. An associated process for the development and operation of surveillance systems which considers privacy (i.e. privacy-by-design) and accountability (i.e. accountability-by-design) from the beginning.

To demonstrate and evaluate the application of the SALT framework concept and its associated process, the PARIS project members defined a specific video surveillance scenario [2]. In this scenario law enforcement agencies (LEAs) search in video surveillance archives of an infrastructure provider during a forensic investigation (see Fig. 1).

The subject of this scenario is a fictitious crime being committed in the premises of an infrastructure provider (e.g. railway operator) that does not interfere with the security or safety of the infrastructure provider (i.e. it does not affect safe operation of their systems). The crime is within the responsibility of the law enforcement agencies. Investigation is done by the LEAs in cooperation with the infrastructure provider.

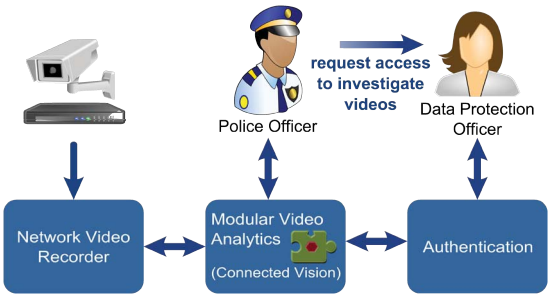


Fig. 1 PARIS video surveillance scenario

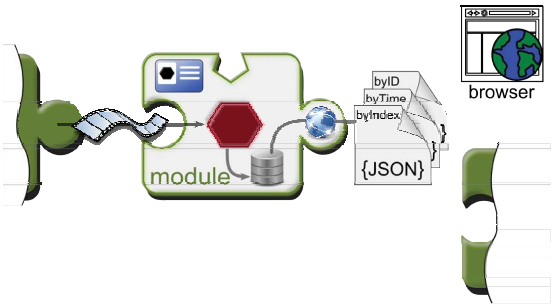


Fig. 2 Modules in Connected Vision

3 PRIVACY IMPACTS OF MODULAR VIDEO ANALYTICS

To provide a better understanding of the special privacy concerns in modular video analytics, a short description of Connected Vision [3] as an exemplary representative of modular video analytics follows. With Connected Vision complex analytic tasks are solved in a modular way. It is a platform independent concept based on modules that follow the microservices architectural style [4], where each module acts as an autonomous web service, implementing a homogenous/unified interface, is self-descriptive and has the capability of decentralized processing and storage of its results. Connected Vision modules, in particular, follow a self-descriptive approach, which is provided through a human- and machine-readable interface. In this way, each Connected Vision module offers information about its inputs, outputs and configuration (settings) to the outside world, called self-description. Respective modules provide instruments for importing, analysis, filtering, evaluation and interpretation of all kinds of data – including video – via their embedded core tasks (see Fig. 2). Through combination and concatenation of different modules (module chains) a portfolio of various forensic investigation templates can be built. Applied on digital forensic data, such investigation templates help solving a specific case.

In general, modular systems are able to do more than each module individually, as this is mainly what they were designed for. Because of the modularity, it is possible to use the system in a way algorithm developers, application designers or system operators never thought of, or by far intended to do. Specifically in the field of video surveillance it is of great benefit to truly make use of the advance in flexibility and scalability that modular systems can offer. However, seen from the viewpoint of privacy and data protection this can quickly turn to the opposite if designers and operators do not pay enough attention to privacy matters. Operating video surveillance in combination with different analytics might be harmless from a privacy point of view and legal for each individual algorithm, whereas performing video analytics using a combination of the same algorithms can be considered questionable. The fact that these privacy-related problems are not obvious, neither for system developers, operators nor for owners of the system, is even more severe.

To demonstrate the problem Fig. 3 shows a simple example where ethical information is extracted with harmless modules/algorithms. For instance, suppose that railway infrastructure providers analyze surveillance video footage using motion detection in combination with a tripwire mechanism. These algorithms are being employed when monitoring material/tool depots or between platforms and railway tracks to prevent

people or obstacles from being run over by a train. Also color or brightness detection gets used for automatic illumination of facilities. Digital zoom and image cropping can be considered being basic features of every image processing system. Let us assume that all above mentioned modules are available within the system and there are justified reasons for their purpose. The example in Fig. 3 puts some of those algorithms in a modified arrangement and in a new context – obtaining soft-biometric information out of surveillance video footage.

Even this oversimplified example shows that there are no restrictions after a system is in operation. Trying to prevent the module chain in our example by means of technical restrictions does not make sense, as the same module combination on a different camera could be used for other, justified purposes. Thus some kind of continuous privacy review or audit has to be carried out during the whole lifetime of the system.

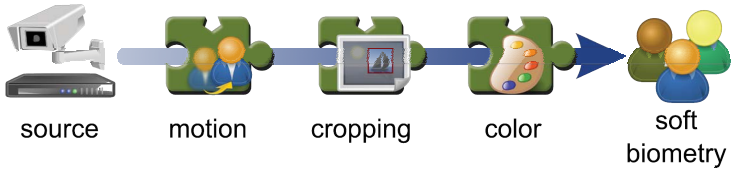


Fig. 3 Example of privacy critical modular video analytics

4 OVERCOME PRIVACY ISSUES WITH SALT FRAMEWORKS

SALT frameworks are interdisciplinary in scope. They encompass a wide variety of perspectives and put experts from several disciplines together (i.e. lawyers, ethicists, engineers). A SALT framework can be defined as a collection of concepts and overarching principles concerning privacy in public spaces that are used as a reference for the design and operation of surveillance systems. Therefore SALT frameworks address surveillance system owners and designers by taking into account socio-ethical, legal and technological dimensions [5].

In the scenario mentioned at the beginning of this contribution, law enforcement agencies search video surveillance archives of an infrastructure provider in a forensic investigation (see Fig. 1) by making use of modular video analytics as explained earlier in section 3. The chosen scenario aims at establishing a trusted relationship between involved persons/roles, authorizing them and permitting secure access to video data stored in a video archive, taking care of the special privacy needs of modular video analytics (secured inter-module communication, authentication, accountability,…) and eventually logging all query and data transmission actions on both sides. In order to guarantee privacy preservation for the system as a whole – including modular video analytics, all these aspects need to be taken into account. They act as SALT references that encompass a SALT framework for a surveillance system that incorporates modular video analytics. SALT references are included in a repository which contains all the relevant knowledge for a specific SALT framework. This knowledge can be processed and applied to specific surveillance systems -- e.g. by system designers.

The SALT framework concept offers a questionnaire-based approach [5] to cope with the dimensions mentioned above. Specifically this means that a user of the SALT framework encounters relevant aspects represented as SALT references by answering a questionnaire. The aims of the questionnaire-based approach are the following: (a) Identify key legal stakes, ethical values and/or technical issues at stake. (b) Accompany development along the steps. (c) Foster a reflection upon socio-ethical, legal and technical dimensions.

5 CONCLUSION

This contribution presented a methodological approach for the design, development and operation of surveillance infrastructure which enforces the right of citizens for privacy, justice and freedom based on the SALT theoretical framework concept. To evaluate this concept, we demonstrated its application in a specific video surveillance scenario that employs modular video analytics.

Connected Vision, as an exemplary representative of modular video analytics, was presented to provide a better understanding of the special privacy concerns in this area. As this contribution has pointed out, there are good reasons to use a modular approach in video analytics, but due to the gained flexibility and power of modular systems, additional privacy concerns arise. In our example it is apparent that the problem does not necessarily lie in any single algorithm (module), as each of them is used by a real and justifiable demand of the end-user. We have shown that a specific combination of modules might be eligible for one task, but lead to privacy concerns if applied to another set of videos.

To overcome these privacy issues, SALT frameworks provide references that support system designers as well as operators in considering the socio-ethical, legal and technical dimensions of the surveillance system. SALT references evolve over time with the knowledge of users who become SALT experts. Following the associated questionnaire-based process encourages them to take other fields of expertise or other domains than the one they are accustomed to into considerations.

ACKNOWLEDGEMENTS

This work was partially funded by the European Commission through the project Privacy Preserving Infrastructure for Surveillance (PARIS) [1] with contract FP7-SEC-2012-1-312504.

REFERENCES

[1] *PrivAcy pReserving Infrastructure for Surveillance – PARIS*. Available online at: http://www.paris-project.org/. The PARIS Project (FP7-SEC-2012-1, Grant agreement No:312504), Public Website. Retrieved on June 3, 2015.

[2] Ma, Zhendong et al. (2014). *D5.1 - Video Surveillance Lifecycle Management Use Case Description*. The PARIS Project (FP7-SEC-2012-1, Grant agreement No:312504), Public Deliverable.

[3] Boyer, Martin and Veigl, Stephan (2014). *A Distributed System for Secure, Modular Computer Vision*. Future Security 2014 9th Future Security Security Research Conference, Berlin, September 16-18, 2014, Proceedings.

[4] Lewis, James and Fowler, Martin (2014). *Microservices*. Available online at: http://martinfowler.com/articles/microservices.html. Retrieved on June 3, 2015.

[5] Thoreau, François and Gayrel, Claire and Jaime, Francisco (2014). *D2.3 - Guidelines for Use Cases for SALT Frameworks*. The PARIS Project (FP7-SEC-2012-1, Grant agreement No:312504), Public Deliverable.

CHARACTERISTICS AND SURVIVAL OF BACILLUS CEREUS IN SPICES

Hendrik Frentzel, Mai Dinh Thanh, Gladys Krause, Juliane Bräunig, Bernd Appel, Anneluise Mader

spiced@bfr.bund.de
Federal Institute for Risk Assessment, Department Biological Safety, Max-Dohrn-Straße 8-10, 10589 Germany

Abstract

The EU market is one of the largest world markets for culinary spices. Spices are generally used as 1% or less of the total weight of foods. Nevertheless, these minor components can pose benefits and risks to the consumer. Despite their low water activity spices can be contaminated with several microorganisms.

One objective of the EU-project SPICED ("Securing the spices and herbs commodity chains in Europe against deliberate, accidental or natural biological and chemical contamination", www.spiced.eu) is to improve the knowledge on biological hazards and diagnostic methods in the heterogeneous matrices of spices. Therefore, we analysed five spices on the presence of *Bacillus (B.) cereus* and characterised detected isolates. All samples were below the DGHM warning value of 10^4 cfu/g. The characterised isolates were able to produce toxins that can lead to gastro-intestinal symptoms. Additionally, pepper and paprika samples were artificially contaminated with *B. cereus* spores to examine survival capacities. The number of spores remained almost unchanged within three month.

Keywords: foodborne pathogen, spores, food safety, tenacity, low moisture

1 INTRODUCTION

Protecting the national and European critical infrastructure of food production is an important responsibility shared by governmental organizations and private industry. As spices are minor food components that can be widely spread and may contain microbial contaminants, including pathogenic and toxigenic ones, we have taken a closer look on this specific food chain. According to the European Food Safety Authority *Bacillus* (*B.*) spp. and dried spices and herbs are on the top four of the ranking groups of food/pathogen combinations in food of non-animal origin [1]. Of special interest is the *B. cereus* group consisting of the species *B. mycoides*, *B. pseudomycoides*, *B. weihenstephanensis*, *B. thuringiensis*, *B. anthracis* and *B. cereus* [2]. The aim of our study was to characterise and investigate the survival of *B. cereus*, a toxin producing sporeformer, in spices.

2 MATERIAL AND METHODS

The occurrence of *B. cereus* group members in allspice, paprika, pepper, cinnamon and nutmeg powder was investigated in accordance with ISO 7932. Presumptive *B. cereus* isolates were characterised in terms of species and present toxin genes via multiplex real-time PCR [3-5] and toxin producing capabilities for Nhe and Hbl using the GLISA Duopath® Cereus Enterotoxins (Gold Labelled Immuno Sorbent Assay, Merck, Darmstadt, Germany). Additionally, the survival of spores of a *B. cereus* strain (DSMZ 4312) was investigated in paprika and pepper samples (powder) at common storage temperatures of 24 ± 1 °C (air dried spore suspension on 0.5 g sand + 4.5 g spice or sand (positive control), final concentration 10^6 cfu/g, 3 parallels). The water activity (a_w) in the test matrices was determined using the a_w-measurement device AquaLab Lite (Decagon Devices, Pullman, USA).

3 RESULTS AND DISCUSSION

Natural contaminations with presumptive *B. cereus* could only be detected in allspice (limit of detection: 200 cfu/g). With a *B. cereus* burden of 1.6 x 10^3 cfu/g the allspice samples were below the warning value of the German Society for Hygiene and Microbiology being 10^4 cfu/g [6]. All of the isolates were identified as *B. cereus* sensu stricto and carried the nheA toxin gene. Eleven of twelve isolates carried the toxin gene hblD, while cytK1 was present in nine of the isolates (Table 1). These toxin genes are related to the production of enterotoxins causing diarrhoea (Nhe: non-haemolytic enterotoxin, Hbl: haemolysin BL, CytK1: cytotoxin K1) [4]. The ces gene (cereulide synthetase), being responsible for the emetic toxin (cereulide) production, was found in one isolate in combination with nheA and cytK1. The actual toxin production capabilities, determined only for Nhe and Hbl, reflected the genetic configuration. Thus, all isolates carrying the nhe and/or hbl genes were also able to produce the respective toxin.

Species	Present toxin genes	Toxin production capabilities		Number of isolates
		Nhe	Hbl	
B. cereus	nheA, ces, cytK1	x	-	1
B. cereus	nheA, hblD	x	x	3
B. cereus	nheA, hblD, cytK1	x	x	8

Table 1: Taxonomic affiliation, present toxin genes (nheA, hblD, cytK1, ces) and toxin production capabilities (only Hbl and Nhe were analysed) of 12 presumptive *B. cereus* isolates from allspice.

First results of the survival study indicate that *B. cereus* spores remain viable for pro-longed periods in the investigated matrices (Figure 2). Within three month the spore concentration decreased from 6.3 x 10^5 to 6.1 x 10^5 cfu/g in pepper, from 8.4 x 10^5 to 2.6 x 10^5 cfu/g in paprika and from 1.1 x 10^6 to 7.7 x 10^5 cfu/g in sand (control). The water activity in the negative control samples averaged 0.35 (± 0.05).

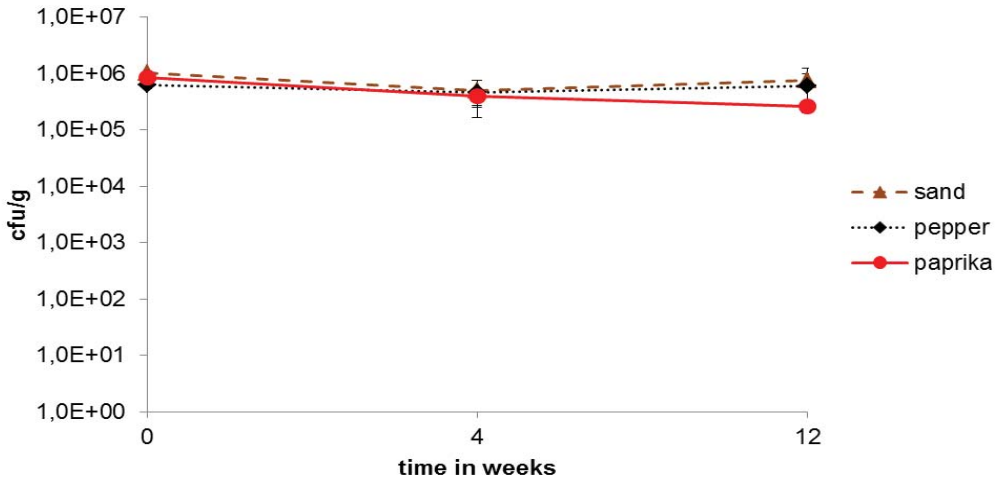


Figure 2: Survival of *B. cereus* DSMZ 4312 in paprika powder, pepper powder and sand (control); mean values ± standard deviation of three parallels.

4 CONCLUSION

Spices can contain natural microbial contaminations including toxin producing *B. cereus*, while especially *Bacillus* spp. spores are known to have high survival capacities for example in food and the environment. Therefore, this food/pathogen combination is of importance regarding risk oriented food safety measures and the general aim to protect the critical infrastructure (and especially the consumers' health).

5 AMENDMENT

This research was executed in the framework of the EU-project SPICED (Grant Agreement: 312631) with the financial support from the 7th Framework Programme of the European Union. This publication reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein. For further information on the project please see www.spiced.eu.

REFERENCES

[1] EFSA Panel on Biological Hazards (BIOHAZ) Panel (2013). *Scientific Opinion on the risk posed by pathogens in food of non-animal origin. Part 1* (outbreak data analysis and risk ranking of food/pathogen combinations). EFSA Journal. 11(1):3025: p. 138.

[2] Blackburn, C.D. and P.J. McClure (2009). *Pathogenic Bacillus species*. Foodborne Pathogens: Hazards, Risk Analysis and Control, Second Edition, (176): p. 844-888.

[3] Oliwa-Stasiak, K., O. Kolaj-Robin, and C.C. Adley (2011). *Development of Real-Time PCR Assays for Detection and Quantification of Bacillus cereus Group Species: Differentiation of B. weihenstephanensis and Rhizoid B. pseudomycoides Isolates from Milk.* Applied and Environmental Microbiology, 77(1): p. 80-88.

[4] Wehrle, E., et al. (2010). *Detection of Bacillus cereus with enteropathogenic potential by multiplex real-time PCR based on SYBR green I.* Molecular and Cellular Probes, 24(3): p. 124-130.

[5] Wielinga, P.R., et al. (2011). *A multiplex real-time PCR for identifying and differentiating B. anthracis virulent types.* International Journal of Food Microbiology, 145: p. S137-S144.

[6] Deutsche Gesellschaft für Hygiene und Mikrobiologie (DGHM) (2011). *Veröffentlichte mikrobiologische Richt- und Warnwerte zur Beurteilung von Lebensmitteln.*

TOWARDS PRIVACY IN MONITORED SHARED ENVIRONMENTS

Kaibin Bao[1], Thomas Bräuchle[2], and Hartmut Schmeck[1]

{bao, braeuchle, schmeck}@kit.edu
Karlsruhe Institute of Technology (KIT),
[1] Institute of Applied Informatics and Formal Description Methods (AIFB),
Kaiserstr. 89, 76133 Karlsruhe (Germany)
[2] Center for Applied Legal Studies (ZAR),
Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe (Germany)

Keywords: privacy, visualization, monitoring, energy data, access rights, surveillance.

1 PRIVACY THREATS OF VISUALIZING ENERGY AND SENSOR DATA

For the purpose of energy efficiency, automation and consumption visualization, an increasing number of sensors like power meters, temperature sensors, and CO_2 sensors, are installed in private households. Such a monitored household, the Energy Smart Home Lab (ESHL)[1], was built on the campus of KIT for research on energy management systems [1]. In addition to ambient temperature and thermal flows, the lab records energy consumption data of 37 electric metering points to monitor each appliance. The recorded data can be visualized in the form of graphs as shown in Fig. 1. Monitored environments like the ESHL are usually shared by multiple residents whose actions and behavior are reflected in the data. By recording and analyzing the data, inferences about the actions and habits of residents of a household can be drawn. Molina-Markham [2] and Lisovich [3], for instance, demonstrated that sensitive information like occupancy, appliance usage, sleeping cycles, and cooking habits, can be inferred using only energy consumption data. On the one hand, revealing such sensitive information to the involved residents is very important to improve energy awareness. On the other hand, sensitive information about other residents can be abused for continuous surveillance.

This work presents a novel concept to defining access rights within an energy monitoring and visualization system capable of actively mitigating the ability for mutual surveillance.

1.1 Scenario and assumptions

In order to define access rights on energy and sensor data, we assume the following use case and application context:

1. An energy and sensor monitoring and visualization system is installed in an environment which is shared by multiple residents. The monitoring aims at finding out how the energy efficiency of their building can be improved, maybe by replacing or repairing appliances, or pointing out wasteful behavior of the residents or of the other activities or processes in the building.
2. The monitoring system consists of multiple sensors, a database to store the energy and sensor data as time series and a visualization frontend, which generates different views on the stored data.
3. The residents are most importantly interested in their own energy footprint as well as long-term trends in total energy consumption of the whole household and of each individual appliance.

[1] http://www.izeus.kit.edu/english/57.php

1.2 Threats and attacks on the privacy of individual residents

Access control in current energy monitoring and visualization systems like Discovery[2], Plotwatt[3], or the web interface of the ESHL, is usually defined on the granularity of whole time series only. In most cases, access rights are granted by the all-or-nothing-principle on complete households or buildings. Such systems allow all residents to observe the complete recorded data in highest resolution. This data can be used to easily determine the time periods when appliances are being used, effectively seeing the actions happening inside the whole household or building. Therefore, all residents having access to the visualization system can abuse the system for surveillance. This kind of continuous surveillance is ubiquitous within a building and is hardly noticeable by human senses. Hence, it poses a serious threat to privacy. As the visualization providers offer access over the internet, even remote surveillance is possible. Thereby, the intensity of surveillance may exceed the level of socially acceptable observation (e.g. an employer supervising his/her employee, parents keeping an eye on their children) and is comparable to constant video surveillance.

From a legal perspective, a legitimation by law or the consent of the affected person to be monitored is required, due to the right to informational self-determination. In order to determine the own behavior free of any suppression, people have the right to decide who should receive which personal information. If people are not able to estimate the knowledge of her/his social environment or potential communication partners concerning their personal detail with sufficient certainty, they can be substantially inhibited in their freedom to make plans or decisions out of their own determination and live according to those plans and decisions. [4]

2 REFINING ACCESS CONTROL TO IMPROVE PRIVACY

The key idea to prevent surveillance is to link the right to access energy and sensor data with the presence of a particular resident. Data recorded during a specific time can only be accessed by residents whose presence was detected at that time.

The access rights can be further refined by dividing the monitored environment into independent domains. Domains can be defined by spatial or ownership properties, for example, if each children should not be able to see what is going on in the other children's room. Domains are also needed to separate office rooms.

We argue that access to highly aggregated data does not violate the privacy of individuals. Also, highly aggregated data provides important information like long-term trends in total energy consumption. The visualization system should display highly aggregated data as a fallback whenever fine-grained data is not accessible.

2.1 Requirements

The proposed privacy enhancement can be summed up to the following requirements:

1. Access to fine-grained energy and sensor data of a domain is only granted if presence of the resident was recorded during the time of recording.
2. The monitoring system thus has to keep track of the presence of particular residents in each domain.
3. Access to energy and sensor data for all residents is only granted as aggregated values. This is needed to calculate long-term trends in energy consumption. The residents should be able to configure the minimal width of the aggregation window. We propose an aggregation window of one day to be a good balance between privacy and usefulness of the aggregated values.

[2] https://discovergy.com

[3] https://plotwatt.com

2.2 Access Control Rules

In this section, we define the $read$ operations of the database which enforces our access control mechanism. There are two $read$ operations, one to access fine-grained data and one for aggregated data. The $read$ operations should meet all requirements above. Timestamps are assumed to be POSIX times with resolution in seconds.

- Let U be the set of users / residents of the monitored environment.
- Let D be the set domains within the environment.
- Let T be the set of all sensor value time series.
- Each time series is a function mapping from a timestamp (as integer value) to a sensor value whereby there might be missing data ($\perp$):
$$t_i \in T : \mathbb{Z} \to \mathbb{R} \cup \{\perp\}.$$
- The function $d : T \to D$ associates each time series to a specific domain.
- Special time series record the presence of a particular resident in a domain:
$$t_{(u,d)} : \mathbb{Z} \to \{\top, \perp\} \text{ with } u \in U \text{ and } d \in D.$$

Now the basic $read$ operation on a time series t_i at time τ can be defined based upon whether the presence of the user u currently requesting the data was detected in the domain t_i is associated with:

$$read(t_i, \tau) = \begin{cases} t_i(\tau), & t_{(u,\ d(t_i))}(\tau) = \top \\ \perp, & otherwise \end{cases}.$$

With this definition, in the time periods where no presence in a specific domain was recorded, all the time series of this domain are displayed as if the data is missing. Thus, requirement 1 is met. Fig. 1 shows the effect of this definition under the assumption that the user was detected absent during the time periods marked purple.

Time series aggregation needs to be defined in order to express requirement 3:

- Let O be the set of aggregation operations (e.g. sum, max, or $mean$).
- $A \subseteq T \times \mathbb{Z} \times O$ is the set of aggregated time series which is used by the visualization system. Each aggregated time series applies a specific operator $o_j \in O$ to a time series in $t_i \in T$ with a time window size $r \in \mathbb{Z}$.
- Let $r_{disclose}$ be the minimal window where all time series data can be accessed by all valid users U (e.g. all residents). In Requirement 3b, we propose $r_{disclose} = 86400$ seconds which is one day.

The read operation on aggregated time series (t_i, r, o_j) at time τ is then defined as:

$$read\big((t_i, r, o_j), \tau\big) = \begin{cases} \perp & , \quad \tau \bmod r \neq 0 \\ o_j(\{t_i(l) : l \in [\tau, \tau + r - 1]\}) & , \quad \begin{array}{c} r \bmod r_{disclose} = 0 \ \vee \\ \exists k \in [\tau, \tau + r - 1] : t_{(u,d(t_i))}(k) = \top \end{array} \\ \perp & , \quad otherwise \end{cases}$$

The first case forces that the requested time τ is aligned to the window r to avoid leaking information about the high resolution time series. In the second case, the aggregated data is provided either if the requested window is a multiple of the minimal window ($r \bmod r_{disclose} = 0$) or the user was present in the domain $d(t_i)$ at least one second. The constraint that r needs to be a multiple of $r_{disclose}$ is also due to avoid possible information leakage.

With these two definitions of the $read$ operation, both requirement 1 and 3 can be met. The bottom row of Fig. 1 illustrates that the average daily consumption of each device can be accessed independently of presence. Requirement 2 is a technical issue which is discussed in the next section.

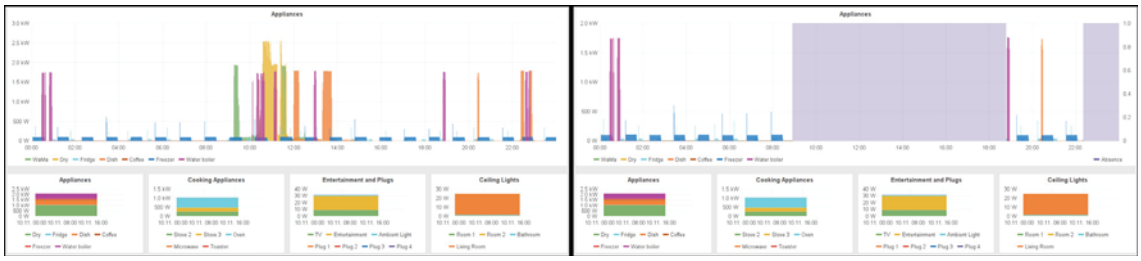


Figure 1 : Visualization systems (left frame) display sensitive information about actions inside the household. In the right frame, data recorded during the absence (marked purple) of the resident is hidden from him.

2.3 Tracking and displaying the presence

The proposed system can only be implemented when a person's presence can be detected in each domain. A practical technology is based on Bluetooth LE beacons which can be attached to key chains. These beacons constantly transmit an identification for the owner. Passive Bluetooth receivers located in each domain can use this identification to assume presence of a particular person which is then stored in the database.

There is no guarantee that the residents will always carry around their identification token. In fact, someone could maliciously hide his token in a domain to gain access to the recorded data later. This threat can be dealt with by displaying all detected presences on a display. Each person can then check whether they are really alone.

3 CONCLUSION AND FUTURE WORK

We presented a concept of a monitoring and visualization system for energy and sensor data, which implements mechanisms to avoid surveillance of fellow residents or co-workers. However a secure implementation requires further investigations. For example, the proposed Bluetooth beacons used for identification can easily be spoofed. We need a non-replayable identification mechanism using cryptographic primitives. Another question is how to handle situations where a resident is accountable for consuming energy, but is not present at the time of the actual consumption. This occurs when appliances are programmed to run later or when appliances are controlled remotely.

3.1 Acknowledgement

This interdisciplinary work was funded in the KASTEL project by the German Federal Ministry of Education and Research (BMBF 01BY1172).

REFERENCES

[1] Allerding, F., Mauser, I., & Schmeck, H. (2014). *Customizable Energy Management in Smart Buildings Using Evolutionary Algorithms*. In A. I. Esparcia-Alcázar & A. M. Mora (Eds.), Applications of Evolutionary Computation (pp. 153–164). Springer Berlin Heidelberg.

[2] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). *Private memoirs of a smart meter*. In Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building (pp. 61–66). ACM.

[3] Lisovich, M. A., Mulligan, D. K., & Wicker, S. B. (2010). *Inferring Personal Information from Demand-Response Systems*. IEEE Security Privacy, 8(1), 11–20.

[4] Decision of the German Federal Constitutional Court in BVerfGE Vol. 65, p.1.

ANALYSING RADARGRAMS AND SONARGRAMS BY BIOLOGICAL INSPIRED SIGNAL PROCESSING METHODS TO OPTIMIZE THE DETECTION OF MINES AND DUMPED AMMUNITION

Matthias Reuter[1] and Sabine Bohlmann[2]

[1] *matthias.reuter@cutec.de*
CUTEC Institute GmbH, Leibnizstr. 21 +23, 38678 Clausthal-Zellerfeld (Germany)

[2] *sabine.bohlmann@cutec.de*
CUTEC Institute GmbH, Leibnizstr. 21 +23, 38678 Clausthal-Zellerfeld (Germany)

Abstract

Even so ground penetrating radar and magnetic techniques are well established since many years, the signal analysis of them lacks still today especially when small ground structures, small objects but also more global soil structures should be detected or interpreted by radar or objects should be found by magnetic procedures. In the last recent years the author and his team worked on this problematic especially to empower special software for anti-mine resp. IED detection on land via ground penetrating radar and to detect and categorise dumped ammunition in the Baltic and Northern Sea with help on magnetic and sonic methods. In our paper we will introduce new methods of the signal processing resulting from these researches, showing that even signals with a bad S/N-ratio or natural weak signals can be interpreted in a better way than common signal processing methods, which leads in turn to a more effective signal/structure detection.

Keywords: biological inspired signal processing methods, enlarging S/N-ratio, hyperbola classification, mine and IED detection technology, SOAM-project.

1 INTRODUCTION

In the last three years the authors worked in the project SOAM at the problem to detect dumped ammunition in the Baltic- and Northern-Sea. Fixed on an AUV, an R2Sonic multi-beam echo-sounder, magnetometers, side scan sonar and forward looking sonar equipment have been tested for detection- and positioning-correctness on test fields and on so far unknown and later on verified areas. Figure 1 shows the principle structure of the SOAM system.

Beneath handling the task to combine several senor-types especially the S/N-problematic was one of the critical points to be solved. First the kernel of the data processing unit of SOAM was a combined hybrid neural net structure which involves two processing levels. The first level was for S/N ration optimization done by so called DLS spectra [1], the second level was for the ammunition signature detection done by a combination of self-organisation maps (SOMs) and backpropagation (BPP) networks.

As the analysis shows standard filter processing chains [4] and even Differential Auto power Spectra (DAS) spectra fail in the signal analysis in the distance ranges of 0-20 cm resp. up 2 meters and deeper. In the upper area these failures are based mainly on the mixed up of diverse hyperbolas; means arms of hyperbolas overlap or interfere, while in the deeper ground the information entropy level is extremely high.

Otherwise we have learned from biology [2] that most of the (biological inspired) visual signal processing routines are able to depress (automatically) undesirable information

and/or can focus on pattern contributions of higher interest. So we decided to study and model the internal structures of retina and here especially the network: Photo-optic sensors, horizontal-cells, bipolar-cells and amacrine-cells. In this article we describe the results of this researches and their transformation in an algorithmic form, whereby we show on ground penetrating-signature - as its structure is very similar to the structure of sonar-grams – which upgrade these new processing strategies leads to.

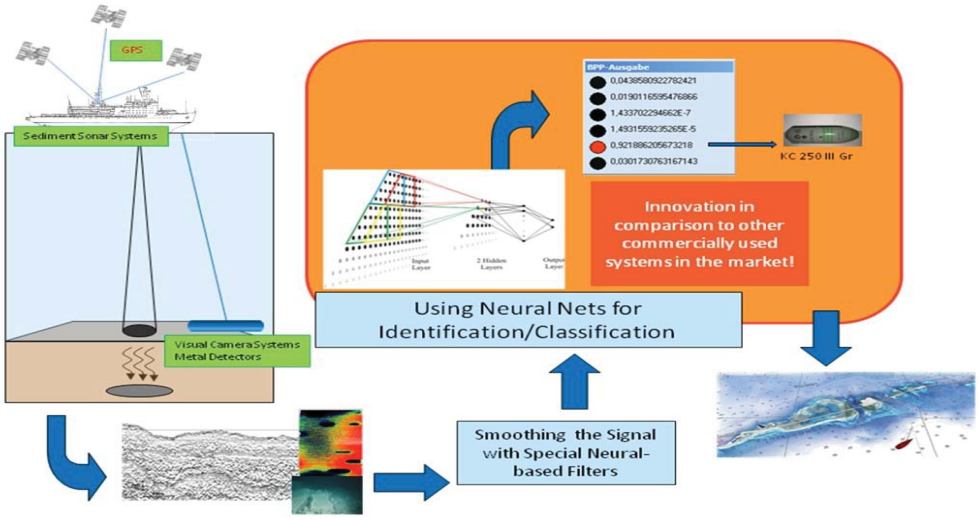


Fig. 1: Scheme of the detection and localization of dumped ammunition via the system SOAM

2 METHODS

It is one of the most surprising findings that the signal processing in the retina of the mammals is done on a more or less none numerical structure, means, is based on the temporary activity of different kinds of neurons, their potential differences, topological characteristic and the co called ON-OFF path ways. We learned rather quickly that the common models of the artificial neurons cannot meet these processing structures, whereby mainly the common structure of the inter-neuronal connections doesn't met reality at all. Otherwise we show some time ago, that changing the basic principle of the synapses and the restrictive condition that an axon has one and only one effector, leads to a totally new behavior of simulated neurons and - for example - solves along the way the 80 years old XOR-problem of the neural nets [3]. Combining those two improvements one ends immediately to the knowledge that in simulated neural structures too, not a single neuron will act "as a standalone system" but "basic neuronal structures" (BN-Structures), involving a minimum size of three neurons. Such a BN-Structure is shown in Figure 2.

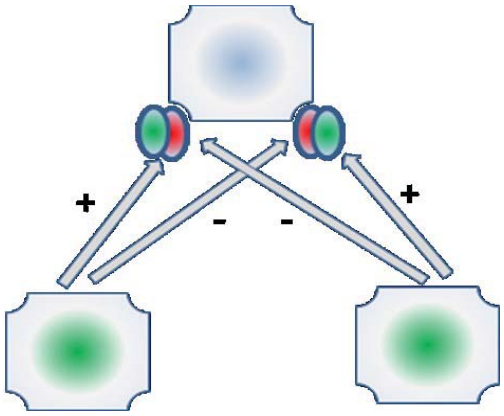


Fig. 2: Scheme of a BN-Structure

The two basic neurons on the lower side on a BN-Structure act a as more or less input layer, innervating at least two synaptic structures of the upper neuron synchronically, whereby – as a kind of supersymmetry – one of the synaptic structures acts in an excitatory and the other in an inhibitory way. (Remark: In nature this structure is more

complicated, as only so called interneurons can change a neurons output from excitatory to inhibitory. These neurons are not visualized in Fig. 2.)

Based on these BN-Structures we modeled retinal structures, means receptive fields of different dimensions, lateral inhibitions done by interneurons, ON/OFF-pathways and the integration of these passes.

3 RESULTS

It follows out of theory that the dimension of the receptive field size defines whether the contour of an object is accentuated or its overall shape. This is demonstrated by the following picture analysis. The original figure 3a shows a scene with three cars. If the receptive field dimension is chosen 3x3 the contours of the object are accentuated, this is shown in figure 3b. In Figure 3c and 3d the receptive field is enlarged by factor 3 and 4.

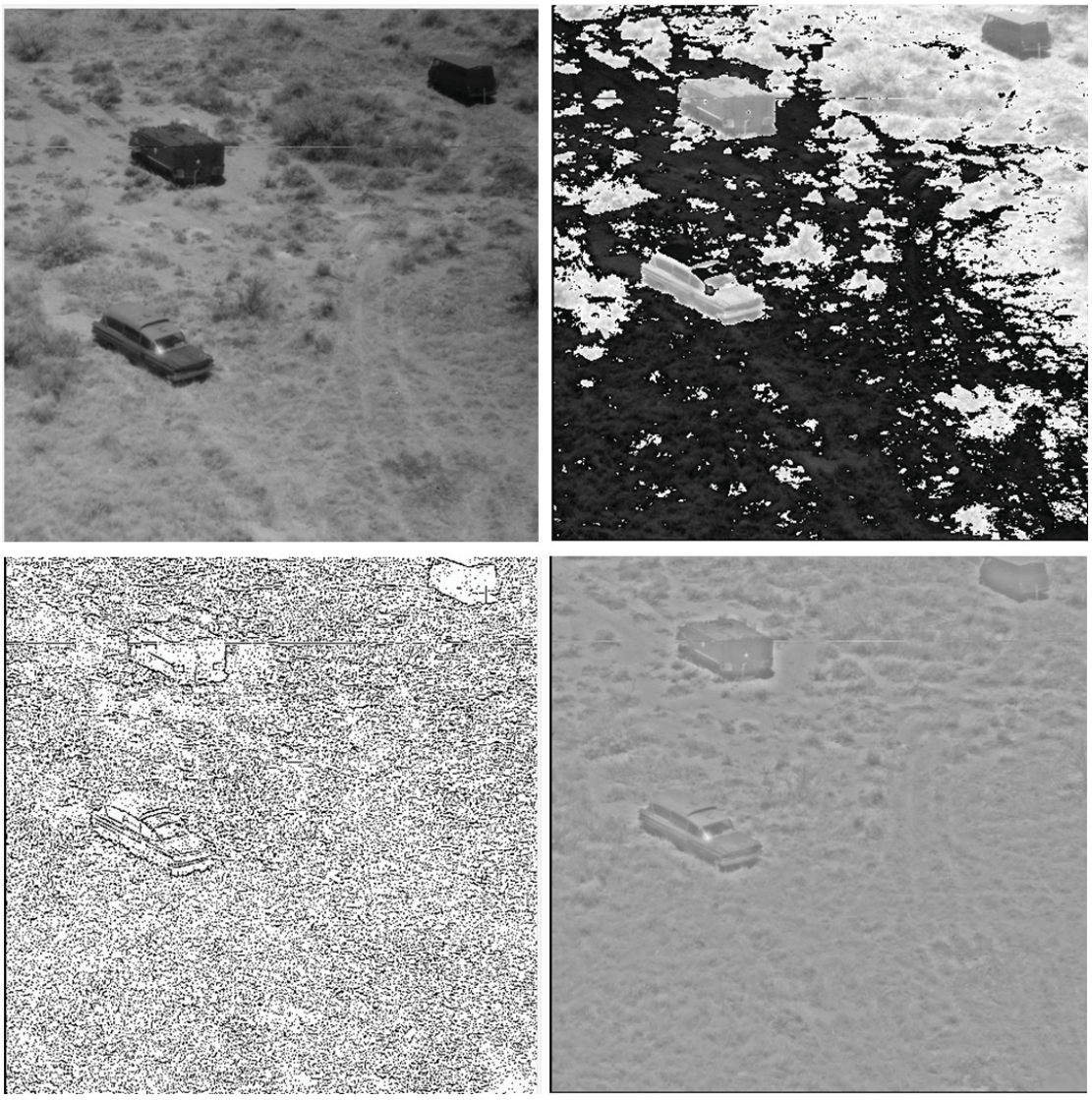


Fig. 3a-3d: Shape or object accentuation influenced by receptive field size

Next we used the same modules to identify hyperbola structures in an on-line object-detection-tool. Figure 4 shows such a detection process, at which the signatures of three mines (two in the middle of the picture, one at the right margin – with half signature present only) are detected and their position are marked by a white triangle.

As the system detect suspicious objects the left hand panel is coloured red and an acoustical signal occurs. Lower sides the A-scan of the radar gram is shown.

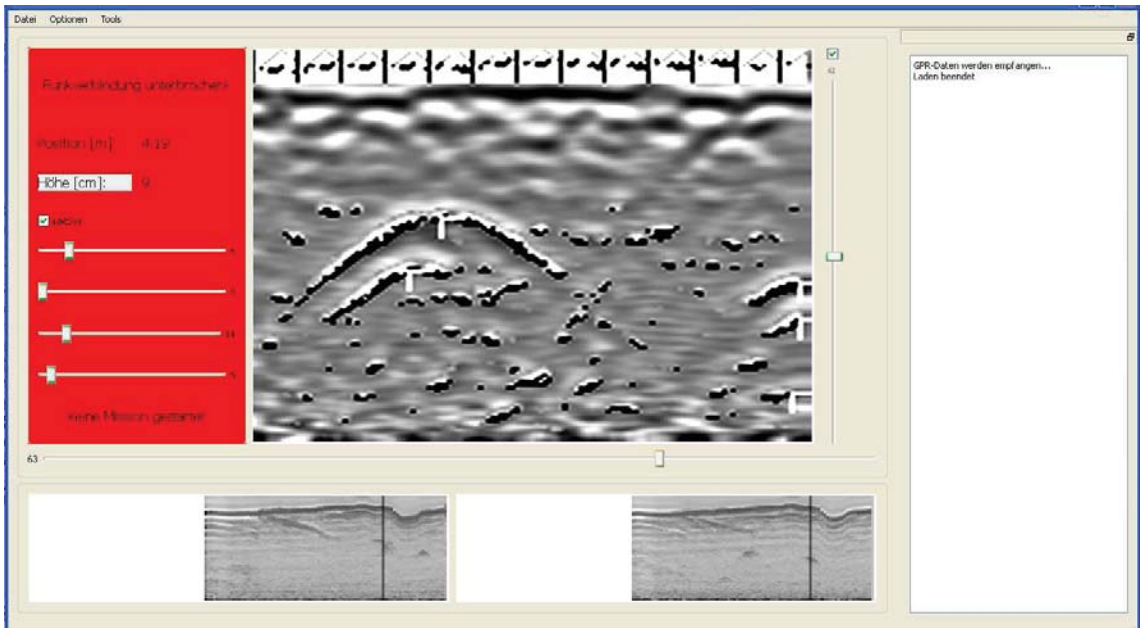


Fig. 4: Landmine detection by potential oriented, non numerical signal processing routines

4 CONCLUSIONS

We showed in our investigations that BN-Structure based signal processing routines will model the biological optical and (here not shown) acoustical pattern recognition in ear and eye by a more or less non-numerical and very quick and simple way and that high adaption to background noise, intensity and mixed information structures can be done by changing the range of the underlying receptive field dimensions of the BN-Structures. Paired with an extreme sensitivity for edged structures these new methods enable to visualize also equipotential lines of magnetic surveys and hyperbolic structures in deeper (up to 7 m) ground areas.

REFERENCES

[1] Reuter, M. (2001). *Analysing the Structure of Poly-Crystalline Materials by 2-dimensional DLS-Spectra and Neural Nets*. Computational Intelligence, LNCS 2206, pp. 420-427

[2] Kim, J. Green, M.J. et al., (2014). *Space-Time Wiring Specificity Supports Direction Selectivity in the Retina*. Nature 509, pp. 331–336

[3] Reuter, M. (2014). *Biological Inspired Synapses and the XOR-Problem*. https://www.researchgate.net/publication/270283328_Biological_Inspired_Synapses_and_the_XOR-_Problem

[4] Jol, H. (2015). *Ground Penetrating Radar Theory and Applications.* Elsevier Science

SAFETY & SECURITY MANAGEMENT SYSTEM IN PUBLIC TRANSPORT

Ing. Slavomira Vargova, PhD.,[1] and Dr.h.c. mult. prof. Ing. Juraj Sinay, DrSc.[2]

[1] *slavomira.vargova@tuke.sk*
Technical University of Kosice, Department of Safety and Quality Production, Letna 9, 042 00 Kosice (Slovakia)

[2] *juraj.sinay@tuke.sk*
Technical University of Kosice, Department of Safety and Quality Production, Letna 9, 042 00 Kosice (Slovakia)

1 PROJECT BACKGROUND INFORMATION

The need to adapt to changing circumstances is inherent in the creation of a system of tasks and measures for ensuring continuous improvement in the field of safety. Facilitating comprehensive safety of a system (machine, machine system, industrial technology, enterprise, or a region) does not mean building a protection system around it. The safety of procedures or safety of an organization is a complex state implemented and maintained by its senior management, in which dangerous situations (risks) are minimized in order to eliminate risks to people and their environment.

The basic principle in the management of human and technical risks assumes that it is necessary to identify possible risks and implement the proper measures with the aim to apply effective forms of prevention in time in order to avoid malfunction/accident. [2]

In most cases, risks result from natural processes and human activities. In this context, it is essential to realise that on one hand a human has the potential for accidental, unintentional cause of an adverse event, but on the other hand, he can cause injury/damage to another human, techniques, technologies and environment intentionally.

The incident which happened in Košice, September 22, 2014 in the afternoon can serve as an example of this intentional action of the human factor. *That day, a drunk passanger attacked a bus driver who was protecting a young mother with her children. According to the Transport enterprise of the city of Košice (DPMK), the driver wanted to exclude the drunk man from the bus. The drunk man attacked him, hit him in the face and the driver fell down on the pavement and hurt his head. The estimated treatement was from two to three months; the driver had only one moth to take up a retirement pension.* [2]

In the official statement, the management of DPMK asked their passengers to immediately contact the police in situations like these and thus help to eliminate the number of problematic situations in the public transport. However, does this really effectively solve the problem? We focused on the implementation of a risks management system integrating both safety & security in the conditions of a public transport provider and assesses the state of public transport security after the installation of CCTV inside the public transport vehicles.

2 METHODS

Public transport system consists of mutually influencing elements and relations that develop and operate over time and continuously interact with their environment. It is a natural, dynamic and open system including both biotic and abiotic components, thus

permitting not only the occurrence of random negative events but also deliberate intentional damage/harm caused to another person, society, technology or environment. The activities of risks management aiming towards effective prevention require understanding of these multi-parametric relationships between technology, work organization and human factor.

When applying the integrated approach to the assessment of the risks of a random object, the resulting risk of the given object is not given by the sum of risks of its elements, but the extent of the risk is given by the lowest level of an element of a part of the object (element of the system). Under *safety* we understand safety of the very object and it is possible to reach it by precautionary measures aimed at the minimisation of the potential risks. *Security* is an immediate risk reduction and thus protection of the system against the effects from the external environment.

A possible approach to ensuring the complex safety is the model in Fig.1 which involves different steps such as defining requirements, trends and limitations (1) of the system under review, defining elements and links in the form of maps of processes of the system (2), defining passive and active parameters: the dangers and threats as well as risks affecting the system (3), risk assessment (4) and its reduction (5) for the purpose of creating a safe system and safe environment in the surroundings of the system under review (6). It is possible to apply the generic model to any system.

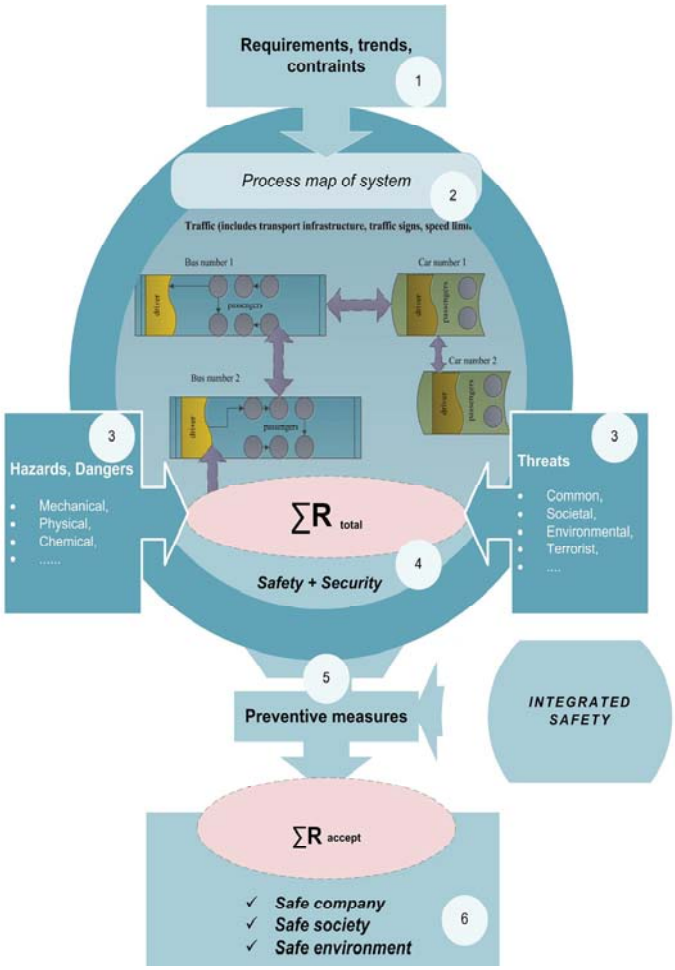


Fig. 1 Generic model of Safety & Security management system

It is very important to identify basic requirements and limitations for the job of a public transport driver [3]. In this case were considered professional requirements (e.g. ability to drive, knowledge of the company´s internal regulations dealing with emergencies), health requirements (e.g. health state and mental capability) and personal

requirements (e.g. kindness in communication with passengers). As limitations were specified external limitations (e.g. pressure from employer to observe the time intervals between stops; arising from the environment as meteorological conditions, night shifts) and internal limitations (current health and current mental state).

As factors that can be included into dangers and hazard of the considered area were identified:

- condition of the vehicle and all the physical, mechanical and chemical threats arising from it,
- psychological problems (actual and long-term mental state of the driver),
- health problems (actual health state of the driver which can deviate from the normal, good state - age, sex, common sickness).

Threats as external factors of the environment which cannot be influenced by the driver and are not easily predicted:

- environmental threats (meteorological conditions),
- social threats:
  - behaviour of the passengers in the vehicle (e.g. noise),
  - intentional or unintentional actions of other road users,
- *criminal threats (one passenger attacking another passenger or the driver).*

It is possible to assure security of the driver and passengers in vehicle by using video control, like they have been doing it abroad for several years. Video control serves to provide security of passengers and protects property from vandalism. [4] [5] The camera systems of individual vehicles are supervised by emergency responders who can intervene when needed. Video control via camera systems in public transport is gradually introducing in Slovakia from 2014. [6] The disadvantage of this camera system is fact that it creates only record (as examination for incident or vandalism) and in many vehicles does it neither.

In this case was for risk analysis in generic model used TESEO method which estimates reliability using five key factors (factor of a type of activity, stress factor of common or emergency activities, factor of workers qualities, factor of stress and anxiety and ergonomic factor). As input data were used data from driving behaviour questionnaire. Driving behaviour questionnaire included questions about length of work as driver, about experience dangerous situations, vandalism and effectivity of camera systems, about health and mental state, and questions about safety perception. If the product of individual factors approaches the value 1, the assumed probability of the failure also approaches the value 1, and the failure will almost certainly occur.

3 RESULTS

In order to estimate the risk of a public transport driver´s failure at addressing an emergency situation, e.g. conflict with a passenger, we chose the values for individual factors provided that:

- it is an unusual situation,
- the standby duration was determined by an average of 45 s,
- drivers are not physically trained to handle this emergency situation,
- depending on the mental state, the situation can be considered serious and unexpected by them
- since this is a special situation, bad microclimate and bad coordination (depends on age and actual health condition) are assumed.

The resulting value of estimate of the risk of a public transport drivers failure 0,9 corresponds to the critical situation of a certain type.

4 CONCLUSION

One of the basic conditions for a smooth performance of this job is a satisfactory technical state of the vehicle. In case of failure, the driver is under pressure and stress, which can be a source of an emergency situation. Another measure would be reducing the pressure on the part of an employer who pushes drivers to respect the time intervals between stops. In most cases, delays do not occur due to the driver but due to the traffic situation or higher number of passengers who get on/get out of the bus in rush hours.

In order to support the implementation of the safety & security management system of effective risk minimization, a generic principle-based operational model was designed, followed by its software version. Software version includes all parts of generic model, it is open and makes it possible to add new requirements and parameters.

5 ACKNOWLEDGMENTS

This contribution is the result of the project Research of Integrated Risk Research into new and newly emerging risks of industrial technologies within integrated safety as a precondition for management of sustainable development, Nr. APVV - 0337 - 11.

REFERENCES

[1] Bischoff, H.J, Sinay, J., Vargova, S., (2014) Integrated risk management in industries from the standpoint of safety and security. In: Sborník vědeckých prací Vysoké školy báňské - Technické univerzity Ostrava : Řada bezpečnostní inženýrství. - Ostrava : VŠB-TU, 2014 Vol. 9, no. 2 (2014), p. 1-7. - ISSN 1801-1764

[2] Karaffova, M., (2014) *Vodiča MHD napadol opitý mladík*. Accessed April 13. 2015. http://www.dpmk.sk/aktuality/vodica-mhd-napadol-opity-mladik

[3] Schneider, W., Dumais, S. T., & Shiffrin, R. M. (2012) B1. 2 Physiologische und psychologische Grundlagen der Fahrsicherheit und Fahreignung. Verkehrsmedizin: Fahreignung, Fahrsicherheit, Unfallrekonstruktion, 144.

[4] Demtröder, E., (2012) *Sicherheit für Busfahrer per Videokamera* Accessed December 8, 2014 http://www.derwesten.de/staedte/nachrichten-aus-luedenscheid-halver-und-schalksmuehle/sicherheit-fuer-busfahrer-per-videokamera-id6544125.html

[5] Berg, F. & Niewöhner, W. (2000) Sicherheit von Bussen. Analysen, Ergebnisse und Bewertungen der DEKRA-Unfallforschung. Verkehrsunfall und Fahrzeugtechnik, *38*(5&6).

[6] Kamerový systém v autobusoch (2014) Accessed April 15. 2015 http://www.dpb.sk/o-podniku/tlacove-spravyelektricka-ma-pred-chodcami-prednost/kamerovy-system-v-autobusoch-022/

[7] Sinay, J., (2014) Safety Management in a Competitive Business Environment. CRC Press.

SCINTILLA – A EUROPEAN PROJECT FOR NUCLEAR SECURITY

Sebastian Chmel[1], Wolfram Berky[1], Thomas Brall[1], Hermann Friedrich[1], Jeannette Glabian[1], Theo Köble[1], Monika Risse[1], Wolfgang Rosenstock[1], Olaf Schumann[1], Guillaume Sannie[2], Stéphane Normand[2], Guillaume Montemont[2], Olivier Monnet[2], Sylvain Stanchina[2], Paolo Peerani[3], Hamid Tagziria[3], Raffaella De Vita[4], Erica Fanchini[4], Gabriele Firpo[5], Enrico Botta[5], András Kovács[6], László Lakosi[6], Christian Baumhauer[7], Tiphaine Deheunynck[7], Elizabeth Haddad[7], Grégoire Petrossian[8], Romain Fossé[8], Grant Crossingham[9],Geraint Dermody[9], Andrew Price[9]

[1]Fraunhofer-Institut für Naturwissenschaftlich - Technische Trendanalysen (INT), Euskirchen, Germany
[2]Commissariat à l'énergie atomique et aux énergies alternatives, Saclay, France
[3]European Commission, Joint Research Centre, ITU, Nuclear Security Unit, Ispra, Italy
[4]Istituto Nazionale di Fisica Nucleare, Sezione di Genova, Genova, Italy
[5]Ansaldo Nucleare S.P.A, Genova, Italy
[6]Hungarian Academy of Sciences, Centre for Energy Research, Budapest, Hungary
[7]ARTTIC, Paris, France
[8]SAPHYMO, Massy, France
[9]Symetrica Security Ltd, Southampton, United Kingdom

1. Background

In the face of the possible misuse of radioactive or nuclear material (RNM) the detection and identification of such material is of outstanding importance. Radiation portal monitors for example can be installed at border crossing stations or, if they are re-locatable, at access courses to major sport events etc. to counteract illicit transport or application of RNM.

2. Goals

The European FP7-project SCINTILLA (“Scintillation Detectors and new Technologies for Nuclear Security”) aimed at building an innovative and comprehensive toolbox of devices and best-of-breed technologies for the enhanced detection and identification of difficult to detect radioactive sources and nuclear material, especially masked and shielded material. The work has included the important task of providing Europe with new neutron detector technologies as an alternative to Helium-3-based neutron detectors which have been used widely within portal monitors in the past but have become scarce and very expensive in Europe in recent years due to a world-wide shortage of He-3. Within this three year project, completed in February this year, 9 partners from 6 different European countries were working on the development of reliable, flexible and cost effective detection systems to address the described challenges.

3. Methods

SCINTILLA was innovating in two technology areas that offer complementary capabilities for the detection and identification of neutron and gamma radiation: scintillator-based technologies (organic and inorganic scintillation material) and CZT technologies (Cadmium Zinc Telluride), complemented by advanced image processing technologies.

The investigations and developments covered in particular:

- Organic Plastic Scintillators using Pulse Shape Discrimination (PSD). New algorithms were developed which significantly improve both time response and gamma rejection level.
- Improvement of Gadolinium-lined Plastic Scintillators by using of Monte Carlo simulations to optimize the detector geometry in view of dealing with multiplicity counting.
- Modular ^{6}LiZnS(Ag)-coated Scintillators for neutron detection.
- A networkable, stabilized, de-convolution enhanced NaI gamma spectrometric detector system. Research activities also covered the spectrometry using PVT (polyvinyl toluene).
- A CZT Gamma camera, integrating new MicroGami technology, with a new concept of CZT gamma-ray detector based on innovative 2N electrode structure.
- Miniature CZT semiconductors for gamma spectrometry with focus on new electronics with enough computation capabilities to enable online spectrum in-situ analysis.

These technologies were further developed and finally integrated into different detector systems addressing different usage contexts. Six usage cases (UC) were defined in detail, user requirements were analysed and specifications were elaborated to give an orientation for the developments, including input from experts and end users. The detection systems comprised re-locatable radiation portal monitors (RPM) and portable devices:

- UC1: RPM for containers
- UC2: RPM for vehicles
- UC3: RPM for luggage
- UC4: RPM for people
- UC5: Portable device for usage by police and customs
- UC6: Miniature devices for usage by first responders

To facilitate the integration and communication of the new devices, communication protocols were developed as input to standardisation efforts.

During the project some partners provided test-bed services in order to evaluate the performance of the developed detection systems and to give feedback to the technology subsystem developers. Three annual technology benchmarks, which were also opened to third party developers, supported the comparison of technologies and the selection of the technologies for the SCINTILLA Toolbox. These benchmarks were held in Ispra, Italy at the Joint Research Centre (JRC) facilities. The measurements were performed in a laboratory which was originally build for the ITRAP+10 project and is explicitly dedicated to testing of equipment for detection of radioactive and nuclear materials. The main parts of the tests were the response to gamma and neutron radiation, the influence of gamma radiation to neutron response, categorization and identification of radionuclides, and masking of Special Nuclear Material sources by medical isotopes, based on international standards namely ANSI, IEC, NSS1 recommendations of the IEAE (Nuclear Security Series) as well on ITRAP+10 testing and evaluation of commercial instrumentation. The test and benchmark activities were subject to scrutiny from expert users and scientific peer review.
In addition to these laboratory tests work was conducted outside the laboratories, e.g. testing vehicle portal monitors on a street with cars and pedestrian portal monitors in a nuclear medicine hospital with real patients. This ensured that the performance of the detector systems was tested in both a rigorous scientific manor and under relevant near real-life conditions.

Furthermore, during the SCINTILLA project the SCINTILLA Partnership Network was built bringing together a worldwide community of technology providers, experts and users on the topic of detection technologies. It will be continued as a part of other FP7-projects and emerging Horizon2020-projects European communities.

4. Results

Most developed instruments reached maturity. When benchmarked, all complied with international standards and most exceeded them with highly promising results. The capability to replace He-3 based neutron detection with other techniques could be proven.
In particular the integration of radiation portal monitors (RPM) for cargo (UC1, see above) that uses both He-3 free neutron detectors and spectroscopic gamma detectors has been generated and evaluated. An RPM for vehicles (UC2), which system design demonstrated integrated neutron detection with He-3 free neutron detectors, has been successfully achieved. A RPM for scanning luggage (UC3) has been built and successfully evaluated. The integration of RPM for people scanning (UC4) has been successfully achieved in 2 versions. It demonstrated integrated neutron detection with He-3 free neutron detectors and a range of spectroscopic detection systems with differing performance for assessment in real life environments. Two devices have been built and evaluated to address UC5: a CZT camera and a low volume He-3 free neutron detector. A first prototype device for UC6 has been developed using CZT.
For some project results, commercial exploitation has already started. All technologies constitute the overall SCINTILLA toolbox for which user guidelines have been established. More detailed information can be found in: www.scintilla-project.eu.

Protection of Smart Grids and IoT in the Wake of the 4th Industrial Revolution (Industry 4.0)

Feliks Vainik
f.vainik@emessage.de
+49 173 549 2152
e*Message W.I.S. GmbH, Schönhauser Allee 10-11, 10119 Berlin, Germany
Mobile Communication Service Provider

Project background information

With the 4th industrial revolution (Industry 4.0) new M2M (Machine-to-Machine) mechanisms were introduced almost everywhere in our daily life alongside with the IoT (Internet of Things) that becomes a reality. Among others, these new mechanisms allow effective remote access to ensure easy control and management. However since the current perception was to utilize the public Internet as the main bearer this newly acquired capabilities both for the public utility industry as well as for private usage (IoT) made the connected systems and devices also vulnerable to external attacks.

Utilization of SCADA and other remote access control and management systems via the open Internet allow 3rd party systems and external persons to gain access and manipulate connected devices.

When public utility companies are targeted, the attacks become the biggest threat to the national resilience as they disturb daily life of whole populations in a severe manner. Introduction of Smart devices in our daily life makes those also easy accessible to external systems, thus making us vulnerable to external attacks in our car, home and everywhere we are.

In recent years supposedly government lead cyber-attacks have caused damages both to knowledge databases as well as public utility infrastructures. In some cases water pumps, gas turbines as well all electricity switching equipment were targeted and caused local failure of aforesaid equipment as well as related services. It is anticipated that state led cyber attacks in times of crisis can create more damage than most conventional weapons ever will.

It is also commonly agreed that in order to protect civil society and keep them unharmed from major infrastructural failures whether it is gas, water or electricity supply as well as specific failure of car functionality or smart home related equipment it is mandatory to think on an alternate communication route that circumvents the needs to go over traditional Internet based communication and go instead over communication infrastructures that prevent the possibility of malicious or brute force attacks.

Goals

To cope with these threats e*Message has introduced e*Nergy, a remote access solution based on NP2M technology.
e*Nergy is a radio-based M2M management solution, which is based on paging broadcast system. e*Nergy is reliable, secure and offers efficient remote management of all consumption and production facilities in modern public utility systems.

Given its small size e*Nergy reception modules can also be introduced in almost any Smart Devices that are in the need of remote access and switching.

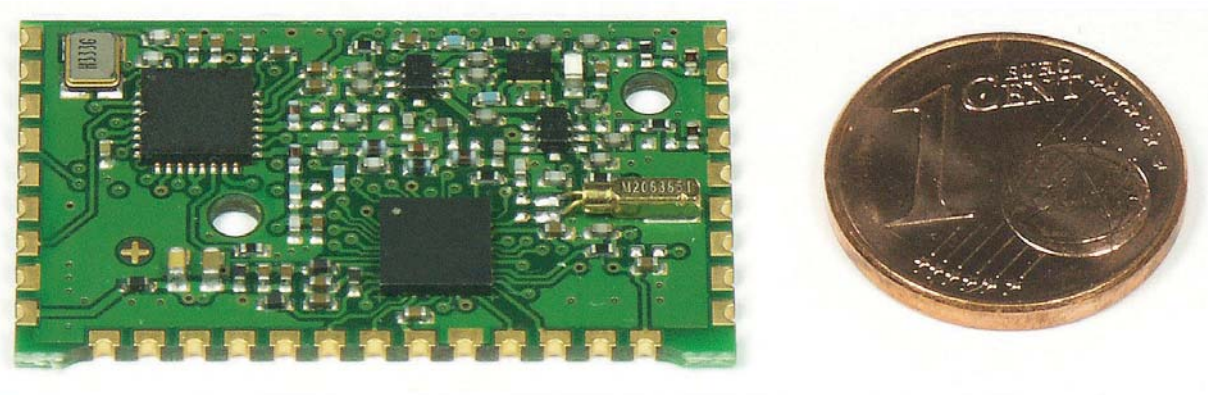


Fig. 1 – e*Nergy Paging Module, Size Comparison

The extremly low energy consumption makes it adequate even for any mobile device. e*Nergy is Internet independent yet more efficient through location based broadcast capabilities that saves the need for dedicated links. As such e*Nergy enables to manage even the largest networks and systems also on national scale as well as connect to almost endless number of devices in real-time.
e*Nergy can serve as the default solution when it comes to effectively manage large scale production systems as well as millions of consumer products in real-time as an alternate offering to the traditional Internet. Additionally it can serve in times of crisis it can serve as a fall back solution to the traditional Internet as well as to other communiciation methods, thus ensuring business continuity as well as the population's safety and security and contribute as such to national resilience.

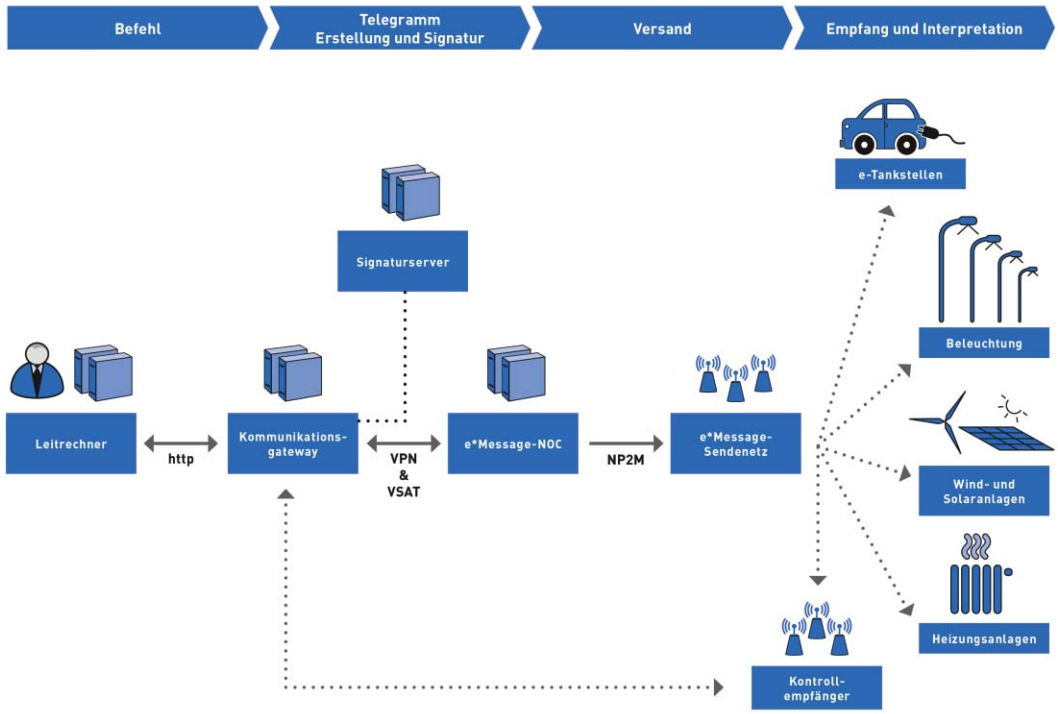


Fig. 2 – Smart Grid Process Flow based on e*Nergy Paging Technology as used by energy companies

It has been acknowledged by Vattenfall Berlin that e*Nergy N2MP technology provides today the best protection to Smart Grids with unreached effectiveness in comparison to alternate communication technologies. e*Nergy was recently introduced as Vattenfall's intial base to build up its German Smart Grid system, in cooperation with e*Message and Bosch Software Innovations.

Fig. 3 – Wireless energy switching module used by Vattenfall and based on e*Nergy technology

The goals are to demonstrate e*Nergy effectiveness and security to a larger public going beyond traditional energy companies, thus positioning itself as the default communication method when security is at stake.

Methods

For succesful demostration of the e*Nergy system and modules, e*Message W.I.S GmbH is intending to cooperate with large service providers both from the public utility as well as private consumer products sector. e*Nergy command & control system will be integrated at the backend of the relevant public utility companies as well as service providers incl. the necessary PKI (Private Key Infrastructure) alongside with integrationof the e*Nergy reception modules in the relevant reception devices whether they are electricity switcher, water/gas pumps or any device used as part of the IoT (cars, household products, etc.)

Intended results and conclusions
To demonstrate the solution's effectivenss, especially when it comes servicing millions of devices as well as the solution's economy. In the wake of recent cyber attacks on international level also the solution's security and immunity to external attacks in comparison to traditional communication methods.

Side effects
From the negative point of view no particular side effects are to be expected. The solution can be managed as the fall back system ensuring business continuity.
From the positive point of view utilization of e*Nergy can accelerate decision making process on national level embracing Smart remote access, control and management without jeopardizing national resilience, thus contributing to acceleration of the 4th industrial revolution in general and IoT in special

Generic Integrated Forensic Toolbox for CBRN incident – GIFT

Contact details:
Mr Andrew Johnston
Falcon Communications - on behalf of the EU funded project GIFT CBRN
Unit 26, Basepoint, 1 Winnall Valley Road, Winchester
SO230LD
Andrew.johnston@cbrneworld.com
Tel: +44 1962832531 Mob: +44 7899734735

Project background

The successful interrogation of evidence either at a crime scene contaminated with chemical, biological, radiological or nuclear (CBRN) agents, or of the agents themselves back at the lab, is an absolutely vital part of CBRN defence. Not only will processing these agents, or being able to handle traditional evidence in a hazardous environment, be vital to the successful trial and prosecutions of the individuals that carried out the attack, but it might provide vital information as to what agent was used and what medicine needs to be given to the survivors.

The Generic Integrated Forensic Toolbox for CBRN Incidents (GIFT CBRN) is designed to close up the many gaps inherent in this complex area and provide an integrated law enforcement CBRN capability that is world class. At present forensic investigation is hampered by a lack of protocols and training in carrying out forensic analysis on CBRN-contaminated materials. The aim of GIFT-CBRN would be to develop a forensic toolbox for investigating CBRN incidents providing:

(**1) Procedures, sampling methods and detection of CBRN agents at the crime scene,**
(2) Traditional forensic laboratory methods for contaminated evidence
(3) Laboratory methods for profiling the CBRN agents released at the incident.

The procedures and methods will be set up and validated according to ISO17025 and the system validation will be performed by a final exercise. Procedures for chain of custody, QC to ensure the integrity of the evidence and investigations done on the evidence from crime scene to court will be developed. An education and training curriculum related to the developed procedures, best practices and methods will be designed and progressed to implementation.
Underpinning the above aims, research will be carried out to develop novel methodologies to enable traditional forensic science (DNA, fingerprint and electronic devices) to be carried out on CBRN contaminated exhibits and analytical procedures to be carried out that not only provide information about the CBRN agent itself but also through CBRN profiling to provide in-depth information which can give valuable forensic information.

Methods

GIFT will seek to focus on establishing common guidelines and procedures for how forensic science should be implemented when dealing with CBRN incidents. At present no such guidelines exist at a European level for CBRN forensic investigations. GIFT will also seek to develop new sampling and measurement strategies at CBRN contaminated scenes in order to perform on-site crime scene investigation. In particular new tools for finger printing, CBRN sensing and DNA sampling and analysis will be investigated. The project will liaise with on-going National and FP7 projects funded in the CBRN and forensic area and leverage from technologies developed to further enhance the forensic toolbox capability. The GIFT concept will enable solid and court-proof CBRN forensic evident in accordance to accredited standards. It would also provide a platform for training and education of CBRN forensic

science which is core to developing the expertise required to successfully bridge the gap between traditional forensic and CBRN forensic investigations.

To establish a baseline from which the advancements will be made, scenarios will be developed and a gap analysis will be done to identify those areas that show potential for advancements. On the basis of the scenarios and gap analysis the areas that require improvements for which this project can develop solutions will be described. These scenarios will also be used to validate the tools developed within this project.
It is the aim of the project to develop a toolbox that covers forensic research for a selected choice of CBRN agents. Three specific application areas for improvements are identified, firstly the gathering of evidence on the scene of the incident or accident, and secondly the research on CBRN contaminated evidence in a laboratory environment and thirdly identifying and profiling the used CBRN agents. These application areas are thought to be different for each of the C-, B- and RN agents in required procedures and activities and may require different tools. Within the project these application areas are dealt with separately. Several tools are identified that may improve forensic research at the scene of an incident or accident and procedures to collect, register and package evidence, to maintain the chain of custody, to perform a safety assessment, as well as several tools that may be applied for forensic research in a laboratory environment. To successfully trace the radiating contamination to the source or vendor, identification and profiling of the CBRN agent may prove valuable. Methods will be developed to identify and profile C- and B- agents, an initial feasibility study will be done during the project to evaluate the possibilities of identifying radiological contamination to such detail that it can be traced back to the original source or vendor.
For forensic research in a laboratory environment, a distinction will be made between newly established laboratories for forensics on contaminated evidence, and existing CBRN laboratories retrofitted for forensic research. It is thought that these two cases differ to such an extent that they need to be dealt with separately. Furthermore, it is thought that for successful implementation of the innovative tools and best practices, an exploration is required of possible mechanisms (including legal issues) of the use of existing EU CBRN forensics laboratories in international cooperation among EU member states. This task fits closely to an action of the EU CBRN action Plan and is also addressed. To ensure the best practices can be adapted by the forensic community within the EU Member States, courses about the best practices will be developed throughout the project for the project deliverables.

Forensic laboratories globally have a variety of techniques and capabilities they can call upon. There are limited numbers of laboratories with advanced capabilities and the members of the consortium represent some of the foremost nuclear capabilities within the EU. For example in the CBRN field specifically, e.g. TNO, FOI, AWE, CEA and ITU are leaders in their specific field of analysis. Modern and purpose-built facilities exist within these organisations to enable work covering a broad range of chemistry, radiochemistry, (micro) biology, analytical science and materials science programmes. State of the art knowledge is required in the area of forensics on contaminated exhibits because the worlds of materials analysis and traditional forensics do not collide on a regular basis, and there are significant limitations to EU capabilities as a result. In particular the field of police investigations and criminal forensics procedures on contaminated exhibits is not well developed within the EU or globally. Terrorist crimes and industrial incidents involving the use of CBRN agents would have a high impact on the EU, its citizens, the environment and public health. There is a pressing need to develop protocols and robust methods to ensure safe forensic investigations that can be used in a court of law. This proposal aims to commence development of those capabilities and will:

- Develop procedures, practices and guidelines for common CBRN investigations at a crime scene and in a laboratory,
- Develop innovative tools to detect and identify CBRN agents and to improve safety of forensic investigators on the scene of an incident Explore how some classical forensics examination procedures, as fingerprints revealing with cyanoacrylate

vapour can work on contaminated evidence whilst preserving a tight chain of custody,
- Explore the practicalities of developing CBRN forensics procedures in a laboratory environment.
- Some come from other domains of scientific research and development, like hyperspectral imagery which found applications in satellite imagery and detection of pollutants for example. These have not been proved to work with forensic evidence treatment.
- Develop guidance and knowledge which is applicable to the European domain and provide some best practice(s) which could form the basis for broader adoption across Europe.
- Explore how some established technologies can be adapted to support CBRN forensics and how these technologies could fit within the overall CBRN forensic toolbox.

The GIFT approach is highly innovative in that it will progress beyond the state of art for the application of established techniques in this new specialised domain. Whilst the work may not be to invent a new and innovative technology it will integrate cross forensic related technologies and nuclear related technologies and improve efficiency within legal constraints. In this regard the approach is truly innovative.

Some of the tools that will be developed are:
- Development of tools for safe localisation and securing of radioactive agents (LQC)
- Development of portable instruments for materials
- Development of an in-situ heavy metal analysis system (Tyndall-UCC)
- Development of a portable instrument to determine on site chemicals (RAMEM)
- Develop a Hyperspectral imager for latent fingerprints (M2L)

Intended Results

Tools for a safe localization and securing of radioactive agents (LQC)
In case radioactive material is present at an incident scene the protective suits of the forensic investigators do not provide effective protection against gamma radiation. A tool for remote controlled localization will be developed. Visualization with a gamma camera will be a part of this tool.

A fully prototype will be developed along the following lines:

- Form factor: hand-held pistol-grip instrument with graphic display.
- A 2D gamma radiation detector consisting of a quadrant of radiation sensitive elements.
- Considerations of performance cost and availability will determine at the design stage the choice among silicon, CsI crystals coupled to silicon, or advanced materials such as CZT (CdZnTe).
- Gamma radiation is collimated by use of a Gershun tube made of tungsten or lead alloy.
- Electronic using standard microprocessor handles the signal from the four quadrants and displays intensity of the gamma field and an arrow indicating where to point the device to locate the source.
- With a field of view of 3 to 20 degrees (selectable by changing Gershun aperture) multiple point sources at corresponding separation can be separately identified.
- Protection of IP in the form (among others) of patent application(s) will be undertaken from this early stage.

Development of portable instrument for material analysis: Mobile Stand-off LIBS platform

Development of a portable instrument for material analysis: Mobile Stand-off LIBS platform. Identification of materials at the incident scene is not only efficient for decreasing the time of the whole investigation, but more knowledge of the nature of materials on the incident scene leads to a more efficient operation. Therefore, a remote controlled or portable tool for identification of materials is necessary. A promising technique in this area is Laser Induced Breakdown Spectroscopy (LIBS). The tool which will be developed will be based on this technique.

Laser induced breakdown spectroscopy (LIBS) is a powerful tool and established technique for the proximity and stand-off analysis of solids to detect their molecular composition. A LIBS system relies on a high pulse energy laser source that irradiates a point of interest, causing the surface material to be evaporated. Once in the gas phase, the excited molecules emit spectra that can be collected and analysed; thereby giving insight into the composition of the irradiated surface.

Development of a portable instrument to determine on site chemicals (RAMEM)

We propose to develop on-site analytical methods to identify organic chemical agents using Ramem's High Resolution Ion Mobility Spectrometer (HRIMS). HRIMS instrument is based on Differential Mobility Analysis (DMA) in which analytes are identified and quantified based on their ion mobilities, which depend on mass, shape, size and charge. Estimated limit of detection is in the low-ppb level (depending on the analyte), and resolving power higher than 50 (current field Ion Mobility Spectrometers (IMS) instrument have resolving powers around 25). This higher resolving power, together with the use of multivariate analysis algorithms, will deliver a better identification power.

Develop Hyperspectral imager for latent fingerprints (M2L)

It is necessary to know where fingerprints can be found on objects to prevent destruction by other kinds of investigations. Swabbing of the objects for the identification of CBRN agents may be necessary. In this way latent fingerprints present will be destroyed. Therefore contact free detection of latent fingerprints on objects is necessary. A technique based on spectroscopic imaging is promising in the visualisation of the location of latent fingerprints on objects.

GIFT will develop a state-of-the-art capability to detect fingerprints at stand-off distances with minimal sample preparation and non-destructive analysis of substrates, based on a new development of M Squared Lasers active IR hyperspectral imaging system. Initial work will be to develop a lab-based capability for technology demonstration, with potential for in-field application at a later stage.

Conclusion

The approach of the GIFT project is highly innovative in that it will progress beyond state of the art the application of established techniques in this specialised domain. Whilst the work may not be to invent a new and innovative technology and, by developing best practices descriptions, improve efficiency within legal constraints. In this regard the approach is truly innovative.

The consortium consists of 21 parties, from nine different European countries. They are, NFI (NL), Tyndall (IRL), TNO (NL), RIVM (NL), M2L (UK), Falcon (UK), Fera (UK), AWE (UK), STUK (FIN), FOI (SWE), NFC (SWE), Analyzed IQ (IRL), NICC (BE), RMA (BE), Space Applications (BE), JRC-ITU (EC), CEA (FRA), Eticas (ESP), RAMEM (ESP), LQC (ESP), and NanoBiz (TUR).

AUTOMATIC DETECTION OF OBJECTS WITH MULTISTATIC MILLIMETER WAVE IMAGING TECHNOLOGY

Athanasios Karamalis[1]

[1] *Athanasios.Karamalis@rohde-schwarz.com*
Rohde & Schwarz GmbH & Co. KG, Mühldorfstraße 15, 81671 München

Abstract

The Quick Personnel Security Scanner R&S®QPS100 and R&S®QPS200 deliver advanced imaging solutions for personnel screening at airports and other critical infrastructures. The fully electronic system acquires high-resolution complex three-dimensional imaging data with planar multistatic sparse arrays. Privacy of personnel is protected by analyzing imaging data automatically with the dedicated threat detection software, without storing or displaying raw image data. Potential threat objects are indicated to the end-user on an abstract avatar. The detection software must fulfill challenging requirements in terms of detection capabilities. A multitude of possible threats scenarios must be recognized with low false alarm rates, in order to provide the necessary throughput. For this purpose, an image processing and machine learning framework was developed for threat detection, which classifies image regions into normal or suspicious.

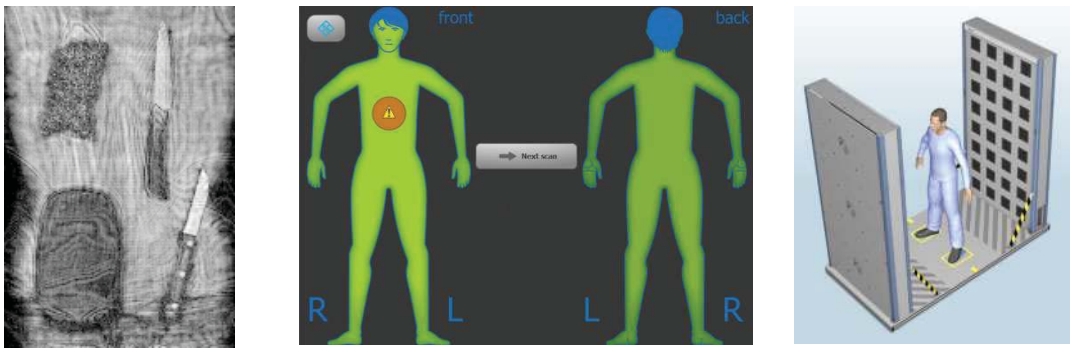
Keywords: millimetre wave imaging, security screening, security scanner, airport security, threat detection, image processing, machine learning

1 INTRODUCTION

Personnel screening technologies have advanced considerably in the last decade, driven by the growing threat from terrorist attacks. They are primarily used for detection of concealed objects at airports and other critical infrastructure. The demand for efficient personnel screening technologies, with broader detection capabilities is increasing; however, ethical and health aspects need to be fully considered for public acceptance. New imaging technologies aim at detecting concealed metallic and non-metallic objects. Imaging systems based on X-ray technology were already used for luggage inspection and lately for personnel screening [1]. X-ray based imaging systems provide high image resolution; however operate with ionizing radiation, which remains a critical health aspect for personnel screening at airports. Imaging technologies based on millimetre waves (mm-waves) offer contactless screening with nonionizing radiation. Moreover, a novel mm-wave imaging technology was developed for the R&S®QPS100 and R&S®QPS200 security scanner, providing state-of-art lateral resolution of ~2mm [2].

The R&S®QPS100 and R&S®QPS200 security scanners offer high-resolution complex three-dimensional imaging data [2]. The raw imaging data depicts concealed objects with rich detail (see Fig. 1a), leading to broad detection capabilities. The raw imaging data is not displayed to the operators of the security scanners. Instead, the built-in threat detection software analyzes automatically the imaging data and indicates suspicious regions - that may contain concealed objects - to the operator on an abstract avatar; see Fig. 1b. Thus, person privacy is protected and security is enhanced as the automatic threat detection software provides reliable and reproducible broad detection capabilities.

The challenges for the threat detection software are manifold. A multitude of possible threat scenarios must be recognized, including objects of different shape, size and material.



(a) Raw image (b) Display detection software (c) R&S®QPS200

Fig. 1: Image (a) shows a raw image of explosive surrogates (left) and knifes (right) concealed beneath clothing, (b) exemplary display result of threat detection software, (c) illustration of R&S®QPS200 and correct body posture

In addition, the software must recognize objects and threats that are a priori unknown to the system. Furthermore, persons with different age, height and body-index must be screened with low false alarm rates, in order to provide the necessary throughput at airports and critical infrastructures.

2 THREAT DETECTION FRAMEWORK

The R&S®QPS100 and R&S®QPS200 security scanner use mm-waves in the frequency range from 70 to 80 GHz. The maximum output power is ~1mW, since non-focusing antenna elements are applied. The transmitted mm-waves penetrate clothing, but are reflected by person skin or objects. The R&S®QPS100 and R&S®QPS200 scanner provides high-resolution three-dimensional imaging volumes of the reflected signal amplitude and phase. Depending on the material, objects appear differently in the imaging data, as for example shown in Fig. 1a.

The automatic threat detection software detects objects, threats and suspicious regions based on the reflection characteristics of regions in the imaging data. The emphasis lies in the detection of suspicious regions. Instead of performing object or pattern matching against a database with predefined threat scenarios, a generalized approach is employed for classifying image regions into normal and suspicious. For this purpose, an image processing and machine learning framework was developed, which will be presented in more detail in the next sections.

2.1 Image and Posture Validation

The detection software validates the image content, before searching for any objects or suspicious areas. For this, the software controls the position and posture of a person inside the reconstruction volume, i.e. the area for which the image volume is computed, to ensure optimal illumination conditions for the different body regions. The system operator is alerted, in case of inadequate positioning or body posture. The posture recognition is performed in 3D utilizing the amplitude and range information available in the imaging data.

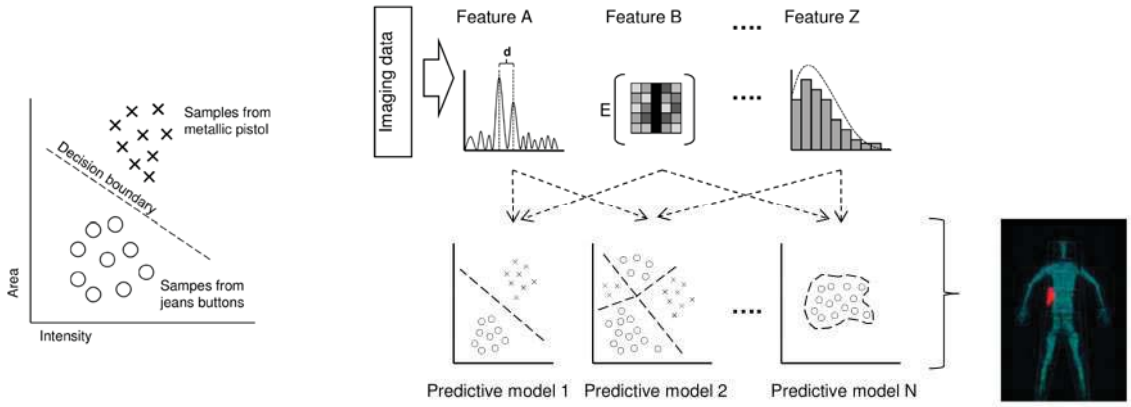


Fig. 2: (Left) illustration of predictive model, (right) illustration of extracted image processing features, predictive models and classification of suspicious region in imaging data

2.2 Image Features

An important aspect in most computer vision applications is the choice of image features [3]. For automatic threat detection image features should separate well normal and suspicious image regions, be invariance to body physique and describe locally the image content, in order to allow targeted alarm resolution by security personnel. The illustrative example in Fig. 2 (left) shows the separation of image samples into normal and suspicious class using intensity and area of identified object as features. The intensity and area feature alone are insufficient to provide a reliably separation, whereas the combination of both features yields a clear decision boundary between the two exemplary sample sets. The high-resolution three-dimensional imaging data allows extraction of a multitude of imaging features. For example, the permittivity of explosives causes distinct reflection characteristics in the receive signal [4], which are extracted with various filter kernels for classification; see illustrative example Fig. 2 (right). Further image features are computed, as for example gradient, texture, context and intensity distribution features, which are combined with features that are tailored to this specific application and imaging modality. Overall, the detection software utilizes thousands of different features, in order to capture the reflective characteristics of normal and suspicious - possibly threat – regions. Manual tuning and combination of these features would lead to suboptimal results. Instead techniques from the field of machine learning are applied to optimally combine image features that separate well the two classes.

2.3 Machine Learning

Machine learning provides methods for learning predictive models from training data [5] and has found numerous applications in computer vision problems [3]. The process involves collecting a training/testing dataset, extracting features from the data, training predictive model(s) and utilizing trained model(s) for classification or regression tasks. In terms of data, a comprehensive collection of thousands of raw imaging data has been collected with and without concealed objects internally at Rohde & Schwarz GmbH & Co. KG. This training dataset is used to extract the aforementioned image features, which in turn are utilized for training the predictive models. There are different types of machine learning and classifiers available for training predictive models [5]. For automatic threat detection, classification of a multitude of possible threats is required, including threat scenarios that are not represented in the training data. For

this purpose, multiple classifiers are trained independently with subsets of the available image features, as illustrated in Fig. 2 (right). This improves the generalization of the predictive models, with classifiers trained on reflective characteristics of threat scenarios and on reflective characteristics of normal human body with clothing. The training with thousands of image data, thousands of image features and numerous classifiers is computationally intensive and performed on a custom distributed computing network/cluster, similarly to MapReduce approaches [6]. During operation of scanners no imaging data is stored, but rather the previously trained predictive models are utilized to classify image regions into normal and suspicious. More specifically, the independent run-time predictions of all classifiers for the imaging data at hand are combined into a pixel-wise probabilistic response. This response indicates the likelihood of a pixel (image region) containing objects or threats, as illustrated in Fig. 2 (right). A continuous response, instead of a binary decision between the two classes, is beneficial for configuration of the threat detection software in terms of detection rate vs. false alarm rate.

3 CONCLUSION

We discussed the various aspects and challenges in the development of automatic threat detection software for classification of image regions into normal and suspicious within mm-wave imaging data. The separation between normal and suspicious, instead of normal and threat regions, results in broader detection capabilities, including detection of a priori unknown threat scenarios. Complementary to the training dataset a comprehensive testing dataset is utilized during the development of the software. Additionally to the rigorous testing during development, the software was independently evaluated and approved for operation by the European Civic Aviation Conference (ECAC). The fully electronic system design and imaging capabilities of the R&S®QPS scanners, together with increasing computing capabilities pave the way for the development of next generation mm-wave personnel scanners; allowing walk-through personnel screening.

REFERENCES

[1] Baukus, W. J. "X-ray imaging for on-the-body contraband detection." *16th Annual Security Technology Symposium & Exhibition*. 2000.

[2] Ahmed, S. S., et al. "Advanced microwave imaging." IEEE Microwave Magazine, 13.6 (2012): 26-43.

[3] Szeliski, R. *Computer vision: algorithms and applications*. Springer Science & Business Media, 2010.

[4] Schiessl, A., and Ahmed, S. S. "W-band imaging of explosive substances." IEEE *Microwave Conference (EuMC), 2009*.

[5] Bishop, C. M. *Pattern recognition and machine learning*. Springer, 2006.

[6] Dean, J., and Sanjay G. "MapReduce: simplified data processing on large clusters." *Communications of the ACM ,*51.1 (2008): 107-113.

IMPROVEMENT OF OPTICAL AND ACOUSTICAL TECHNOLOGIES FOR THE PROTECTION OF CAMPS OR MOBILE TROOPS: PROJECT IMOTEP

Sébastien Hengy, Martin Laurenzis, Bernd Michael Fischer, Pierre Naz, Véronique Zimpfer

sebastien.hengy@isl.eu, bernd.fischer@isl.eu
French-German Research Institute of Saint-Louis (ISL)
BP 70034, 68301 SAINT-LOUIS, France

Abstract

Snipers have emerged as a major threat to troops in recent conflicts. To reduce this menace, the objective of the French-German Research institute of Saint Louis (ISL) research project "IMOTEP" (improvement of optical and acoustical technologies for protection) is to improve the detection of snipers on the battlefield. Our basic approach is to combine several sources of information for a fast and appropriate reaction when an unusual signal (e.g. a flash or a shot) is detected. The project includes several technologies developed at ISL: acoustical detection, fusion of distributed sensor network data, active imaging and 3D audio communication. The objectives are to provide to the soldier an individual capability to detect snipers by the use of a wearable system associated with other distributed UGS (Unattended Ground Sensors) allowing the protection of camps, convoys by the detection and localization of sniper attacks.

Keywords: sniper localization, acoustic detection, active imaging, audio 3D.

1 INTRODUCTION

The presented realization consists in a network of portable "detection" systems integrating an acoustic array for the detection and localization of sniper shots. An early estimation of the threat position is transmitted through a network to an active imaging system in order to confirm, to refine this position by 3D imaging and to deliver a clear image of the scene. The range-gated active imaging system is used to explore the scene, and then all the images produced are used to reconstruct a virtual 3D model of the scene. In parallel, a 3D audio warning message is generated depending on the position and orientation of each soldier. For this purpose a GPS and a magnetic heading-sensor are used to track in real time the displacement of the soldier's head and to refresh the direction of the detected sniper. In addition, the camp is protected by an adhoc sensor network used for intruder detection. This paper presents the results obtained for the various technologies involved in the Interdisciplinary Technology Project IMOTEP [1]. This aims on a fundamental investigation of complementary sensor units as sources of processed information. The fusion of this information allows for enhanced localization ability compared to the ability of their single components.

The use of acoustics for such a system can easily be explained by the specific characteristics of the signal corresponding to a supersonic shot (Mach wave and blast wave) and considering the capability of acoustics to detect NLOS (Non-Line-Of-Sight) sound sources, 24 hours a day (day and night), with a 360° field of sensing and by passive means [2].

The visual information is very important for confirmation purpose. Our eye-safe active imaging system [3] offers day/night capabilities associated to a high spatial resolution with horizontal and vertical IFOV of some tens of µrad i.e. some meters on a kilometric

scale. In addition the photon time-of-flight measurement enables 3D imaging and precise range estimation.

2 ACOUSTIC SENSOR NETWORK

ISL developed various shooter detection and localization prototypes in the past years based on acoustic microphone technologies. Based on this knowledge, ISL wanted to enhance the localization performance of those prototypes by developing data fusion techniques that would not need any prototype hardware modification to allow the integration of existing devices in the fusion process. This led to the choice of the use of asynchronous localization algorithms based on the use of the time difference of arrival separating the Mach and muzzle waves generated during small arm firing.

The fusion algorithm gathers the data that have been transmitted via the wireless network (ZigBee). These data have been locally pre-processed by all the acoustic nodes that have detected a transient wave and. In the scope of this project, two types of acoustic nodes are used in the network (Fig. 1):

• Individual acoustic arrays: Three prototypes of helmet-mounted acoustic arrays and two prototypes of vehicle mounted acoustic arrays both equipped with 8 microphones,

• Networked acoustic nodes: up to ten two-microphones acoustic nodes, so-called doublets, can also be part of the network.

Figure 1: acoustic nodes that are part of the data fusion network

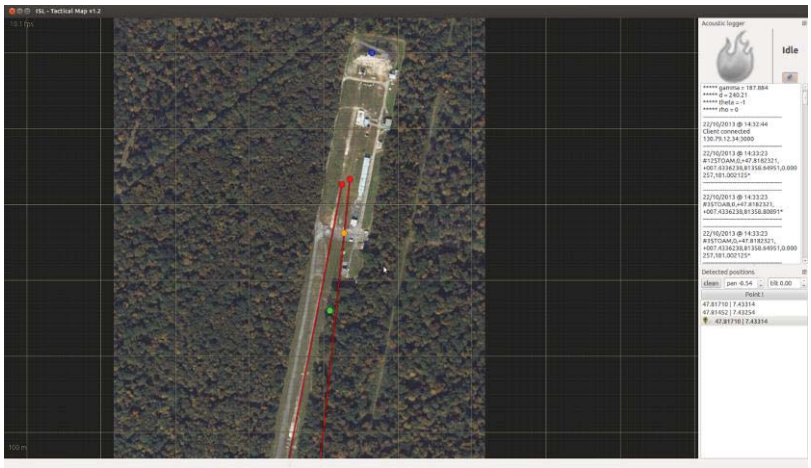


Figure 2: Acoustic detection live results displayed on a tactical map. Display of the estimated shot corridor (two solid lines define this corridor) and position of the shooter (green dot).

3 LASER GATED VIEWING

For applications, such as camp protection, a range-gated imaging sensor is used for identification and verification of the threat by an operator. This active sensor consists of an intensified image sensor which is dedicated to a laser illuminator (Fig. 3). Here, a solid-state laser is used to emit light in the eye-safe short-wave infrared (SWIR) spectral range. The laser is collimated and homogenized by an ISL-patented waveguide technology to enable illumination thanks to a homogeneous and flat rectangular top hat profile which matches perfectly the field of view of the sensor. The imaging sensor is an array with a resolution of 1360 × 1024 sensor elements attached to a motorized zoom optic with a variable focal length of 75 mm to 500 mm. The sensor head was installed on a motorized pan & tilt unit which can be remotely controlled to orientate the system in the direction of the estimated position of the sniper.

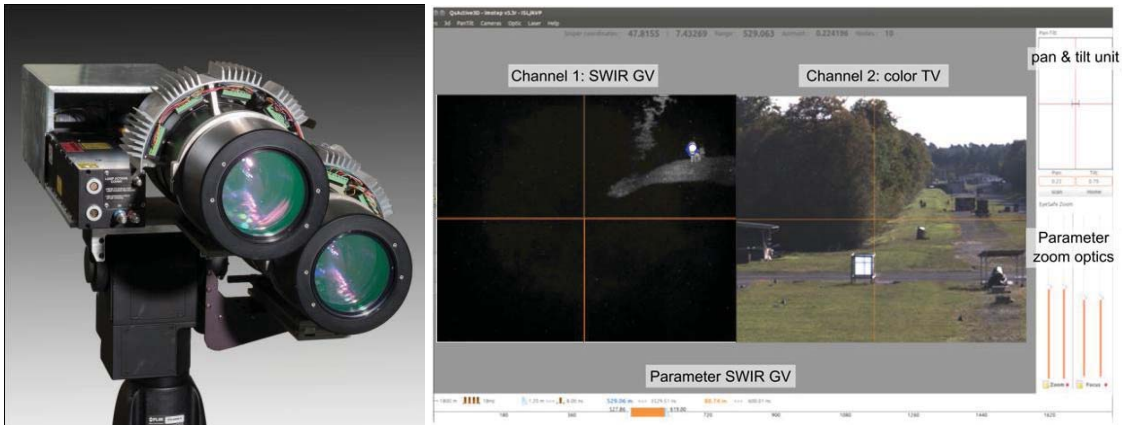


Figure 3. Setup of the IMOTEP electro-optical sensor unit and man-machine interface

4 3D AUDIO RESTITUTION

Threat restitution can be transmitted to the members of the security forces by various means. As the detection part of our system provides geolocalized data, the estimated position of the threat is indicated on a tactical map at the command post, and a live video of the scene is transmitted by the active imaging system. A warning tone is transmitted to each of the dismounted soldiers who is singled out from a group, by using 3D-audio techniques.

The developed 3D audio prototype allows the direction of the location of the sniper to be displayed by using the natural human capacity for localizing sounds. Acoustic warning signals are reproduced via a multifunctional communication headset in such a way that they appear to point in the direction of the sniper who is detected by the acoustic sensors.

Fig. 4 presents the principle of the 3D audio display. The electrical speech signal is filtered by means of appropriate filter functions for the right and left ears (using Head-Related Transfer Functions, HRTFs). Then it is reproduced by the loudspeakers of the headset. The filter function depends on the position of the source and the position of the listener's head.

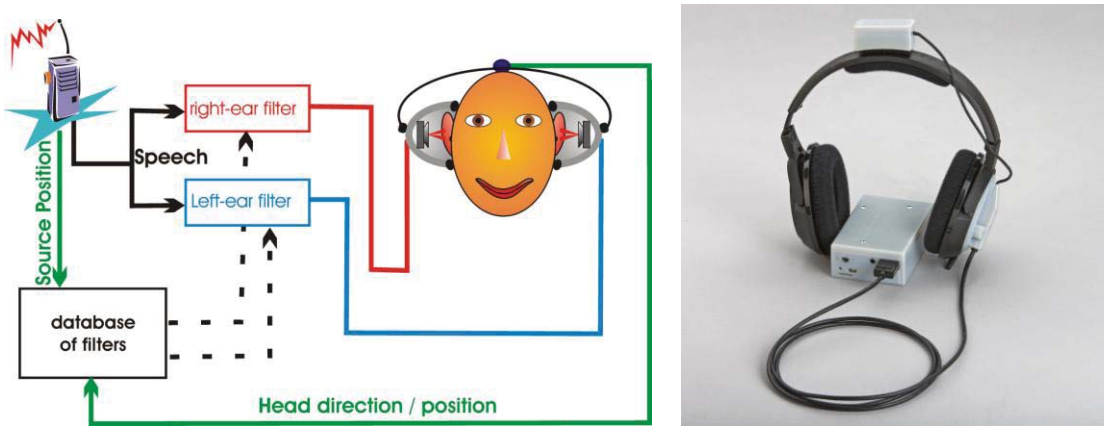


Figure 4. Principle of the 3D audio display and view of the headset with magnetic compass and GPS receiver on top and signal processing unit

5 CONCLUSION

During this project, we developed and tested different technologies and system approaches for area surveillance and for wearable equipments of security forces and soldier system. The objectives were to increase individual protection by means of increasing the situational awareness and to enhance the operational effectiveness. The networking capabilities within a group of soldiers for the detection and restitution of threats in the domains of acoustics and active imaging have been demonstrated.

The results obtained during the final demonstration at ISL's proving ground (58 small calibre shots at range varying from 100 to 600 meters) show that in the worst case, the measured shooter position error is less than 5% of the actual shooter-to-array distance for 60% of the detected shots. It is less than 10% for 86% of the detected shots, and less than 15% for 96% of the shots.

Novel processing algorithms are a key feature to improve these performances and are currently developed in order to adapt this technology to an urban environment for civil security applications. Furthermore, innovative concepts are investigated in order to develop acoustic and active imaging detection systems for moving platforms as well as to extend the detectable threat to systems such as UAVs.

ACKNOWLEDGMENTS

These studies have been initiated by the ISL in the context of its program of work and have been supported by governmental contracts from the DGA and the BAAINBw. We are grateful for all these supports and the active involvement of the participants.

REFERENCES

[1] Hengy , S., Laurenzis, M., Schneider, A., Zimpfer, V. (2015). *Improvement Of optical and acoustical Technologies for the Protection (IMOTEP)*. NATO Joint Symposium IST-106 and SET-189, 04-05 May 2015, Norfolk, Virginia, USA.

[2] Naz , P., Hengy , S., Laurenzis, M. (2015). *Acoustic sensor network for Hostile Fire Indicator for ground bases and helicopter-mounted applications*. SPIE DSS, Proc. 9464, 20-24 April 2015, Baltimore, Maryland, USA.

[3] Laurenzis, M., Christnacher, F. (2013). *Laser gated viewing at ISL for vision through smoke, active polarimetry, and 3D imaging in NIR and SWIR wavelength bands*. Advanced Optical Technologies, 2 (5-6) pp. 397-405

SECTOR: SECURE COMMON INFORMATION SPACE FOR THE INTEROPERABILITY OF FIRST RESPONDERS

Jana Mauthner[1], Sandra Frings[2], Wolf Engelbach[3], Lukasz Szklarski[4], Piotr Gmitrowicz[5], Yann Semet[6], Frank Wilson[7], Jean-Paul Pignon[8]

[1] *jana.mauthner@iao.fraunhofer.de,* [2] *sandra.frings@iao.fraunhofer.de,*
[3]*wolf.engelbach @iao.fraunhofer.de*
University of Stuttgart, Institute for Human Factors and Technology Management (IAT)/ Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart (Germany)

[4]*lukasz.szklarski@itti.com.pl,* [5]*piotr.gmitrowicz@itti.com.pl*
ITTI Sp. z o.o., ul. Rubież 46, 61-612 Poznań (Poland)

[6]*yann.semet@thalesgroup.com*
Thales Research & Technology, Campus Polytechnique, avenue Augustin Fresnel 1, 91767 Palaiseau Cedex (France)

[7]*frankwilson@btconnect.com*
Stichting Studio Veiligheid (SSV), Saturnusstraat 60, 2516 AH Den Haag (Holland)

[8]*jean-paul.pignon@thalesgroup.com*
Thales Communications & Security SAS, 4 Avenue des Louvresses, 92622 Gennevilliers Cedex (France)

Extended Abstract

Nowadays, crisis management faces many challenges since societies become increasingly vulnerable to disasters. Natural and man-made disasters impact various communities and place multiple demands for crisis management organisations [3]. Successful response to disasters and crises mainly depends on the quality of planning, collaboration, cooperation, and coordination of actors involved in crisis management. Crisis management organisations need to respond quickly and effectively to new risks and unexpected threats [7]. Accordingly, there is an ever growing need for the interoperability of a great variety of organisations ranging from international organisations, first responders and police authorities to governmental authorities, commercial suppliers and volunteers. Collaboration can be supported at best, if these organisations combine their strengths and create synergies. Based on a shared understanding and organisational procedures, this can be improved by (IT-supported) information systems that enable multilevel, multi-organisational and cross-border information flows [6], [5].

Accordingly, an effective interoperable crisis management has to consider:

- Semantic interoperability to support exchange between agencies for joint planning of improved resilience.
- Pragmatic technical and syntax aspects, taking into account first responders' needs and mass notification to the population as conditions for rapid operational improvements.
- Communication interoperability between safety partners to improve coordination and cooperation efficiency [8].

No known common approach, technique or tool is available to support the interoperability in the whole crisis management cycle (from prevention to recovery) across agencies and across borders. The European project SECTOR – Secure

European Common Information Space for the Interoperability of First Responders and Police Authorities – acknowledges the importance of IT supported strategic and tactical collaboration and coordination in the field of crisis management by defining interoperability between crisis management actors and systems as one of the most important prerequisites for successful crisis management. The project aims to design a new concept for a European Common Information Space (CIS) for Collaborative Crisis Management (CCM) for information, knowledge resources as well as services sharing and coordination based on (1) an inventory and analysis of past critical events as well as European CCM processes, (2) the collection of system and user needs, (3) the definition of a set of CCM scenarios and (4) the design of a European Meta-Model for CCM.

There are different definitions of common or shared information spaces. According to Christensen [4] Common Information Spaces *'describe document repositories commonly accessible as well as the environment in which multiple actors can convey information to each other'.* Common Information Spaces are not only computer-based systems and databases, but constitute social systems, in which actors can create a common understanding, share values and decide on goals. Such a Common Information Space can serve as a medium to support communication and conversation, as well as to provide storage facilities (e.g. information on past critical events and operational information) [4], [8].

The SECTOR project intends to implement a computer-based Common Information Space to:

- Support exchange of information from IT systems involved in crisis management.
- Support collaborative crisis response by safety partners using the CIS.
- Enhance coordination of all actors involved in crisis management by supporting specific tasks and activities.
- Support the rapid sharing of data among responder organisations.

SECTORs CIS can accordingly be defined as an inter-organisational information system acting as a middleware component between information systems and external Emergency Management Systems of the involved partners. It will be developed and built upon an architecture adapting and integrating some existing CIS related tools such as IsyProc [9] and OMAR [1], in which a cross-agency collaboration process and system architecture have been modelled. The SECTOR CIS-prototype will be demonstrated and validated by end-user agencies in the following cross-agency and cross-border test scenario (both simulations and field exercises): a flood incident focussing on loss of transport in European waterways that entails several social, commercial and ecological effects.

To get an overview of existing crisis management procedures, processes and tools, we conducted 48 interviews with experts in fire departments, fire brigades, police authorities, emergency services, crisis management centres and ministerial departments (e.g. Ministry of Health, Ministry of Interior, etc.) in Poland, Ireland, Northern Ireland, the Netherlands, Germany, Italy, Portugal, France and Scotland. The same target group was addressed by a questionnaire specifying user and data requirements needs in a CIS. In addition to that we organised several international workshops with representatives of the above mentioned authorities and organisations to validate and discuss initial findings of the interviews and the questionnaire. This allowed us to refine, which functionalities a CIS needs to have from an end user oriented point of view. Accordingly we aim to show how a CIS can help to enhance effective and efficient information sharing, crisis response and even avert crisis. The design of the CIS is mainly driven by guidance from leading experts and the CIS will be

iteratively designed and refined in constant coordination with relevant end users. The SECTOR project intends to support formal arrangements for the coordination of cross-border and cross-agency information flows by such a CIS [2].

The inventory and analysis of past critical events, the survey on data sets, procedures and tools used in cross-border and multi-agency CCM processes as well as the CCM scenario definition conducted in the framework of the project supports the general finding that the management of crisis is influenced and supported by a large variety of organisations. The types of organisations involved in monitoring and response to potential and actual disasters, as identified from our sample, include: Government, Military, Civil Defence, Non-Governmental Organisations; First Responders, Industry; and Social Organisations (Civil Society such as sailing clubs, volunteer mountain rescue etc.). They are a source of intelligence related to these scenarios, and so are critical for enrichment of the common operational picture (COP) during response and recovery. A strong message for SECTOR is that in the area of monitoring for natural disasters, the whole range of types are present, and so must be involved in the longer term in planning, training, and system usage.

The thorough analysis has further shown that all organisations have established own responsibilities, but large scale incidents often require the collaboration of different stakeholders. In many countries there exist processes of coordination between police, fire-brigades and administrative staff, often prescribed in regulations and laws. Furthermore, all organisations involved in crisis management strongly rely on individual IT infrastructures. With the help of these systems, organisation's crisis management is supported by maintaining an overview of the current situation at the incident sight - especially the organisation's area of responsibility - by providing information about available and required resources for crisis response measures as well as means to coordinate and plan emergency response measures and activities.

These findings allowed us to identify the following high level collective needs of organisations involved in crisis management activities:

- Common language of international crisis management allowing for semantic interoperability of data and vocabularies.
- Common procedures that define typical roles and responsibilities (e.g. internal processes for crisis management).
- Collaborative, standardised assessment of threats, harms, risks and (limited) resources.
- Aggregation, visualisation, individualisation and accessibility of information compositions.
- Interoperable communication paths provided through national and international information management networks.
- Interoperable IT-systems that enable actors to gain an accurate situational awareness of the event.
- Expertise of actors in multi-agency and cross-border environments.

In order to take into account these needs SECTOR does not try to support collaboration through a single unique system or platform, since that will not be accepted by the crisis management organisations. Instead, the Common Information Space (CIS) provides a shared environment for critical safety partners where joint ownership of precious information will empower those on whom we rely for civil and critical infrastructure protection. This approach has already benefitted from intensive collaborations with a range of very scarce experts to establish their requirements. With their continued guidance we will implement and fully test the CIS and report its usage

in a realistic flooding scenario. This approach will demonstrate how several agencies can learn and utilise the CIS to explore its support for collaborative decision making and response planning.

Keywords: Crisis management, interoperability, common information space, inter-organisational coordination, information management, IT

REFERENCES

[1] Aligne, F., Savéant, P. (2011). *Automated planning in evolving context: An Emergency Planning Model with Traffic Prediction and Control.* Future Security 2011.

[2] Bharosa, N., Lee, J., Janssen, M. (2009). *Challenges and obstacles in sharing and coordinating information during multi-agency disaster response*. *Propositions from field exercises.* Inf Syst Front, pp 49-65.

[3] Boin, A.,'t Hart, P. (2010).*Organising for Effective Emergency Management: Lessons from Research*. Australian Journal of Public Administration, pp.357-371.

[4] Christensen, U. (2000*). Common Information Spaces.* Ph.D. Course on Plans and Situated Actions: The problem of human-machine communication revisited, Oslo, Norway, May 8-12 2000.

[5] DKKV (2015). Das Hochwasser 2013. Bewährungsprobe für das Hochwasserrisikomanagement in Deutschland. DKKV Schriftenreihe 53.

[6] Grant, T., van der Wal, A. J. (2012). *A Taxonomy of Market Mechanisms for Information*. Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012. URL http://www.iscramlive.org/ISCRAM2012/proceedings/288.pdf (accessed 15.05.2015).

[7] Schraagen, J.M., Huis in't Veld, M., de Koning, L. (2010). *Information Sharing During Crisis Management in Hierarchical vs. Network Teams.* Journal of Contingen-cies and Crisis Management. doi: 10.1111/j.1468-5973.2010.00604.x.

[8] Tahir, O., Andonoff, E., Hanachi, C., Sibertin-Blanc, C., Benaben, F., Chapurlat, V., Lambolais, T. (2008). *A Collaborative Information System Architecture for Process-based Crisis Management.* Knowledge-Based Intelligent Information and Engineering Systems Lecture Notes in Computer, pp. 630-641.

[9] Truptil, S. et al. (2010). *Mediation Information System Engineering for Interoperability Support in Crisis Management*. Enterprise Interoperability IV, pp. 187-197.

Acknowledgements

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement n°607821. We thank the SECTOR project partners for fruitful discussions about concepts, solutions and approaches. The paper reflects only the authors' views, the Commission and the Project are not liable for any use that may be made of the information contained therein.

NETWORKED IT-SECURITY FOR CRITICAL INFRASTRUCTURES – THE RESEARCH AGENDA OF VESIKI

Sandra Bergner[1], Benedikt Buchner[2], Sebastian Dännart[1], Albrecht Fritzsche[3], Andreas Harner[4], Sophia Harth[4], Max Jalowski[3], Dennis-Kenji Kipker[2], Ulrike Lechner[1], Kathrin Möslein[3], Andreas Rieb[1] and Martin Riedl[1]

[1] *Lehrstuhl für Wirtschaftsinformatik, Universität der Bundeswehr München*

[2] *Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen*

[3] *Lehrstuhl für Wirtschaftsinformatik I, FAU Erlangen-Nürnberg*

[4] *VDE|DKE, Frankfurt*

Abstract

In order to evaluate and to improve IT security of critical infrastructure that considers also aspects beyond technical ones, the project VeSiKi accompanies various projects from different critical infrastructure backgrounds to establish a collaborative research process among these projects. It serves as a platform which allows research institutions and providers to access results derived within this collaborative process.

Keywords: IT-Security, Critical Infrastructure, Research Project

1 INTRODUCTION AND PROJECT BACKGROUND

IT systems of a critical infrastructure (CI) are never completely isolated from their environment due to interaction, in terms of data exchange, maintenance, software updates and manual input to control and change the operation of the system. These interfaces make CIs vulnerable, in particular when individual human interaction is involved. Technical measures to increase the protection of infrastructures against external attacks increase the pressure on other aspects of security, regarding employee behaviour, institutional culture and procedural routines of daily work etc. [1]. To ensure functional IT security architectures, it is necessary to consider technical, human and organizational aspects at the same time as well as legislation, norms and standards. In order to address the above aspects and to establish new approaches for evaluating and improving IT security of CIs, the BMBF research program “IT-Security for Critical Infrastructures” has been initiated as part of the “High Tech Strategy 2020” of the German Federal Government. Hereby, the Project “Networked IT-Security of Critical Infrastructures” (Vernetzte IT-Sicherheit Kritischer Infrastrukturen, acronym “VeSiKi”; FKZ:16KIS0214) is the accompanying research project beside other selected projects carrying out a collaborative research process. VeSiKi started in January 2015 and runs for a period of 3.5 years.

2 RESEARCH ACTIVITIES AND APPLIED METHODS

VeSiKi´s research perspective is trans-sectoral and will engage the other projects in a collaborative research process and reach out to the IT security community as well.

As depicted in Figure 1, all collaborative research activities of the project VeSiKi, which will be detailed in the following section, will result in a framework of reference processes for IT security of CIs. Hereby, also the communication of researchers and practitioners in the project, including various stakeholders will get a common foundation

by means of a reference model for IT security. In long-term, this reference model will address small and medium sized providers of CIs as an ontology-based tool which allows them to identify suitable procedures and technology to assess and improve IT security for their CIs and align with legislation and governmental regulations.

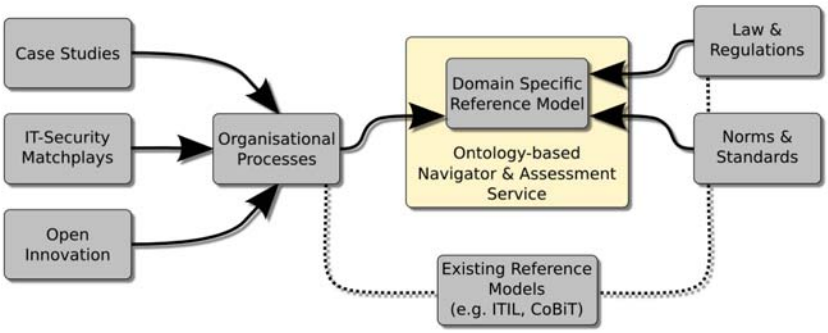


Figure 1: Research Activities

2.1 Case Studies and IT-Security Matchplays

Identifying all relevant requirements specific for IT security of CIs will be a key factor for delivering a valid and practical framework in this domain. In order to learn how CI providers currently ensure security of their information systems and which processes are implemented, we will conduct two approaches in close cooperation with the joint projects within the research program. On one side, we invite IT service operators of CIs to contribute case studies, either concerning established IT security relevant processes, measures and ongoing or finished projects in the organization. Beyond delivering workshops, templates and guidelines, we will accompany the partners during the development of their case studies and carry out a cross-case analysis afterwards which will help us identify best practices and common criteria for the design of a domain-specific framework. On the other side, we will perform IT-Security Matchplays with project partners to challenge leadership processes as well as resilience and business continuity measures in a setting which enable us to see trans-sectoral influences and common issues.

2.2 Open Innovation

Various authors like Hawkey et al. distinguish a variety of different factors and dimensions of IT security and IT security management [2]. IT security is accordingly not only a matter of individual competencies and capacities, but also has strong connections to all aspects of interaction in communities and networks of knowledge and information [3]. Community and network-related activities across institutional boundaries are reflected in open approaches to innovation [4] which intensify the use of knowledge and allow flexible setups and targets of research and development. Open innovation, however, also means that internal knowledge is conveyed to the outside. In an area as sensitive as CIs, open innovation activities therefore have to be designed very carefully. Security concerns of all stakeholders require special attention. Individual interests have to be weighed against each other in order to reach a satisfactory solution for everyone and a suitable overall result. We propose a framework for open innovation based on a representation of IT security for CIs as a service system. Systemic structures allow identification of different instances of value creation on different levels, which can then be addressed individually by specific open innovation activities reflecting the requirements of each instance individually.

2.3 Legislation and Regulations

The IT security of CIs is not only a technical challenge. Legal aspects for the realization of IT security can not be ignored, rather they have to be integrated into the development of IT security measures on from the beginning during the design phase of new technical infrastructures. Likewise, this kind of integration is essential to guarantee the practical character of the IT security law [5]. As a result, an authority which sets legally binding standards has to be in cooperation with the institution which implements these standards. Only under these circumstances, it is possible to realize a coherent, systematic and in a sufficient manner made concrete IT security law. To achieve these research goals, the Institute for Information, Health and Medical Law (IGMR) at the University of Bremen follows a research agenda which can be structured into two different parts. The first part addresses legal questions arising from CI providers that are partners within the research program. For example, solutions to up to date legal problems will be presented in seminars or workshops during visits of enterprises or industrial plants. The second part of the research agenda is focused on the evaluation and classification of applicable laws for CI regarding the different sectors. Besides these two research focuses and on a long dated basis, the IGMR will also develop new legislative proposals for the IT security of CIs. These proposals will mainly be focused onto the results of the dialogue between the researchers and the operators of CIs so that their wishes and complaints can be integrated into future regulations as far as it is possible. To reach this goal, the IGMR seeks the contact to legislative institutions during the complete duration of the VeSiKi research project.

2.4 Norms and Standards

Norms and standards are important for the sustainability and transferability of research results as they bring together interested parties of industry and science. They also guarantee the transfer of the research results into the market. To give the joint research projects the opportunity to work on this topic together, the VDE|DKE will host a working group “norms and standards” (Fachgruppe “Normung und Standardisierung”). The aim is to achieve a common view on standardization of IT security for CIs. As there are a lot of standards and guidelines concerning this topic, it is important to simplify the applicability of those documents so that small providers can easily use those standards. On one hand, the working group will produce recommendations for new standards resulting from the outcome of the research projects, on the other hand it will identify and close gaps in already existing standards. Furthermore it will categorize those existing standards for IT security for CIs. The aspects of norms and standards in general and especially for IT security will be presented and discussed in workshops as and when required by the joint research projects. In the end of the process the VDE|DKE will take care that the derived results find their way into the relevant standardization-committees, even beyond the project duration.

3 INTENDED PROJECT ARTEFACTS

Besides accompanying the joint research projects, a major output will be our own artifacts, derived from the research activities described above. In the following section we will address exemplary deliverables in more detail.

3.1 Reference Model IT-Security for Critical Infrastructures

Since governments more and more recognize the importance of CIs, regulations and legislation, in particular focusing their IT security systems, are increasing. Due to the fact, that many providers of CI are small or medium enterprises, they simply don’t have the resources to develop and implement their own concept of conform IT security.

Current IT-Management frameworks and reference models, such as ITIL or COBIT do consider IT security, but they don't focus it, far less taking CI in account. Based on identified best practices, processes and special requirements of CI, derived from the case studies and IT-Security Matchplays as well as open innovation activities, we will deliver a reference model for the Management of IT security for CI. This will enable organizations to adopt proved processes and align their IT-Security management to both reliable IT security and their duties towards governmental demands. In order to standardize and simplify the adoption we aim at delivering a framework, which is either based on, extending or at least compatible to common de-facto standards. Since many organizations yet are conform and aligned to these standards, the change and approach will be well known and easy to handle.

3.2 Ontology-based Navigator and Assessment Tool as a Platform Deployed Service

The derived reference model as well as the classification of applicable laws, regulations, norms and standards will be made accessible via an ontology-based webservice in order to simplify and accelerate CI assessment. Such a service may be the first, fast and easy to gain reference point for every legal assessment of a CI even for non-jurists. This service applies for sectoral norms and standards in the field of IT security of CIs as well. It is further planned to eventually support CI providers to assess their organization by denoting the infrastructure type, processes and assets. This may give hints on how to improve their current situation based on the reference model serving as a framework for implementing relevant norms and to conform to legislation, best-practices and state-of-the-art methods as developed within the joint projects of this research program.

4 CONCLUSION

Beyond the exchange between the joint projects of the research program via conferences, workshops and the developed platform to allow project partners to share research results and to establish public visibility, VeSiKi carries out its research agenda. Therefore, CI providers are included to carry out case studies, perform IT-Security Matchplays and to use open innovation as a tool for improving information security. A cross-sectoral analysis and classification of common practices and processes, applicable laws, regulations, norms and standards is performed in order to derive a common knowledge model accessible via an ontology based service integrated as part of the provided webplatform.

REFERENCES

[1] Halliday, S., Badenhorst, K., and von Solms, R. (1996). *A Business Approach to Effective Information Technology Risk Analysis and Management*. Information Management & Computer Security 4(1), pp. 19-31.

[2] Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagne, A., & Beznosov, K. (2008). *Human, organizational, and technological factors of IT security*. CHI'08 Extended Abstracts on Human Factors in Computing Systems (ACM), pp. 3639-3644.

[3] Fenz, S., Parkin, S., & Van Moorsel, A. (2011). *A community knowledge base for IT security*. IT Professional 13(3), pp. 24-30.

[4] Chesbrough, H.W., West J & Vanhaverbeke W (eds) (2006) *Open Innovation: Researching a New Paradigm*. Oxford: Oxford University Press.

[5] Spindler, G. (2008). *IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen*. MMR 11(7), pp. 7-12.

MOBILE UNITS FOR CHARACTERIZATION OF SITES CONTAMINATED BY ACCIDENTS

Thomas Streil and Veikko Oeser

streil@sarad.de
SARAD GmbH, Wiesbadener Straße 10, 01159 Dresden, Germany

Abstract

As part of an environmental, accidental or terroristic action remediation plan to be applied to areas affected by past activities, accidents or terroristic attacks, characterization of the site is a mandatory step. This activity will determine the extent of the contamination, contaminants' distribution, etc. Traditionally, this activity involves the collection of different environmental samples and laboratory analysis of the relevant radio nuclides (and eventually other contaminants like heavy metals). When the results are available they are interpreted and then a decision is made. This process is normally very expensive and time consuming. In recent years many techniques have been made available for in-situ measurement that can provide reliable information on the contamination profile in radiological contaminated land. Such measurements tend to be less expensive, faster and with the aid of GPS/GIS systems decisions can be made on-site in real time. To overcome this situation we developed the DACM (Data Acquisition and Control Module) technology. Instruments based on this technology can be modified anytime by the user without special knowledge and the claiming of the manufacturer.
The DACM based offers a set of components which can be configured, parameterized and controlled with respect to the requirements on site. Typical components are signal inputs for sensors like Co_2, Methane, So_2.., control outputs for instance for pumps, magnetic valves but also complex functional blocks like spectrometers, GPS receiver, PID regulators etc. A complex sampling schedule can be created within few minutes by a graphical software interface.
One version of this system is the NucScout as a handy and robust 2“ x 2“ (optional 3”x3”) NaI(Tl) Nuclide Identifier and quantifier. With less than 2 kg including GPS and ZigBee wireless connection, if the device is operated in inaccessible or contaminated areas, he can be so calibrated by use in 1 m high from the soil, that he shows direct the nuclide activity in Bq/kg. So you can get with a time resolution of 10 sec and a speed of 1 m/s a local resolution of 10 m and you can detect a specific activity less than 200 Bq/kg soil activity on the surface.
The NaI(Tl) detector is also used to analyze food and material probes regarding specific nuclides (e.g. Iodine, Cesium, and Americium). By means of the gamma spectrum, the net activity of six user definable nuclides is automatically calculated.
A version with an aerosol sampling head with its spectroscopy filter and its silicon detector samples continuously and detects even small quantities of aerosol carried radioactivity. Both alpha and beta radiation are measured. The spectrometric analysis allows e.g. detecting Plutonium aerosols which cannot be detected by measuring gamma radiation.
Optionally, the DACM can be connected to a portable vacuum chamber with Ion-implanted Silicon detector up to 2000mm², to allow on-site analysis of mop tests and other samples under circumstances similar to those prevailing in a laboratory. The employed vacuum pumps can be connected to a 12V source (car battery
All detectors can be operated simultaneously. The concept of the system allows an easy handling and a standardized data basis.

Keywords: radiation detection, surface contamination, gamma spectrometry, radiological terrorism, nuclear accidents,

1. Introduction

As part of an environmental remediation plan to be applied to areas affected by past activities and accidents, characterization of the site is a mandatory step. This activity will determine the extent of the contamination, contaminants' distribution, etc. (see IAEA Safety Guide No. WS-G-3.1 – Remediation Process for Areas Affected by Past Activities and Accidents). Traditionally,

this activity involves the collection of different environmental samples and laboratory analysis of the relevant radionuclides (and eventually other contaminants like heavy metals). When the results are available they are interpreted and then a decision is made. This process is normally very expensive and time consuming. In recent years many techniques have been made available for in-situ measurement that can provide reliable information on the contamination profile in radiological contaminated land. Such measurements tend to be less expensive, faster and with the aid of GPS/GIS systems decisions can be made on-site in real time. Many States facing the challenge of implementing environmental remediation projects do not have adequate analytical infrastructure for site characterization. They will then need to make this available prior carrying out site characterization efforts. Therefore the place of remedial works implementation will be reduced or these activities will not be implemented at all. Mobile units may also be useful to member states who do have laboratory analysis facilities, but are faced with large, unforeseen characterization challenge, such as following and accident or radiation emergency.

2. Nuclide specific Gamma spectrometry

The NucScout (see Fig.1) is a handy and robust 2“x 2“(optional 3”x3”) NaI(Tl) The objective of the mission was to assess the efficacy of the remediation actions undertaken in a site that were contaminated in the past with NORM (high Radium content in charcoal used as absorber for Iodine production) in regard to surface radiological hazards. A remediated area was analyzed by mobile devices. Mobile Unit demonstration activities were performed in the vicinity of Baku, Azerbaijan [1].

Nuclide Identifier and quantifier. With less than 2 kg including GPS and ZigBee wireless connection he can be so calibrated by use in 1 m high from the soil, that he shows direct the nuclide activity in Bq/kg from up to 6 nuclides, which can be chosen from a big nuclide library with more than 50 nuclides. So you can get with a time resolution of 10 sec and a speed of 1 m/s a local resolution of 10 m and you can detect a specific activity less than 200 Bq/kg soil activity on the surface (see Fig 2).
The measured value showed that in this case the 200 Bq/kg was only a little bit higher in areas which were till now not remediated.

Fig.1 NucScout with wireless 2.4 GHz ZigBee Data transfer

Fig 2 NucScout screening measurement of Bi214 (Bq/kg) soil activity from a location in Azerbaijan

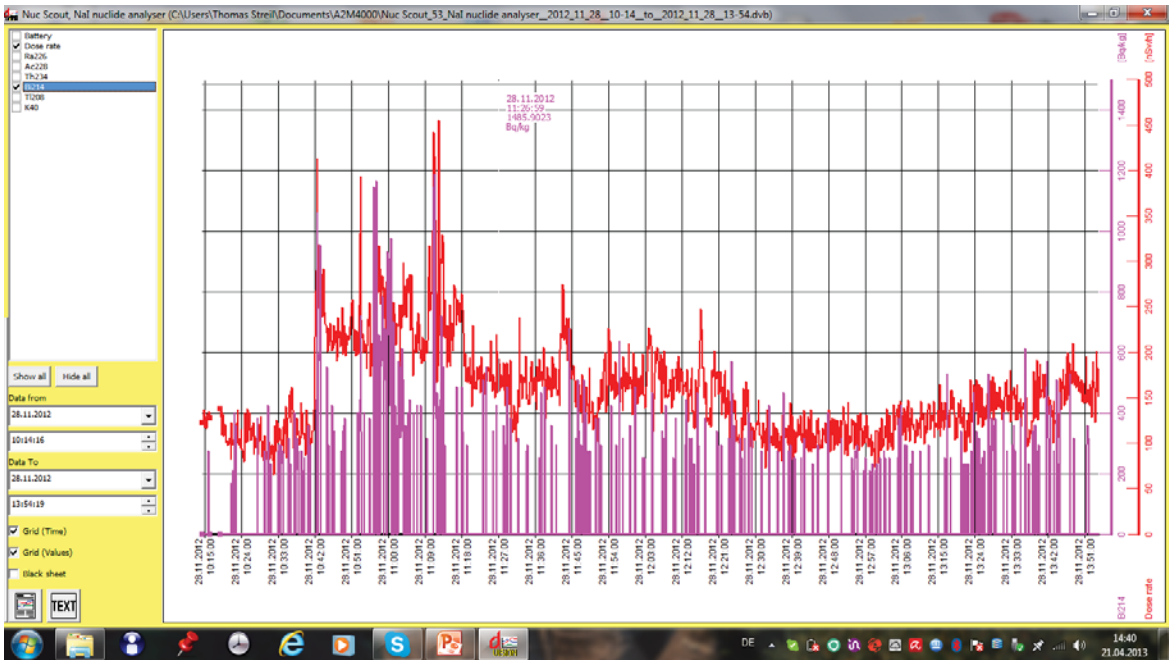


Fig 3 show a slightly increased surface soil activity in a deposit for the contaminated material, which was not fully covered by protective soil layers.

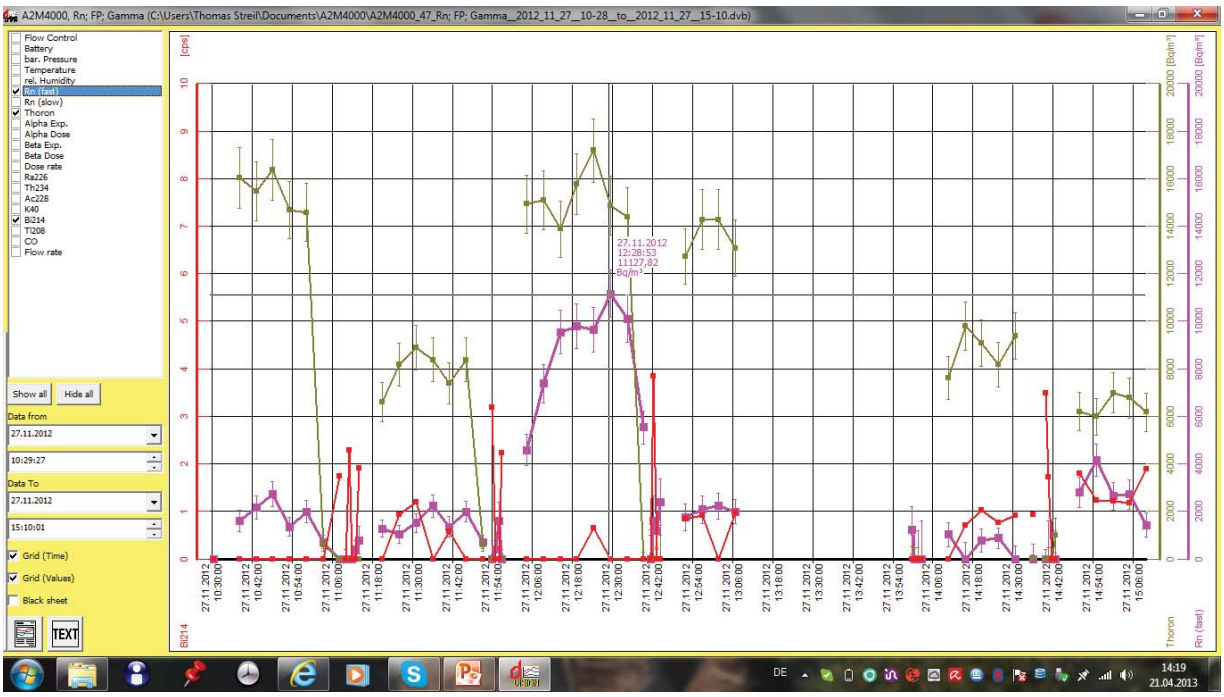


Fig 4 Radon /Thoron soil gas activity and the Bi214 count rate of the screened area in Azerbaijan

In fig 4 is shown like with a A2M 4000 area monitor in a short time can be measured several data. The comparison of the Bi214 count rate and Radon soil gas concentration is in a good agreement. The data show also that in covering material (after remediation process) the Thoron concentration is a little bit higher because of natural small increased Thorium concentration in this soil material. But the dose rate of 200nSv/h was in the examined area not extended.

3. Conclusion

The used mobile devices for site Characterization in environmental remediation projects from NORM material (high Radium content in charcoal used as absorber for Iodine production) show the possibility in less than 2 days to examine an area of more than 30 ha. Such mobile systems are also possible to use for the characterization of the contamination after terroristic attacks (dirty Bombs) or nuclear accidents like Fukushima. The new DACM technology allows creating device with special customer specifications. This is a big step to reduce the time a cost consuming lab procedures and show in time the results.

REFERENCES

[1] IAEA report “Results of surface radiological characterization of past NORM contaminated sites of Ramana and Surakhany” 26-30 November 2012, Azerbaijan

[2] Private communication Miroslaw Janik, Ph.D. National Institute of Radiological Sciences (NIRS),4-9-1 Anagawa, Inage-ku, 263-8555 Chiba, Japan, e-mail: mirek@fml.nirs.go.jp

INDEX OF AUTHORS

INDEX OF AUTHORS

INDEX OF AUTHORS

INDEX OF AUTHORS

EDITORIAL NOTES

Editors

Jürgen Beyerer, Andreas Meissner, Jürgen Geisler

Contact

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
Fraunhoferstrasse 1
76131 Karlsruhe, Germany
www.iosb.fraunhofer.de

Marion Staub
Press and Public Relations
Phone +49 721 6091-333
E-Mail presse@iosb.fraunhofer.de

Layout Christine Spalek, Fraunhofer IOSB

Conference host

Fraunhofer Group for Defense and Security
www.vvs.fraunhofer.de

Bibliographic information published by Die Deutsche Bibliothek

Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliografic data is available in the Internet at http://dnb.d-nb.de.

ISSN 2364-3986

ISBN 978-3-8396-0908-8

Fraunhofer Information-Centre for Regional Planning and Building Construction IRB
P.O. Box 80 04 69, D-70504 Stuttgart
Nobelstrasse 12, D-70569 Stuttgart
Phone +49 711 970-2500
Fax +49 711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

Druck und Bindung
Konrad Triltsch Print und digitale Medien GmbH, Ochsenfurt-Hohestadt

ISBN 978-3-8396-0908-8