Fraunhofer
VVS

Future Security
Security Research Conference

FRAUNHOFER GROUP FOR DEFENSE AND SECURITY VVS

SECURITY RESEARCH CONFERENCE 11TH FUTURE SECURITY

BERLIN, SEPTEMBER 13–14, 2016
PROCEEDINGS

Oliver Ambacher, Rüdiger Quay, Joachim Wagner (Eds.)

FRAUNHOFER VERLAG

FRAUNHOFER VVS

SECURITY RESEARCH CONFERENCE 11TH FUTURE SECURITY

BERLIN, SEPTEMBER 13 – 14, 2016 PROCEEDINGS

Oliver Ambacher, Rüdiger Quay, Joachim Wagner (Eds.)

PREFACE BY THE EDITORS:

CURRENT STATE-OF-THE-ART OF SECURITY RESEARCH AT FUTURE SECURITY 2016

We are proud to present to you the proceedings of the Future Security Conference 2016. For the 11th time this well-established, prestigious conference series brings together diverse stakeholders of the safety and security community. This conference has become the top forum for addressing security research, a topic of increasing importance and relevance to all of us, in a holistic inter- and multidisciplinary approach.

Having covered a wide range of security research aspects over the past years, this year´s conference has a special focus on sensors and sensing networks for safety and security. Among a great variety of technical sessions on sensors and sensor networks, border security, protection of critical infrastructures, and safety and security for Industry 4.0 – just to mention a few of the session headlines – Future Security 2016 features two special sessions: one on the security aspects of autonomous driving and the other on airport security, two areas which strongly benefit from advanced sensors and sensing systems.

This year's conference comprises a total of 87 technical papers of excellent quality, presented in 15 oral sessions and one poster session. Of these papers, 73 have been submitted as proceedings papers contained in this volume. We would like to thank all members of the program committee for their help and support in putting together an excellent conference program, as documented in this proceedings volume. Besides printed copies, the proceedings of the 11th Future Security Conference 2016 are also available electronically in an open access format via Fraunhofer e-prints (http://eprints.fraunhofer.de), which further increases their accessibility and hence their impact.

At this point we would like to thank everyone who has contributed to the success of Future Security 2016, making this conference such a successful event.

The Editors
Oliver Ambacher (Conference Chair)
Rüdiger Quay (Program Chair)
Joachim Wagner (Program Chair)

PROGRAM COMMITTEE

Prof. Dr. Oliver Ambacher
Fraunhofer IAF

Prof. Dr. Jürgen Beyerer
Fraunhofer IOSB

Dr. Antje Bierwisch
Fraunhofer ISI

MinR Gerhard Coors
Federal Ministry of Defence BMVg

Prof. Dr. Claudia Eckert
Fraunhofer AISEC

Prof. Dr. Peter Elsner
Fraunhofer ICT

Achim Friedl
Director of the German Federal Police retd.

Prof. Dr. Hans-Joachim Grallert
Fraunhofer HHI

Prof. Dr. Albert Heuberger
Fraunhofer IIS

Prof. Dr. Stefan Hiermaier
Fraunhofer EMI

Dr. Rüdiger Klein
Fraunhofer IAIS

Dr.-Ing. Peter Knott
Fraunhofer FHR

Prof. Dr. Dr. Michael Lauster
Fraunhofer INT

Peter Löffler
Siemens Switzerland Ltd.

Prof. Dr. Peter Martini
University of Bonn

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

Dr. Harald Niggemann
Federal Office for Information Security BSI

Dr. Henric Östmark
FOI - Swedish Defence Research Agency

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

Dr. Rüdiger Quay
Fraunhofer IAF

Prof. Dr. Christopher Schlick
Fraunhofer FKIE

Prof. Dr. Viola Schmid
TU Darmstadt

Frank Schnürer
Fraunhofer ICT

Gunther Schwarz
BDSV, Airbus Defence & Space

Matthias Steil
Federal Ministry of Defence BMVg

Prof. Dr. Klaus Thoma
Fraunhofer EMI

Thomas Tschersich
Deutsche Telekom AG

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

Prof. Dr. Joachim Wagner
Fraunhofer IAF

MinR Norbert Weber
Federal Ministry of Defence BMVg

Dr. Karin Wey
VDI Technologiezentrum GmbH

TABLE OF CONTENTS

PROCEEDINGS

Keynote

Special Session: Autonomous Driving - Security

Session 1: Border Protection and Control

Session 2: Sensors and Sensor Networks

Session 3: Protection of Critical Infrastructures I

Session 4: Crisis Management

TABLE OF CONTENTS

Session 5: Protection of Critical Infrastructures II

Session 6: Safety and Security for Industry 4.0

Session 7: Detection of Explosives, Chemical and Biological Threats

Session 8: Protection of Critical Infrastructures III

Session 9: Data Protection

Session 10: Video, Image, and Sensor Signal Processing

Session 11: Detection and Interdiction of UAVs

TABLE OF CONTENTS

Session 12: Smart Infrastructures (Smart Cities, Internet of Things)

Special Session: Airport Security

Poster Session: Extended Abstracts

SENSORS AND NETWORKS FOR PROTECTION AND SECURITY

Ryszard Bil[1] and Markus Hölscher[2]

[1] *ryszard.bil@airbus.com*
Airbus DS Electronics and Border Security, Wörthstraße 85, 89077 Ulm (Germany)

[2] *markus.hoelscher@airbus.com*
Airbus DS Electronics and Border Security, Wörthstraße 85, 89077 Ulm (Germany)

Abstract

This paper addresses various aspects of sensors and networks for protection and security, starting with para-public agencies and then diving deeper into sensor networks followed by the security surrounding individual sensors and products themselves. Some examples of key modern technologies are also addressed, including Unmanned Air Vehicles (UAVs) and counter-UAV systems. A key aspect is the need for interaction between agencies, users and sensors and the need to ensure a secure production and maintenance environment for the sensors. The paper does not intend to provide answers to a multitude of current issues, but rather to trigger some thought and discussion on the problem environment and potential solutions.

Keywords: Protection, security, networks, sensors, autonomous.

1 INTRODUCTION

This paper begins with the motivation driven by increasing needs for protection and security and the respective necessary, comprehensive, cooperative approach of involved stakeholders. This will be followed by deriving the benefits of timely, realistic situational awareness and the pivotal role sensor usage plays. Based on the shown sensor importance, the related supply chain and challenges to protect its integrity will be elaborated. From these rather generic considerations, some thoughts about the enabling capabilities to operate autonomous vehicles, as well as provide protection against them, lead to some brief conclusions about the challenges using growing volumes of sensor data.

The flyer for this event states that “it becomes increasingly challenging to maintain or to increase our standard of protection and security even further, given the great challenges and current threats Europe is facing”. These threats, or potential threats, arise beyond European Union (EU) borders as well as from within the EU; and at this time in history, rather many simultaneously, e.g. refugee movements, terror threats in home countries, asymmetric conflicts in failed states with increasing numbers of (militarily potent) stakeholders and hybrid conflicts. Besides the importance of sensor (network) information to prevail as a party in conflicts, it is often valuable to be able to prove specific details of (politically) important situations (e.g. the shooting down of the Malaysian airliner over Ukraine) over large distances. This can contribute to the containment of potential crises right at the very beginning.

2 PARA-PUBLIC AGENCIES & INFORMATION EXCHANGE ENABLED BY SENSOR NETWORKS

The meanwhile usually “mixed character” of crises requires a cooperative approach of different state organizations. The related state actors dealing with these challenges need related capabilities to “Uphold and restore the necessary level of safety and security we are accustomed to.” Meanwhile usually more than one organization is tasked to cope with challenges following a comprehensive approach that considers all available means.

Effective cooperation requires automated (technical) networks connecting all stakeholders as a prerequisite to sharing collected information. This is the mandatory basis to enable an educated decision right up to the highest hierarchical levels. Relying on separated information domains bears the risk of diverging perception of the singular reality resulting in organizations being “out of sync” with likely insufficient and ineffective results.

Related operational processes exist and are outlined in various occurrences. A basic scheme you likely all know is the SEE – UNDERSTAND – DECIDE – ACT (SUDA) principle. This approach is based on the gathering of all available kinds of data – the SEE – about the reality (= current AS-IS situation). Besides various elements of information about the environment, cultural topics, language, plans of infrastructure, intelligence data and many more, sensor information is an extremely important contribution to provide data in real time about “who (sometimes only “something”) is where and moving towards there”.

Being part of a network ensures that this information can be used instantaneously by all network participants, assuming data sharing as a leading operational principle – which is unfortunately often not the case. Critical data for the benefit of, for example, the EU as a whole is still a “currency” used for trading. As so often demonstrated in the recent past, the latter often reduces the overall timely efficiency of appropriate and pro-active measures, such as 9/11, the Paris attacks or the Brussels bombing. All this information, being evaluated, assessed and appropriately shared, leads to a level of sufficient situational awareness – the UNDERSTAND element and is the basis for developing suitable courses of action. Without sensors it is difficult to get an adequate level of precision leading to an incomplete perception of the AS-IS situation and subsequently to suboptimal decision-making – the DECIDE element. Choosing means/effects – the ACT element – to get a step closer to a SHOULD-BE situation, based on poor quality information could lead to negative results (e.g. collateral damage as individuals have not been sensed) sometimes deviating from the desired SHOULD-BE situation.

A good cooperation example of organizations from different domains is the participation of North Atlantic Treaty Organisation (NATO) naval forces for surveillance purposes in the Mediterranean, supporting the detection of refugees with their sensor equipment (and providing related Search and Rescue support). Such a border control task is not the typical main military task, but the available capabilities provide significant benefit for the mission.

On the other hand, it also became extremely visible that the lack of capability to oversee large areas (at the beginning) of the refugee movements resulted in late reaction activities and many individual tragedies.

To contribute to a sufficient SEE element “it requires the development and implementation of innovative technical solutions such as intelligent sensing systems and sensor networks. These hold the promise that hazards and threats can be detected early enough to avoid severe adverse impact.”

“Early enough” and additionally widespread under all environmental conditions is the mandatory precondition for all operational forces to generate a sufficient level of situational awareness to be able to act in an ideally optimal manner, pro-actively thought out, and not only limited to react. In this manner sensor (network) usage (=surveillance) is a focal contribution to protect own personnel and resources by preventing dangerous surprises and ensure keeping the operational initiative. This is not only true for (usually strategic or operational level) early warning systems (e.g. NATO Airborne Warning & Control System (AWACS)) but also for nearly all stakeholders / levels involved in security, crisis or military missions.

Advances in sensor and Information Technology (IT) allow rapid adoption to effectively share information to such a degree, that security, crisis response or military missions are increasingly well supported/supportable by technical solutions in nearly all functional domains such as surveillance, command & control, effects and support. The expected benefit is a greatly improved level of situational awareness by means of increased speed of information flow and quality of information. Besides the rarely sufficient bandwidth of necessary communication systems, the vast amount of available information and fast update cycles become a challenge in their own right. Preventing the limited numbers of personnel from drowning in too much information requires intelligent means to filter and aggregate information necessary to be able to exploit information superiority. Eventually this capability has to be integrated into the sensor systems to exploit the advances in sensor technology even under suboptimal bandwidth conditions.

3 THE IMPORTANCE OF SENSOR TECHNOLOGY

The importance of sensor technology is reflected in the perception as a nationally relevant technology focus area in many countries. The necessary technologies and their related supply chain are available in-country as a focus area to ensure access to the latest technologies and subsequently independent decision-making, including asking for permission to procure and/or use related assets.

In order to be able to ensure future (security) sensor technology, the cooperation of the scientific community, industry and the user (organizations) are important to cope with the fast changing operational environments. The relevance of access to the full supply chain is underlined by several national activities to establish such supply chains for specific sensor technologies, e.g. radar, optronics and electronic support and countermeasures.

Meanwhile the rapid and cost-efficient technological developments for civil markets often set the trends, later followed by security and military applications. This is a (not new but) major difference compared with the situation in the past (e.g. first automotive radars were a spin-off from military radars)

<u>What are the consequences?</u>

- Cheaper components ➔ Makes it cost attractive
- Available for everybody ➔ No operational advantage

  ➔ International supply chain

  ➔ Difficult to assure (cyber) security
- Rapid obsolescence ➔ Different approach for maintenance necessary

  ➔Potentially new administrative processes to speed up decision-making for procurement
- Characteristics for the main (commercial) market (volume wise)

  ➔ Difficult to get realization of often more specific requirements for security and military needs

  ➔ Tendency of insufficient focus on high level of (cyber) security

4 SENSORS & THEIR INDUSTRIAL ENVIRONMENT

So far we have considered aspects such as networking between nations and their respective agencies and organizations responsible for safety, security and defence to ensure a high level of effectiveness. We have also considered the importance of the SUDA reaction chain and the very important contribution that sensors and sensor networks contribute to the overall safety and security situation.

Next we need to consider the vulnerability of the sensors and their production and supply chains themselves, especially as we move ahead into the so-called digitization or production

4.0, with its highly integrated digital functional chain. How safe and secure are the sensor products themselves, or their production and maintenance infrastructure? Too often we have heard about doctored USB sticks and malicious code infiltrating the industrial infrastructure which is supposed to provide key sensor technology, which should be inherently safe and secure as a basis for the SUDA reaction chain.

The related challenges are becoming more and more obvious. The national armed forces are building up their own service organizations to cope with this operational dimension. On the industry side the implications are immense, not only since STUXNET became known to the public. Due to the fast innovation cycles of commercial IT, hardening against cyber threats is a challenge in its own right, to ensure the integrity of products as well as the production means at all levels of the involved suppliers. This is not only about software related threats but also ensuring the integrity of related hardware (components). To make a complex story even more challenging – it is not only about technology. The human factor as an important intrusion vector adds to the complexity too and so requires that stand-alone IT systems become objects of cyber-hardening also, e.g. via ground stations or any other hardware with (manually) accessible interfaces. This is reflected in upcoming national security regulations, which impose specific methods and tools to industry dealing with defence and security business. Or even further, legal requirements, such as the recently implemented additions to the DFARS in the USA. In case of incidents respective customers want to get the right to inspect IT infrastructures of organizations. The implications can result in clashes of contradicting legal and national regulations until an internationally harmonized approach is settled.

These challenges are as relevant for traditional IT systems as for sensor systems, the latter incorporating a good deal of software and being interfaced with either platforms or wider system setups. This implies attack vectors potentially threatening the sensor (results). The results of e.g. spoofed sensor data (= not instantaneously detected dedicated wrong information) can lead to a “biased” situational awareness picture with eventually fatal consequences, due to decisions based on incorrect or poor quality information.

Therefore, if the lives of personnel depend upon the integrity of the used equipment (sensors and sensor networks), the necessary measures to ensure the respective protection have to be undertaken. These range from safe components along the supply chain (= check you get what you want and no more) to security considerations starting with the system design up to organizational means, e.g. digital rights management for malware detection to counter the well-known digital hijacking of an SUV while being driven. Whether certifiable standards with guaranteed and quantifiable protection levels against security and cyber threats can be found is uncertain, due to the many unknown unknowns in a fast evolving technical environment. Defined trust remains one of the best methods.

5 AUTONOMOUS VEHICLES & COUNTER-UAV SYSTEMS AS AN EXAMPLE

The need for probably different security and cyber protection levels can be discussed for the very different application areas e.g. for autonomous vehicles. While all Unmanned Air Vehicles (UAVs) strictly have to comply with safety regulations, hardening against hostile capturing should be thought about more deliberately in detail. Due to the potential consequences, the “capturing” of military, potentially armed UAVs has to be prevented by all means, whereas private or other civil applications can perhaps be operated with a more cost effective protection level.

Moving on to considerations about a more specific domain - the protection and reliable use of autonomous systems, especially autonomous vehicles is becoming more important. The upcoming use of automated platforms is highly visible, as known from several announcements for autonomous cars, parcel delivery drones as well as the discussion around autonomous (military) UAV systems. The latter have also highlighted the lack of related regulations as necessary preconditions for official usage.

The existing regulations were often based upon the capabilities of the human operator (e.g. a pilot). Trying to map this scheme to a machine can leave out the (easy to implement) potential of technical means (due to stricter regulation) or significantly increase the effort to realize some human capabilities (one by one), that could easily be substituted by other technical means. A conscious definition to balance the capabilities and difficulties according to a desired, high security level is necessary.

Many such capabilities involve sensing the environment by means of a variety of sensors. The level of performance for security and military purposes can vary significantly compared to civil applications. A semi-autonomous private car today can generate an impressive level of situational awareness around it with (meanwhile) quite cost effective built-in sensors. In the future, such cars will potentially rely on additional information provided by an infrastructure network.

Vehicles for security or military use often have more complex requirements since they operate in less structured, harsh environments and may not rely on an available support network.

Nevertheless, independent of the performance level of the used sensor equipment, they enable the respective platform to operate and protect it in the first instance against bumping into something else (also protecting the "something else"). This provides the basis to be able to be integrated into transportation networks without dangerous interference. Examples are navigation aids like Global Positioning System (GPS) for reliable integration into regulated air space or upcoming Sense and Avoid sensor systems, usually radar systems, often complemented with electro-optical components for UAVs. These detect all elements around a platform with the intent to discriminate between environmental elements like clouds or flocks of birds and other platforms. In addition, a sensor payload is often applied to or integrated within the platform. Again, security and especial military needs like all-weather, remote, large area surveillance is probably rarely found in civil requirements.

Without the need to host a pilot the platform can be reduced in size and weight with impact on (=reduction of) the payload characteristics. Advances in technology allow the reduction of the overall sensor size and volume, reducing antenna size allowing structure integration and combining the functionalities of various, so far single purpose Radio Frequency (RF) sensor systems, such as radar, electronic support and countermeasures, as well as communications, into integrated multifunction RF sensor systems. This could lead for example, to a sensor that provides surveillance and imaging (Synthetic Aperture Radar) capabilities as well as electronic support and countermeasures. The latter are often seen as dedicated military capabilities, but the importance and widespread use of electronic communication systems especially in the civil and para-public domains, means there is an increased need of availability also for non-military organizations.

Dedicated sensors detecting threats of a different nature, e.g. "kinetic" or energy (=laser) threats for the platform, also supporting the integrity of an Unmanned Air System (UAS). Examples are warning capability against helicopter rotor strike or detection of various kinds of attacking missiles (e.g. man pads or laser beam rider). All of these threats are unfortunately no longer restricted to pure military conflict. Having mentioned many kinds of sensors it is probably clear that the trend is clearly towards platforms equipped with multiple sensors, at least in non-civil application domains.

Unfortunately UAVs, being easily available today, may not only be used with good intentions. As quite a new phenomenon, misuse of the mobility and low observability are still a challenge to counter. Incidents in the last months involving (small) unmanned aerial vehicles (UAV) (e.g. apparent collision with an airliner at Heathrow, the crash near an alpine skier at a championship race, observation of nuclear plants or public political events (with Chancellor Merkel and other government members)) underline the potentially dangerous capabilities of such drones but also the current capability gap of sufficient warning and protection. Thank goodness, so far no major damage has occurred and various activities around counter-UAV systems have been started.

Of course sensors are once again an important element of such systems needed to detect small threats, often without much metal inside (= few/weak reflections) against clutter rich backgrounds at sufficient ranges to ensure a timely response. The “right” sensor choice – and there are many potential choices – is highly dependent upon the operational environment, the available budget and the desired results. Requiring sufficient reaction time (assuming hard kill effects are no option in many non-military domains), the detection of challenging threats at several kilometres and in all-weather conditions requires different (=Radar) sensors than short range detection systems, which are perhaps possible to realize with (low cost) optical or acoustic sensors.

Such systems should provide a simple user interface and important characteristics such as low false alarm rates. That is, birds and small objects, most often built without metal, should not trigger such systems, which in turn implies the need for reliable classification means that can be e.g. acoustic or optical sensor based. Such classification becomes even more necessary, when emerging civil UAV applications (e.g. parcel or emergency medicine delivery) becomes a normal encounter.

Having addressed the enabling sensor capabilities for UAS operation as well as necessary characteristics of sensor based systems to protect against them, let’s have a brief look how UAS’ are embedded in an operational infrastructure.

The many potential sensors in a single platform are usually connected through a network (e.g. in NATO AWACS). The complete UAS can also be participating in a higher level network connecting other sensors / platforms and being itself part of another network (level), creating a complex scenario needing dedicated management processes. Each network should ideally be composed according to the needs of the operational environment and made up from sensors of different types and origin. This is not a trivial requirement! A key prerequisite is the definition and use of standard interfaces across various (national) customers and multiple (industrial) providers in a limited and not so agile market.

In the past pre-planned single provider networks were set up e.g. the US SOSUS sensor network. Pre-planned networks using dedicated (tactical) data link standards are in use today. To ensure the needs and capabilities of different sensors in ad hoc networks are met, the technology will not be a bottleneck if the “structuring” conditions are clearly set. From a sensor (provider) perspective the demanding operation of networks should be transparent for the participating sensor.

The availability of more and more sensor information available via networks creates an increasing demand to process all that (sensor) data. In order to automatically create a coherent picture of the current situation, data fusion technologies are being developed further. Being able to handle more data types, the future will eventually see adaptive and learning systems. Cognitive sensors will allow the reduction of manual user sensor management by automatic adaptation of equipment parameters according to environmental and mission characteristics. The trend of relocating more functionality to the sensor itself does not neglect the need for sophisticated ground/mission evaluation systems. In the future, new user needs will also require some manual analysis of data and information, at best using common systems for identical tasks, preventing diverging data interpretation caused by differently implemented functionalities.

6 CONCLUSIONS

With this support of sensible manual sensor data evaluation and the future outlook on more intelligent, automated sensor data processing, let us close this extremely wide, varied and challenging topic of security and protection in various operational environments.

It is hoped that the importance of sensors and “their” networks for protection and security has been demonstrated. There is still an incredible amount to do to make some of the mentioned possibilities reality. To achieve a high level of security, all the resources of the institutes, of industry and the various state organizations are necessary. To maximally benefit from these individual contributions a high level of open cooperation is necessary, following common or at least known and understood objectives.

There is a huge amount of work, with all its challenges, that remains ahead for all the stakeholders.

FALLBACK STRATEGY AND SAFETY ANALYSIS FOR AUTOMATED DRIVING

Thomas Raste

[1] thomas.raste@continental-corporation.com
Continental, Division Chassis & Safety, Competence Center Global Chassis & Motion Control, Guerickestr. 7, 60488 Frankfurt / Main (Germany)

Abstract

A potential fallback strategy for automated driving is stopping the car in case of an emergency without environment sensors. The autopilot needs to be fault tolerant with redundant paths for motion control, steering and braking. The new System Theoretic Process Analysis (STPA) method is applied for safety analysis and provides insights that the redundancy adds more interactions into the system but will not eliminate the unsafe control actions by itself.

Keywords: Automated Driving, Motion Control, Fallback Strategy, System Theoretic Process Analysis

1 INTRODUCTION

Automated Driving will be a key element of future mobility, as it will enhance the safety, efficiency and comfort of individual mobility even further. Automation will lead to a significant decrease in the number of road traffic casualties and it allows drivers to use their time in the car in other ways and therefore more efficiently.

The complexity of the automated driving socio-technical system is a major challenge for automotive manufacturers, system suppliers and the legal framework. System safety is the indispensable basis on which automated driving must be built. The development of the E/E architecture is compliant to the ISO 26262 standard. The safety concept has to account for the fact that the driver is out-of-the-loop and therefore cannot achieve a safe state. For a short period of time, e.g. until a safe stop, the system has to be fail operational. The appropriate means are redundancies in the motion control with braking and steering. One of the last possible degradation is the fallback strategy to come to a safe stop. The strategy is allocated in a backup brake module.

The System Theoretic Process Analysis (STPA) was performed to develop a safety concept for the safety-critical fallback strategy. The analysis starts with the system-level goals, requirements and constraints of the fallback strategy. A hazard and risk analysis preceding the STPA is used to determine the hazards and high-level safety goals. To focus on failure events and adding redundancy to prevent them is not sufficient to account for hazards which arise from interactions among fault-free components. Especially time delays are crucial regarding the stability and performance of the motion control.

The STAMP/STPA method is well suited to deal with the complex feedback loops necessary for automated driving in general and in particular the fallback strategy. The method provides the causal factors for unsafe control actions leading to hazards. The causal factors in turn provide the safety requirements according to the ISO 26262 norm. Based on the STPA method effective safety measures to the architecture are provided in a very early phase in the development without knowing every detail of the system.

Research is currently under way to test that the system theoretic causality model may benefit security the same way it is benefitting safety. With STPA-SEC, the method can also be applied to identify system vulnerabilities prior to a cyber security attack.

2 AUTOMATED DRIVING STRATEGIES AND BUILDING BLOCKS

2.1 Strategies and Levels of Driving Automation

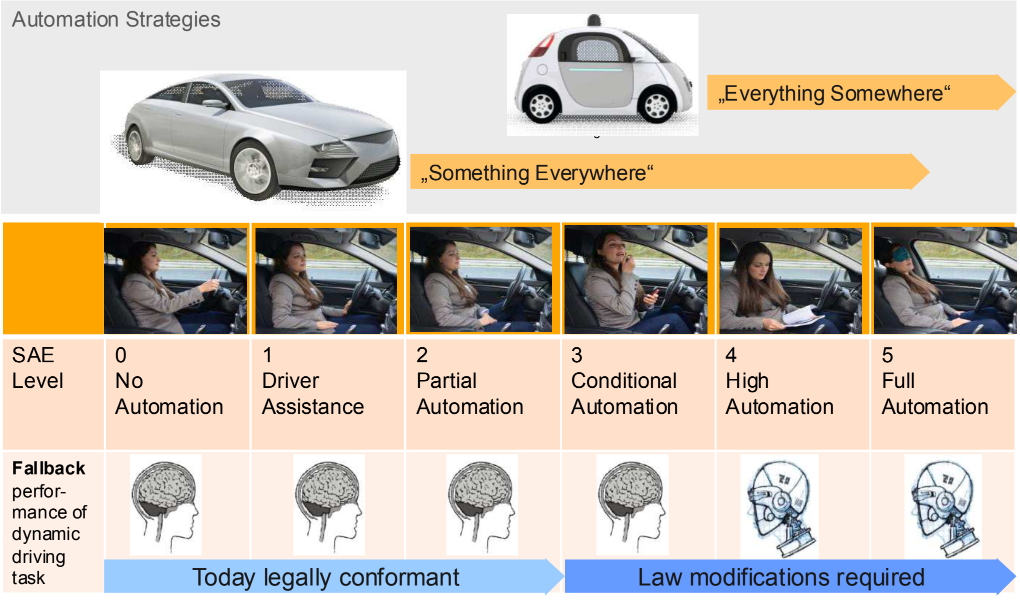
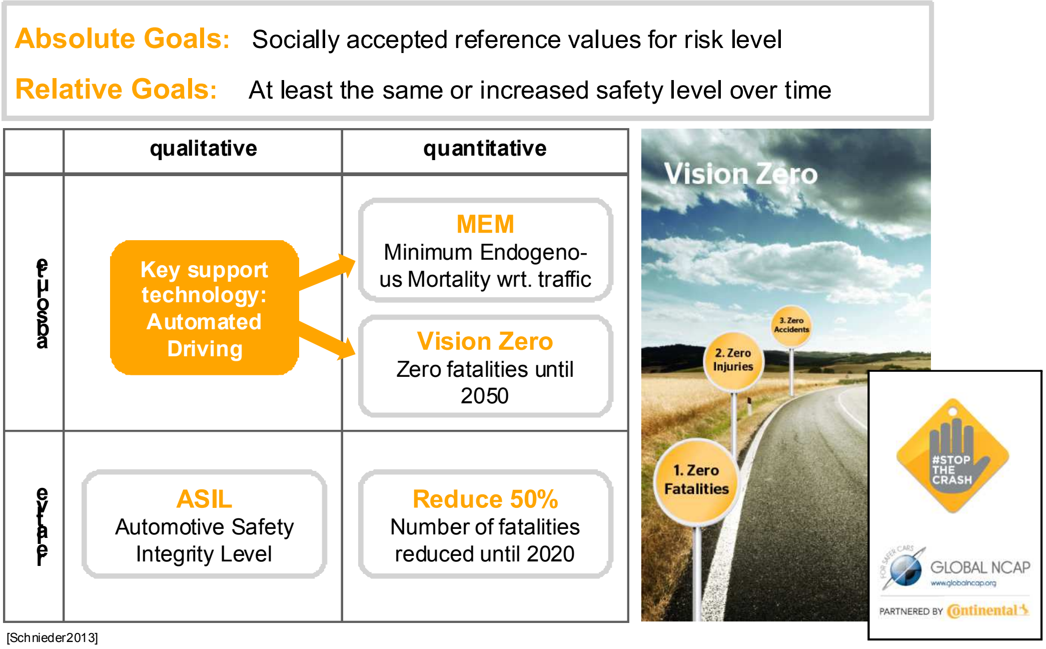


Fig 1.: Strategies and Levels of Driving Automation

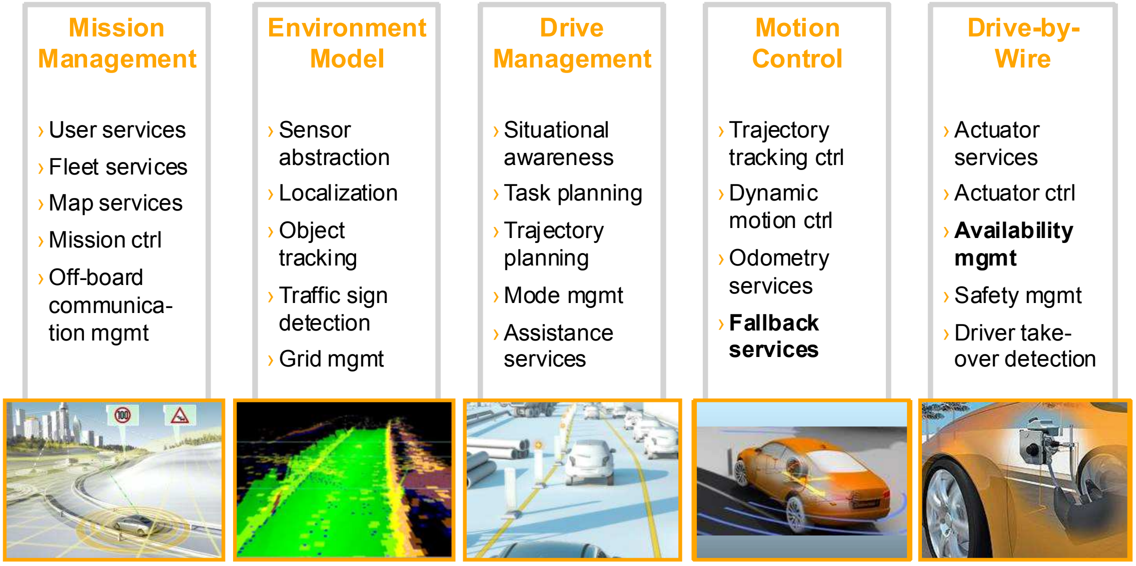
2.2 Road Safety Goals


Absolute Goals: Socially accepted reference values for risk level
Relative Goals: At least the same or increased safety level over time
qualitative
quantitative
absolute
relative
Key support technology: Automated Driving
MEM
Minimum Endogenous Mortality wrt. traffic
Vision Zero
Zero fatalities until 2050
ASIL
Automotive Safety Integrity Level
Reduce 50%
Number of fatalities reduced until 2020
Vision Zero
1. Zero Fatalities
2. Zero Injuries
3. Zero Accidents
#STOP THE CRASH
GLOBAL NCAP
www.globalncap.org
PARTNERED BY Continental

[Schnieder2013]

Fig 2.: Road Safety Goals

2.3 Building Blocks for Automated Driving



Mission Management
- User services
- Fleet services
- Map services
- Mission ctrl
- Off-board communication mgmt

Environment Model
- Sensor abstraction
- Localization
- Object tracking
- Traffic sign detection
- Grid mgmt

Drive Management
- Situational awareness
- Task planning
- Trajectory planning
- Mode mgmt
- Assistance services

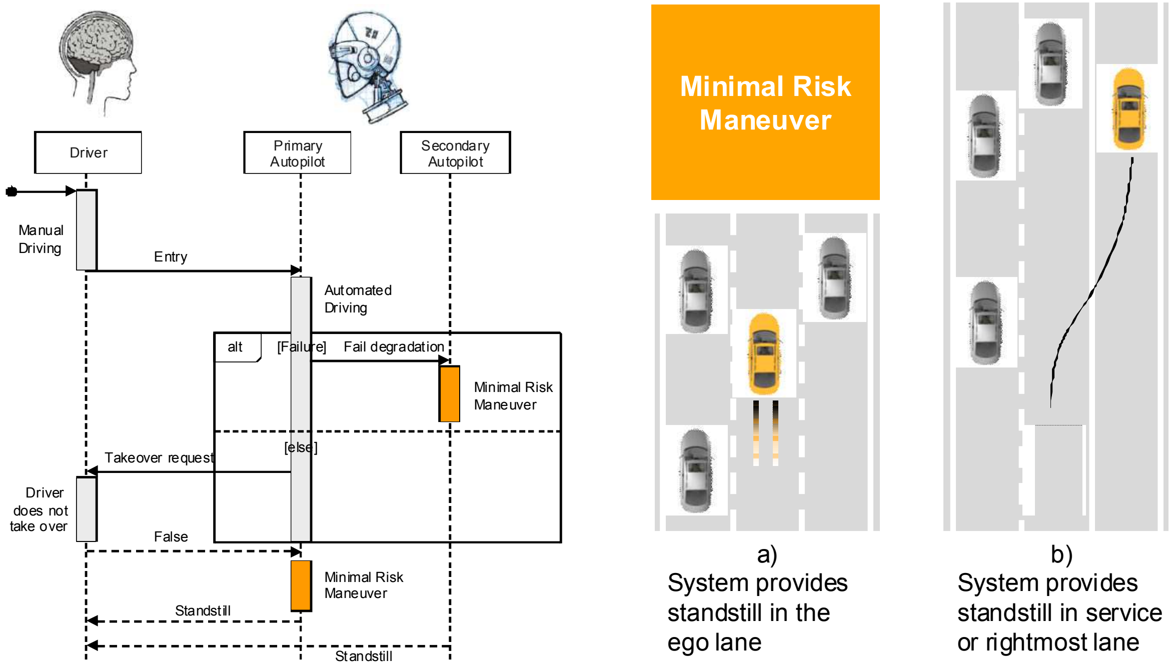
Motion Control
- Trajectory tracking ctrl
- Dynamic motion ctrl
- Odometry services
- **Fallback services**

Drive-by-Wire
- Actuator services
- Actuator ctrl
- **Availability mgmt**
- Safety mgmt
- Driver take-over detection

Fig 3.: Building Blocks for Automated Driving

3 FALLBACK STRATEGY CONCEPT AND PERFORMANCE

3.1 Minimal Risk Condition as Fallback Strategy

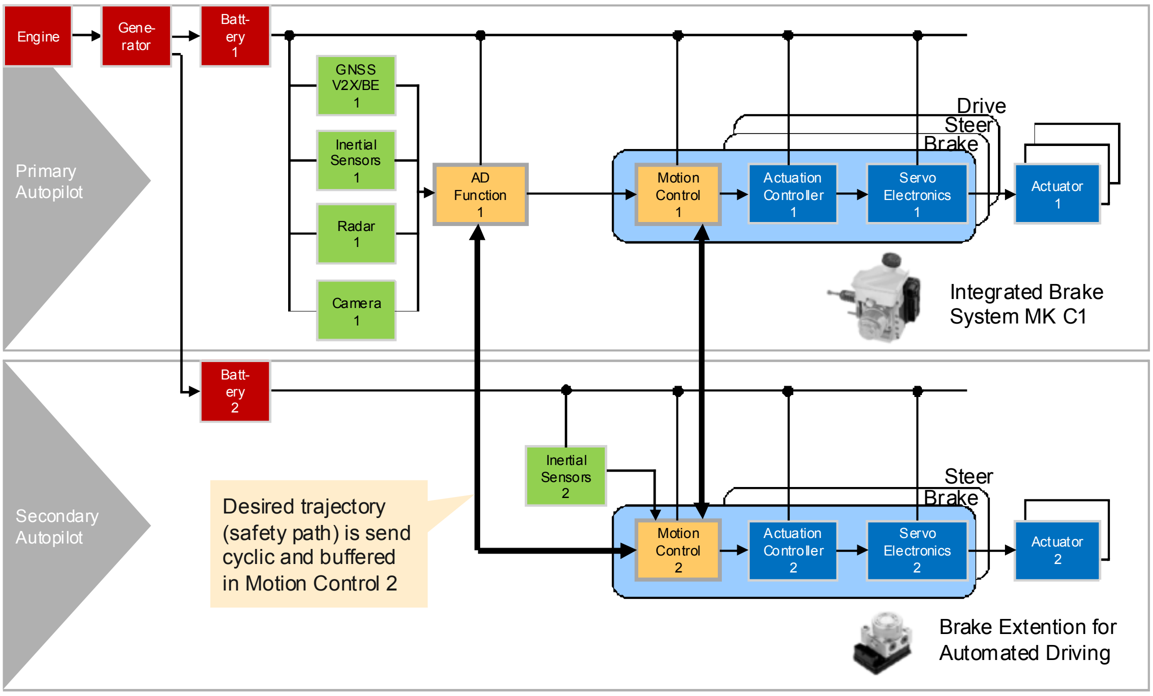


a)
System provides standstill in the ego lane

b)
System provides standstill in service or rightmost lane

Fig 4.: Minimal Risk Condition as Fallback Strategy

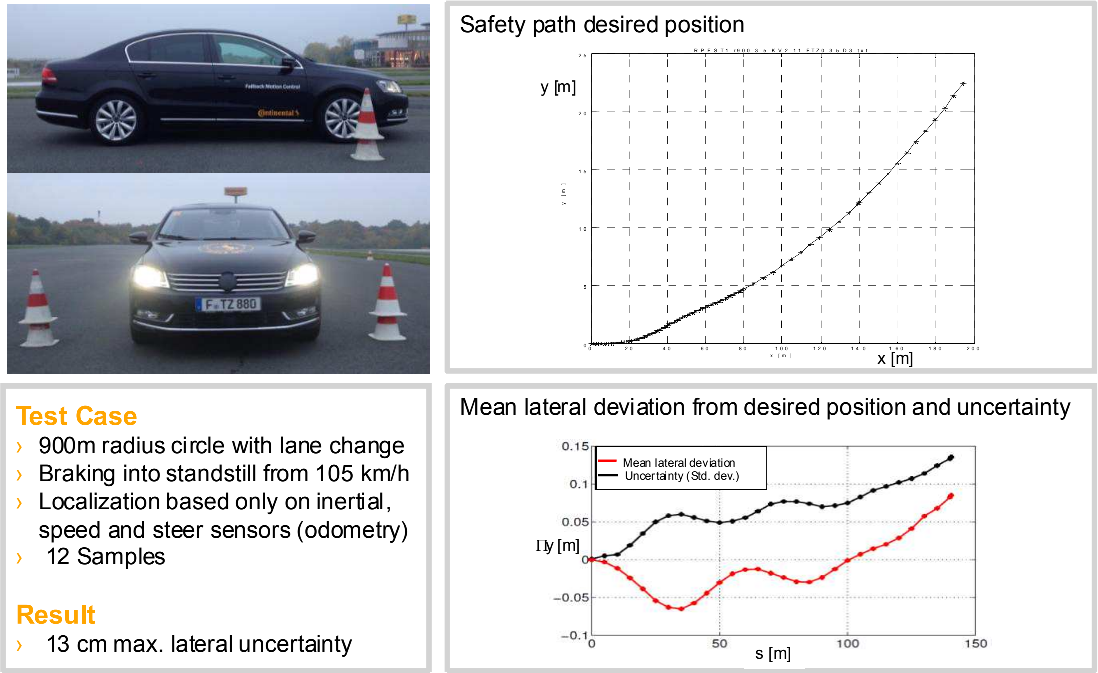
3.2 Redundancy for Automated Driving (Example)



Desired trajectory (safety path) is send cyclic and buffered in Motion Control 2

Fig 5.: Redundancy for Automated Driving (Example)

3.3 Fallback Strategy Testing



Test Case

- 900m radius circle with lane change
- Braking into standstill from 105 km/h
- Localization based only on inertial, speed and steer sensors (odometry)
- 12 Samples

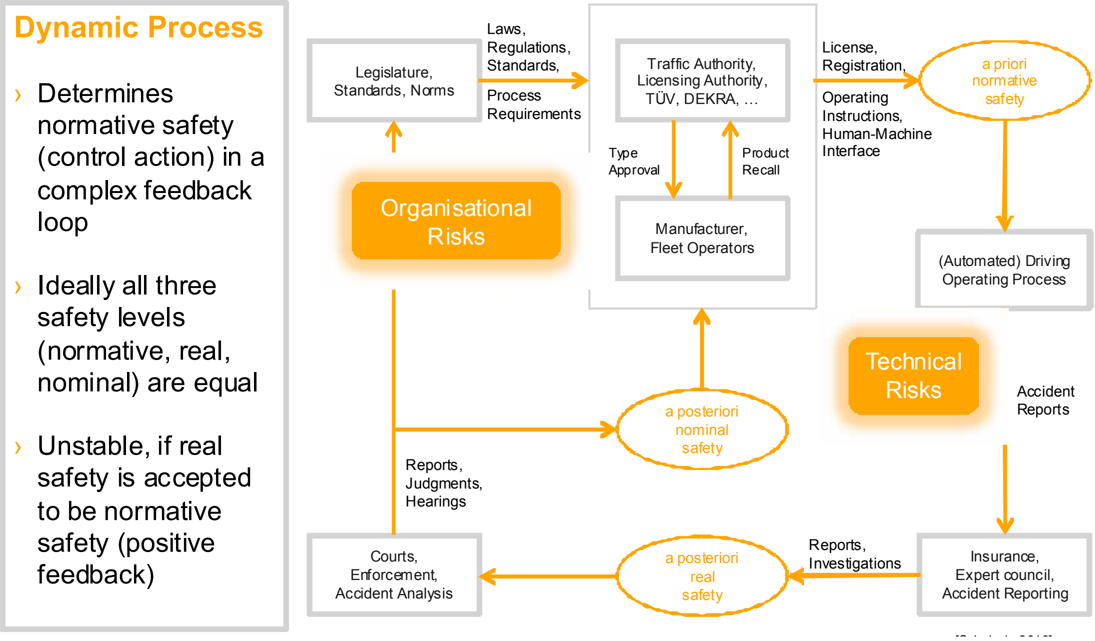
Result

- 13 cm max. lateral uncertainty

Fig 6.: Fallback Strategy Testing

4 SOCIO-TECHNICAL SYSTEM FOR ROAD SAFETY

4.1 Socio-Technical System for Road Safety



Dynamic Process

- Determines normative safety (control action) in a complex feedback loop
- Ideally all three safety levels (normative, real, nominal) are equal
- Unstable, if real safety is accepted to be normative safety (positive feedback)

Legislature, Standards, Norms

Laws, Regulations, Standards,

Process Requirements

Traffic Authority, Licensing Authority, TÜV, DEKRA, …

Type Approval

Product Recall

Manufacturer, Fleet Operators

License, Registration,

Operating Instructions, Human-Machine Interface

a priori normative safety

(Automated) Driving Operating Process

Organisational Risks

Technical Risks

Accident Reports

a posteriori nominal safety

Reports, Judgments, Hearings

Courts, Enforcement, Accident Analysis

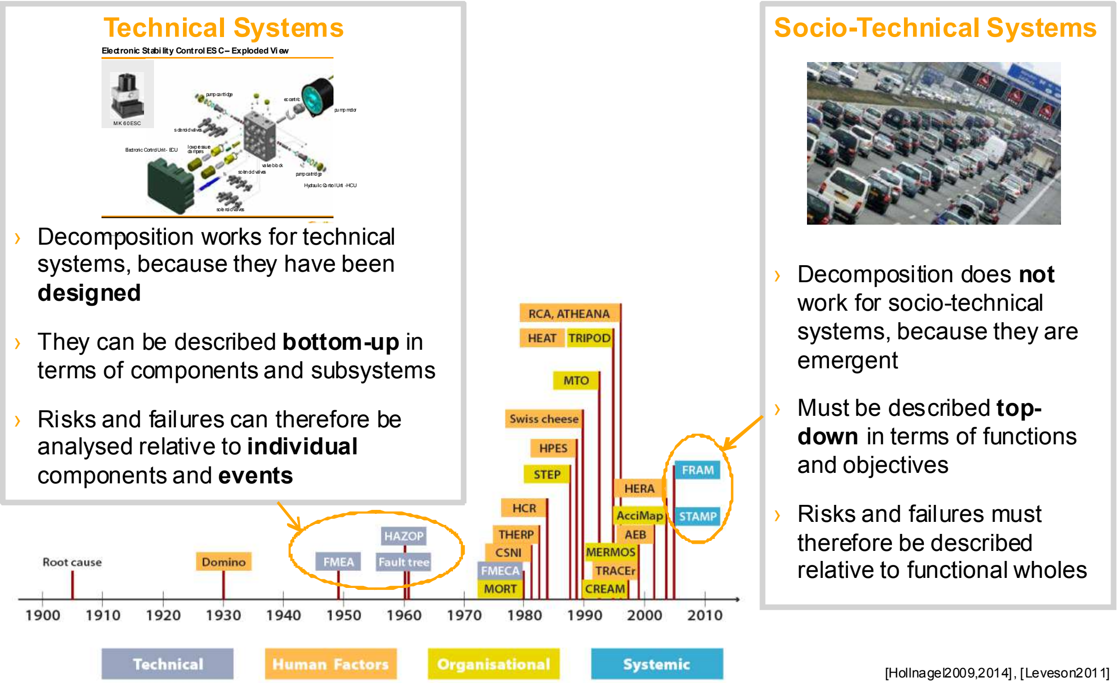
a posteriori real safety

Reports, Investigations

Insurance, Expert council, Accident Reporting

Fig 7.: Socio-Technical System for Road Safety

4.2 Risk Assessment Methods



Technical Systems

Electronic Stability Control ESC – Exploded View

- Decomposition works for technical systems, because they have been **designed**
- They can be described **bottom-up** in terms of components and subsystems
- Risks and failures can therefore be analysed relative to **individual** components and **events**

Socio-Technical Systems

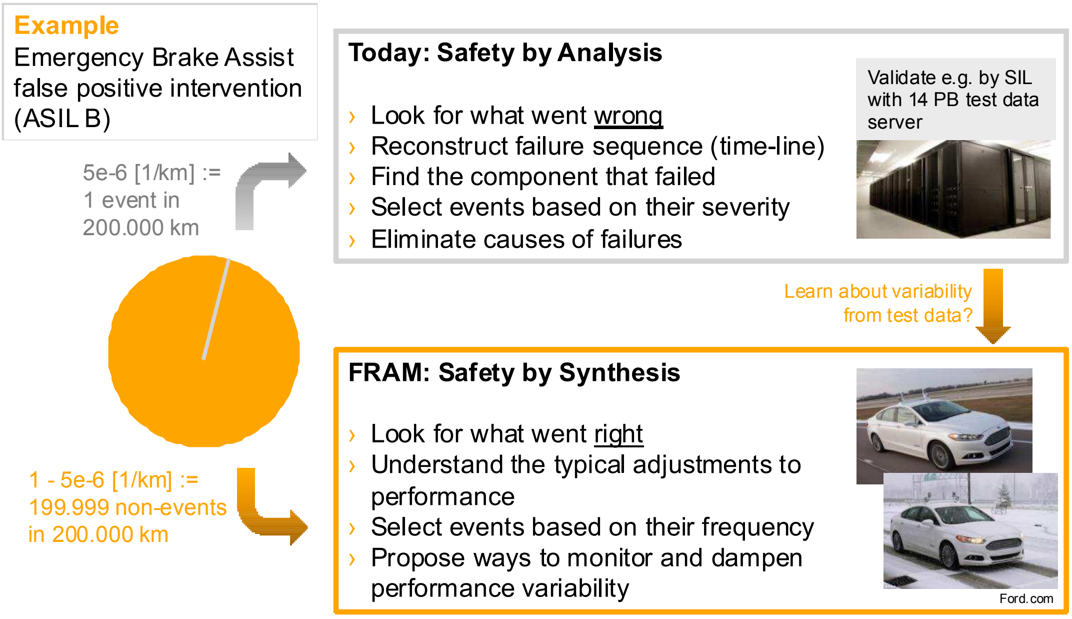
- Decomposition does **not** work for socio-technical systems, because they are emergent
- Must be described **top-down** in terms of functions and objectives
- Risks and failures must therefore be described relative to functional wholes

[Hollnagel2009,2014], [Leveson2011]

Fig 8.: Risk Assessment Methods

5 RISK ASSESSMENT AND SAFETY ANALYSIS

5.1 Functional Resonance Analysis Method (FRAM)



Example
Emergency Brake Assist false positive intervention (ASIL B)

5e-6 [1/km] := 1 event in 200.000 km

1 - 5e-6 [1/km] := 199.999 non-events in 200.000 km

Today: Safety by Analysis

- Look for what went wrong
- Reconstruct failure sequence (time-line)
- Find the component that failed
- Select events based on their severity
- Eliminate causes of failures

Validate e.g. by SIL with 14 PB test data server

Learn about variability from test data?

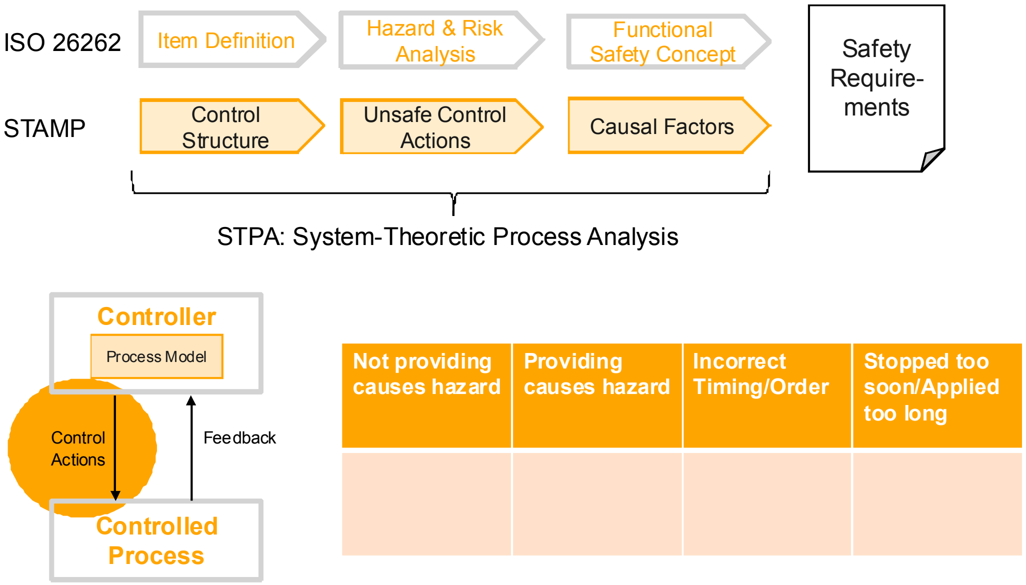
FRAM: Safety by Synthesis

- Look for what went right
- Understand the typical adjustments to performance
- Select events based on their frequency
- Propose ways to monitor and dampen performance variability

Ford.com

Fig 9.: Functional Resonance Analysis Method (FRAM)

5.2 System-Theoretic Accident Model and Processes (STAMP)



ISO 26262: Item Definition → Hazard & Risk Analysis → Functional Safety Concept

STAMP: Control Structure → Unsafe Control Actions → Causal Factors

Safety Require-ments

STPA: System-Theoretic Process Analysis

Not providing causes hazard	Providing causes hazard	Incorrect Timing/Order	Stopped too soon/Applied too long

Fig 10.: System-Theoretic Accident Model and Processes (STAMP)

5.2.1 *STAMP Control Structure*

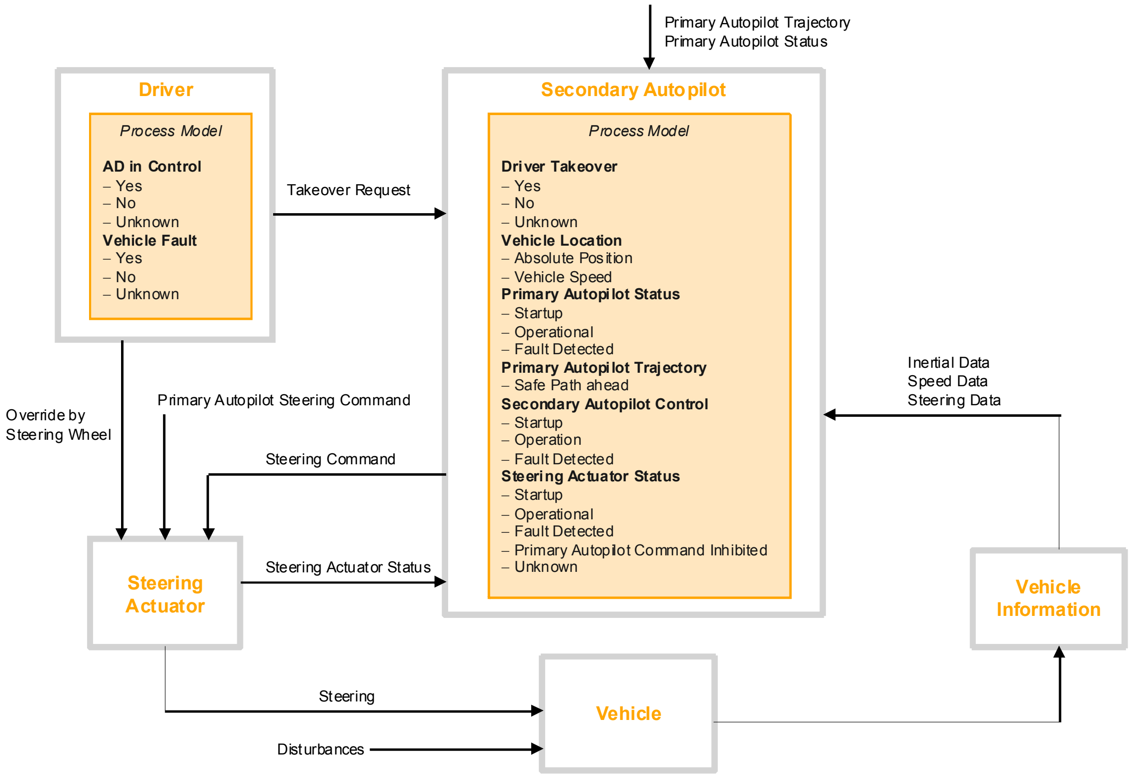


Fig 11.: STAMP Control Structure

5.2.2 *STAMP Unsafe Control Actions*

ID	Safety Goal	ASIL
SG-01	The autopilot shall avoid unintended steering requests during manual mode.	ASIL D
SG-02	The autopilot shall avoid no steering requests.	ASIL D
SG-03	The autopilot shall avoid steering requests with wrong values	ASIL D

Control Action	Action required but not provided		Unsafe action provided		Incorrect Timing/Order		Stopped too soon /Applied too long	
	Description	Safety Goal	Description	Safety Goal	Description	Safety Goal	Description	Safety Goal
Steering command from secondary autopilot to steering actuator	**UCA01** Vehicle does not steer while following safety path trajectory and lateral movement is required	SG-02 ASIL D	**UCA02** Vehicle steers, but following safety path trajectory and lateral movement is not required	SG-01 ASIL D	**UCA03** Vehicle steers too early while following safety path trajectory and lateral movement is required	SG-03 ASIL D	**UCA05** Vehicle stop to steer while following safety path trajectory and lateral movement is required	SG-03 ASIL D
					UCA04 Vehicle steers too late while following safety path trajectory and lateral movement is required	SG-03 ASIL D	**UCA06** Vehicle continue with a stuck value to steer while following safety path trajectory and lateral movement is required	SG-03 ASIL D

Fig 12.: STAMP Unsafe Control Actions

5.2.3 STAMP Causal Factors

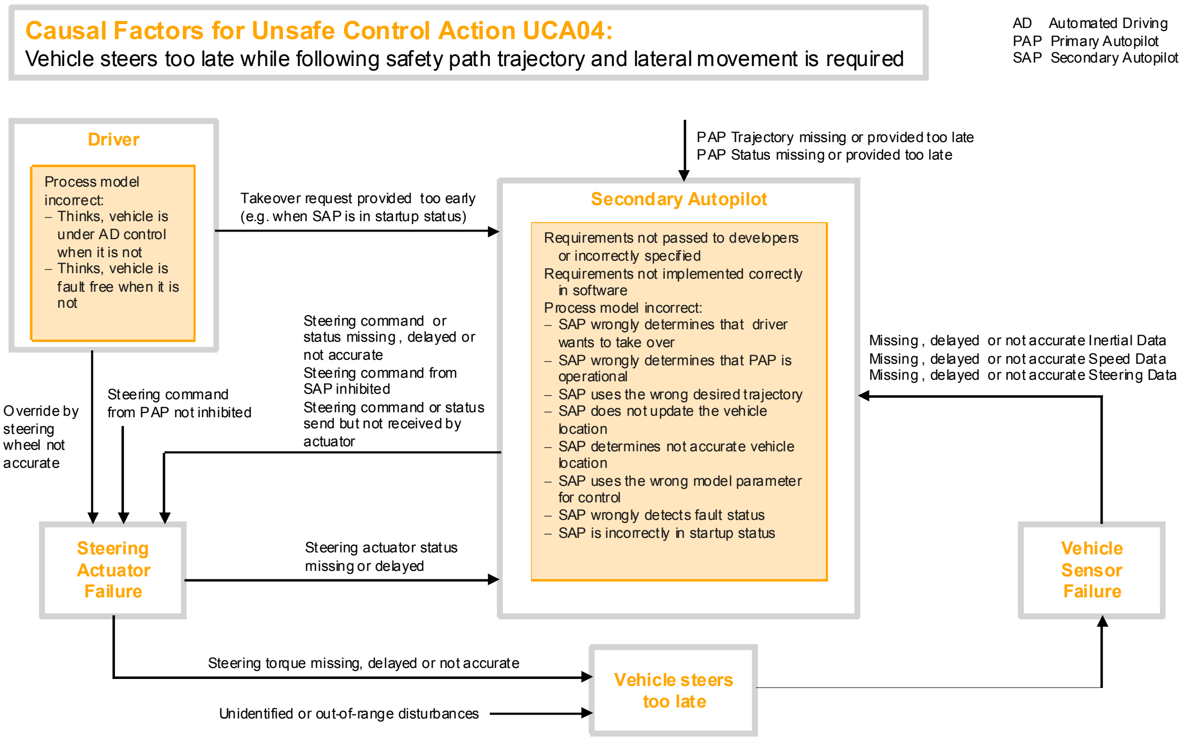

Causal Factors for Unsafe Control Action UCA04:
Vehicle steers too late while following safety path trajectory and lateral movement is required
AD Automated Driving
PAP Primary Autopilot
SAP Secondary Autopilot
Driver
Process model incorrect:
– Thinks, vehicle is under AD control when it is not
– Thinks, vehicle is fault free when it is not
Takeover request provided too early (e.g. when SAP is in startup status)
PAP Trajectory missing or provided too late
PAP Status missing or provided too late
Secondary Autopilot
Requirements not passed to developers or incorrectly specified
Requirements not implemented correctly in software
Process model incorrect:
– SAP wrongly determines that driver wants to take over
– SAP wrongly determines that PAP is operational
– SAP uses the wrong desired trajectory
– SAP does not update the vehicle location
– SAP determines not accurate vehicle location
– SAP uses the wrong model parameter for control
– SAP wrongly detects fault status
– SAP is incorrectly in startup status
Steering command or status missing, delayed or not accurate
Steering command from SAP inhibited
Steering command or status send but not received by actuator
Override by steering wheel not accurate
Steering command from PAP not inhibited
Missing, delayed or not accurate Inertial Data
Missing, delayed or not accurate Speed Data
Missing, delayed or not accurate Steering Data
Steering Actuator Failure
Steering actuator status missing or delayed
Vehicle Sensor Failure
Steering torque missing, delayed or not accurate
Vehicle steers too late
Unidentified or out-of-range disturbances

Fig 13.: STAMP Causal Factors

REFERENCES

[1] Abdulkhaleq, A. (2015). *A Comprehensive Safety Engineering Approach for Software Intensive Systems based on STPA.* European STAMP Workshop, Amsterdam.

[2] Ericson, C.A. (2005). *Hazard Analysis Techniques for System Safety.* John Wiley & Sons, Hoboken, New Jersey.

[3] Hollnagel, E. (2006). *Capturing an Uncertain Future: The Functional Resonance Accident Model.* SKYbrary Bookshelf.

[4] Hollnagel, E.; Leonhardt, J.; Macchi, L.; Kirvan, B. (2009). *A White Paper on Resilience Engineering for ATM.* EUROCONTROL.

[5] Hollnagel, E.; Hounsgaard, J.; Colligan, L. (2014). *FRAM – The Functional Resonance Analysis Model.* Centre for Quality, Denmark.

[6] Kaiser, B. (2014). *Systemsicherheit von ADAS und Hochautomatisiertem Fahren.* Technikforum Funktionale Sicherheit, Braunschweig, Germany.

[7] Leveson, N.G. (2011). *Engineering a Safer World.* MIT Press. Cambridge, Massachusetts.

[8] Schnieder, E.; Schnieder, L. (2013). *Verkehrssicherheit.* Springer Verlag, Berlin.

[9] Thomas, J. (2015). *STPA-based Method to Identify and Control Software Feature Interactions.* European STAMP Workshop, Amsterdam.

[10] Young, W.; Leveson, N.G. (2014). *Inside Risks. An integrated Approach to Safety and Security based on Systems Theory.* Communication of the ACM, Vol. 57, No.2.

HIGHLY-INTEGRATED MILLIMETER-WAVE RADAR SENSORS FOR AUTONOMOUS TRANSPORTATION

(Invited Paper)

D. Kissinger[1,2], R. Weigel[3], R. Lachner[4], K. Aufinger[4], K. Pressel[5], and H. J. Ng[1]

[1] dkissinger@ihp-microelectronics.com; ng@ihp-microelectronics.com
IHP, Im Technologiepark 25, 15236 Frankfurt (Oder) (Germany)

[2] kissinger@tu-berlin.de
Technische Universität Berlin, Einsteinufer 17, 10587 Berlin (Germany)

[3] robert.weigel@fau.de
Institute for Electronics Engineering, FAU Erlangen-Nürnberg, Cauerstr. 9, 91058 Erlangen (Germany)

[4] rudolf.lachner@infineon.com; klaus.aufinger@infineon.com
Infineon Technologies, Am Campeon 1-12, 85579 Neubiberg (Germany)

[5] klaus.pressel@infineon.com
Infineon Technologies, Wernerwerkstr. 2, 93049 Regensburg (Germany)

Abstract

This invited paper describes silicon-based radar sensor systems that are characterized by high performance as well as integration level and suitability for automotive applications. These sensors have been commercially available for some time and successfully used to improve the driving safety as well as comfort. Developments of these radar sensors are currently directed towards applications dominated by other types of sensors like camera and LiDAR. One of these applications is the vehicle’s environment recognition system, which can be efficiently implemented by using radar sensors and thus help the autonomous driving become more robust, viable and affordable. To further promote the widespread deployment of the radar sensors in these applications, research and developments are being carried out in the areas including the reduction of manufacturing cost as well as the size of the sensors, increase of the integration level and use of novel modulation schemes suitable for MIMO operations.

Keywords: Radar, MIMO, millimeter-wave, high-frequency packaging, pseudo-noise

1 INTRODUCTION

Continuous advances in silicon-based semiconductor technology in terms of high frequency characteristics have opened up the mm-wave frequency region that offers an unprecedented level of resolution and an extremely high miniaturization potential due to the shrinking of the passive structures such as antennas [1]. A number of different high-frequency integration techniques with miniaturization potential have emerged in the last few years. The traditional frontend integration using wire-bonding is increasingly abandoned and replaced with a more advanced technique based on the flip-chip concept that features high-frequency interconnects with a lower loss. Printed circuit boards (PCB) with improved laminated substrates or ceramic materials are becoming more low-priced and common. Furthermore, the introduction of packaging technologies with a chip redistribution layer (RDL) significantly relaxes the fine-line spacing requirements on the PCB. One of these technologies is the so-called embedded wafer-level ball grid array (eWLB) package, that features a number of favorable high-frequency characteristics. Since the size of the mm-wave antennas is small enough, these antennas can be implemented in the redistribution layer of the package. This eWLB package technology allows thus the implementation of system-in-package (SiP) radar sensors. Another miniaturization approach is the system-on-chip (SoC) solution with integrated on-chip antennas made possible by the smaller wavelength. Several efforts have been carried out to improve the radiation efficiency of the on-chip antennas. One approach is to remove the lossy silicon under the antennas by using the so-called localized backside etching (LBE) technique. Current automotive radar sensors work with the frequency-modulated continuous-wave (FMCW) principle that can be implemented cost-effectively in a small quantity. MIMO radar sensors are becoming more popular and important to satisfy the demands of enhanced spatial resolution and improved estimation accuracy. Novel modulation schemes that are able provide a large set of uncorrelated signals and suitable to replace the classical FMCW radars in the automotive applications have been reported. Among these novel modulation schemes are the pseudo-random noise (PRN) and orthogonal frequency division multiplexing (OFDM) techniques, which have various advantages and disadvantages.

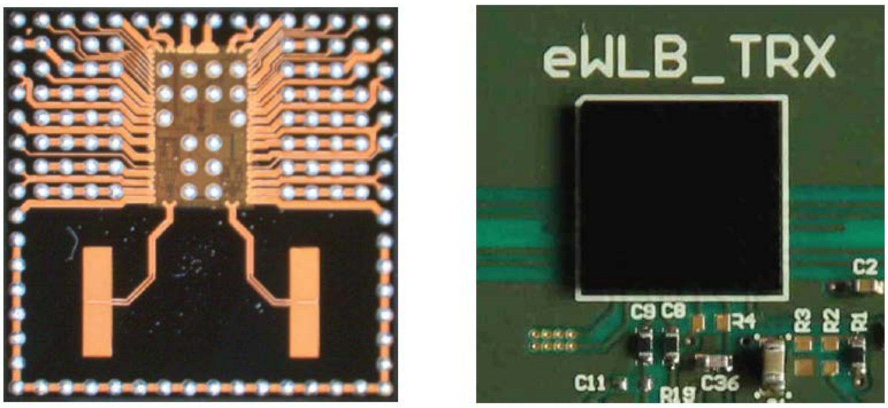
2 CURRENT STATUS AND KEY DIFFERENTIATORS

Fueled by the vision of fully autonomous driving, promoted by a various global players, the field of integrated millimetre-wave radar sensors has rapidly evolved since the last ten years. Following initial efforts in single-chip integration of formerly discrete solutions in SiGe technologies the main focus of development has turned to multi-channel systems featuring beam-forming capabilities. At the current manufacturing level, one key differentiator is lowering the costs of such transceivers through the addition of integrated high-frequency test features [2], [3] for lowering test cost overheads (sometimes as high as 50% of the total IC costs) and the transition to online built-in test monitoring which is important for safety applications.

A second highly important step that has recently been made is the realization of high-frequency packaging solutions to enable the use of standard assembly processes for the radar system manufacturer. For the realization of such low-cost highly integrated radar sensor solution, millimeter-wave integrated circuits can be packaged using an embedded wafer-level ball-grid array (eWLB) technology that includes a redistribution layer (RDL) to increase the fan-out area [4]. This technology exhibits good thermal and high-frequency characteristics and the additional RDL does not limit integrated circuit pin count to the solder ball pitch.

3 INTEGRATED MILLIMETER-WAVE ANTENNAS

The RDL of an eWLB package can been used to additionally embed the 60 GHz transmit and receive antennas in the same package [5]. An example of an embedded 60 GHz multi-purpose transceiver is given in Fig. 1. It shows a photograph of the packaged transceiver including dipole antennas (a) and a photograph of the transceiver frontend mounted on a low-cost standard FR-4 printed circuit board. The circuit has been fabricated in a fully qualified low-cost SiGe bipolar technology (B7HF200) from Infineon Technologies that features an effective emitter width of 0.18 µm with transit frequencies up to 200 GHz. The chip occupies an area of 3.2 x 2.1 mm^2 and has a maximum power consumption of 280 mA from a single 3.3V supply. The transceiver can be operated in the 57-66 GHz range.



(a) Backside view (b) Mounted frontend-in-package

Fig. 1. Backside (a) and front view after mounting (b) of a 60GHz frontend with dipole antennas for TX and RX integrated into the eWLB package [6].

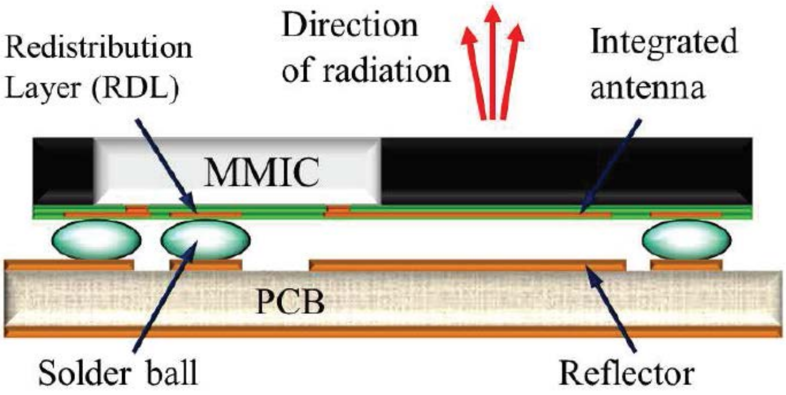


Fig. 2. Cross section of the implemented eWLB packaging concept with integrated antenna-in-package and reflector realization on the carrier PCB.

The transmit path features an IQ vector modulator and achieves an output power above +10 dBm in the whole frequency range. Furthermore, the implemented IQ receiver path including a VGA achieves a maximum gain around 30 dB at a noise figure of 7 dB. The package occupies an area of 8 x 8mm^2 and the antennas show a maximum antenna gain of 8 dBi. This technique offers the opportunity for fully integrated millimeter-wave radar front-ends without high-frequency connections to the PCB, which drastically increases the handling of the 60 GHz radar sensor at the board level and provides the opportunity for the use of standard low-cost FR-4 substrates without the need for high-frequency laminates.

As the operating frequency of radar transceivers is further increased beyond 100 GHz, the wavelength permits direct on-chip integration of the antennas on the integrated circuit, e.g. 2.5 mm at 120 GHz. The resulting reduced efficiency due to the lossy silicon substrate can largely be circumvented using a localized backside etching (LBE) process which selectively removes the silicon in critical areas under the antennas. Fig. 3 shows the implementation of an on-chip double folded dipole antenna with an improved mechanical stability. The dipoles and their microstrip feeding lines are realized on the thickest top metal layer while the ground plane is formed on the bottom metal layer. Air trenches are formed around the dipoles by the LBE process, while no silicon is removed under the metal structures. The on-chip antenna requires an external metal reflector, which can be implemented as a metal plane on the package or PCB. The two folded dipoles together with the reflector form a 2-element broadside array that achieves an antenna gain of 6 dBi with a radiation efficiency of 54%.

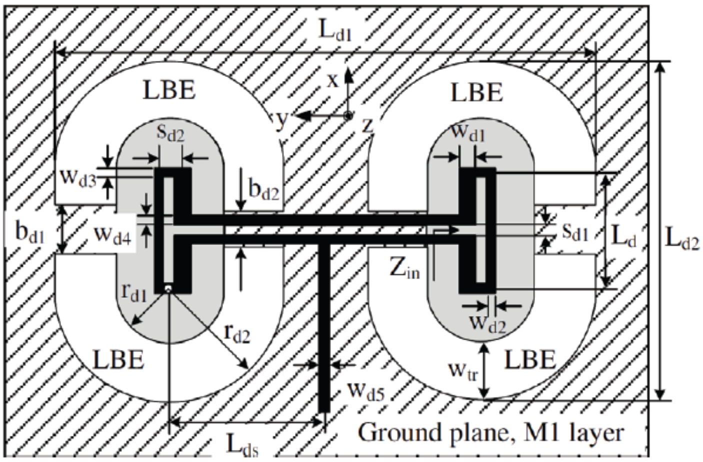


Fig. 3. Layout concept of the integrated double-folded 120 GHz dipole antenna including feedline and localized backside etching (LBE) [7].

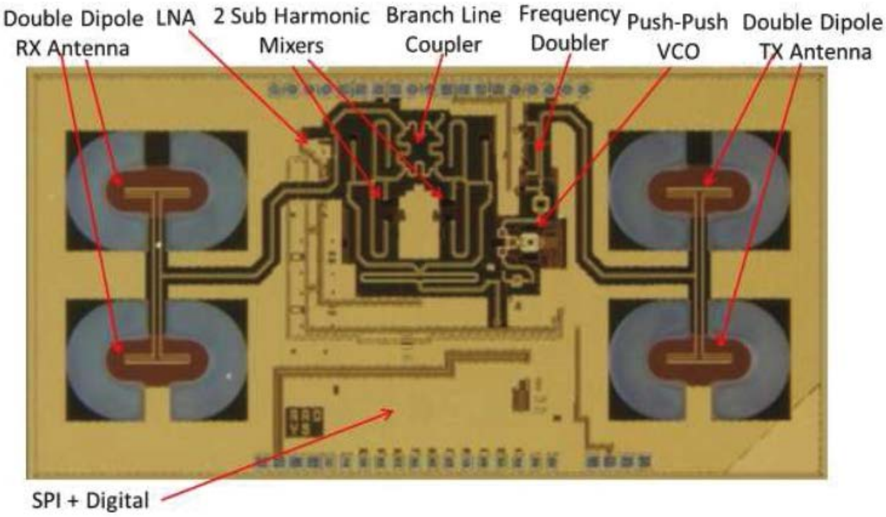


Fig. 4. Micrograph of the fabricated 122 GHz radar system-on-chip including two integrated double-folded dipole antennas with backside etching [7].

The micrograph of a highly integrated 120 GHz radar transceiver including on-chip antennas is shown in Fig. 4. It has been implemented in IHP 130 nm SiGe BiCMOS technology with f_T/f_{max} of 220 GHz / 300 GHz and has a size of 4.5 mm x 2.3 mm. The two double folded dipole antennas for the receiver and the transmitter are located at the most left and right side of the chip, while the active part of the transceiver is located in the center of the circuit.

4 PSEUDO-RANDOM NOISE RADAR

One of the future directions in radar transceiver design is the transition to a so-called “digital radar”. Such a radar is mainly characterized by a communication transceiver architecture with bit sequences used as modulation signals and corresponding digital correlator architectures in the receiver unit. A pseudo-random noise (PRN) radar is a very good candidate to fullfill these requirements and further enables interference-robust operation using orthogonal codes. It does not require a linear frequency sweep as a TX signal or a complex frequency synthesizer. Instead, it uses an ultra-wideband (UWB) pseudo-random binary sequence (PRBS) as a stimulus. The PRBS generator needs much less gates than the DDS or the ΣΔ-modulator of an FMCW radar and can thus be integrated on the same transceiver chip in the SiGe technology.

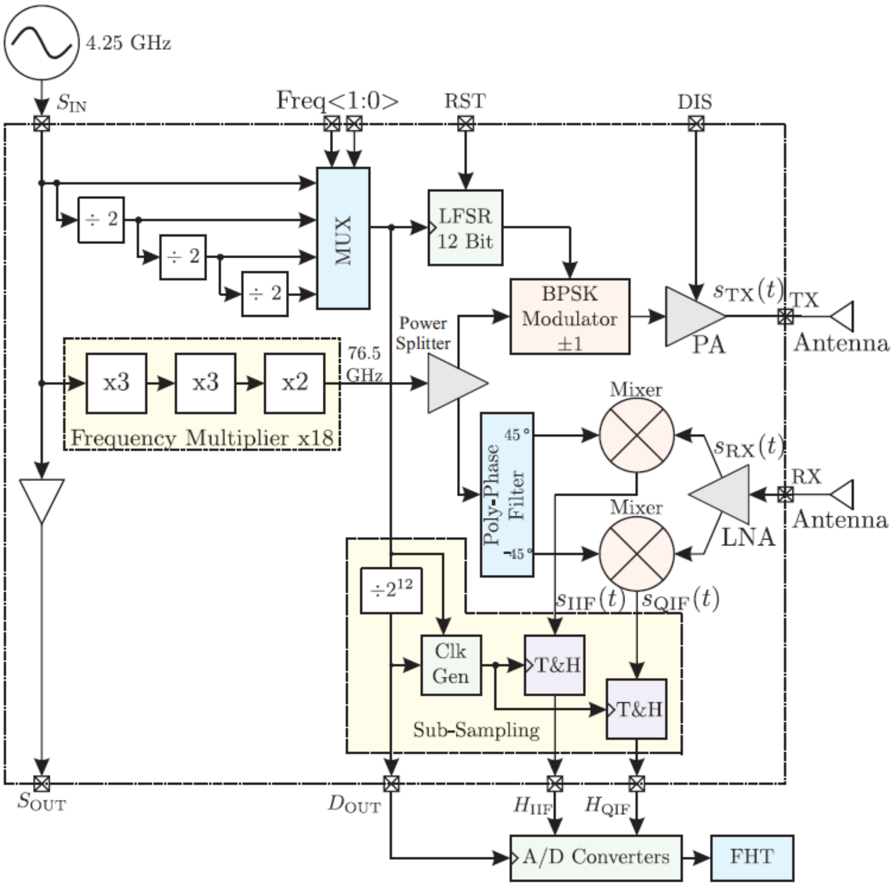


Fig. 5. Block diagram of an integrated 77 GHz pseudo-random noise transceiver including PRBS generator and sub-sampling acquisition [8].

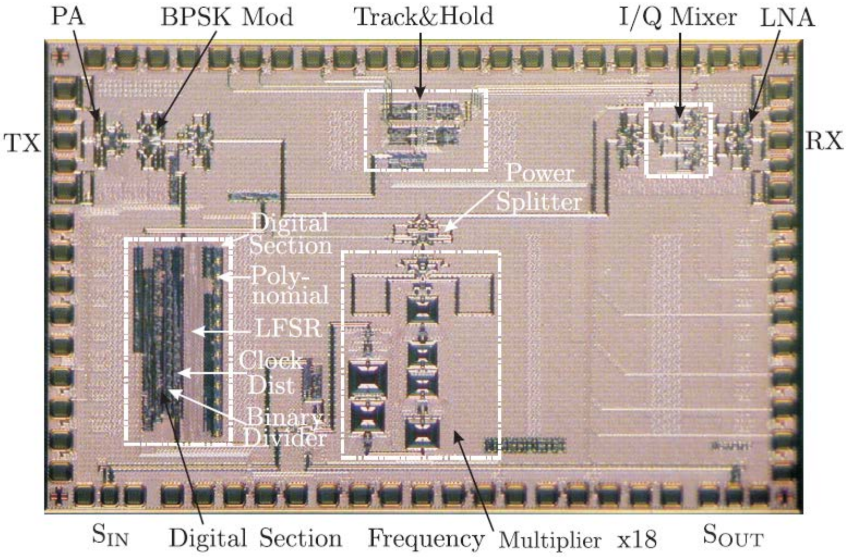


Fig. 6. Die photograph of the integrated ultra-wide band 77 GHz pseudo-random noise transceiver circuit in a SiGe bipolar technology [8].

It is much easier to realize and there is no requirement on the linearity of the TX signal. The target resolution of the PRN radar depends on the modulation bandwidth, which is determined by the clock frequency of the PRBS generator. Therefore, no VCO with a high tuning range to achieve a high target resolution. Fig. 5 shows a block diagram of a PRN radar. An external signal source provides the transceiver chip with a 4.25 GHz signal, which is multiplied by 18 to create a carrier signal at a frequency of 76.5 GHz. The 4.25-GHz input signal is also fed to a multiplexer and a three-stage binary divider to serve as the clock frequency for the LFSR. A power splitter is used to split the carrier signal to TX and receive (RX) paths. The LFSR generates the maximal length sequence (MLS), which is modulated onto the carrier signal by using a binary phase-shift keying (BPSK) modulator. The output signal is then fed to a power amplifier (PA), which drives a TX antenna. On the RX path, the output signal of the power splitter is fed to a poly-phase filter, which outputs two signals with a phase difference of 90°. These output signals are fed to the LO inputs of the I/Q mixers. The RX signal is amplified by a low-noise amplifier (LNA) and is splitted to be fed to the RF inputs of the I/Q mixers. The track-and-hold (T&H) elements deliver the IF outputs of the mixers to the external analog-to-digital (A/D) converters. The cross-correlation operations are done externally by using a fast Hadamard transformation (FHT). The PRN transceiver chip was implemented in a 200-GHz f_T SiGe:C bipolar technology. Fig. 6 shows the micrograph of the fabricated chip, which has a size of 3mmx 1.8 mm. The digital section of the chip occupies the area on the left side of the chip and is isolated from other circuit blocks. The frequency multiplier occupies the area in the middle of the chip and the power splitter separates it from the TX and RX paths. The TX path is on the top left of the chip and includes pads to the transmit antenna. The RX path is on the top right of the chip and includes pads to the RX antenna. The PRN transceiver draws a current of 375mA from a 3.3V supply.

The fully integrated 76.5 GHz PRN radar transceiver features a modulation bandwidth of up to 4.25 GHz resulting in a range resolution of 3.5 cm. The architecture includes a frequency multiplier to create a carrier signal from a single input signal, that is further used as a clock signal for the PRBS generator. A phase noise of −105 dBc/Hz was achieved. The PRBS generator, which is realized by using a 12-stage LFSR with a programmable primitive polynomial, needs much less gates than a DDS or a ΣΔ-modulator of an FMCW radar and can thus be integrated on the same transceiver chip in the SiGe technology. The various MLSs with a length of 4095, which are generated by the LFSR, enable a high dynamic range and allow the operation of several PRN transceivers at the same time to cover different spatial regions. By applying the subsampling technique with the help of the T&H circuits included in the transceiver, the IF data rate is reduced to a frequency in the range of 1MHz. Low cost A/D converters can thus be used to convert the IF signals to digital domain.

5 MIMO RADAR CONCEPTS

Fig. 7 shows the block diagram of a scalable radar sensor platform concept consisting of several multipurpose transceivers. An external signal source provides the transceivers with a 30.5 GHz LO signal, which is internally multiplied with a factor of 2 or 4 to create carrier signals with a frequency of 61 GHz and 122 GHz in the transceivers, respectively. Inside each transceiver, the LO signal is also fed to an output buffer that is connected to an output pad to provide an LO signal source for the next transceiver and thus enables the cascading of multiple transceivers. At the output of the frequency multiplier, a power splitter is used to split the carrier signal to the TX and the RX path. In the TX path, the carrier signal is fed to a BPSK modulator, of which output is connected to the power amplifier that is used to drive the TX antenna. In the RX path, the carrier signal is fed to another BPSK modulator. Its output is connected to a poly-phase filter, which provides two signals with a phase difference of 90° to the LO inputs of the I/Q mixers. The RX signal is amplified by a low noise amplifier (LNA) and is split and fed to the RF inputs of the I/Q mixers. Fig. 8 shows the micrograph of the scalable 122 GHz transceiver chip, which was implemented in the IHP 130 nm SiGe BiCMOS technology with f_T/f_{max} of 220 GHz / 300 GHz and has a size of 2.14 mm x 1.74 mm.

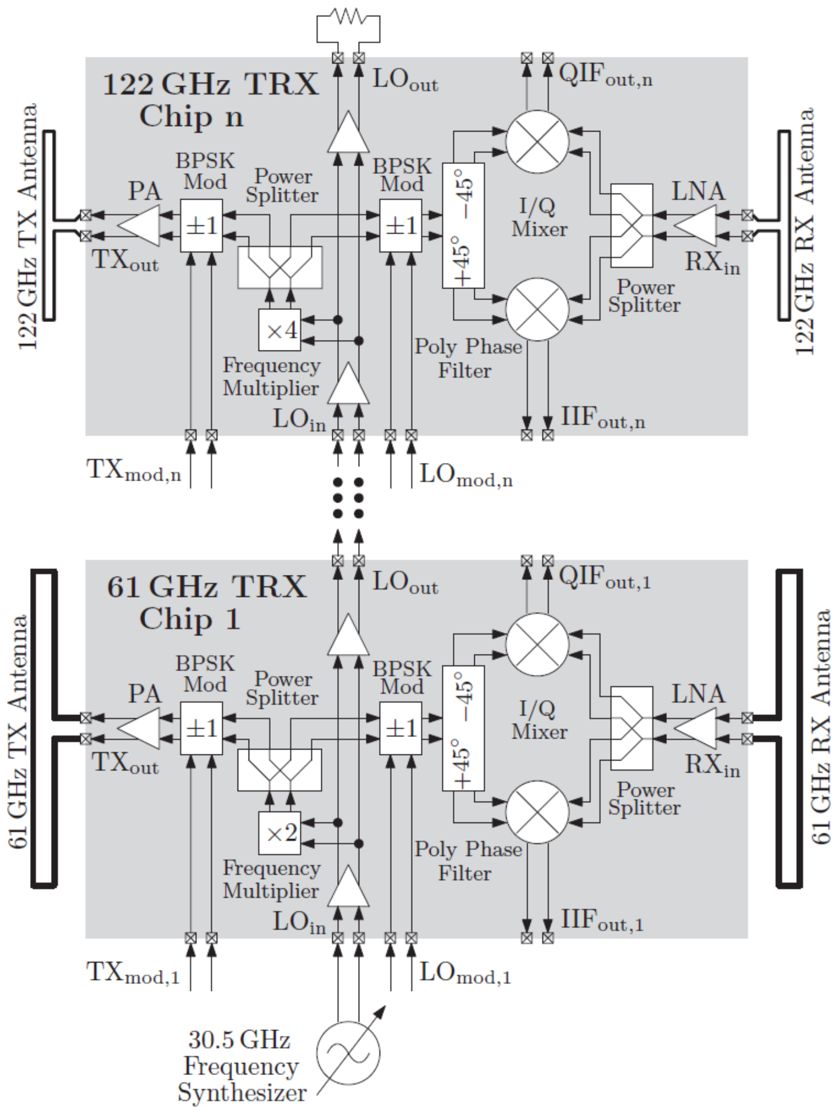


Fig. 7. Block diagram of a scalable MIMO transceiver system concept based on multiple 60 and 120 GHz cascadable transceivers in a daisy-chain [9].

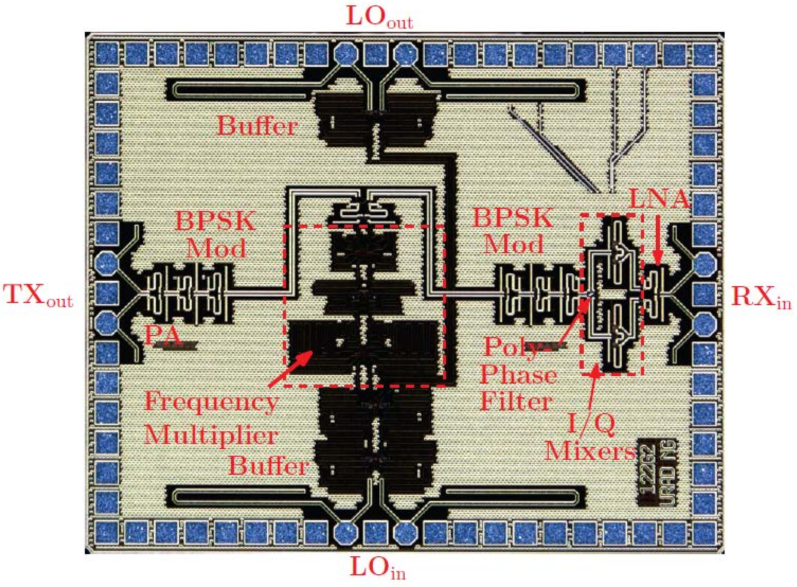


Fig. 8. Die photograph of a scalable 120 GHz transceiver circuit [9].

6 CONCLUSION

In this paper an overview of transceiver frontend concepts and realizations for highly integrated millimeter-wave radar sensors has been given. The presented 60 GHz embedded frontend with antenna integration in a wafer-level packaging technology and 120 GHz radar sensor with on-chip antennas can be applied in low-cost short-range applications. Furthermore, approaches for distributed digital radar concepts based on pseudo-random noise modulation and powerful MIMO radar systems have been shown that can be used for environmental sensing solutions for complex autonomous transportation.

REFERENCES

[1] E. Kasper, D. Kissinger, P. Russer, and R. Weigel, “High speeds in a single chip,” *IEEE Microw. Mag.*, vol. 10, no. 7, pp. 28–33, Dec. 2009.

[2] D. Kissinger, B. Laemmle, L. Maurer, and R. Weigel, “Integrated test for silicon front ends,” *IEEE Microw. Mag.,* vol. 11, no. 3, pp. 87–94, May 2010.

[3] D. Kissinger, R. Agethen, and R. Weigel, “A versatile built-in test architecture for integrated millimeter-wave radar receiver front-ends,” in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Graz, Austria, May 2012, pp. 254–258.

[4] M. Wojnowski and K. Pressel, “Embedded wafer level ball grid array (eWLB) technology for high-frequency system-in-package applications,” in *IEEE MTT-S Int. Microw. Symp. Dig.*, Seattle, WA, Jun. 2013.

[5] R. Agethen, M. PourMousavi, H. P. Forstner, M. Wojnowski, K. Pressel, R. Weigel, and D. Kissinger, “60 GHz industrial radar systems in silicon-germanium technology,” in *IEEE MTT-S Int. Microw. Symp. Dig.*, Seattle, WA, Jun. 2013.

[6] D. Kissinger, T. Girg, C. Beck, I. Nasr, H. P. Forstner, M. Wojnowski, K. Pressel, and R. Weigel, “Integrated millimeter-wave transceiver concepts and technologies for wireless multi-Gbps communication,” in *IEEE MTT-S Int. Microw. Symp. Dig.*, Phoenix, AZ, May 2015, pp. 1–3.

[7] H. J. Ng, J. Wessel, D. Genschow, R. Wang, Y. Sun, and D. Kissinger, “Miniaturized 122 GHz system-on-chip radar sensor with on-chip antennas utilizing a novel antenna design approach,” in *IEEE MTT-S Int. Microw. Symp. Dig.*, San Francisco, CA, May 2016.

[8] H. J. Ng, R. Feger, and A. Stelzer, “A fully-integrated 77-GHz UWB pseudo-random noise radar transceiver with a programmable sequence generator in SiGe technology,” *IEEE Trans. Circuits Syst. II*, vol. 61, no. 8, pp. 2444–2455, Aug. 2014.

[9] H. J. Ng, M. Kucharski, and D. Kissinger, “Scalable sensor platform with multi-purpose fully-differential 61 and 122 GHz transceivers for various MIMO radar applications,” in *Proc. IEEE Bipolar/BiCMOS Circuits Technol. Meeting*, New Brunswick, NJ, Oct. 2016.

IMPROVING THE CROSS-BORDER FLOW OF THIRD COUNTRY NATIONALS

Łukasz Szklarski[1], Piotr Gmitrowicz[2], Mateusz Oleś[3], Krzysztof Samp[4], Andreas Kriechbaum-Zabini[5]

[1]*lukasz.szklarski@itti.com.pl,* [2]*piotr.gmitrowicz@itti.com.pl,* [3]*mateusz.oles@itti.com.pl,* [4]*krzysztof.samp@itti.com.pl*
ITTI Sp. z o.o., ul. Rubież 46, 61-612 Poznań (Poland)

[5]*andreas.kriechbaum-zabini@ait.ac.at*
AIT Austrian Institute of Technology GmbH, Donau-City-Straße 1, 1220 Vienna (Austria)

Abstract

The paper delves into several issues related to the European border crossing processes. It is motivated by the ongoing numerous research on automated border control (ABC) systems, which have been tested at a number of EU border crossing points (BCP) of various type. Moreover, taking into account the continuously growing influx of third country nationals (TCNs) travellers into the EU, the paper presents the complex procedures this group of passengers is currently required to go through. Facing these issues, potential remedies to highlighted problems are indicated including legislative as well as technological in nature. Central to the discussion, is the proposal to facilitate the cross-border movement of TCNs thanks to the ABC technologies and processes developed within EU-funded FastPass project. Based on the carried out technological and desk research, the paper provides a contribution to the further discussion on the automation of border processes for TCNs entering the European Union/Schengen zone pinpointing possibilities as well as obstacles lying ahead.

Keywords: Innovation, Automated Border Control, Smart Borders, EU borders, EU research projects, FastPass.

1 THIRD COUNTRY NATIONALS AND CURRENT EU PROCEDURES

Over the recent years, the EU border authorities have been experiencing an increased workload, which might be attributed to the number of factors. Most of all, such a situation is the result of the on-going migration crisis and steady growth of the number of passengers coming into the European Union/Schengen zone countries. All of the above contribute to exert a major strain upon the border guards at the external EU borders. The paper will primarily tackle the rise in the number of third country nationals and the complex procedures they have to go through in order to cross the EU external borders further suggesting potential facilitation of their cross-border movement. It is reported that in 2014 alone there were approximately 29 million TCNs entering and exiting EU borders. Future forecast indicate a substantial growth to 63 million in 2020 and 76 million in 2025 [1].

Currently, Third Country Nationals are required to undergo a complex process while travelling to the EU/Schengen countries. According to the Schengen Border Code, non-EU nationals are undergoing more detailed checks compared to the EU/EEA/CH area travellers. They are obliged to have a valid travel document and visa, present their travel purpose and prove that are in possession of sufficient means of subsistence. Additionally, TCNs are allowed to stay within the EU no longer than 90 days in any 180-day period. In compliance with the current procedures, each traveller from a third country is obliged to have his/her travel document stamped on entry/exit occasion in order to have a record of stay duration. Facing an increasing flow of travellers into the EU and existing complicated procedures, the European Commission proposed the "Smart Border" initiative in 2013 with the intention of external Schengen borders management improvement, provision of data on overstayers as well as facilitation of cross-border flow of pre-vetted TCNs [2].

The EU Commission's proposal included the creation of Registered Traveller Programme (RTP) and Entry/Exit System (EES). The former, according to the 2013 proposal, was to take shape of a central database, which would store the data of pre-vetted and pre-screened TCNs including biometrics, alphanumeric data and unique identifier. Then, the unique identifier would be a token for a swift cross-border movement while maintaining the EU level of security. Furthermore, the proposal assumed the storage of personal data for a period of no longer than five years [5]. However, in a ruling presented in [4], issued in 2016, the EU Commission withdrew its proposal regarding the Registered Traveller Programme. The other assumption of 2013 proposal was the establishment of Entry/ Exit System. The original proposal was encouraged by the lack of Schengen Border Code's stipulation on recording traveller's entries and exits. At the moment, the only method to determine stay duration of a given TCN are the stamps in the travel document. As a consequence, monitoring and identifying overstayers seem to be quite problematic issues for the border guards. In response, EES was to replace the obsolete system based on stamps and monitor the remaining time duration for a given TCN staying within the Schengen zone, provide border guards with detailed information on an overstayer in order to facilitate proper counter-measures, biometric data storage of visa holders, and implementation of automated border control as soon as manual stamping is replaced. The system would also store the collected data of regular cases in a central database for six months [3]. The main purpose of such a system is to keep the border guard informed immediately, like ABC, if the checked person is an overstayer or not.

Following the release of the technical study in 2014 and a report from testing phase in 2015, the EU Commission published an updated legislative proposal for the development of Entry/Exist System in 2016, which featured several amendments in comparison to the original proposal. Namely, it is highlighted that the EES shall be interoperable with the Visa Information System, rely on four fingerprints and facial image as biometric features and storage of data for the period of five years. Additionally, the EU Commission proposed EES to be based on self-service systems and e-gates and allow Europol as well as national law enforcement agencies to have access to the EES database. The overall cost of EES implementation, taking into account the withdrawal of RTP proposal, is estimated at €480 million [4].

Feasibility of EES implementation was supported by the report released in 2015, which gave a glimpse at the carried out Smart Borders Pilot, which focused on operational tests as well as desk research. The pilot was conducted at air, sea and land border in twelve EU member states including Germany, Estonia, Greece, Spain, Finland, France, Hungary, Italy, the Netherlands, Portugal, Romania, and Sweden. The pilot delved into the biometric aspect of the Smart Borders initiative and provided statistical data regarding the acceptance of proposed solutions by Third Country Nationals. The report concludes with a positive outlook for the implementation of EU Commission's proposals acknowledging that ABC gates and kiosk at border crossing points can shorten the overall duration of cross-border processes [6].

The EU's interest and determination to test and implement the new border procedures is not solely reflected by the proposal made in 2013 (revised in 2016), but also by the number of EU-funded research projects handling the issue of Automatic Border Control implementation in the form of e-gates and kiosks, which include projects such as ABC4EU or FastPass. The research paper will present the FastPass project in more detail highlighting its goals, assumptions and approach towards modernisation of the current EU border procedures.

2 FASTPASS INNOVATIONS

One of the goals of the EU-funded FastPass project was to correspond to the EU Commission's Smart Borders initiative. Therefore, the project aims at developing and subsequently testing automated border control solution with demonstrations taking place at all three border crossing types (i.e. air, land and sea). An inherent part of the project is close compliance with privacy, social, ethical and legal aspects, all of which are the basis of the modernized border control processes. Furthermore, project partners recognize that implementation of ABC gates is more complex than just solely depend on the guidelines provided by either government official or industry representatives. Therefore, FastPass handles the issue in a more holistic manner acknowledging the importance of meeting the expectations of both types of ABC users, i.e. border guards as well as travellers. The adopted user-centric approach relies on the feedback collected during the project lifetime from border guards as well as travellers. Apart from that, FastPass provides a comprehensive research of ABC technological components such as biometric identification technology, document verification tools, pre-border and border area surveillance, interoperability and adaptability of the system architecture and gate technology used for more comfortable and rapid movement. In addition, the joint work of the entities involved in the production of ABC gates is believed to pave the way for the standardisation of ABC equipment and harmonisation of border processes.

2.1 New cross-border processes for handling travellers

A set of solutions that is proposed by the FastPass solution is the outcome of the gathered user requirements towards automated border control and technological research. The proposed processes were developed so that they would be compliant with the EU legal, societal, and ethical values. As already mentioned, FastPass solution proposes a two-step approach, which requires a traveller to go through an enrolment process prior to e-gate crossing. The paper presents in detail the FastPass approach on the basis of the land border border type, which requires more complex checks to be performed than in the case of the other two border types. Also, the land border pilot will be supported by participating TCN (Serbian citizens). The project's land border scenario is to be tested at Moravita border crossing point between Romania and Serbia. Nevertheless, all processes proposed by FastPass require both enrolment as well as e-gate phases. It is assumed that the new harmonized procedures can be applicable both to EU citizens and Third Country Nationals facilitating and making their cross-border movement more convenient.

First of all, each passenger is required to enrol to the FastPass database. In case of the land border scenario, the enrolment process is performed for both a traveller and a vehicle. Moreover, the pilot at Moravita BCP is restricted only to Romanian and Serbian citizens over the age of 18. Additionally, FastPass land border solution is limited to two passengers per vehicle, which stems from the design of the e-gate.

In order to successfully complete the enrolment process, all passengers need to register as frequent travellers in a kiosk (see Illustration 1). The process starts with a scanning of a machine readable zone (MRZ) of a travel document (either passport or ID). The collected data are then verified in the SISII, VIS, and national police databases. The process continues with a facial recognition and enrolment of passenger's face IR template. The collected data are saved in the FastPass database with the travellers consent. The traveller's registration is valid until the expiration date of the passport or ID. The enrolment process is further carried on for the driver/vehicle registration purposes.

Welcome to cologne
MODI
Vision for Identification

Illustration 1. Enrolment Kiosk by MODI Modular Digits GmbH.

The driver continues the registration process by scanning the driving licence. The remaining part of the process shifts to the enrolment of the vehicle, which begins with a scan of the vehicle registration certificate and extraction of the vehicle number plates. Subsequently, the driver issues the expiration date of technical inspection and scans the green card. All of the gathered data are saved in the FastPass database. Following the enrolment procedure, the driver and passenger (if present) resume to the vehicle and approach the e-gate (see Illustration 2).

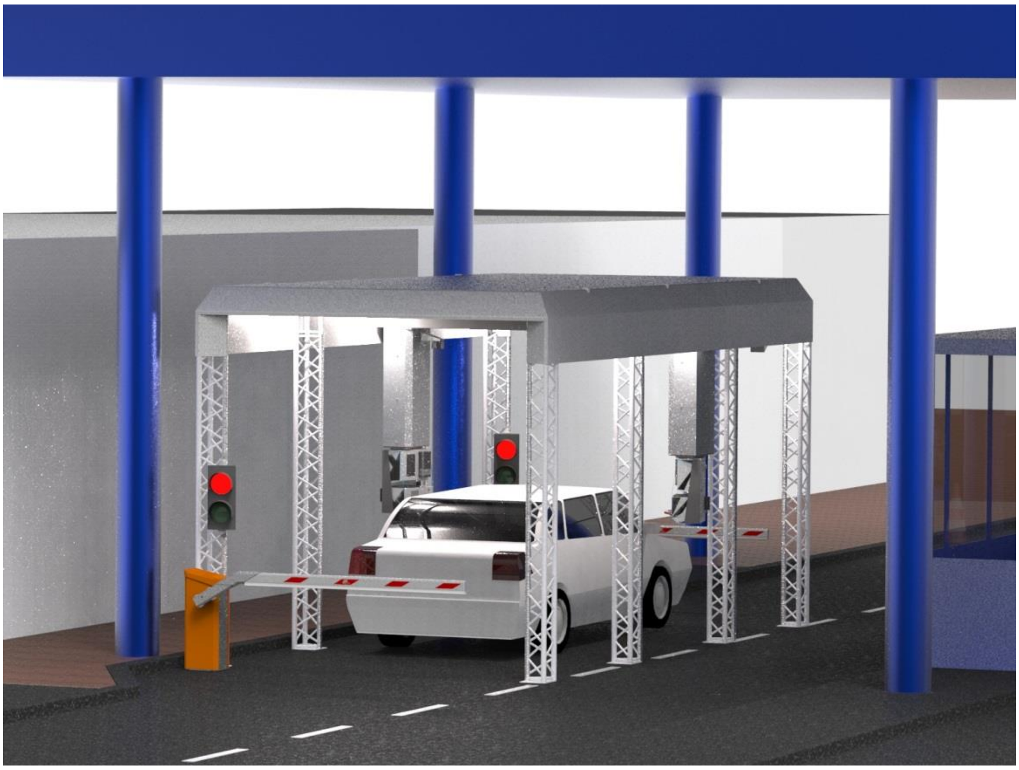


Illustration 2. The concept of the e-gate at Moravita BCP developed by Magnetic Autocontrol GmbH.

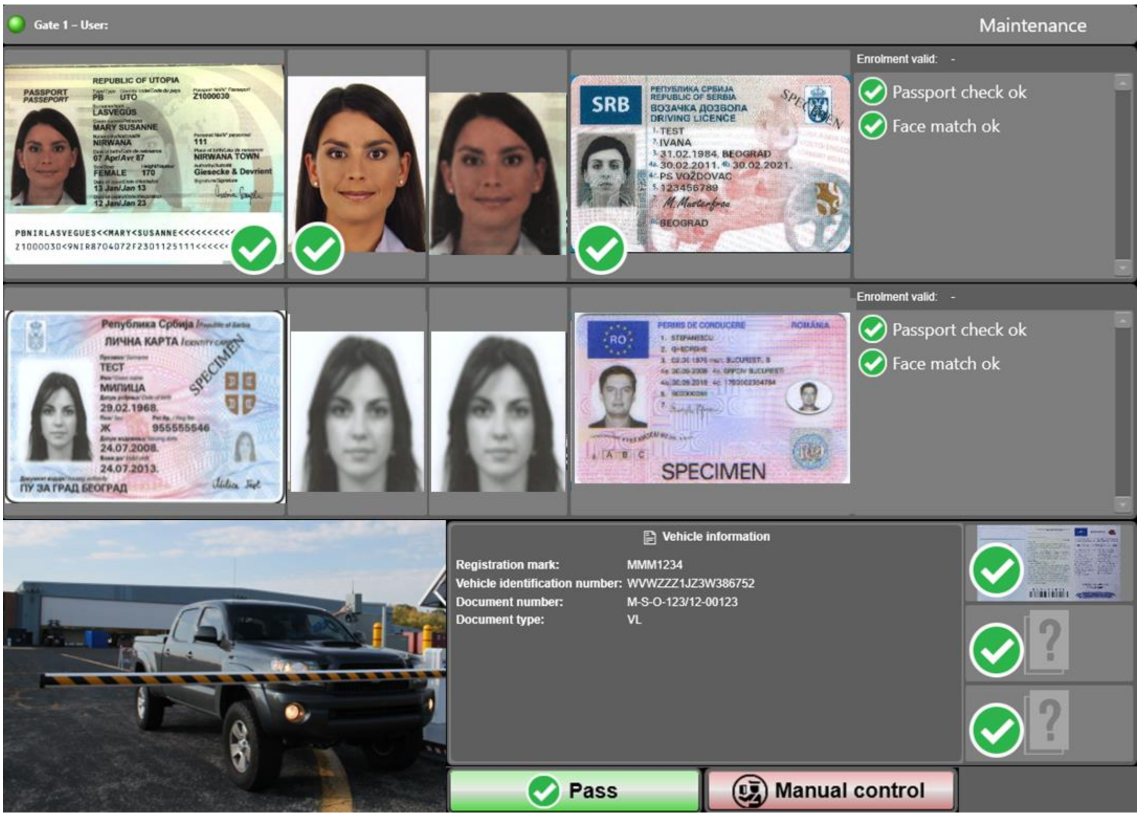
Prior to the e-gate entry, the surveillance camera reads out the vehicle's number plates and the system verifies whether the vehicle is entitled to use the FastPass solution. The process inside the gate was designed to take as little time as possible. Therefore, it requires the driver and co-driver (if present) to scan MRZ of their travel documents (passport or ID). Then, passengers' live images are captured inside the gate and compared to the templates stored inside the FastPass database. It must be added that the process, though automatic, is under the constant supervision of a border guard, who can decide to manually verify a given traveller if a suspicion arises. Of course, the travellers can use the e-gate directly if they are already registered

2.2 Technological components

The automation of border processes proposed by the FastPass project requires state-of-the-art technologies including hardware and software components. A crucial components of the FastPass solution are kiosk and e-gate. It is worth mentioning that the technologies used in the project are modular in nature and, thus, can be adjusted to a given scenario. The applied technologies allow for the collection of various biometric attributes including face, iris and fingerprint. In the land border scenario, however, only facial recognition is used as a biometric feature. Both kiosk and e-gate, in land border case, use a face-iris camera developed by MODI and document scanner provided by REGULA, both of which constitute a hardware basis of the entire automated system.

Starting with the camera, it has been developed by MODI and unlike other similar tools using a moving camera or multiple cameras, MODI's equipment applies a rotating mirror technology. It is, therefore, possible to capture a person's face as well as iris scan. The camera's scope of view may be changed in all directions. The tool is capable of providing up to 30 high resolution face pictures regardless of the person's height or position in front of the gate. Also, the camera makes it possible to handle people with height ranging from 1,20m up to 2,20m. The added value is the capability to carry out a facial recognition process while a traveller is on the move. During the enrolment process, the camera generates a near infrared (NIR) face template, which is then saved in the database. The advantage of NIR face template is its lack of susceptibility to external light. According to the data provided by the manufacturer, the camera has the capacity to conduct a facial recognition process on approximately 1000 people per hour. Regarding the document scanner, Regula 70X8 has been applied. The scanner is used both in the kiosk and in the e-gate. The device provides scans of all documents during enrolment (kiosk) and verification (e-gate) processes.

An important part of the technological components is software, which has been tailored to the applied hardware and user requirements. One of the software components is Optical Character Recognition (OCR), thanks to which alphanumeric data from the documents can be read out. An essential aspect of the FastPass software, during the developmental phase, was to create a user interfaces (UIs) meeting the border guards requirements. The step was essential since the border guard needs to supervise the entire process. The developed interface (see Illustration 3) gives an oversight over all collected data from a passenger. The submitted data can be either accepted or rejected by the border guard.



Vehicle information

Registration mark: MMM1234
Vehicle identification number: WVWZZZ1JZ3W386752
Document number: M-S-O-123/12-00123
Document type: VL

Illustration 3. FastPass UI for border guard by Mirasys Oy.

3 CHALLENGES

Though the proposed FastPass solutions and project-related actions might be a measure for facilitation of cross-border movement, harmonization and standardization of border processes and ABC equipment, there are still several obstacles to be overcome in order to implement modern automated border control. The difficulties stem from a variety of reasons including conflicting opinions about the overall shape of automated border control indicating a series of implications or legislative restrictions. The carried out research within FastPass gives a glimpse into existing objections across Europe. The conducted study required 44 participants to express their opinion on a series of questions related to the implementation of ABC and Smart Borders initiative. The participants were political figures and experts in areas such as border control, data protection, technology, policy and legal issues from European Union member states. The study concluded with three distinct views on the given questions.

Starting with the first and most popular view in the study, the participants highlighted their objections towards automated border control and identified several data protections issues. The majority of respondents were mostly left-of-centre political figures and several liberal politicians. According to their opinion, the decision on ABC implementation in purely political and its main objective is to collect data about the passengers. The participants put forward a concern regarding fair treatment of asylum seekers. Namely, still unclear is the process of asylum seekers registration with ABC solutions. Also, the open issue remains whether the passenger profiling may ultimately result in discrimination on the basis of nationality, race or ethnicity. Apart from that, doubts remain with regard to the use and collection of biometric data. The scepticism stems from the reported data mishandling from the past but also fear of the governments storing such sensitive personal data that could also serve other purposes than border control. Speaking of data sharing, the view represented by the group of participants argued that the collected passenger data should be only used for border control purposes. It was also pinpointed that law enforcement's access to large databases are not necessarily a facet improving their work effectiveness. Further argument was given that the automated border control and the proposed by the EU Commission Smart Borders initiative may lead to the encroachment of EU citizens' rights reflected by the potential surveillance and misuse of the stored data.

The second view, which appealed to thirteen mostly right-of-centre political figures, is more supportive of the automated border control implementation. It has been highlighted that ABC solution is an essential one believed to enhance European security and integration. The group of respondents does not object passengers' data sharing. What is more, it is proposed that the law enforcement agencies would gain access to the EU-wide database, which would boost counteracting organized crime and terrorism. Moreover, the second view supporters contradict some of the statements presented in the previous view including the fact that ABC allegedly might infringe the rights of the EU citizens by surveillance. It is acknowledged, however, that transparency of such a solution is a must. Furthermore, study participants stressed the need for the harmonization of the automated border control. Such a process would contribute to the cost-efficiency of ABC solution, increased security across EU and would give impetus for the further integration of EU member states.

The remaining view included in the study was supported by the far right and Eurosceptic political figures. They highlighted that the EU is threatened by the illegal immigration and human trafficking. Therefore, there are no objections expressed towards fingerprint collection of third country nationals at border crossings. The overall attitude towards the implementation of automated border control is quite sceptical. The participants elaborated that ABC, in their opinion, would not be more successful than hiring more border guards. In addition, the participants supporting the sceptical view indicated the privacy issues should be brought to the centre of the discussion. It is argued that people may grow suspicious about the governmental actions aiming at collection of sensitive personal data.

Nevertheless, the study found that all participants, regardless of the political affiliations, expressed some shared opinions regarding the automated border control. First of all, the respondents agreed on the data minimization in the ABC processes. This means that the scope of collected personal data and data retention period should be limited to the bare minimum, which is needed for cross-border procedures. The second agreement was reached with regard to the transparency. It was agreed that the passengers should be clearly informed about the entire process of biometric data collection including what biometric features are to be collected, by whom and for what purpose they shall be used. Moreover, the transparency is required in the legal context. It is, therefore, required that proper legal instruments as well as oversight procedures should be implemented prior to the EU-wide system goes live. Furthermore, the participants argued that ABC process and implementation of Smart Borders proposals shall be preceded by providing democratic legitimacy at least on a parliamentary level of all EU member states. The remaining shared view is the accessibility of ABC systems for the disabled. It is highlighted that new solution should not in any way encroach on a fundamental civil rights and, thus, it is required that state-of-the-art ABC systems respect equal rights of the disabled.

4 CONCLUSIONS

Having considered all of the aforementioned issues, it seems that the flow of TCNs will, in all likelihood, continue to rise. As presented in the paper, existing border procedures for third country nationals are time-consuming and complex. Facilitation of their cross-border movement via automated border control will inevitably lead to the revision and amendment of the current border procedures. The automated border control, as indicated by the pilots across the European Union and the research carried out within FastPass project, is technologically feasible. The presented novel processes for automated border control, both enrolment and at the e-gate, are assumed to speed-up the passenger flow across EU/Schengen borders. Nevertheless, in spite of the technological readiness to implement automated border control solutions for third country nationals, there are still obstacles lying ahead. This issue was partly addressed by the revised legislative proposal for the implementation of Entry/Exit System that was passed in 2016 by the European Commission. However, several other aspects need to be taken into account, especially the shared views described in the FastPass study included in the chapter 3 of the paper. Namely, the EU as well as national legislative bodies should consider such ideas as data minimisation, transparency, data protection, legitimacy of ABC approach as well as accessibility of automated border checks for the disabled. Therefore, it is assumed that further investigation is needed with regard to the legislative aspects of ABC implementation, considering the evidence described in this paper.

5 REFERENCES

[1] PwC, “Technical Study on Smart Borders,” European Commission, Brussels, October 2014.

[2] Frontex, “Guidelines for Processing of Third-Country Nationals through Automated Border Control,” Frontex, Warsaw, 2016.

[3] European Commission, “Proposal for establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union,” European Commission, Brussles , 2013.

[4] European Commission, “Proposal for establishing an Entry/Exit System (EES),” European Commission, Brussels, 2016.

[5] European Commission, “Proposal for establishing a Registered Traveller Programme,” European Commission, Brussels, 2013.

[6] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, “Testing the borders of the future,” European Commission, 2015.

DETECTION OF ANOMALOUS BEHAVIOUR IN SHIP REPORTING DATA FOR IMPROVED MARITIME SECURITY

Harm Greidanus, Michele Vespe and Marlene Alvarez

harm.greidanus@jrc.ec.europa.eu
European Commission - Joint Research Centre (JRC),
Via E. Fermi 2749, 21027 Ispra (Italy)

Abstract

Nowadays, most of the world's medium and large ships use equipment to self-report their positions. The data from these systems add up to large amounts, and provide detailed insight in ship traffic and ship behaviour. It is sought to exploit these data to find security risks in the maritime domain, by finding anomalies, i.e., behaviours that are different from what is normal. A few examples of different methods and their results are discussed, using data acquired over the Mediterranean Sea and the Western Indian Ocean. It is concluded that automatic algorithms for anomaly detection already provide some functionality, but that their design needs further improvement; and that for the final interpretation a human analyst is still needed.

Keywords: Maritime Surveillance, Maritime Security, Ship Self-Reporting Systems.

1 INTRODUCTION

Ship traffic carries most of the world's commerce, but also some security risks, in particular related to bringing in undesired goods or people. A thorough inspection of all ships and cargo approaching and entering is unattainable, so it is important to have risk indicators to focus inspections on the most questionable cases. One source of such risk indicators can come from the analysis of ship tracks, which is nowadays made possible for practically all of the larger ships and some of the smaller ones, by collecting the data from automatic ship position reporting systems. With such data, one can find the route of a ship and its behaviour at sea, and flag the occurrence of abnormal behaviour, such as loitering at sea, encounters with other ships, or not following the most logical route.

One approach to (automatically) find anomalies is location-based, in the sense that the normal behaviour of the ship traffic at a certain geographic location is determined from historical data, and then compared with the instantaneous behaviour of ships in that location. Another approach is track-based, comparing the track or position of a certain ship with a collection of historic tracks.

The paper will discuss and show the results of several approaches to implement this, with examples in the Mediterranean Sea and in the Western Indian Ocean. Both areas were monitored for one year or more using multiple ship self-reporting sources.

2 TOOLS

Today's main ship reporting system is AIS (Automatic Identification System). Most of the world's medium and large ships have to use AIS, as mandated by the UN's International Maritime Organisation (IMO). The global AIS carriage requirement extends to all passenger ships, and all other ships of 500+ GT (gross tonnage) or 300+ GT if on international voyages [1]. Some countries extend this further, e.g. the EU requires fishing vessels of 15+ m length to carry AIS [3, 4]. In addition, many smaller ships carry a "lighter", voluntary type of AIS equipment, called Class B. With AIS, ships automatically broadcast short messages on VHF containing information about their identity, position, movement, voyage and properties. The messages can be received by anyone within radio line of sight. AIS was designed as an anti-collision system, and the interval of the AIS position reports is seconds to minutes, depending on the ship's speed and status. Using AIS receivers on the coast, the ship traffic out to the radio horizon can be tracked continuously. The radio horizon can typically be some 30 nautical miles (NM) out, but the range can be much longer depending on the height of the receiver and atmospheric conditions. Coastal AIS stations are nowadays typically linked up in networks, providing easy access to AIS data along large sections of the coast. Using AIS receivers on satellites, the coverage can become global. However, such satellites are typically in low Earth orbit, and consequently the ships can only be seen when a satellite passes over. Many such satellites are presently available, mostly operated commercially.

Another widely used ship reporting system is LRIT (Long Range Identification and Tracking). Its worldwide use is similarly mandated by IMO, in this case on all passenger ships, all ships of 300+ GT and mobile offshore drilling units [2]. Automatic position reports of LRIT are sent normally every 6 hours to the ship's Flag State authorities. In contrast to AIS, this information is therefore not generally accessible, and much less frequent but – to the recipients – more consistently available since the message reception is (practically) assured. Besides the Flag State, other authorities entitled to access a ship's LRIT data are Coastal States within 1,000 NM of the ship and the Port State of destination.

A third main ship reporting system is VMS (Vessel Monitoring System), used for fishing ships. No VMS data are used in this study however.

Stringing together reports received from different AIS sources (coastal networks, satellites), from LRIT and/or from VMS (the latter two from governments), it is possible to obtain the track of a ship to the extent that the ship is covered in space and time by the available sources.

In addition to these main tools, a number of auxiliary ones are needed to further interpret the ship position data and a ship's behaviour. Such auxiliary data include maps (coastline, bathymetry, offshore installations, maritime zoning, …), met/ocean data (wind, waves, currents, …), data bases (ship registers, port locations, …) and regulations (traffic separation schemes, fishing restrictions, …). Ship registers are e.g. needed to link ships seen in AIS (where they are identified with their so-called MMSI number) with the same ship seen in LRIT (where they are identified with their IMO number) or in VMS (where yet other identifiers are used). The list of auxiliary data can be extended to include more detailed and specialist aspects such as e.g. economic conditions, which may determine whether loitering behaviour of a tanker is or is not suspicious. For a reliable recognition of anomalous behaviour, detailed domain knowledge, specific for the geographic area of interest, is essential.

One possible reference to decide if behaviour is anomalous, is the pattern of normal behaviour as established by statistical analysis of the available ship position data. The normal pattern can be codified as properties per geographic grid cell [5], or as properties of routes (connections between geographic reference points) [6,7]. Knowledge about activity patterns and context can be extracted using data-driven approaches [8]. As examples, exploration and offshore activities have been mapped [9]; as have fishing activities yielding fishing intensity layers [10].

Besides data from ship reporting systems, Earth observation (imaging) systems can be used to obtain additional information on normal and suspicious ship behaviour. Further alternative methods to flag elevated risk in ship traffic – more specifically in seaborne trade – are based on container tracking [11]. These data sources can be complementary to ship position reporting systems, but are not further discussed here.

3 EXAMPLES FROM THE MEDITERRANEAN SEA

LRIT data have been used to calculate ship traffic density as a reference pattern for normal behaviour in the Mediterranean Sea. The regularity of the LRIT data and the lack of (spatial and temporal) gaps over wide areas and long intervals, contrary to AIS data, make the derivation of ship density maps and the statistical analysis of routes [12] relatively straightforward. Fig. 1 shows the density map in a part of the Mediterranean Sea derived from two years of historical LRIT data of ships flying the Flag of States contributing to the EU LRIT Cooperative Data Centre (CDC) run by EMSA (European Maritime Safety Agency): all EU Member States and Overseas Territories, Iceland and Norway. Although this subset of ships excludes widely used Flags such as Panama, Liberia, etc., it is assumed that in the Mediterranean the ships with EU-associated Flags are representative of all similar traffic. The shipping routes are clearly delineated in the density map. Overlaid are the real-time positions of all cargo ships seen on coastal AIS at a certain time on 3 June 2016. In addition, the multi-day past track of one of those ships in the Ionian Sea is plotted. This ship is located off any of the routes, although it has followed a route coming out of the Black Sea and going around the Peloponnesus. What is more, the ship has just turned 180° and is now retracing its route backward for the last few hours. This is clearly anomalous behaviour on two accounts, which may justify further investigation.

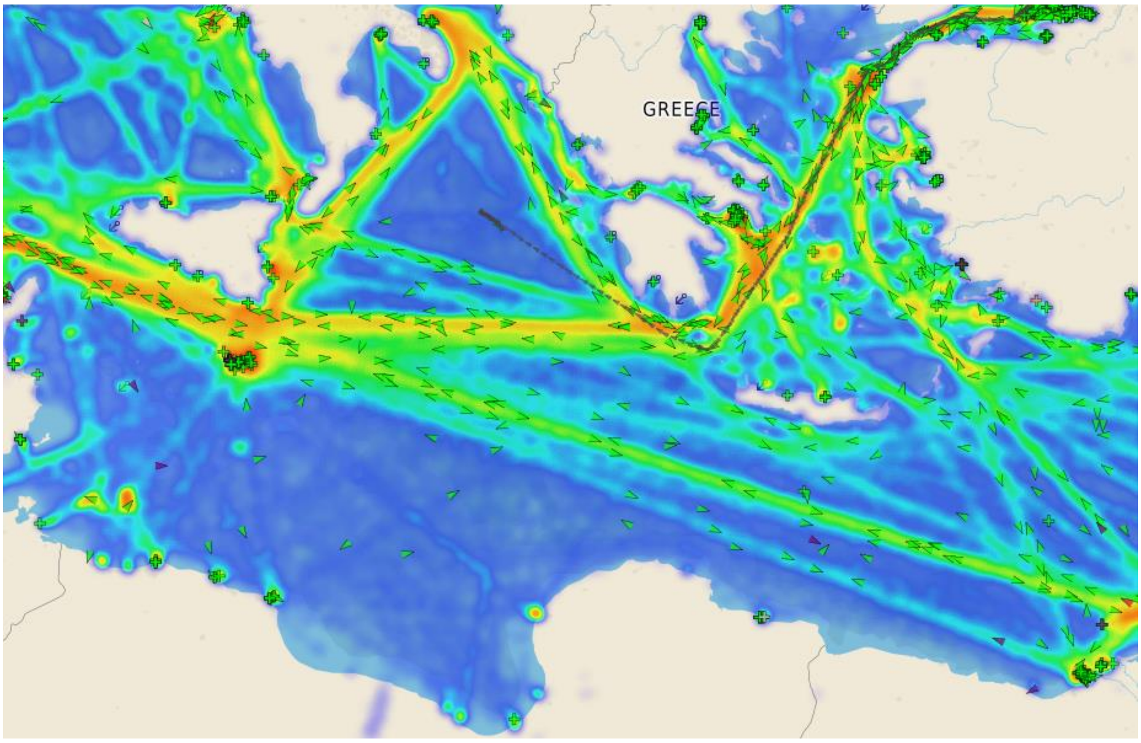


Figure 1. The AIS-based instantaneous cargo ship traffic (green arrowheads) in the Central-East Mediterranean on 3 June 2016 07:00 UTC, overlaid over a ship density map derived from historic LRIT data that shows the main traffic routes. The recent past track of one cargo ship that is located in a triangle outside the main routes between Greece and Italy is shown, tracing the ship’s origin back to the Black Sea. The ship in question has just doubled back on its track, creating the impression of a thick end to its track.

An example of anomaly detection with the cell-based approach [5] is shown in Fig. 2. Sampling the ship traffic on a discrete grid in space and time with cells of size 0.25 NM x 0.25 NM x 15 min, it is checked whether two ships occur in the same space-time cell. If so, a proximity condition is flagged. A prolonged proximity of two ships at high seas may point to illegal transhipments. The top part of Fig. 2 shows the proximity-flagged cells highlighted in green spatially projected on a map. A trail of green dots can be seen across the middle, suggesting that two ships have been close together while traveling. Indeed, after retrieving which ships were responsible for the proximity condition and plotting their tracks (bottom), it is found that this pair of ships, one of which is a tug, have travelled together all the way from the Canary Islands to Port Said. Other concentrations of green dots in the top figure are associated with ship proximity in ports and anchor areas and near off-shore installations. None of these proximities after all point to illegal activities.

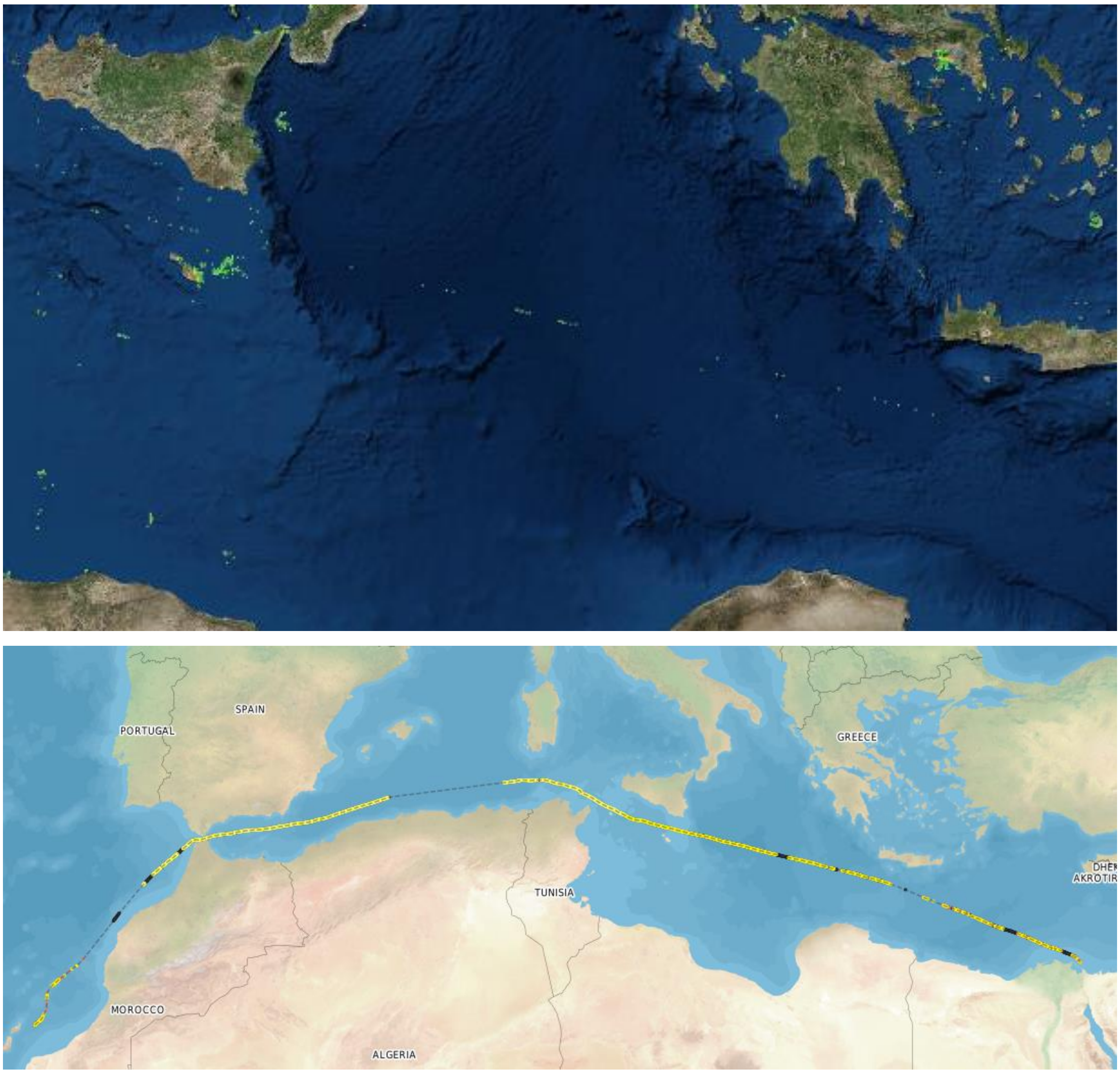
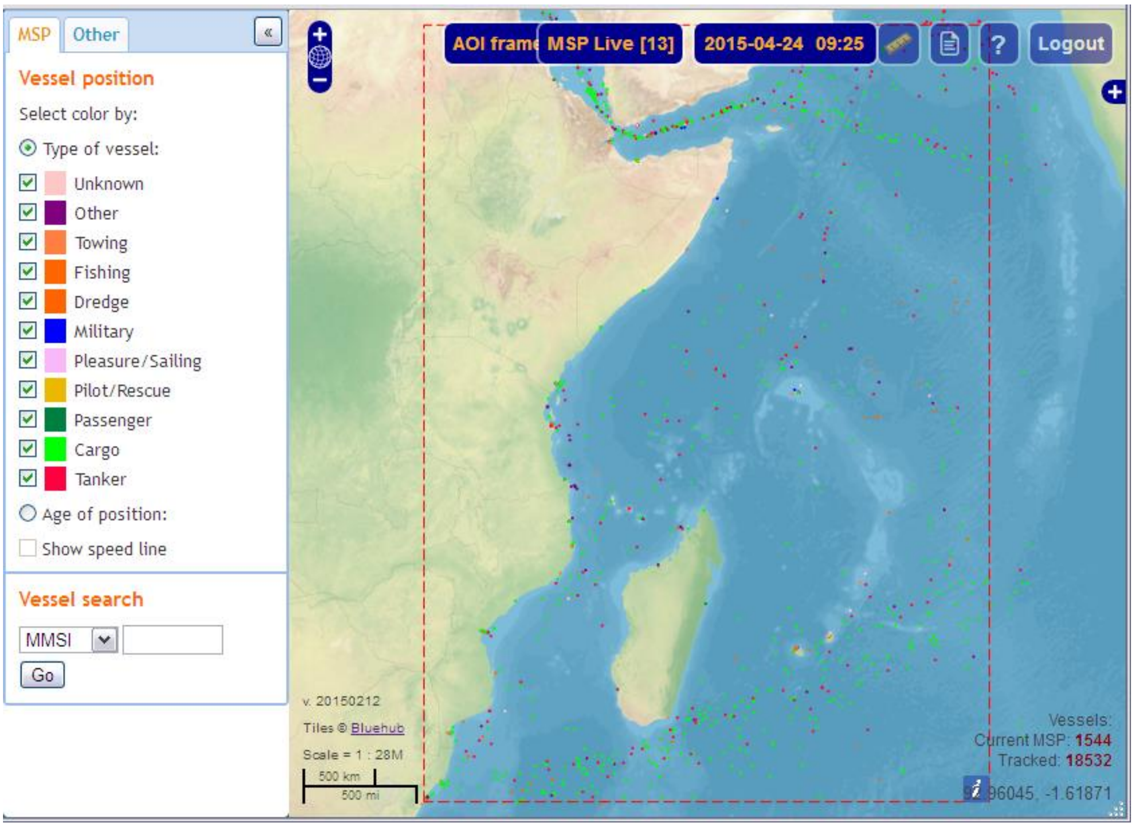


Figure 2. Top: Three-day proximity indication shown as green dots on a map. The trail of dots across the figure is caused by two ships that have travelled together across the Mediterranean, as shown in the multi-day track in the bottom plot.

4 EXAMPLES FROM THE WESTERN INDIAN OCEAN

The PMAR-MASE project for “Piracy, Maritime Awareness and Risks” was carried out by JRC under the “MAritime SEcurity” program for the Eastern-Southern Africa / Indian Ocean (ESA/IO) region. The MASE program is funded by the EU, and the PMAR-MASE project was overseen by the Indian Ocean Commission (IOC). In PMAR-MASE, the Maritime Situational Picture of the entire Western Indian Ocean based on automatic ship position reports (as in Fig. 3) was continuously provided in real-time to two operational authorities in the region, viz., the IOC's Anti-Piracy Unit in the Seychelles and the Regional Maritime Rescue Coordination Centre of the Kenya Maritime Authority in Mombasa. This was done during one year starting 15 Sep 2014 [13].



MSP | Other

Vessel position

Select color by:

● Type of vessel:

- ☑ Unknown
- ☑ Other
- ☑ Towing
- ☑ Fishing
- ☑ Dredge
- ☑ Military
- ☑ Pleasure/Sailing
- ☑ Pilot/Rescue
- ☑ Passenger
- ☑ Cargo
- ☑ Tanker

○ Age of position:

□ Show speed line

Vessel search

MMSI

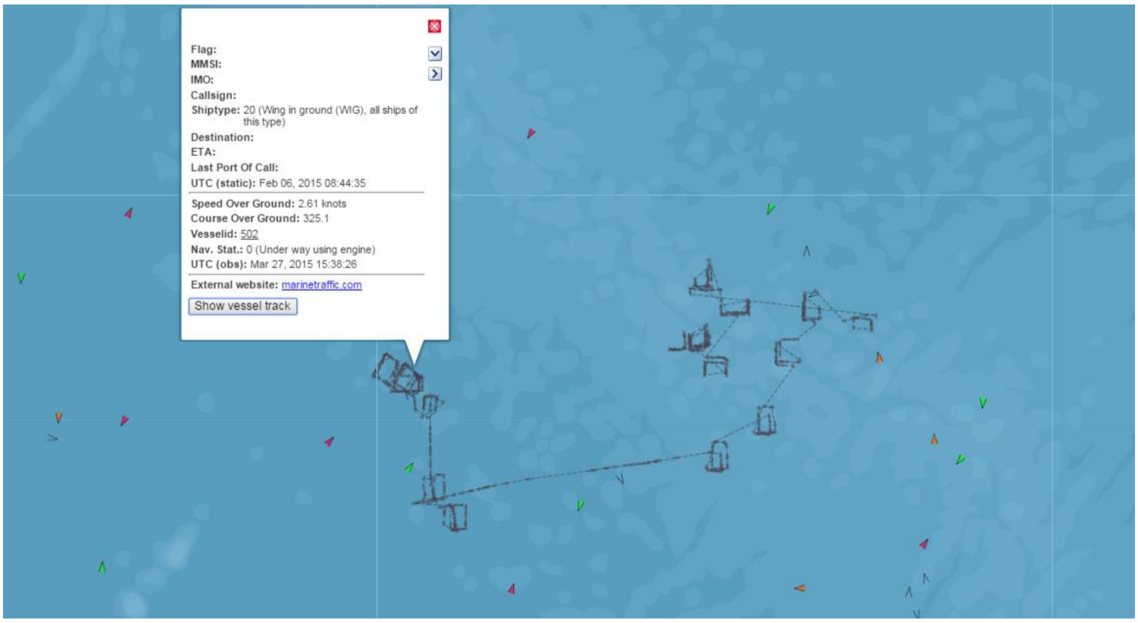
Go

Vessels:
Current MSP: 1544
Tracked: 18532

Figure 3. The ship traffic in the Western Indian Ocean on 24 Apr 2015, 09:25 UTC. The monitored area was between 31° and 68° East and between 30° South and 19° North (red box).

Under PMAR-MASE, ship reporting data were collected from satellite AIS, coastal AIS and LRIT. The satellite AIS data came from government-operated satellites (Norwegian Coastal Administration / Norwegian Defence Research Establishment) and from commercially operated satellites (companies exactEarth, SpaceQuest, and ORBCOMM/LuxSpace). In total, between 11 and 17 AIS satellites were used simultaneously, the number varying throughout the year of the trial. Coastal AIS data came from the international government-operated MSSIS network and commercial networks. LRIT data came from the Flags that use the EU LRIT CDC. On average, 570k ship position reports were received daily from all these sources together, representing somewhat more than 1,500 different ships on average daily within the PMAR-MASE area.

Anomalies, or at least inconsistencies, may be found by inspecting the tracks of vessels. Fig. 4 shows the 20-day track of a ship that in its AIS message is identified as being of the type "Wing In Ground". Its track, however, shows a peculiar pattern that is not consistent with that declared type. Instead, the shape of the track points to fishing activity. Tuna fishing, with longliners and purse seiners, is an important economic activity in the Indian Ocean, but also one that must be carried out sustainably to prevent a future collapse. If control authorities would make a selection based on the AIS declared type as "fishing", this ship would not have shown up, and would have escaped notice.



Flag:
MMSI:
IMO:
Callsign:
Shiptype: 20 (Wing in ground (WIG), all ships of this type)
Destination:
ETA:
Last Port Of Call:
UTC (static): Feb 06, 2015 08:44:35

Speed Over Ground: 2.61 knots
Course Over Ground: 325.1
Vesselid: 502
Nav. Stat.: 0 (Under way using engine)
UTC (obs): Mar 27, 2015 15:38:26

External website: marinetraffic.com

Figure 4. The 20-day track of vessel, revealing a characteristic pattern of fishing activity. The coloured arrowheads show the instantaneous ship traffic. (Identification information has been removed from the interrogation box.)

Fig. 5 displays the density of the slow-moving component of the ship traffic in the Western Indian Ocean during two periods of one month. Left for November 2014, right for April 2015. Coastlines are drawn in black and 200 nautical miles ranges in magenta. The densities were computed using position reports from satellite AIS and EU LRIT. The AIS data are very irregularly sampled, related to the overpass times of the satellites and to the successful reception of the AIS messages. Gaps of many hours in the series of messages received from a ship are very common. The gaps also vary per individual ship, apparently depending on the transmission characteristics of the AIS equipment on the individual ships. Therefore, a re-gridding is necessary before making density maps. Based on the received position reports, the track of each ship was reconstructed with a maximum extrapolation time of 9 hours, and resampled at 15 min intervals. From that, a density map was constructed to give the average number of ships that are present per square degree at any one time. To map the presence of slow moving traffic, in Fig. 5 only ship positions were counted that have a velocity of maximum 6.5 knots. Outside of the port and anchor areas and away from the coast, this map predominantly shows fishing activity, plus some slow-moving transiting ships that can be recognised as linear features. In Fig. 5 left, it can be seen that fishing activity is concentrated in the southwest, mid-south and centre-mid-east. A few conspicuous empty areas encircled by activity can be seen northeast of Madagascar, a larger polygonal one that coincides with the magenta boundaries and above that a smaller circular one that is actually centred on Agalega Island. There is also no fishing activity visible within 200 miles of the Somali coast, and this is also true for most other months of the year. In the right-hand map of April 2015, most of the fishing activity is north of the centre. Both months display a presence of slow-moving traffic close along the Somali coast.

Against these normal patterns, deviations stand out as anomalies, as seen in the density maps or in the real-time data. Some blue points in Fig. 5-left in the otherwise empty convex areas northeast of Madagascar could indicate unwanted activity. And in the right-hand map, it can be seen that in April 2015, the fishing activity spills over to within the 200 nautical miles range of Somalia that is otherwise mostly empty.

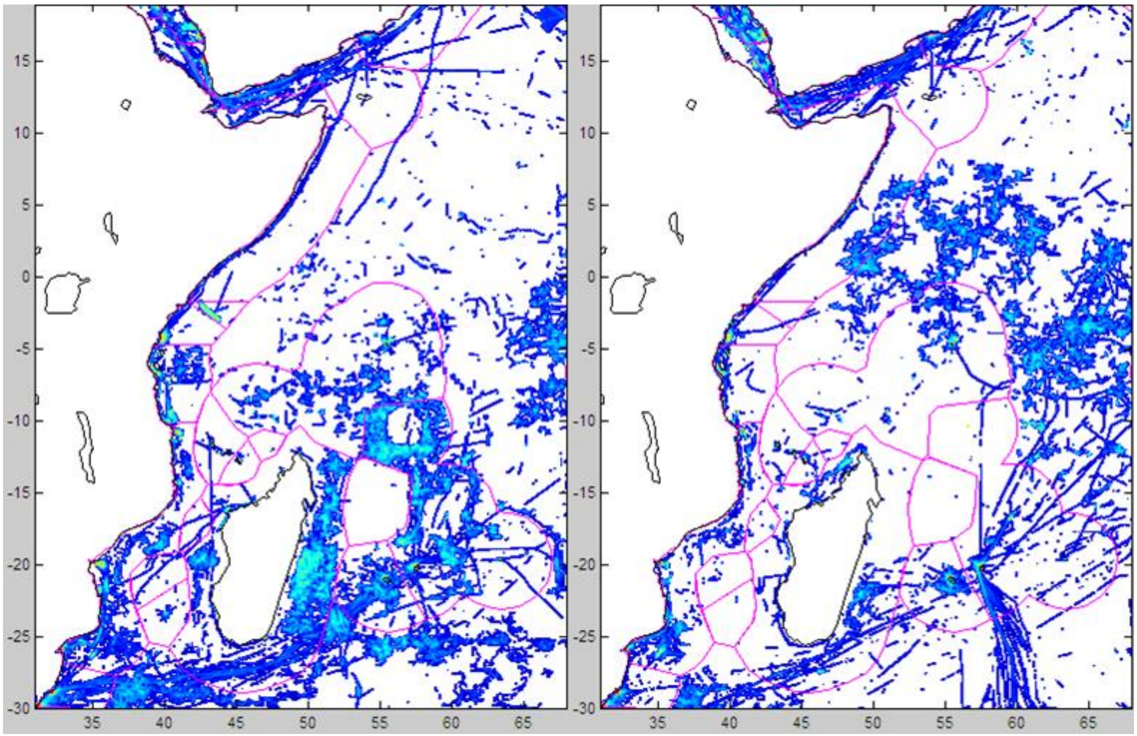


Figure 5. Density map of slow (< 6.5 knots) moving ship traffic in the Western Indian Ocean. Left, for the month of Nov 2014; right, for the month of Apr 2015. The colour scale is logarithmic from blue, cyan, green, yellow, orange to red. The high values occur only at the coast, in or near ports. Magenta lines are 200 nautical miles ranges.

5 CONCLUSIONS

The data from automatic ship reporting systems constitute rich grounds to search for maritime activities that compromise the security, safety or sustainability of the seas. Considering that most of the maritime activities are innocent, and that the sheer large amount of the ship reporting data presents a challenge to their analysis, the definition of anomalies as events that deviate from normal patterns is a useful approach to find potential risks.

Defining anomaly situations that flag risks efficiently is still a field of ongoing development. What really represents a risk situation is strongly dependent on local circumstances and on many external factors outside the domain of the ship positions and tracks. Errors and incompleteness in the data – especially for AIS, much less so for LRIT – throw up false anomaly conditions, forcing major efforts in the design of algorithms that do not mistake outliers due to data errors for ship behaviour anomalies.

A few examples were shown of anomalies detected in combined AIS and LRIT data, that rely partly on automatic processing and partly on subsequent human analysis. Although the processing of the bulk data for anomalies is (and has to be) automatic, the final interpretation remains up to the human analyst.

Acknowledgments

Satellite AIS data from NORAIS, AISSat-1 and AISSat-2 were obtained courtesy of the Norwegian Coastal Administration and the Norwegian Defence Research Establishment (FFI).

MSSIS data were obtained courtesy of the Volpe Center of the U.S. Department of Transportation, the U.S. Navy and SPAWAR.

LRIT data were obtained courtesy of the National Competent Authorities of the Flags that participate in the EU LRIT Data Centre, with the help of EMSA.

References

[1] IMO (1974). *SOLAS - International Convention for the Safety of Life at Sea*, Chapter V - Safety of navigation, Regulation 19, Art. 2.4, introduced by resolution MSC.99(73) adopted on 5 Dec 2000.

[2] Ibid., Regulation 19-1, Art. 2, introduced by resolution MSC.202(81) adopted on 19 May 2006.

[3] European Council (2009). *Council Regulation (EC) No 1224/2009 of 20 Nov 2009 establishing a Community control system for ensuring compliance with the rules of the common fisheries policy*, Art. 10.

[4] European Commission (2011). *Commission Directive 2011/15/EU of 23 Feb 2011 amending Directive 2002/59/EC of the European Parliament and of the Council establishing a Community vessel traffic monitoring and information system*, Art. 1.2.

[5] Alvarez, M., Fernandez Arguedas, V., Gammieri, V., Mazzarella, F., Vespe, M., Aulicino, G. and Vollero, A. (2016). *AIS Event-Based Knowledge Discovery for Maritime Situational Awareness*. 19th International Conference on Information Fusion.

[6] Pallotta, G., Vespe, M. and Bryan, K. (2013). *Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction*. Entropy, 15(6), pp.2218-2245.

[7] Fernandez Arguedas, V., Pallotta, G. and Vespe, M. (2014). *Automatic generation of geographical networks for maritime traffic surveillance*. Proc. 17th International Conference on Information Fusion (FUSION), IEEE, pp. 1-8.

[8] Alessandrini, A., et al. (2014). *Data Driven Contextual Knowledge from and for Maritime Situational Awareness*. Context-Awareness in Geographic Information Services (CAGIS 2014): 39.

[9] Vespe, M., Greidanus, H., Santamaria, C., Barbas, T. (2015). *Knowledge Discovery of Human Activities at Sea in the Arctic using Remote Sensing and Vessel Tracking Systems*. Proc. Joint WMU-IMO-Arctic Council International Conference ShipArc 2015, Malmö.

[10] Vespe, M., Gibin, M., Alessandrini, A., Natale, F., Mazzarella, F., Osio, G.C. (2016). *Mapping EU fishing activities using ship tracking data*. Journal of Maps, DOI: 10.1080/17445647.2016.1195299.

[11] Camossi, E., Dimitrova, T. and Tsois, A. (2012). *Detecting Anomalous Maritime Container Itineraries for Anti-fraud and Supply Chain Security*. In Proc. 2012 European Intelligence and Security Informatics Conference (EISIC 2012), ISBN 978-0-7695-4782-4, pp. 76-83.

[12] Vespe, M., Greidanus, H. and Alvarez, M. (2015). *The declining impact of piracy on maritime transport in the Indian Ocean: Statistical analysis of 5-year vessel tracking data*. Marine Policy, 59, pp.9-15.

[13] Greidanus, H., Alvarez, M., Gammieri, V., Santamaria, C., Alessandrini, A. and Argentieri, P. (2015). *Maritime Awareness Systems Performance in the Western Indian Ocean 2014-2015 – Results from the PMAR-MASE project*. JRC Technical Report JRC97935, EUR 27612 EN, ISSN 1831-9424 (online), Luxembourg: Publications Office of the European Union. doi:10.2788/420868.

SMUGGLING RADIOACTIVE MATERIAL – A DEMONSTRATION EXERCISE IN THE FRAMEWORK OF EU-PROJECT EDEN

Sebastian Chmel[1], Hermann Friedrich[1], Jeannette Glabian[1], Theo Köble[1], Monika Risse[1], Stefan Ossowski[1], Olaf Schumann[1], Luigi De Dominicis[2], Antonio Palucci[2], Colin Hetterley[3] and Derek Jordan[3]

[1] *sebastian.chmel@int.fraunhofer.de*
Fraunhofer-Institut für Naturwissenschaftlich - Technische Trendanalysen (INT),
Appelsgarten 2, D-53879 Euskirchen (Germany)

[2] *luigi.dedominics@enea.it*
ENEA - Italian Agency fro the New Technologies, Energy and Sustainable Development
Via E. Fermi 45 - 00044 Frascati (Italy)

[3] *colin.hetterley@baesystems.com*
BAE Systems (Operations) Limited, Warwick House, PO Box 87, Farnborough
Aerospace Centre, Farnborough, Hants, GU14 6YU, UK

Abstract

In the framework of project EDEN – a European FP7 Demonstration Project with 36 partners from 15 countries - different field demonstration exercises were performed to present countermeasures against attacks or accidents involving chemical, biological, radioactive, nuclear or explosive materials (CBRNE). During each exercise a number of tools provided by project partners and external suppliers were demonstrated in action. The present presentation focuses on such a demonstration simulating the smuggling of radioactive material, which was organized by Fraunhofer INT and executed at ENEA Research Centre in Frascati, Italy. The demonstration comprised two scenarios: First the attempt to smuggle a radioactive source at a border crossing station equipped with different detection systems and secondly a blackmailing attempt, where the source was hidden in a car in a public parking place and covert search was necessary. In both cases it was demonstrated that the radioactive material could be remotely detected, localized and identified successfully.

Keywords: Field demonstration exercise, RN material, covert search, radiation portal monitors, EU FP7 demonstration project.

1 INTRODUCTION

The EDEN (End-User Driven Demo for CBRNe) Demonstration Project is a European Union-wide collaborative project which is funded within the 7th framework program and involves a consortium of 36 members from 15 countries, including practitioners, corporate stakeholders, universities and research institutes [1]. In the three-year project, which will be finalized at the end of 2016, a central question is, how and with which tools one can counteract deliberate attacks or accidents involving chemical, biological, radioactive, nuclear or explosive materials. The aim of the project is the demonstration of a comprehensive system of systems of measures against such events that require prevention before they can happen, response if they occur, and recovery afterwards. In the framework of the project different related methodological and technical tools were compiled into systems, further developed, tested and demonstrated in exercise scenarios. The tools include for example protocols, measuring devices, communication systems or simulation programs. The EDEN solutions matured during the project give the opportunity to evaluate large scale integration of CBRNE Security and Counter-Terrorism techniques whilst improving cross border cooperation and interoperability. A sustainable impact will be achieved by an open and secure internet platform, the EDEN Website, where a database with tools and expert services etc. can be addressed by selected suppliers and practitioners - also after the project has ended.

Aside from large scale demonstrations regarding biological and chemical risks in a food facility, multi-chemical attacks in chemical plants and public areas, and a radiological accident in a nuclear power plant, several medium size demonstration exercises were executed. The present presentation focuses on a medium sized thematic demonstration, which was organized by Fraunhofer INT and executed at the ENEA Research Centre in Frascati, Italy in 2015, together with another demonstration organized by ENEA. During these exercises tool suppliers which were not a member of the EDEN consortium, but were associated to EDEN via the so called "EDEN supplier platform" or the "EDEN SME platform" had the opportunity to get their tools involved, too.

The demonstration with the topic "Smuggling radiological material and subsequent blackmailing attempt" comprised two parts: In part one – a 'border crossing scenario' – a radioactive source was hidden in a car and then it was simulated that the driver tried to smuggle the material across a border, where different types of detector systems were deployed. In part two – a 'parking place scenario' – it was assumed that another group of the fictitious smugglers had been successful in transporting the radioactive material across the border and that there were hints, that the material was hidden at a public car park. In this case a covert search was necessary.

2 THE BORDER CROSSING SCENARIO

The border crossing scenario was demonstrated at an area inside the ENEA site, where several deployable radiation portal monitors (for vehicles as well as for pedestrians) were installed to simulate a border crossing station equipped with detectors out of the EDEN store. While doing so the high flexibility of the vehicle monitors could be shown: It was possible to set up the systems within 20 minutes, even by a technical team without previous experience with the tools.

Since the devices had to be tested with real radioactive sources, for safety reasons only the technical teams who had to operate the tools were allowed to be present at the demonstration area. All the observers – experts and end users - were accommodated in a conference room 300 meters away. Therefore streaming video into the conference room was necessary, where a facilitator explained and commented the scenario and the tools. To give insight in the functionality and the quality of the tools and the demonstrated procedures simultaneously the visual display of the measurement devices was shown on another screen. This demonstrated at the same time the capability to transfer the data directly to a control centre or another reach back unit.

During the border crossing scenario the following tools to prevent illicit trafficking of radioactive material were demonstrated (provider in brackets):

1. Portal Monitor JANUS (Indra) [3]
2. Radiation Portal Monitor PM 5000 C (Polimaster Europe) [4]
3. Deep Discovery Pedestrian Portal (Symetrica) [5]
4. Handheld device VeriFinder (Symetrica) [6]
5. Spectroscopic Personal Radiation Detector PM 1704 M (Polimaster Europe) [7]

The radioactive source, a Co-60 source shielded with lead, was hidden in the boot of a car. When the car approached the simulated border and passed the installed portal monitors with low velocity, the portal monitors instantaneously gave an alarm (optically and acoustically) and the measurement results could be seen on the related displays. The assignment to the car in question was unique.

The driver then was separated from the car and checked via the portal monitor for pedestrians. He pretended to have had a medical treatment and this would be the reason for the radiation alarm. Indeed the pedestrian monitor could detect this – it was simulated with a weak Ba-133 source. This source could not only be detected but also identified by the system via a unique spectral processing system that enhances the native resolution of the used NaI scintillation detectors in the pillars to a high quality performance. The capability to identify real medical isotopes was already proved with the system in the former EU FP7 project, SCINTILLA [2], with real patients in a nuclear medicine department of a hospital.

Parallel to the investigation of the person the car was checked systematically with the handheld devices VeriFinder and PM 1704 M and in this way the hidden source was found. Also an identification of the isotope could be demonstrated. So the simulated attempt to smuggle and mask the radioactive source with another one was elucidated successfully.

3 THE PARKING PLACE SCENARIO

The second part of the demonstration was performed at a parking place inside the ENEA site close to the area where the first part was conducted. A number of cars were parked and in one car a shielded radioactive source was hidden. The task was to find the source via covert search. Two different ways of search were demonstrated: First a search with a measurement system, installed in an ordinary car, and then a search by foot with a backpack detector was performed. Again the visitors could participate via streaming video.

During the parking place scenario the following tools were demonstrated (provider in brackets):

1. Generic Ground Station (BAE Systems) [1]
2. First Responder Equipment (BAE Systems) [1]
3. DeGeN measurement car (Fraunhofer INT) [8]
4. Backpack detector (Symetrica) [9]

The actions were conducted in a coordination post, where the measurement data were transferred and the mission could be planned and supervised. This was done amongst others with the help of the Generic Ground Station, a work station for the Incident Commander, which allows real-time tasking, location tracking and display of surveillance data from multiple assets. One of these assets was the First Responder equipment (FR). The latter is a man-portable equipment consisting of an android mobile phone application linked to sensors (e.g. radiation sensors) with Bluetooth interface. First responder tasking and safety hazard information were transmitted to the first responder, and location and data was transmitted back. The real-time data communications were transmitted between the Generic Ground Station and first responders using personal role radios in this demonstration, however the system is also designed to work with WiFi networks.

The first search was performed with the car-borne measurement system DeGeN that consists of an array of gamma and neutron detectors, powered by a specific energy management system. Neutron slab counters filled with He-3 and 12 litres plastic scintillation detectors are placed on both sides of the car, allowing directional measurements of the gamma dose rates and neutron counts. With this capability it was possible to identify the car with the hidden radioactive source already during the first passing and verified during a second passing. The scintillators are so called NBR (natural background rejection) detectors which enable the user to distinguish between natural and artificial radiation. For the latter it distinguishes between artificial low and middle energy region, which was indicated in the demonstration. Those regions are consistent with the energy regions for Cs-137 (low energy) and Co-60 (middle energy). The measurement results were displayed on a touch screen monitor mounted at the instrument board. The position of the car is recorded by GPS synchronized with the measurement data. All measurement results could be seen remotely on a screen in the conference room in real time.

An electrically cooled germanium detector is included in the measurement system and can be used for identification of the nuclear or radioactive material. Since it is a hand-held device this can be done either on-site after the radioactive material has been located by means of the car's built-in detectors or from inside the car as the detector can be remote controlled from the monitor in the front. Also this capability was demonstrated in the scenario and the Co-60 source was identified.

The second covert search was performed on foot with the backpack detector, where the software is similar to the software used for the pedestrian portal monitor by Symetrica. During the demonstration the backpack device was carried by an expert and operated with a tablet as an operation unit. The final version of the tool shall be equipped with an ergonomic readout which enables the carrier to do covert search measurements. In contrast to the measurement shown with measurement vehicle DeGeN the backpack enables one to do measurements at positions which cannot be reached with a car. The display was also transferred into the conference room. When the count rate increased beside the car with the hidden source the measurement situation was optimized in that way that the person pretended to tie the shoelaces and did an identification measurement, where again Co-60 could be identified.

4 CONCLUSION

The demonstration was observed by 110 visitors, experts and stakeholders from 9 countries. Since the visitors were not allowed to be present in the exercise area in person for safety reasons, the streaming video was the only possibility to let them take part in the event and it turned out that the simultaneous presentation of the video of the activities together with the visual display of the measurement results on another screen was a good way to let observers get insight in the quality of the tools and the procedures. Also the presence of a facilitator who explained everything in detail was acknowledged. The visitors had the opportunity to have a closer look at the involved tools and to use them after the scenarios were finished and the radioactive sources were removed. An evaluation showed that an added value was attested to most of the tools. In the border crossing scenario as well as in the parking place scenario with the covert search it was demonstrated that the radioactive material which was even shielded could be detected, localized and identified successfully and also a simulated masking attempt could be elucidated.

REFERENCES

[1] EDEN Security [online] [viewed 20 June 2016]. Available from: https//eden-security-fp7.eu

[2] SCINTILLA Project, 2012. SCINTILLA - Welcome to the SCINTILLA Project website || a pan-European research collaboration funded by the European Union [online] [viewed 20 June 2016]. Available from: http://www.scintilla-project.eu

[3] Security Systems JANUS [online] [viewed 20 June 2016]. Available from: http://www.indracompany.com/sites/default/files/janus_2.pdf

[4] Deployable Radiation Portal Monitor - PM5000C-05M [online] [viewed 20 June 2016]. Available from: http://www.polimaster.com/products/radiation_portal_monitors_/pm5000c-05/

[5] Symetrica Security Pedestrian Portal Data Sheet Handheld [online] [viewed 20 June 2016]. Available from http://www.symetrica.com/contact by email to info@Symetrica.com

[6] Symetrica Security VeriFinder Handheld [online] [viewed 20 June 2016]. Available from: http://www.symetrica.com/verifinder-2

[7] Spectroscopic Personal Radiation Detectors PM1704/M/GN [online] [viewed 20 June 2016]. Available from: http://www.polimaster.com/products/spectroscopic_personal_radiation_detectors/_1704/

[8] Risse, M.; Berky, W.; Chmel, S.; Friedrich, H.; Glabian, J.; Köble, T.; Ossowski, S.; Rosenstock, W.; Schumann, O.; Kronholz, H.-L.: Car-borne measurements of radioactive material, 3rd International Symposium on Development of CBRN Defence Capabilities, Bonn: German Association for Defence Technology, Centre for Studies and Conferences, 2015, S. 1216-1251. – URN:nbn:de:0011-n-3673179

[9] Symetrica Security Backpack Data Sheet Handheld [online] [viewed 20 June 2016]. Available from http://www.symetrica.com/contact by email to info@Symetrica.com

MOBILE BIOMETRICS DEVICE FOR FUTURE BORDER CONTROL

Bernhard Strobl[1] and Eduardo Monari[2]

[1] *bernhard.strobl@ait.ac.at*
AIT – Austrian Institute of Technology GmbH, Department Digital Safety and Security,
Donau-City-Straße 1, 1220 Vienna (Austria)

[2] *eduardo.monari@iosb.fraunhofer.de*
Fraunhofe Institute of Optronics, System Technolgies and Image Exploitation (IOSB)
Fraunhoferstraße 1, 76131 Karlsruhe (Germany)

Abstract

Preliminary results and a short demonstration of the prototype device of the European funded project MobilePass (GrantNr.: 608016). MobilePass developed technological advanced mobile equipment for border control authorities. In the project advanced technology beyond state-of-the-art has been done for:

(i) dedicated device for border control officers

(ii) cooperative and fast face capturing and verification

(iii) contactless multiple fingerprint capturing and verification and

(iv) device security and trusted platforms.

Keywords: contactless fingerprint scanning, border control device, trusted platform module, cooperative face verification

1 DEDICATED DEVICE FOR BORDER GUARD OFFICERS

In the beginning of the project there was an in depth analysis [11] of the actual need of the border guards to carry out the needed Schengen border code checks in a mobile way. These checks include checking the travel document (or eMRTD [9][10] passport) for security features, read the included RFID chip, do the necessary database queries to the relevant databases (e.g. SIS-II, Visa, Interpol and eventual national ones), and verify that the traveller is the authenticated holder of the document by the means of biometrics (face verification and fingerprint verification). In addition to this Schengen requirements, Border guards defined additional needs as the device should be able to operate at least one whole shift, it should be lightweight (less 0.5 kg), it should be able to be operated with one hand (while the other is holding the travel document) and it should have included enough processing power for fast biometrics. There are try-outs and test to use modern smartphones for this purpose, but the project build a dedicated completely European build device with an adapted LINUX operations system. There are more technical requirements [12] to mention, a list of more than 200 entries had been worked out by the project.

The consortium partners developed a prototype of a device, based on several requirements formulated by the border guards during the requirements capturing phase of the project.

1.1 Dedicated device

It turned out that there are some devices available, but not really suited to fulfil the work of the guards.

The developed solution consists of a wrist worn prototype and a hip-worn passport scanner. This is one possibility to operate the system, but the reader can also be omitted in later developments because RFID reading can also be done in the developed device itself. The prototype includes a sunlight readable display; it can be worn on the wrist of the border guard so both hands are free for passport inspection. It includes a camera for fingerprint, facial and MRZ (machine readable Zone) capturing, it includes a special lighting system for fingerprint or face illumination. Novel development techniques, like HLS (High Level Synthesis) for FPGA´s (Field Programmable Gate Arrays) and the usage of powerful heterogeneous multicore chipsets will enable implementation of CPU-demanding algorithms for biometrics and image processing.

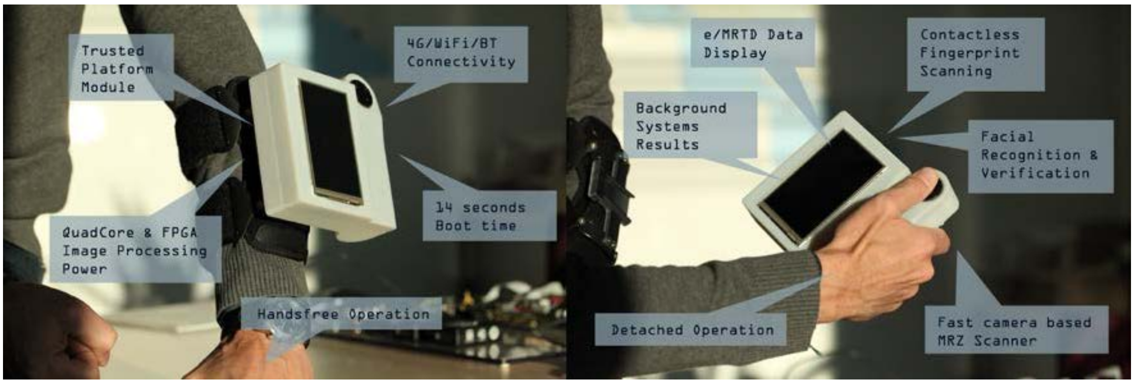

Trusted Platform Module
4G/WiFi/BT Connectivity
14 seconds Boot time
QuadCore & FPGA Image Processing Power
Handsfree Operation
e/MRTD Data Display
Contactless Fingerprint Scanning
Background Systems Results
Facial Recognition & Verification
Detached Operation
Fast camera based MRZ Scanner

Fig 1: Summary of MobilePass Device functionality and operating modes

1.2 Hardware setup

This platform enables also other solutions in the embedded domain. The design goals were to have a versatile, high performance adaptable platform for image processing which also can be used in a mobile way. The CPU is a trusted platform enabling high secure applications like biometric scanning and verification for border control purposes. As accelerator a plugin FPGA Module provides enough processing power for complex real-time applications. Its overall power consumption does not exceed 10W (when every component is utilised to 100%) which is much lower compared to a laptop and the LINUX boot time is only 14 seconds. It differentiates from smartphone hardware with the following unique features: complete source for adaptions available, industrial components with long availability, scalability in terms of processing power, accelerator hardware with scalable FPGAs, secure boot capabilities and extended temperature range.

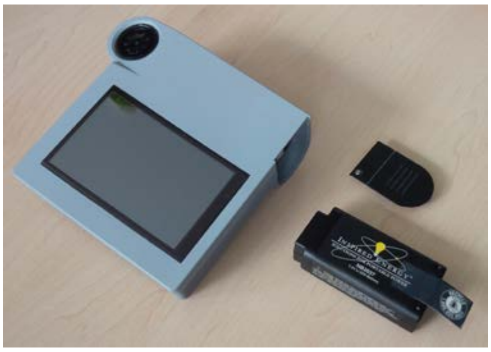


Fig 2: MobilePass Device with exchangeable battery

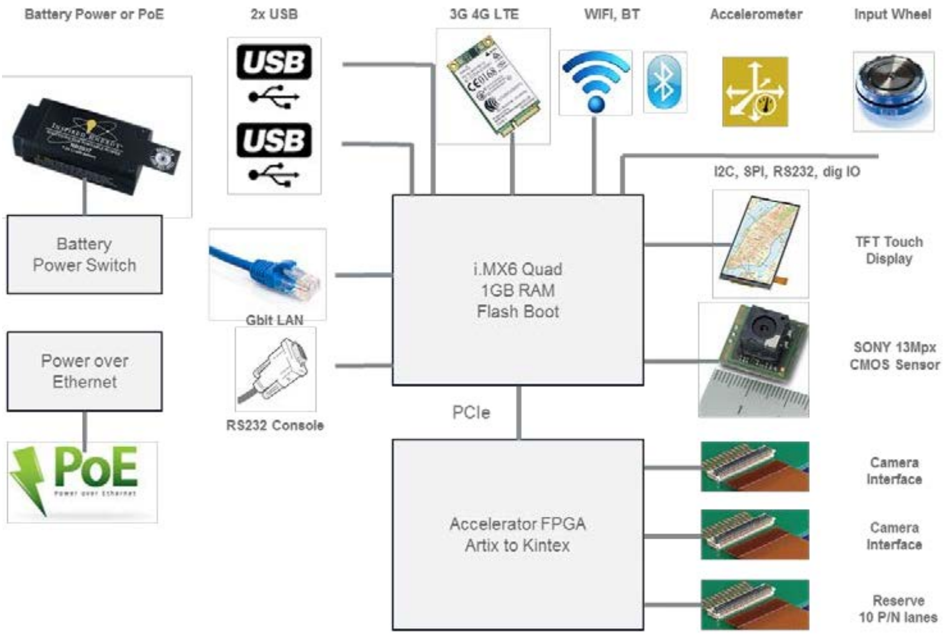


Fig 3: Summary of MobilePass Device elements and future usages

1.3 Device security

The consortium carried out research and development of electronics and algorithms embedded in a trusted platform module with secure boot mechanisms to raise resilience against rootkits, trojans, viruses, worms, key loggers, hacking, offline & reverse engineering. One important requirement was device security, this includes the used transmission channels, but also the hardware itself, as it should be highly impossible to hack into the device if unauthorized people get hands on the unit. No change of Operating System or Application Software after deployment should be possible.

The device itself is a so called TPM [4][5][6][7], a trusted platform module. This enables an advanced boot mechanism called secure boot: the boot-image (including the operating system and the application) is hashed or encrypted. At boot time the hash value or the decryption key are used to verify if the software is authentic. In case of an encrypted boot image even the content of the FLASH memory of the device is secured and cannot be read out or reverse engineered. The decryption key, respectively the hash value is “burned” into the Silicon, but access mechanisms inside the silicon are destroyed and can´t be read out (except CPU itself at boot time).

The CPU itself also incorporates hardware counteractive measures: At setup time, an electronic signal is applied to electronics and complete assembly. The response signal is captured and analysed. The response signal is compared to the stored “normal” signal and if the response shows deviations above threshold, the device does a denial of service, e.g. if the device is opened.

Additional security measures are possible but had not been implemented which would lead to a denial of service from the device side:

- “Dead Man” detection: if the operator does not authenticate within a given time interval
- Movement of device in unauthorized area (with GPS and local stored operating zone)

1.4 Communication Security

As this mobile device will transport, capture and process biometric and personalised data it is of highest importance to have secure communications capabilities. The developed system secures in- and outgoing transmissions by the following means: a firewall on an embedded device, performing the following tasks:

- Intrusion detection (IDS)
- Stealth port scans
- Common Gateway Interface (CGI) web attacks
- Operation System (OS) fingerprinting attempts
- Traffic flow anomalies

To assess the vulnerability of the system the future plan is to carry out some tests with a vulnerabilities assessment system

- Penetration Tests
- Black, white and grey box tests
- Vulnerability scanner, Security scanner, Vulnerabilities Assessment System

2 COOPERATIVE AND FAST FACE CAPTURING AND VERIFICATION

The face verification and capturing method is completely carried out on the device. When the function is selected on the device the camera system constantly captures live images and compares them to the ones in the chip of the e(Passport). The border guard points the device to the traveller and a continuous capturing process is started. Only faces which are sufficient for verification are used. The software in the device detects closed eyes, too high tilt and yaw angles, etc. Only the best shots during the capturing phase are automatically selected.

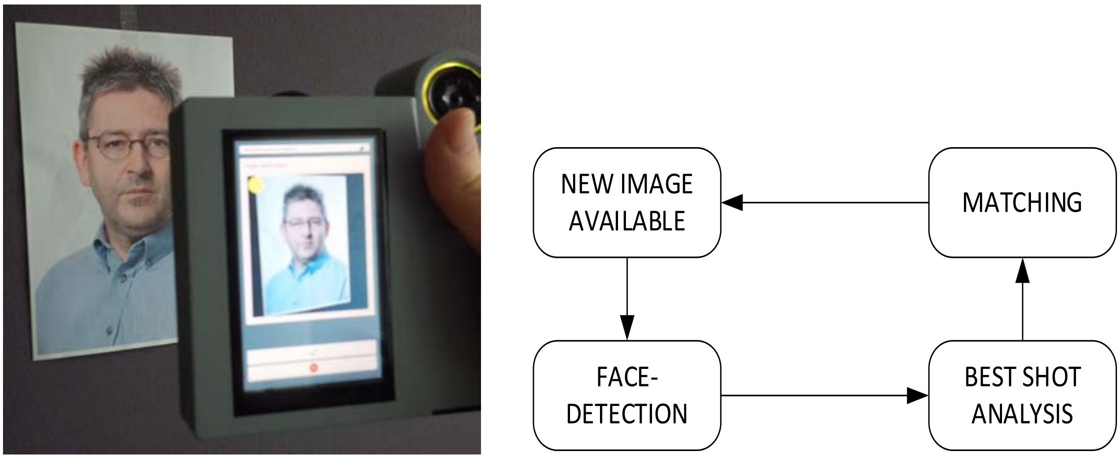


Fig 4: Picture shows how Facial Verification works on the device

Face analysis – including image enhancements, quality assessment as well as the verification is basically performed by the following steps:

1. Reference image has to be set in a first step. This reference image is provided by the VERIDOS workflow to the mobile device, after decoding the data from passport. Once reference face image from passport is available, video processing for face analysis is executed.

2. Using camera driver handler, provided by the main application on MobilePass device, video frames a grabbed and processed continuously by the integrated video processing engine. Analysis is performed each time, the current video frame is pushed to a face analysis module. A repeating loop as shown in Fig. 4 is used to grab video frames and perform the analysis loop. Hereby the following steps are performed by the face analysis library:
    a. Face Detection: To find area of interest in the current video frame, face detector is applied as a very first step. Hereby, FaceSDK provided by the partner VIDEMO is used.
    b. Best Shot Analysis: This step first estimates the level of sharpness of the captured face, also to avoid unnecessary further processing of motion blurred frames. Next, a learning-based (boost classifier) face quality assessment is performed to discard face images with too hard illumination conditions, side views, blurring/noise, etc. Only face images with a sufficient high quality are by passed to the matching algorithm, to avoid false positives due to low image quality.
    c. Matching: Face images of sufficient high quality are processed by the VIDEMO Face-Verification Library.

The result is a direct feedback as “match” or “no match” to the user. Typical processing time is 2 to 4 seconds.

3 CONTACTLESS MULTIPLE FINGERPRINT CAPTURING AND

The partners of the MobilePass consortium worked together for a novel method to capture and verify fingerprints in a contactless way captured by a camera. This novel method decrease the time that is needed to capture fingerprints and it is much less “invasive” for travellers as there is no direct contact to a device or a surface. This also improves the hygienic situation. The implemented method is not a one-shot function as usual when operating a camera, the capturing method continuously measures the quality of the taken fingerprints, by applying the NFIQ (NIST Fingerprint Image Quality) algorithm and a special sharpness measure. A special best-shot selection method automatically takes the fingerprint image with the highest quality for verification.

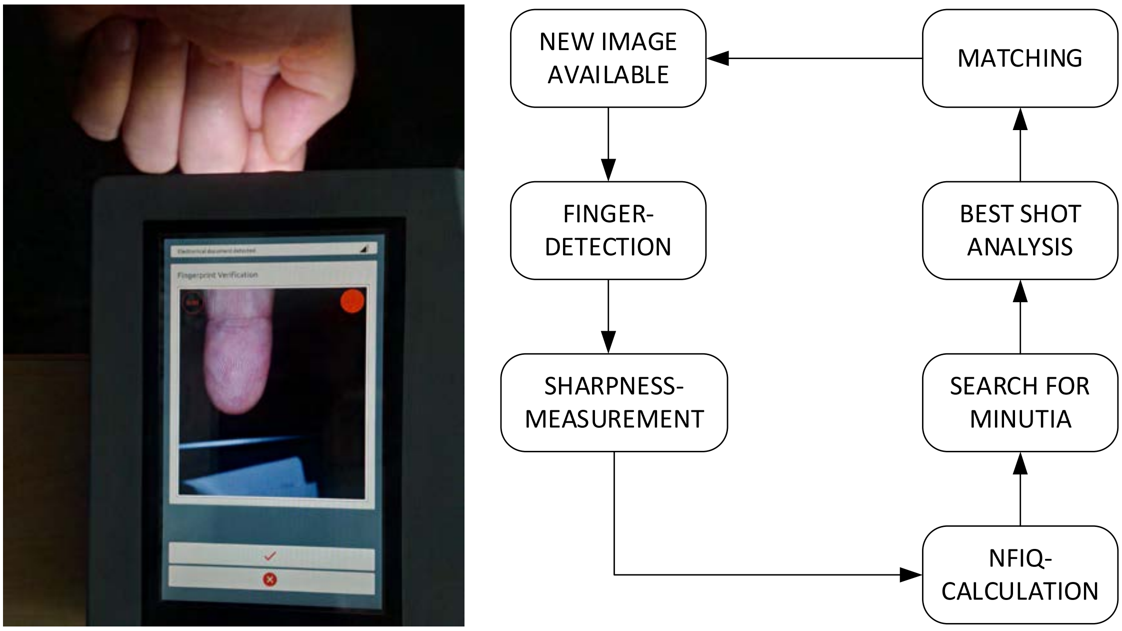


Fig 5: Picture shows how Fingerprint Verification works on the device

Fingerprint analysis – including image enhancements, quality assessment as well as the verification is basically performed by the following steps:

1. Reference image has to be set in a first step. This reference image is provided by the VERIDOS workflow to the mobile device, after decoding the data from passport. Once reference image is available, video processing for verification is executed.
2. Similar as for face analysis video frames a grabbed and processed continuously by the integrated video processing module. As shown in Fig. 4 the following steps are performed inside the fingerprint analysis library:
    a. Finger Detection: To find area of interest in the current video frame, finger detector is applied as a very first step. Hereby, Fraunhofer IOSB developed several algorithms and performed a benchmark of the performances [1][2]. The best approach – call edge pair detector – has been finally integrated in this library. The result of the detector step is a rectangle-shaped area of interest, which is in focus of further processing by the next steps.

    b. Sharpness Measure: This step first estimates the level of sharpness of the captured finger. This is an important metric, to decide, if further processing (and usage of CPU load) makes sense or not. If the finger image is of sufficient (or minimal sharpness) second, pre-process the area of interest in terms of de-noising and contrast enhancement. Also, color channels are re-weighted to avoid clutter caused by skin color. Also, de-blurring algorithms have been evaluated for image enhancement at this step. However, since shutter time is short enough in practice, for performance reasons, this kind of enhancement has not be enabled as default feature.

    c. If image of the finger fulfills minimum criteria (defined by a threshold) for sharpness (focus distance of the finger approximately correct), as a further quality level, NFIQ [3] (NIST Fingerprint Image Quality) is determined using NBIS library.

    d. Search for Minutae / Best shot analysis: A NFIQ-threshold is defined heuristically to determine, if available number and quality of minutiae is sufficient for our purpose. If not, the current frame is discarded for performance reasons. Also sharpness measure is used in combination with NFIQ to evaluate the overall quality of the current fingerprint image. Only “sufficiently good” fingerprint (best shots) a further analysed by the matching algorithms, to avoid false positive validation.

    e. Finally “best shots” video frames are evaluated by NBIS fingerprint minutiae matching algorithm.

4 SUMMARY AND CONCLUSIONS

The partners of the MobilePass consortium developed a prototype of a device that can do contactless fingerprint verification, face verification, has a secure operating system, is capable of showing results from backend systems and scanned document data.

As it was the intention of the MobilePass project also to evaluate how good these novel technologies work, an evaluation is foreseen at the border guard premises, either in Romania or in Spain. The analysis will be of qualitative and quantitative nature. These evaluations will take place in September and October 2016 when technical developments are done.

It is expected that the work of MobilePass will be extended by the BODEGA project which assesses human factors in border control. So the user interface of MobilePass will be improved and the developed device will be the test case for these improvements.

One conclusion of the project is that contactless fingerprint capturing is needed in mobile scenarios but it is necessary to further improve the speed of the fingerprint capturing technique.

REFERENCES

[1] C. Jonietz, E. Monari and C. Qu, "Towards Touchless Palm and Finger Detection for Fingerprint Extraction with Mobile Devices," Biometrics Special Interest Group (BIOSIG), 2015 International Conference of the, Darmstadt, 2015, pp. 1-8.

[2] Jonietz, C.; Monari, E.; Widak, H.; Qu, C.; Towards mobile and touchless fingerprint verification; Proceedings of the 12th IEEE International Conference on Advanced Video and Signal based Surveillance (AVSS) Workshops Karlsruhe, S. 1-6, IEEE, 2015.

[3] NIST Biometric Quality Homepage - NFIQ: http://www.nist.gov/itl/iad/ig/bio_quality.cfm

[4] Trusted Computing Group (TCG), Konsortium, Beaverton (Oregon), USA, www.trustedcomputinggroup.org

[5] Trusted computing architectures for a mobile IT infrastructure, Vijay Anand, Jafar Saniie, Erdal Oruklu, Southeast Missouri State University and Illinois Institute of Technology, Cape Girardeau, MO, USA

[6] Trusted Platform Module (TPM) Specifications. TCG - Trusted Computing Group

[7] Roots of Trust in Mobile Devices, ISPAB, February 2012, Andrew Regenscheid, NIST – national Institute of Standards and Technology

[8] Securing the core root of trust (malware, counterfeiting and IP theft in hardware), Ramesh Karri, ECE Department, NYU – New York University

[9] Machine Readable Travel Documents. Part 1, Machine Readable Passports – Volume 1, Passports with Machine Readable Data Stored in Optical Character Recognition Format. (ICAO Doc 9303; englisch;), International Civil Aviation Organization 2006, ISBN 92-9194-753-9.

[10] ICAO 9303 Machine Readable Travel Documents, Part 1- Machine Readable Passports. Volume 2 - Specifications for Electronically Enabled Passports with Biometric Identification Capability, 6th edition, 2006

[11] Axel Weissenfeld, et al, "Scenario list: Deficiencies, Handling problems Deliverable 1.1", MobilePass - A secure, modular and distributed mobile border control solution for European land border crossing points, FP7-SEC-2013-3-2-3

[12] Christoph Weiß, et al, "Vision and Requirements of the Future, Deliverable 1.3", MobilePass - A secure, modular and distributed mobile border control solution for European land border crossing points, FP7-SEC-2013-3-2-3

SENSOR FUSION SUPPORTING HIGH RESOLUTION RADAR FOR SECURITY APPLICATIONS

R. Herschel[1], S. Lang, N. Pohl

[1] *reinhold.herschel@fhr.fraunhofer.de*
Fraunhofer Institute for High Frequency Physics and Radar Technology (FHR),
Fraunhoferstr. 20, 53343 Wachtberg (Germany)

Abstract

Sensor fusion of millimeter wave radar imaging and optical 3D imaging is presented. A basic description of different sensor fusion approaches is provided before several examples of implemented sensor suite solutions are shown. This ranges from passenger and luggage screening to environment screening by LIDAR and radar measurement.

Keywords: Sensor fusion, sensor suite, security scanner, millimeter wave radar, 3D imaging

1 INTRODUCTION

Whenever optical imaging systems get to their limitations, radar imaging systems provide a promising alternative. This can be the case due to view restrictions caused by smoke, dust or fog, but also simply if imaging through walls or imaging of luggage is required. Radar has the great advantage that in the millimeter wave range many things get transparent, which they are not for visible light. Different to most camera technologies, radar systems do not only measure the power of the reflected radiation, but also its phase. This provides additional information which can be used for material analysis or real 3D imaging. On the other hand, visible light enables a higher resolution due to its far smaller wavelength. The suitability of each imaging approach depends on the desired application. However, instead of being seen as competitors, optical and radar imaging can be combined to give a more comprehensive set of image information. These multi-technological sensor-suites are of increasing importance for future security systems merging different fields of research.

In this contribution, different approaches for image sensor fusion are presented. The applications are focused on security systems for threat detection and rescue support. After a short introduction to the field of image sensor fusion, the combination of infrared imaging and millimeter wave person scanners will first be presented. Combined 3D images, based on the use of a time-of-flight camera in combination with RGB images and millimeter wave 3D radar images are shown as a further step of development. Additionally, a radar scanner is presented, which is capable of screening the environment in combination with a laser scanning system. The different systems are briefly presented and experimental results are shown to compare the different image sensors and to demonstrate the performance of those sensor suites. Together with a summary, an outlook will be provided, pointing out opportunities of radar-optic sensor suites for developing integrated imaging systems for future security solutions.

2 SENSOR FUSION

„Sensor fusion is a process, where data from different sensors or information sources is linked to generate new or more precise knowledge about physical quantities, events or situations.“ [1]

Sensor fusion should be more than only collected information from different sources. Instead, the used sensors should form a comprehensive sensor suite being far more than only the sum of its individual modules. The implementation mainly depends on the sensor application and the effort which can be spent in data analysis. Advantages of sensor suites can be a far better coverage of the measured scene, redundant measurements to avoid measurement outages or a more efficient use of the individual sensor. From a physical point of view one might differentiate between sensors using the same technology with slightly different parameters, such as multi-frequency band radar systems or sensor suites using completely different technologies as, for example, a combination of gas sensing and optical imaging. From a more abstract point of view three different architectures can be distinguished [2]:

1. **Complementary Integration**

   Equal sensors covering independent measurement ranges. Classical examples are multi-sector radars or cameras.

2. **Competing Integration**

   Measurements by equal sensors covering the same range are combined to enhance the quality of the measurement. The most well-known example is averaging of a measured quantity over time.

3. **Cooperative Integration**

   All sensors are used to obtain information which would not be accessible for a single sensor. This is commonly used for imaging such as stereo camera concepts or synthetic aperture radar.

Another way to look at sensor fusion concepts is the data flow within the sensor suite. Of course, the final aim is the centralized collection and fusion so that all architectures finally send all data to a single knot.

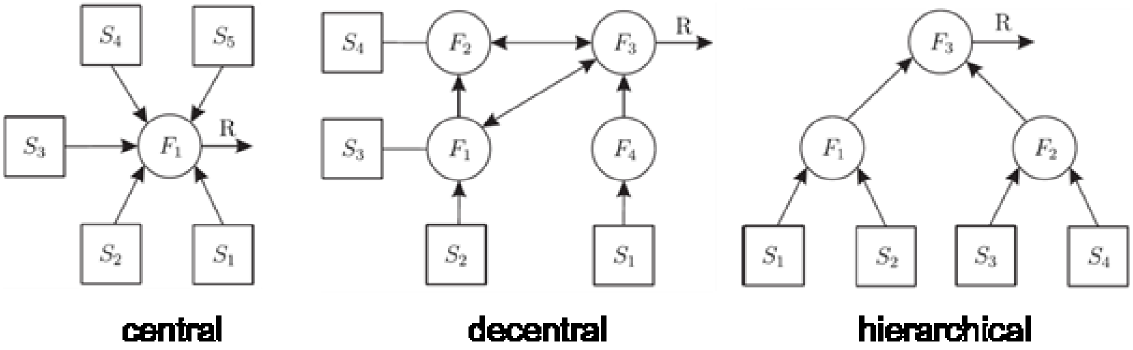


Figure 1: Principle architectures for sensor suites

The easiest implementation is the central architecture as shown in Figure 1. All sensors measure data independent of each other and send this to a central knot. Depending on the integration concept described above the collected data can than simply be fused within multi-sensor packages or be further processed to generate new data to be transmitted to the system. By principle this architecture does not provide the capability of feedback between different sensors. This can be obtained by decentral concepts. The information gained from one sensor is used to support the processing of the data provided by another sensor. This can potentially lead to closed loops within the sensor suite resulting in measurement latency. However, if real-time operation is not considered to be the most crucial constraint, this architecture can significantly enhance the performance and efficiency of the sensor suite. In many systems sensors can be grouped to form a sub-suite within the architecture. One of the most prominent examples is the RGB camera, where images obtained with different filters are merged to form a colored image which is fused before being further processed together with other data sets. This approach allows creating a common data format before fusion with other information is performed. Since the merging of sub-suites creates a hierarchy through the fusion process this approach is called hierarchical architecture.

3 PASSENGER SCREENING

One of the most prominent applications for sensor fusion is passenger screening at airports or other sensitive areas. Radar technology is used to allow imaging through clothing to guarantee the detection of possible threats. Different to optical imaging not only the surface is screened.

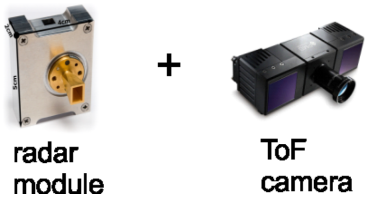


Figure 2: Sensors fused within the passenger scanning system developed within the ATOM project

The imaging technology developed by Fraunhofer FHR within the FP7 project “ATOM” combines two technologies. A highly resolved 2D radar image generated by a SAR scanner is used to detect suspicious objects under clothes such as weapons or explosives. The images are combined using a 3D Time-of-Flight (ToF) camera operating in the infrared range.

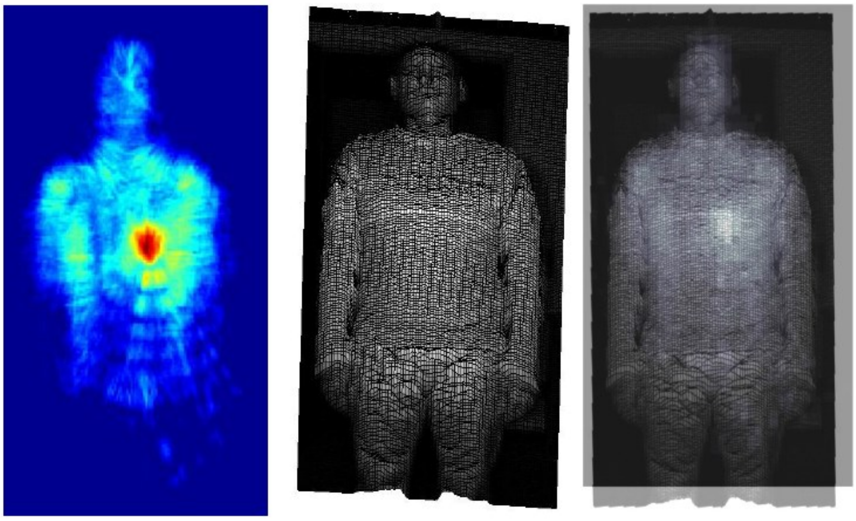


Figure 3: SAR image, ToF image and fused images of a scanned person carrying a hidden grenade

In Figure 3 the data originating from the two imagers as well as the fused image is shown. The radar image on the left clearly shows a highly reflecting object in the center of the upper body of a person. The head and the shoulders can be also clearly seen. This is achieved by imaging the person from the top rather than the front so that the upper parts of the body scatter a significant amount of millimeter wave radiation. However, the contours of the person are hard to see on a radar image. Especially at the lower part of the body significant shadowing effects lead to very weak illumination. For an untrained person the IR image in the center is far easier to interpret. The 3D capability of the ToF camera even allows seeing the contours of the person’s face as well as the outline of clothing. A combination of both images results in an intuitively interpretable view where the suspicious object hidden under the clothes is present as a shiny spot within the optical image of the passenger. While the SAR scanner itself forms a cooperative sensor suite, the IR image performs a similar measurement at a far higher frequency range. Therefore, the sensor suite can be interpreted as a hierarchical combination of the cooperative radar data processing and a complementary integration of millimeter wave and IR range data. In this setup no cooperation between the two sensor suites took place. The images shown in Figure 3 illustrate the easiest way of sensor fusion. The obtained data is overlaid to ease the interpretation by the viewer. This can be further supported by automatic object classification leaving this image interpretation process to an algorithm which only presents the results to the user without showing the raw data. This approach is implemented in another passenger scanning system developed within the FP7 project TeraSCREEN [3]. In this sensor suite radar data and radiometer images obtained at millimeter frequencies are combined for automatic threat detection for next generation airport scanning systems.

4 LUGGAGE SCANNING

A very similar application for radar imaging is the security check of luggage to detect suspicious objects. Very promising results have been obtained in that field using 3D millimeter wave scanners [4]. Since 3D images are provided by the millimeter wave SAR scanner it appears absolutely reasonable to merge the images with 3D optical images obtained by a ToF camera.

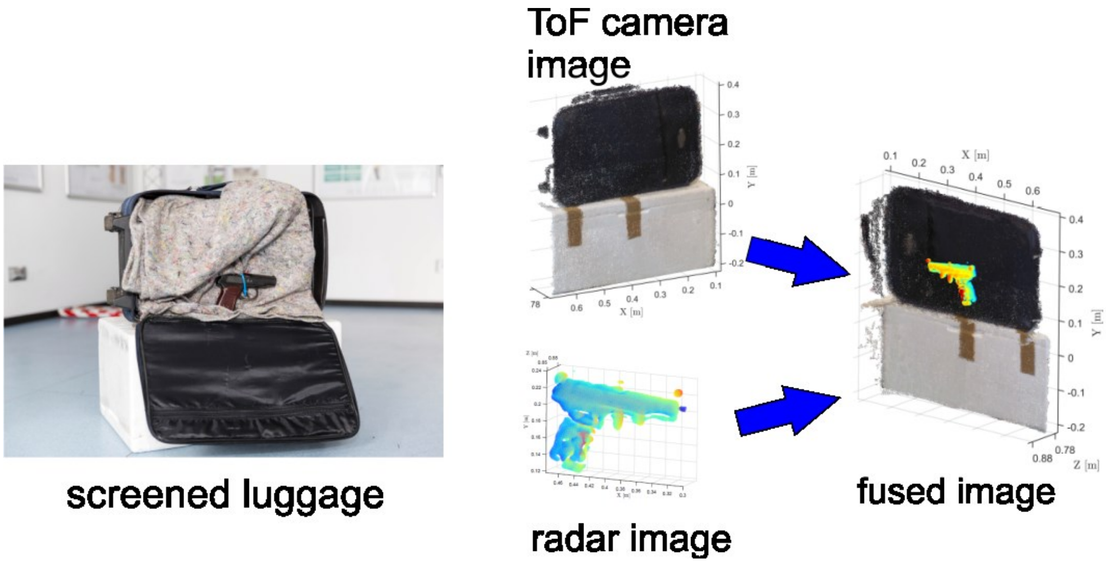


Figure 4: Screened luggage, optical and radar image and fused 3D representation

The ToF camera image itself is fused with a 2D RGB image resulting in highly resolved colored 3D images. If the geometry of the sensor suite is well known the 3D radar image obtained from the inside of the luggage can be placed at the right point so that the content appears flying within the well-defined luggage surrounding. The sensor suite was calibrated before with a 3D object visible in the optical as well as in the millimeter wave range. As it can be seen in Figure 4 the SAR image shows the hidden weapon in impressive detail. The sensor fusion took place in several stages. First multiple optical 3D images taken from different perspectives were fused to fill gaps caused by high reflections and shadowing. At the second step the corresponding points in the set of RGB images were selected and the color values were used to create a detailed, photorealistic representation of the luggage. The last step was placing the sector of the SAR image surrounded by the luggage outline in a common visualization. The SAR imaging made use of the optical image by restricting the image generation to the region of interest within the suitcase. This sensor fusion therefore represents a classical decentral architecture. The data sets obtained by the ToF and the RGB camera were fused and the result used for image generation of the SAR scanner. After the SAR image generation all images are merged in a common visualization. This visualization does not only allow an easy identification of the position of the suspicious object, but also enables to find the critical suitcase within a bunch of luggage in a busy airport environment.

5 ROBOTIC SENSING

In the growing field of robotics it is a crucial factor to know the environment of the robot. Especially in the security sector robotic platforms help to reach areas where human helpers cannot access. A remotely controlled robot operating out of sight of its base station needs to send detailed information about its environment to give the operator feedback about the surrounding environment. Today digital camera and LIDAR systems are easy to integrate. These sensors operating in the optical spectrum can provide highly resolved images and 3D models of objects within the field of view of the robot. For security applications such as rescue during disasters it is crucial to keep the overview even if sight is restricted by smoke, fog or dust. Optical systems only provide a very limited view in such cases. As discussed before radar systems can help to see things where light cannot transmit. In the FP7 project "SmokeBot" a robotic sensor suite is developed which helps to explore disaster sites in order to support rescue teams in planning and organizing their mission. As shown in Figure 5 the robot is equipped with an optical LIDAR and a radar sensor. Both sensors provide a 2D time of flight measurement of the environment. Depending on the presence of smoke or fog the radar signal is used to fill the gaps of the created LIDAR image.

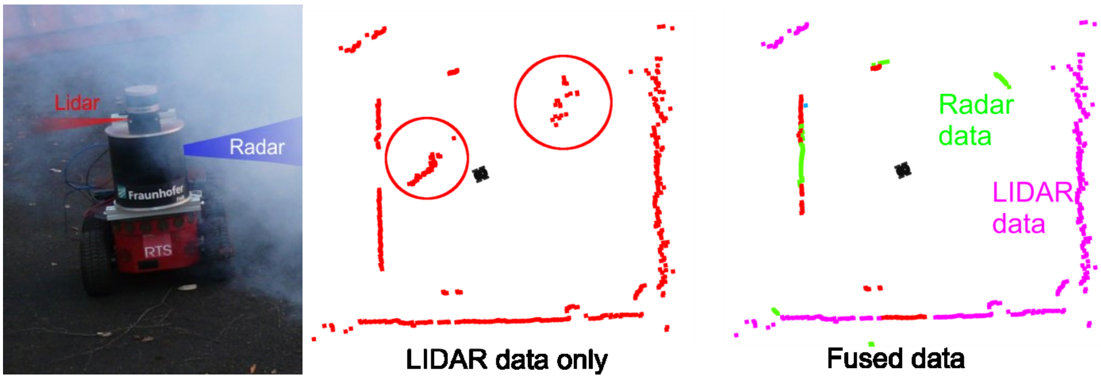


Figure 5: Robot carrying a LIDAR and a Radar sensor for unrestricted vision developed within the Horizon 2020 project "SmokeBot" and first 2D environment scanning results

As shown in Figure 5 the LIDAR scanning model does indeed fail where it the visibility level is too much reduced by smoke as being marked by red circles in the figure. The fused image does not suffer from that restriction. The sensor fusion developed at the University of Hanover [5] merges the data from both sources implementing a competing approach. In a later stage of the project the 2D profile is replaced by a 3D radar image of the environment based on millimeter wave MIMO radar. As the 2D profile is fused with the LIDAR data, the 3D images can be fused with optical ToF images resulting in similar fusing schemes as presented for passenger and luggage security screening.

6 CONCLUSION

In this paper several applications of optical and radar imaging sensor fusion were presented. Different approaches in structuring the field of sensor fusion have been described. The implementation for passenger screening did in this case mainly assist the manual interpreter to locate suspicious objects detected by the radar scan. In luggage scanning two 3D images were combined to enhance the interpretability of the images. The luggage is internally screened by the rdar scanner while a 3D image of its outside created by a time-of-flight camera helps to localize the object within the baggage and to identify it from the outside at the airport. The fusion was performed with an accuracy of several millimeters enabled by an external calibration. For fusion LIDAR scanners a mechanical radar scanner was used forming a compact module to be used in robotics. Here it was successfully shown that the presence of dust and smoke harms the optical detection, but is easily overcome by the sensor suite. Only using the final images for sensor fusion is not the full scope of opportunities. Instead, the data obtained by one sensor can be used to speed up the processing of another. Especially in SAR imaging a huge potential is there to proceed further in this field. The presence of numerous sensors in mobile phones and PCs will allow very impressive results in the field of imaging. Therefore, sensor fusion can play a key role in developing the next generation of technology in the growing field of imaging for security applications.

REFERENCES

[1] J. Beyerer et al. *Informationsfusion in der Mess- und Sensortechnik*. 2006..

[2] S. Thiele, *Konzeptentwicklung und Umsetzung einer Sensordatenfusion aus Radarsensorik und optischer 3D-Umgebungserfassung*, Master Thesis, University of Applied Sciences Koblenz, 08/2015

[3] Alexander, N. E.; Alderman, B.; Allona, F.; Frijlink, P.; Gonzalo, R.;Hägelen, M.; Ibez, A.; Krozer, V.; Langford, M. L.; Limiti, E.; Platt, D.;Schikora, M.; Wang, H.; Weber, M. A.,TeraSCREEN: *Multi-frequency multi-mode Terahertz screening for border checks*, Passive and ActiveMillimeter-Wave Imaging XVII, SPIE Proceedings, vol. 9078, 06/2014

[4] Haegelen, M.; Stanko, S.; Essen, H.; Briese, G.; Schlechtweg, M.; Tessmann, A., *A 3-D millimeterwave luggage scanner*, Infrared, Millimeter and Terahertz Waves, 2008. IRMMW-THz 2008. 33rd International Conference on, 15-19 Sept. 2008

[5] Fritsche, P.; Kueppers, S.; Briese, G.; Wagner, B., *Radar and LiDAR Sensorfusion in Low Visibility Environments*, ICINCO 2016, 07/2016

OFFSHORE WIND ENERGY – SAFETY AND SECURITY WITH SENSOR SYSTEMS

Jürgen Gabriel[1], Karin Jahn[1] and Julia Klatt[2]

[1] *juergen.gabriel@ifam.fraunhofer.de and karin.jahn@ifam.fraunhofer.de*
Fraunhofer Institute for Manufacturing Technology and Advanced Materials IFAM,
Department of Energy System Analysis, Wiener Straße 12, 28359 Bremen (Germany)

[2] *jklatt@deutscheoffshore.de*
Deutsche Offshore Consult GmbH, Office Bremerhaven, Barkhausenstraße 4,
27568 Bremerhaven (Germany)

Abstract

The Offshore Wind Energy Supply System (OWESS) faces a number of threats and vulnerabilities which could result in a failure of the power supply to the transmission system, and thereby affect the power supply for onshore customers. This paper shows which elements, processes and risks of the system are able, in extreme cases, to cause a regional black-out. Sensors and sensor systems can be deployed for the early detection of special threats and dangers, although this happens more often for reasons of safety than of security. The lack of negative security experiences seems to be responsible for this situation, whereby security sensor technologies, such as those that represent standard solutions in the offshore oil and gas industry, have not yet been applied within the OWESS.

Keywords: Offshore wind; energy; critical infrastructure, safety; security; sensor systems

1 OFFSHORE WIND ENERGY – CHALLENGES FROM A SECURITY PERSPECTIVE

Offshore wind energy is expected to contribute significantly to Germany’s future electricity supply without decreasing the security either of the electricity supply or of German citizens. This constitutes a considerable challenge for wind park operators, not solely due to the volatility of wind energy generation. The long distances between plant sites and the onshore electricity grid, occasionally harsh weather conditions and, consequently, limited plant accessibility present challenges for those responsible for the security of this critical infrastructure.

In our opinion, the volatility of offshore wind energy production does not endanger the security of the electricity supply. As the risk of a large-scale and long-lasting lack of wind-power is well-known in the German offshore regions, the electrical supply system has alternative supply technologies to cover these time periods. Various types of fossil and renewable power plants work irrespective of weather conditions, using coal, gas, biomass, biogas or hydro-power, for example. Additionally, the import of electrical power from neighbouring countries could be an alternative, as could future large-scale use of energy storage such as pump-storage, batteries or gas from power-to-gas production.

Special challenges to be analysed are those that result from the placement of wind turbines at sea and the necessity to transport the electricity by submarine power cable, sometimes at a length of over 150 km, thunderstorms, collision by ships or aircraft, attacks by terrorists, acts of sabotage or cyber-attacks on the monitoring and management systems, to name but a few.

2 THE OFFSHORE WIND ENERGY SUPPLY SYSTEM: CRITICAL ELEMENTS

The German government is planning an offshore wind energy supply system (OWESS) which should reach a maximum power of 6,500 MW (Megawatt) in the year 2020 [1]. This production power will be delivered by about 1,450 wind turbines (WT) with a single system output between 2.3 and 6.0 MW. Up to 80 WTs will be combined in each offshore wind farm (OWF) with a maximum power of 400 MW. Three-phase current is delivered from the WTs of one OWF to a central offshore substation and from there on by submarine cable and land cable to an onshore substation, which is the connection point to the high voltage transmission grid. In the North Sea region, alternating current is normally transformed into direct current on an offshore converter platform and re-transformed on an onshore converter station. This double transformation minimizes grid losses on the way to the coast.

Every element of the OWESS is exposed to different threats, depending on its type. Offshore platforms, for example, could be hit by ships unable to manoeuvre or could be a potential target for terrorists while submarine cables could be damaged by drag anchors and land cables could be damaged by earthworks. Onshore and offshore stations can be affected by storms and extraordinary weather phenomena. A question arises regarding the consequences of a failure of a single OWESS-element with respect to the security of the electricity supply for the German customers. As the German electricity supply has a peak load of around 80,000 MW [2], the failure of one WT with 5 MW will not be detectable within the system. The breakdown of a converter platform or station with an electrical load of 900 MW is far more difficult to evaluate. Table 1 shows the maximum electrical load of selected elements of the OWESS. Geographically concentrated elements of the same type merit special concern: converter platforms, converter stations, submarine cables and land cables. Such spatial clusters of elements could be exposed to a single threat, for example a thunderstorm, a ship collision, an intentional aircraft crash or an explosion, and thus the overall respective hazard rises for the electrical supply system.

Table 1: Typical Elements of the Offshore Wind Energy Supply System in the Year 2020

Category	Maximum load	Geographically concentrated?
Offshore substation	400 MW	No
Offshore converter platform	900 MW	Yes, a so called parent/subsidiary arrangement with 1,800 MW.
AC grid connection system	340 MW	No
DC grid connection system	900 MW	Yes, cases of parallel arrangement of several submarine or land cables up to 3,000 MW.
Onshore converter station	900 MW	Yes, location with 3 elements (2,130 MW) realized, with 3 elements (2,700 MW) planned.

Aside from the geographical concentration, the “virtual concentration” of OWESS elements offers a high potential for danger. If several OWF are monitored and managed by the same operator and from one control room, or if some hundred WT are managed by the same producer control system, then a single cyber-attack directed to the control room concerned could cause the common failure of several geographically spread OWESS elements. Such an attack could cause a breakdown in the electrical load across a magnitude of several converter platforms.

3 VOLATILE OFFSHORE POWER PRODUCTION AND SECURITY OF ELECTRICAL SUPPLY

A drop in or a failure of the power production of one OWF – like any other large power plant – will cause an imbalance between electricity generation and consumption at the level of the electricity supply system. To bridge this gap, extensive back-up capacities exist within the European electricity supply system [3]: A primary balancing power with a capacity of 3,000 MW can be automatically activated within 30 seconds. Additionally, German transmission system operators can activate secondary balancing power with a capacity of about 2,000 MW within five minutes and tertiary reserve power with a capacity of about 2,400 MW within 15 minutes. The secondary and tertiary balancing powers first increase and then replace the primary balancing power capacities. If the starting imbalance exceeds 3,000 MW, the automatic compensation mechanism could fail with the result of a partial black-out for a limited number of customers across a particular region.

The magnitude of the power drop and the velocity of the decline in power are decisive factors for the extent of the effects to the power supply of the population caused by an offshore power failure. The longer the time period of the power drop from maximum to zero MW, the greater are the available reserve power capacities that can be deployed to compensate for the imbalance. This lowers the risk that a failure within the OWESS will cause a disturbance to the power supply for the consumers. Three categories of velocity of power decline are combined with three categories of magnitude of power decline in the research project “Offshore Wind Energy – Safety and Security” (OWISS) [4]. As fig. 1 shows, only the combination of a very fast power drop within 30 seconds with a maximum loss of power of more than 1,000 MW is evaluated to be a “large” failure of power supply.

Time span between the occurence of the start event and the drop of the feed in of electricity to 0 MW	≤ 30 sec.	░	▒	▓
	30 sec. < x ≤ 300 sec.	░	▒	▒
	> 300 sec.	░	░	▒
		≤ 500	500 < x ≤ 1,000	> 1,000
		Maximum loss of power (MW)		
		Evaluation of failure of power supply		
		░ small	▒ medium	▓ large

Figure 1: Evaluation of failure of power supply

4 ENERGY ECONOMIC ANALYSIS OF SAFETY AND SECURITY SCENARIOS

In the OWISS project, more than 180 safety and security scenarios were selected for further analysis. The description and the analysis of these scenarios took place with the participation of the industry and members of security organisations with the aim to identify critical elements, processes and results that can endanger the security of the electricity supply.

First of all, those scenarios that present a high risk to society according to the evaluation by the joint project partners were filtered out. This evaluation was done with respect to the possible material and immaterial damages as well as with respect to the frequency (safety scenarios) or the success probability (safety scenarios) [5]. The perspective of the energy industry was taken into account on the basis of three criteria:

- The final result of the scenario is a “disturbance in the power supply to the transmission grid”, because only these scenarios impact on the power supply to consumers.
- The scenario shows a very quick drop in the power fed into the transmission grid. The time span between the occurrence of the start event and the drop in the feed of electricity to 0 MW is less than 30 seconds. In this case, primary balancing capacities are needed to compensate the imbalance.
- The maximum loss of power is higher than 1,000 MW (full utilization of the particular OWESS element). In such a case the German primary balancing capacities (583 MW as of 2016 [6]) cannot compensate the imbalance and foreign assistance in balancing becomes necessary.

The provisional results of this security analysis with special respect to the energy industrial perspective are as follows:

- The break-down of a single OWESS element, regardless of type, will not cause a large failure in the power supply to the transmission grid.
- There is a risk of a large failure in power supply that could result in a black-out in those scenarios where two or three single large OWESS elements, such as offshore converter platforms, onshore converter stations or land cables, show a geographical concentration and could be commonly affected by a single security or safety event.
- This risk by concentration also occurs when a control room that manages several OWF with their substations is affected. Such a failure of the control system could result in a breakdown of geographically dispersed but virtually concentrated OWESS elements.
- Further analysis must concentrate on safety and security events that can cause a very quick drop in power, such as an explosion, fire, short-circuit, lightning strike with explosion and intentional intervention via the centralised control system. These events are connected with a high risk to the power supply system.
- Security against cyber-attacks, which could affect and break down several OWESS elements with one strike, deserves particular attention.

The following chapters will show the role of sensors and sensor systems in the detection of hazards and the protection of critical offshore infrastructure. From the perspective of electricity supply security, sensor systems can help to detect risks earlier than human controls so that endangered OWESS elements can be cut off from the grid by the transmission system operator before they run out of control.

5 THE IMPORTANCE OF SENSOR SYSTEMS FOR THE PROTECTION OF OWESS

Due to the harsh environmental conditions offshore and the big distance to control rooms and service personnel, Condition-Monitoring-Systems (CMS) are an essential element of OWESS. The main task of these monitoring systems is the surveillance of the operational parameters of OWESS elements such as foundations, wind turbines, substations and submarine power cables. For this reason, about 100 sensor monitoring key components are used [7]. The key elements of the CMS are sensors that observe OWESS elements including:

- Temperature
- Humidity
- Motion
- Fluid level
- Smoke
- Power failure
- Current
- Acceleration

Furthermore, meteorological station sensors provide meteorological and oceanographic data on the conditions at site. Sometimes additional environmental data are collected via bird radars or hydrophones. These weather observation systems enable wind farm operators and transmission network operators to take foresighted measures if necessary. Thus, a sudden power failure caused by a thunderstorm or rogue waves can be avoided.

Aside from environmental parameters such as weather conditions, the sensor systems basically survey the indicators of operating conditions, structural integrity, safety and security. Based on the data collected, conclusions can be drawn concerning the current state, the productivity and the durability of the single components. Offshore, the early identification of changing target values is very important in order to react before damages occur. In the offshore environment, damages lead to high material, logistics and personnel costs which are multiplied by missing feed-in remuneration, especially in case of a damaged converter platform or a damaged export cable. Therefore, sensors are vital instruments for risk mitigation in offshore wind farms and serve as the “eyes and ears of the operators”. A central fire alarm system can detect heat and smoke before a fire occurs. Modern submarine cables can be equipped with monitoring systems [8] which allow the temperature of the cable to be controlled, can detect any mechanical disturbance and even warn of threats like an approaching anchor or the appearance of fishing gear. In addition, the monitoring system can detect the location of a flashover, which accelerates reaction time in cases of damage.

Due to unexploded ordnance (UXO) from the Second World War, regular surveys of the sea bed are necessary. The UXO may move due to currents and tidal forces. To monitor the UXO, remote operated vehicles (ROV) with magnetic sensory technology are used. If such a UXO approaches a foundation or a cable tray, appropriate measures can be taken.

For survey purposes, several sonar and echo-sounder systems are used, such as side scan sonars for cable inspections and cable tracker systems for an evaluation of the excavation depth.

Table 2 shows some of the sensors in relation to their scope of application.

6 RESILIENCE OF CONTROL ROOMS AND INFORMATION CHANNELS AS CENTRAL SECURITY ASPECT

The common information channels between control rooms and OWESS components are fibre-optic cables embedded in the inner-array and export submarine power cables. Via these cable connections, control information is sent to the wind farms and the electricity produced offshore is transported back to shore.

Table 2: Type of sensors used in offshore wind farms

Purpose	Type of sensor	Application
Structural integrity	Strain gauge	Foundation, tower, blade, topside
	Fibre optic cable	Submarine power cable
	Vibration sensor	Tower, nacelle
	Acceleration sensor	Rotor
	Captive sensors	Foundation - detection of scour
Safety	Central fire alarm system (visual smoke detectors, Closed Circuit Television (CCTV), heat detectors)	Tower, nacelle, substation, converter station
	Magnet sensor	Mobile use to search for UXO
	Metocean sensors	Met mast (Wave heights, sea level, current)
	Pressure sensors	Hydraulic systems
	Meteorological sensors	Met station (wind speed, wind direction, temperature, pressure, humidity, solar radiation, visibility)
Security	Key cards, door sensors, CCTV	Access to tower, lift, topsides and control rooms
	Fibre optic cable	Submarine power cable
	Marine Automatic Identification System (AIS)	Substation, converter platform

If the export cable is damaged, then no communication with the wind farm is possible. For this reason, a redundancy for information transmission is necessary, e.g. via microwave wireless bridging or a satellite-based system.

All elements of an OWESS are interconnected, either directly or indirectly. The wind turbine generators (WTGs) are connected with the offshore substation (OSS) and the OSS with the converter platform. In addition, the WTGs are connected to the control rooms of the turbine manufacturer and the wind farm operator (WFO). The OSS is connected to the control room of the transmission system operator (TSO) and to the WFO. The converter platform is connected to the TSO and the control room of the operator of the inter-array cable system. This constellation creates a multitude of interfaces within the Supervisory Control and Data Acquisition Systems (SCADA). At the moment there are only a few manufactures of OWESS components. This leads to “virtual concentrations” within the offshore landscape even if the physical parts are some distance apart. The control room of a single turbine manufacturer can have, for example, access to about 200 WTGs with 5 MW output each, and this number is rising week by week. If this control room were to become a victim of a cyber-attack, about 1,000 MW could be shut down within a second.

It is a similar situation regarding the OSS and converter platforms. There are also only very few manufacturers who build the electro-technical equipment for the topsides. The physical and virtual security of the control rooms is essential to decrease the vulnerability of those critical infrastructure elements.

7 SECURITY-RELATED SENSORS IN OWESS – LESSONS FROM THE OIL AND GAS INDUSTRY

So far, no security incidents in OWESS have taken place during operation. Some fatal accidents were reported due to safety events during installation works. Therefore, security is not yet the focus of OWESS operators, at least not in the area of offshore structures. Onshore facilities, such as control rooms and substations, are secured in the manner of other onshore energy producing facilities, for instance through fences, armoured glass and access protection via the use of key cards.

However, there are some lessons to be learnt from the offshore oil and gas industry, which has a completely different situation. Due to the number of past attacks on offshore platforms, a wide range of security services and devices have become available. The observation of the surrounding area plays a key role in the security concepts. Common sensor systems for this task are:

- Echo sounding
- Motion sensors
- Radar
- Marine Automatic Identification System (AIS)
- Infrared sensors [9]

These sensors enable operators to detect boats and even approaching swimmers. The software systems in which the sensors are embedded are able to record and store the data of e.g. passing vessels or weather conditions such as temperature and visibility. The previously mentioned VALCAP® cable monitoring system [8] is able to track vessel data. In the case of damage, whether or not intentional, operators can analyse the data and identify the vessel that caused the damage.

Not only physical security is an important topic on oil and gas platforms, an awareness of cyber threats is also very high. There have been several attacks on the SCADA systems of floating platforms. If a hacker were to manipulate the ballasting systems, for instance, the consequences could be serious, including even the total loss of a platform and its personnel. Some of these oil rigs have been offline for several days.

The future deployment of sensors and sensor systems in OWESS will depend on the experiences with safety and security events in this new critical infrastructure and on further technical development, both on the side of surveillance as well as on the side of threats and vulnerabilities.

8 RESULTS AND CONCLUSIONS

OWESS is a complex system with direct connections to the electricity supply for the population. Various elements of the system are exposed to different threats and vulnerabilities, some of which are at risk of a black-out. This risk is particularly high if both an element with high capacity is involved and, at the same time, the drop in the power fed into the transmission grid takes place very quickly, i.e. within 30 seconds. A situation could then arise where the balancing system of the TSO is unable to meet the requirements, resulting in a black-out. The fast and proactive detection of hazards can reduce potential damage by threats and may, in individual cases, avoid a black-out with its negative results for the security of the population. Sensors and sensor systems are able to provide a major contribution to this aim. Therefore, they are deployed on a large scale in the installation of OWESS. At the moment, the emphasis lies rather on CMS and safety systems and on meteorological observation. Sensor systems for security reasons are mainly deployed on onshore installations, for example to protect control rooms substations and converter stations. Offshore use of security sensor technologies is well established in the oil and gas industry and could be easily transferred to OWESS if the need for protection arose. So far comparatively few OWF are in operation, and these only for a short time. Therefore, there is little experience with security events of OWESS elements. There has been little need for an extensive use of security sensor systems during the operation of OWF. This does not apply to the special case of IT-security, which is of great importance to all OWESS elements. Therefore, it is also a subject of OWISS. However, there currently are no results regarding IT-security to be reported in this paper.

REFERENCES

[1] German Renewable Energy Sources Act (Erneuerbare-Energien-Gesetz – EEG 2014). Bundesgesetzblatt Jahrgang 2014 Teil I Nr. 33, Bonn, 24. July 2014.

[2] 50hertz et al.: Report of German TSO on the power balance 2015 (Bericht der deutschen Übertragungsnetzbetreiber zur Leistungsbilanz 2015 nach EnWG § 12 Abs. 4 und 5). Last draft February 2016.

[3] Scharf, R.: „Security of Supply – A Challenge of the Energy Turnaround“ (Versorgungssicherheit – Eine Herausforderung der Energiewende), Lecture in the context of the lecture series „Transforming the Energy System“ on 22. April 2015 at Leibnitz University Hanover. https://www.ikw.uni-hannover.de/693.html (Download 21.01.2016)

[4] Offshore Wind Energy – Safety and Security (Offshore Windenergie – Schutz und Sicherheit (OWISS)). Research project in the context of the program: Research for civil security - maritime security. Part of project: Economic and societal view on security of supply and security of people. Fraunhofer IFAM, Bremen 2015. Funded by The Federal Ministry of Education and Research (BMBF).

[5] Horstmann, T. / fk-wind, University of Applied Science Bremerhaven: Offshore Wind Energy – Safety and Security (OWISS). Preliminary catalogue of threats and vulnerabilities, 04. February 2016. Revised version, 06. April 2016

[6] Balancing power (Regelleistung.net): Electronic platform of German TSO for placing public procurement of balancing power; Procurement details PRL 08-14.02.2016. https://www.regelleistung.net/ext/tender/details/4785 (Download 01.02.2016)

[7] The Crown Estate: A Guide to an Offshore Wind Farm – T1.7. Control system. http://www.thecrownestate.co.uk/media/5408/ei-a-guide-to-an-offshore-wind-farm.pdf (Download 24.05.2016)

[8] http://www.nktcables.com/de/support/movies/valcap/

[9] http://www.hgh-infrared.com/Applications/Security/Offshore-Platform-Security

THE EFFECT OF LIGAND BINDING ON THE HYBRIDIZATION ISOTHERM OF DNA CHIP

Stefano Bellucci[1], Sh. Tonoyan[2], V.F. Morozov[3], and Y.Sh. Mamasakhlisov[4]

[1] *Stefano.Bellucci@lnf.infn.it*
INFN - Laboratori Nazionali di Frascati, Via Enrico Fermi 40 - 00044 Frascati (Roma) (Italy)

[2] *sh.tonoyan@ysu.am*
Yerevan State University, 1 A. Manoogian St., 0025 Yerevan (Armenia)

[3] *morozov@ysu.am*
Yerevan State University, 1 A. Manoogian St., 0025 Yerevan (Armenia)

[4] *y.mamasakhlisov@ysu.am*
Yerevan State University, 1 A. Manoogian St., 0025 Yerevan (Armenia)

Abstract

One of the important directions of DNA – chips improvement is the increasing selectivity and sensitivity in expense of enhancement of electric signal and target probe hybridization stability. The increase of selectivity and sensitivity of DNA – sensors can be reached by using electro-chemically active compounds with higher affinity to the dsDNA than to the ssDNA. This kind of compounds can substantially increase the dsDNA stability and at the same time, the amplitude of generated signal, which increases the DNA – sensor sensitivity. Among this kind of ligands are intercalators, molecules with a heterocyclic structure, which fit between nucleic bases and change the local structure of dsDNA. It is shown that the intercalating ligands binding with hybridized probes not only substantially decreases the concentration of one-half hybridization and then improve the sensitivity of the DNA-chip, but also increase their selectivity for the appropriate choice of binding constants, parameters, etc.

Keywords: DNA, biosensor, ligand, hybridization.

1 INTRODUCTION

DNA – chips are one of the promising tools with very diverse areas of application such as medical diagnostics, environmental pollutants monitoring, biological weapons defence etc. One of the important directions of DNA – chips improvement is the increasing selectivity and sensitivity in expense of enhancement of electric signal and target – probe hybridization stability. Efficiency of such devices as DNA-sensors and DNA-chips depends on precise prediction of experimental parameters responsible for thermostability of nucleic acids' duplexes and specific times of formation of DNA duplexes. The thermodynamics of hybridization is affected by multiple factors, such as: density of single-strand DNA assays (the length 25-49 nucleotides) immobilized on the surface; presence of competing hybridization; nucleotide sequences; solvent conditions, including pH, ionic strength, low-molecular compounds (ligands), interacting with nucleic acids and other co-solutes; the presence of interphase borders and geometrical restrictions; etc. The paper is focused on the isotherm of hybridization of DNA on the surface in presence of ligands, binding with double – stranded regions of DNA. In practice, the DNA chips are immersed in the target solution for a relatively short time and kinetic of hybridization plays a crucial role. However, understanding of the equilibrium state is also necessary to identify the relative importance of kinetic and thermodynamic issues of the performance of the DNA chips.

2 THE COMPETITION-FREE HYBRIDIZATION

2.1 Reaction equations

Let us compare the equilibrium hybridization isotherms for two idealized but experimentally accessible situations, where DNA chip immersed in solution containing intercalating ligands and: 1) only one type of single-stranded target (Fig.1) or 2) containing targets of two different types that do not hybridize in the bulk but are both capable of hybridizing with the same probe on the surface (Fig. 2). In this section we will focused on the first scenario. In both cases, we consider the length N of probes and targets to be equal. Let us consider the spot of N_0 single - stranded probes p, wherein the N_{pt} of them are hybridized with target t.

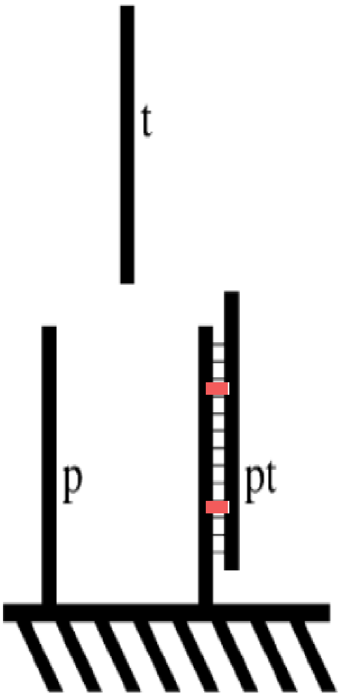


Fig. 1. The scheme of non-competing surface hybridization affected by ligands.

The hybridization of p and t creates a double-stranded oligonucleotide, pt, at the surface. In simplest case of single species of ssDNA target, surface will be covered only by free probes p and hybridized ones pt. In this case the only reaction is

$$p + t \leftrightarrow pt \tag{1}$$

and no competitive hybridization reactions occur (Fig. 1). The dependence of the hybridization degree, $x = N_{pt}/N_0$, on the concentration of the target, c_t, is described by hybridization isotherm. For the intercalating ligands ℓ the binding reactions are written where pt is the free duplex, while pt_j is the target – probe duplex bound to i ligands, ℓ

$$pt_{i-1} + \ell \leftrightarrow pt_i \;\; (i=1\ldots N) \tag{2}$$

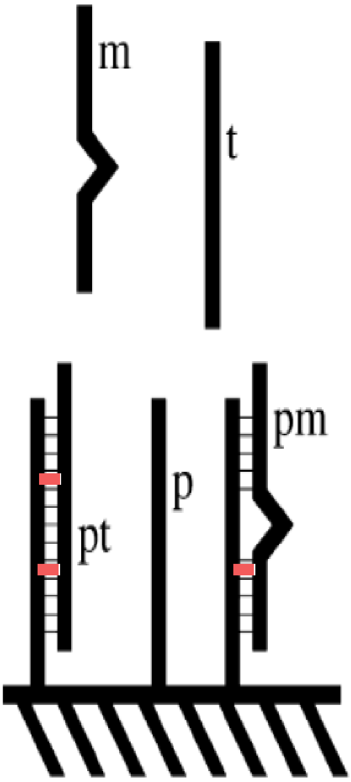


Fig. 2. The scheme of competing surface hybridization affected by ligands

2.2 The non – competing hybridization

The free energy of the probe layer without ligands was estimated in [1] as a function of N_{pt}, the number of hybridized probes, $G=G\ (N_{pt})$. If intercalation is the only mechanism of ligands binding, DNA-ligand complex formation will be restricted only by double-stranded regions and in case of non – competing hybridization the free energy of probe layer yields

$$G_L = G + N_{pt}\{m\mu^0{}_b + k_BT[m\ ln(m/N) + (N\text{-}M)\ ln((N\text{-}m)/N)]\}, \tag{3}$$

where m is the number of bound ligands per hybridized probe pt and $\mu^0{}_b$ is the chemical potential of the bound ligand in a reference state. It is supposed that the available number of binding sites on the pt duplex is coincides to the length N.

The equilibrium state for the reactions (1) and (2) are determined by conditions

$$\mu_{pt} = \mu_{p\,+}\ \mu_t \text{ and } \mu_b = \mu_\ell\ , \tag{3}$$

where μ_{pt} is the chemical potential of hybridized probe pt, μ_t is the chemical potential of target, μ_p is the chemical potential of probe, μ_b and μ_ℓ are the chemical potentials of the bound and free ligand, correspondingly. On the basis of the equations (3) the hybridization isotherms were estimated (see Fig. 3) in case of non – competing hybridization.

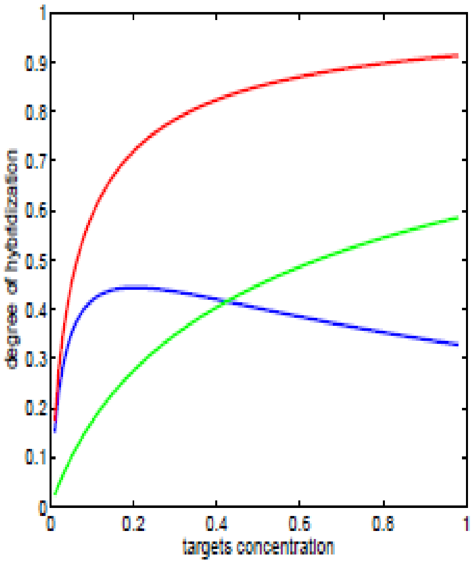


Fig. 3. Isotherm of hybridization in: ligand-free case (green line); in presence of ligands (red line). The shift of the hybridization isotherm is indicated by blue line.

Thus, intercalating ligands caused the substantial increase of the degree of hybridization.

2.3 The surface – competing hybridization

Let us consider the second scenario, where solvent containing targets of two different types *t* and *m* that do not hybridize in the bulk but are both capable of hybridizing with the same probe *p* on the surface as presented in the Fig. 2. *t* is the target sequence, complementary to the probe *p*, while *m* is the mismatched sequence only partially complementary to the probe *p*. It is supposed that the available number of binding sites for the intercalating ligands on the *pm* duplex is equal to *M*, where $M < N$. Following the approach described above, the free energy of the ligand-free probe layer can be presented in dependence on the number of complementary hybridized probes N_{pt}, the number of probes hybridized with mismatches N_{pm} and the numbers of ligands bound to *pt* and *pm* duplexes, N_1 and N_2 , $G_{CL} = G_{CL}(N_{pt}, N_{pm}, N_1, N_2)$. The equilibrium between ligands, targets and mismatched sequences in solution and hybridized probes is determined by appropriate chemical potentials, derived from the free energy G_{CL} and gives the fraction of incorrectly hybridized probes in dependence on targets concentration c_t, presented in the Fig. 4.

Difference between ligand – free hybridization and those, affected by ligands is substantially defined by difference between the number of binding sites on the complementary and mismatched probes. Thus, the intercalating ligands binding with hybridized probes not only substantially improve the sensitivity of the DNA-chip, but also increase their selectivity for the appropriate choice of binding constants, parameters, etc.

3 ACKNOWLEDGEMENT

Authors were supported by the NATO Science for Peace Program under grant SFP 984537.

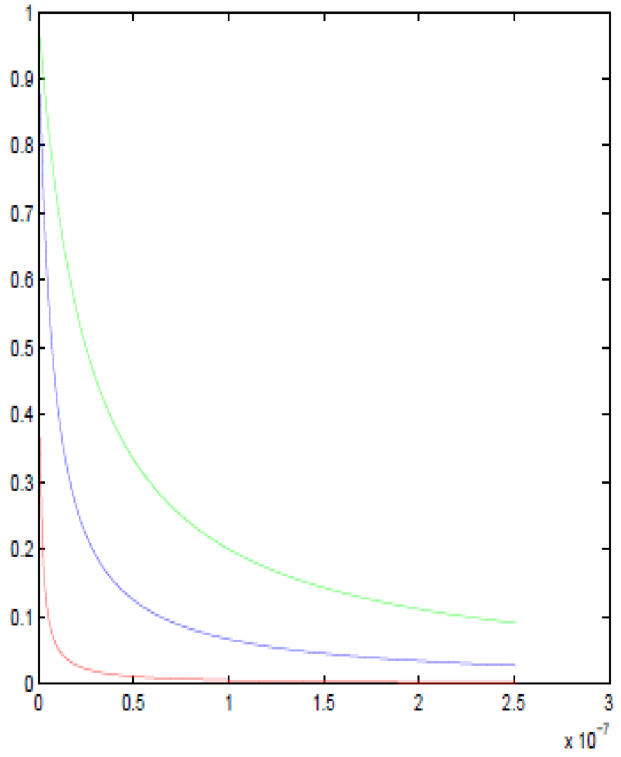


Fig. 4. The fraction of incorrectly hybridized probes in dependence on targets concentration c_t: $M = N$ (green line); $M = N - 1$ (blue line); $M = N - 3$ (red line).

REFERENCES

[1] Halperin, A.; Buhot, A.; Zhulina, E. B. Biophys. J. **86**, 2004, 718.

AIRBORNE SENSE & AVOID RADAR – ARCHITECTURE AND DEMONSTRATOR DESIGN

Peter Feil[1], Dietmar Klarer[2], Hans-Jürgen Peters[3] and Wolfram Schwob[4]

[1] peter.feil@airbus.com
[2] dietmar.klarer@airbus.com
[3] hans-juergen.peters@airbus.com
[4] wolfram.schwob@airbus.com
Airbus DS Electronics and Border Security GmbH
Wörthstr 85, 89077 Ulm (Germany)

Abstract

"Sense & Avoid" is known to be a key capability when it comes to the integration of unmanned aerial vehicles (UAVs) into the civil airspace. Compared to manned aviation a capable sensor equipment is needed in order to substitute the perception of the pilot. Radar is the preferred technology as long as the unmanned platform is able to carry the respective payload, e.g. MALE or HALE UAVs (Medium/High Altitude Long Endurance).

The paper describes the derivation of an appropriate Sense & Avoid Radar architecture based on the key requirements. Further on, the design of a flight demonstrator is outlined.

Keywords: Sense & Avoid, Radar, AESA, Flight Demonstrator.

1 INTRODUCTION

A safe integration of unmanned aerial vehicles (UAV) into the civil airspace requires a so called "Sense & Avoid" (S&A) system in order to substitute the "See & Avoid" task that has to be performed by the pilot on board a manned aircraft.

A generic S&A system consists of several sensors and avionics equipment ("Sense" part of the system) connected to a central computer. This unit collects all available information in order to gain a comprehensive situational awareness and to compute a safe escape trajectory in case of a conflict with other aircrafts ("Avoid" function). Conflicting aircrafts are called "intruders" in the context of S&A.

In general, one has to distinguish cooperative and non-cooperative intruders. Cooperative aircrafts provide means such as TCAS (Traffic Collision Avoidance System) or ADS-B (Automatic Dependent Surveillance – Broadcast) in order to identify themselves and to provide their position, speed and direction. All the remaining non-cooperative intruders have to be detected by appropriate sensors on board the UAV. Typical sensor candidates are Radar and electro-optic or infrared sensors. Among those sensors only Radar can provide:

- all-weather capability,
- instantaneous range, velocity and angle measurement,
- straight forward separation from clutter
- and long detection range.

Hence a S&A Radar will be a mandatory equipment, at least for UAVs exceeding a certain mass, flight speed and altitude.

Performance requirements of S&A Radars have been analysed for several years, e.g. in the scope of the multi-national European study MidCAS (Midair Collision Avoidance System). It turns out, that the measurement accuracy is the most crucial issue. Special attention has to be spent on the angular (rate) accuracy. The trajectory of intruders have to be assessed at a far range greater than 10 km, which leads to accuracy values down less than 5 mrad/s. This figures have to be met under strong constraints regarding size, volume and prime power.

2 RADAR CONCEPT

The primary task of a sense and avoid radar is observing a given angular field of view within a limited time.

When analysing the Radar equation under this constraints it turns out, that the performance of a search Radar only depends on the power-aperture-product, which is the product of the average transmit power and effective receive antenna area (1).

$$P_{TX} \cdot \eta_{DC} \cdot A_{RX} = \theta^2_{search} \cdot \frac{S/N \cdot 4\pi \cdot R^4 \cdot kT \cdot F \cdot L_{ges}}{t_{search} \cdot \sigma} \qquad (1)$$

It is remarkable that the search performance does not depend on the operating frequency of the radar. Of course, if measurement accuracies and atmospheric losses are considered, the frequency plays an important role as well.

The respective requirements of the S&A Radar are stated in Table 1.

Table 1. Required Search Performance of the S&A radar.

Parameter	Value	Comment
Radar Cross Section	1qm	
Range	10km	
Signal to Noise Ratio	18dB	Swerling 1, Pfa=10-6, 80% Pd (Single Pulse)
Noise Figure	5dB	
Search Volume	220° x 30°	
Tsearch	1s	

The values for search volume and time are as proposed in [1]. The remaining parameters are chosen in order to achieve the required track probability.

Evaluating equation (1) with the above stated values and an aperture area of 5dm^2 leads to a mean transmitted power of 20W.

Figure 1 shows the respective probabilities of detection (Pd) on a single pulse and cumulative basis. It can be seen that the cumulative Pd approaches 99.9% at an approximate distance of 14km. Hence, a track will be established at this distance with very high probability. Even at very high closure rates there is still a margin of several seconds, which is needed to achieve the track accuracy required at a range of 10km.

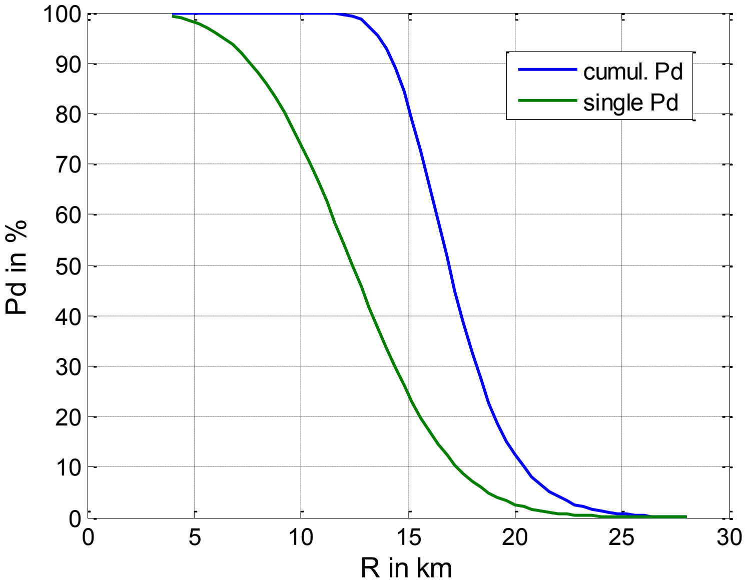


Figure 1: Single pulse and cumulative probability of detection for 20W mean TX power.

3 ARCHITECTURE

A compliant S&A Radar architecture consists of:

- an active electronically scanned array (AESA)
- a highly integrated Radar core electronic incorporating
  - digital and analog signal generation,
  - signal acquisition and processing,
  - Radar control and data processing.

Due to regulatory reasons [2] [3] and as a good trade-off between cost, complexity and angular accuracy, an operating frequency within the X-Band (9.5Ghz) was chosen.

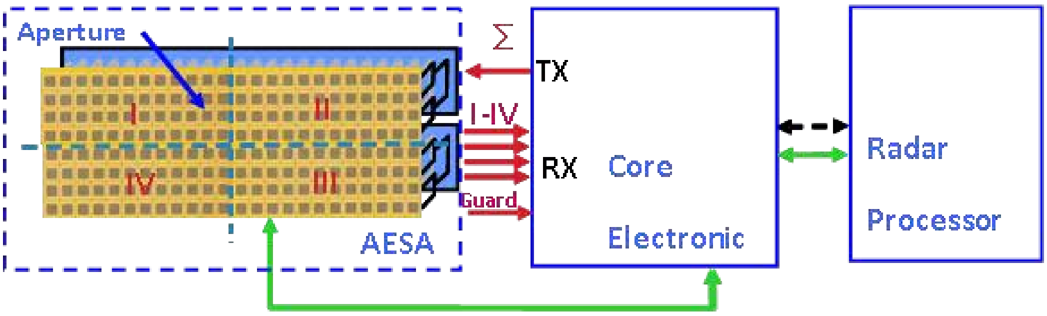


Figure 2: Proposed overall S&A Radar architecture.

In order to achieve the required angular accuracy the use of a 4 quadrant monopulse antenna is mandatory. An additional guard antenna provides the elimination of sidelobe detections. Depending on the implementation of the monopulse processing (analogue or digital), the receiver has to provide an overall number of 4-5 channels.

Due to the large azimuthal field of view (220°) it is not possible to use just one planar antenna, as a single AESA face is limited to a maximum scan angle of 60°.

In a straight forward approach 3 antenna faces are sufficient to cover the required field of view in azimuth (s. Figure 3).

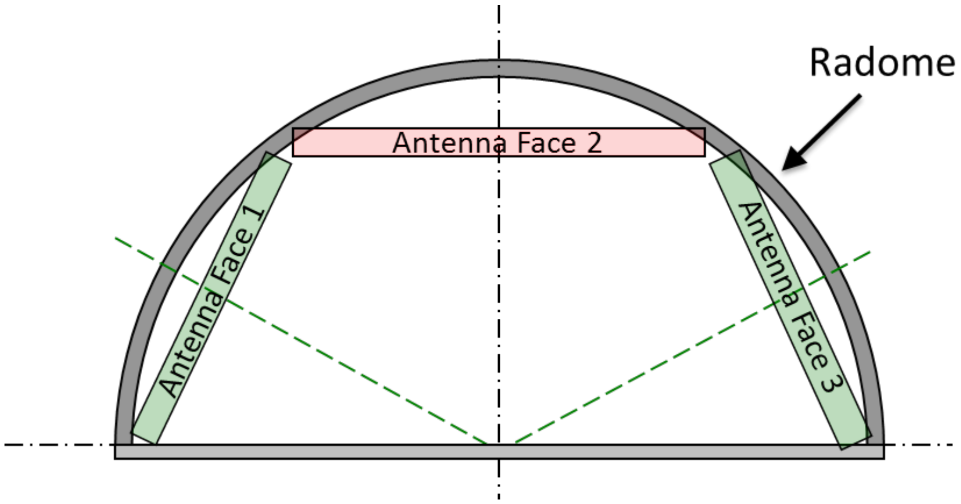


Figure 3: Multifaceted Planar Array for Sense and Avoid Radar (Azimuth +/-110°).

As a more sophisticated solution a conformal array could be used, in order to avoid the need of several planar faces.

4 DEMONSTRATOR DESIGN

The Radar architecture described above was implemented in a demonstrator hardware as shown in Figure 4.

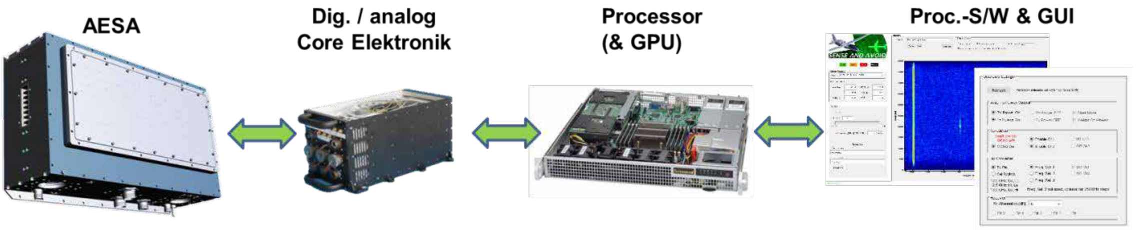


Figure 4: S&A Radar Demonstrator Sub-Units.

The radiating aperture of the AESA is a patch array consisting of 192 microstrip patches. These patches are driven by “Standardised Transmit/Receive Modules” (SMTR®, s. [4]) that are available off the shelve. Commercial, connectorized components form the so called RF interface that provides the Core Electronic with the necessary analogue interfaces. Due to this cost effective approach, the AESA is still too bulky compared to the requirements. However, new technology approaches are under evaluation in order to solve this.

Within the Core Electronic a very high level of integration was achieved, compared to other state-of-the-art high performance multi-channel X-band Radars. As size and weight is an important issue in airborne platforms, studies have been launched in order to further miniaturize this item.

At the current state the core electronic provides raw or preprocessed data to a COTS PC via an optical 10GB/s Ethernet interface. The signal processing is performed in a MATLAB® environment with strong utilization of its GPU processing support. With this setup real-time operation is feasible up to a RF signal bandwidth of several MHz.

The demonstrator described above has undergone comprehensive tests within a complex environment providing means to simulate dynamic Radar targets in the RF domain. By now, intermediate results are available regarding

- Antenna and system patterns,
- signal purity,
- noise performance,
- processing gain,
- and Direction of Arrival estimation.

Further tests on a system level are still ongoing, results will be provided during the conference presentation.

5 SUMMARY AND OUTLOOK

A S&A Radar concept based on a set of key requirements has been outlined. Based on this concept an architecture was derived, enabling the design of a flight demonstrator. With this demonstrator system test results within a synthetic environment are being gathered. A detailed view on the demonstrator and the results will be provided at the conference.

REFERENCES

[1] “MidCAS – Midair Collision Avoidance System”, *www.midcas.org*.

[2] ITU, “Characteristics of and protection criteria for terrestrial radars operating in the radiodetermination service in the frequency band 8 500-10 680 MHz”, Recommendation ITU-R M.1796-2, February 2014

[3] ITU, “Characteristics and spectrum considerations for sense and avoid systems use on unmanned aircraft systems”, Report ITU-R M.2204, November 2010

[4] R. Rieger, B. Schweizer, H. Dreher, R. Reber, M. Adolph, H.-P. Feldle, „Highly Integrated Cost-effective“ Standard X-Band T/R Module Using LTCC Housing Concept for Automated Production“, Proceedings of EuSAR 2002.

DEVELOPMENT OF A MODULAR OPEN SOURCE RISK ASSESSMENT KNIME EXTENSION

Guido Correia Carreira[1], Miguel de Alba Aparicio[2], Alexander Falenski[3], Annemarie Käsbohrer[4] and Matthias Filter[5]

[1]Guido.Correia-Carreira@bfr.bund.de,[2]Miguel.De-Alba-Aparicio@bfr.bund.de, [3]Alexander.Falenski@bfr.bund.de, [4]Annemarie.Kaesbohrer@bfr.bund.de, [5]Matthias.Filter@bfr.bund.de

Federal Institute for Risk Assessment (BfR), Max-Dohrn-Str. 8-10, 10589 Berlin (Germany)

Abstract

Risk assessment (RA) is an important element of the food safety and public health risk analysis process. For microbial risk assessments (MRA) there are several guidelines on how to conduct them, but these do not contain technical specifications on exchange formats for models and simulation scenarios. As a consequence software tools available for creation and application of MRA models currently do not share any common "language" thus making direct exchange of information between those tools impossible. In addition, this insufficiency hampers the development of community-driven MRA model repositories which could be exploited by different independent software solutions. Here, we describe the newly developed Food Safety Knowledge (FSK) framework which provides for the first time flexible data formats (FSK-ML) and rules for standardised annotation of MRA models and simulation scenarios. Further, we describe the first FSK reference implementation extending the open source software framework KNIME. It facilitates the generation and application of re-useable MRA models and model components.

Keywords: microbial risk assessment, MRA, KNIME, FSK-ML, modeling, data standards.

1 INTRODUCTION

The assessment of risks posed by microorganisms in food or feed products is a critical task for private and public sector stakeholders. One international guideline for such risk assessments is the Codex Alimentarius [1] which, among other things, defines how to perform microbial risk assessments (quantitative as well as qualitative) and lists in an exemplary manner the information and methods relevant for each step. According to Codex Alimentarius a microbial risk assessment (MRA) contains the following steps: Statement of Purpose, Hazard Identification, Exposure Assessment, Hazard Characterization and Risk Characterization. However, the Codex guidelines are quite general and do not provide detailed specifications on technical issues, like the used programming language or data exchange format. Even though several scientific publications and reports elaborate on specific MRA concepts [2-7] there are currently no coherent and generic standards which would ensure a harmonized description of MRA models, simulation scenarios and simulation results. This is true despite the fact that such infrastructure is an important pre-requisite for efficient re-use and application of MRA models. Linked to this is the fact that in the domain of food safety modeling there are currently no open, shared MRA model repositories available. Platforms like http://FoodRisk.org currently only provide bibliographic references to models as well as data and software tools relevant for MRA modeling. One effort to create a real MRA model repository has been the Interactive online Catalogue on Risk Assessment (ICRA) (http://icra.foodrisk.org). This repository contains structured descriptions of risk assessment models, but this ICRA model representation is based on an internal data format. Thus the exchange and re-use of models in the ICRA portal is still not possible.

In contrast to this situation other scientific disciplines have been able to establish necessary resources to facilitate the exchange of models, specifically the domain of Systems Biology. Systems like the BioModels Database (https://www.ebi.ac.uk/biomodels-main) or the CellML model repository (https://models.cellml.org/cellml) contain several hundreds of curated and even more uncurated models, each described in a standardized software-independent format, for example in the Systems Biology Markup Language (SBML) or in the Cell Markup Language (CellML).

Inspired by these examples the work presented in this paper aims at the development of standards and software tools that facilitate the exchange of model-based knowledge in the MRA domain. We denominate our strategy the Food Safety Knowledge (FSK) framework as it covers several interrelated issues relevant for reaching the final goal of curated, community-driven MRA model repositories.

2 MATERIAL AND METHODS

2.1 Requirements

In order to develop MRA model repositories the new framework has to meet the following requirements:

1. Metadata on models is encoded using eXtensible Markup Language (XML). This requirement originates from the fact that XML is a highly flexible and widely adopted standard. Furthermore, there are already many XML-based domain extensions available ready to be used, for example SBML or MathML. Using XML thus allows leveraging the FSK development process by building on and extending existing software tools. One of the XML-based domain extensions is the Predictive Modeling in Food Markup Language (PMF-ML) [7]. PMF-ML is a precursor for FSK and adapts the technical standards of Systems Biology to the field of MRA. PMF-ML has been designed for the software independent representation of predictive microbial models and extends SBML v.3. Following the principle of building on existing work FSK should adopt as many resources from PMF-ML as possible.

2. The FSK framework has to allow the representation of models encoded in a software-independent format (e.g. using PMF-ML, SBML) as well as models encoded in a scripting language (e.g. R, Perl, Python, Matlab). The latter type of encoding is specifically important as a plethora of MRA models has been developed using scripting languages like R and Matlab in the past (e.g. [8-11]). A re-implementation or conversion of these legacy models into a software-independent format would not be realistic, even if this was technically feasible.

3. The FSK standard has to define how data as well as the configuration of model-based simulations should be represented.

4. The FSK framework has to provide a standard for exchanging sets of heterogeneous files.

2.2 Reference Implementation

To achieve a wide adoption of the FSK data standard it is necessary to develop supporting software resources, e.g. to simplify the creation, export and import of FSKX files. We decided to provide a first reference implementation for FSK inside the open source Konstanz Information Miner (KNIME) data analytics platform. The KNIME graphical user interface (GUI) allows the creation of data processing workflows from modular building blocks (so called nodes). In addition, KNIME already integrates several scripting languages like R, Python and MATLAB. This means that scripts in these languages can be executed within KNIME using existing KNIME nodes. The FSK reference implementation can exploit this infrastructure.

3 RESULTS

3.1 FSK framework

The Food Safety Knowledge (FSK) framework provides necessary format specifications and rules facilitating the establishment of curated, community-driven MRA model repositories (Figure 1). It has been developed on the basis of experience and resources from the Systems Biology domain.

Specifically, the FSK framework provides standards for:

- encoding and annotating MRA models (FSK-ML) (see 3.1.3)
- encoding and annotating simulation scenario settings (FSK SED-ML) (see 3.1.2)
- sharing information (FSKX file format) (see 3.1.2)

The FSK framework further adopts and adapts the “Minimum Information” concept [12] (here now called Minimum Information Required for Annotation of Food Safety Knowledge “MI-FSK”), which is of special importance for the successful establishment of curated MRA model repositories. The MI-FSK rules define which metadata has to be at least provided by authors for any of their FSK models if they apply for inclusion into a curated FSK model repository.

Finally, the FSK framework addresses the issue of software tools for end users by provisioning an open source reference implementation in the data analytics platform KNIME. It also makes relevant software code libraries available outside of KNIME as Java software code libraries.

All technical details on the FSK standards and rules are specified in the FSK guidance document published on the community portal “OpenML for Predictive Modeling in Food” (https://sourceforge.net/projects/microbialmodelingexchange/).

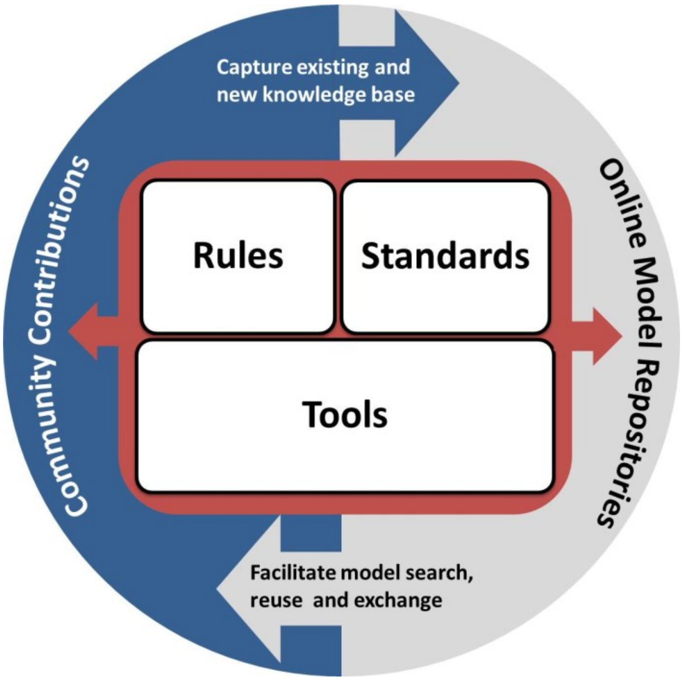

Capture existing and new knowledge base
Community Contributions
Online Model Repositories
Rules
Standards
Tools
Facilitate model search, reuse and exchange

Figure 1: The FSK framework. The framework is centered on rules, standards and tools for harmonized description of models and simulation scenarios. FSK allows models to be

encoded in a scripting language (e.g. R) or in a software independent representation (e.g. PMF or SBML format). The framework aims at broad adoption by the MRA community in order to generate input for future online MRA model repositories. These - preferably curated - resources will facilitate the search, comparison, reuse and exchange of models.

3.1.1 FSK-ML for MRA models

In contrast to Systems Biology there is a large legacy of script-based models in the MRA domain. This means these MRA models usually will not be made available in a software independent representation. As a consequence FSK-ML has been developed such, that information on the model (metadata) can be encoded in a separate XML-formatted file while the scripted model code itself can be provided in its original software dependent scripting language.

A selection of model metadata is given in Table 1. Whenever possible the use of a controlled vocabulary is encouraged.

Table 1: A selection of model metadata in the FSK framework. Multiple entries for a specific information field can be separated with "||"

Information	Example
Name	Dose Response Model for PRRS virus
FSK Type	Dose Response Model
Hazard	Porcine Reproductive and Respiratory Syndrome Virus (PRRS)
Route of Exposure	Food: Pork (raw)
Note	Infection of pigs with PRRSV after ingestion of 0.5 kg of pork (raw)
Dependent-Var(s) - Name	P
Dependent-Var(s) – Unit	[] (not applicable)
Independent-Var(s) - Name	dose
Independent-Var(s)_Unit	$\log_{10}$ TCID50
Creator	Guido Correia Carreira
Reference-Description	Brookes et al. (2014) Import risk assessment incorporating a dose-response model: introduction of highly pathogenic porcine reproductive and respiratory syndrome into Australia via illegally imported raw pork. Prev. Vet. Med. 113, 565-579
Software	R

3.1.2 FSK SED-ML for simulation scenarios settings

Systems Biology provides a technical standard to encode model-based simulation experiments. This standard is called Simulation Experiment Description Markup Language (SED-ML). The FSK framework proposes to extend this description such that it meets the requirements of MRA simulation experiments and to term it FSK SED-ML. Following the principles of SED-ML each MRA simulation is described by five program code templates, so called classes. The five classes are termed Model, Simulation, Task, DataGenerator, ListOfOutputs.

In the Model class the model to be used for the simulation is specified. Changes to the original model can be specified in this component as well.

In the Simulation class we extended the original SED-ML simulation types by the following simulation types: “Deterministic” (for simulations based on point-estimate models) and “Probabilistic” (for simulations based on probabilistic methods like Monte-Carlo or Bayesian networks).

The Task class defines which Models have to be combined with which Simulation at execution time.

The DataGenerator class defines which output values from which Task will be considered for output. Post processing of values may also be defined here in order to bring values in appropriate form for later output.

The ListOfOutputs class can be used to define specific plots that will be automatically generated from the data specified in the DataGenerator class. FSK deviates from classical SED-ML in so far as it allows an additional way of specifying plots, namely referencing to a script file which describes the plotting commands in the corresponding scripting language. To this end FSK SED-ML includes an additional element for the ListOfOutputs, called “Script”.

3.1.3 FSKX file format for information exchange

In the FSK framework the adoption of the COMBINE archive format [13] is proposed. A COMBINE archive is a ZIP file that contains at least a “Manifest.xml” file that lists the content, format and location of all objects inside the archive. For an easy identification of MRA-related files the suffix was named “.fskx”. Figure 2 illustrates the typical content of an FSKX file comprising a Manifest.xml and one or more files with model scripts, each annotated by a separate xml-formatted annotation file. In case of model scripts there are additional files specifying the default values of all independent model variables. This means that each FSKX file is equipped with enough information to be executed with those default parameters. In case authors want to provide specific preconfigured simulation scenarios this information can be stored in the FSK SED-ML scenario setting file.

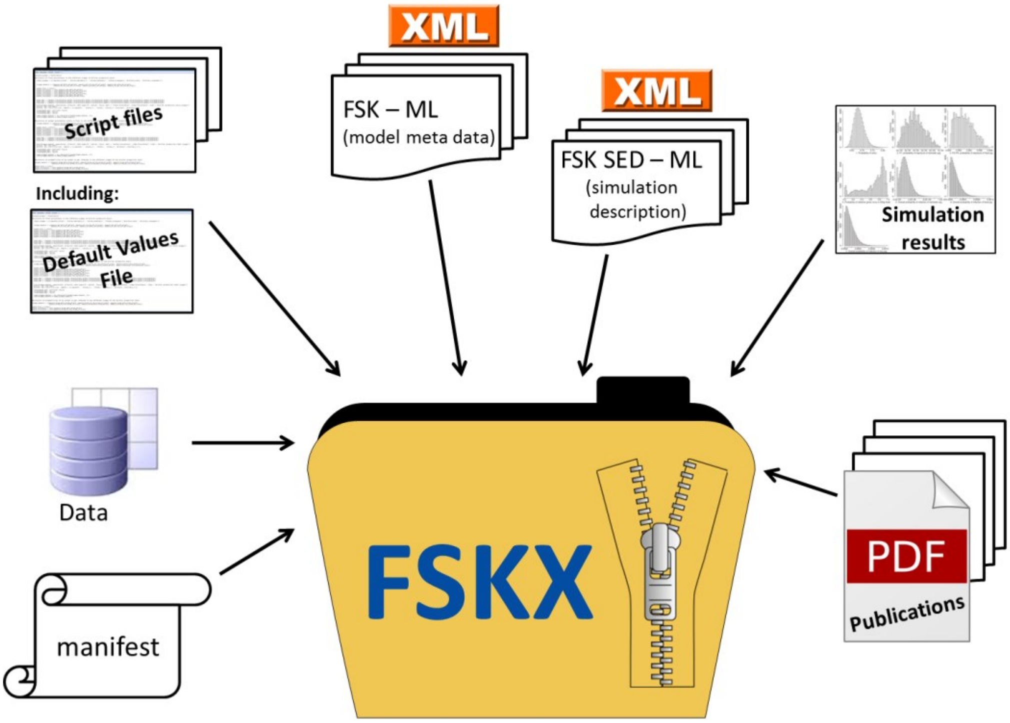


Figure 2: Concept of the FSKX file format to store information on MRA models and model-based simulations. Besides the Manifest.xml file all relevant information can be

included into the Zip file. Specific content can be described and annotated using dedicated formats, e.g. the FSK-ML for models, FSK SED-ML for simulation settings. The FSKX file may also contain PDF documents, e.g. depicting the result of simulations.

3.2 KNIME-based reference implementation

The FSK KNIME reference implementation so far contains five new KNIME nodes. The "FSK Creator" node allows the creation of an internal data object from R script files and a XML-encoded file with metadata on the R model. This internal data object can for instance be passed directly on to the "FSKX Writer" node which saves the internal data object into an FSKX file (Figure 3A)).

To read a saved FSKX file into KNIME the "FSKX Reader" node is used, which gives back the corresponding FSKX object, an entity which can then again be handled within KNIME using the other FSK nodes. For instance, having read the FSKX file the model scripts can be edited with the "FSKX Editor" and the modified model can then be passed to the "FSK runner" node. There, a model-based simulation using the default parameter is performed (Figure 3B)). Creating, editing, running and saving a model is shown in Figure 3C).

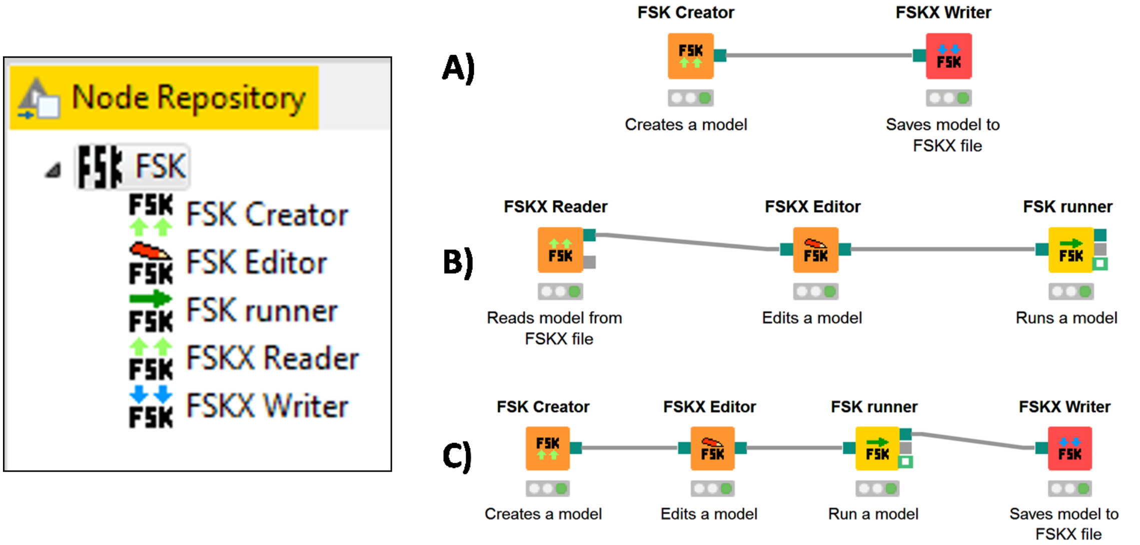


Figure 3: Three example workflows showing some possible combinations of the five currently available FSK KNIME nodes (shown in the KNIME Node repository on the left). A) Workflow for the creation of an FSK model with the "FSK Creator" and a subsequent export into an FSKX file. B) Using an "FSKX Reader" node to read an FSKX file. The corresponding model scripts are then modified using the "FSKX Editor" node and the modified model is executed in the "FSK runner" node. C) Creation, editing, running and saving of an FSK model.

4 CONCLUSION

The FSK framework provides the first set of rules and technical standards for harmonized annotations and representations of MRA models and simulations. Since such technical standards have been successfully applied in the Systems Biology domain the FSK framework likewise can lead the way towards the establishment of curated, community-driven MRA model repositories. Future work will focus on providing FSK support for additional software tools currently applied within the MRA domain.

REFERENCES

[1] Codex Alimentarius Commission, *Principles and guidelines for the conduct of microbiological risk assessment.* CAC/GL, 1999. **30**: pp. 1-5.

[2] Cassin, M.H., et al., *Quantitative risk assessment for Escherichia coli O157: H7 in ground beef hamburgers.* International journal of food microbiology, 1998. **41**(1): pp. 21-44.

[3] Marks, H.M., et al., *Topics in microbial risk assessment: dynamic flow tree process.* Risk Analysis, 1998. **18**(3): pp. 309-328.

[4] McNab, W.B., *A General Framework Illustrating an Approach to Quantitative Microbial Food Safety Risk Assessment.* Journal of Food Protection, 1998. **61**(9): pp. 1216-1228.

[5] National Research Council - Committee on the Institutional Means for Assessment of Risks to Public Health, *Risk Assessment in the Federal Government: Managing the Process.* 1983: National Academies Press.

[6] Nauta, M.J., *A modular process risk model structure for quantitative microbiological risk assessment and its application in an exposure assessment of Bacillus cereus in a REPFED.* 2001, NATIONAL INSTITUTE OF PUBLIC HEALTH AND THE ENVIRONMENT (Netherlands).

[7] Plaza-Rodríguez, C., et al., *A strategy to establish Food Safety Model Repositories.* International journal of food microbiology, 2015. **204**: pp. 81-90.

[8] Brookes, V., et al., *Import risk assessment incorporating a dose–response model: Introduction of highly pathogenic porcine reproductive and respiratory syndrome into Australia via illegally imported raw pork.* Preventive veterinary medicine, 2014. **113**(4): pp. 565-579.

[9] Haas, C.N., J.B. Rose, and C.P. Gerba, *Quantitative Microbial Risk Assessment*. 2014: Wiley. p. 350.

[10] Pouillot, R., et al., *Listeria monocytogenes in Retail Delicatessens: An Interagency Risk Assessment—Model and Baseline Results.* Journal of Food Protection, 2015. **78**(1): pp. 134-145.

[11] Vigre, H., et al., *Characterization of the Human Risk of Salmonellosis Related to Consumption of Pork Products in Different EU Countries Based on a QMRA.* Risk Analysis, 2015. **36**(3): pp. 531-545.

[12] Le Novère, N., et al., *Minimum information requested in the annotation of biochemical models (MIRIAM).* Nature biotechnology, 2005. **23**(12): pp. 1509-1515.

[13] Bergmann, F.T., et al., *COMBINE archive and OMEX format: one file to share all information to reproduce a modeling project.* BMC bioinformatics, 2014. **15**(1): pp. 369.

HUMAN SECURITY RADAR: THE BRAVE NEW WORLD OF NON-COOPERATIVE INSPECTION

Viktor Meshcheryakov, Semen Semenov, Valery Averyanov, Alexey Evsenin,
Igor Gorshkov, Pavel Iurmanov, David Kellermann, Andrey Kuznetsov, Grigory Labzovsky,
Marina Mokhova, Dmitrii Vakhtin[1], Igor Vorobev, Stanislav Vorobyev, Viktor Vorobev,
Evgenii Zarubkin

[1]*vakhtin@apstecsystems.com*
APSTEC Systems, Kesk-Sõjamäe tn 2, 11415, Tallinn (Estonia)

Abstract

An automatic standoff real time early warning system capable of non-cooperative detection of concealed metallic objects and dielectrics is described. The Human Security Radar™ (HSR) relies on active probing with low-power centimeter radio waves to detect person-borne threats at distances of several meters, as well as threat objects in suitcases and backpacks. Concealed dielectrics are detected and identified by their permittivity, while metallic objects are found by cross-polarization effect. Examples of the system's performance with different types of objects concealed on body ("suicide belts"), in backpacks and in wheeled luggage are presented.

Unlike other existing inspection methods, which require some degree of cooperation from the inspected people, HSR offers the unique capability to inspect a moving crowd in real time, so that only a small fraction of people is diverted for a more detailed inspection. This opens a completely new range of possibilities in extending security measures to places where they were previously considered to be prohibitively expensive and disruptive: approaches to train and bus stations, markets, administrative quarters, mass gatherings, etc. Possible CONOPs for the system are discussed.

Keywords: non-cooperative; early warning; detection; metals; dielectrics; standoff; radar; centimeter waves; automatic detection.

1 INTRODUCTION

One of the main problems currently facing the security community is the growing dissatisfaction of the public and businesses with the high operational costs and disruptions of normal functioning of the protected sites that are often associated with current security measures (see, e. g. [1] for an overview of financial cost of aviation security). This dissatisfaction, which is for the most part totally justified, not only threatens to undermine the current achievements in the traditional security areas, such as aviation security, but also prevents deployment of security solutions to other high-risk locations, such as urban transport infrastructure (metro, trains, buses), mass sports and political events, government buildings etc.

Dramatic reduction of the operational costs and the inconveniences caused by security measures to the protected sites would thus be the key to maintaining and increasing both the level and proliferation of security measures.

In this article we describe the emerging completely new approach to security: non-cooperative operator-free real time wide area inspection, which is made possible by the Human Security Radar (HSR) [2], [3]. HSR is capable of detecting metallic, dielectric and mixed threats hidden on human body, in backpacks or in luggage, in real time and from distance of several meters. First we discuss the notion of "non-cooperative security" as opposed to traditional security measures that require cooperation from the inspected people. Next we briefly describe the technology behind HSR with the emphasis on the features that make it suitable for operation in the "non-cooperative" mode. Then we give some examples of the systems performance and capabilities. Finally, we discuss the place of the non-cooperative HSR technology among the existing techniques and possible CONOPs for its deployment.

2 COOPERATIVE VS. NON-COOPERATIVE INSPECTION

Most of the threat detection technologies that have been used in the security field so far require some cooperation from the inspected people. The degree of expected cooperation varies from relatively mild requirement to stand in certain position for a certain time to really annoying "take everything out of your pockets" request. Whatever the cooperation requirements are, somebody has to ensure that the inspected people cooperate properly. This means that even for fully automatic systems, such as metal detectors, the performance will depend on the skills and motivation of the security staff, and the need to have such staff near every inspection system makes operational costs very high[1].

Direct consequence of the standard cooperative inspection approach is prohibitive cost of using existing inspection systems in crowded places: even for automatic detection systems, too much personnel would be needed to ensure that everybody cooperates properly.

The only widely used non-cooperative security-related hardware are CCTV cameras, which often work without people even knowing that they are viewed. However, CCTV cameras typically require human operators to interpret video stream, and are thus mainly useful after the incident has already happened.

Any threat detection system that would not require cooperation from the inspected people should meet the following minimal list of requirements:

1. It should not require inspected people to alter their normal behavior in a significant way. At most, mild crowd control measures such as queue fences may be used. Ideally, the person would not even know about the fact of inspection.
2. It should not require constant attention from security personnel, who would only occasionally receive information about an alarm via network (possibly, wireless), and may be busy with other things rest of the time.
3. It must be followed by an established procedure to resolve alarms, for example diverting people who caused alarms for additional inspection, automatically controlling some access blocking system, using face recognition or other analytic software, etc.
4. It should have very low false alarm rate, so that it would not cause inconvenience to the security personnel, the public, or the protected site.
5. It should have high throughput and work unattended in an operator-free mode, so that no queues are created in the place of inspection.

If these requirements are met, the system would not interfere with the normal operations of the protected site, and operational costs would be very low due to savings on personnel.

In the following section we describe what we believe to be the first non-cooperative inspection, operator-free threat detection system capable of working in crowded places: the Human Security Radar (HSR).

3 DESCRIPTION OF HSR

HSR is based on sending very low-power centimeter radio waves into a wide-angle area, and receiving and analyzing scattered and transmitted waves. Different types of materials produce distinctively different responses to radio waves:

- human body is a good reflector for radio waves in the used frequency range, so it looks like a large reflective surface;
- dielectrics are partially transparent for radio waves and have refractive index larger than 1, which leads to the apparent increase of the flight path traveled by the wave between the emitter and the receiver;
- edges of the metallic objects lead to rotation of the polarization of the incident wave.

The principles behind HSR have been described in some details in [2] and [3] and references

[1] http://www.homelandsecurityresearch.com/blog/purchasing-price-of-whole-body-scanners-represents/

therein. HSR is a flexible system that can be implemented in portal configuration, as a longer-range flat-panel configuration, or as a combination of both. HSR operates in two distinct modes: “reflection” and “transmission” [2].

In the stand-off “reflection” mode the system measures the radio waves reflected from objects in different polarizations. Position of scatterers with different reflecting properties on the scene are then reconstructed from the measured complex electromagnetic field using high-speed parallel processing units. The obtained distribution of scatterers may be then compared to an optical or depth image of the scene. Properties of found dielectrics, such as thickness, shape, and permittivity, can be obtained from subsequent automatic analysis and used in the decision making procedure to distinguish between dangerous and benign objects. Analysis of the response of the scene in different polarizations allows one to detect metallic objects.

In the close-range “transmission” mode the system measures the time shift and amplitude of electromagnetic waves passing right through the dielectric when the person is between the emitting and receiving antennae. Any apparent increase of the flight path in an indication of presence of a substance with refractive index larger than 1 between the antennae. Further analysis involving for example building multiple tomographic images at different time slices allows one to detect presence of dielectric objects on human body, in backpacks, or in wheeled luggage.

HSR collects data at a rate of tens of frames per second and then analyzes them using high-speed parallel processing units, thus achieving true real time performance.

The system may be complemented by additional video or depth sensors, so that a photograph of the suspect carrying a threat with superimposed information about threat location and type can be send to an existing security network. Alternatively, HSR has its own user interface (Fig. 1), which runs on a remote device and can accumulate information from several systems. There is no need for the security staff to constantly monitor the data from the HSR: it only sends information when the threat has been detected.

HSR fulfills the following requirements for the system capable of non-cooperative operation in crowded environments without disrupting normal operation of the site:

- it is fully automatic and operator-free;
- it works in real time from standoff distance of several meters;
- it inspects multiple people simultaneously;
- it can detect a wide range of threats, including improvised ones;
- it has very low false alarm rate.

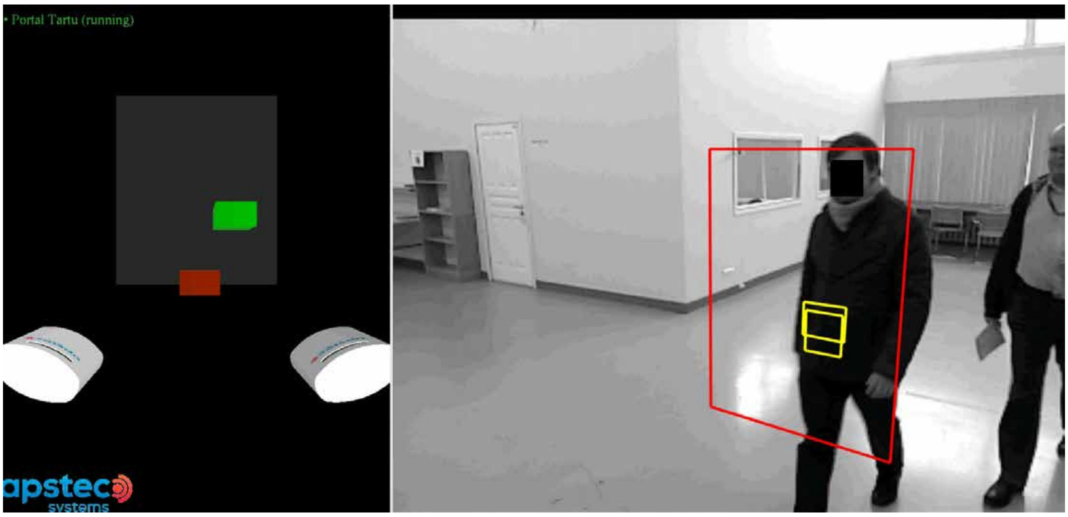


Figure 1. Example of a detailed user interface with a reported alarm. The user interface may run

4 HSR CAPABILITIES

4.1 Detection of metallic weapons and shrapnel

Metallic threats are detected by automatically comparing relative intensities of signals reflected from some point with different polarizations (see, e. g. [4], page 33).

The radio waves emitted towards the scene are polarized along one or several directions. Reflected waves are measured both in the same and in the orthogonal polarization to the incident one. Metallic objects with complex shape, such as guns, tend to rotate the polarization of the incident wave by 90 degrees. Distributions of the reflecting points across the scene measured in two orthogonal polarizations are automatically compared, and regions with excess cross-polarized component are marked as potential metallic anomalies. Parameters and trajectories of these anomalies are then automatically tracked within many consecutive frames, and compared with the location of dielectric objects found by the respective algorithms. Then the decision is made whether the anomaly is the actual metallic object, an artifact, or part of a mixed (metal-dielectric) threat. The objects considered dangerous are reported to the user in the form of a photograph with superimposed rectangle showing the location of the threat (Fig. 2).

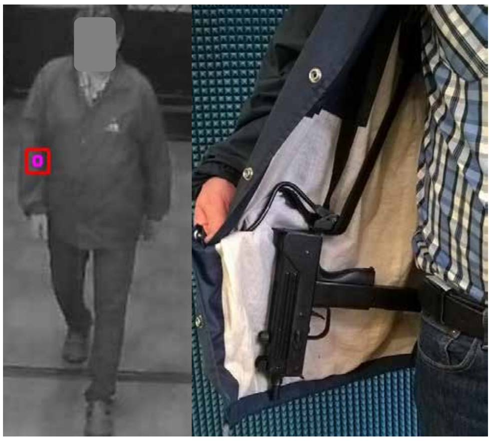


Figure 2: Detection of a concealed machine gun. Photograph shown on the left accompanies alarm information, which is sent to the remote user.

Fig. 3 shows example of an internally processed image of the person carrying a “suicide belt” surrounded by shrapnel. This image is not sent to the user, but instead analysis of a sequence of such images gives rise to an alarm similar to one shown on Fig. 2.

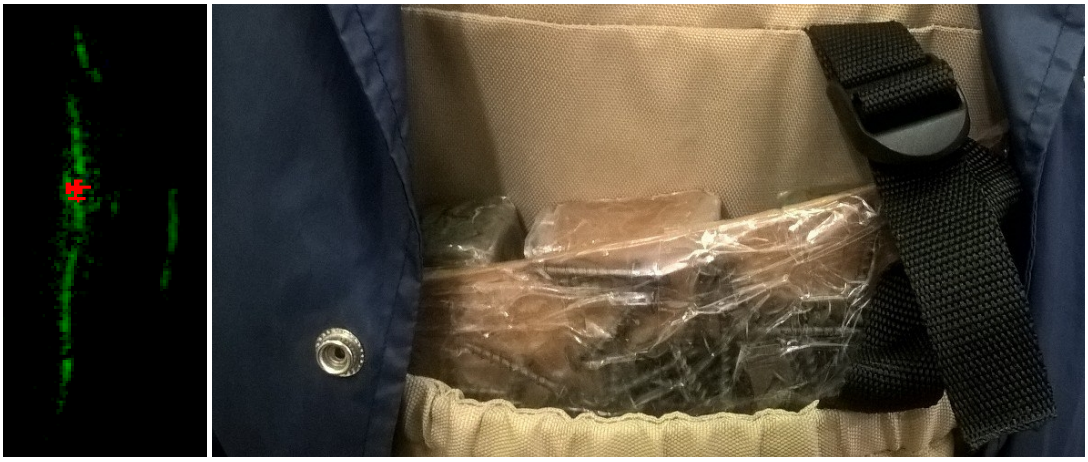


Figure 3. Detection of a “suicide belt” surrounded by shrapnel; a sequence of images similar to the one showed on the left are processed internally by the system to produce an alarm.

Metal detection capability is currently integrated into the walk-through portal configuration of HSR.

Another way the HSR can potentially detect large metallic objects hidden in luggage (for example, of the type used in Boston Marathon attack on April 15, 2013) is by detecting anomalous blocking of the radio waves passing through the backpack ("transmission") in conjunction with the properties of the reflected waves ("reflection"). This allows the system to detect a large metallic objects in backpacks even if they do not have the characteristics that cause strong cross-polarization effect.

4.2 Detection of "suicide belts"

Dielectrics are detected by automatically analyzing the areas with apparent increase of the flight path of the wave on its way from emitter to receiver. Depending on the configuration of the system and location of the moving person this increase appears either on the reconstructed reflected field ("reflection" mode) or on the field transmitted through the dielectric ("transmission" mode).

Fig. 4 shows a screen-shot from user interface showing an alarm from a suicide belt.

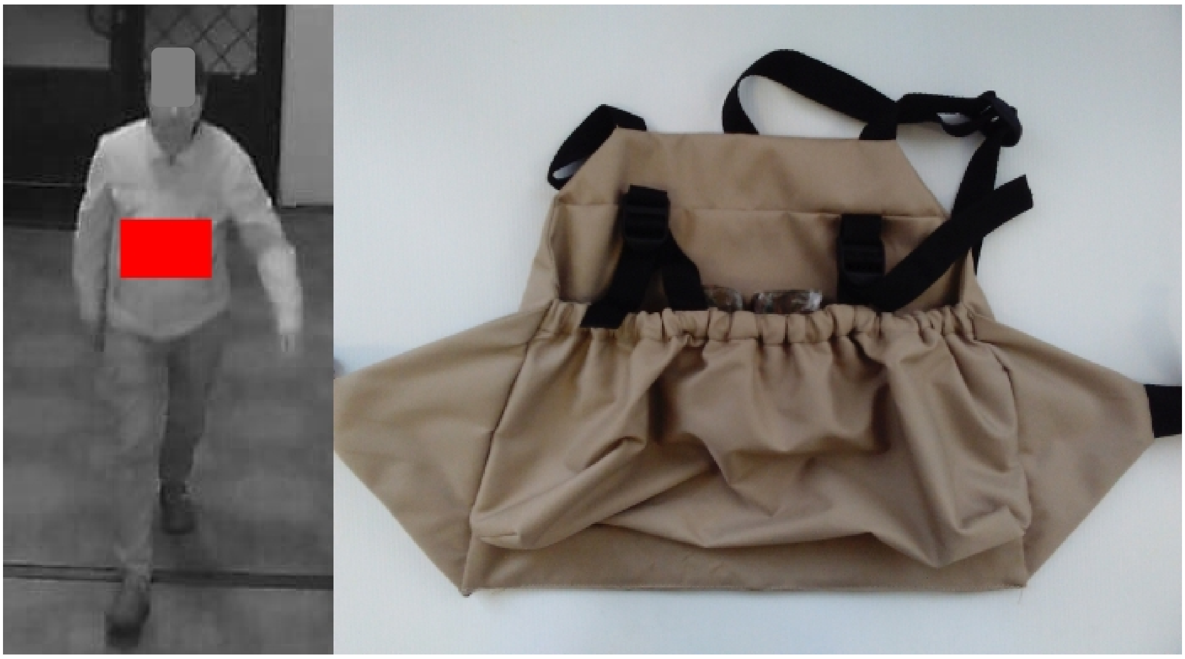


Figure 4. Example of detection of a mockup "suicide belt" with two small bricks of dielectric explosives' simulant. The location of the threat is shown by a rectangle superimposed on a photograph.

The capability to detect dielectrics has been demonstrated during tests at an industrial facility (see [3]). The rate of false alarms was shown to be less than 1%, while the detection rate for the realistic explosives simulants used was about 90%.

If the explosive charge is completely surrounded by shrapnel, it can still be detected by the characteristic signature of metals (see section above).

4.3 Detection of bombs in luggage

HSR can look for threats not only on human body but also in wheeled or carried luggage. The main difference between detecting explosives in suicide belts and in luggage is that a typical luggage item contains large amounts of dielectric stuff (for example, clothes, shoes, paper, plastic), which should not be mistaken for an explosive substance. One can rely here on the fact that most explosives are somewhat denser than widespread "benign" dielectric materials. Typical density of standard explosive is about 1.7 g/cm^3, while density of clothes, shoes, dry paper etc. is usually lower. Thus, an explosive hidden among other dielectrics in a suitcase would appear to the system as a dielectric "anomaly" consisting of a dense "core" surrounded by less dense dielectric "peel" with both the "core" and the "peel" increasing the apparent path of the wave but to different degrees. HSR uses a path-based "peeling" algorithm to separate the dense "core" of the anomaly from surrounding materials. Then the parameters such as apparent increase of the wave path, amplitude of the corresponding peak, volume of the anomaly etc. are determined separately for the "core" and for the "peel".

Fig. 5 shows example of distributions of path increase and the corresponding peak amplitude for anomaly "cores" and "peels". Each point represents a dielectric "anomaly" found on a person passing through the system with a large backpack with or without an explosive simulant (green squares and red circles), or with different simulants hidden in "suicide belts" (orange diamonds).

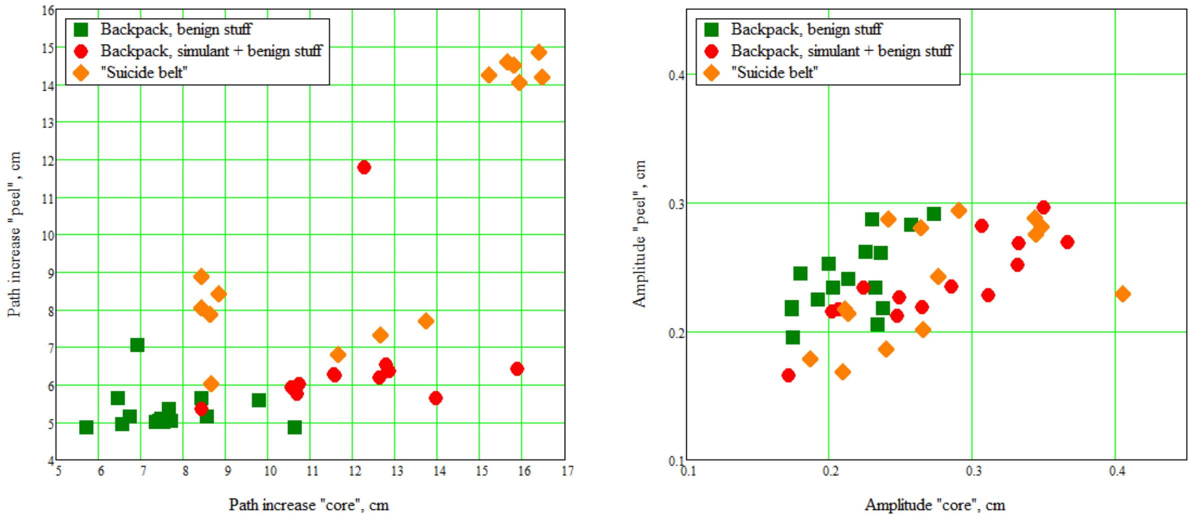


Figure 5. Distribution of the apparent path increase of the wave due to passage through dielectric (left panel) and amplitude of the shifted peak (right panel) for the dense "cores" of the found anomalies and for the less dense "peel". Each point represents one anomaly.

These and other similar graphs are used to train the automatic data analysis system, which is then capable of automatic detection of dense objects with required characteristics surrounded by less dense objects in luggage. While on every individual plot the regions corresponding to luggage with threats and with no threats may largely overlap, multidimensional machine learning algorithms can separate them very reliably.

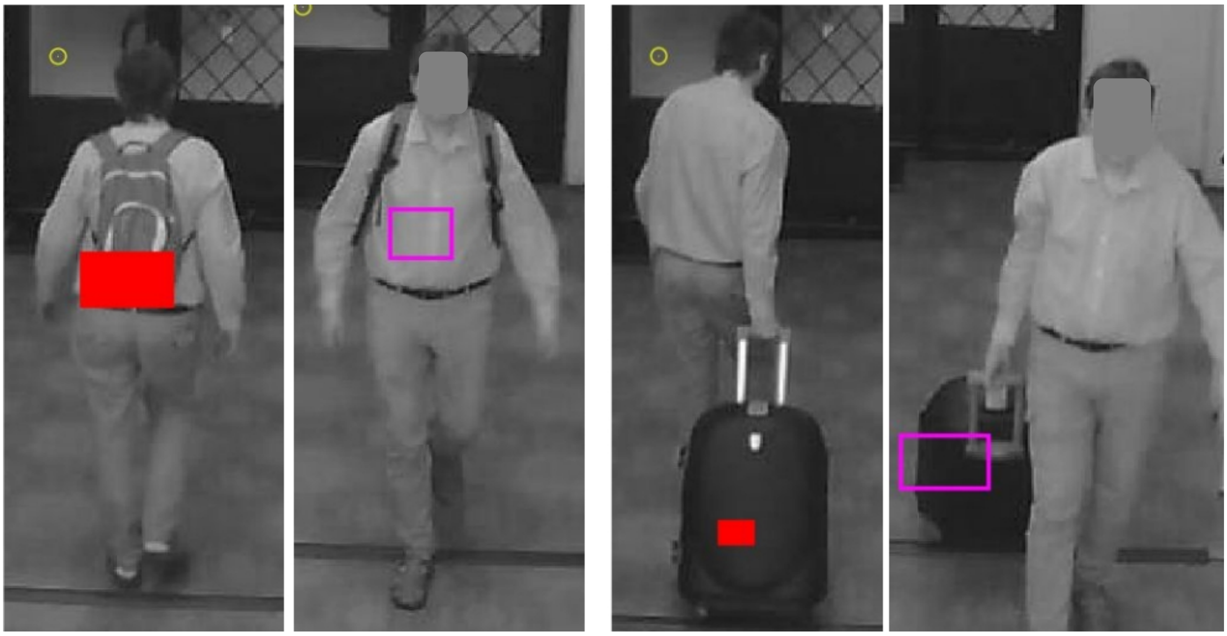


Figure 6. Examples of the images available to the user showing locations of threats in luggage. Filled red squares indicate that the threat is visible to the camera; open magenta squares indicate that the threat may be obstructed from the camera by the body.

Fig. 6 shows examples of images that are included into the alarm information. Left to right: small backpack containing a large simulant; large backpack with a simulant surrounded by clothes; suitcase with simulant and clothes carried away from the camera; suitcase with simulant and clothes carried towards the camera. The type of the colored square indicates whether the detected threat is visible by the camera (filled), or part or all of it may be obstructed by the body (open). For example, the open square on second photo from the left indicates that the threat is in a large backpack on the person's back. Thus, the security staff gets better idea about the location of the threat even if only one camera is used.

5 WHERE TO USE HSR: POSSIBLE CONOPS

When planning a deployment of an inspection technology one should consider both how it would affect the “innocent general public” and how it would help to prevent an “offender” from carrying illicit substance or object, or a “terrorist” from carrying out an attack.

In the case of cooperative inspection the inspected person (whether it is a terrorist or not) always knows about the fact of inspection, while in the case of non-cooperative inspection this is not necessarily the case. Knowing about the inspection deters the terrorist, while also makes it relatively easy for him to prepare and avoid being detected.

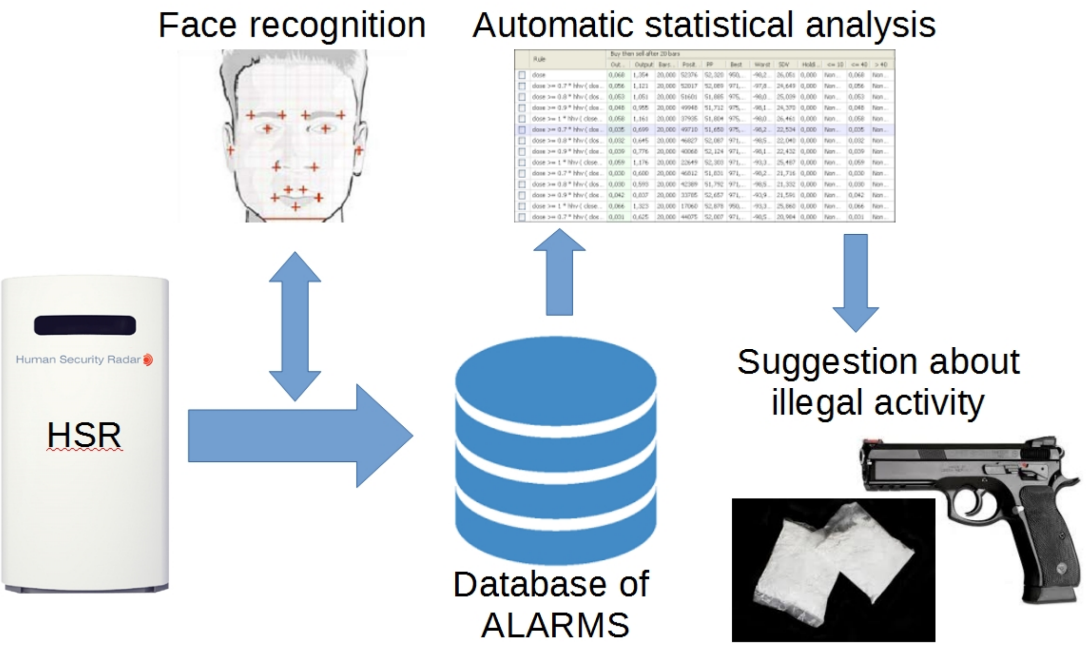

Face recognition
Automatic statistical analysis
Human Security Radar
HSR
Suggestion about illegal activity
Database of ALARMS

Figure 7. Possible use of HSR as data source for automatic crime prevention network.

In the case of non-cooperative inspection, the inspected people may or may not know about the fact. In both cases:

1. There is no negative effect of human factor on detection;
2. Inspection causes no inconvenience for the site;
3. Inconvenience only for those causing false alarms; others are not affected;
4. No queues, no staff, so less damage in case of an explosion at the checkpoint.

If the inspection is covert, then in addition to the above:

1. There is no risk of an explosion at inspection point, which is not an attractive target due to lack of queues and no personnel on the spot;
2. Probability of detecting a threat may be higher than if the terrorist is aware of the inspection, even though the nominal detection probability of a non-cooperative technology

may be lower than that of the technology that requires cooperation.

With that in mind, one can envisage two main ways of using HSR:

1. Open inspection: an early warning system operating well before the people are actually entering the protected area (for example, hundreds of meters away from the entrance to a stadium or a train station). It will signal the possibility of a high-risk target, which should be attended to by a relevant procedure.
2. Covert inspection: a standalone system installed at some distance from the protected area (for example, a military checkpoint) or right within the area with high crime risk (for example, area with high proliferation of illegal guns). It will quietly inform the military personnel or law enforcers about the potential threat or illegal activity (Fig. 7).

In both cases HSR can be followed by a face recognition database, which will provide identification of the threat carrier while he or she is still at a safe distance.

6 CONCLUSIONS

Human Security radar (HSR) is the first system capable of non-cooperative automatic security screening in crowded places. It is operator-free and only notifies the security personnel about found threats without the need for anybody to constantly monitor video or other data streams. This would lead to a dramatic reduction of operational costs.

HSR has been demonstrated to be able to detect both metallic (weapons), dielectric (explosives) and mixed (IEDs with shrapnel) threats in real time from stand off distance with very low false alarm rates. Being a non-cooperative inspection system, HSR causes very little inconvenience to general public and, unlike existing methods, causes no disturbance to the normal operation of the protected site.

Depending on whether the fact of inspection is disclosed, HSR can be used in one of the two modes:

1. Open inspection: an early-warning system that scans the crowd approaching the protected area and selects high-risk targets for in-depth inspection by the existing means. In this mode HSR provides the security personnel with enough time to evaluate the threat and take counter measures.
2. Covert inspection: a standalone system monitoring security situation at a high-risk location and providing remote or local security personnel with an alarm about possible illegal activity (for example, people carrying “suicide belts” or machine guns under their clothes).

Alarm signals produced by HSR include information about the type and location of the threat, as well as photographs of the suspected offenders, which may be used in the context of a broader security network featuring, e. g. face recognition, automatic doors etc.

REFERENCES

[1] David Gillen, William G. Morrison, “Aviation security: Costing, pricing, finance and performance”. Journal of Air Transport Management 48, pp.1-12 (2015)

[2] Valery Averianov et al., “Automatic Standoff Detection of Threats in Crowded Areas”, // Proceedings of the Security Research Conference “9th Future Security”, Klaus Thoma, Ivo Häring, Tobias Leismann (Eds.), September 16 –18, 2014, pp. 319-326 (2014)

[3] Andrey Kuznetsov et al., “Extending Security Perimeter and Protecting Crowded Places with Human Security Radar” // Proceedings of the Security Research Conference “10th Future Security”, Jürgen Beyerer, Andreas Meissner, Jürgen Geisler (Eds.), Berlin, September 15–17, 2015, pp.371-377 (2015)

[4] 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).

RISK ANALYSIS OF THE VULNERABILITY OF CRITICAL INFRASTRUCTURE ON INTENTIONAL EMI THREATS

Tim Peikert[1], Heyno Garbe[2] and Stefan Potthast[3]

[1] *peikert@geml.uni-hannover.de*
[2] *garbe@geml.uni-hannover.de*
Leibniz Universität Hannover, Institute of Electrical Engineering and Measurement Technology, Appelstr. 9a, 30167 Hannover (Germany)

[3] *stefanpotthast@bundeswehr.org*
Bundeswehr Research Institute for Protective Technologies and NBC Protection, Humboldstraße 100, 29633 Munster (Germany)

Abstract

This paper discusses a risk estimation for a complex electronic system in its environment and infrastructure. The estimation of the vulnerability of a system with the respect to intentional electromagnetic interference (IEMI) is based on the fuzzy set theory. In addition to estimate the risk with exact values, the approach can handle unprecise data, uncertainness, objective and subjective knowledge from experts in one mathematical model. The approach uses fuzzy sets, membership function, fuzzy rules and logic to handle the uncertainness to predict the hazard level of the investigated system.

Keywords: IEMI, IEME, risk analysis, fuzzy, critical infrastructure, fuzzy rules, fuzzy logic.

1 INTRODUCTION

The complexity of critical infrastructure is predominant manageable with electronic controlling units based on IT systems. The misbehaviour of the IT systems can lead to a failure of subsystems or as worst-case scenario to a breakdown or loss of the whole system. That malfunction can be caused by criminal activities using electromagnetic tools, which is adopted in a resolution by the URSI in 1999 at its XXVIth General Assembly in Toronto [1].

In the following ten years several investigations started by different research groups, for e.g. Bäckström [2], Giri [3] and Sabath [4], to classify and analyze the physical mechanism of electromagnetic interferences and caused effects on electronic systems. Every study leaded to an increasing risk by criminal use of electromagnetic tools. To estimate this risk a mathematical and systematically approach is needed to analyse the critical infrastructure against an IEMI threat.

Typical statistical and computational risk analyse tools are the fault-tree analysis (FTA), electromagnetic topology (EMT) and Bayesian networks (BN). These methods are mainly based on exact information and have its difficult to analyse highly complex systems, such as critical infrastructure is. The complexity of such infrastructure and the interconnection of many different systems will be raising in the foreseeable future. In the last years the power grid change to a complex smart grid (Fig. 1), other keywords are Industry 4.0, internet of things (Fig. 2), Building Information Modelling and Smart Home which will lead to a stronger interconnection between different systems.

The approach, to estimate the potential risk is based on the fuzzy theory [5] which can handle imprecise data and non-technical attributes. To describe the probability of occurrence of an IEMI source which can harm the victim system, imprecise and non-technical information are needed to rate the potential risk. Typical attributes to estimate the probability of occurrence of such sources are the mobility level, the technical challenge, the

Acknowledgements. The results shown in this paper were partly produced with the support of the Bundeswehr Research Institute for Protective Technologies, NBC-Protection in Munster, Germany. (E/E590/CF149)

cost, the hazard level, acquisition level and the discoverability. For these attributes principally no precise information exist. Mainly the opinion of experts is used to classify this different attributes. An example for the classification of the mobility level is presented by Sabath et al. [4] and they are stationary, transportable, mobile, very mobile and highly mobile. Thereby, a problem occurs between the boundaries from one level to another one. The opinion between different experts can slightly differ from each other which lead that one classifies the source as very mobile and the other one as highly mobile. The fuzzy theory can handle that difference with crossing boundaries with their assessment function. Additional, the fuzzy theory has some more advantages. This mathematical model consists of fuzzy sets [6] with their membership functions and the fuzzy logic in the form of a multi-valued logic. Also it allows to describe the behaviour of a system with linguistic terms instead of exact values. With this model it is possible to describe the IEMI sources, the victim system and the infrastructure in combination with their environment. An example for the estimation of the risk of a victim system including its infrastructure is shown in Fig. 1.

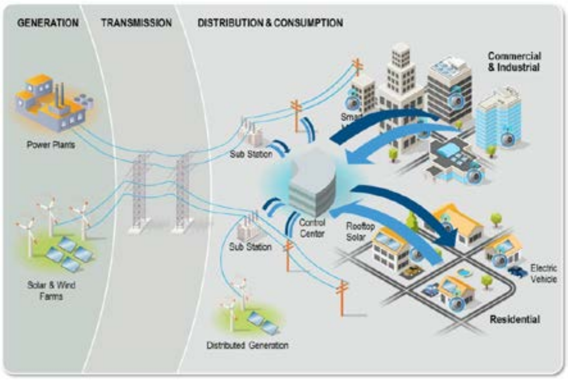


Figure 1 Overview of a Smart Grid [7]

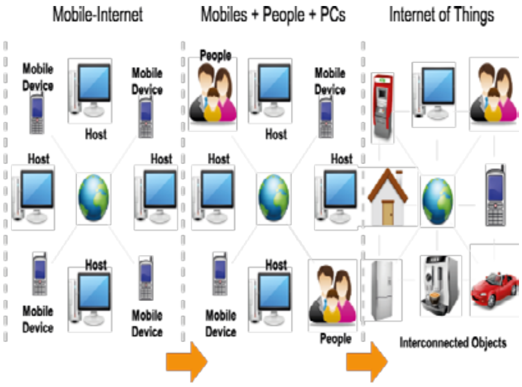


Figure 2 Example for Internet of Things [8]

2 FUZZY APPROACH

The fuzzy approach [5] is divided into three main functions, the fuzzy set theory, set of rules and fuzzy logic. The classical set theory defines that an object belongs to a set or not. Instead the fuzzy set theory [6] allows an object belonging to multiple exclusive sets with a degree of membership. The membership function $\mu_A(x)$ characterized a fuzzy set $\tilde{A}$ of X which is associated with a number in the interval $[0,1]$ and is expressed as follow:

$$\tilde{A} = \{(x, \mu_A(x)) | x \in X\} \ with \, \mu_A : X \rightarrow [0,1].$$

Typical membership function have often a shape of triangle, trapezoid, sigmoidal or Gaussian bell. An example for a membership function of the breakdown failure probability (BFP) [5] of an electronic device is expressed with the following equation:

$$\mu_{BFP,ra}(x; \alpha, \beta) = \begin{cases} 0 & x \leq 0, \\ \int_0^x f(t, \alpha, \beta) dt & 0 < x \leq 1, \\ 1 & x > 1, \end{cases} \tag{1}$$

in which $f(t, \alpha, \beta)$ stands for the standard beta probability density function (PDF) and ra in BFP_{ra} means the random angle of incident. The PDF is calculated from the beta distribution function $B(\alpha, \beta)$, its shape is determined by the two factors α and β and is expressed as follows:

$$f(t;\alpha,\beta)=\begin{cases}\frac{1}{B(\alpha,\beta)}t^{\alpha-1}(1-t)^{\beta-1} & 0\leq t\leq 1\\ 0 & otherwise\end{cases} \tag{2}$$

The fuzzy logic operators such as union (Fig. 1a), intersection (Fig. 1b) and complement (Fig. 1c) are similar to the aggregation operators in the classical set theory. The operation on two sets A as $\mu_A(x)$ and B as $\mu_B(x)$ are defined as follow:

union: $A\cup B \Leftrightarrow \mu_{A\cup B}(x)=\mu_A(x)\cup\mu_B(x)=max\{\mu_A(x),\mu_B(x)\}$,

intersection: $A\cap B \Leftrightarrow \mu_{A\cap B}(x)=\mu_A(x)\cap\mu_B(x)=min\{\mu_A(x),\mu_B(x)\}$,

complement: $\hat{A} \Leftrightarrow \mu_{\hat{A}}(x)=1-\mu_A(x)$,

which is based on the model of Takagi and Sugeno (T-S) [9]. The difference from the fuzzy set to the classical set theory is, that the degree of truth of an element belongs to the union of some fuzzy sets is the maximum of the degree of truth that the element belongs to each of the fuzzy sets.

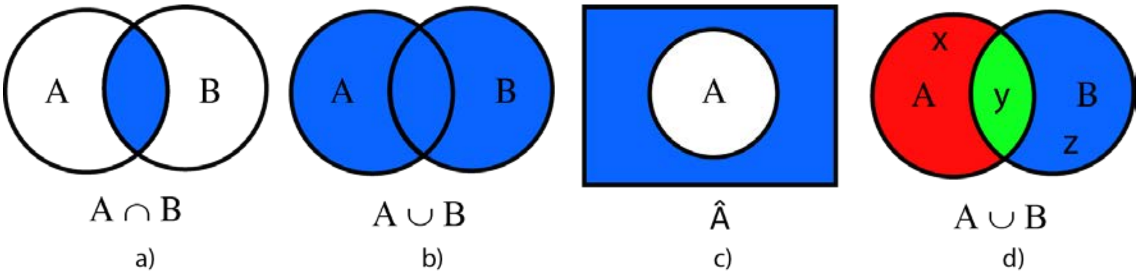


Figure 3 Fuzzy logic operator: disjunction, conjunction and complement [10]

The last main function are the fuzzy rules, which can be considered as the knowledge of an expert who knows exactly the system behaviour. The fuzzy rules is represented by a sequence of the form IF-THEN. They associates a condition described by linguistic variables and/or fuzzy sets to a conclusion or output. More than one input could be combined by the Boolean algebra (AND = min; OR = max; NOT = additive complement). The IF part is used to capture the knowledge by using the input conditions and the THEN part can be utilized to give the conclusion or output in linguistic variable form. An example for two fuzzy rules with two inputs are shown in table 1.

Table 1 Example of two fuzzy control rules with the Mamdani method

No.	**Rule**
R_1	IF x is A_1 AND y is B_1 THEN z is C_1
R_2	IF x is A_2 AND y is B_2 THEN z is C_2

3 RISK ESTIMATION

To assess the risk of a complex system in consideration of the infrastructure and the environment many information are needed. Obtaining this information can be divided in three main parts.

The first one is the analysis of the vulnerability of the considered electronic system. Therefore, the susceptibility of the system has to be analysed, the electromagnetic shielding, the interconnection and the dependencies between the different subsystems.

The second part is the analysis of the infrastructure and the environment. The main points for the analysis are the localization of the victim system and other dependent systems which can directly lead to a misbehaviour of the system. An example for dependent systems are the cable distributors for power and telecommunication, which are often near borders of the infrastructure area. Another point is to divide the area in zones of accessibility.

And the last one is to classify the potential IEMI sources and the outgoing hazard level of them. Therefore, the mobility level of the source has to be estimated, the possibility of detection and the likelihood of occurrence.

3.1 System Breakdown Behaviour

For the prediction of the vulnerability of the system, it is necessary to characterize the behaviour of each subsystem. Also the fault propagation from any subsystem to subsystem has to be taken into account. To estimate the BFP of a subsystem, Genender [11] presents an analytic expression with a random angle of incident. A membership function (Fig. 4) of the BFP expression (Eq. 1 and 2) is presented in Peikert [5].

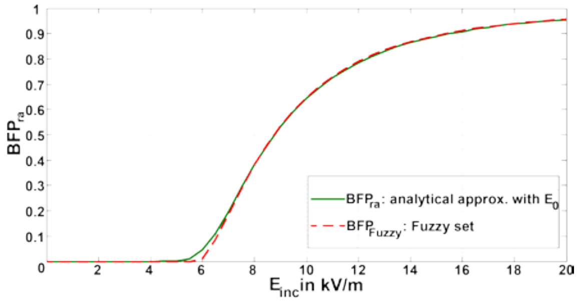


Figure 4 ***BFP$_{ra}$*** **membership function by Peikert [5]**

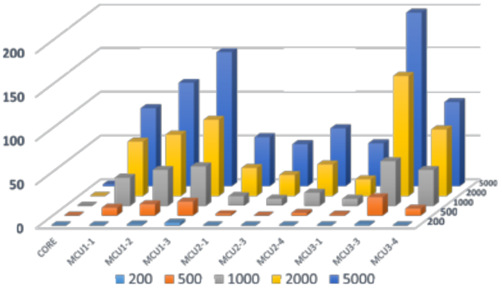


Figure 5 Breakdown behavior of a compound of microcontroller by Peikert [12]

In Peikert [12] a compound of different microcontroller circuits is used as the victim system. A result of the determination of the breakdown failure behaviour from the different subsystems exposed by a double exponential pulse is shown in Fig. 5. The intersection result of the breakdown behaviour rate (BFR) of the whole victim system lead to follow expression [12]:

$$\mu_{BFR,whole} = min\{\mu_{BFR,core}, \mu_{BFR,MCU1-1}, \mu_{BFR,MCU1-2}, \dots, \mu_{BFR,MCU3-4}\}$$

3.2 Risk Estimation

Many pieces of information are needed to estimate the risk level of a complex system and its infrastructure with including the surrounding area. Some expert opinions about IEMI sources are published by Sabath [13] and Giri [14] published a classification of the intentional electromagnetic environment. Other keywords for a systematically approach to estimate the risk are published by Sabath [15], for example some keywords are the mobility level (ML), threat level (TL), hazard level (HL), zones of accessibility (ZoA), likelihood of occurrence, level of detection, technology challenge (TC) and some more.

Table 2 Example of fuzzy rules for the technology challenge

1.	IF (SfA is restricted acquisition) AND (SfrK is expert) AND (CS is extreme cost) AND (LoS is development group) THEN (TC is highly sopisticated)
2.	IF (SfA is of-the-shelf) AND (Sfrk is novice) AND (CS is low cost) AND (LoS is open literature) THEN (TC is low tech system)
3.	IF (SfA is commercial available) AND (Sfrk is specialist) AND (CS is increased cost) AND (LoS is technical literature) THEN (TC is medium tech system)
4.	IF (SfA is specialized trade) AND (Sfrk is graduate) AND (CS is high cost) AND (LoS is technical literature) THEN (TC is high tech system)

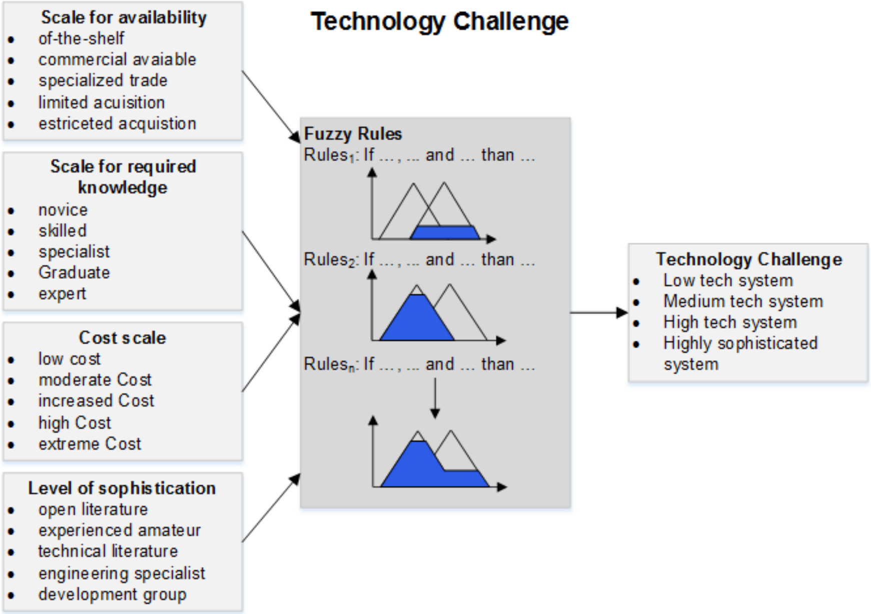


Figure 6 Fuzzy system for the technology challenge

This keywords are partly dependent on each other and one keyword can be divide into some more detailed ones. The technology challenge of HPEM sources can be divide into the scale for availability (SfA), scale for required knowledge (SfrK), cost scale (CS) and the level of sophistication (LoS). A fuzzy system to estimate the TC with the four inputs SfA, SfrK, CS and LoS is illustrated in Fig. 6 and lead to the linguistic terms for the TC which are low tech-, medium tech., high tech- and highly sophisticated system. The expert opinions from Sabath [13] are used to define the rules for the fuzzy systems. Exemplary four of the more than 500 rules are show in Table. 2.

Another example is the estimation of the hazard level which could emanate from an IEMI source. The input for this fuzzy system (Fig. 7) are the mobility level (ML), the accessibility zone (AZ), the likelihood of occurrence (LoO) and the level of detection (LoD) and lead to the linguistic terms of the hazard level (HL). The terms for the hazard level are low (< 0.1 kV/m), little (0.1 – 1 kV/m), middle (1-10 kV/m), high (10-100 kV/m) and very high (>100 kV/m).

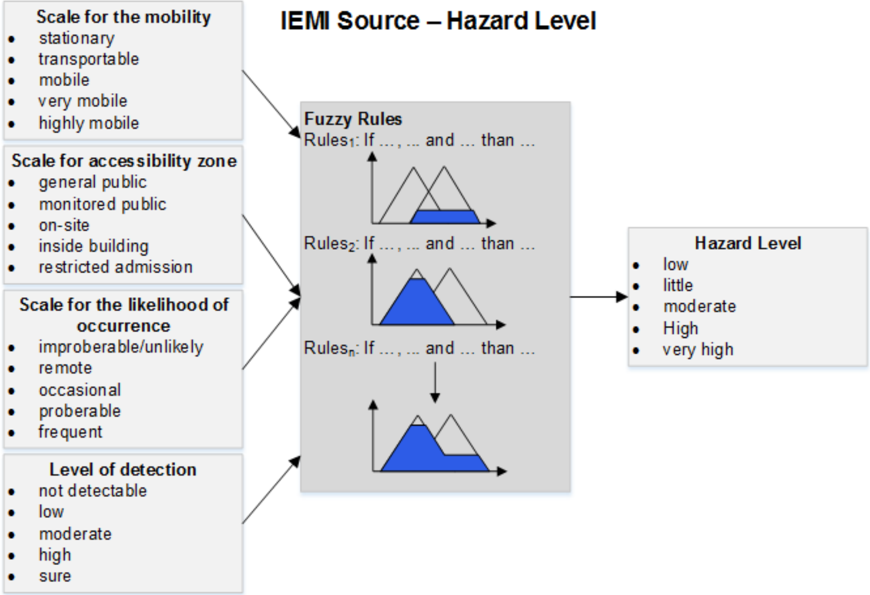


Figure 7 Fuzzy system to analyze the hazard level of an IEMI source.

An area plan for an exemplarily infrastructure with different security levels is introduced in [16] and shown in Fig. 8. The capability of a HPEM source to come close to the victim system is addicted to the mobility and the accessibility level. The higher the access level is, the higher would be the mobility level and smaller the source itself. The size of the source defines the hazard level which is estimated with the fuzzy system in Fig. 7.

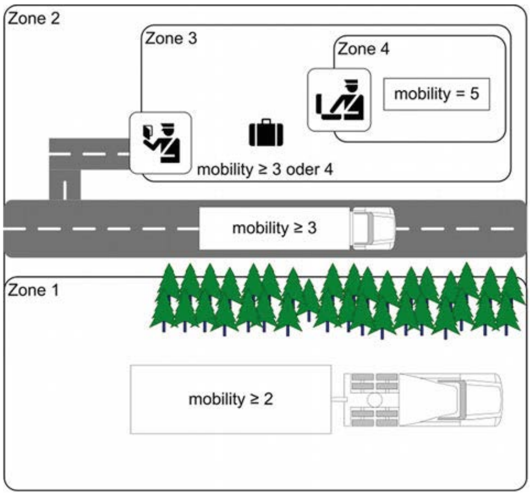


Figure 8 Accessibility zones and needed mobility level by Sabath [16].

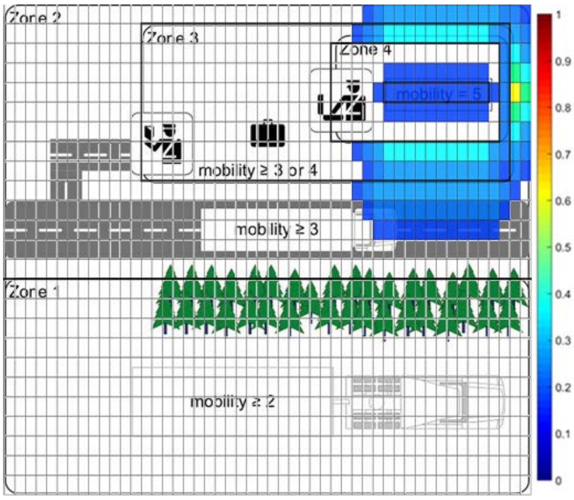


Figure 9 Estimated Risk level of the victim system and the possible localization of the IEMI source.

By combining every fuzzy system for ML, TL, HL, ZoA, TC and the other ones into one system with the vulnerability of the whole system and infrastructure area plan, it is possible to estimate the risk of possible types of HPEM sources in dependency on their location. For the analysing of the area plan in Fig. 8 for places in which a HPEM source could be located to disturb the protected system, the area plan is meshed to rectangle with a fix size of the area. Every rectangle has its limitation which is definite in his mobility and accessibility level. This restrict the possible hazard level in this area. Furthermore, the distance between the centre of every rectangle and the protected system leads to an attenuation of the maximum possible field strength by a factor of $1/r$, in which r is the distance. The obtained field strength and the result for the HL of the HPEM sources lead to an estimation of the risk level for the protected system.

In Fig. 9 is an example shown for a system which is located in the zone with the mobility level five in the upper right corner of the area. The rectangles without a filled colour have nearly a risk level of zero. The risk level has a colour range from dark blue, the level is nearly zero, to dark red, the risk really high for the system. In the right side beside the system (Fig. 9) leads the estimation to a risk level of 0.6 (yellow filled rectangle). The results in Fig. 9 can be used to raise the protection level for intentional electromagnetic attacks.

4 CONCLUSION

The presented approach based on fuzzy systems helps to analyse the risk of a system exposed to IEMI. The advantage of the fuzzy approach is the combining of physical attributes (e.g. BFP, field strength and shielding) with non-physical attributes (e.g. linguistic terms and experts opinions). This risk analysis method also can handle non-precise and uncertain data for the risk estimation. It combines the breakdown behaviour of an electronic system with the infrastructure and the surrounding area and highlighted location in which a HPEM source can be located to harm the protected system. The results can be used to improve the electromagnetic shielding of the system.

REFERENCES

[1] URSI, *URSI resolution on criminal activities using electromagnetic tools*, URSI resolutions adopted at the Toronto general assembly, Minutes of the XXVIth General Assembly of the URSI, 1999.

[2] Bäckström, M., Nordström, B. and Lövstrand, K.G., *Is HPM a threat against the civil society?*, Proceedings of the 27th General Assembly of the URSI, Maastricht, Netherlands, August 2002

[3] Giri, D.V., *Documented Electromagnetic Effects (EME)*, Proceedings of the EU-ROEM 2008, Lausanne, Switzerland, July 2008.

[4] Sabath, F. and Garbe, H., *Risk Potential of Radiated HPEM Environments*, Proceedings of the 2009 IEEE International Symposium on Electromagnetic Compatibility, Austin (TX), USA, August 2009, pp. 226-231,

[5] Peikert, T., Garbe, H. and Potthast, S., *A fuzzy approach for IEMI risk analysis of IT-Systems with respect to transient disturbances*, Electromagnetic Compatibility (EMC), 2015 IEEE International Symposium on, Dresden, 2015, pp. 1077-1082.

[6] Zadeh, L.A:, *Fuzzy sets*, Information and Control, Vol. 8, Issue 3, June 1965, pp. 338-353, doi:10.1016/S0019-9958(65)90241-X

[7] Trilliantinc, *Why We Need a Smart Grid.*, 2013, http://trilliantinc.com/smart-grid

[8] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, *Context Aware Computing for The Internet of Things: A Survey*, in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 414-454, First Quarter 2014. doi:10.1109/SURV.2013.042313.00197

[9] Aliev, R. Az., Fundamentals of the Fuzzy Logic-Based Generalized Theory of Decisions, Springer, Berlin, Germany 2013.

[10] E. Genender, A. Kreth, D. Zamow, H. Garbe, and S. Potthast, *Combination of the failure probability with a random angle of incidence of the radiated interference*, in General Assembly and Scientific Symposium, 2011 XXXth URSI, Aug 2011, pp. 1–4.

[11] Peikert, T., Garbe, H. and Potthast, S., *Fuzzy Based Risk Analysis for IT-System and their Infrastructure*, Electromagnetic Compatibility (EMC), 2016 IEEE International Symposium on, Ottawa, 2016.

[12] Peikert, T., Garbe, H. and Potthast, S.,Electromagnetic Environment and Interference Risk Analysis with a Fuzzy-Logic Approach of a Complex Installation, Adv. Radio Sci, 2016, to be published.

[13] Sabath, F. and Garbe, H., *Assessing the Likelihood of Various Intentional Electromagnetic Environments*, 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), pp. 1083-1088, 2015, doi:10.1109/ISEMC.2015.7256319.

[14] D. V. Giri and F. M. Tesche, *Classification of intentional electromagnetic environments*, IEEE Trans. Electromagn. Compat., vol. 46, no. 3, pp. 322–328, Aug. 2004, DOI:10.1109/TEMC.2004.831819

[15] Sabath, F.; Garbe, H., *Concept of stochastic modeling for High-Power Electromagnetics (HPEM) risk analysis at system level*, 2013 IEEE International Symposium on Electromagnetic Compatibility (EMC), pp.401-406, 5-9 Aug. 2013, doi: 10.1109/ISEMC.2013.6670446

ON DETECTING AND LOCALIZING IEMI SOURCES BY USING MULTIPLE ANTENNA SENSORS

Benjamin Menssen, Felix Burghardt, and Heyno Garbe

{menssen;burghardt;garbe}@geml.uni-hannover.de
Leibniz Universität Hannover, Institute of Electrical Engineering and Measurement
Technology, Appelstr. 9a, 30167 Hannover, Germany

Abstract

Nowadays, a failure due to IEMI is still likely to be undetected. Instead, it may be blamed on faulty hardware or software, especially if the failure is intermittent. It is therefore beneficial to develop IEMI detection systems in order to increase the protection level of so called “critical infrastructures”.

In this work, we want to present an alternative method for localizing an IEMI source. We present an attack scenario that consists of a victim infrastructure represented by a building that is surrounded by a distributed sensor network surrounding the building. The alternative method evaluates the direction of maximum power (DoMP) with an antenna array of directional antennas. The method is tested by simulations and measurements and shows promising accuracy for the localization of IEMI sources.

Keywords: IEMI, Detection, Localization, Antenna array.

1 INTRODUCTION

The vulnerability of electronic equipment to electromagnetic interference is known in the field of electrical engineering for decades. Thus, equipment is well characterized with respect to classic EMC disturbances. However, in recent years, the topic of intentional electromagnetic interference (IEMI) poses an increasing threat to electronic systems due to the increasing availability and expertise on building disruptive sources. The increasing availability of such sources comes in hand with an increasing threat of electromagnetic attacks against critical infrastructures [1]. Hence, the need of reviewing current protection strategies and mitigation philosophies to increase the resilience of critical infrastructures is arising [2].

The European Commission opened a call in the context of the overall FP7 Security Call SEC-2011.2.2-2 in order to address this topic. One of the projects that followed this call was the “STRUCTURES” project, which started in July 2012 and ended in October 2015 [3], [4]. One important outcome from this project was the fact that, up to today, failures due to IEMI may still be blamed on faulty hardware or software. Hence, a task within the project was to develop a detection system to detect, identify, and localize an IEMI attack. As in most common approaches, in that work the time difference of arrival (TDoA) Method was chosen as the localization method [5].

In this work, we are going to present an alternative localization method that has been rejected during the review process of the project. The method uses multiple antenna sensors in order to find the direction of maximum power (DoMP) and triangulate the source location [6]. Hence, the method is based on a sensor network while each single sensor is equipped with an array of directional antennas to obtain the DoMP. Simulations and measurements that we are going to present in the following test and validate the method.

2 IEMI SCENARIO

The threat of intentional electromagnetic attacks has evolved an increasing importance for the protection strategies of critical infrastructures [7]. Hence, it is beneficial to install detection systems to detect, identify, and localize a possible IEMI source.

In order to develop detection systems with respect to IEMI attacks, knowledge about the characteristics of such sources is essential. Sources can be classified by non-technical characteristics as mobility, technological challenge, and threat level [8]. Although sources are more readily available due to the technological progress, high-energy sources that are capable of producing distinct disruptions are still quite immobile [9].

Therefore, we choose an attack scenario that assumes the attacking source to be located outside the victim facility area, which is typically surrounded by a fence (see Fig. 1). Around the building, we propose a network of equally spaced EM sensors.

In this work, for the sake of simplicity, we reduce the description and evaluation to a 2D scenario. Nevertheless, it can be transferred to a 3D scenario.

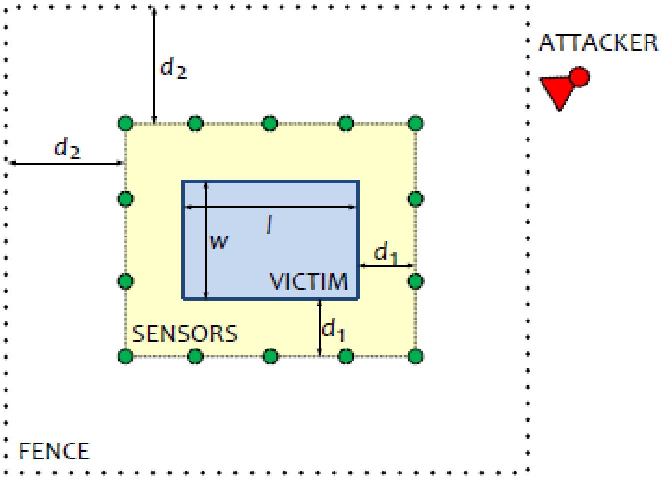


Fig. 1: Scenario illustration of an IEMI attack. The victim equipment is inside a building. A set of distributed EM field sensors and an IEMI source outside the protected area. [5]

3 DIRECTION OF MAXIMUM POWER

The most common localization technique makes use of the time difference of arrival (TDoA) algorithm. However, the TDoA method needs a complex computation system to solve for the source location; especially when performing in real-time. Hence, we are going to present an alternative method, the DoMP method. It makes use of an easier and therefore cheaper computation algorithm whereas it requires directional antennas.

3.1 Basic Method

The basic concept of the DoMP method does an angle of arrival (AoA) estimation based on a simple peak measurement [6]. It uses a sensor network while each sensor location is equipped with an array of directional antennas. Each antenna points into a different direction and thus monitors respectively illuminates a sectorial area. Such an array of horn antennas is exemplarily used in this work and is illustrated in Fig. 2. The corresponding superposition of radiation patterns is depicted in Fig. 3

Due to the fact that the antennas have a distinct main lobe, we can assume that there will always be one antenna in an array that will receive the maximum power. Therefore, this antenna will point into the direction of the source. By using several sensor locations, the source location can be triangulated as depicted in Fig. 4. However, it can be seen that each antenna illuminates a sectorial area. Hence, the source could be located within the complete overlapping area resulting in a very high uncertainty.

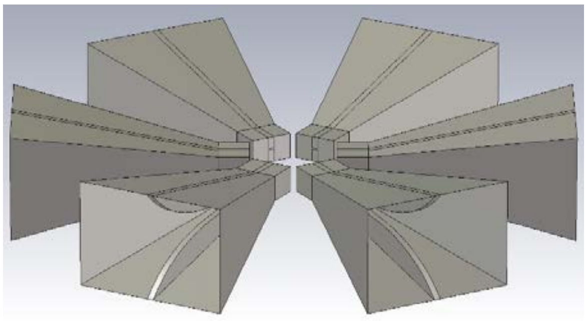


Fig. 2: Illustration of the investigated antenna array of double-ridged horn antennas [10]

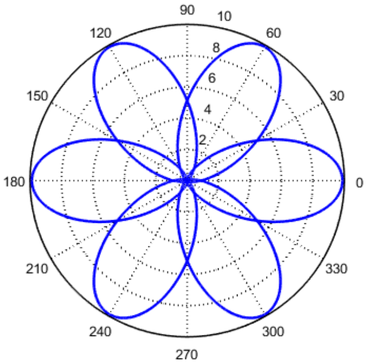


Fig. 3: Radiation pattern of the horn antenna array at f = 2 *GHz*

This uncertainty can be reduced by several factors:

- Redundant sensor locations
- Reducing the beam width of a single antenna
- Increasing the number of antennas at a single sensor location

However, these factors will increase the equipment costs so that we do not gain any advantage with respect to the TDoA method. Furthermore, it is obvious that we reject a lot of information, if we only consider the antenna that receives the maximum power. Hence, the uncertainty should be reduced by adding the information of the antenna that receives the second maximum power. Such a method will be presented in the following section.

3.2 Monopulse Method

The basic method of the DoMP method searches for the direction of the antenna that receives the maximum power. However, this may lead to a high uncertainty due to the fixed orientation of each antenna. It is most likely that the angle of arrival is an angle in between the orientation of two collocated antennas. Hence, it appears useful to also consider the information of the antenna that receives the second maximum power within an array and perform a weighted superposition of their orientations. In a first step, we performed a linear superposition based on the received power, which led to an improvement. Yet, the uncertainty may still be very high because the radiation patterns of

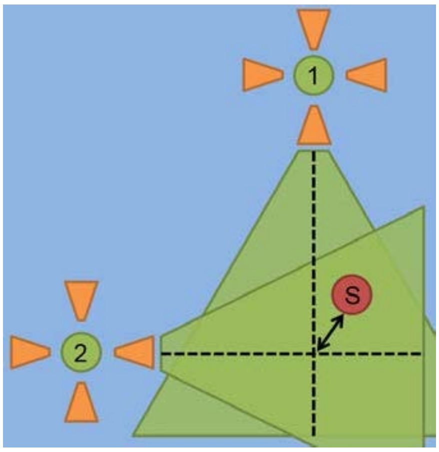


Fig. 4: Sketch of the localization method by the use of multiple antenna sensors

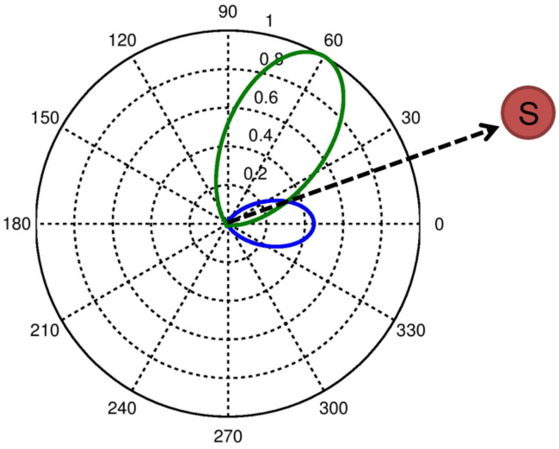


Fig. 5: Illustration of the extension by the monopulse method

the antennas are not linearly dependent on the azimuth angle.

Therefore, we propose to apply the monopulse method [11]. This method considers the radiation patterns for determining the angle of arrival. The basic principle of the method is illustrated in Fig. 5. A first important fact is that the radiation patterns of the collocated antennas need to be overlapping. Depending on the received power, the radiation patterns will be weighted and afterwards, the intersection of the resulting patterns will be determined. Finally, the direction of the intersection represents the estimated direction of the source location. Thus, the source location can be triangulated from several sensor locations.

4 SIMULATIONS

4.1 Analytical analysis

In a first step, we performed analytical simulations where we assumed ideal spherical wave expansion so that the received power is reduced by $1/r^2$ and weighted with the radiation pattern. Fig. 6 shows the result for the linear superposition. As expected, the lines do not cross ideally in one single point. Therefore, the result is calculated by the mean of all intersection points that appear.

Fig. 7 shows the result after applying the monopulse method. It can be seen that the linear superposition leads to a distinct error whereat the monopulse method is capable of determining an almost ideal match of the source location.

4.2 Transient analysis

While the analytical analysis shows promising results, we need to look for a more realistic scenario. In an IEMI scenario, we do not know which equipment the attacker will use. Thus, we do not have knowledge about the signal characteristics. However, the attacker will most likely use transient HPEM signals to overcome the protection mechanisms of the infrastructure.

The transient shape of a signal brings some complications for the proposed localization method. In general, simple antennas do not transmit shape inherently. This means that the radiation pattern of an antenna is varying with the frequency and thus the shape of a signal will be deformed after reception. However, the monopulse method needs one distinct radiation for its analysis.

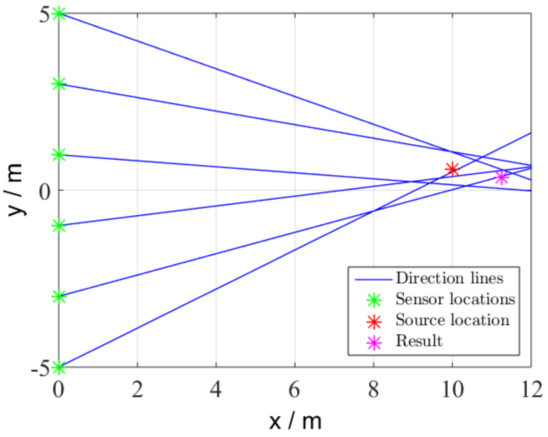


Fig. 6: Result from the analytical simulation with linear superposition

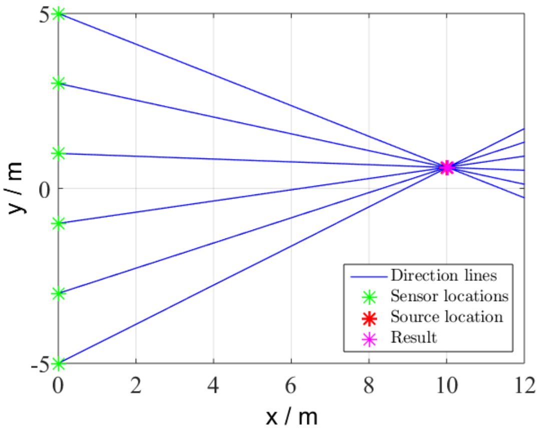


Fig. 7: Result from the analytical simulation with the monopulse method

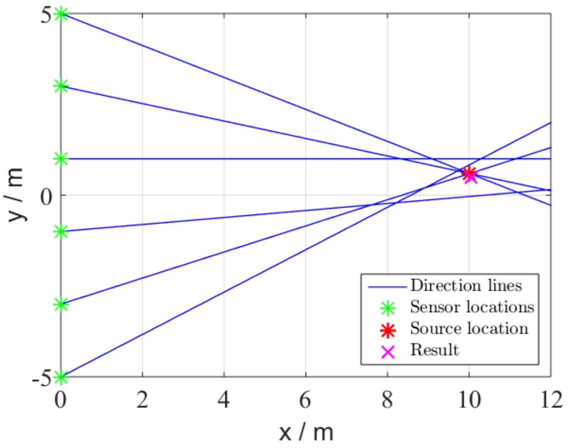


Fig. 8: Result from the transient simulation at f = 3 GHz

Therefore, we propose to use a bandpass with the center frequency corresponding to the desired frequency of the radiation pattern.

Thus, as a next step, we performed numerical simulations with CST Microwave Studio [12] to evaluate the applicability of the method for transient signals. In the simulation scenario, we use six sensor locations each equipped with an array of six horn antennas. The result of the localization algorithm is depicted in Fig. 8. It shows that the error of the source location is in the range of approximately 10 cm. Due to computational restrictions, we could not extend the scenario for bigger distances. However, the proof of concept is given.

5 MEASUREMENTS

After having validated the method by transient simulations, we performed measurements on an open area test site (OATS). Here, we are able to position the source at different distances. We use distances of 10 m, 30 m, and 50 m while the sensor arrays are separated by 5 m. As the source, we use a broadband horn antenna with a PBG3 pulse generator [13]. The PBG3 pulse generator produces high voltage pulses with a double-exponential waveform and thus represents a typical type of source in an IEMI scenario.

In Fig. 9, we present two results of the evaluation for distances of 30 m and 50 m. In both evaluations, the source is centrally positioned (red star) with respect to the five sensor locations (green stars). The result of the localization algorithm is marked as a pink cross. Both figures show a good accordance. The absolute errors are 2,4 m at 30 m distance and 3,4 m at 50 m distance. Hence, the error of the presented method is less than 10 % depending on the distance of the source.

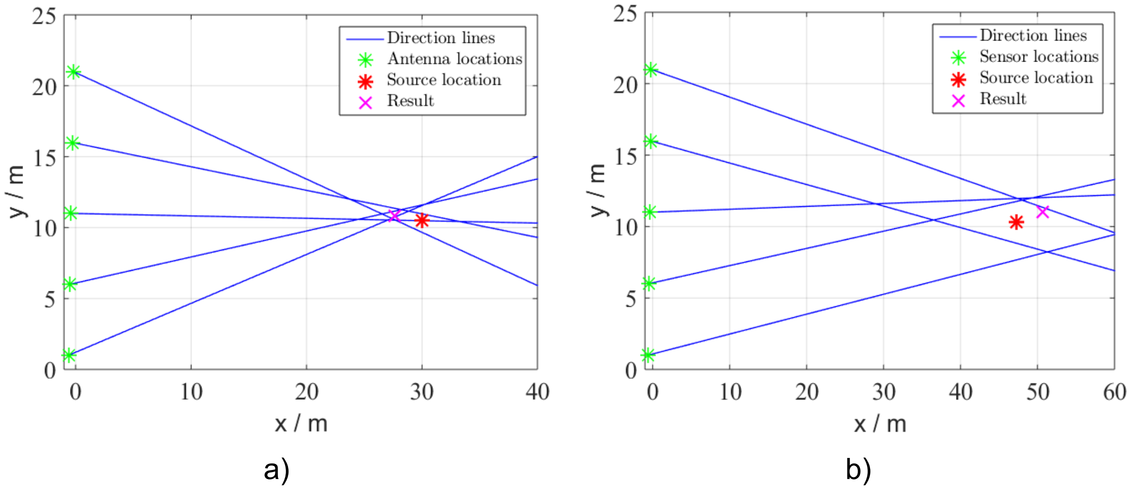


Fig. 9: Localization result of the double-exponential pulse at two different distances: a) 30 m, b) 50 m each evaluated at f = 2 GHz

This is a good result for a first investigation because we did a simple proof of concept. We only used two antennas so that the measurements at the different sensor locations are not performed simultaneously. The distances are measured with a laser distance meter and the orientations of the antennas are approximated with a simple compass. Hence, there are many uncertainties in the setup, which justify the generated errors. We are confident that an accurate positioning and a simultaneous measurement with multiple antennas can reduce the uncertainties.

6 CONCLUSION

In this work, we presented an alternative localization method for the localization of IEMI signals. The method uses antenna arrays to determine the direction of maximum power. We extended the basic algorithm by applying the monopulse method, which considers the radiation patterns of the antennas and interpolates the angle of arrival from two collocated antennas.

We performed transient simulations in CST Microwave Studio in order to investigate the influence of transient, broadband pulses on the non-linear receiving characteristics of antennas. As a result, we propose to use a bandpass filter to match the signal to the desired frequency of the corresponding radiation pattern. The simulations results show a good accordance with small errors of the estimated source location.

For the further validation, we performed measurements on an OATS. The measurements could also proof the concept of the presented method. We achieved errors less than 10 % depending on the distance of the source location, whereat the uncertainties can be justified by the simplicity of the measurement setup.

Finally, the presented method shows promising results so that it may be considered as an alternative localization method. The algorithm appears to be very simple so that the costs of the computation are quite low. Costs for this method are hidden in the antenna equipment since we need to use directional antennas (here: horn antennas). Yet, we see potential for further research on antenna systems to solve this issue.

REFERENCES

[1] F. Sabath, “What can be learned from documented intentional electromagnetic interference (IEMI) attacks?” in General Assembly and Scientific Symposium, 2011 XXXth URSI, Aug 2011, pp. 1–4

[2] URSI resolution on criminal activities using electromagnetic tools, URSI resolutions adopted at the Toronto general assembly, 1999. [Online] Available: http://www.ursi.org/

[3] EU-Project: “STRUCTURES”, Available [Online]: http://www.structures-project.eu

[4] S. van de Beek et al., "The European project STRUCTURES: Challenges and results," 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, 2015, pp. 1095-1100, doi: 10.1109/ISEMC.2015.7256321

[5] M. Stojilović, B. Menssen, I. Flintoft, H. Garbe, J. Dawson and M. Rubinstein, "TDoA-based localisation of radiated IEMI sources," 2014 International Symposium on Electromagnetic Compatibility (EMC Europe), Gothenburg, 2014, pp. 1263-1268, doi: 10.1109/EMCEurope.2014.6931098

[6] B. Zhang and F. Yu, "LSWD: localization scheme for wireless sensor networks using directional antenna" in IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2208-2216, November 2010, doi: 10.1109/TCE.2010.5681092

[7] W. A. Radasky, C. E. Baum and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," in IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 314-321, Aug. 2004, doi: 10.1109/TEMC.2004.831899

[8] F. Sabath and H. Garbe, "Risk potential of radiated HPEM environments," 2009 IEEE International Symposium on Electromagnetic Compatibility, Austin, TX, 2009, pp. 226-231, doi: 10.1109/ISEMC.2009.5284566

[9] G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein and R. Cherkaoui, "Overview of IEMI conducted and radiated sources: Characteristics and trends," 2013 International Symposium on Electromagnetic Compatibility (EMC EUROPE), Brugge, 2013, pp. 24-28

[10] Schwarzbeck - Mess Elektronik OHG, Schwarzbeck BBHA 9120 B,
Available [Online]: http://www. http://schwarzbeck.de/Datenblatt/k9120b.pdf

[11] S. M. Sherman und D. K. Barton, Monopulse Principles and Techniques. Artech House, 2011

[12] CST - Computer Simulation Technology AG, CST Microwave Studio,
Available [Online]: http://www.cst.com/

[13] Kentech Instruments Ltd., PBG High Voltage Pulse Sources,
Availble [Online]: http://www.kentech.co.uk/PDF/PBG3_flyer.pdf

DETECTION, IDENTIFICATION, AND LOCALIZATION OF ELECTROMAGNETIC ATTACKS WITH A MODERATE-COST SYSTEM

W. Hirschi[1], N. Mora[1], M. Stojilović[2], M. Rubinstein[2]

[1] *werner.hirschi@montena.com, nicolas.mora@montena.com*
Montena technology SA, Route de Montena 89, 1728 Rossens (Switzerland)

[2] *mirjana.stojilovic@heig-vd.ch, marcos.rubinstein@heig-vd.ch*
University of Applied Sciences and Arts Western Switzerland, Route de Cheseaux 1,
1401 Yverdon-les-Bains (Switzerland)

Abstract

Intentional electromagnetic interference (IEMI) attacks on critical infrastructures have raised significant attention during the last two decades. Given the low probability of a successful attack during the initial attempts, there is a strong interest in installing warning and diagnostic tools for triggering safety shutdown procedures and supporting the search for and elimination of IEMI sources.

This paper presents a concept of a detection, identification, and localization system that uses a novel approach for measuring the characteristics of broadband and high dynamic-range IEMI signals with inexpensive, off-the-shelf components. This work was completed in the framework of the European research project STRUCTURES (Strategies for The impRovement of critical infrastrUCTUres Resilience to Electromagnetic attackS).

Keywords: IEMI, Identification, Localization, STRUCTURES, research project.

1 INTRODUCTION

An IEMI threat is characterized by a very large frequency and dynamic range. Electronics dealing with signals having such characteristics are generally expensive.

The system for identification and localization of IEMI, described here, includes a dedicated set of functionalities allowing it to collect automatically all required information at the needed quality level and at affordable costs:

- Automatic adjustment of the signal levels.
- A peak-hold circuit for measuring the IEMI signal amplitude. High bandwidth and accuracy are achieved by full characterization of the circuit imperfections and software algorithms for correcting them.
- A fast comparator for one-bit digitization and pre-selecting the waveform type.
- Frequency analysis and waveform analysis using the multi-Gigabit/s processing rates provided by a field-programmable gate array (FPGA) tailored for the telecommunication mass-market.

2 CHARACTERISTICS OF IEMI

Potential IEMI sources exist in a large variety of types [1], [2] and they represent threats at different degrees of severity. The great majority of IEMI interferences can be classified into the following basic waveforms: single pulse, oscillatory, sinusoidal wave or bursts of sinusoidal waves. The CW frequencies or the cutoff frequencies resulting from the fast rise times in the waveforms cover the range from 100 MHz to 15 GHz. State of the art sources produce peak field strengths reaching up to 350 kV/m at 15 m.

3 RISK ASSESMENT

Past experience with IEMI on electronic systems has shown that it takes a certain time to trigger significant effects on the target. Therefore, from the point of view of the infrastructure under attack, there is an available timeframe during which the IEMI is perceptible, alarms can be set and safety shutdown procedures can be initiated. In parallel, identification and localization algorithms can be run to locate and disable the attacker.

To inflict damage, IEMI antennas must be directive. An attacker must therefore find optimum orientation e.g. the one that allows high energy levels to couple to the sensitive links or systems in the victim infrastructure. The success of an attack is also strongly dependent on the frequency. Maximum impact is achieved when the frequency of the IEMI signal corresponds to the resonance frequencies of the wirings or circuits of the victim infrastructure.

From the point of view of the protection of an infrastructure, identification of the type of source being used allows to estimate the attacker's resources used, in order to

- get an idea of the size of equipment to search for

and

- be able to establish an appreciation of the dangerousness of the attack.

These facts summarize the motivation that led to the formulation of a research project for the design of a system for the processing of IEMI attacks.

4 SYSTEM ARCHITECTURE

The system performs the following three functions: detection, identification and localization of IEMI attacks.

Fig. 1 shows the architecture chosen for the detection and identification. We will refer to it as a sensor chain that comprises an acquisitions chain (shown in the larger, red dashed rectangle in Fig. 1) and a processing unit. The sensing chain consists thus of the field sensor, a balun, tree functional blocs for identification (signal conditioning, amplitude measurement and single bit digitalization) and the processing unit. An external server is used to derive the location and the type of the IEMI source. Also shown in the figure is an optional high-frequency oscilloscope used to check the attack waveforms during commissioning or in case of need for more detailed analysis.

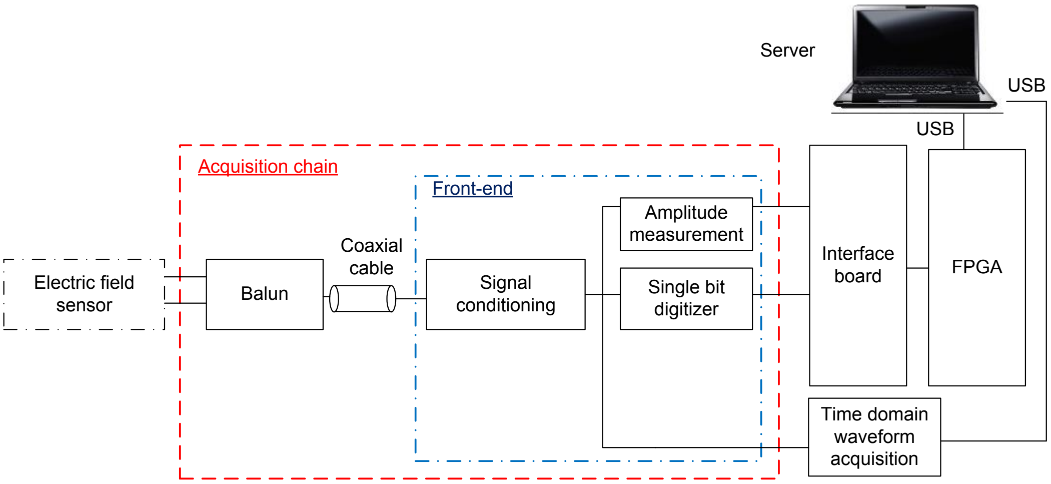


Fig. 1 Architecture of a sensor chain with the functional blocs for identification.

Localization is performed by creating a network of sensor chains and applying the time difference of arrival (TDOA) method (see Fig. 2) [3].

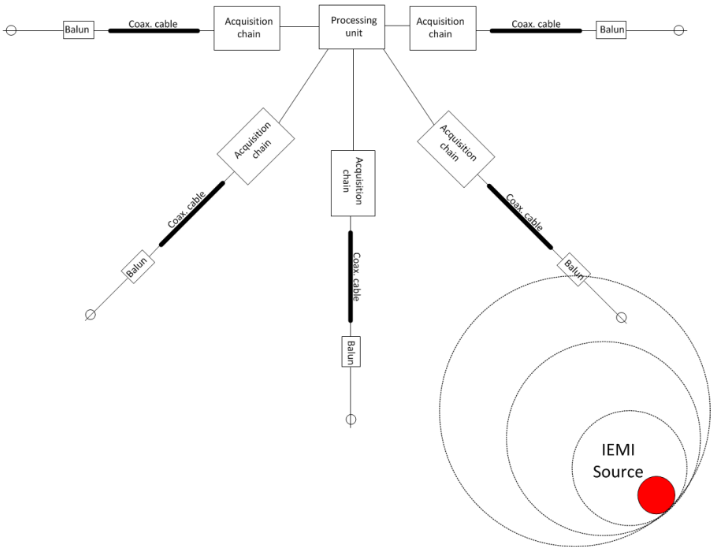


Fig. 2 System architecture for localization.

5 FUNCTIONALITIES AND DESIGN

5.1 Detection

A detailed analysis of existing and expected future sensors has shown that derivative sensors (D-dot for the electric field -see Fig. 3- or B-Dot sensors for the magnetic field [4]) that are already well established in the HPEM community fit well the requirements of IEMI sensing.

These types of sensors cover a very large frequency range, as shown in Fig. 3. They do not exhibit the frequency dependent phase shifts introduced by conventional antennas. The robustness with respect to phase changes is a condition for the proper detection and processing of pulse signals in the time domain. The D-dot sensor also has a low sensitivity, which is an advantage regarding the expected high field strengths. Lake of sensitivity at low frequencies is compensated by amplification.

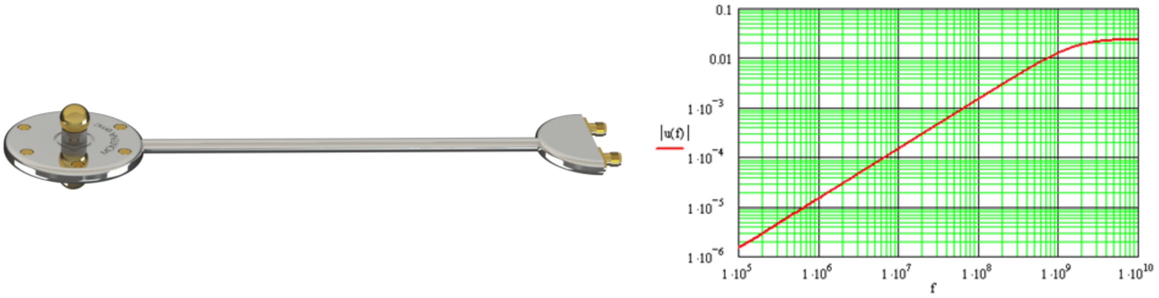


Fig. 3 Derivative sensor for electric free field and its response (Output voltage / V/m).

5.2 Signal conditioning

The D-dot sensor has an output signal that is proportional to the frequency. When dealing with pulse fields, this implies that faster rise times (high field derivatives) produce higher output voltages.

Therefore, the system requires a high dynamic range. An estimation performed with the characteristics of the state of the art sources having cutoff frequencies ranging from 100 MHz to 15 GHz gives a ratio of about 120 dB between the two extremes of the expected field derivatives.

In addition, the ratio between the minimum and the maximum expected level also needs to be considered. Past experience in the EMC community [5] shows that pulsed electric fields of 1 kV/m to 2 kV/m can already disturb or damage electronic devices. Therefore, it was decided to set the minimum field to 100 V/m. This value includes a safety margin and nevertheless allows avoiding a large fraction of false alarms resulting from environmental EMI.

Fig. 4 summarizes the expected field strengths of the state of the art sources. The highest expected value is about 1 MV/m. From these considerations, the ratio between the minimum and the maximum field strength is about 80 dB.

The presented values of 120 dB and 80 dB have to be added arithmetically in order to define the required dynamic range. The design of electronics with such dynamic range is very difficult from a technical point of view and, at this time, prohibitively expensive.

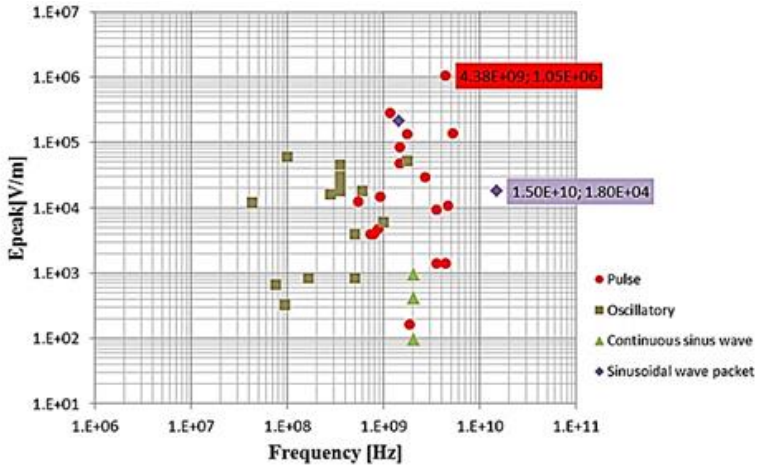


Fig. 4 Expected peak electric field at 5m distance from the state of the art sources. The frequency axis represents either the self-oscillatory frequency or the upper cut-off frequency of the source.

It has been shown during the European FP7 STRUCTURES project that the frequency dependent attenuation of the relatively long coaxial sensor cable can be used for reducing the required dynamic range. Notice that this attenuation can be well characterized and compensated by computation in order to not lose signal information.

5.3 Amplitude measurement

An important parameter for the estimation of the danger represented by an attack is the peak amplitude of the field strength. The measurement of this quantity is often achieved by a so-called peak-hold circuit (see Fig. 5). The peak-hold in that figure works by charging a capacitor up to the peak voltage of the input signal and digitizing this amplitude before a resistor discharges the capacitor, to prepare the circuit for the next measurement. This procedure becomes less accurate when measuring very fast and short pulses like the ones expected from IEMI. Therefore, a full characterization of the behavior of the peak-hold circuit over large frequency and rise time ranges was performed for further correction by software.

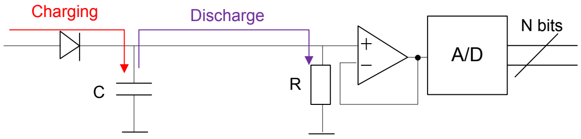


Fig. 5 Peak hold circuit for the measurement of the peak field strength.

The peak hold circuit designed for the STRUCTURES demonstrator is able to measure the peak amplitudes of pulses with rise times of about 300 ps with an acceptable accuracy.

5.4 Single bit digitizing

Digitizing high frequency signals or very fast pulses is still expensive, especially for multiple channels. The challenge was to find another way to obtain the required information, namely, the type of waveform, the frequency or the rise time and the time of arrival. We therefore proposed to use a fast (but low-cost) comparator as a single bit digitizer. This allows keeping all the required temporal information of the IEMI signals.

Fig. 6 shows the use of the comparator for identifying the wave shape. The three square signals allow differentiating between a single pulse, a sinusoidal wave and a damped sine-wave.

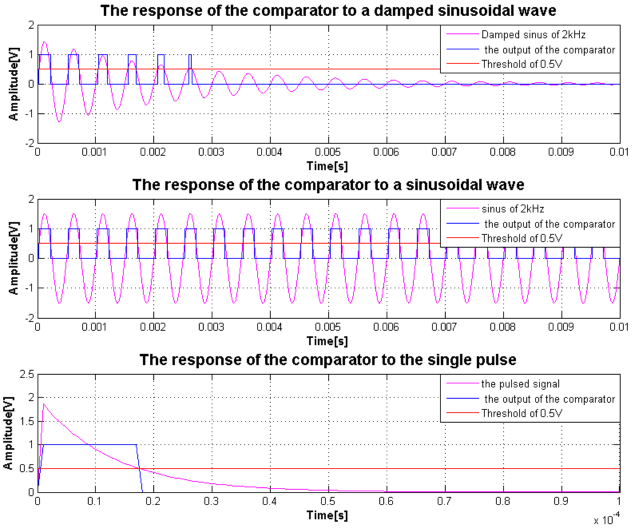
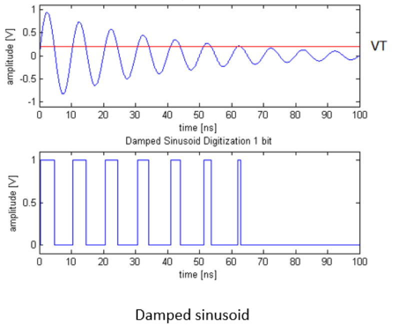


Fig. 6 Comparator output for different wave shapes.

Changing the threshold voltage of the comparator allows estimating the decay time and the fundamental frequency of an oscillatory wave [6] (see Fig. 7).



$$t_{Start,m} = m / f$$

$$t_{End,m} = (2m-1) / 2f$$

$$e^{-t/\tau} \geq V_T$$

$$t \leq -\tau \ln(V_T)$$

$$\frac{2m-1}{2f} \leq -\tau \ln(V_T)$$

$$\boxed{\tau \geq -\frac{2m-1}{2f \ln(V_T)}}$$

$$x(t) = \sin(2\pi ft)e^{-t/\tau}$$

$$\sin(2\pi ft)e^{-t/\tau} = V_T$$

$$f = \frac{n-1}{2\Delta t} \quad \text{if} \quad n>1$$

$$\boxed{f \approx \frac{p-1}{2\Delta t_{n,V_T \neq 0}}}$$

Fig. 7 Estimation of the main characteristics of an oscillatory wave.

5.5 Processing of the comparator output signal

In order to process the output of the comparator, the pulse duration and the period between pulses is measured with an FPGA gigabit transceiver. With such transceivers, at a clock frequency of 12.5 GHz, it is possible to get a time resolution of 80 ps at lower cost than with traditional sampling schemes.

After having triggered on an IEMI event, the control unit adjusts the attenuators and the thresholds of the single bit digitizers. It also provides communication and the data exchange platform with the local server that provides an interface to the users. The identification and the localization of the electromagnetic attack are performed through the seven steps described in Fig. 8.

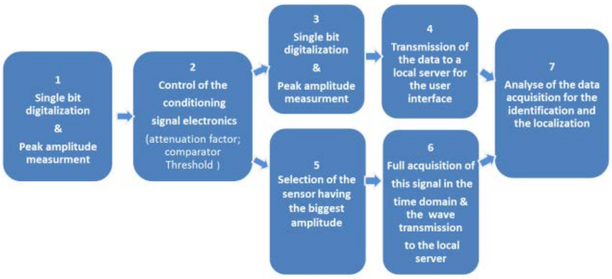

1
Single bit digitalization
&
Peak amplitude measurment
2
Control of the conditioning signal electronics
(attenuation factor; comparator Threshold)
3
Single bit digitalization
&
Peak amplitude measurment
4
Transmission of the data to a local server for the user interface
5
Selection of the sensor having the biggest amplitude
6
Full acquisition of this signal in the time domain & the wave transmission to the local server
7
Analyse of the data acquisition for the identification and the localization

Fig. 8 Description of the steps to follow for identification and localization of IEMI sources.

5.6 Localization algorithm

The following localization methods were analyzed [3], [7]–[10] [11]:

- Magnetic Direction Finding (MDF),
- Time Difference of Arrival (TDoA),
- Time Reversal (TR),
- Power Amplitude (PA),
- Direction of Maximum Power (DoMP),
- Rotating Antenna Pattern (RAP) ,
- Doppler direction finding (DDF), and
- Direction Finding by Interferometry (DFI).

Based on detailed analyses and simulations, the TDoA method was selected as the most appropriate one [11].

The sensitivity of this method depends on:

- synchronization between sensors (jitter),
- resolution of the sampling time,
- distance between the sensors, and
- relative position of the sensors and the source.

The two first factors can be managed by using appropriate hardware. The third can be readily optimized for a given infrastructure and its optimization leads to improvement in the first two factors. The fourth point is imposed by the possible expected location of the IEMI attacker antenna.

The minimum number of sensors was evaluated to be 5.

6 IMPLEMENTED DEMONSTRATOR

Fig. 9 shows a picture of the developed sensor board containing the signal conditioning, the amplitude measurement (peak hold) and the single bit digitizer (comparator). The threshold voltage control with a digital to analogue converter (DAC) is also built in.

The complete system box containing five sensor boards and a Xilinx Kintex 7 FPGA board with its five GTX transceivers is presented on Fig. 10.

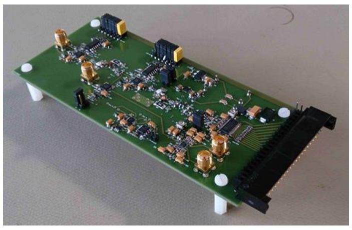


Fig. 9 Sensor board.

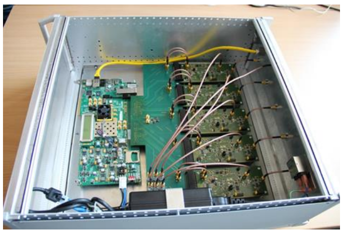


Fig. 10 Full system.

The sensor boards are connected to the FPGA-board through an interface board, which was especially designed for this purpose with 50 Ohm-paths having all the same length in order not to introduce transmission time differences between channels.

7 TEST RESULTS

7.1 Amplitude measurement

Fig. 11 presents an example of an amplitude measurement with the designed peak-hold circuit. The rise time of the detected pulses is less than 4 ns and the repetition frequency is 1 MHz. The peak measurement error is smaller than 2 %.

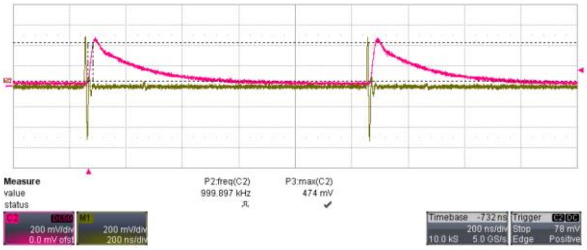


Fig. 11 Voltage at the peak hold input (green curve) and its output (pink curve).

7.2 Single bit digitization

The response of the demonstrator's comparator to a pulsed signal with FWHM of 1 ns is presented in Fig. 12. The flanks of the signals are limited to about 300 ps. This is due to the bandwidth limitation of the oscilloscope (1 GHz). The comparator is able to detect rise times down to 35 ps.

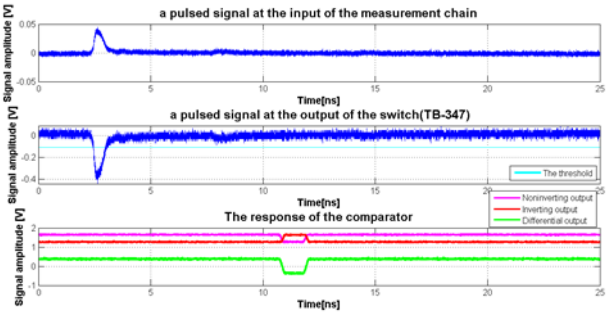


Fig. 12 Single bit digitalization in the case of a short pulse.

7.3 Detection with a real IEMI source

Tests were performed with a mobile HPEM case (see Fig. 13) at the Swiss Federal Office for Defence Procurement - Armasuisse - in Spiez, to check the ability of the STRUCTURES demonstrator system to detect IEMI. The HPEM case radiates oscillatory waveforms with a ringing frequency of a few hundred MHz.

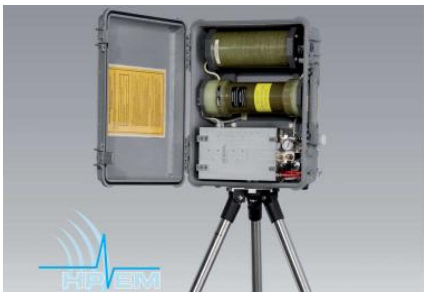


Fig. 13 HPEM case from Diehl.

Fig. 14 shows an IEMI single pulse (lowest curve of the graphic with indication of field strength scale). The difference between the two comparator outputs (two top curves) is represented with the third curve (f1). The non-square waveform of the comparator signals is due to the fact that the oscilloscope input impedances were not perfectly matched.

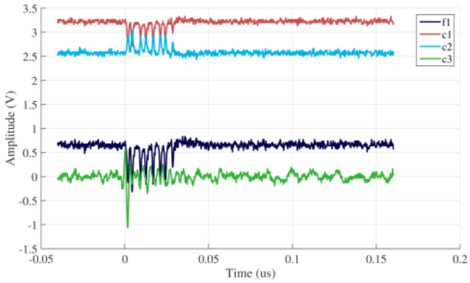


Fig. 14 Measured field pulse and comparator signals.

The proof of the hardware concept was well established with the above result.

7.4 Localization

Localization tests were performed in the perimeter of the Montena facility, which is constituted of metallic walls (see Fig. 15). There is also a metallic fence around the estate. Due to the expected reflections, this configuration represents a problematic but realistic case.

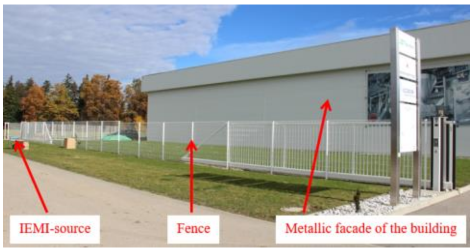


Fig. 15 Location of the localization tests.

A simple IEMI source was placed outside the fence, at a distance of 5 m (see Fig. 16).

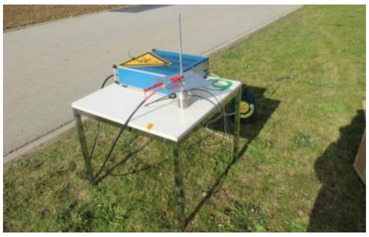


Fig. 16 Simple IEMI source.

Five D-dot sensors were placed on cardboard boxes and distributed in different configurations between the metallic wall of the building and the metallic fence (see Fig. 17).

The localization tests were performed by detecting the time of arrival with oscilloscopes. The TDOA was retrieved with the oscilloscope cursors and introduced manually into the software for computing the localization.

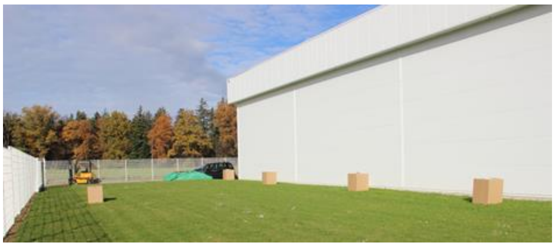
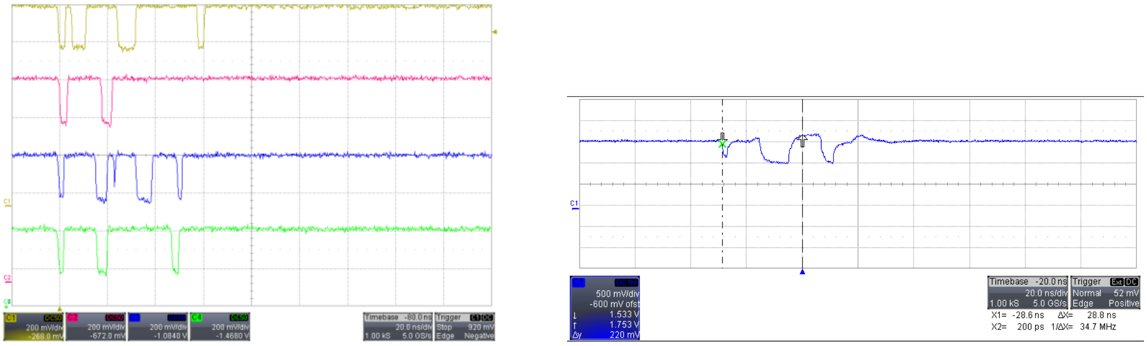


Fig. 17 Five sensors placed on cardboard boxes.

Fig. 18 show the comparator signals of the five sensor channels after an IEMI event. The waveforms are relatively similar; the differences are due to the fact that the received signals do not have the same amplitude. Therefore, the comparator outputs cannot be identical. Nevertheless, the captured signals are good enough for measuring the time delays and applying them to the localization algorithm.



C1 DC50 200 mV/div -268.0 mV
C2 DC50 200 mV/div -672.0 mV
C3 DC50 200 mV/div -1.0840 V
C4 DC50 200 mV/div -1.4680 V
Timebase -80.0 ns 20.0 ns/div 1.00 kS 5.0 GS/s
Trigger C1 DC Stop 920 mV Edge Negative

C1 DC1M 500 mV/div -600 mV ofst ↓ 1.533 V ↑ 1.753 V Δy 220 mV
Timebase -20.0 ns 20.0 ns/div 1.00 kS 5.0 GS/s
Trigger Ext DC Normal 52 mV Edge Positive
X1= -28.6 ns ΔX= 28.8 ns
X2= 200 ps 1/ΔX= 34.7 MHz

Fig. 18 Example of signals captured from one IEMI event on the 5 sensors.

The localization algorithm requires the data of the sensor topology for its computation. Fig. 19 presents the topology of the sensors (small stars), the real position of the IEMI source (bigger star) and of its computed localization (circle).

Fig. 20 shows another distribution of sensors. One of them was placed besides the building. Even under these conditions, the derived and the actual localizations were in relatively good agreement.

Future efforts will concentrate on:

- controlling the gain and threshold level adjustment automatically in order to get comparable signals on every sensor chain and
- improving the localization accuracy.

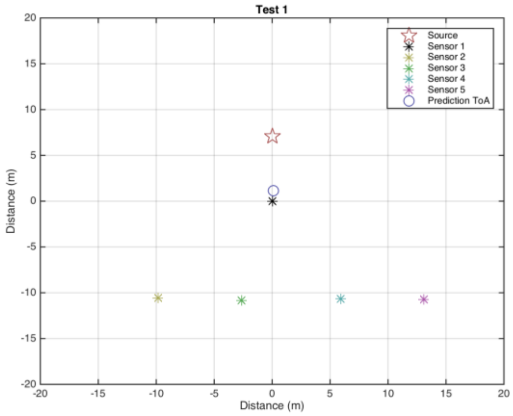


Fig. 19 Results with sensor topology Nr. 1.

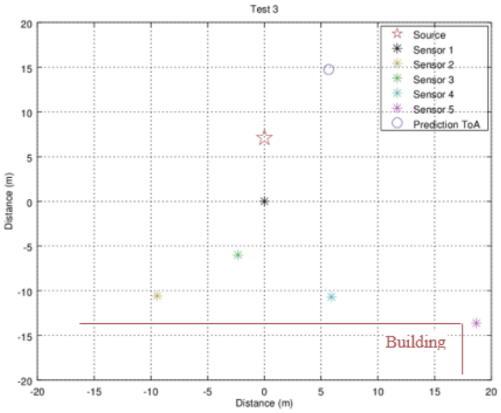


Fig. 20 Results with one sensor besides the building.

8 CONCLUSION

IEMI threats cover a very wide frequency range and require a large dynamic amplitude range. These two parameters usually make electronics for detection and processing expensive. The IEMI identification and localization demonstrator developed in the framework of the European FP7 research project “STRUCTURES”, uses off-the-shelf components for evaluating the key parameters of an attack.

Instead of digitizing the detected signals in real time at very high sampling speed and digitization resolution, the system measures the amplitude, the wave shape, the frequency and the repetition frequency with a peak hold and a fast comparator circuit. The processing of the comparator output signal is performed with a Gigabit-Transceiver and an FPGA-circuit designed for the high speed data transmission mass market.

Operating multiple input channels with such hardware concept allows the localization of IEMI attacks by applying the Time Difference of Arrival method.

Tests realized with this demonstrator have allowed establishing the proof of concept. Even if the physical characteristics of the threat are extreme, IEMI detection and analysis do not need to be expensive. With the proposed approach, a system with five channels and the software for identification and localization should become affordable.

REFERENCES

[1] G. Lugrin, N. Mora, S. Sliman, F. Rachidi, M. Rubinstein, and R. Cherkaoui, “Overview of IEMI conducted and radiated sources: Characteristics and trends,” presented at the Electromagnetic Compatibility (EMC EUROPE), 2013 International Symposium on, 2013, pp. 24–28.

[2] N. Mora, F. Vega, G. Lugrin, F. Rachidi, and M. Rubinstein, “Study and Classification of Potential IEMI Sources,” *System Design and Assessment Notes, Note 41*, 2014.

[3] Y. Tian, A. Tatematsu, K. Tanabe, and K. Miyajima, “Development of Locating System of Pulsed Electromagnetic Interference Source Based on Advanced TDOA Estimation Method,” IEEE Transactions on Electromagnetic Compatibility, vol. 56, no. 6, pp. 1326–1334, Dec. 2014.

[4] C. E. Baum, E. L. Breen, J. C. Giles, J. O’Nelll, and G. D. Sower, “Sensors for Electromagnetic Pulse Measurements Both Inside and Away from Nuclear Source Regions,” IEEE Transactions on Electromagnetic Compatibility, vol. EMC-20, no. 1, pp. 22–35, Feb. 1978.

[5] W. A. Radasky, C. E. Baum, and M. W. Wik, “Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI),” Electromagnetic Compatibility, IEEE Transactions on, vol. 46, pp. 314–321, 2004.

[6] D. Recordon, M. Rubinstein, M. Stojilovic, N. Mora, G. Lugrin, F. Rachidi, L. Rouiller, W. Hirschi, and S. Sliman, “A comparator-based technique for identification of intentional electromagnetic interference attacks,” Sep. 2014.

[7] E. Jacobs and E. W. Ralston, “Ambiguity Resolution in Interferometry,” IEEE Transactions on Aerospace and Electronic Systems, vol. AES-17, no. 6, pp. 766–780, Nov. 1981.

[8] R. B. Dybdal, “Monopulse Resolution of Interferometric Ambiguities,” IEEE Transactions on Aerospace and Electronic Systems, vol. AES-22, no. 2, pp. 177–183, Mar. 1986.

[9] S. V. Schell and W. A. Gardner, “18 High-resolution direction finding,” vol. 10, B.-H. of Statistics, Ed. Elsevier, 1993, pp. 755–817.

[10] “An FPGA Implementation Feasibility Study of the Correlative Interferometer Direction Finding Algorithm - Part 1: Algorithm Review | Nutaq | Nutaq.” [Online].

[11] M. Stojilovi’c, B. Menssen, I. Flintoft, H. Garbe, J. Dawson, and M. Rubinstein, “TDoA-based localisation of radiated IEMI sources,” Sep. 2014.

HPEM VULNERABILITY OF SUBSTATION CONTROL SYSTEMS AS COMPONENTS OF THE SMART GRID

Marian Lanzrath[1], Michael Suhrke[2], Thorsten Pusch[3], Christian Adami[4], Michael Joester[5]

[1] *marian.lanzrath@int.fraunhofer.de*
[2] *michael.suhrke@int.fraunhofer.de*
[3] *thorsten.pusch@int.fraunhofer.de*
[4] *christian.adami@int.fraunhofer.de*
[5] *michael.joester@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT
Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

Nowadays, sectors like trade, mobility, health care or even public policy do highly depend on the power grid. Furthermore, there is a trend to move the electrical energy generation from central power plants towards spread out renewable energies. To manage their fluctuating production, the former demand-based control system has to be replaced by a supply-fitted consumption system. The additional electronics integrated into the power grid potentially raises its susceptibility to intentional electromagnetic interference (IEMI). Initial tests with the Smart Meter device category revealed a high susceptibility to High Power Electromagnetic (HPEM) interferences in the whole tested frequency range. In order to probe components more critical to grid stability, we are expanding our research to a higher hierarchical level – the substation control systems. These critical devices revealed a lower susceptibility than the Smart Meters, but the still occurring failures have a greater impact on the grid. The application of different test methods served the attempt to identify coupling paths into the configuration under test.

Keywords: Smart Grid, HPEM, IEMI, Critical Infrastructure, Vulnerability

1 INTRODUCTION

The Smart Grid as one of the most important critical infrastructures is an enhancement of the present power grid. Being supplied with electricity without interruption is a common good deeply rooted in modern society. A lot of activities in public life, e.g. communication, trade, mobility, banking business or even health care, are based on IT infrastructure and hence rely on electricity. This increasing addiction increases the need of a reliable energy supply. These days, the energy sector is in a rebuilding phase, the trend steps back from large central power plants, which use limited fossil fuels, and moves towards a spread out generation with renewable energies [1]. One emerging problem with introducing renewable energy resources lies in the energy production now fluctuating, which requires a paradigm change in the control system. It has to be migrated from a demand-based to a supply-oriented approach. Hence ensuring stable energy supply is one of the most challenging tasks for the future.

Within concept of the Smart Grid the power grid has an associated communication network to handle continuous real-time data communications between the connected devices, e.g. Smart Meters, smart actuators, power management systems or renewable energy generators. This is necessary to collect real-time grid condition data to manage the power flow properly inside the grid without overloading any components. As a flipside of introducing additional electronic devices for grid management, these might also be considered as potential gateways for manipulation and criminal activities aiming at interrupting the power supply. In the last few years, various types of electronic devices were investigated regarding their susceptibility to HPEM attacks. The results show that they often have a high susceptibility with various kinds of error patterns [2-5]. As argued by Radasky et al., one potential threat to the power grid and also the Smart Grid is such an HPEM attack which disturbs attached computers and electronic devices [6, 7]. For the determination of the power grid's HPEM vulnerability, it is necessary to get an overview of device reactions and field strengths required for disturbances. Some insight regarding accessibility of devices and countermeasures presently installed is needed as well.

Initial investigations were performed focussing on Smart Meters as easily accessible electronic devices of the lowest hierarchical level applied in the power grid [8]. The meters revealed a very high susceptibility against HPEM disturbances during the tests, even with severe outages, but the failure of Smart Meters even in greater numbers will not result in serious consequences for the power grid. More important is the question if critical devices installed in the grid display similar vulnerabilities and error patterns as the Smart Meter devices which will result in a greater impact for the grid. Potential outages of control devices could be malfunctions, communication or functionality losses. Based on the fact that the control centre must be able to remotely control the power switches at all times, these failures might possess a major influence on the grid.

This paper presents susceptibility tests with Smart Grid electronic devices, adding upon previous research. In the following section the Devices Under Test (DUT) as well as the test setup is introduced. The next section presents the test results gained with different coupling methods and performed both on system and component level in order to identify coupling paths. Finally, we put forward our conclusion that despite their lower vulnerability compared to end user devices malfunctions of substation control units may have serious consequences for Smart Grid functionality.

2 MEASUREMENT SETUP

2.1 Devices Under Test

Subject under investigation were components with critical functionalities inside the power grid. The attention was focussed on electronic devices deployed in substations. The first device was a power switch protection device which has the task to secure the power switch and power lines from overloads. The second component was a supervisory control device which establishes a data communication link to the control centre. This connection allows the control centre to remotely control the power switch for grid management or safety purposes. A malfunction of these devices could result in an unwanted shutdown of the power switch, which means a blackout for the attached consumers. Furthermore, it is conceivable that the devices could lose their data connection whereupon critical commands or data cannot be executed or transmitted.

2.2 Test Setup and Resources

The tests were performed at the Fraunhofer INT HPEM test facility which offers several test environments. Available is one BCI test site (Bulk Current Injection) operational within a frequency range from 10 kHz to 1 GHz. Furthermore, there is an open TEM (Transverse Electromagnetic) waveguide operational between 1 MHz to 8 GHz. Both environments are driven with high power sources generating maximum field strengths of several kV/m within the waveguide. One special test procedure for determining the threshold levels of failures at a single frequency is the ramp test. During this procedure the generator's output power is steadily increased until maximum output is reached. Device failures may occur while the ramp is running whereas the specific threshold levels and error patterns are recorded as test results. In our facility the applied disturbance signal with a fixed frequency for each run is standardly superimposed by a pulse modulation with 1 kHz repetition frequency and 1µs pulse width. Alongside with the determination of the coupling path the influence of different pulse modulation parameters was investigated. For these tests the pulse modulation parameters were set to different arbitrary combinations with repetition frequencies between 0.1-10 kHz and pulse widths between 0.4-10 µs. The limitation was a peak duty-cycle value of 0.1%.

The test setup for the investigation was designed according to the ISO 11452-2 standard. This standard offers the possibility to perform tests with both the BCI method and the TEM waveguide using one single setup. The devices and the wiring loom were installed on a base plate to ensure high mobility and data reproducibility during the campaign. A suitable monitoring system for each susceptibility test was required to allow the operator to capture all failures occurring during the tests. One part was a video monitoring system with four cameras used to monitor the led indicators and displays integrated into the devices, but also to observe the indicators connected to the emulated power switch. In addition for real-time data analysis a suitable software was used which established a data connection to the protection device. The software was running on a server pc outside the test facility, it offered the possibility to log all sensor and actuator events as well as measurement data in a specific log file.

3 SUSCEPTIBILITY TESTS

The result plots display the frequency on the X-axis in MHz and the Y-axis shows the field strength or current in arbitrary units. Color-coded in light red is the range between minimum and maximum field strength tested according to the ramp function. The vertical indicators above the X-axis indicate the respective test frequencies.

3.1 BCI Tests

First tests were performed in the frequency range between 140-1000 MHz to investigate the conducted HPEM susceptibility of the DUT using the BCI method. Figure 1 shows the test setup at the BCI test site with the BCI coupling device attached to the wiring loom at a distance of 15 cm to the protection device.

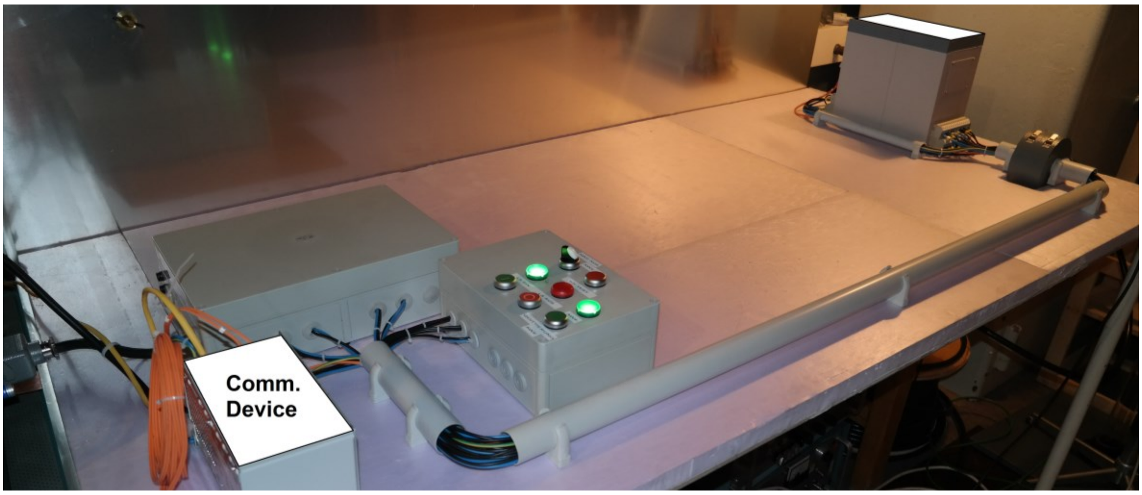


Figure 1: BCI test-setup

The following Figure 2 displays the result plot of the susceptibility test using the BCI method. The DUT shows high interference immunities, almost all disturbances were detected in the frequency range between 140-300 MHz with high outage threshold values. Most of the failures were caused to the communication device, one common effect was the temporary disturbance of the device while the data communication between protection device and server was still up. The few detected failures of the protection device were more serious, typical issues were ongoing disturbances of the device until it was restarted or reconfigured by the operator. The worst failure detected was the hang-up of the protection device which caused a total functionality loss until it was restarted. In this case, the data communication with the server was terminated and the overload protection procedure for the grid components was shut down as well.

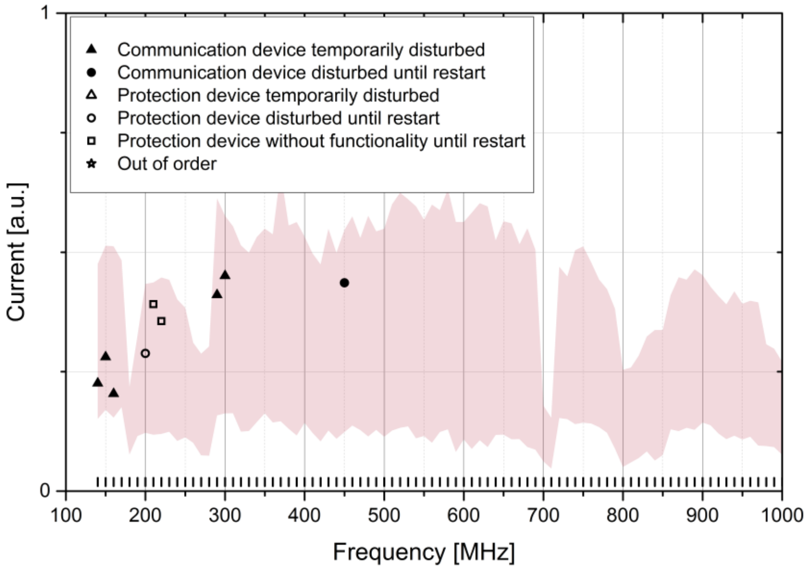


Figure 2: BCI Test 140-1000 MHz

3.2 TEM waveguide Tests

3.2.1 System Tests at the far end of the waveguide

Additional tests were performed inside the TEM-waveguide at MP2 (measurement point 2) in the rear section of the waveguide. At this spot, the test-setup as installed on a base plate was investigated within a frequency range between 140-3400 MHz.

An important criterion for normative investigations inside the TEM waveguide is the illumination of the DUT with different electromagnetic field polarizations. Based on the fact that the TEM waveguide is fixed the DUT was rotated into different orientations.

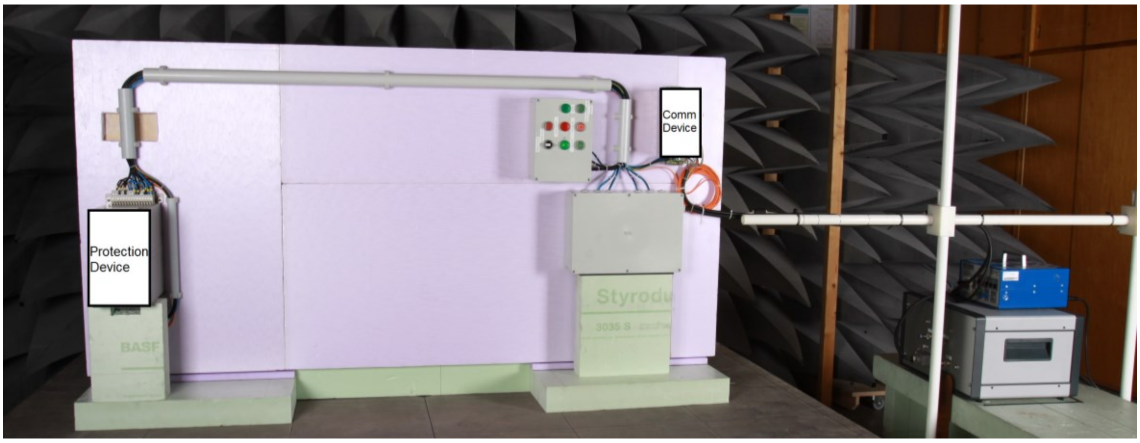


Figure 3: Horizontal orientation of the wiring loom – setup 2

For the investigations three different DUT orientations were inspected. Setup 1 was the vertical orientation of the wiring loom with the electrical field parallel to the long part of the wiring loom (maximum coupling to the lines). Setup 2 was the horizontal orientation of the wiring loom as shown in Figure 3, in this setup the long part of the wiring loom was arranged vertical to the electrical field but the short sections were parallel to the electrical field (minor coupling). The third setup was the horizontal orientation of the wiring loom with the base plate parallel to the ground plane, in this case there was no part of the wiring loom parallel to the electrical field (slightest coupling).

Figure 4 to Figure 6 show the result plots of the TEM waveguide investigation. The DUT displayed a high immunity with only few outages of the communication device for setup 1. For setup 3 more outages of the communication device were noticed, they focus on the frequency range 800-1000 MHz with even lower threshold values. By contrast the communication device showed a high susceptibility during the test according to setup 2 with many outages spread over the whole tested frequency range up to 2.5 GHz. One frequent failure occurring was the temporary disturbance of the communication device which has no influence on the functionality for the power grid. More interesting was the fact that the disturbances are presumably caused by direct coupling into the communication device and not by coupling into the wiring loom. That is based on the fact that setup 1 with the best wiring loom coupling revealed the fewest errors whereas setup 2 with a lower coupling but a different device orientation offered a higher susceptibility with many outages. The protection device showed a high resilience with no outages while investigating all three setup configurations.

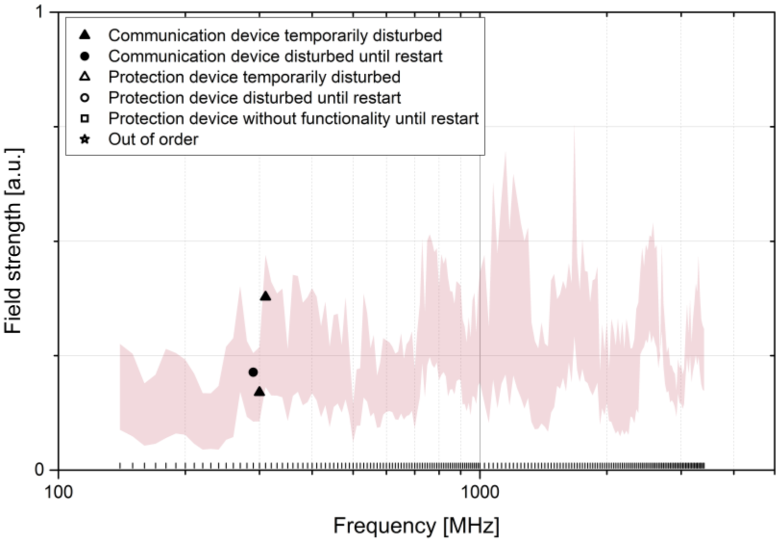


Figure 4: TEM waveguide test MP2 - Setup 1

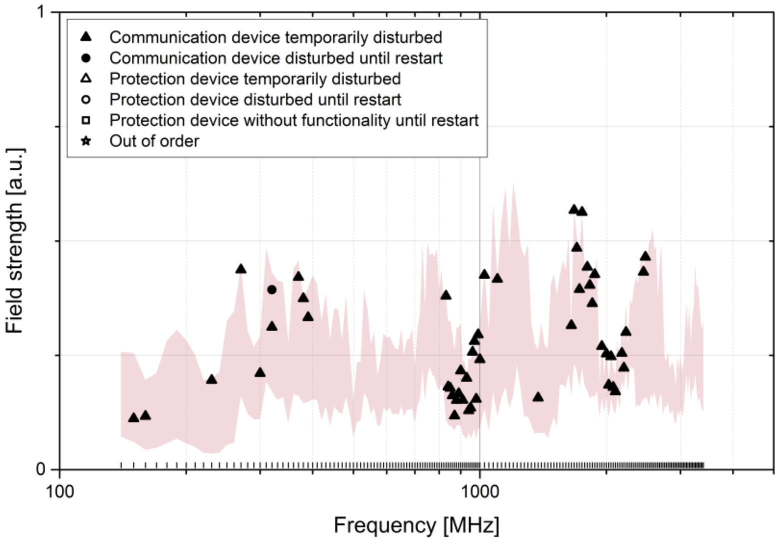


Figure 5: TEM waveguide test MP2 - Setup 2

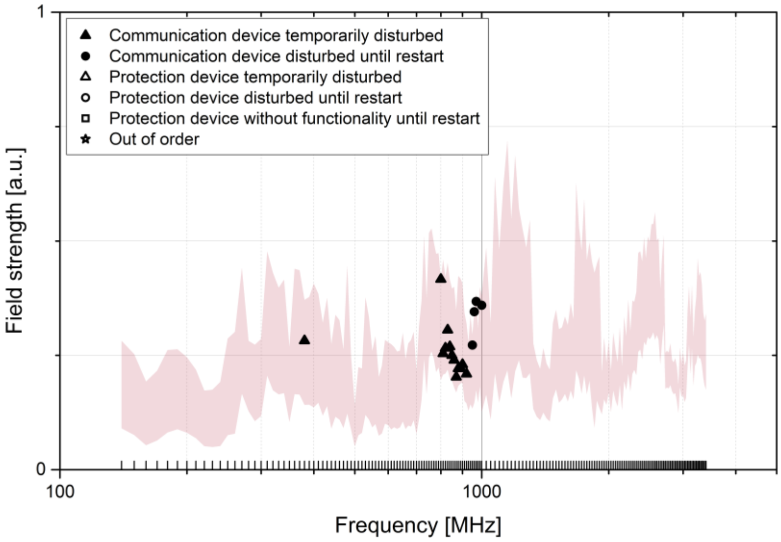


Figure 6: TEM waveguide test MP2 - Setup 3

3.2.2 Direct coupling close to the injection of the waveguide

The last tests were performed at MP8 in the front section of the TEM waveguide within the frequency range of 140-3400 MHz. At this spot, the direct coupling into the protection device was investigated. For this reason the communication device and the wiring loom were positioned outside the waveguide with the lowest electrical field coupling whereas the protection device itself was positioned inside the TEM waveguide with the same device orientations as described for the tests at MP2.

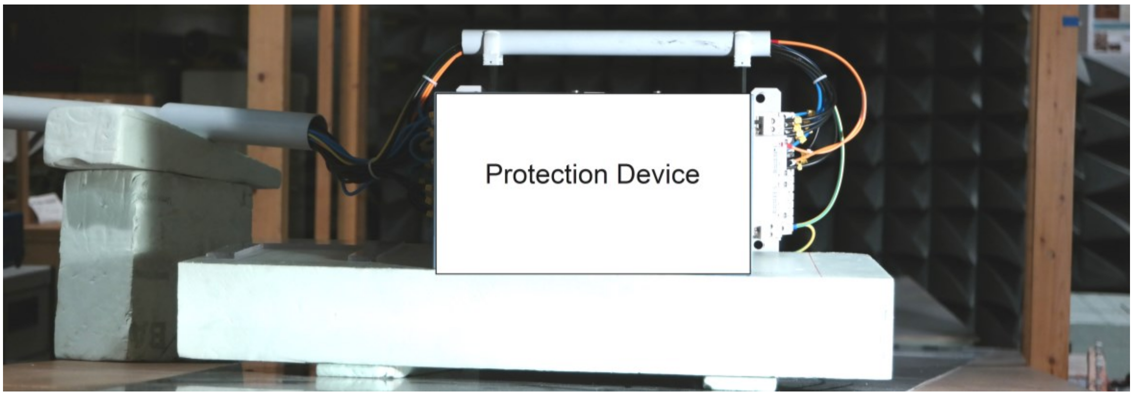


Figure 7: Direct coupling - setup 1

Figure 8 to Figure 10 display the test results for the direct coupling investigation. It is obvious that the susceptibility of the protection device highly depends on the device orientation within the waveguide. Setup 2 and setup 3 show the highest susceptibility with many failures spread out the whole tested frequency range even with low threshold levels. On the other hand, setup 1 show a minor susceptibility with only a few outages which often occurred near the maximum of the ramp. There were many different outages detected during the tests, starting with temporary disturbances like e.g. display errors or communication losses of the fibre optic interface integrated in the protection device. Other outages were ongoing contrast value adjustments, automatic restarts as well as lasting disorders with functionality loss until the device was restarted by the staff. Despite the precaution to position the communication device outside the waveguide, next to the facility walls with a minimum distance of several meters to the waveguide, the parasitic fields outside the waveguide sufficed to disturb the device at several frequencies which emphasizes its high susceptibility.

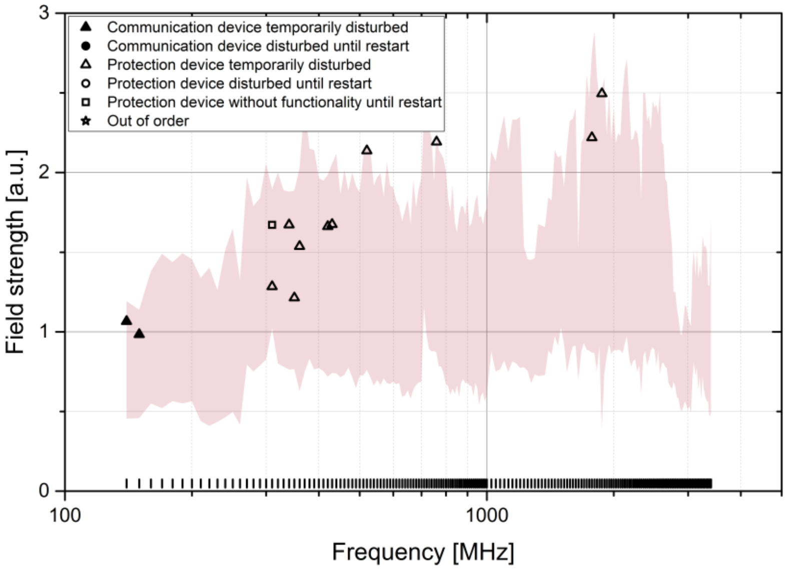


Figure 8: TEM waveguide test MP8 - Setup 1

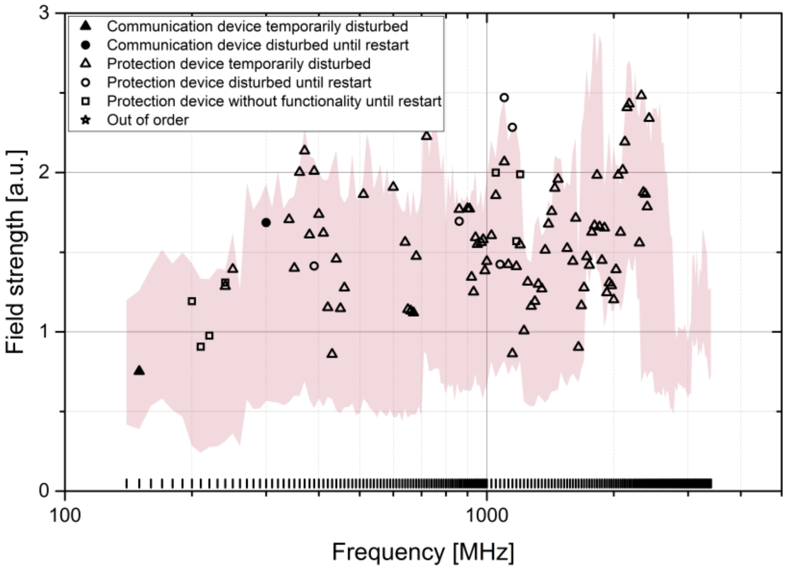


Figure 9: TEM waveguide test MP8 - Setup 2

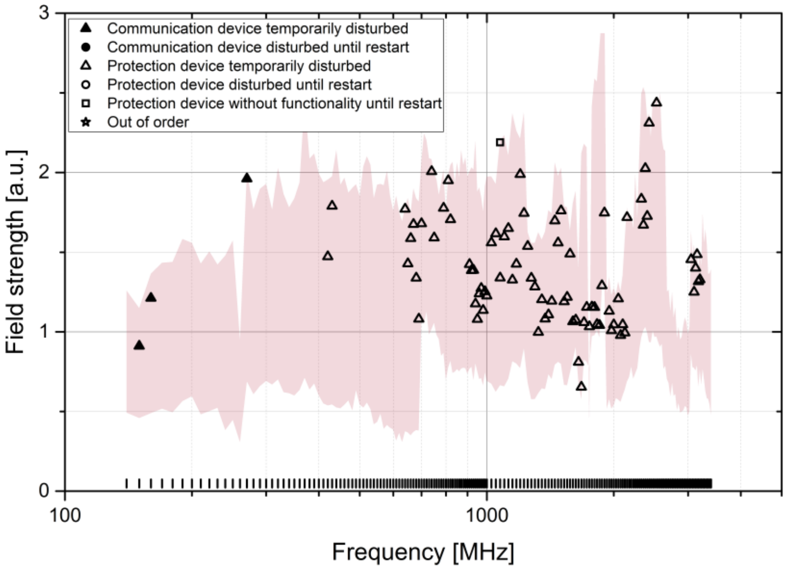


Figure 10: TEM waveguide test MP8 - Setup 3

3.2.3 Pulse Variation Tests

Finally, the above mentioned investigations with different arbitrary pulse modulation parameter combinations were performed. These tests were executed with the same setups as for the direct coupling investigations. The test results show similar susceptibilities with comparable threshold values. In addition, some new failures were detected, e.g. temporary manipulation of voltage and current values displayed by the protection device but also one permanent breakdown of the protection device.

4 CONCLUSION

The objects under investigation were devices installed in power grid substations. Although the considered control systems were less susceptible to HPEM interference than the investigated Smart Meter devices, the threat for the power grid is even higher because of their critical functionality. The severest disturbance detected was a breakdown of the protection device, followed by an ongoing disorder with functionality loss until restart. In this state, the protective circuit is disabled, thus a short circuit with a damaging current flow in the system cannot be interrupted. Besides, a command send by the control centre cannot be executed in this state which could result at worst case in a destabilisation of the grid. The determination of coupling paths helps to implement suitable protection measures for critical infrastructures. The required field strength for a disturbance of the protection device was several orders of magnitude higher than the levels requested in the EMC standards (Electromagnetic Compatibility). Nevertheless, these field levels might be generated at the target inside the substation due to its easy accessibility. The stations are typically located all over the country with no dedicated security personal or perimeter surveillance systems. That offers attackers with HPEM sources the possibility to get close to stations with a low risk of getting observed. In addition, it is conceivable to launch simultaneous attacks on critical devices over a wide area or at important locations to increase the impact on the grid.

REFERENCES

[1] International Energy Agency: “*Harnessing Variable Renewables – A Guide to the Balancing Challenge*“ ISBN: 978-92-64-11138-7

[2] C. Adami, C. Braun, P. Clemens, H.-U. Schmidt, M. Suhrke, H.-J. Tänzer, U. Weber, “*High Power Microwave Susceptibility of IT Network Components*“, ISBN: 978-3-8396-0051-1, p. 400-410, Future Security 2009 Karlsruhe

[3] C. Adami, C. Braun, P. Clemens, M. Jöster, M. Suhrke, H.-J. Tänzer, “*High Power Microwave Tests of Media converters*“ ISBN: 978-1-4673-0718-5, EMC-Europe 2012 Rome

[4] M. Joester, C. Adami, M. Suhrke, H.J. Taenzer: “*HPEM Tests of Security Systems*“ AMEREM 2014 Albuquerque, ID040

[5] F. Brauer, F. Sabath, J. L. ter Haseborg “*Susceptibility of IT network systems to interferences by HPEM*“ ISBN: 978-1-4244-4266-9, IEEE EMC 2009, Austin (TX)

[6] W. A. Radasky, R. Hoad, “*An Overview of the Impacts of Three High Power Electromagnetic (HPEM) Threats on Smart Grids*“ ISBN: 978-1-4673-0718-5, EMC Europe 2012 Rome

[7] W. A. Radasky, E. Savage, “*Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid*“, Metatech, Meta-R-323, January 2010

[8] M. Lanzrath, T. Pusch, M. Jöster, M. Suhrke, “*HPEM-Empfindlichkeit von intelligenten Stromzählern als Komponenten des Smart Grid*”, ISBN: 978-3-86359-396-4, p. 11-18, EMV 2016 Düsseldorf

INFLUENCE OF BUILDINGS ON HPEM VULNERABILITY OF IT INFRASTRUCTURES

Michael Joester [1], André Bausen [2], Stefan Pohlenz [3], Thorsten Pusch [4], Martin Schaarschmidt [5], Michael Suhrke [6]

[2] *AndreBausen@bundeswehr.org*
[3] *StefanPohlenz@bundeswehr.org*
[5] *MartinSchaarschmidt@bundeswehr.org*
Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS),
Humboldtstraße 100, 29633 Munster (Germany)

[1] *michael.joester@int.fraunhofer.de*
[4] *thorsten.pusch@int.fraunhofer.de*
[6] *michael.suhrke@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT,
Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

When evaluating the vulnerability of an electronic system against an external threat like High Power Electromagnetics (HPEM), its immediate surroundings have to be included. IT equipment will typically be located inside buildings, whose walls can considerably attenuate and deform electromagnetic waves. The layout of IT and supply cabling shapes the system response as well. A topological abstraction model renders analysis of our complex HPEM attack scenario possible. One can identify three topological zones: the outside as well as the inside of the building, and the IT equipment itself. We have performed radio frequency exposure experiments with reasonably simplified substitutes for the outer area, the building and a cabling scheme including two IT devices as the minimum IT system setup. The results give information about the key parameters of RF coupling from one zone to the next. Finally, some recommendations for protection measures at CI have been derived from the results.

Keywords: Critical Infrastructure, IT, HPEM, IEMI, Vulnerability, Protection, RF, Building.

1 INTRODUCTION

Electromagnetic waves of high frequency (Radio Frequency, RF) can carry electromagnetic energy into electronic systems over a distance. Thereby induced excess voltages and currents might influence device functionality. An attacker can exploit this effect to weaken electronic control or security systems by RF sources close to CI buildings, thus perpetrating a so-called Intentional Electromagnetic Interference (IEMI).

The residual amount of disturbance energy inside the target buildings is strongly related to reflections at large surfaces in the environment of the scenario location and the attenuation by materials located in the RF propagation path. The latter might include walls, windows, doors and holes in the outer walls. Furthermore, within the interior of buildings a complex electromagnetic field distribution establishes itself by a combination of internal reflections and attenuation.

In a last step of energy transfer, the electromagnetic field in the room enters the distributed electronic system by coupling into the mesh of cables and device nodes directly. The magazine article [1] describes the coupling into distributed systems with cable and reference ground loops.

The topology of the building defines clear boundary conditions between the outer electromagnetic field generated by an RF source in the outdoor environment and the electromagnetic field inside the building. Conceptually, the coupling from interior electromagnetic field into the distributed electronic system can be described in the same way.

To investigate these phenomena, it makes sense to define zones separated by boundary surfaces as a border between two zones with different characteristics, as described within the concept of Electromagnetic (EM) Topology [2].

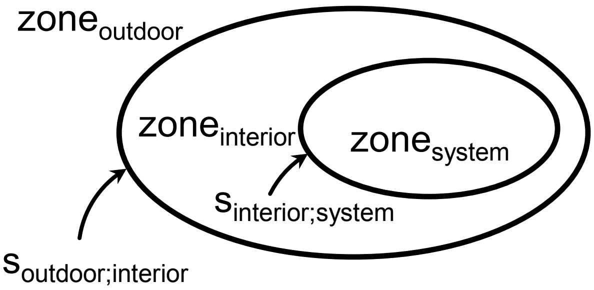


Fig. 1: The Zone / Boundary Surface model of EM Topology tailored to our scenario [2]

The boundary $s_{outdoor;interior}$ in Fig. 1 describes the influence of the building in this model of an HPEM attack scenario: an RF source is located outside the building in zone $zone_{outdoor}$, and the interior $zone_{interior}$ houses the distributed IT infrastructure defined as $zone_{system}$. The electromagnetic field in $zone_{outdoor}$ might be complex as scattering at surfaces in the environment leads to multi-path coupling into the building. The energy reaching $zone_{system}$ leads to an IT system response potentially including malfunction or even damage. Therefore, the injected energy as spread over a frequency range together with the characteristic system response describe the vulnerability of this system.

There are other unknown values in the chain of this model, the complex interior electromagnetic field in $zone_{interior}$ and the frequency-specific coupling into the distributed system represented by the boundary $s_{interior;system}$. The methodology to solve such a zone and surface model of EM Topology of an IEMI attack on CI in general is described in [3]. There are simulation works available describing a similar HPEM attack scenario on CI with multi-path coupling [4], including conducted coupling through cables into the building. The cable coupling as part of $s_{outdoor;interior}$ is investigated in [5] separately. The experimental work [6] determined RF transfer functions for the coupling between rooms within a building and outdoor with rooms in the building.

We will present in the following an experimental project of the Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS) together with the Fraunhofer Institute for Technological Trend Analysis INT, adhering to the zone and boundary model as presented above. All model components in Fig. 1 have been investigated separately by experiments with reasonable simplifications and predefinitions to reduce complexity and to get an overview on the key parameters of RF coupling. Apertures like windows and doors degrade the building walls' attenuation, depending on the materials in use. Cable loops are the gateway for RF into distributed IT systems and should be avoided. These results are the base for protection measures recommendations.

2 COUPLING OF RF INTO A BUILDING

The characteristics of $zone_{outdoor}$ are mainly defined by the test site the experiment took place at. To get simple but realistic conditions, a free field test area has been chosen, without any buildings close-by, but with an RF-reflecting ground. The field generated by laboratory RF sources is well defined by geometries e.g. antenna height and polarization and the field strength is measured and adjusted in the frequency range of interest.

The representation of a building for determining the influence of boundary $s_{outdoor;interior}$ should be as simple as possible, but realistic. Therefore, the WIS has chosen a garage- sized reinforced concrete container module with windows and a door as a generic one-room office, denominated Electromagnetic Office Module (EMOM). Such a simple geometry can be easily simulated with 3D-solvers in parallel to the experiments. Fig. 2 shows the generic building placed on the test site at WIS.

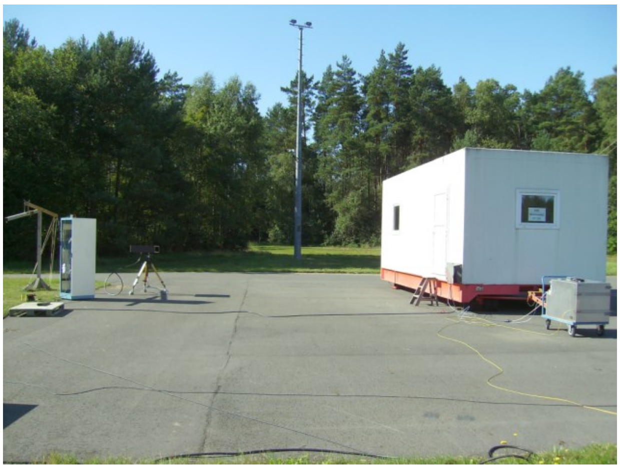


Fig. 2: Generic WIS one-room office building at test site

The attenuation of the container's concrete walls with reinforcement is a rising function of frequency in the frequency range of interest and can be estimated based on the experiment results of Pauli and Moldan [7] and the work of Giri and Tesche [8]. They measured the RF behavior of different wall materials used in architecture. Apertures like windows and doors lessen this attenuation. Conventional insulated glazing features metal coating to reduce IR transmission and it has an RF attenuation in the same order of magnitude as the concrete walls [9]. The door and the window frames of the EMOM are made of plastic and therefore, the overall attenuation of the building is expected to be smaller than what the materials could obtain. On the other hand resonance effects within the building can be assumed. In that case, RF field amplitudes will vary over the volume due to superposition effects of RF waves.

During the experiments, a broadband pulse source generated RF waves with horizontal and vertical antenna polarization at the test site, cf. Fig. 2, left-hand side. The magnetic component of the RF field has been measured in all three axes, that is the X-, Y- and Z-direction, at a probe position defined for further investigations of coupling into distributed IT systems. By two test runs, the difference of field values with and without the generic building in place has been determined. The door of the building was directed towards the RF source.

Fig. 3 shows the transfer function of the magnetic field component H_y in the tested frequency range up to 4 GHz as a solid black line. The magnetic component of the outdoor RF field is generated horizontally. The blue curve is the expected attenuation of concrete with reinforcement according to [7] - apertures and window attenuation are neglected -, the red dashed curve is the linear fit of the result curve. The outdoor H_y

component might be transformed to some degree into the other two interior field directions, but this mechanism can be neglected for the attenuation discussion.

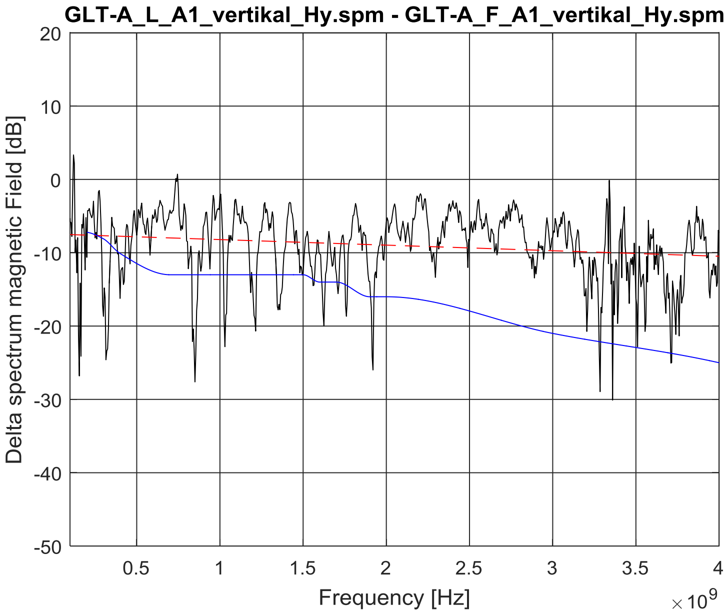


Fig. 3: Transfer function of magnetic field component H_y (black) of vertical polarized RF waves at a fixed probe position with and without generic building, together with a linear fit (red) and the estimation for attenuation by concrete [7] (blue).

As a result, one can see the degradation of wall attenuation with rising frequency by the apertures for windows and the door. The attenuation of the window glass might partly be suspended by the plastic frame. Anyhow, the door made of plastic is a large aperture without significant attenuation.

Also, the resonance behaviour of the volume versus frequency can be observed as characteristic dips in the field difference curve in Fig. 3. Simulations of the EMOM-shaped reinforcement as a simplified model validate the experimental evidence. As an example the result of the prominent resonance at 720 MHz is illustrated in x-/y-plane and in x-/z-plane in Fig. 4.

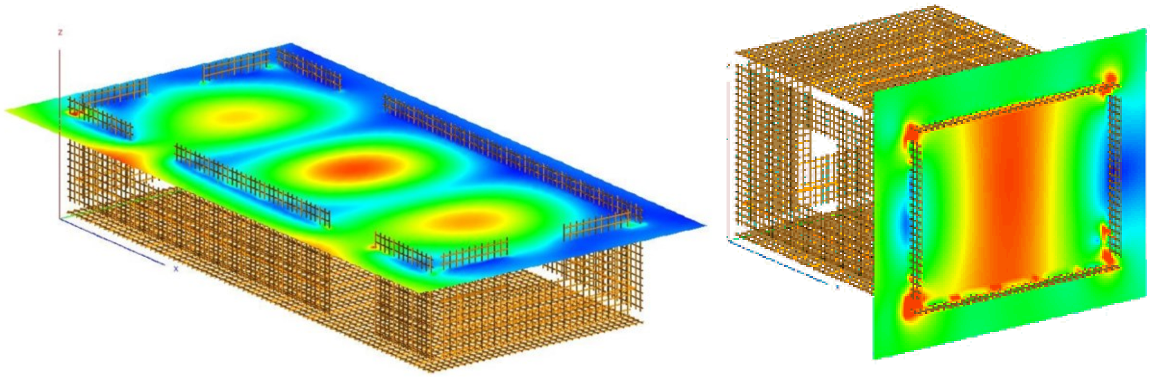


Fig. 4: Numeric simulation result of EMOM at 720 MHz as an example, the field amplitude is color-coded.

At each of the observed resonance dips, such spatially modulated field distributions will be established, leading to varying degrees of exposure depending on the position within the room.

3 COUPLING OF RF INTO A DISTRIBUTED IT SYSTEM

To investigate the RF coupling from the building's interior $zone_{interior}$ into the distributed IT system characterized by $zone_{system}$, the model representative $s_{interior;system}$ for this coupling has to be determined. Again, a preferably simple, but realistic test setup has been chosen for the experiments.

Today, an office IT system consists of a desktop tower PC, commonly placed under a table, a computer monitor, a mouse and a keyboard on the table, and the connections to mains and LAN. As an abstraction, one can find two overlaid meshes of copper wires, connected in loops with the devices PC, monitor, and a LAN router as nodes, illustrated in Fig. 5.

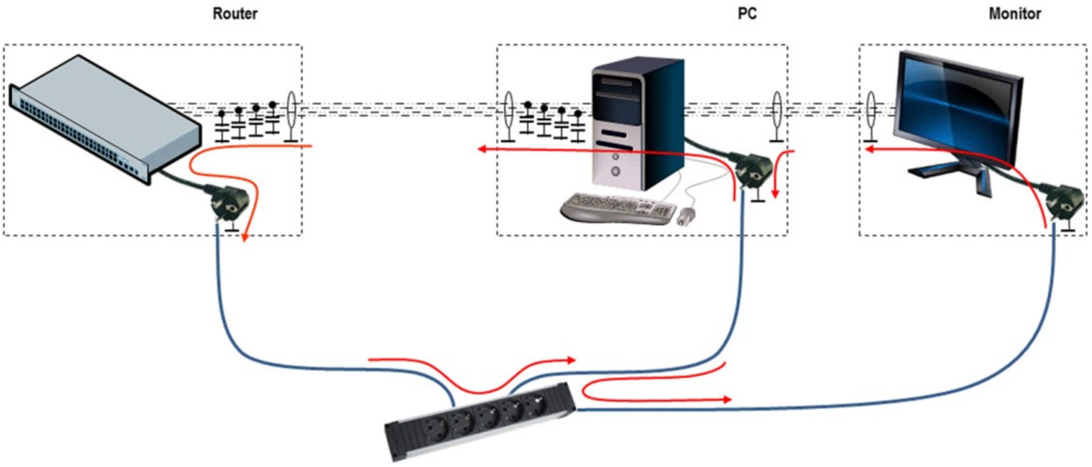


Fig. 5: Wire loops of a typical office workplace

Within the loops RF currents can flow, indicated by the red arrows in Fig. 5. The abstraction down to one loop and two devices leads to the following simplified test setup as shown in Fig. 6a.

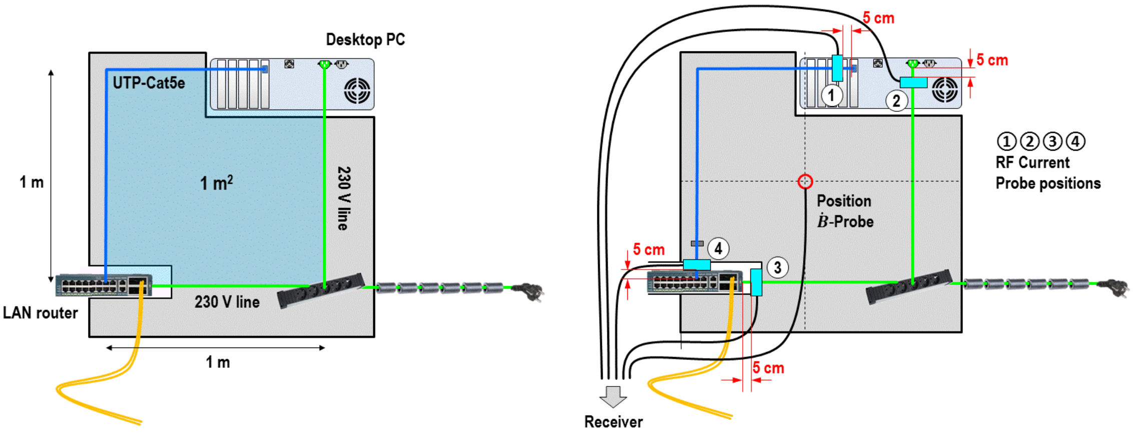


Fig. 6: a) Simplifed distributed IT system with one wire loop and two devices as nodes, propped up by a Styrofoam stand.
b) Measuring the RF currents on the IT system lines during testing

The goal of the experiments is to investigate the magnetic and electrical coupling of RF fields into this setup. During the tests, the RF currents on the wires close to the connectors of the devices and the magnetic component of the RF field in the middle of the square meter loop have been recorded. The monitoring setup is illustrated in Fig. 6b.

The coupling function of this setup can be determined with a transfer function measurement, performed in a TEM waveguide up to 2,5 GHz. Fig. 7 shows the maximum of the four RF currents on the wires at each frequency, normalized to an RF field strength of 1 V/m. The setup was placed into the TEM waveguide in the position illustrated in Fig. 6b.

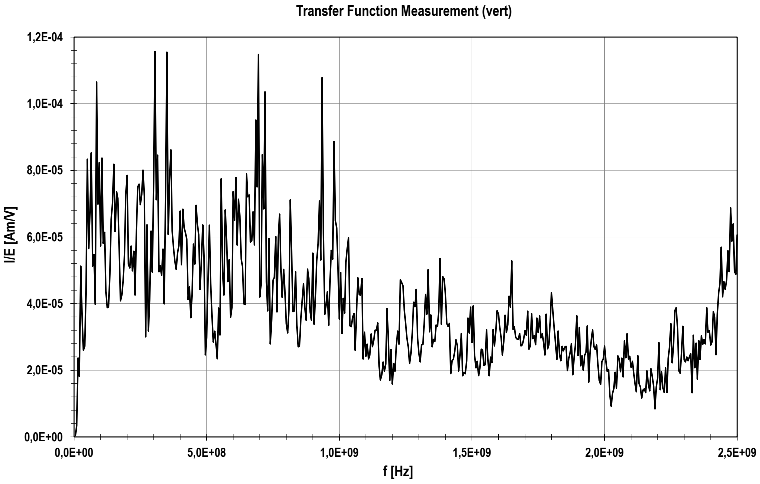


Fig. 7: Result of transfer function measurement

As expected, the magnetic coupling is effective up to approximately 1 GHz, beyond this frequency the impedance of the wires is too large for a magnetic RF field to couple into the loop. In that case the meshed characteristic of the distributed IT system dissolves into separate and independently susceptible sub-parts with rising frequency beyond 1 GHz.

4 COUPLING RF INTO A DISTRIBUTED IT SYSTEM WITHIN A BUILDING

For the prediction of failures in an IT system, additional information has to be considered: The RF susceptibility test results for each IT component, where functional failures are determined in dependence on the RF fields. In further experiments the overall coupling from $zone_{outdoor}$ to $zone_{system}$, implicitly including $s_{outdoor;interior}$, $zone_{interior}$, and $s_{interior;system}$, and the susceptibility of IT devices were investigated. The simplified test loop and a real office workplace were placed into the generic building, as shown in Fig. 8. The two PCs interacted via LAN, an RF hardened video camera was aimed at the computer monitor of the office workplace.

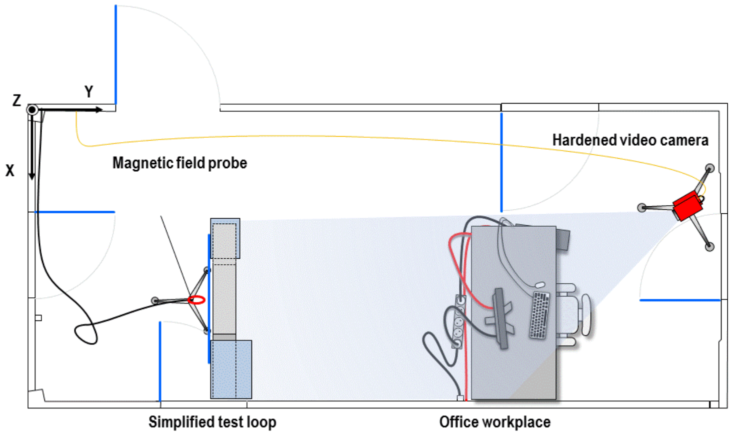


Fig. 8: Experimental setup for combined coupling in the generic building

Different program applications generated LAN traffic in both directions between the test loop PC and the workplace PC, passing the test loop router. The transmission has been evaluated for throughput and the hardware has been monitored for functionality, e.g. computer monitor display failures. Again, the magnetic RF field in the middle of the loop and the currents in the test loop have been recorded during the tests.

As a last experiment an attack scenario has been defined using this setup. A High Power Microwave (HPM) source was placed in front of the building similar to the setup shown in Fig. 2. This RF source generated pulsed RF in the frequency range from 150 MHz to 3400 MHz with a pulse power of maximum 35 kW. At each test frequency, the source increased the output power from start level to maximum level in a certain time.

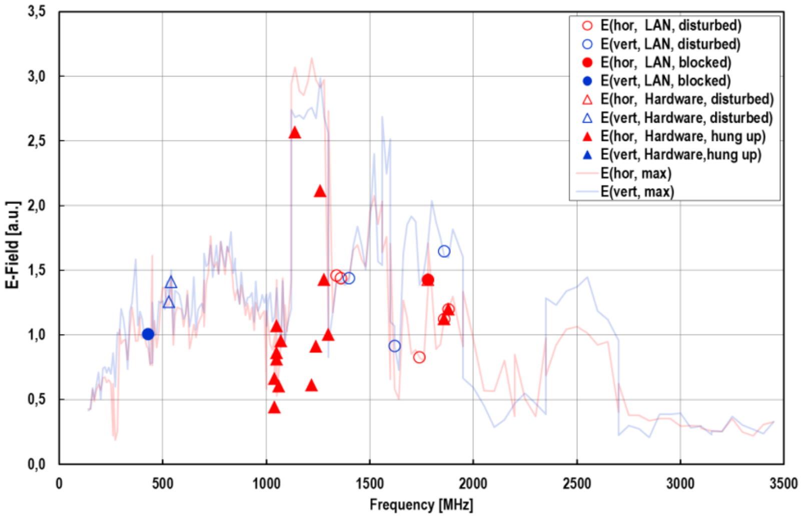


Fig. 9: Test result of HPM attack scenario on generic building with office desk and test loop inside

As a result the majority of failures occurred above 1 GHz and with horizontal field polarization (Fig. 9). In that frequency range, mainly the PC of the test loop hung up suddenly without any disturbance phenomena in advance. According to the transfer function result shown in Fig. 7 the coupling mechanism seems to be direct coupling into the housings of IT equipment. Only a few failures occurred with vertical polarization. Summing up the result of this experiment, the distributed IT system seems to be more susceptible in this frequency range, where it already split into individual devices.

5 CONCLUSIONS

In general, many CI buildings will be made of concrete with reinforcement and one expects a certain RF attenuation. Apertures like windows and doors degrade this attenuation, depending on the materials in use. RF experiments with a simplified building showed the degradation of the expected attenuation by apertures fitted with cost-effective materials.

Once the RF is inside a building, the rooms act as resonating cavities with RF field superposition leading to a stationary 3D-pattern of different field strengths. The RF field distribution with areas of higher and lower field strengths depends on the RF frequency and the dimensions of the room as well as on the interior (in particular metallic parts).

The placement of distributed IT systems within the rooms spatially related to the aforementioned RF field distribution influences the amount of RF energy coupled into the IT system. Experiments with a simplified test loop made of IT components showed a frequency limit where the distributed IT system initially considered as a single influenced unit transforms into a set of independent IT devices, influenced individually by the RF. Below frequencies of approximately 1 GHz, wiring loops formed by mains and LAN cables allow RF to couple into the wiring, which can disturb the functionality of the IT. At higher frequencies, the impact on IT devices is independent of the wiring mesh due to direct coupling into housings. The individual IT devices are roughly of the size of the higher field strength areas in case of cavity resonances above 1 GHz.

Summarizing, the individual frequency depending HPEM susceptibility of the involved IT devices completes the total picture of IT vulnerability. The complex two-stage transfer function couples RF energy from outside the building into a room and then into the distributed IT system. In case the amount of RF energy inside the IT system exceeds the susceptibility threshold levels system failures will occur.

Some protective measures recommendations for operators of CI can be derived from the experiments. Besides keeping distance to CI buildings realized with fences as part of a basic counter-IEMI practice, windows frames, doors, ventilation and similar openings in the walls and roof should be made of metal. Window glass should be selected with RF rejection capabilities. The layout of distributed IT systems should be planned before realization. The goal is to avoid cable loops, especially in the overlay of mains and LAN meshes. This will lead to device cable bundling and device clusters as well as a star-shaped routing. The work [10] gives additional hints for cable managing in trays, earthling and bonding. Finally, the CI IT devices themselves should be hardened against RF, in addition to the general EMC performance.

REFERENCES

[1] Mardiguian, Michel. (2015). *A Review of the principal EMI Coupling Paths – The key to understanding and preventing or solving EMI problems.* Magazine Electronic Environment 01.2016, pp. 32-37.

[2] Baum, Carl E.. (1981). *Electromagnetic Topology for the Analysis and Design of Complex Electromagnetic Systems.* Proc. EMC Symposium Zürich, pp. 209-214.

[3] Runke, Simon et al.. (2015). *IEMI Analysis of Critical Infrastructures by Simulations using a Multi-Method Coupling Strategy*. Proc. of the 2014 International Symposium on Electromagnetic Compatibility (EMC Europe 2014), pp. 1238-1241

[4] Nana, Richard Kanyou et al.. (2009). *EMT based methodology for the vulnerability analysis of complex systems to IEMI*. Proc. 2009 IEEE Symposium on EMC, pp. 243-248

[5] Karcoon, Hamed et al.. (2012). *Shielding Effectiveness of Screened Rooms with Line Feed-Throughs - a Semi-Analytical Approach.* Proc. 2015 IEEE Symposium on Electromagnetic Compatibility (EMC), pp. 312-316

[6] Junqua, I. et al..(2014). *Evaluation of RF Transfer Functions Between the Outside and the Inside of Building Room.* Book of Abstracts AMEREM 2014 Albuquerque, ID092.

[7] Pauli, P., Moldan D.. (2000). *Reduzierung hochfrequenter Strahlung im Bauwesen, Baustoffe und Abschirmmaterialien*. Druckerei Huegelschaeffer, Mainbernheim.

[8] Giri, D. V., Tesche, F. M.. (2013). *Electromagnetic Attenuation throughVarious Types of Buildings*. 2013 Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC), pp. 438-441

[9] Ragulis, P., Kancleris, Ž., Simniškis R.. (2014). *Transmission and Reflection of Microwave Radiation from Novel Window Panes*. Book of Abstracts AMEREM 2014 Albuquerque, ID101.

[10] Hoad, R. et al.. (2007). *EMC for Installations – Practical Design and Assessment Methods*. IET Seminar on New Regulatory Requirements and Techniques for Achieving Electromagnetic Compatibility in Commercial Buildings, 2007, pp. 49-76.

PV-GENERATORS, A SOLUTION FOR CRITICAL INFRASTRUCTURE PROTECTION?

Markus Nyffeler[1] and Armin W. Kaelin[2]

[1] *markus.nyffeler@armasuisse.ch*
Federal Department of Defence, Civil Protection and Sport DDPS, armasuisse,
Science and Technology, Feuerwerkerstrasse 39, 3602 Thun (Switzerland)

[2] *armin.kaelin@emprotec.ch*
EMProtec GmbH, Rebhaldenstrasse 14, 8340 Hinwil (Switzerland)

Abstract

Possible causes for a continental blackout of the electrical energy supply and the distribution grid might be a High altitude EMP (HEMP) or presumably the volatility of the European power network due to the increasing use of decentralized renewable energy. A Photovoltaic (PV)-generator is a possible local backup solution in the case of an electricity blackout, provided it is immune against most established threats, including HEMP. In order to prove this, both radiated and conducted high power electromagnetic environment (HPEM) threats – as mentioned in HPEM standards – have been applied on each component level of PV-generators, except the inverters, which are relatively easy to be protected by well-known protection measures. Extensive practical experiments proved that the HPEM immunity of individual PV-cells is quite high. Assemblies of PV-cells in PV-modules including their cabling can be protected with some reasonable measures to comply with highest electromagnetic protection requirements for PV-generators of any size.

Keywords: HPEM, HEMP, PV-cell, PV-generators, grid ,off-grid, infrastructure, protection

1 INTRODUCTION AND MOTIVATION

The most critical among all critical infrastructures is ELECTRICITY!

Renewable energy sources remain increasingly popular. Photovoltaic (PV)-generators, which convert sunlight into electricity, in the past few years became affordable also due to increasing production. Many PV-generators have already reached “grid-parity”, which means that their overall energy production cost became equal or even lower compared to electricity from the grid. With an increase of 34% in 2015, the total worldwide installed PV-power reached 256 GW at the end of the year. PV-generators produce decentralized renewable electricity and provide certain independency from the grid, especially in the case of off-grid systems which are combined with local energy storage.

Some countries or regions already have a high density of many small power generators (each with a peak of a few kW), typically used on roofs of private buildings, or medium power generators (peak of tens to hundreds of kW) used for industrial electricity production. Often PV-generators of organizations which run critical infrastructure are not identified as critical parts deserving protection against martial acts. Especially off-grid PV-generators have a potential to be used as emergency power.

How vulnerable is a PV-generator system in the case of a high altitude electromagnetic pulse (HEMP) -event? Can it be protected efficiently for use as emergency power?

Recently an EMC-Consultant proposed to shield the PV-modules by a thin wire mesh, which is not a very suitable option. The shield (wire mesh) partially obstructs the sunlight and therefore reduces the efficiency and simultaneously increases the overall costs. Once the HPEM immunity of PV-generators is assessed it will be possible to determine the protection gap for standardized HPEM protection requirements. So far, only a few publications about EMC characteristics of PV-cells exist. This fact gave the motivation to further investigate the immunity.

2 BASIC PRINCIPLES OF PV-GENERATORS

A single PV-cell (Figure 1) with the size of 156 x 156 mm^2 in full sunlight generates approx. 0.6 V / 8 A providing 1000 W/m2. Electrically a PV-cell is a diode (pn-junction, Figure 2), which produces a voltage of 0.6 V and a current if exposed to light. Typically 60 or 72 cells are connected in series to form a PV-module. A single PV-module generates a power of 200 to 300 W DC, typically at 36 V / 8 A. PV-modules are connected in series to form a string producing up to 1000 V DC. String power is fed into an inverter, which manages electricity production using maximum power point tracking (MPPT) and converts DC into AC. Immunity and protection of inverters were not considered in this study since published protection measures can be applied to protect them.

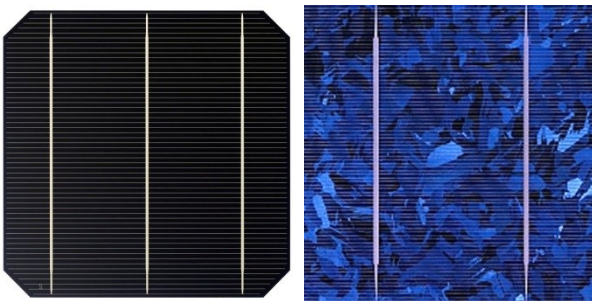


Figure 1: Monocrystalline cell (left) and Polycrystalline cell (right)

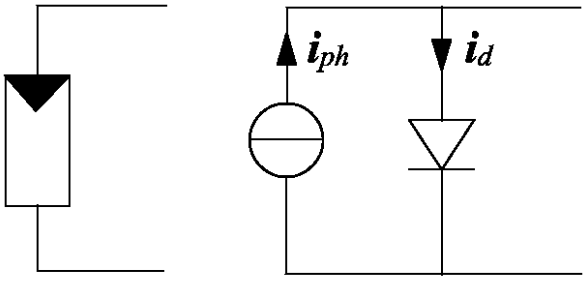


Figure 2: Schematic / Principle of PV-cells

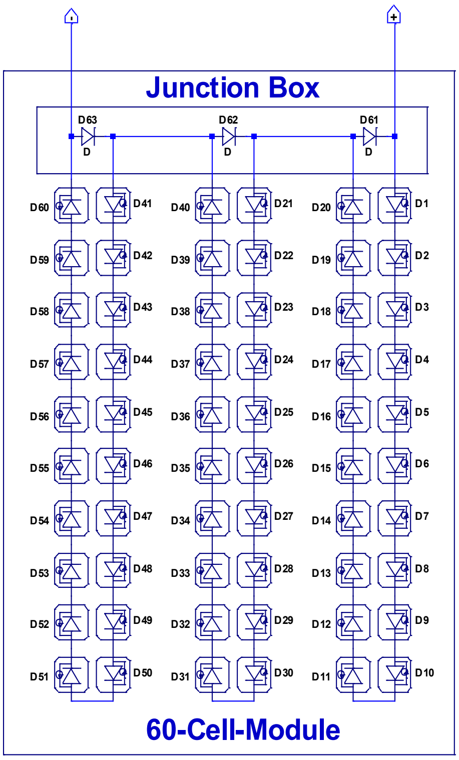


Figure 3: Electrical circuit of a module

A typical PV-module consists of 3 groups. Each group consists of 20 or 24 cells electrically connected in series. The 3 groups are as well electrically connected in series (daisy chained). A junction box collects all group wires and provides connection to the next module or to the inverter. Each group has a bypass-diode located in the junction box. The bypass-diode protects the group from too high reverse voltages in case of local shading of one or several cells. Electrically the bypass-diode is anti-parallel to the cells in the string. **A typical home system** consists of 1 to a few 10’s of PV-Modules connected in series to build one or two strings with a DC voltage up to

1000 V and ~10 kW peak power. Currents in a string are in the order of 10 A. The inverter converts DC to AC for coupling into the AC-grid. **Large scale PV-generators,** with a peak of up to 100 MW, have 1000's of modules, which are always divided into many strings consisting of 20 to 30 modules each. Each string is connected to an inverter.

3 DETERMINING THE DAMAGE LEVELS OF TYPICAL PV-COMPONENTS

3.1 Radiated induction on models and components

In order to better understand the damage levels and safety margins typical PV-components such as PV-cells, bypass-diodes and PV-modules were investigated with regard to transient surge behaviour. A single PV-cell is a diode with a large pn-junction surface, which forms a relatively large capacitor. Often one side is fully metallized like an electrode. As the second electrode a thin wire grid collects the current on the side which is directed towards the daylight . Typically 10 to 12 cells, which are electrically connected in series, form a closed loop with a so called bypass-diode in reverse direction. The loop area is typically 0.3 x 1.5 m^2 = 0.45 m^2.

The bypass-diode protects the cells of this group in case of partial shading. The energy fluence of a HEMP is 114 mJ/m^2 [1]. Current induced in this loop depends on polarity and flows either in forward or reverse direction through all diodes. Experiments with a wire model have shown that less than 100 A of peak current and less than 2 mJ of HEMP-energy are coupled into a single loop. A single PV-module consists of three loops, which are electrically in series. Experiments with a wire model of such a PV-module have shown (Figure 4) that less than 200 A of peak current and less than 4 mJ of HEMP-energy are coupled into a single module of three groups.

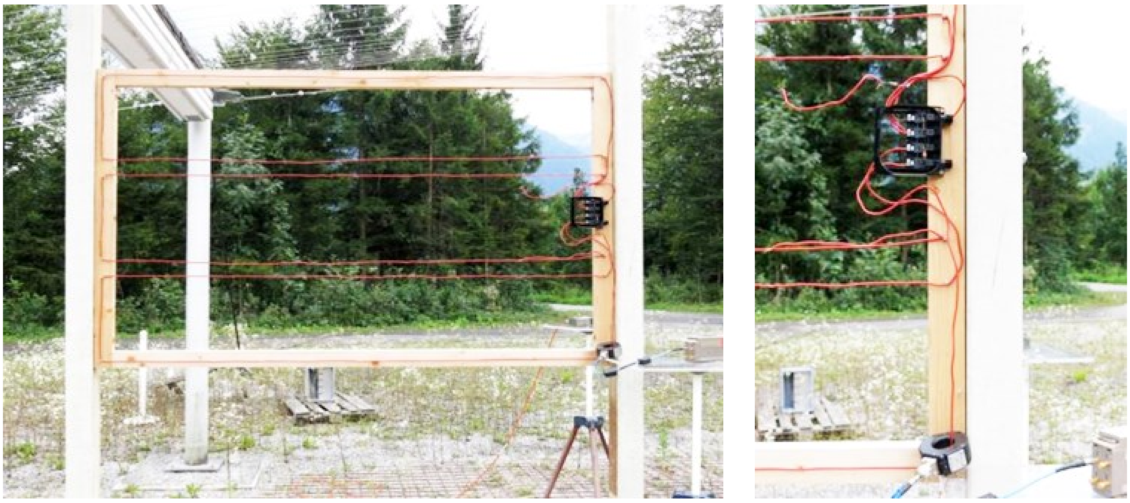


Figure 4: Wire model of module (left) and a single loop (right) in the HEMP simulator

However, there is also HEMP-coupling from external cables interconnecting the modules and the inverter. Depending on cable length and geometry these early time HEMP (E1) currents can be as high as 2 kA. No coupling of intermediate time HEMP (E2) is expected because cables are usually shorter than 100 m. PV-cell diodes in a loop and its bypass-diode are electrically anti-parallel. Externally coupled currents always flow in forward direction through either cell diodes or bypass-diodes and therefore provide already limited protection without any additional measures on the module. Another experiment has shown that a metal frame around the module has a significant influence on the current wave shape. The frame reduces the amplitude by

20 to 50%. Therefore all following experiments were carried out without a metal frame in order to represent a worst case testing.

3.2 Conducted induction on components

The following components were available for the experiments:
PV-cells of different technologies: Poly- and monocrystalline versions (ERSOL Blue Power, Black Power); Standard and Hetero-Junction technology (HJT, Meyer Burger); in glass-glass and glass-back-sheet technology; Standard, smart wire grid connection (SWCT, Meyer Burger); Interdigitated back contacts (SunPower® Maxeon).
Bypass-Diodes: SL1110 (Schottky diode); SL1515 (Schottky diode); SBR12U45LH (SMD Schottky diode); new technologies not yet available at the time of the tests: active bypass-diodes with ultra-low forward voltage.
PV-modules: 60-cell module with polycrystalline cells in 3 loops, 3 bypass-diodes; module with the same parameters but with monocrystalline cells; module with the same parameters but with monocrystalline HJT cells in SWCT.
I-V-Characteristics of bypass-diodes and PV-cells (diodes as well) were measured in forward and reverse direction of the diode (Figure 5). This is important in order to observe any test related changes and to determine partial failure of the components.

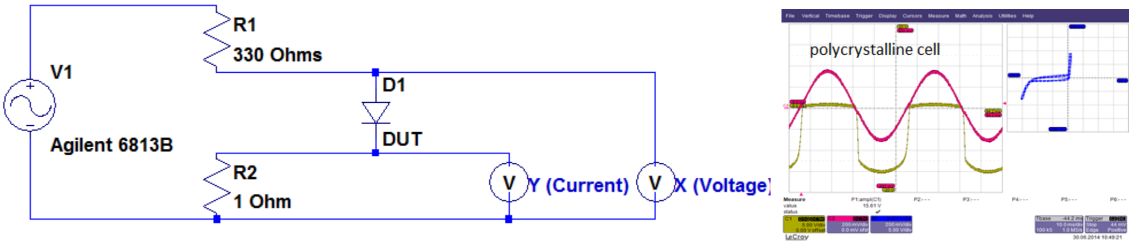


Figure 5: I-V Diode characteristic test setup (left) and test result (right)

After the characterisation of electrostatic discharges (ESD) [2] both arc-discharge and direct contact method were performed on the naked cell surface or the metal sheet in order to test reactions to nanosecond rise time currents (Figure 6 left). This is a brute-force method as it usually does not happen when embedded in a module. Several 100 ESD pulses up to 17 kV with both polarities – positive and negative – were randomly distributed over the surfaces of the cells.
Then surges [3] of 8/20 µs, from 80 A up to 2 kA were applied to PV-cells and bypass-diodes, first in forward direction (Figure 6 right) starting with a 160 A amplitude. Voltage was measured across the cell and no-damage was verified by measuring and comparing I-V-characteristics and increasing amplitude until I-V-characteristics changed due to damage. In a second step the same test was repeated in reverse direction on new diodes or cells.

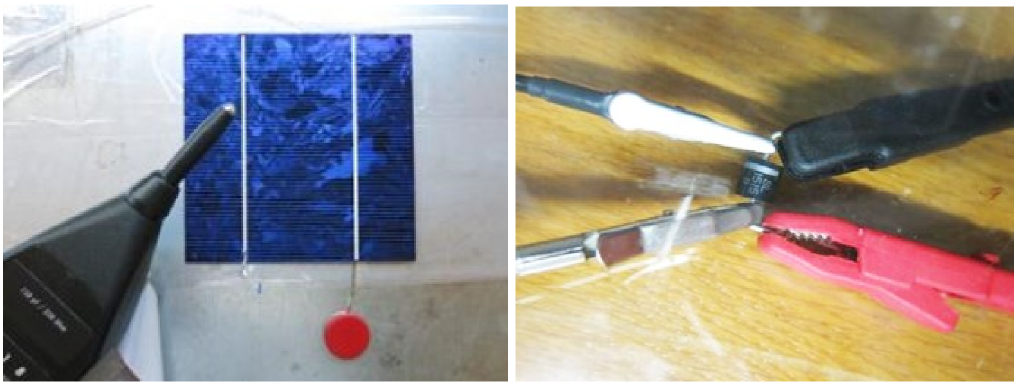


Figure 6: ESD on cell surface (left) and surge on a bypass-diode

Finally HEMP pulsed current injection-tests (PCI) with currents up to 2.5 kA 20/500 ns, as required by [4] MIL-STD-188-125, were applied to PV-cells and bypass-diodes. For this current injection the cells were laid between two copper sheets for full surface connection. First, currents were applied in forward direction starting with a 1500 A amplitude, measuring voltage across the cell, verifying no-damage by measuring and comparing I-V-characteristics, then increasing amplitude to 2500 A, measuring I-V-characteristics to determine damage. If the cell was damaged a new diode was used and the same procedure was repeated in reverse direction.

4 TEST RESULTS

4.1 ESD test on cells

About 30 positive and 30 negative polarity discharges, respectively forward and reverse 17k V ESD-discharges, of 10 mJ each were applied directly to the naked PV-cells and randomly distributed over the cell surface. It was observed that arc discharge did not only hit the metal fingers of the cell as expected, but also entered directly into the semiconductor. Under the microscope a slight colour change was observed directly at the entrance of the current into the semiconductor. Although the punctual discharge resulted in a relatively high current density there was absolutely no change in the I-V-characteristics. No damage was observed.

4.2 Surge test on cells

On mono- and polycrystalline cells 8/20 ms forward and reverse surges with increasing levels of 250 A, 500 A, 1000 A and 2000 A were injected. No damage was observed with 2000 A on both types of cells in forward direction.
The monocrystalline cell first lowered its breakdown voltage at 250 A and was punctured and broke at the entry point with a 500 A reverse surge current.
By feeding an external current to a cell in a dark environment the current distribution on the cell can be seen using an infrared camera. A comparable method is to take an IR picture of the cell without load in sunlight. Figure 7 shows the punctured, locally damaged (short-circuit) PV-cell using both methods. It is assumed that the failure was caused by a too high current density in the avalanche breakdown mode.

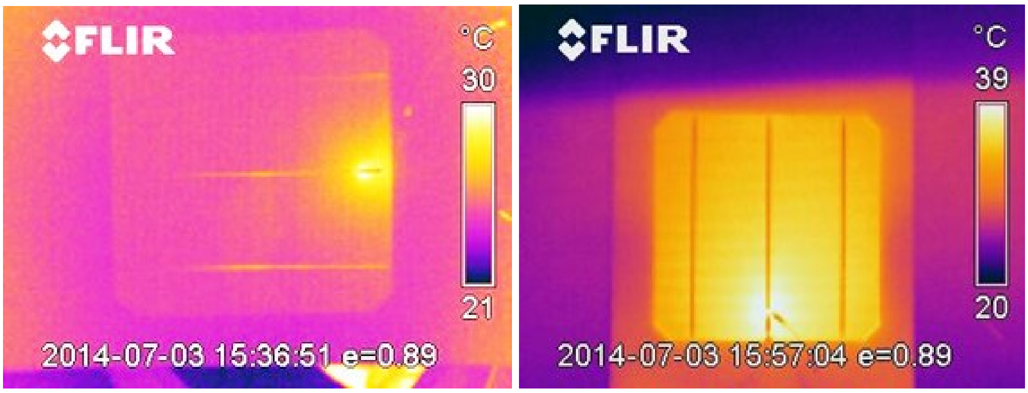


Figure 7: Current density on the broken monocrystalline cell using an external current of 0.1 A (left) and same active cell without load in sunlight (right).

On the polycrystalline cell some leakage was caused from a 250 A surge and a strong leakage arose from a 500 A reverse surge. HJT cells withstand surge currents up to 1000 A in forward direction and are therefore more sensitive to surges than other cells. But these cells also withstand surge currents up to 1000 A in reverse direction and are therefore less sensitive than other cells.

4.3 Surge tests on bypass-diodes

Schottky bypass-diodes SL1110 and SL1515 have easily survived all surges in forward direction up to 2000 A. But surges of less than 100 A (8/20 μs) in reverse direction damaged the bypass-diodes.

4.4 HEMP field fests

Four PV-modules with different cell technologies, different wiring and packaging were exposed to the full HEMP threat level (50 kV/m) [5], later to the double level and finally to the triple threat level (150kV/m) in 6 different orientations using three different loads. As a nominal load 3 Halogen bulbs of 35 W each were used in series, which immediately showed the modules function when directed towards sun light. Other loads were open-circuit and short-circuit. At least 3 pulses per configuration and 3 field levels were fired. In total, more than 150 HEMP-pulses were applied per module.

No damage to any of the four PV-modules was observed in any of the above configurations. In two cases one of totally 12 bypass-diodes failed in short-circuit during the 150 kV/m test after more than 100 cumulative HEMP-pulses. It remained unclear whether this was a random or cumulative effect. The modules worked normally after replacing the defective bypass-diode. In the factory, the performance of all PV-modules was tested with the flasher . Absolutely no alterations could be observed, all cells in the modules worked with the same power as before the HEMP-tests.

5 COUPLING AND PROTECTION

HPEM protection devices for conductors installed in Swiss armament goods always combine protection against HEMP, lightning and many other pulsed threats and retain the function of both the connected systems as well as of the protection devices themselves. Using this approach for the combined protection against the high energy of lightning and the fast rise time of HEMP allows minimizing the measures for any size of PV-generators. Like mentioned above, off-grid PV-systems or systems in local grids, with the possibility to be disconnected from the public power grid, are potentially secured electrical energy suppliers for critical infrastructure.

5.1 Coupling paths into PV-systems

In order to determine the locations for protection measures it is important to know the coupling paths. Figure 8 shows these locations for HEMP early time short pulse E1 coupling.

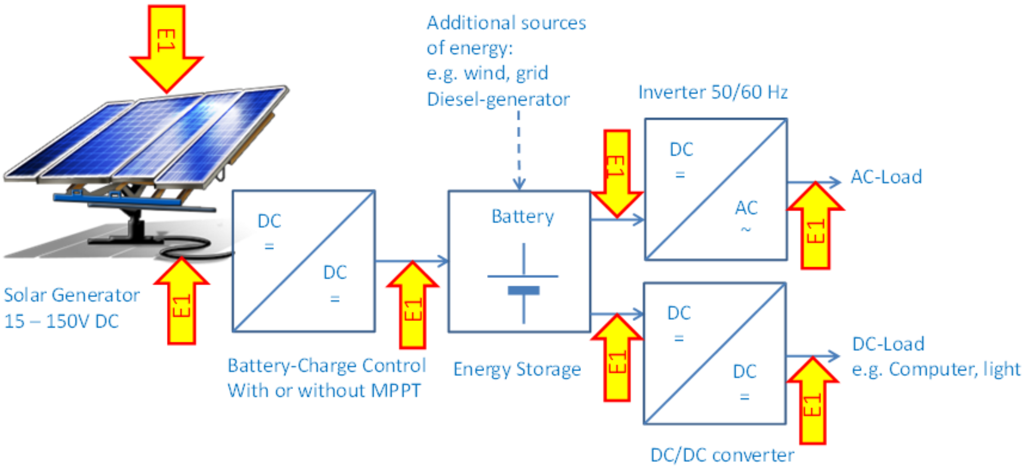


Figure 8: E1 coupling paths for HEMP and lower frequency coupling to PV-systems

5.2 Protection of PV-systems

The presented tests showed that PV-modules survive induced HPEM currents. However, external cables should be shielded. The use of transient voltage suppressor (TVS) diodes for each PV-module is recommended in order to protect against conducted disturbances from cabling. Subsystems containing electronics, like battery charge control or others, can be protected by partially shielded enclosures and conventional surge protection devices (SPD). Depending on the construction of the PV-system, the whole system apart from the entity of modules might be protected with an integral shielding enclosure shown in Figure 9. When metal frames are used for construction reasons, the module cables might be guided along the metal construction for small PV-generators.

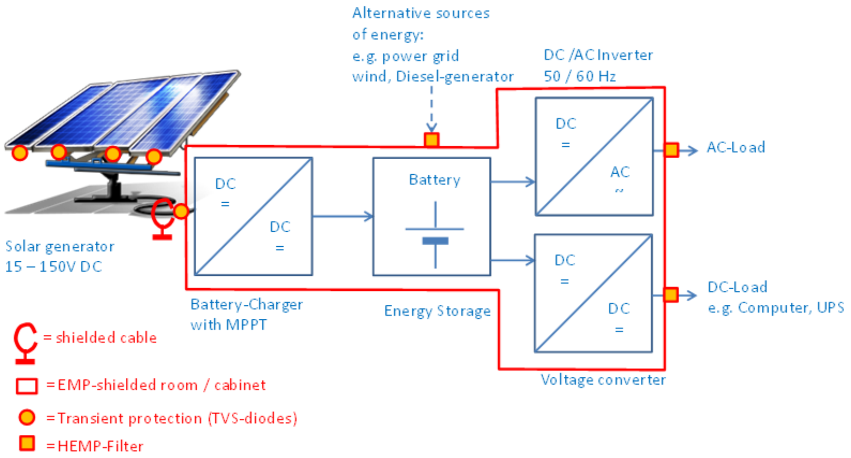


Figure 9: Transient voltage suppressors on modules and integral shielding enclosure of control system

6 CONCLUSIONS

The vision of having an independent emergency electrical energy distribution network for a part of the fixed critical infrastructure of the Swiss Army only makes sense, if acknowledged martial threats are conquered without function loss. Therefore, it was the goal to prove that PV-generators might be hardened against HPEM disturbances. Experiments have shown that photovoltaic cells and strings of cells in form of modules are strongly resistant against radiated intentional electromagnetic interferences (IEMI). Connected cables allow induction of overvoltage which endangers modules or bypass-diodes by flashovers when applied in reverse direction because these components are the weakest parts. By using shielded module connection cables and TVS diodes antiparallel to the bypass-diodes the whole PV-generator might be hardened at reasonable cost, assuming that the other subsystems (controller, converter, batteries) and their interconnections are also protected by well-known protection measures.

REFERENCES

[1] IEC 61000-2-9:1996, Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance

[2] IEC 61000-4-2:2008, Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test

[3] IEC 61000-4-5:2014, Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test

[4] MIL-STD-188-125-1:1998, High-altitude electromagnetic pulse (HEMP) protection for ground-based C4I facilities performing critical time-urgent missions, part 1, fixed facilities

[5] MIL-STD-461G: 2015, Requirements for the control of electromagnetic interference characteristics of subsystems and equipment, RS105

TWITTER SENTIMENT ANALYSIS FOR GERMAN FOOTBALL MATCHES

Désirée Hilbring[1], Jürgen Moßgraber[2], Manfred Schenk[3] and Joshua Link[4]

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

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

[3] *manfred.schenk@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[4] *joshua.link@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation,
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

Abstract

Football is the most famous sport in Germany. Therefore, football matches itself and incidents around the organization of football events are main topics in the media. The stakeholders involved in the organization ('Organizers Group') of football events like clubs, public transportation services, police authorities, private security services and town councils are interested in improving the football events for the 'Consuming Group' (supporters, other spectators in the stadium and TV spectators). To come up with improvements understanding the needs and emotions of the spectator group is essential.

This research paper concentrates on methods for a Sentiment Analysis of tweets in German language posted on Twitter before, during and after football matches to find out the needs and emotions of the 'Consuming Group'. The paper describes and evaluates methodologies for the creation of a database for football tweets, the creation of a German Football Event Vocabulary and a Sentiment Analysis of Football Matches using the database and the vocabulary.

Keywords: twitter, sentiment analysis, football.

1 INTRODUCTION

In the football season 2013/2014, about 13 million people attended the matches of the German Bundesliga (first league)[1]. The games of the second, third and lower leagues were attended by several additional millions of spectators. On their journey to the stadium and back home, they travel through crowded urban regions and depend on using the local infrastructures. In order to implement such big football events a cooperation of police forces, local town councils, football clubs and private security services is necessary to provide a safe and secure environment. Together with spectators and supporter groups, these stakeholders strive for peaceful and positive sport events. The purpose of the research of this paper was to analyze the needs and

[1] http://www.kicker.de/news/fussball/bundesliga/spieltag/1-bundesliga/zuschauer-geschichte.htm, visited in February 2015

emotions of the ‘Consumers Group’ Group’ (supporters, other spectators in the stadium and TV spectators) as base for improvements of the ‘Organizers Group’ (stakeholders of football events, like clubs, public transportation services and town councils). New media, such as Twitter, provide opportunities for flexible, timely and rapid publication of opinions and discussions for the ‘Consumers Group’. Therefore, tweets posted on Twitter related to Bundesliga matches serve as basis to our sentiment analysis.

2 RELATED WORK

Regarding the research field of football and Twitter we are aware of only one study analyzing the usage of Twitter for marketing and fan communication [1]. This study collected Twitter data for an entire Bundesliga season. It focused on the identification of official Twitter accounts of Bundesliga clubs for data collection. Therefore, their research concentrates on the perspective of the club. In contrast, we collected our sample data concerning specific Bundesliga matches via hash tags. Our goal was not to realize an entire study, but to research possible software solutions for the execution of such studies like the one of Weller and Bruns.

More technical research is taking place in the field of football and its stakeholders. “Modelling of an Ontology for a Communication Platform” describes a new ontology in the context of a football event [2].

Dodds et al. researched “Temporal Patterns of Happiness and Information in a Global Social Network: Hedonometrics and Twitter” [3]. Their objective was to do a Sentiment Analysis on Twitter data. The same principles are applied in the section “Creation of a German Football Event Vocabulary for Sentiment Analysis” as their “Algorithm for Hedonometer”. They did the base work with Twitter data from 4.6 billion expressions sampled in 33 month. This cannot be compared to our dataset, which is small, domain specific and based on the German language. That is why we focus in the following on the publication of Remus et al. [4]. However, the paper of Dodds et al shows that these principles are suited for Sentiment Analysis.

Remus et al. describe in “Senti-WS – a Publicly Available German-language Resource for Sentiment Analysis” how they created a German-language Resource for Sentiment Analysis using the Pointwise Mutual Information algorithm [4]. The work described in the section “Creation of a German Football Event Vocabulary for Sentiment Analysis” is based on this paper. The resulting vocabulary Senti-WS “contains 1650 negative and 1818 positive words”. It is freely available and used by us in the evaluation section[2].

Furthermore the paper “Normalized (Pointwise) Mutual Information in Collocation Extraction” from Bouma, which discusses normalized variants of pointwise mutual information is of interest [5].

3 BASE OF DATA FOR GERMAN FOOTBALL SENTIMENT ANALYSIS

The first goal was the creation of a database containing football related tweets. The database should contain tweets because the characteristic of tweets differ heavily from normal running texts[3]. Additionally the tweets must have a relation to Bundesliga matches. This database is used later on as base for two tasks:

- The creation of a German Football Event Vocabulary
- The Twitter Sentiment Analysis of Bundesliga Matches

[2] http://asv.informatik.uni-leipzig.de/download/

[3] https://www.wired.de/collection/life/wie-sich-twitter-sprache-verschiedenen-sozialen-situationen-aussert

The questions to be solved were the following:

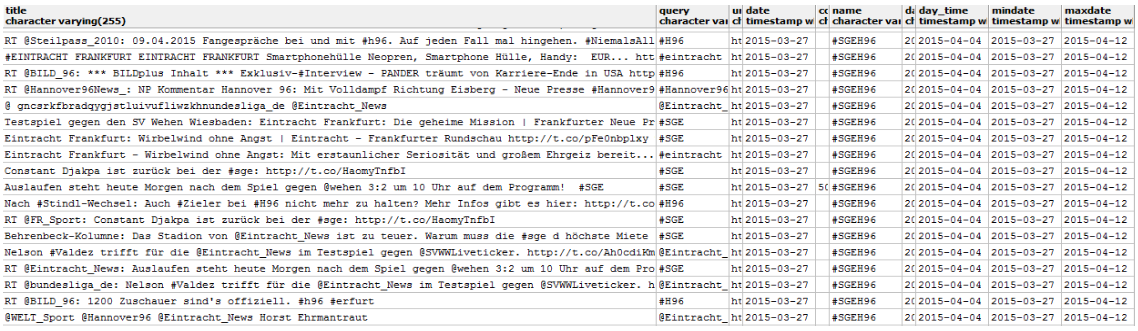
- How the database does needs to be structured?
- How can the appropriate tweets be filtered from Twitter?

Since data about Bundesliga matches needs to be stored, the decision was to structure the database per match. Each match is identified uniquely by the combination of club names together with the day and time of the match. A hashtag system Twitter presented for identification of Bundesliga matches in 2012 was reused for this purpose[4]. Each club is identified by a hashtag with three characters. To identify a match two of these hashtags are combined starting with the home team followed by the guest team. E.g. #SGEH96 is the hashtag for a match "Eintracht Frankfurt" against "Hannover 96". The database saves tweets related to matches using these hashtags combined with day and time of the match.

To filter appropriate Tweets from Twitter for a specific match the following method was used:

- The combined club hashtags are used as search terms.
- Only tweets, which have been posted in a time interval of 8 days before the match and 8 days after the match are relevant.
- For each club the user has the possibility to add further search terms to a list. It is possible to add club nicknames, Twitter accounts of clubs, etc.

Of course depending on the additional search terms irrelevant tweets might be stored. Therefore tweets are stored together with the search term in our database. This will be useful in future for customized in-depth analyses. Fig. 1 shows some examples.



title character varying(255)	query character var	ur ch	date timestamp wi	cc ch	name character var	da ch	day_time timestamp wi	mindate timestamp wi	maxdate timestamp wi
RT @Steilpass_2010: 09.04.2015 Fangesprāche bei und mit #h96. Auf jeden Fall mal hingehen. #NiemalsAll	#H96	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
#EINTRACHT FRANKFURT EINTRACHT FRANKFURT Smartphonehülle Neopren, Smartphone Hülle, Handy: EUR... htt	#eintracht	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
RT @BILD_96: *** BILDplus Inhalt *** Exklusiv-#Interview - PANDER träumt von Karriere-Ende in USA http	#H96	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
RT @Hannover96News_: NP Kommentar Hannover 96: Mit Volldampf Richtung Eisberg - Neue Presse #Hannover9	#Hannover96	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
@ gncsrkfbradqygjstluivufliwzkhnundesliga_de @Eintracht_News	@Eintracht_	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Testspiel gegen den SV Wehen Wiesbaden: Eintracht Frankfurt: Die geheime Mission | Frankfurter Neue Pr	#SGE	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Eintracht Frankfurt: Wirbelwind ohne Angst | Eintracht - Frankfurter Rundschau http://t.co/pFe0nbplxy	#SGE	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Eintracht Frankfurt - Wirbelwind ohne Angst: Mit erstaunlicher Seriosität und großem Ehrgeiz bereit...	#eintracht	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Constant Djakpa ist zurück bei der #sge: http://t.co/HaomyTnfbI	#SGE	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Auslaufen steht heute Morgen nach dem Spiel gegen @wehen 3:2 um 10 Uhr auf dem Programm! #SGE	#SGE	ht	2015-03-27	5(	#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Nach #Stindl-Wechsel: Auch #Zieler bei #H96 nicht mehr zu halten? Mehr Infos gibt es hier: http://t.co	#H96	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
RT @FR_Sport: Constant Djakpa ist zurück bei der #sge: http://t.co/HaomyTnfbI	#SGE	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Behrenbeck-Kolumne: Das Stadion von @Eintracht_News ist zu teuer. Warum muss die #sge d höchste Miete	#SGE	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
Nelson #Valdez trifft für die @Eintracht_News im Testspiel gegen @SVWWLiveticker. http://t.co/Ah0cdiKm	@Eintracht_	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
RT @Eintracht_News: Auslaufen steht heute Morgen nach dem Spiel gegen @wehen 3:2 um 10 Uhr auf dem Pro	#SGE	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
RT @bundesliga_de: Nelson #Valdez trifft für die @Eintracht_News im Testspiel gegen @SVWWLiveticker. h	@Eintracht_	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
RT @BILD_96: 1200 Zuschauer sind's offiziell. #h96 #erfurt	#H96	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12
@WELT_Sport @Hannover96 @Eintracht_News Horst Ehrmantraut	@Eintracht_	ht	2015-03-27		#SGEH96	2(	2015-04-04	2015-03-27	2015-04-12

Figure 1: Structure of stored tweets.

4 CREATION OF A GERMAN FOOTBALL EVENT VOCABULARY

The existing German vocabulary for Sentiment Analysis (Senti-WS) does not contain terms related to football. Additionally, the creators did not provide the source materials, which have been used for the creation of Senti-WS [4]. Therefore a new rated vocabulary for a working Sentiment Analysis of Bundesliga Matches was required. The decision was to follow the methods of Senti-WS and to normalize the results with the method of the paper of Bouma and adapt them to a data store filled with Football tweets [5]. Both papers use the Pointwise Mutual Information (PMI) algorithm:

$$(1) PMI(w1, w2) = log2\left(\frac{P(w1\&w2)}{(P(w1) * P(w2)}\right)$$

"P(w1) is the probability that w1 occurs, respectively P(w2) is the probability the w2 occurs and P(w1&w2) is the probability that w1 and w1 occurs in sentences of a

[4] https://blog.twitter.com/de/2012/twitter-und-fussball

language corpus." The language corpus is the data base filled with tweets and since tweets are often fragmented and do not contain correct sentences one tweet has been defined as representation of one sentence. To find out the strength of a semantic association between words in a sentence seed words, which are either clearly positive or clearly negative are needed. The seed words presented by Remus et al. have been adapted and some slang terms have been introduced, because football tweets often contain common speech.

Positive Seeds (DE) = geil, schön, glücklich, erst-klassig, großartig, ausgezeichnet, toll, gut, phantastisch, gewinnen

Negative Seeds (DE) = schlecht, unschön, falsch, unglücklich, zweitklassig, negativ, scheisse, minderwertig, verpfiffen, böse, mies

The second goal was to create normalized rating values for each term, since they shall be used to calculate the entire mood of a match. Bouma led to the following formula, which has been used for the calculation of normalized positive and negative PMI values [5]:

$$(2)\ counter = {}^{\log \frac{Ps\&Pr}{Ps * Pr}}\Big/_{\log(2)}$$

$$(3)\ denominator = -\frac{\log(Ps\&Pr)}{\log(2)}$$

$$(4)\ PMI = \frac{counter}{denominator}$$

Ps represents seed words. It means the seed word is occurring in a tweet. Pr represents words, which shall be rated. That means the word to be rated is occurring in a tweet. Ps&Pr are the occurrences of both, the seed word and the word to be rated, in a tweet.

Afterwards the semantic orientation of Remus et. al. has been followed: "The semantic orientation SO of a given word w is calculated from the strength of its association A with a manually-selected set of positive seed words P minus the strength of its association with a set of negative seed words N"[4]. The PMI is calculated for a word to be rated for every negative and every positive seed word. Then the sums for the negatively and positively rated words are taken. The rating result for the word to be rated is the difference between the positive and negative sum:

$$(5)\ Rating\ result\ of\ word = \sum PMIpos - \sum PMIneg$$

Fig. 2 shows some examples of football related words, which have been rated by this approach. The classification is sometimes interesting: "Angreifen" for example is the German word for "to attack". In a normal context one would expect a negative association. However in the context of a football match "to attack" gets a positive rating, because attacking the opposing team leads to an active match and positive feelings of the spectators. This shows that for a Sentiment Analysis based on rated vocabulary it is important that the vocabulary takes into account the specific needs of the topic to be analyzed.

Term	Rating
Polizei (police)	-0,029
Rauch (smoke)	-0,022
angreifen (to attack)	0,005
aggressive (aggressive)	0,009
singen (to sing)	0,003

Fig 2: Examples of rated terms

5 METHODOLOGY OF TWITTER SENTIMENT ANALYSIS

Having completed the Football Vocabulary it could be used for the Sentiment Analysis of Football Matches. The developed Sentiment Analysis workflow use the following variables:

- “suchwort” (e.g. “Abstieg”): the search term. The possibility to search for specific words in the Twitter database is provided.
- „ereignis“ (e.g. #VFBSGE): the event variable limits the number of tweets to be analyzed for a specific event. In the football context the event is a specific match between two football clubs.
- „analyseZeitraumUmEreignis“ (e.g. 3TageBisAnpfiff): another variable defines different analysis time intervals around the event. Usually the time before, during and after an event are of interest. In the football data base the following time intervals have been defined:
    - „Bis 3 Tage vor Spieltag“ (8-3 days before the event)
    - „3 Tage bis Anpfiff“ (three days before event)
    - „Erste Halbzeit“ (first half)
    - „Halbzeitpause“ (half time break)
    - „Zweite Halbzeit“ (second half)
    - „Schlusspfiff bis 5 Tage danach“ (until 5 days after the event)
- „analyseZeitraumFix” (e.g. 2015-03-14T00:04:24.0;2015-03-20T00:00:00.0) is the alternative for the analyseZeitraumUmEreignis variable. The user can define a time interval of interest directly.
- „zielVerzeichnis“ (e.g. C:\AnalysisResults): this variable defines the places to store the analysis results.

The following steps are executed in the created workflow. The “German fast” tagger model of the Stanford tagger has been used to tag the tweets und break them into terms. The workflow then combines the remaining words with our German Football Event Vocabulary and the positively or negatively rated words for the analyzed event of the workflow are identified. The resulting dataset is used to create the following kinds of results:

Firstly, one tag cloud is created containing all remaining words of the event without considering the rating step of the algorithm. This tag cloud is useful for analyzing results of specific searches via “suchwort”.

Secondly, one Tag Cloud is created containing all negative words, identified via our German Football Event Vocabulary.

Thirdly, one Tag Cloud is created containing all positive words, identified via our German Football Event Vocabulary.

Fourthly, the rated vocabulary is used to derive a single rating value for the analyzed time interval of the event. The goal was to create a normalized mood number between -1 and 1.

$posr = positively\ rated\ words\ of\ analyzed\ tweets$

$negr = negatively\ rated\ words\ of\ analyzed\ tweets$

$$(6) Mood\ result = \frac{\sum posr}{row\ count} + \frac{\sum negr}{row\ count}$$

$Values\ > \ 1\ are\ positive, values\ < \ 1\ are\ negative.$

6 EVALUATION OF THE SENTIMENT ANALYSIS

The implementation of the methods for the creation of a data base for German Football Sentiment Analysis, for the creation of a German Football Event Vocabulary and for the Sentiment Analysis was performed with sampled data from a number of matches in winter of the Bundesliga Season 2014/2015.

6.1 Evaluation of Data Base

Currently around 450000 tweets are stored in the data base. However, only 10000 of them use the combined club hashtags, which clearly identify a specific match. This means the current data store was sufficient for the development of methodologies but for real analyses we propose to sample data for all matches of an entire Bundesliga Season. Therefore, the following can only be a first basic evaluation.

6.2 Evaluation of Football Event Vocabulary

The small size of the dataset was a problem for the creation of the German Football Event Vocabulary. To create a good Football Event Vocabulary many tweets covering all aspects of interests of a football match are necessary. Here are some example topics of interest: security issues (e.g. allowed and forbidden objects, police information), travel information (e.g. individual traffic problems, parking issues, delays of public transport), sport discussions, etc. Terms to be rated must be identified and rated with the algorithm for each topic. Currently the data base is just a proof of concept. It does not yet contain many tweets covering all proposed topics. Therefore it was difficult to rate terms, because terms to be rated often did not occur in the database or did not occur together with defined seed words. Currently only 680 words could be rated. This means the Football Event Vocabulary needs to be improved.

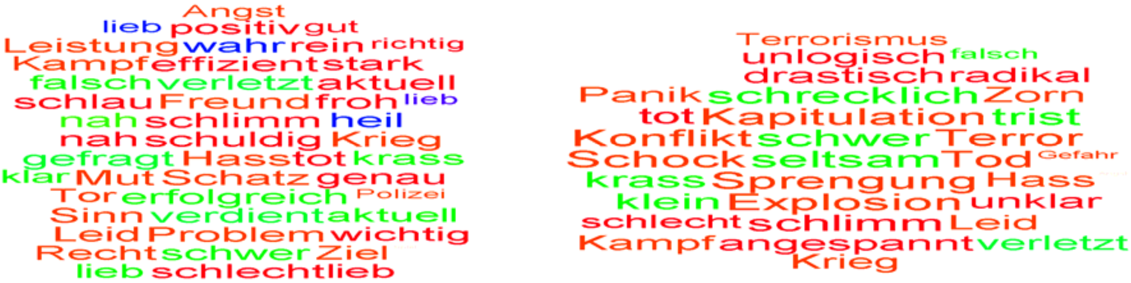


Figure 3: Negative Tag Clouds (left usage of Football Event Vocabulary; right usage of Senti-WS) from match GERNED, which has been cancelled because of security reasons, after the terror incidents in Paris.

Due to the recently happened terror incidents, we tested the transferability of the approach for analyzing security issues and therefore tried to analyze the football match Germany against Netherlands, which has been cancelled shortly before the beginning of the match because of urgent security reasons. The negative tag cloud created with tweets originated after the cancellation with the Football Event Vocabulary shows new terms like “Krieg” (war) or “tot” (death), which we do not find usually in Tag Clouds from Football matches (see Fig. 3 left side). We also did the analysis with Senti-WS (see Fig. 3 right side). One can see, that the rating values of Senti-WS are more suitable. Thus for a good sentiment analysis of different topics fitting vocabularies are essential.

6.3 Evaluation of Sentiment Analysis

A test Sentiment Analysis for the match “Eintracht Frankfurt” against “Hannover 96” has been performed. Fig. 4 shows a comparison of the mood results for the different analysis intervals of the match data. The analysis has been created with both vocabularies the Senti-WS and the Football Event Vocabulary.

Time Interval	Mood result with Senti-WS	Mood result with Football Event Vocabulary
8-3 days before event	0,001	-0,002
3 days before event	0,002	-0,002
First Half	-0,004	-0,003
Half Time Break	-0,001	-0,003
Second Half	-0,001	-0,005
Until 5 days after the event	0,001	-0,002

Figure 4: Comparison between Senti-WS and Football Event Vocabulary Mood Results of a match.

Firstly, looking at the mood results one can see, that the reduction of the Sentiment Analysis to one number is critical. It is difficult to derive a meaning from the results.

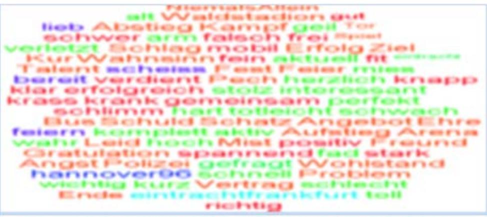
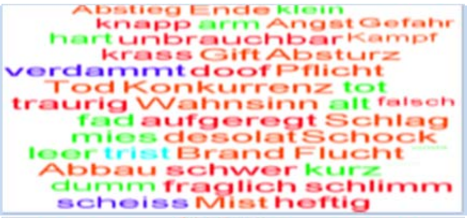
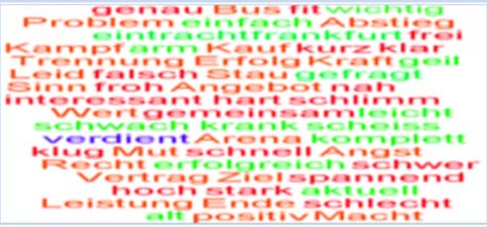
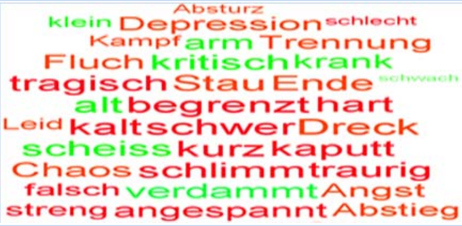
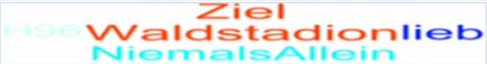
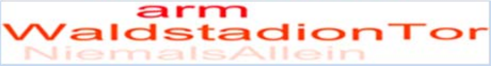
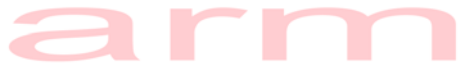
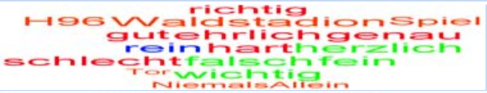
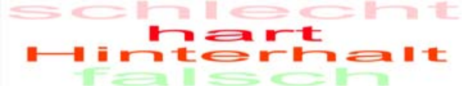
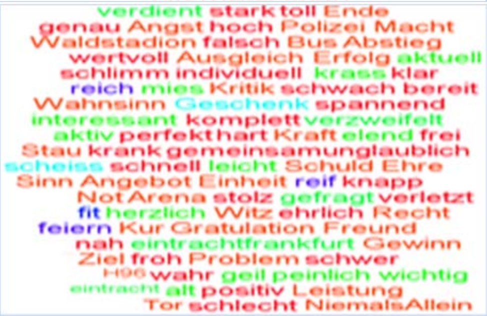
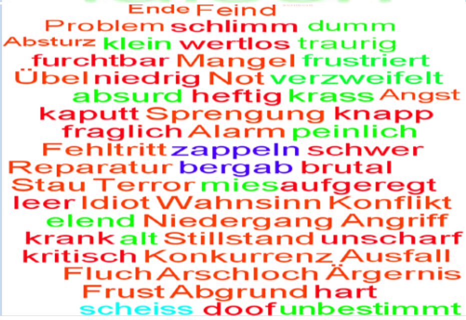
Time Interval	Football Vocabulary – Negative Tag Cloud	Senti-WS – Negative Tag Cloud
8-3 days before event		
3 days before event		
First Half		Not enough data
Half Time Break		
Second Half		
Until 5 days after the event		

Fig. 5: Resulting negative Tag Clouds of the match "Eintracht Frankfurt" against "Hannover 96"

The resulting tag clouds shown in Fig. 5 are more meaningful. Looking at the resulting negative tag clouds it is obvious that the mass of data in the intervals "First Half" "Half Time Break" and "Second Half" is insufficient. Not enough tweets could be assigned to these intervals. It makes no sense to derive mood results for these time intervals. Therefore a statistical measure must be developed for the Sentiment Analysis algorithm which includes checks for sufficient data in future. One can see also that the Football Vocabulary better suites the analysis, more issues can be identified: The tag clouds on the left contain for example the words police or bus and traffic jam. Thus, spectators might have had some trouble during the journey.

7 CONCLUSION

The work presented in this paper shows, that it is possible to use Twitter as a base for a Sentiment Analysis in the Football Domain. Twitter data related to specific Football matches has been sampled. Methodologies were developed for the creation of a German Football Vocabulary and for a Sentiment Analysis utilizing that vocabulary.

Different Tag Clouds show negative or positive terms connected to the match. The current evaluation led us to the conclusion that the resulting Tag Clouds provide promising user readable analysis results. In contrast, the evaluation showed that the reduction of the data in the analysis to derive a single value rating (the mood result) is critical.

Additionally our evaluation showed that different vocabularies are needed for different analysis topics. Therefore, we propose to create a set of search terms for each topic and collect Twitter data independent from specific matches to serve as a data base for the creation of a specific vocabulary. For example, while the Football Event Vocabulary supports the analysis of the process of the match, searching Twitter for security issues will serve as a basis for the creation of a Security Vocabulary.

Afterwards it will be possible to support the Organizers Group in understanding the needs of the Consuming Group. Depending on the analysis topic (e.g. process of the game, marketing, ticketing, issues concerning public and private transport, security, popularity of stadiums, etc.) a Sentiment Analysis of a Football match can be performed with the corresponding vocabulary.

8 ACKNOWLEDGEMENT

This work has been financed by the German research project “Mehr Sicherheit im Fußball – Verbessern der Kommunikationsstrukturen und Optimieren des Fandialogs” which is funded by the German Ministry of Education and Research (BMBF) [6].

REFERENCES

[1] Weller, K., Bruns, A. (2013), Das Spiel dauert 140 Zeichen – Wie deutsche Fußballvereine Twitter für Marketing und Fankommunikation entdecken, HIER 2013, Proceedings des 8. Hildesheimer Evaluierungs und Retrievalworkshops

[2] Moßgraber, J., Schenk, M., Hilbring, D., Modelling of an Ontology for a Communication Platform, Proceedings of SEMAPRO 2015; The Ninth International Conference on Advances in Semantic Processing, Nice, France

[3] Dodds, P.S., Harris, K. D., Kloumann I. M., Bliss C.A., Danforth C.M, 2011, Temporal Patterns of Happiness and Information in a Global Social Network: Hedonometrics and Twitter, Open Access, http://www.uvm.edu/~pdodds/research/papers/files/2011/dodds2011e.pdf, visited in December 2015

[4] Remus, R., Quasthoff, U., Heyer, G. Senti-WS – a Publicly Available German – language Resource for Sentiment Analysis, http://asv.informatik.uni-leipzig.de/publication/file/155/490_Paper.pdf, visited in May 2015

[5] Bouma, G.,Normalized (Pointwise) Mutual Information in Collocation Extraction, https://svn.spraakdata.gu.se/repos/gerlof/pub/www/Docs/npmi-pfd.pdf , visited in May 2015

[6] Moßgraber, J., Kubera, T., Werner, A. 2014, More Safety for Football Events: Improving the Communication of Stakeholders and the Dialogue with Supporters, Proceedings of the Future Security 2014, Berlin, Germany

LEARNING FROM PAST DISASTERS TO IMPROVE CRISIS MANAGEMENT

Roman Grüner[1], Carsten Dalaff[1], Georg Neubauer[2], Alexander Preinerstorfer[2], Gerald Lichtenegger[3], Wolfgang Vorraber[3] and Uberto Delprato[4]

[1] Roman.Gruener@dlr.de, [1]Carsten.Dalaff@dlr.de
DLR German Aerospace Center, Institute of Transportation Systems, Rutherfordstr. 2, 12489 Berlin (Germany)

[2] Georg.Neubauer@ait.ac.at, [2]Alexander.Preinerstorfer@ait.ac.at
AIT Austrian Institute of Technology GmbH, Digital Safety & Security,
Donau-City-Str. 1, 1220 Vienna (Austria)

[3] Gerald.Lichtenegger@tugraz.at, [3] Wolfgang.Vorraber@tugraz.at
Graz University of Technology, Institute of Engineering and Business Informatics,
Kopernikusgasse 24/III, 8010 Graz (Austria)

[4] U.Delprato@i4es.it
IES Solutions srl, Via Monte Senario 98, 00141 Roma (Italy)

Abstract

In the event of a disaster the coordinated response of emergency services is crucial for saving lives and protecting critical infrastructure. Efficient communication and access to relevant information are essential elements in the immediate aftermath and all phases of the crisis management cycle to maintain public safety. As part of the European Commission funded FP7 project EPISECC (Establish Pan-European Information Space to Enhance Security of Citizens), an inventory of past disasters and critical events was developed. Information was obtained by systematic interviews with experts active in the field of crisis and disaster management on both national and international level. They represent organisations such as first responders, emergency services and civil protection offices from 15 EU (European Union) countries. The paper will outline several aspects such as the quality of information exchange between crisis managers and the analysis of key recommendations for improvement identified during the management of past disasters.

Keywords: Crisis and Disaster Management, Critical Infrastructure, Emergency Services, Cross-Border Cooperation

1 INTRODUCTION

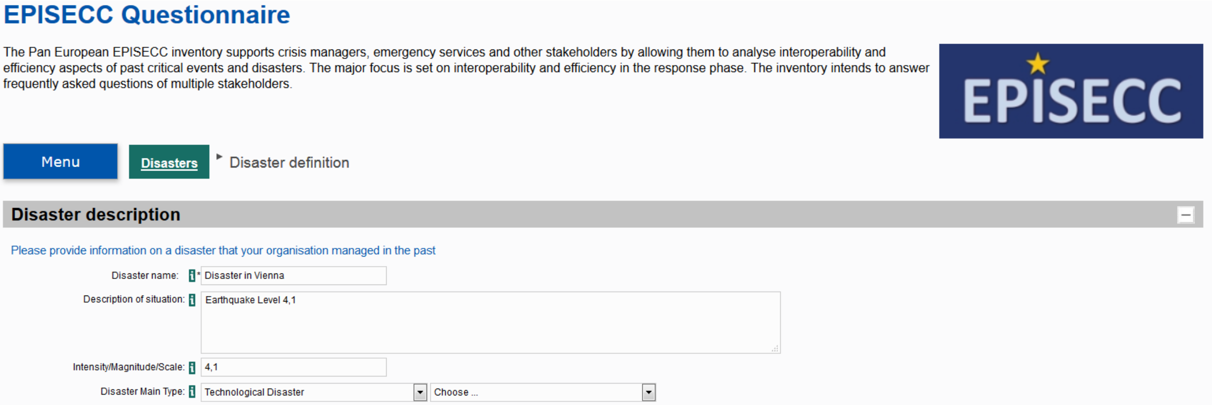
When a disaster strikes the possibility of exchanging information is vital for a successful management and to prepare, coordinate and dispatch the necessary resources. However, if events such as floodings, forest fires or earthquakes occur, the capabilities of communication and information are either interrupted or stretched to their limits due to wide scale destruction of critical infrastructure such as the transport, electricity or telecommunication networks. A successful management of the post-disaster phase depends on the reestablishment of communication channels between relevant emergency services and on their ability to work together. In particular the sharing of information, the ability to effectively communicate and an informed understanding of the exact content of exchanged messages are crucial when reacting to disasters. This is a particular challenge in cross-border events where stakeholders and their systems must be able to communicate effectively [1].

In order to collect information about past critical events and disasters the EPISECC inventory was developed consisting of a questionnaire, a database and a data analysis module. Altogether 49 interviews with various stakeholders in crisis and disaster management were carried out. These interviews were the basis for an in-depth data analysis and enabled the identification of areas of improvement to enhance disaster assessment and to leverage the preparation of disaster managers for future events. During the interviewing process a variety of information on standards, guidelines, recommendations, IT tools, processes and data sources of organisations involved in crisis and disaster management across Europe was collected. Based on the analysis of the inventory data the paper will outline several aspects such as (i) the role of critical infrastructure, (ii) interoperability (including quality) of information exchange between European crisis managers, (iii) individual responses from stakeholders on what would have helped in previous disasters and (iv) recommendations for improvements identified by studying the management of past disasters.

2 METHODOLOGY

2.1 Establishment of EPISECC inventory

The implementation of the EPISECC inventory was based on an already existing framework of AIT Austrian Institute of Technology EMIKAT [2] which is used in Austria for analysing emission data since many years. This framework has the ability to integrate data models of various domains. Therefore, it was possible to include the developed EPISECC inventory data model into the AIT framework and create the EPISECC questionnaire from that input (Fig. 1).



EPISECC Questionnaire

The Pan European EPISECC inventory supports crisis managers, emergency services and other stakeholders by allowing them to analyse interoperability and efficiency aspects of past critical events and disasters. The major focus is set on interoperability and efficiency in the response phase. The inventory intends to answer frequently asked questions of multiple stakeholders.

Disaster description

Please provide information on a disaster that your organisation managed in the past

Disaster name: * Disaster in Vienna

Description of situation: Earthquake Level 4,1

Intensity/Magnitude/Scale: 4,1

Disaster Main Type: Technological Disaster | Choose ...

Figure 1: Extract from the EPISECC Questionnaire

The interviewed experts can enter available information about data from various categories such as the description of the past disasters. The inputs of these fields can be combined and compared with information from other interviews in an anonymised way. After applying the data analysis module the general results and the combinations of these fields can be made available via graphs or tables (Fig. 4).

2.2 Interview process

To gather the necessary information from actors involved in crisis and disaster management, it was necessary to interview stakeholders about the management of past critical events and disasters with an electronic questionnaire. This process of interviewing was carried out by the members of the EPISECC consortium with personal interviews, in person or by phone. The questions cover a broad variety of issues in disaster management and included information on the interviewee, the organisation and the specific disaster in which he was involved. The respondents were asked about topics such as processes used, standards applied, data resources used, cooperation with other organisations and interoperability in disaster relief actions. The questionnaire was designed in such a way to gather as much information as possible from various kinds of organisations working on strategic, tactical and operational level. Currently, 49 representatives from various organisations in the field of crisis and disaster management were interviewed.

3 RESULTS

3.1 General Results of Inventory

The respondents represent a wide range of stakeholders of which the vast majority of 78 % categorized themselves as government organisations, 14 % as NGOs and the rest as other organisations. According to the type of organisation (Fig. 2) 35 % are active in the area of Civil Protection on different governmental levels. Federal Ministries account for 18% of which a big majority are the ministries of the interior responsible for disaster management in most countries. Equally important are the Fire Services with 18 % followed by Emergency Medical Services with 12 % and the Police with 8 %. The remaining 8 % belong to the category of Other which include Armed Forces, UN (United Nation) organisations or other government agencies.

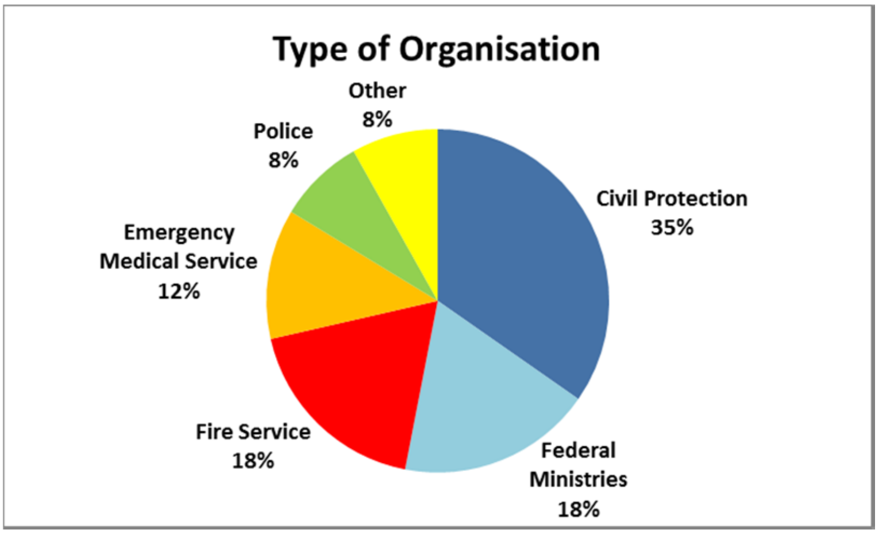


Figure 2: Type of interviewed organisation

The interviewed representatives cover a variety of organisations from 15 EU countries plus Switzerland, Norway and Israel. A considerable share of 63% of the interviews was conducted in four countries (Austria, Italy, Croatia and Germany). Due to the different governmental structures and responsibilities within these countries (federal vs. centralized systems) the balance within the survey was still maintained.

With regard to the type of disasters, the majority consist of extreme weather events and cascading effects which are common throughout many parts of Europe. The biggest natural disasters are Floodings with 28 % of all events. Landslides are closely related to floods as a cascading effect and account for another 9%. Furthermore, major Fires are the second largest category with 14 % of which the vast majority are forest fires. In addition, events related to the current Migration of refugees are equally important with 14 %. Earthquakes account for 12 % and disasters related to Snow/Ice (e.g. snowstorms or sleet) for 7%. The category of Other accounts for 16 %, which includes a large variety of events such as plane crash, traffic accident and blackout (Fig. 3).

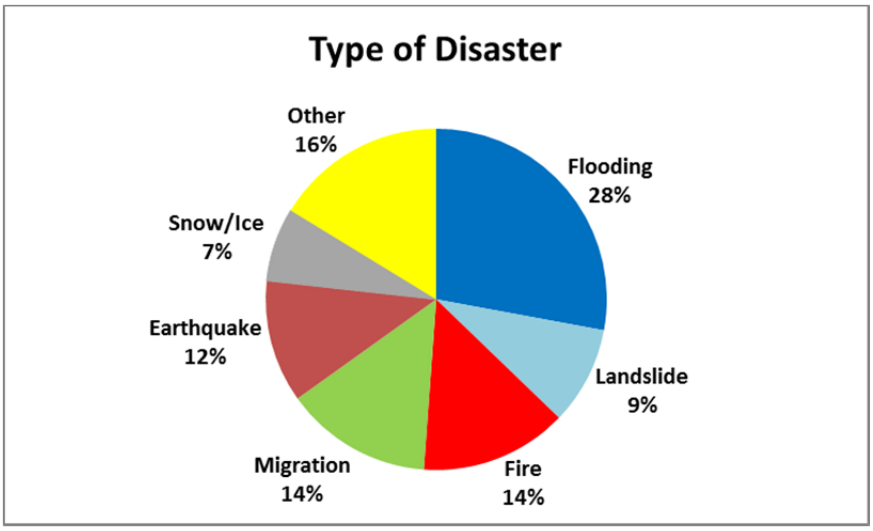


Figure 3: Type of Disasters

3.2 Critical Infrastructure

In case of a large-scale disaster, Critical Infrastructure is very often affected by the destructions caused with negative impacts on the population. This is also reflected in the results of the inventory. From a total of 45 entries to different types of disasters, infrastructure was affected 37 times. As provided in [2] Transportation was mostly affected in 92 % of all cases. In the second place Energy Supply was affected with 62% followed by Communication with 60 %. Health Infrastructure reached a probability of 35 %. The category of Other included 43 % of which damage to Buildings (44 %) and Water Supply (35%) were mostly named. If the different disasters are analysed by category (Hydrological, Geological, Climatological, Technological and Complex) Transportation dominates as most affected infrastructure [3].

It is interesting to notice that impacts on some Infrastructures seem to be related. If Health (HE) is affected the same applies to Communication (COM) in 93 % of all cases. A similar result can be observed by analysing the combination of Transport (TR), Communication and Health. In this case the probability of combined impacts reaches 91 %. If Energy (EN) is included the likelihood of all four infrastructures being affected is 77 % (Fig. 4).

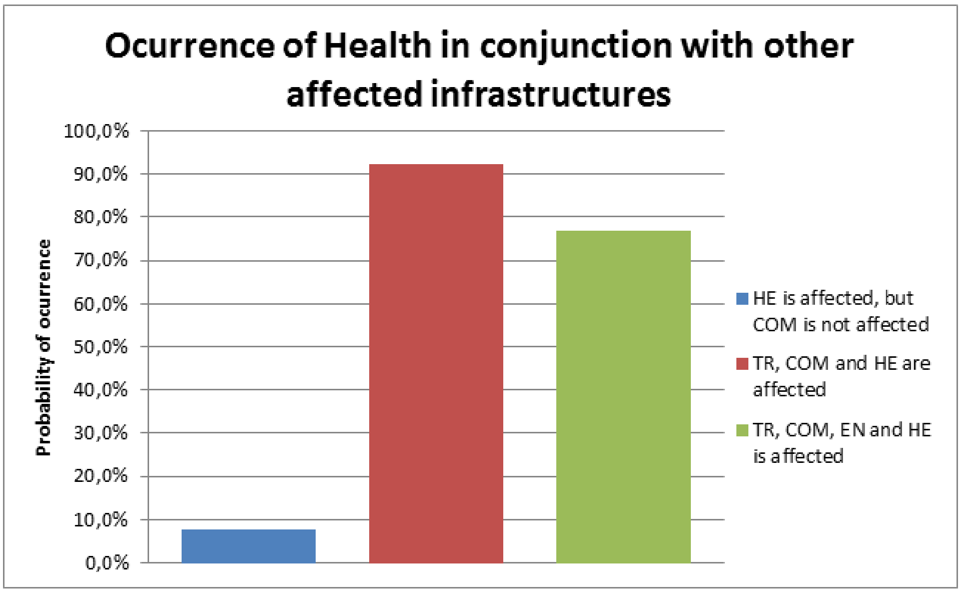


Figure 4: Combinations of Affected Infrastructures

The damage or destruction of infrastructure during a disaster has an impact on the fast and efficient operation of emergency services to provide assistance to the affected population. The quick rehabilitation of infrastructure plays a major role for successful crisis management.

3.3 Interoperability of Information Exchange

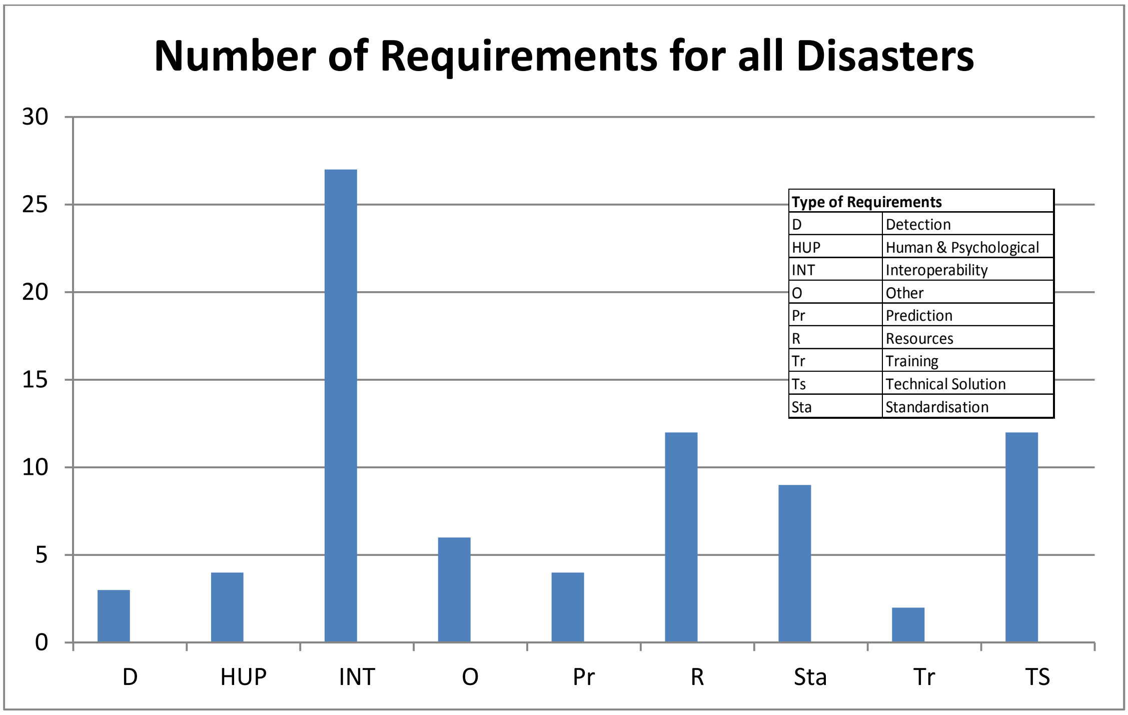
One main focus of the inventory was the establishment of methods to measure the quality of information exchange. For this purpose a key indicator for information interoperability was developed. In the following the main parameters of the indicator will be described briefly. A detailed description of the indicator can be found in [3]. The indicator can reach values between 0 (worst case, no information exchange) and 1 (excellent information exchange). The indicator consists of four parameters:

1. The time to establish a channel to communicate
2. The time required to communicate
3. The amount of data that was exchanged
4. The amount of data that was understood

All four values are normalized: DATA to the ideal amount of data exchanged or understood and TIME to the maximum acceptable time. The average indicator value of more than 160 analysed processes is 0.79 - a value that can be considered to be quite good. Only 7% of the indicators were below 0.50 showing that the majority of processes reached at least acceptable values. Nevertheless it turned out that stakeholders identified interoperability as a main requirement in order to improve disaster management (Section 3.4).

3.4 Individual Responses and Requirements from Stakeholders

The authors asked stakeholders for requirements that arose while managing past disasters and possible solutions and would have helped to improve the situation. In total 79 requirements were collected as indicated in Fig. 5.



Type of Requirements	
D	Detection
HUP	Human & Psychological
INT	Interoperability
O	Other
Pr	Prediction
R	Resources
Tr	Training
Ts	Technical Solution
Sta	Standardisation

Figure 5: Requirements to improve disaster management

It turned out that the predominant requirement is Interoperability (34%). Other requirements such as Resources or Technical Solutions reached considerably lower values of less than 15 %. When comparing requirements according to the types of disasters the patterns are slightly changing but Interoperability remains the predominant category.

4 DISCUSSION

Given the fact that by the time this paper was written a considerable number of interviews had been conducted with organisations from countries located in central and southern Europe one could argue that this geographical bias will limit the feasibility of drawing general conclusions for the entire European Union. When looking closer at the public and governmental structures, the crisis and disaster management systems in place, and the exposure and/or involvement to/in transnational crisis and disasters, this group of countries (Austria, Italy, Croatia and Germany) give a fairly good representation of the “European Situation”.

The at the first glance ambivalent results between the computed interoperability indicator (medium to good interoperability) and the strong need for further interoperability improvements stated by the interviewees also require further discussion. Despite the interoperability challenges with common ICT systems and the lack of unified semantics, stakeholders and actors in crisis and disaster management found their ways to bridge the gaps. One strategy is to bypass defined (suboptimal) process steps by informal ones. Another approach is to introduce human-activity-based process steps such as using dedicated peer-to-peer sharing of data/information via email, phone or other public available channels rather than relying on already available ICT systems. Furthermore, almost every interviewee has answered the questions related to interoperability in the context of his or her sphere of responsibility. Therefore, those people have a two-fold experience. On the one hand that the challenges of information interoperability might be handled very well in their limited environment for at least their own (sub) processes and on the other the entirety of the information exchange processes and thereby the overall system performance still suffer from effects caused by the absence or insufficient degree of interoperability in information exchange.

A detailed follow up analysis specifically focusing on the levels of interoperability may support a more detailed investigation of the reported interoperability requirements. Furthermore, these results may be compared to the research on interoperability levels of existing ICT tools for disaster management published in the EPISECC deliverable D2.1 “PPDR Information Space – Status quo of commercial, research and governmental projects and applications” [4] and in [1].

Apart from information exchange, the analysis of the type of affected infrastructures requires further attention. Independent of the type of disaster, transportation is the predominant affected infrastructure, potentially stressing the importance of optimized processes for resource provision. This is line with the second largest category of requests related to resources. Moreover, the interpretation of the combination of the affected infrastructures health, communication and energy needs further investigations. These results seem to indicate that the infrastructure health strongly depends on energy and communication.

5 OUTLOOK

The study carried out in the EPISECC project about a key indicator for information interoperability was tested on a good number of disaster situations across Europe. The developed inventory and the method implemented for adding content by questionnaires and interviews proved useful for both the practitioners and the researchers.

Since Information Interoperability has been recognised by practitioners and stakeholders as one of the major challenges in disaster management, there is plenty of scope for enlarging the inventory and refine the interoperability index, aiming at identifying both the elements in the communication chain that affect (positively and negatively) the understanding between authorities and the impact of new technological solutions and operational processes on disaster management.

The project is currently expanding the database of the inventory by performing further investigations. One focus is set on the current migration of refugees with focus on cross border information exchange as well as request of resources. Additional fields of application such as use of the inventory for analysing the way organisations managed past large scale accidents are currently investigated. Finally, the results of the inventory are used to improve the design of the Common Information Space developed in the frame of EPISECC.

The members of the EPISECC project evaluate the best course of action for making the inventory a living tool, available for being enriched with events from the past and updated with recent experiences and new solutions.

REFERENCES

[1] Hübner, K., Dalaff, C., Vorraber, W., Lichtenegger, G., Delprato, U., Neubauer, G., Preinerstorfer, A. (2015). Towards a Pan-European Information Space. *The 12th International Conference on Information Systems for Crisis Response and Management.* Kristiansand, Norway.

[2] EMIKAT - Emissionskataster, Weblink: http://www.emikat.at [accessed 02.06.2016]

[3] Neubauer, G., Preinerstorfer, A., Schirnhofer S., Humer H., Lichtenegger, G., Vorraber, W., Linke H., Tusa, G., Gruener, R., Dalaff, C., Knezic, S., Blaha, M. (2016). Validation of the Management of past Crisis and Disasters. *IDIMT 2016 – 24th Interdisciplinary Information and Management Talks.* Podebrady, Czech Republic.

[4] EPISECC Deliverable 2.1 – Public Protection and Disaster Relief (PPDR) Information Space – Status quo of commercial, research and governmental projects and applications, Weblink: https://episecc.eu/sites/default/files/EPISECC_WP2_D2.1_deliverable_final_1.pdf [accessed 02.06.206]

THE DESTRIERO PLATFORM FOR MULTI-HAZARD DISASTERS AND COMPLEX CRISES RECONSTRUCTION AND RECOVERY

Sandra Frings[1], Christian Knecht[2] and Michele Fiorini[3]

[1] *sandra.frings@iao.fraunhofer.de*
Fraunhofer Institute for Industrial Engineering (IAO), Information Management,
Nobelstrasse 12, 70569 Stuttgart (Germany)

[2] *christian.knecht@iao.fraunhofer.de*
Institute for Human Factors and Technology Management IAT of the University of
Stuttgart, Human-Computer Interaction,
Nobelstrasse 12, 70569 Stuttgart (Germany)

[3] *michele.fiorini@leonardocompany.com*
Leonardo - Finmeccanica S.p.A., Engineering Dept., Security & Information Systems
Division, Via Tiburtina km12.4,
00131 Roma (Italy)

Abstract

The EU funded project DESTRIERO[1] (a DEcision Support Tool for Reconstruction and recovery and for the IntEroperability of international Relief units in case Of complex crises situations, including CBRN contamination risks) covers the reconstruction and recovery phase after a disaster. It is delivering a platform prototype to collect information through the integration of information sources and third party systems as cooperation tool for reconstruction organizations. The project hypotheses are to improve planning for reconstruction projects through more accurate information from sensors as well as to improve decision making through aggregating information. The framework and its functionality are described herein and a live demo will be shown in the presentation at the conference.

Keywords: information/communication/cooperation platform, reconstruction and recovery phase, decision support for reconstruction projects, CBRN

1 INTRODUCTION AND STATE OF THE ART

In today's world, large natural disasters which have multi-hazard impacts including CBRN (Chemical, Biological, Radiological, and Nuclear) risks are unfortunately not uncommon due to either the increase density of humans activities that require more and more space and power (energy) or the lack of investment on maintenance and upgrade of old systems dated back to last century either civil (power stations) or military (nuclear defenses). It is on recent news that nuclear defenses are exposed to antiquated systems: “America's nuclear defenses rely on floppy discs and 1970s computers, according to audit” [2]. And the disaster at Fukushima (Japan, 2011) [3] or the Chernobyl catastrophe (Ukrainian, 1986) [4] are still in everybody's minds.

Such events impact different organizations from different countries who need to work together to create area and expertise related task plans which often need to be created ad hoc and as soon as possible after the damage event. In this phase it is important to find out what the situation in the affected area is. There is a need for different information types directed towards different first responder organizations deployed

[1] This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312721.

within the area of interest [5]. Due to the inability to recover a situation effectively by a single (local or even on national level) first response organization, the scale and the severity of the disaster might call for a wider crisis management. This would involve different organizations to act together in a synchronized scenario that should be coordinated by a CCM (collaborative crisis management) at international level often in accordance with over-national organization such as OCHA (Office for the Coordination of Humanitarian Affairs). The impact is huge on economic and social scale. It is estimated that the Sept. 11th terrorist attack in New York resulted in a cumulative loss (in terms of rebuilding) estimated at 105 billion US dollars [6].

The organizations deployed within the damaged area need to cooperate effectively in short time to avoid tasks overlapping on the same area. As a result it is of paramount importance to overcome the intrinsic heterogeneity (either technological or syntactic and semantical) of information and procedures belonging to the multiple crisis management organizations. The making use of DESTRIERO overcomes this obstacle by providing an information, communication and cooperation platform to be initiated at the start of the reconstruction and recovery phase.

The following chapters give an overview of the DESTRIERO project and platform (its scenario, use cases and functions) as well as of the usability tests and their evaluation.

2 THE PROJECT DESTRIERO

DESTRIERO aims to facilitate the knowledge of real time on-field situations offering a systematic, holistic, inter-governmental and multi-disciplinary approach to the collaboration of heterogeneous first responders when managing large-scale disasters [7]. The middleware platform prototype for crisis information systems was designed and developed to fit crisis management recovery and reconstruction needs to facilitate cross-border information exchange and to support decision makers in the selection and prioritization of the activities to be conducted on the field where the disaster has occurred. A schematic architecture is presented in Fig. 1.

One of the key priorities in case of a disaster is the possibility for heterogeneous and distributed legacy systems to share their information in a coordinate way interacting and cooperating with each other without interfering one another. This is possible by the means of the proper legacy interfaces (Adapter) and services available on the platform.

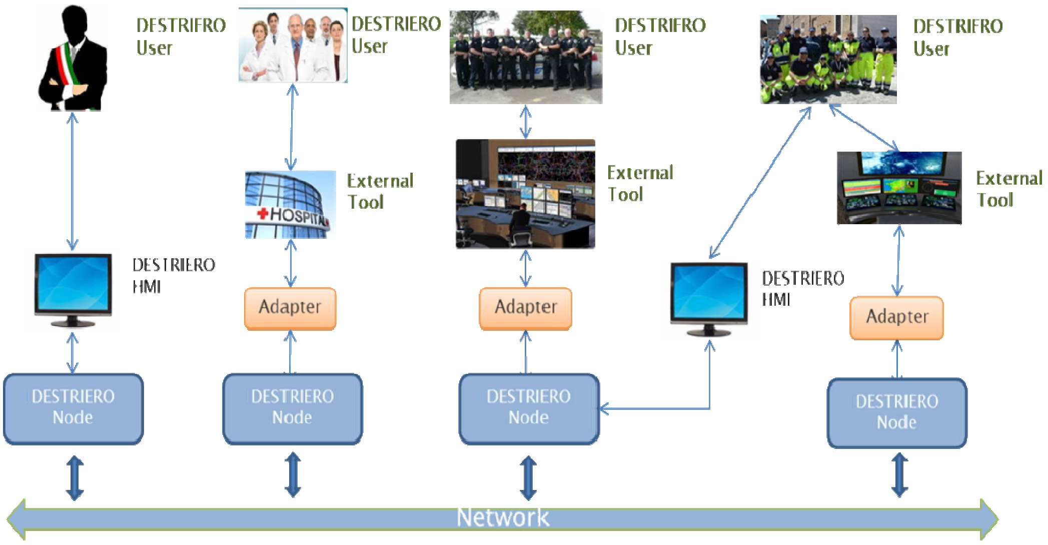


Fig. 1: Schematic representation of DESTRIERO deployment

The DESTRIERO platform is derived from the Leonardo - Finmeccanica experience on Mission Critical Systems such as Air Traffic Management [8] and Border Control and

Surveillance Systems [10]. It adopts a super-peer architecture so as to limit changes to legacy solutions, where a special node acts as gateway for the communications towards other systems.

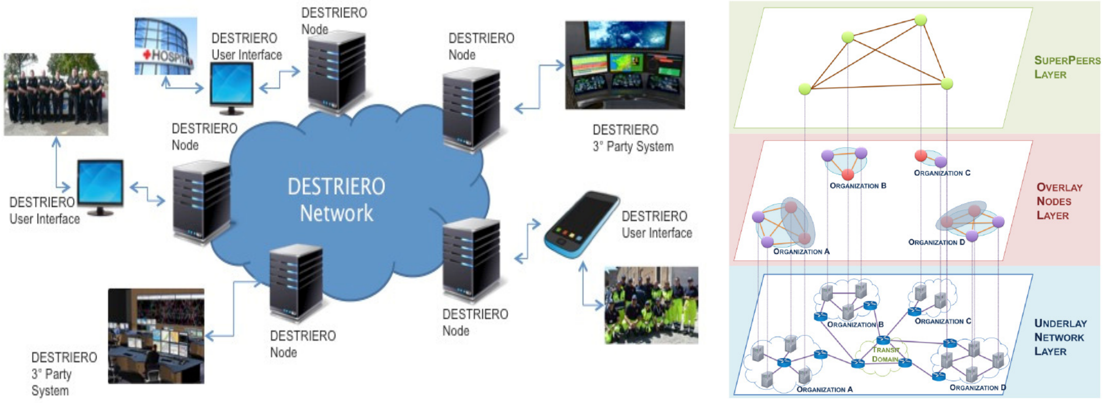


Fig. 2: The DESTRIERO network architecture proof of concept

3 DESTRIERO PLATFORM

The functionality of the platform – interface to the end user – was derived from end user needs which were collected in a requirements analysis; they were evaluated and prioritized. This process was necessary to differentiate between nice-to-have functions and really needed functions to reach the objectives of the projects.

From these requirements a scenario and specific use cases where defined. Research on and the selection of relevant information sources were performed as well as on relevant third party systems. In the next steps, the DESTRIERO platform architecture and its adapters and the HMI components were designed and implemented. The core components were integrated and tested, the HMI (human machine interface) components which make up the platform were usability tested, and during the final DESTRIERO project event (in June 2016) the functions of the prototype were demonstrated to end users. During the conference in September 2016, we can report on this demonstration and the estimated added value the platform gives to end users.

The following sections summarize the scenario and its use cases. Then selected HMI components are covered in more detail using screenshots of the software.

3.1 Scenario and use case overview

The simulated DESTRIERO scenario [9] can be summarized as follows: In Spain, the Buendía dam broke due to an earthquake and that caused a flood which broke the nearby Bolarque dam. This broken dam caused another flood through the Tajo River which reached the José Cabrera nuclear plant. The water entered the power plant due to ruptures caused by the earthquake and led to a black out in the power plant affecting the cooling system and also affecting the structure of one of the reactors. A radioactive leakage was produced.

The DESTRIERO use cases concentrate on collecting and discussing the relevant information on the crisis situation as well as on planning and prioritizing the reconstruction projects. All use cases start three days after the disaster according to DESTRIERO scope. This makes it clear that DESTIERO is focusing on the reconstruction and recovery phase and not on the response phase.

3.2 Description of selected platform functions

In Fig. 3 the top navigation bar of the platform can be seen. To the right of the main menu (tabs) there are four symbols that represent the system menu. It allows the user to display and filter notifications (e.g. due to the creating or modification of objects, log in or out of users), define own settings, modify the user profile or log out.

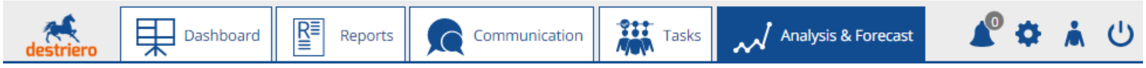
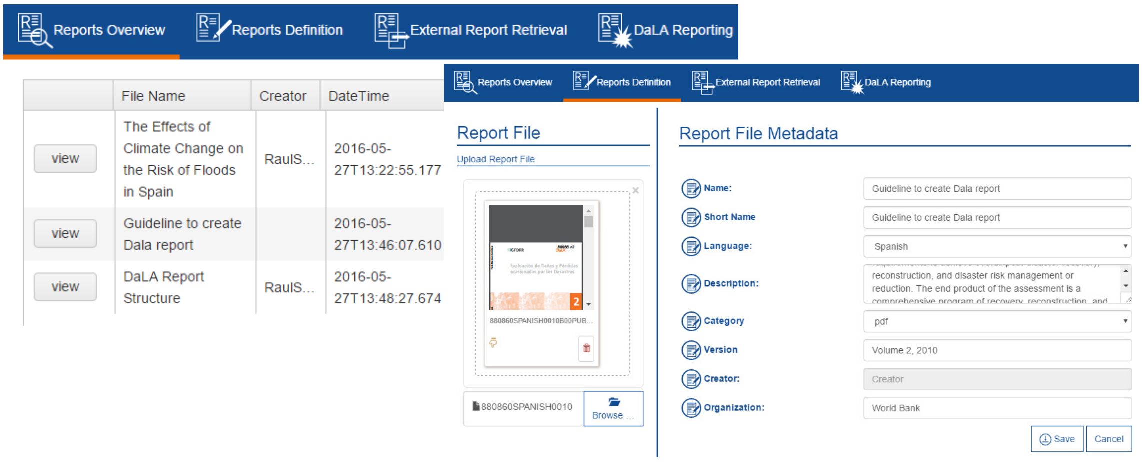


Fig. 3: Top navigation bar and function overview

The first menu item is the dashboard which displays general information on the scenario.

Reports (see Fig. 4) allow the user to view, modify, upload, and retrieve relevant information and reports on the crisis. External information services like ReliefWeb [11] and WHO [12] are directly connected to the system.



	File Name	Creator	DateTime
view	The Effects of Climate Change on the Risk of Floods in Spain	RaulS...	2016-05-27T13:22:55.177
view	Guideline to create Dala report		2016-05-27T13:46:07.610
view	DaLA Report Structure	RaulS...	2016-05-27T13:48:27.674

Report File

Upload Report File

880860SPANISH0010B00PUB...

880860SPANISH0010 Browse ...

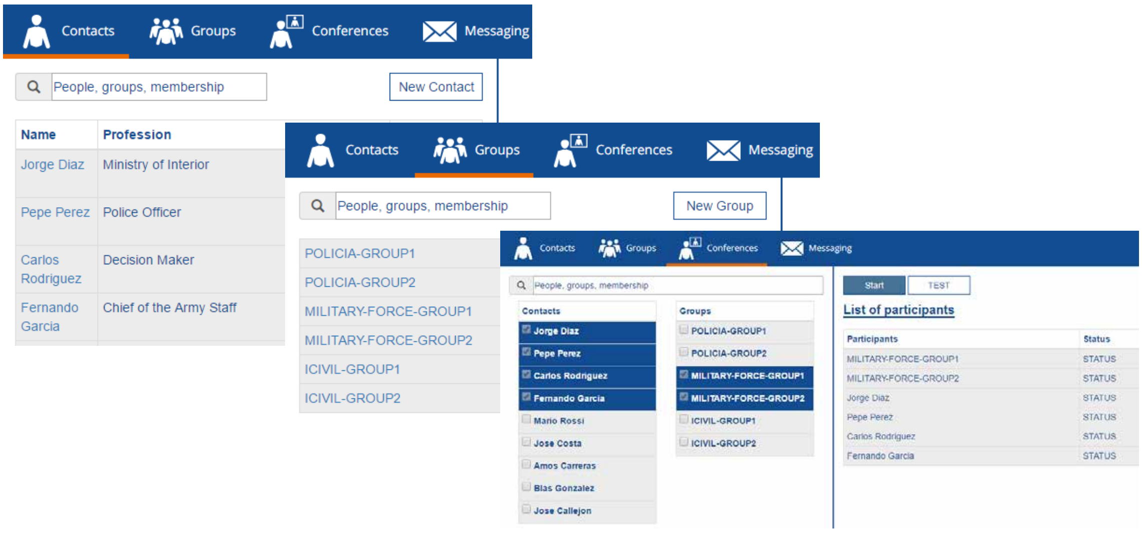
Report File Metadata

Name:	Guideline to create Dala report
Short Name	Guideline to create Dala report
Language:	Spanish
Description:	reconstruction, and disaster risk management or reduction. The end product of the assessment is a comprehensive program of recovery, reconstruction, and
Category	pdf
Version	Volume 2, 2010
Creator:	Creator
Organization:	World Bank

Save Cancel

Fig. 4: Screenshots of the HMI Reports Component

In the communication function (see Fig. 5) the user can create, modify and delete user contacts as well as user groups. These can then be used in case the user wants to initiate a conference call using the stored telephone numbers. Furthermore, the user can send a message to selected users or groups. These messages are sent via the standard SMS (Short Message Service) text messaging functionality (through an integrated third party system) and are listed in the platform for later reference.



Name	Profession
Jorge Diaz	Ministry of Interior
Pepe Perez	Police Officer
Carlos Rodriguez	Decision Maker
Fernando Garcia	Chief of the Army Staff

POLICIA-GROUP1
POLICIA-GROUP2
MILITARY-FORCE-GROUP1
MILITARY-FORCE-GROUP2
ICIVIL-GROUP1
ICIVIL-GROUP2

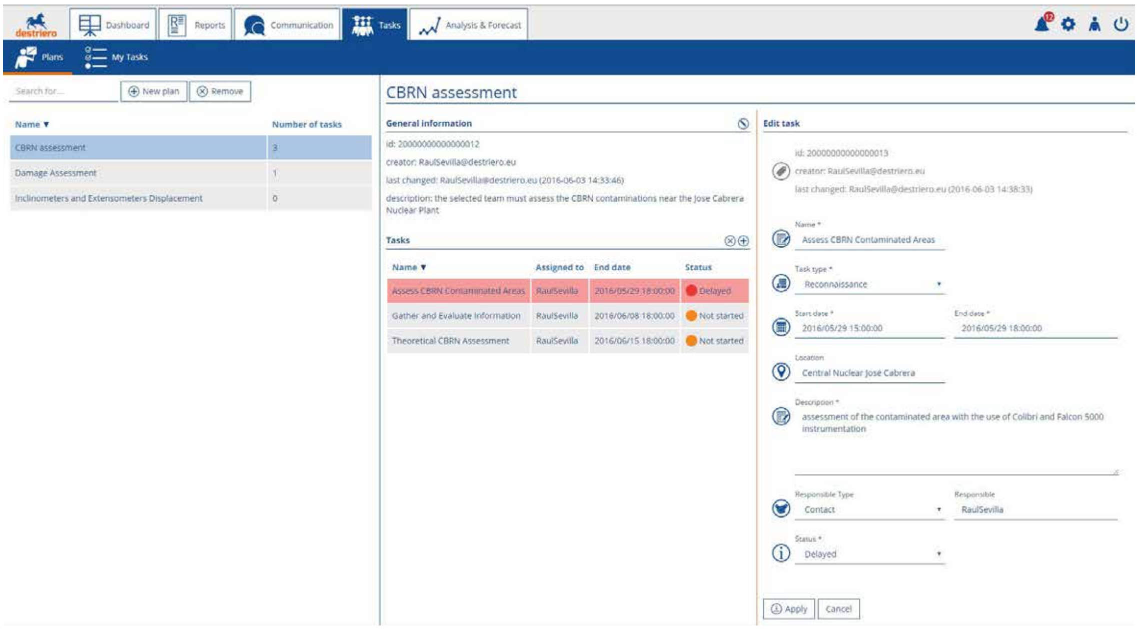
Contacts	Groups
☑ Jorge Diaz	□ POLICIA-GROUP1
☑ Pepe Perez	□ POLICIA-GROUP2
☑ Carlos Rodriguez	☑ MILITARY-FORCE-GROUP1
☑ Fernando Garcia	☑ MILITARY-FORCE-GROUP2
□ Mario Rossi	□ ICIVIL-GROUP1
□ Jose Costa	□ ICIVIL-GROUP2
□ Amos Carreras	
□ Blas Gonzalez	
□ Jose Callejon	

List of participants

Participants	Status
MILITARY-FORCE-GROUP1	STATUS
MILITARY-FORCE-GROUP2	STATUS
Jorge Diaz	STATUS
Pepe Perez	STATUS
Carlos Rodriguez	STATUS
Fernando Garcia	STATUS

Fig. 5: Screenshots of the HMI Communication Component

The user can manage tasks within the platform which are defined in so-called plans (see Fig. 6), e.g. for performing assessments or placing sensors assigned to teams and defined for specific locations previously defined.



Name ▼	Number of tasks
CBRN assessment	3
Damage Assessment	1
Inclinometers and Extensometers Displacement	0

CBRN assessment

General information

id: 20000000000000012

creator: RaulSevilla@destriero.eu

last changed: RaulSevilla@destriero.eu (2016-06-03 14:33:46)

description: the selected team must assess the CBRN contaminations near the Jose Cabrera Nuclear Plant

Tasks

Name ▼	Assigned to	End date	Status
Assess CBRN Contaminated Areas	RaulSevilla	2016/05/29 18:00:00	● Delayed
Gather and Evaluate Information	RaulSevilla	2016/06/08 18:00:00	● Not started
Theoretical CBRN Assessment	RaulSevilla	2016/06/15 18:00:00	● Not started

Edit task

id: 20000000000000013

creator: RaulSevilla@destriero.eu

last changed: RaulSevilla@destriero.eu (2016-06-03 14:38:33)

Name *: Assess CBRN Contaminated Areas

Task type *: Reconnaissance

Start date *: 2016/05/29 15:00:00

End date *: 2016/05/29 18:00:00

Location: Central Nuclear José Cabrera

Description *: assessment of the contaminated area with the use of Colibri and Falcon 5000 instrumentation

Responsible Type: Contact

Responsible: RaulSevilla

Status *: Delayed

Fig. 6: Screenshot of the HMI Plans and Tasks Component

Through the Analysis&Forecast functions the user can specifically use map functionality (see Fig. 7) to place and display different objects on a map (e.g. area of interest, reference data, previously defined plans and radiological events, weather information), get detailed weather information for a selected city (through an integrated external information source) as well as crisis relevant twitter messages through the Geo-CrowdSourcing function.

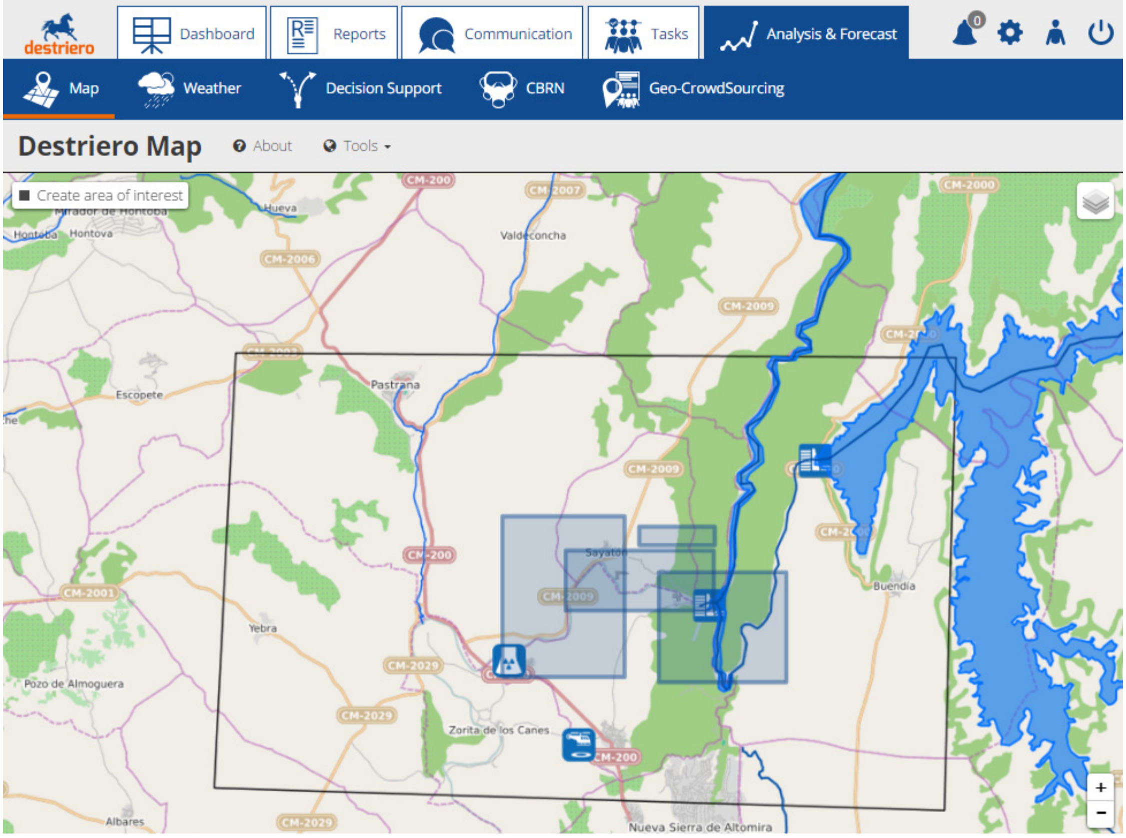


Fig. 7: Screenshot of the HMI Map Component

With the CBRN functionality (see Fig. 8), the user can define and analyze CBRN activities through inputting data for prediction or using real-time data (through sensors) and then analyzing this data using the third party Command and Control system ne.on advance [13].

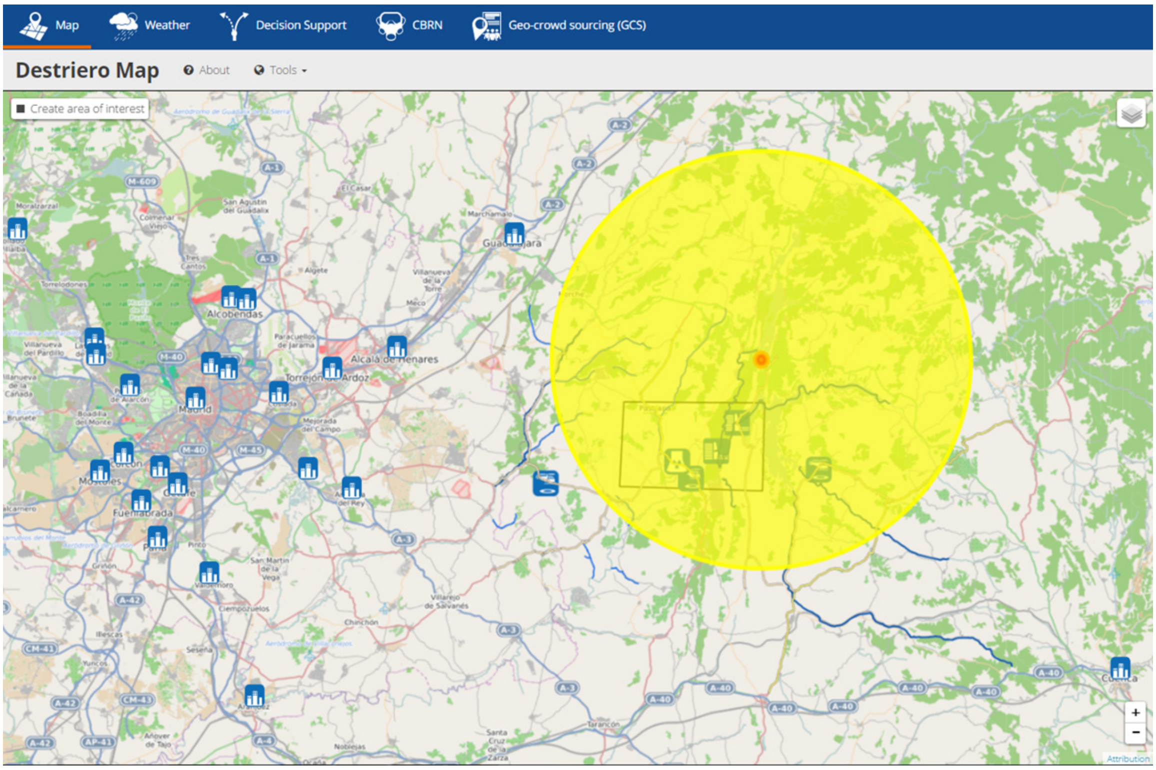
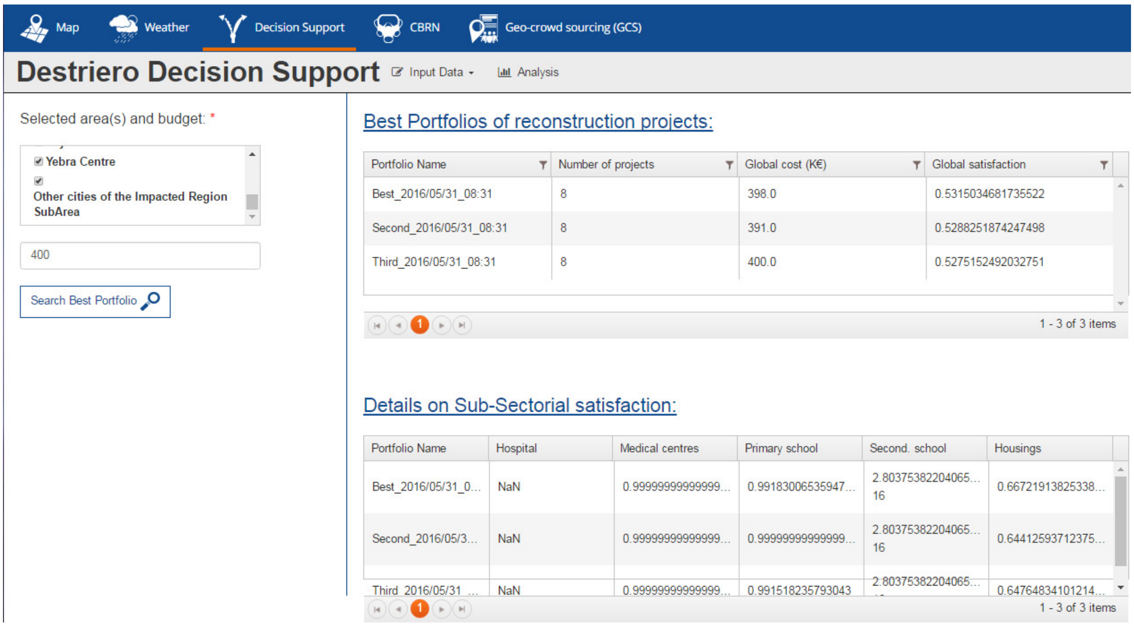


Fig. 8: Screenshot of the CBRN analysis

With the decision support function the user can define and prioritize reconstruction projects using the integrated third party system MYRIAD [14], which is a multi-criteria decision support tool to handle complex decision situations by supporting risk-based assessment of scenarios (situations) and possible courses of action.



Destriero Decision Support

Selected area(s) and budget: *

☑ Yebra Centre

☑ Other cities of the Impacted Region SubArea

400

Best Portfolios of reconstruction projects:

Portfolio Name	Number of projects	Global cost (K€)	Global satisfaction
Best_2016/05/31_08:31	8	398.0	0.5315034681735522
Second_2016/05/31_08:31	8	391.0	0.5288251874247498
Third_2016/05/31_08:31	8	400.0	0.5275152492032751

1 - 3 of 3 items

Details on Sub-Sectorial satisfaction:

Portfolio Name	Hospital	Medical centres	Primary school	Second. school	Housings
Best_2016/05/31_0...	NaN	0.99999999999999...	0.99183006535947...	2.80375382204065... 16	0.66721913825338...
Second_2016/05/3...	NaN	0.99999999999999...	0.99999999999999...	2.80375382204065... 16	0.64412593712375...
Third_2016/05/31_...	NaN	0.99999999999999...	0.991518235793043	2.80375382204065...	0.64764834101214...

1 - 3 of 3 items

Fig. 9: Screenshot of the decision support for reconstruction projects

3.3 Usability testing and evaluation

The setting in which the DESTRIERO system is intended to be used can be described as follow: in the reconstruction phase different organizations work together and want to use a common information platform. One organization starts with an empty platform since all its information will be added to by the users who may be no experts in using the platform. Therefore, the project goal was to provide a tool that is simple to be used by persons with all kinds of background. This quality criterion was tested in April 2016 during usability tests with ten end users led by the Fraunhofer usability experts. The aim of the test was to find out if the visualization interface is intuitive and clear even if the user has had no training at all.

The usability tests were performed online (telephone and screen sharing) by a moderator who gave tasks to the test person according to the DESTRIERO scenario, as well as an observer, who documented answers using a specific recording tool [15]. Furthermore, the test person filled out different questionnaires (before and after the test [16] and [17]) which gave detailed information on the test persons' opinion regarding the usability of the platform. The presentation at the Future Security 2016 will go into detail regarding the evaluation. Some final statements by the test persons are as follows: "the prototype platform is easy to use; intuitive; friendlier than expected; nice and clean; and some improvements are left".

4 CONCLUSIONS AND OUTLOOK

The paper described a post-crisis needs assessment tool for reconstruction and recovery planning, including structural damage assessment through advanced remote sensing enriched by in-field data collection and related data integration and analysis in combination with an advanced multi-criteria decision analysis tool and methodology for multi-stakeholder information analyses, priority setting, decision making and recovery planning. It is a prototype, not yet fully mature to be used in operation by final users. Nevertheless, the usability and end user tests as well as the project final demonstration held in June 2016 in Madrid with end-users of DESTRIERO have shown that it is very promising platform. It has been pointed out that there is a strong need for such next generation of systems based on international standards, novel (automated) data and information interoperability across organizations and systems, which are very relevant to support everyday life for the end users while planning for and performing reconstruction and recovery projects.

REFERENCES

[1] DESTRIERO (2016). Project website http://www.destriero-fp7.eu/, retrieved 02.06.2016.

[2] The Telegraph on line (2016). *America's nuclear defences rely on floppy discs and 1970s computers, according to audit.* http://www.telegraph.co.uk/news/2016/05/26/americas-nuclear-defences-rely-on-floppy-discs-and-1970s-compute/, retrieved 29.05.2016.

[3] Fukushima Accident (2016), World Nuclear Association, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-accident.aspx, retrieved 02.06.2016.

[4] Chernobyl Accident 1986 (2016). World Nuclear Association, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx, retrieved 02.06.2016.

[5] OECD (2004). *Large-scale disasters, lessons learned.* http://www.oecd.org/futures/globalprospects/40867519.pdf, retrieved 02.06.2016.

[6] Goodrich, J.N. (2001). *September 11, 2001 Attack on America: Impact on Tourism Security*. Journal of Travel and Tourism Marketing, Vol. 11(4), pp 1-12.

[7] Cinque, M., Esposito, C., Fiorentino, M., Carrasco, F., Matarese, F. (2015). *A collaboration platform for data sharing among heterogeneous relief organizations for disaster management*. Proc. ISCRAM 2015, pp. 1-8.

[8] Di Crescenzo, D., Strano, A., Trausmuth, G. (2010). *SWIM: A Next Generation ATM Information Bus-The SWIM-SUIT Prototype*. Proc. of the 14th IEEE Int. Enterprise Distributed Object Computing Workshop (EDOCW), pp. 41-46.

[9] DESTRIERO public deliverable. http://www.destriero-fp7.eu/public-deliverables/

[10] Fiorini M., Maciejewski S. (2013). *Lesson Learned During the Realization of the Automated Radar Control System for Polish Sea-waters (ZSRN).* Marine Navigation and Safety of Sea Transportation, CRC Press, pp. 217-221.

[11] ReliefWeb (2016). http://reliefweb.int, retrieved 02.06.2016.

[12] WHO (2016). http://www.who.int/en/, retrieved 02.06.2016.

[13] ne.on advance (2016). http://www.thalesgroup.com/en/worldwide/security/cbrn-detection-and-identification, retrieved 02.06.2016.

[14] Myriad (2016). http://www.predict-project.eu/myriad-0, retrieved 02.06.2016.

[15] Morae – TechSmith (2016). www.techsmith.de/morae.html, retrieved 02.06.2016.

[16] SUS (2016). http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html, retrieved 02.06.2016.

[17] User Experience Questionnaire (UEQ) (2016). www.ueq-online.org, retrieved 02.06.2016.

FIRST RESULTS FROM A LARGE FIELD TRIAL OF THE CROWDTASKER IN AUSTRIA

Jasmin Pielorz[1], Daniel Auferbauer[1], Christian Flachberger[2] and Gerald Czech[3]

[1] *{jasmin.pielorz, daniel.auferbauer}@ait.ac.at*
AIT Austrian Institute of Technology, Donau-City-Strasse 1, 1220 Vienna (Austria)

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

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

Abstract

Unaffiliated volunteers may offer professionals an opportunity to enhance crisis and disaster response. However, guiding or integrating them into coordinated relief efforts poses a challenge. Crowdtasking is a form of crowdsourcing that offers a way to provide meaningful tasks with a limited temporal and spatial scope to such unbounded volunteers. In this paper we present our findings from the first large field trial of a crowdtasking implementation that took place in Vienna in February 2016. Our conclusions from this event address both the setup of the field trial itself as well as our insights regarding the crowdtasking approach.

Keywords: Crisis and Disaster Management, Crowdsourcing, Crowdtasking, Situation Awareness, Volunteer Management.

1 INTRODUCTION

Volunteers play an important role during disaster relief activities. Spontaneous volunteers are of special interest, since they organise themselves quickly, e.g. via social media [1–3], and often appear on the scene without proper guidance from professional crisis managers. In order to integrate them into existing crisis management processes, it is possible to rely on conventional, established communication channels [4–6]. An example for this could be observed during the early stage of the refugee crisis in Europe, when the Austrian Red Cross initiated a crowdsourcing effort via Facebook to develop a picture-based dictionary for migrants who neither speak English nor German. In a similar way, grassroots approaches tend to organise schedules and commodity donations via social media channels.

A more direct form of volunteer engagement can be achieved through the *crowdtasking* approach. The idea of crowdtasking is to address spontaneous volunteers pro-actively and to guide and integrate them as a valuable resource into the overall disaster management efforts. Originally conceptualised and developed in the Austrian research project RE-ACTA between 2013 and 2015 [7,8], the prototypic implementation of this concept called *CrowdTasker* is now being tested and applied in the European research project DRIVER. In February 2016, CrowdTasker was tested successfully for the first time in a large-scale field trial by the three DRIVER partners Austrian Institute of Technology (AIT), Austrian Red Cross (ARC) and Frequentis (FRQ). As part of our field trial, 200 volunteers all over Austria and in parts of Germany participated and performed 748 micro-tasks that were designed in cooperation with the Austrian Red Cross and distributed through the CrowdTasker tool by 6 crisis managers (also of ARC).

This paper reports first results from that large-scale field trial with respect to usefulness for coordination of unaffiliated volunteers, improved situation awareness and usability. Starting with a brief description of the underlying crowdtasking process and its technical realisation in Section 2, we describe in Section 3 the design of the experiment and the methodology applied for evaluating the results. This is followed by a description of the concrete experimentation procedure in Section 4. After a presentation of the quantitative results from the questionnaire in Section 5, we conclude in Section 6 with a discussion of the lessons learnt from three perspectives: (a) key success factors for a successful experimentation, (b) efficiency of the crowdtasking procedure and possible improvements, and (c) usability of the crowdtasking implementation (CrowdTasker) and possible improvements on a technological level.

2 THE CROWDTASKING CONCEPT

Crowdtasking is a special form of crowdsourcing. It is defined as a request for concrete and well-defined actions within a limited temporal and spatial scope, resulting in the performance of micro-tasks with no further obligations [9,10]. Crowdtasking discerns between three roles: people executing assigned tasks in the field are referred to as volunteers, professionals defining and distributing those tasks are called coordinators. There is also a third role, the crisis manager, who consumes information, retrieved from volunteers, through a Common Operational Picture (COP) system. The roles of coordinator and crisis manager may or may not be mutually exclusive. In crowdtasking, potential volunteers are selected by their geographical location and their skill set. They are asked to participate and, once they accepted the initial request, are eligible to be offered tasks. Volunteers may individually accept or decline tasks they are offered. Each task consists of an arbitrary number of task steps. Each step has a well-defined type of end result, which may either be: a multiple choice selection, a single choice selection, a photo, a number or a free text. After a volunteer has completed all steps of a task, the data is sent back to be evaluated and visualized. This is repeated until the coordinators declare the crisis event to be finished (see process overview in Figure 1). Crowdtasking, by design, does not include an option for volunteers to submit information on their own initiative. They may only submit data that was specifically asked for.

A prototype implementation of the crowdtasking concept was developed in RE-ACTA for evaluation purposes [7, 8]. It consists of three components: a web interface for defining and publishing tasks (CrowdTasker by AIT), a smartphone application for executing these tasks (CrowdTasker mobile by AIT) and another web interface for visualizing volunteer’s responses (LifeX COP by Frequentis). These components are represented in Figure 1 through color coding (violet, green and grey, respectively).

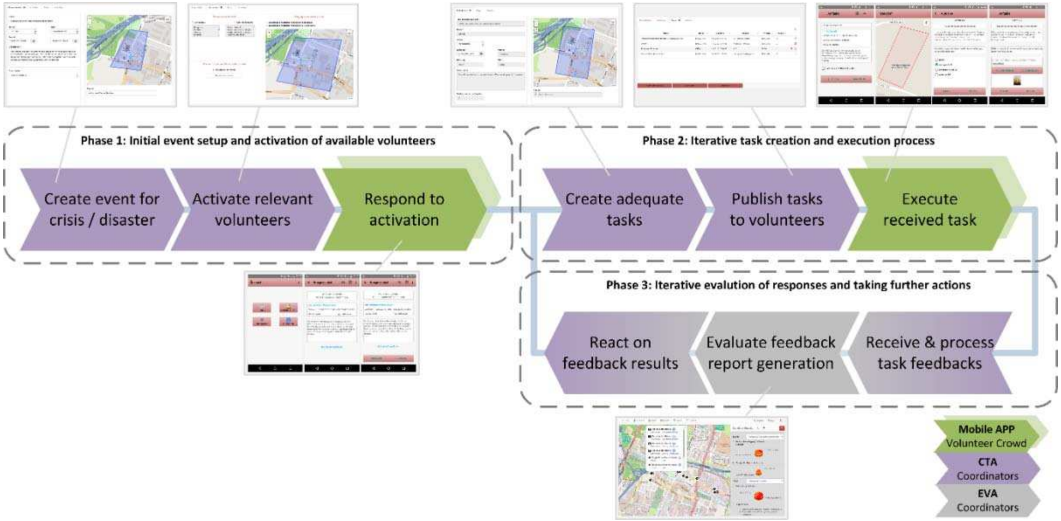

Phase 1: Initial event setup and activation of available volunteers
Create event for crisis / disaster
Activate relevant volunteers
Respond to activation
Phase 2: Iterative task creation and execution process
Create adequate tasks
Publish tasks to volunteers
Execute received task
Phase 3: Iterative evalution of responses and taking further actions
React on feedback results
Evaluate feedback report generation
Receive & process task feedbacks
Mobile APP Volunteer Crowd
CTA Coordinators
EVA Coordinators

Figure 1 Simplified crowdtasking workflow

3 EXPERIMENT DESIGN AND METHODOLOGY

The combined CrowdTasker and LifeX COP field trials are part of a campaign of experiments in the scope of the EU FP7 project DRIVER[1]. They were conducted in three different countries: Israel (January 2016), Austria (February 2016) and the Netherlands (April 2016). The aim of this campaign was to investigate how the interaction with citizens and the management of volunteers in crisis events could be improved. This paper describes the outcomes and implications of the second of these experiments, conducted in February 2016 on two consecutive days in Vienna. The particular focus here was to investigate and evaluate:

- The viability and usefulness of crowdtasking for specific use cases.
- Its acceptance by volunteers and professional relief organisations.
- The usability of our specific crowdtasking implementation (CrowdTasker web interface and mobile application together with LifeX COP).

To gain insights into these topics we used a mix of quantitative and qualitative methods to evaluate the field trial results. Qualitative methods were used to investigate the professional crisis manager’s point of view with the help of group discussions and interviews. Data from participants acting as volunteers were mostly quantitative in nature and gathered via the mobile app itself and with a questionnaire after the experiment.

In order to allow a seamless execution of the experiment, each person involved had a clear role with specific responsibilities. The *experimentation management team* designed and prepared the whole experiment, communicated with all participants, gathered observations and feedback from participants and observers. The *crisis staff* was represented by a team of the Austrian Red Cross and consisted of one coordinator and five crisis managers using CrowdTasker and LifeX COP tools. They were situated at the premises of AIT in a separate room to be used as command and control centre; we will refer to this as “HQ”. This room was cleared of external personnel during the exercise to minimise

[1] http://driver-project.eu/

disturbances, except for dedicated *scientific staff* to support them. *Volunteers* were acting on the streets at different locations in Austria and Germany. They contributed by receiving tasks via the crowdtasking application and reacting to them. As additional communication channel, the experimentation management team established an online blog with a connected chat room, allowing the volunteers to stay informed about the activities in headquarter while they are idle and to maintain a continuous contact. As *external observers* we invited practitioners from different European member states, scientists and representatives of the industry. For these observers, an additional observer room was installed, allowing them to follow all activities of the crowdtasking system. Members of the crisis staff of the Austrian Red Cross were also present in the observer room in order to explain all activities to the observers.

During the field trials three observers were present at HQ: two members of the Fraunhofer IAO payed close attention to the user's interaction with software tools to evaluate usability by using the Thinking-Aloud method [12]. One member of AIT observed the progress of the exercise, provided help with the tools where needed and took note of the communication between participants. The focus of this participant observation lay in the interaction of participants between each other: how tasks are handed down from crisis manager to coordinators, how labour was divided and how cooperative work was achieved. A video recording, spanning all of Friday's exercise, was taken for later analysis. Additionally, screen-capturing software was active on all of the participants' devices for the duration of the field test.

Group discussions were held the day before and immediately after the exercise. They were of semi-structured manner, whereby guiding questions and topics to be discussed are defined beforehand, together with an approximate timeslot for each. The first discussion revolved around the topics of what makes a good tool for volunteer management, how to deal with unaffiliated volunteers and which best practices did or did not work for participants in their last deployment with volunteers. This was not yet specific to CrowdTasker or crowdtasking. In the group discussion immediately after the field test, we asked participants to discuss first impressions, possible roles and use cases of crowdtasking as well as any further feedback they might have. All discussions were recorded either in video or audio for later analysis with the informed consent of all participants.

In contrast to the detailed observation of professionals, we did not have any direct contact with participants in the field, who were acting as volunteers. Indeed, their identities are largely unknown to us, apart from what they willingly shared (such as email address or first and last name). As it was not possible to observe a large crowd of volunteers in the field directly, we took a quantitative approach. First, we surveyed user acceptance and feedback through the CrowdTasker system. This was achieved by asking the following two questions as the last steps of each task that the user executed: 1) Rate this task's difficulty (easy/normal/difficult) and 2) Would you do a task like this again? With this, we hoped to acquire data regarding what type of task is best received by users. Additionally, we asked volunteers to participate in an online survey after the exercise. This questionnaire covers topics like the volunteer's background and their feedback regarding tasks and user interface.

4 RUNNING THE FIELD TRIAL

The participants of the field test consisted of two distinct groups: professional crisis managers at the headquarter (HQ), with experience in volunteer management, who published tasks and a second group consisting of participants in the field, who received these tasks and acted as volunteers willing to support in a crisis situation.

Participants acting as crisis managers at HQ were contacted directly by the Austrian Red Cross, which all of them are affiliated with. To recruit participants for the role of volunteers, we published requests for participation on mailing lists of Frequentis and AIT roughly two weeks before the event. One week before the event, we sent out a task to participants that had already registered, asking them to "recruit" one new participant. Lastly, the Austrian Red Cross published an invitation for participation on their Facebook page two days before the event (9th Feb). As indicated in Figure 2, the latter was likely the most effective way of recruitment and brought on the bulk of registrations. At the beginning of the live field test, we had 200 registered users on record.

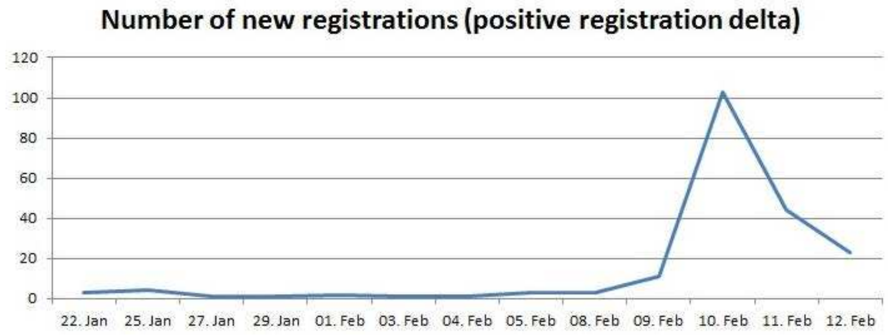


Figure 2 Number of new registrations per day

To provide information and registration opportunities for potential participants, we set up a homepage for the experiment. This homepage provided background information about the field test, CrowdTasker and how to participate. The website also required that users read and acknowledge a code of conduct and informed consent before their registration. To make sure that participants read this information, registration through the smartphone app was locked by an access code. This access code was only visible if the user had agreed to the code of conduct and informed consent. We found this to be the most reasonable way of making sure participants are aware of the informed consent form. Starting two days before the experiment, we also published a blog with up-to-date information regarding the experiment. During the experiment, we would use it to push information regarding tasks and progress to volunteers. This worked well as a way to stay in touch with participants and can also be used to steer the field trial.

To prepare volunteers for working with the CrowdTasker smartphone application, we pushed out an introduction task several days before the start of the field test. This task was available to everyone who had signed up. Its purpose was to walk participants through the basic steps of accepting an event and executing a task. Incidentally, this also provided a good indication of where our volunteers were located and how many of them were ready to participate.

For members of the Austrian Red Cross at HQ, preparation consisted of an introduction event on Thursday afternoon, the day before the field test, after the first group discussion was concluded. We introduced them to the crowdtasking idea and workflow as well as the user interface of our implementations. This included a live, practical walkthrough of creating an event, sending requests for participation, creating a task, publishing it and reviewing the results.

On Friday, 12th February, the live field test started at 9:00 am, when the participants took their positions at HQ. In accordance with ARC, we declared one participant to be head of operations and four others to act as volunteer managers. The head of operations would receive instructions, on what needed to be achieved with the help of volunteers in the field. Examples of such tasks included: determining the number of people in front of a certain subway station, finding volunteers to provide warm blankets in a specific state or organising volunteers to help at a defined date and time. The live field test continued in this way until 14:15 pm, intermitted by a lunch break.

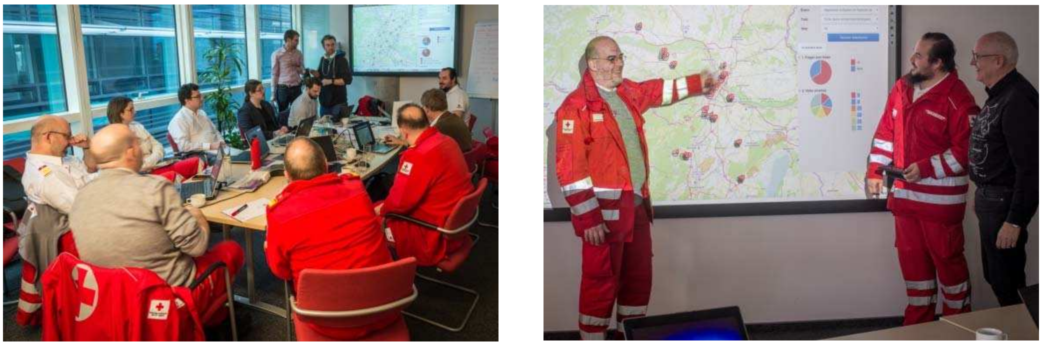


Figure 3: Headquarter: crisis coordination room (left side), observation room (right side).

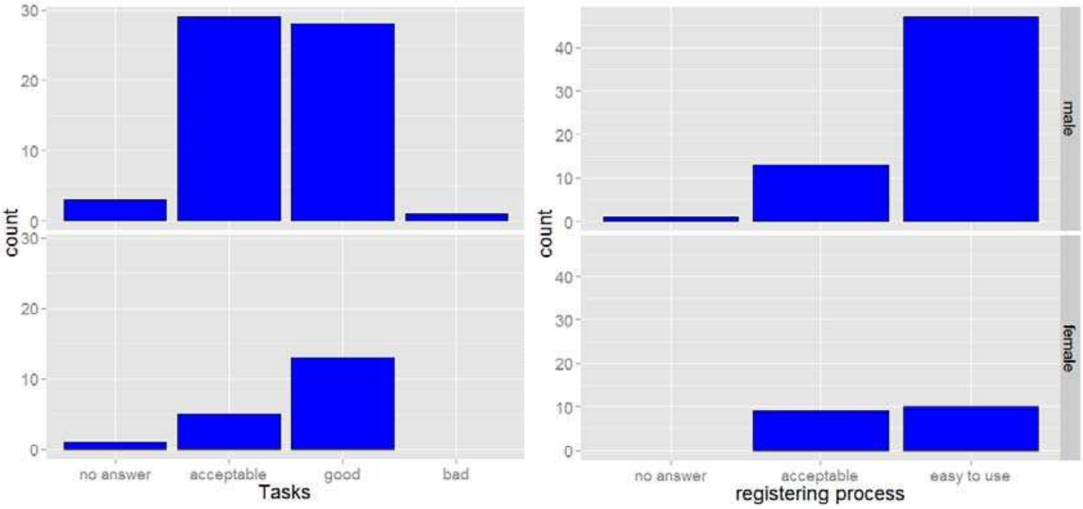
Figure 4: Volunteers using the CrowdTasker mobile application.

Following the conclusion of the field test, we again held a group discussion with the Red Cross crisis managers. This time, we focused on feedback regarding the relevance of the crowdtasking concept for volunteer management and possible use cases for crisis and disaster management. Observers from Fraunhofer IAO furthermore held interviews with individual participants to evaluate the usability of the CrowdTasker tools. The day was concluded by a summary of events and a feedback round with participants. All participants and visitors were dismissed at roughly 4:00 pm.

5 SURVEY RESULTS

After the field trail all registered participants, who used our mobile application, were asked to fill out an online questionnaire. It consisted of 17 questions that could be answered in 7-10 minutes. While the first set of questions covered the general background of our participants with respect to volunteerism and use of social media, the second set focused on the overall sentiment with respect to the tasks and the user interface. The last set of questions allowed free text and provided the possibility to give general feedback on the experiment design, execution and our crowdtasking application.

Approximately one week after the field trial 91 participants had answered our questionnaire, out of which 89 completed all questions. 61 came from male, while 19 were answered by female participants with one person providing no answer. The bulk of volunteers was in the age group between 20 and 30 years, approximately 15 in the age group between 30 and 40 years, and 5 indicated to be older than 50 years. The majority of volunteers were associated with the Red Cross (47), while the others were evenly distributed among Team Österreich, AIT, Frequentis or with no affiliation. Due to the high participation of Red Cross staff, most of our volunteers indicated to have experience in volunteer work and with providing support in crisis events. Approximately 30% have previous experience in using social media in crisis management, among them mostly male participants.



The field test was in general perceived very positive: More than 95% of the questioned volunteers are interested in participating in another such event, the majority liked the posed tasks or found them at least acceptable and perceived the registering process as easy to use. Male participants were in general more critical towards the tasks than females, but perceived the registration process more positive than female participants. A lot of participants provided feedback in the form of free text with encouragement to continue our developments along this line and specific remarks pointing towards shortcomings in the software implementation and suggestions for future developments.

6 CONCLUSIONS

The field trial described in this paper was the first large scale test of our crowdtasking implementation with 200 registered volunteers, 10 experiment team members, 10 observers and 6 crisis managers resulting in 748 solved micro-tasks. The experiment preparation and execution went very well and was perceived in this way, both by volunteers and experiment participants. Volunteers in the field liked in particular the blog accompanying the experiment and the prompt answers with respect to arising questions. Nevertheless, a few volunteers and observers would have preferred a clearer storyline for the posed tasks in order to have a better idea how this can be used in actual crisis events. While the general usability of our smartphone application was evaluated positively, volunteers indicated problems with the battery and storage space consumption for some mobile devices. Additionally, not everybody received their accepted tasks timely, indicating the necessity for further testing of our application. In summary, the experiment indicated that our crowdtasking concept provides an interesting alternative to existing social media channels that has to be further investigated in the future.

REFERENCES

[1] L. Palen, S. Vieweg, S.B. Liu, a. L. Hughes, Crisis in a Networked World: Features of Computer-Mediated Communication in the April 16, 2007, Virginia Tech Event, Soc. Sci. Comput. Rev. 27 (2009) 467–480. doi:10.1177/0894439309332302.

[2] K. Starbird, L. Palen, "Voluntweeters": Self-organizing by Digital Volunteers in Times of Crisis, in: Proc. 2011 Annu. Conf. Hum. Factors Comput. Syst. - CHI '11, ACM Press, New York, New York, USA, 2011: p. 1071. doi:10.1145/1978942.1979102.

[3] K. Starbird, L. Palen, Working and sustaining the virtual "Disaster Desk," Proc. 2013 Conf. Comput. Support. Coop. Work - CSCW '13. (2013) 491. doi:10.1145/2441776.2441832.

[4] Y. Tyshchuk, W. Wallace, The Use of Social Media by Local Government in Response to an Extreme Event : Del Norte County , CA Response to the 2011 Japan Tsunami, (2013) 802–811.

[5] C. Reuter, A. Marx, Social Software as an Infrastructure for Crisis Management - a Case Study About Current Practice and Potential Usage, in: Proc. 8th Int. ISCRAM Conf., 2011: pp. 1–10.

[6] C. Rizza, Building a resilient community through social network : ethical considerations about the 2011 Genoa floods, in: Proc. 11th Int. ISCRAM Conf., University Park, Pennsylvania, USA, 2014: pp. 289–293.

[7] D. Auferbauer, R. Ganhör, H. Tellioglu, Moving Towards Crowd Tasking for Disaster Mitigation, in: Palen, Büscher, Comes, Hughes (Eds.), Proc. ISCRAM 2015 Conf., Kristiansand, 2015.

[8] C. Flachberger, G. Neubauer, C. Ruggenthaler, G. Czech, Crowd Tasking – Realising the Unexploited Potential of Spontaneous Volunteers, in: J. Beyerer, A. Meissner, J. Geisler (Eds.), Secur. Res. Conf. 10th Futur. Secur. Proc., Fraunhofer Verlag, Berlin, 2015: pp. 9–16.

[9] G. Schimak, D. Havlik, J. Pielorz, Environmental Software Systems. Infrastructures, Services and Applications, 2015. doi:10.1007/978-3-319-15994-2.

[10] G. Neubauer, A. Nowak, B. Jager, C. Kloyber, C. Flachberger, G. Foitik, et al., Crowdtasking – A New Concept for Volunteer Management in Disaster Relief, in: J. Hřebíček, G. Schimak, M. Kubásek, A. Rizzoli (Eds.), Environ. Softw. Syst. Foster. Inf. Shar., Springer Berlin Heidelberg, 2013: pp. 345–356. doi:10.1007/978-3-642-41151-9_33.

[11] D. Auferbauer, G. Czech, H. Tellioglu, Communication Technologies in Disaster Situations: Heaven or Hell?, in: J. Beyerer, A. Meissner, J. Geisler (Eds.), Secur. Res. Conf. 10th Futur. Secur. Proc., Fraunhofer Verlag, Berlin, 2015: pp. 25–32.

[12] J. Nielsen, Usability engineering, Elsevier, 1994.

A HOLISTIC APPROACH TO FUTURE PUBLIC SAFETY COMMUNICATION SYSTEMS' EVOLUTION – OVERVIEW OF FP7 EU PPDR-TC PROJECT'S OUTCOMES

Dimitris Kanakidis[1], Evangelos Sdongos[2], Damien Lavaux[3], James Jackson[4], Natasha McCrone[4], Michalis Tsagkaropoulos[5], John Burns[6], Henryk Gierszal[7], Piotr Tyczka[8], Krzysztof Samp[8], Pedro Antonio[9], and Maurizio Casoni[10]

[1] *dkan@exus.co.uk*
EXUS SA, Athens, Greece

[2] *esdongos@iccs.gr*
Institute of Communication and Computer Systems (ICCS), Athens, Greece

[3] *damien.lavaux@thalesgroup.com*
Thales Communications & Security SAS, Gennevilliers, France

[4] *{james, natasha}@rinicom.com*
Rinicom Ltd., Lancaster, UK

[5] *m.tsagkaropoulos@teletel.eu*
TELETEL SA, Athens, Greece

[6] *john.burns@plumconsulting.co.uk*
Plum Consulting, London, UK

[7] *gierszal@amu.edu.pl*
Adam Mickiewicz University, Poznań, Poland

[8] *{piotr.tyczka, krzysztof.samp}@itti.com.pl*
ITTI Sp. z o.o., Poznań, Poland

[9] *pedro.antonio@tekever.com*
TEKEVER SA, Obidos, Portugal

[10] *maurizio.casoni@unimore.it*
University of Modena and Reggio Emilia, Modena, Italy

Abstract

The paper presents the main results and conclusions of the recently completed FP7 EU project entitled "*Public Protection and Disaster Relief – Transformation Centre*" – PPDR-TC. The major objective of PPDR-TC project was to provide the strategic roadmap towards the full migration path of future PPDR system's evolution satisfying the mid and long-term requirements for the next 10-15 years. In order to cope with this goal PPDR-TC established a modular study approach with several building blocks. In addition, PPDR-TC project produced a series of techno-economical recommendations, supported by a comprehensive set of simulations and field trials to prepare a transition roadmap from current voice-centred PPDR networks to broadband-capable communication systems.

Keywords: Public Protection and Disaster Relief (PPDR), mission critical communications, public safety communication systems.

1 INTRODUCTION

Human-provoked and natural disasters are forcing governments to utilize their Public Protection and Disaster Relief (PPDR) resources more efficiently. The traditional security objectives are changing as new challenges and threats emerge and there is a need for better integration and co-operation with the emergency services at national, European and international levels. Europe is actuating its internal security mechanisms in the context of a framework for increased cooperation between Police, Fire, Rescue, Health and Military. At the moment there is an urgent need for rapidly deployable broadband communication facilities, to meet the increasingly demanding requirements of PPDR users; also, there is an increasing demand for spectrum harmonization for PPDR services (video and high speed data) through a in Europe. The main characteristics identified as particularly desirable for broadband PPDR communications are:

- Interoperability between systems from different vendors and countries that are able to interoperate at some predetermined level without any modifications or special arrangements.
- Economies of scale should support the equipment design layered on top of existing commercial communication networks (WiMAX, LTE, etc.).

The FP7 EU “Public Protection and Disaster Relief – Transformation Centre” – PPDR-TC project’s vision was to research and provide technical and economic recommendations in order to enhance cross-border coordination, increase potential for interoperability and international cooperation and improve spectrum management and planning. PPDR-TC vision’s realization was based on three main elements, namely:

- identification of current PPDR Communications status and requirements for future applications,
- data synthesis and scenarios development,
- technical, economic and organizational analysis of future PPDR Communications development.

The main objectives of PPDR-TC project were the following:

1. Gathering of European PPDR facts and figures data.
2. Definition of PPDR Communications reference usage scenarios and identification of service requirements and future needs in the European context.
3. Implementation of a detailed study of the reference scenarios with a view to establishing service classification and identifying key technical issues.
4. Identification of candidate PPDR Communications technologies and architectures.
5. Development of validation tools for future PPDR Communications.
6. Elaboration of technical recommendations on candidate technologies and architectures.
7. Provision of economical recommendations on candidate technologies and architectures.
8. Provision of a roadmap towards full satisfaction of future PPDR Communications requirements and development of recommendations for PPDR Communications standards for decisions-makers.

The project was organized in seven work packages that were responsible to fulfill the aforementioned objectives. The main technical results produced within the project are highlighted in the following sections.

2 DEVELOPMENT OF REFERENCE USAGE SCENARIOS

The objective was to define the typical current and anticipated future operational scenarios faced by PPDR operatives and the related communication needs, including routine "day-to-day" operations, planned major events and unplanned major incidents or disasters. Information was sourced from previous studies, feedback from PPDR stakeholders contacted by the consortium members and additional desk research carried out by the task leaders.

Five distinct communication requirements for PPDR users were identified, namely voice, narrowband data (e.g. for messaging), broadband data (e.g. for images or large files), video and the use of repeater stations to extend coverage or provide air-to-ground communication. Eight high level communication scenarios were also identified, namely:

- A: Between a Central Control Station and Field Personnel at an Incident
- B: Between PPDR Vehicles and an Incident Location or Control Station
- C: Between Individuals at an Incident
- D: Between Different PPDR Entities (e.g. Police, Fire, Ambulance, Volunteers)
- E: Accessing External Data Sources (e.g. Internet)
- F: Communication in Enclosed Spaces (e.g. Tunnels Or Basements)
- G: Communication With Remote Locations (e.g. Mountains or at Sea)
- H: Communication with or between Machines (e.g. Remotely Controlled Vehicles).

Stakeholder responses were received and used in the analysis of usage scenarios. In addition, eight specific major incident / event scenario case studies were undertaken, each based on a real-life incident or event.

The analysis uncovered deficiencies in existing PPDR communication capabilities in several areas, including:

- Inadequate network coverage
- Lack of Interoperability (both at the technology and working protocol level)
- Insufficient resilience (e.g. unreliable power supplies or non-rugged terminals)
- Excessive reliance on public networks which are unreliable in crisis situations.

Applications identified as particularly important in the future for supporting PPDR operations included video, other data applications (e.g. breathing apparatus telemetry, vital signs monitoring and access to on-line forms and databases) and location services (e.g. for tracking of personnel, vehicles and other assets). Resilience, flexibility and better interoperability between different agencies and ICT systems were also considered important. Existing PPDR communications were found to vary considerably between EU countries but all suffered deficiencies in coverage, interoperability and/or data capability [1].

3 ESTABLISHMENT OF A PPDR FACTS AND FIGURES DATABASE

Another aim of the project was to develop an on-line database to provide facts and figures relating to PPDR activities, networks and technologies within the EU. The database is fully operational and can be accessed through a sub-domain of the PPDR-TC web site at http://db.ppdr-tc.eu/.

The architecture is client-server providing a front-end with advanced capabilities of searching and retrieving data as well as a back-end mainly offering storage of data and mechanisms for data correlation. Access rights with different levels of authorization were identified focusing on two distinct system roles, namely.

- Administrator/ Contributor with Read/Write/Modify/Add new entries privileges
- User with Read Only and Search rights

To make the database more attractive to the end-users, additional content and functionality has been added, including:

i) Added tooltip functionality (popup text) on selected fields to provide explanatory notes to better clarify field contents

ii) Added page for download of the free-of-charge and free-to-use “Financial-Economic Basic Tool” which is a business-oriented tool that can deliver a series of efficiency indices for different scenarios of acquiring a PPDR system (also developed within the activities of the PPDR-TC project)

iii) Contact point information on each entry (i.e. contact person name, email, telephone, address)

iv) Inclusion of new technical fields related to the supported services and owned systems, e.g. network specific information such as number of base stations.

v) Updated user interface, extended statistics figures and extended search filters and results based on technologies and services used.

4 PPDR REFERENCE SERVICES

The project also targeted at defining a set of reference services that are valuable for PPDR agencies, given their needs and requirements, as well as the current technological availability. It produced the definition and classification of a set of 31 reference services that include PPDR voice, narrowband data, broadband data and video, as well as transversal services for the extension of capabilities and challenging services enabled by the next generation of technologies.

Parameters such as the technological maturity, applicable scenarios and service timeframe were used to analyse and classify services. Each service was also placed in a classification scale of potential interest that ranges from near-term evolution, mid-term evolution to long-term evolution. As final result of this activity, the following table summarises the services that have been analysed and their classification in accordance with the analysis.

Service	Classification
Push-to-talk	Near-term evolution
Private call	Near-term evolution
Emergency/priority call	Near-term evolution
Call retention/busy queuing	Near-term evolution
Direct mode operation	Near-term evolution
Ambience listening	Near-term evolution
Voice over the public switched telephone network	Near-term evolution
Area selection/dynamic group number assignment	Near-term evolution
Messaging and notifications	Near-term evolution
Low resolution photos	Near-term evolution
Location-based information	Near-term evolution
Extension of coverage	Near-term evolution
Extension of availability	Near-term evolution
Security tools	Near-term evolution

Service	Classification
Group call	Mid-term evolution
Automatic telemetrics	Mid-term evolution
Mobile workspace applications (narrowband)	Mid-term evolution
Access to internal databases (narrowband)	Mid-term evolution
Access to external sources (narrowband)	Mid-term evolution
Rapid file transfer	Mid-term evolution
High resolution photos	Mid-term evolution
Mapping with geographic information system layers	Mid-term evolution
Mobile workspace applications (broadband)	Mid-term evolution
Access to internal databases (broadband)	Mid-term evolution
Access to external sources (broadband)	Mid-term evolution
Video transmission	Mid-term evolution
Video file transfer	Mid-term evolution
Video call	Mid-term evolution
Proximity services	Mid-term evolution
Augmented reality	Mid-term evolution
Remote operations	Long-term evolution

Table 1: Summary of the services classification activity

The main conclusion drawn from this analysis work was that the value or interest to introduce a certain communications service into a PPDR system is not solely determined by the needs and requirements manifested by potential end-users of such a service, being also constrained by:

- The availability of mature network technologies and terminals, able to support the service in a cost-efficient manner;
- The applicable regulations and standards which, among other issues, may limit the RF spectrum that can be allocated for the service or network.

5 ANALYSIS OF RADIO SPECTRUM REQUIREMENTS

It was performed an analysis of the radio spectrum currently utilised by PPDR agencies around the world and the projected future needs for radio spectrum to support new enhanced services such as broadband data and video in the future, based on a variety of publicly available sources and additional internal analysis. Spectrum requirements for wide area mobile networks, local area networks, direct mode operation (DMO), air to ground (A2G) communications, satellite communications and network backhaul were addressed. Table 2 summarises the most likely future spectrum resources for broadband PPDR services in Europe at the time of writing, based on publicly available literature and discussions within regulatory entities, notably CEPT and ITU-R [3].

6 BUSINESS MODELS, ECONOMIC ANALYSIS AND TOOLS FOR DECISION-MAKERS

Several business models with sub-models presenting different approaches to set up a PPDR system were identified. The elements used to construct business models reflect the broad range of options analysed in the project, including a range of actors as well as value and cash flows, though the dominant view is supposed to be that of a PPDR service organisation. Three general models have been identified with respect to owning and operating entities; three sub-models of system acquiring, three sub-models of system building, four sub-models of financing, and two sub-models of operations. Drawing conclusions from various studies reported in last years, PPDR-TC project claims that in practice 'business models' general alternatives available for implementation of critical communications broadband services are the following [3]:

a. **User Owned – User Operated (UO-UO)**: Building, ownership & operation of the network(s) by the end-user agency (or agencies) themselves.

b. **User Owned – Commercial Operated (UO-CO)**: Build & ownership of the network(s) by the end-user agency (or agencies). Operation of the network(s) by a commercial provider of outsourced managed network services.

c. **Commercial Owner – Commercial Operated (CO-CO)**: User agencies subscribe for services provided by a commercial network owner / operator.

Application	Preferred band(s)	Comments	References
Wide area cellular network	700 MHz (698-733/ 758-803 MHz)	2x10 MHz required but equipment should tune over full band to facilitate interoperability with commercial networks. Lower 2x5 MHz has been mooted as a harmonised PPDR band	CEPT document FM49(13) 085 Annex 1, ITU-R document 5A/265
Local area / ad-hoc networks	4940-4990 MHz and 5150-5250 MHz	Higher band is shared with commercial Wi-Fi. May also be used to support direct mode operation	CEPT ECC Recommendation (08)04
Air to ground (A2G) communications	1900-1920/ 2010-2025 MHz 2300-2400 MHz	Based on current utilisation in some countries and on-going CEPT considerations	CEPT ECC, National Regulatory Authorities

Table 2: Likely preferred bands for future PPDR deployment in Europe (as of May 2014)

An illustration of the considered acquiring models is provided in Fig. 1, and models are tagged (red labels in Fig. 1) with respect to the general Ownership/Operation models listed above.

Important outcomes of the project's activity in this area are also two software tools:

- the business oriented tool entitled "model_PPDR_TC" that delivers a series of efficiency indicators that can be used by decision makers to simulate different scenarios of acquiring a PPDR communications system
- an enhanced set of tools (toolbox) that offers to a user (decision-maker) the possibility of performing comprehensive multi-domain analysis that takes into account telecommunication techniques, communication services, financing and business models, and economic expectations.

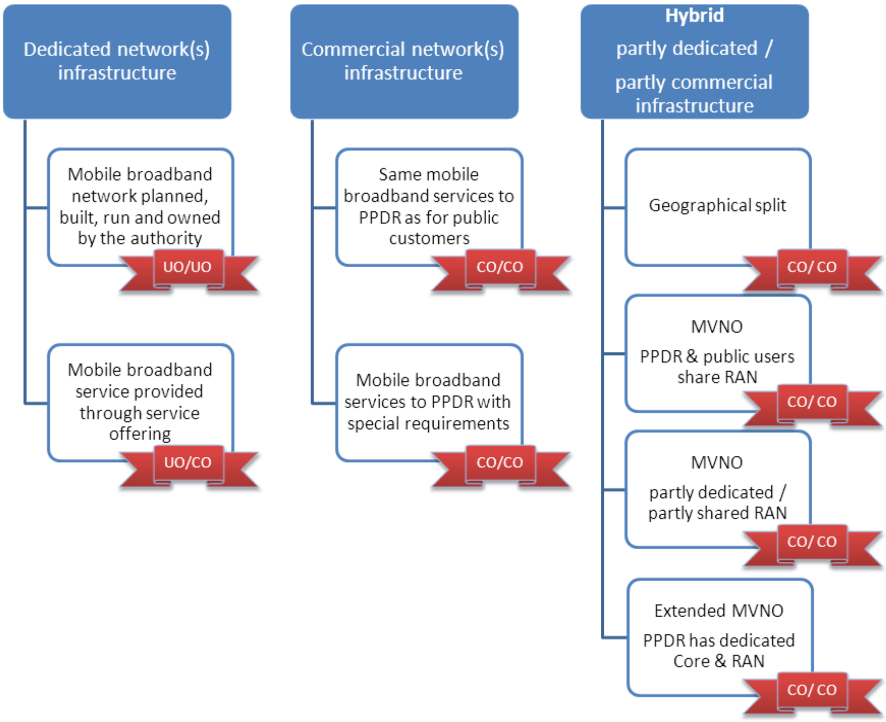

Dedicated network(s) infrastructure
Mobile broadband network planned, built, run and owned by the authority
UO/UO
Mobile broadband service provided through service offering
UO/CO
Commercial network(s) infrastructure
Same mobile broadband services to PPDR as for public customers
CO/CO
Mobile broadband services to PPDR with special requirements
CO/CO
Hybrid
partly dedicated /
partly commercial infrastructure
Geographical split
CO/ CO
MVNO
PPDR & public users share RAN
CO/ CO
MVNO
partly dedicated / partly shared RAN
CO/ CO
Extended MVNO
PPDR has dedicated Core & RAN
CO/ CO

Fig. 1. Models overview for PPDR communications system acquisition

7 TECHNICAL AND ECONOMIC RECOMMENDATIONS FOR FUTURE PPDR SYSTEMS

The following table summarises the selected recommendations elaborated by the PPDR-TC project.

Code	Recommendation title	Targeted organisations	Timeline for implementation
WTC1	Wireless technologies combination for PPDR communications	National Regulators; procurement groups	Short to medium-term
WTC2	Usage of a single wireless technology for PPDR communications	National Regulators; Standardization Bodies; industries; PPDR agencies	Medium to long-term
EP2	MVNO business models	National Regulators; MNOs with deployed LTE networks	Short to long-term
EP3	Differentiated Quality of Service (QoS) for PPDR users using commercial networks	PPDR agencies	Short-term
SR1	PPDR spectrum allocation based on “flexible harmonization”	National Regulators / Procurement groups.	Short to medium-term
SR2	Identify harmonised frequencies for Device-to-Device and Air to Ground Communication	National Regulators / CEPT.	Short to medium-term
TC1	Rapidly deployable resilient MESH networks	Network operators; PPDR procurement groups; System integrators; Vendors	Short to medium-term

8 ROADMAP FOR MIGRATION PATH TOWARDS FULL COMPLIANCE TO PPDR REQUIREMENTS

Finally, the PPDR-TC project elaborated the roadmap towards the adoption of a broadband PPDR communication network. The migration path to broadband PPDR is illustrated in Fig. 2. Detailed description of the major milestones of the proposed roadmap to be undertaken by the PPDR-TC community to reach a full-fledged broadband PPDR network is given in [5].

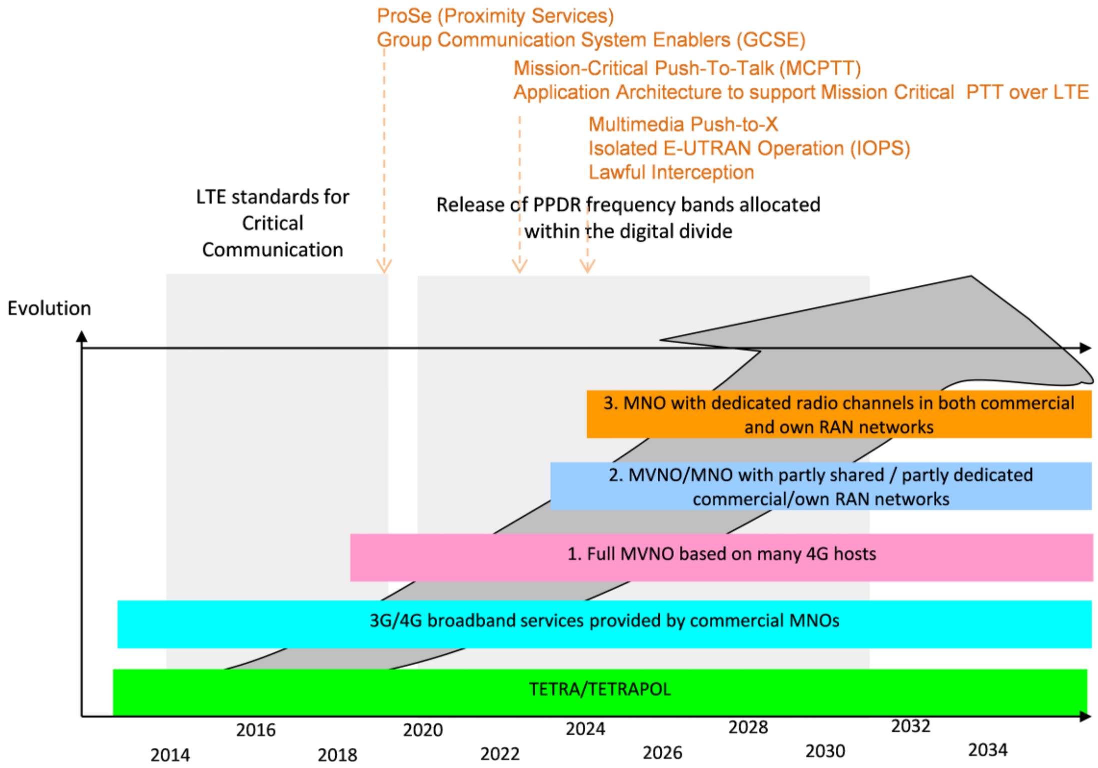

ProSe (Proximity Services)
Group Communication System Enablers (GCSE)
Mission-Critical Push-To-Talk (MCPTT)
Application Architecture to support Mission Critical PTT over LTE
Multimedia Push-to-X
Isolated E-UTRAN Operation (IOPS)
Lawful Interception
LTE standards for Critical Communication
Release of PPDR frequency bands allocated within the digital divide
Evolution
3. MNO with dedicated radio channels in both commercial and own RAN networks
2. MVNO/MNO with partly shared / partly dedicated commercial/own RAN networks
1. Full MVNO based on many 4G hosts
3G/4G broadband services provided by commercial MNOs
TETRA/TETRAPOL
2014
2016
2018
2020
2022
2024
2026
2028
2030
2032
2034

Fig. 2. Illustration of the migration path to broadband PPDR communications

REFERENCES

[1] Deliverable D2.1: *PPDR's Current and Future Scenarios,* FP7 EU PPDR-TC, July 2013 (public document available at http://www.ppdr-tc.eu).

[2] Deliverable D2.2: *PPDR's Needs and Requirements*, FP7 EU PPDR-TC, July 2013 (public document available at http://www.ppdr-tc.eu).

[3] Deliverable D3.2: *Spectrum Demand Modelling and Identification of Suitable Frequency Bands*, FP7 EU PPDR-TC, June 2014 (restricted document).

[4] Deliverable D4.1: *Business models*, FP7 EU PPDR-TC, March 2015 (public document available at http://www.ppdr-tc.eu).

[5] Deliverable D6.2: *Roadmap Towards Full Compliance To PPDR Requirements*, FP7 EU PPDR-TC, July 2015 (public document available at http://www.ppdr-tc.eu).

INTEGRATION ASPECTS OF NEXT GENERATION REAL TIME SERVICES FOR MARITIME SECURITY

Rolf Müller

Innovation Manager Maritime Security Systems

rolf.mueller@atlas-elektronik.com
ATLAS ELEKTRONIK GmbH, Sebaldsbrücker Heerstraße 235, 28309 Bremen
(Germany)

Abstract

The Project EMSec: real-time services for the maritime security - co-financed by the BMBF (German Ministry of Education and Research) - endeavors to support maritime security by improving the availability and accessibility of relevant data and information ashore and offshore. Within the project new services based on aircraft, optional piloted systems and earth observation satellites have been developed. The paper will present service integration challenges solved within EMSec from architectural, information fusion and usability perspectives. It will show how existing maritime security systems may be integrated with EMSec based on information exchange standards like the IALA IVEF standard. A practical example of this approach will be presented.

Keywords: Maritime Security; Coastal Surveillance; Unmanned Systems; Earth Observation Services

1 INTRODUCTION

EMSec is a BMBF (Federal Ministry of Research and Education) funded project, aiming to demonstrate the utility and value of integrating information derived by earth observation data and aircraft with conventional data streams for improved maritime control and maritime situation awareness. The target is to initiate a coordinated service network to provide all the national users (BOS – security agencies and organizations) with integrated maritime services in Real Time (RT). EMSec is intended to provide clear and credible responses to the following for main areas: Criminal Activities, Natural Hazards, Maritime Casualty and Collision, and Hazardous Material.

Fig. 1. Visualisation of EMSec context by DLR (© DLR)

The research & development within EMSec is scenario oriented. Scenarios covered include dangers of criminal activity, (natural) disasters and storm floods. Based on the analysis of the scenarios current information gaps and relevant data and information to object, orient, decide and act in the context of maritime security tasks have been identified. Major research actives within the project with respect to sensor related information sources covered the following areas:

- Detection, tracking and counter measures in case GNSS jammers,
- Algorithms for validation and verification of Automatic Identification System(AIS) data, including the detection of anomalies,
- Enhanced algorithms for information products derived from Synthetic Aperture Radar(SAR) Satellites including environmental information and objects Detection and Tracking,
- Development of a new and enhanced operating environment implemented as backbone of a Satellite Ground Control Station (GCS) to provide real time services with reduced overall processing time,
- Optimization and integration of air route planning and flight control for time critical mission systems into a real time service environment and
- The development of a specialized Modular Aerial Camera Systems for Maritime Security with high-resolution, real-time image maps of relevant maritime areas that automatically recognizes objects in the water, and independently sends the data to the control center.

On the systems integration level research actives cover [1]:

- The development of a real-time maritime situation awareness system (RMSAS),
- The development of a human-machine-interaction interface for maritime security (MaSiMMI) and
- The development of a maritime domain specific framework to support systems-of-systems engineering in the context of maritime safety and security applications

This paper will focus different integration aspects covering service integration, user integration and system integration.

2 DOMAIN ANALYSIS, SCENARIOS AND CHALLENGES

The International Maritime Organization (IMO) defines Maritime domain awareness as the effective understanding of any activity associated with the maritime environment that could impact upon the security, safety, economy or the environment. An effective understanding of the maritime domain is relevant to prevent, manage, and recover from maritime incidents [3]. Maritime surveillance is a prerequisite and indispensable to achieve MDA. The in deep analysis of the Future of Maritime Surveillance [3] concludes that MDA is a prerequisite for the effective use of the maritime domain emphasizing that shifts in global trade patterns, rivalries on resources and demographic trends in key coastal area, lead to an increasingly contested global maritime domain. “Interoperability and integration of existing maritime surveillance and monitoring systems, across different maritime sectors” is a key factor to achieve MDA [5]. Exiting systems addressed include Vessel Traffic Management Systems (VTS), Vessel Management Systems, Long Range Identification and Tracking, Automatic Identification System (AIS) and the Global Maritime Distress and Safety System (GMDSS). A vehicle on the European level to enable the generation of “maritime situational awareness” is the joint European activity to set up a Common Information Sharing Environment (CISE) for the European maritime domain. The CISE will support different user communities:

- Border Control,

- Fisheries Control,
- Defense,
- Maritime Safety and Security,
- Marine Environment,
- Customs and
- General Law Enforcement.

Each user community will be able to provide and subscribe relevant information. In many practical scenarios this requires the integration of incomplete, biased or event incomplete data (see [8], page 11). So a main goal of a maritime information system is to collect, request, and fuse and analyze different source ranging from sensors, other systems to databases. Exchange of data in the maritime domain is addressed by ongoing standardization activities and research actives related to higher level fusion services for the maritime domain (e.g. [12] [13], [14], [15]). So a major task of a maritime security system like EMSec is "The process of combining data and information from all sources into an integrated product from which significant and actionable knowledge can be derived. This includes assessing situations, identifying anomalous behavior, determining relationships, estimating or predicting activity/ intentions, or assessing potential impacts of changes, threats, risks and vulnerabilities" (see [8], page 22). A major task of systems of systems engineering is additional to understand the physical limitations, time and energy budget constraints and influence of environmental conditions on the service quality provided by the different systems of systems.

In Germany, it is the task of several government institutions on federal and county levels alike to ensure maritime security and to perform risk management. The specifics of the German requirements have given emphasis to additional requirements addressing collaboration and support of workflow management: "…It has been identified, that the maritime community is predominantly challenged by communication and cooperation issues. It is often not possible to exchange information between federal states and large organizations. There seems to be resistance/friction to share information on maritime situations amongst agencies and on the status and availability of their forces/agents. This information exchange is either prohibited or fuzzy/not properly regulated. …" (See [1]).

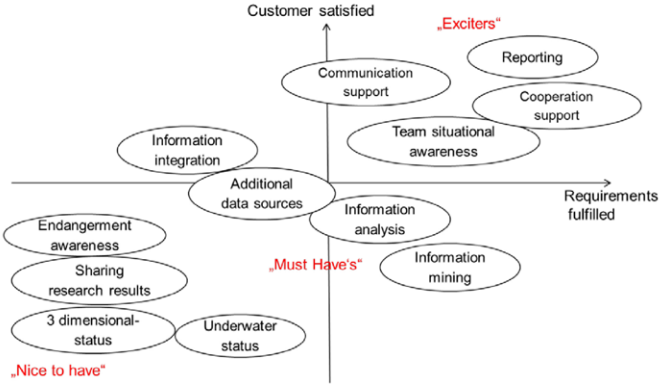


Fig. 2. Identified User Requirements for RMSAS and MaSiMMI ([1])

3 SERVICE INTEGRATION

A major research and development topic within the project is the integration of the different services in a real time service world. Both RMSAS and MaSiMMI provide the core layers of the real-time service system of EMSec. RMSAS interfaces all data services and provides the related services to MaSiMMI. The task of MaSiMMI is provide all services to the user and support him in the interaction with EMSec based on his role, his task and his workload.

3.1 RMSAS: Real-time Maritime Situation Awareness System

The Real-time Maritime Situation Awareness System is the heart of EMSec. It is capable of integrating data from different data sources with source specific semantics and data context. RMSAS is designed as a distributed federated system. The description in this part is derived from [2] which provide a detailed insight in the challenges solved by our project partner AIRBUS Defence and Space responsible for the RMSAS subsystem of EMSec.

The RMSAS is implemented in EMSec as a system of systems to:

- integrate vessel data coming from various sensors,
- enrich these data with data from other sources (e.g. open data),
- harmonize these data using established maritime standards,
- retrieve new information from these integrated data,
- infer knowledge from this information,
- retrieve and deliver this knowledge in near real-time,
- create a maritime domain awareness for the end user, and
- Enable maritime decision makers to handle maritime situations more efficiently.

RMSAS implements a federated information system based on separate services (SOA). Data are integrated in RMSAS in near real-time, next they are consolidated based on semantic data models and techniques and provided to the end user as information products. Ontologies are used in the consolidation of these heterogeneous data.

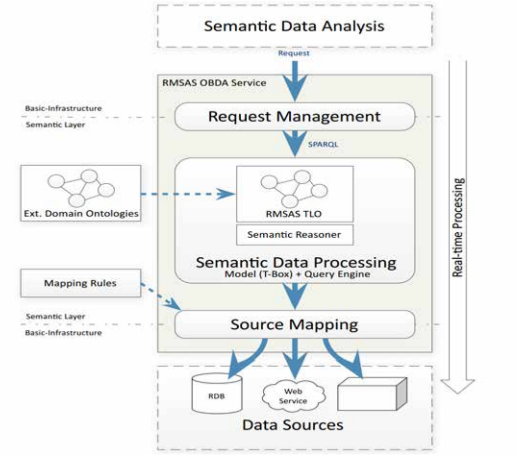


Fig. 3. Request Management within EMSec provided by RMSAS ([2])

Within EMSec RMSAS solves the task of Service and Information Source Integration. RMSAS provides a consistent service interface to MaSiMMI which implements the user interface to the EMSec real time services.

3.2 MaSIMMI: Real-time Maritime Situation Awareness System

MaSiMMI provides the user interface for EMSec including the representation of the different services and assistance functions to support the interaction of the operator with the real time services. MaSiMMI provides the following services:

- Providing a context and role dependent, ergonomic graphical user interface
- Visualizing maritime situations in 2D and 3D employing mixed reality approaches
- Managing workflows e.g. command and control cycles
- Enabling seamless cooperation with other users and agencies using multimodal interfaces
- Data source management regarding validity, plausibility, reliability, etc.
- Supporting user decisions through model-based interaction with cognitive systems

MaSiMMI is based on a User Interface framework named Extended Visual Objects (EVO). EVO allows the easy configuration of user interfaces for command and control and situational awareness system based on the selection and orchestration of fragments. This approach is proven in real world application and allows static adaption of the interface to specific tasks needed by an operator acting in a maritime security role e.g. as a Search and Rescue on Scene Commander. Within the EMSec project it was original planned to base MaSiMMI on Microsoft .net Windows Presentation Foundation (WPF). This approach gave a good technical start to build MaSiMMI but has been in contradiction to Lessons learned from user workshops which gave a clear focus that a good solution should integrate with existing maritime information systems. This let finally to the decision to switch over to a Java FX 8 based UI Technology based on the higher degree of platform independence and support of HTML5.

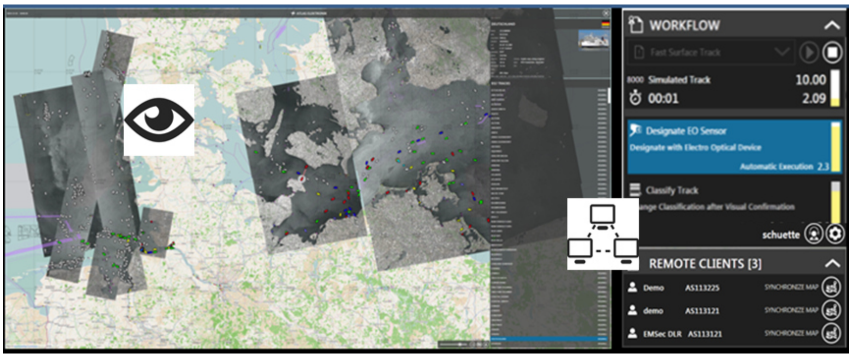

WORKFLOW
Fast Surface Track
8000 Simulated Track
10.00
00:01
2.09
Designate EO Sensor
Designate with Electro Optical Device
Automatic Execution 2.3
Classify Track
ange Classification after Visual Confirmation
schuette
REMOTE CLIENTS [3]
Demo AS113225 SYNCHRONIZE MAP
demo AS113121 SYNCHRONIZE MAP
EMSec DLR AS113121 SYNCHRONIZE MAP

Fig. 4. MaSiMMI integration of NUI, Cognitive Support Functions, Workflow and Collaboration

Major extensions to classical user interfaces of maritime security and safety systems featured by MaSiMMI to extend the integration of the user include:

- Integration of Natural User Interfaces e.g. eye tracking, multi touch, speech
- Integration of workflow support and assistance
- Integration of information exchange with remote clients (users)

Additional MaSiMMi implements services to allow access to different semantic services provided by the RMSAS system including access to satellite images, image data from aircraft, environmental data derived from SAR images, anomaly services based on AIS and control and display of airplanes and real time mission data.

4 SYSTEMS ENGINEERING AND INTEGRATION

Systems engineering and integration in the domain of maritime security applications requires more than the development of good Service Oriented Architectures and Natural User Interfaces. Both of these elements are pre-requisites for good maritime security systems, but they do not a guarantee a sound solution. Working experience shows that in addition system engineering including analysis and simulation is required. In this chapter we describe our research activities related to Model based System Engineering. The goal of our research is to provide a Maritime Domain Specific Architecture Framework tailored for Maritime Security Applications.

UML and SysML provide a common language to describe software and systems in a defined way supported by standard modelling tools. Within the military context so called architecture frameworks have been developed to guide the system engineering process, e.g. the NATO Application Framework (NAF). The NAF provides standard views to support the engineering process which cover operational, technical and organizational aspects of the system engineering discipline. NAF itself has its roots in US (DoDAF) and UK (MoDAF) frameworks. The OMG provides for all three of them a Unified Profile (UPDM) as a graphical enterprise modelling language which supports views of NAF, MoDAF and DoDAF. This process is complex and the engineering team has to align and take into account a number of interrelated views which leads to a complex and sometimes error prone analysis and design approach. Within the EMSec project we decided to follow a design approach based on SYSMOD developed by Tim Weilkiens ([11]). SYSMOD is an extension to the SysML/UML language and provides a core engineering profile with additional elements relevant for the Maritime Information Systems domain, e.g. sensor, actuator environmental effect and external system building blocks. To support the analysis and design of sound maritime information systems we added additional stereotypes as a language extension to SysML to support the engineering process within the EMSec project.

4.1 IALA Specification as starting point for EMSec MBSE

As a starting point we decided to implement an IALA profile. The IALA standard already defines scenarios, standard target types and characteristics as well as quality goals for Vessel Traffic Systems. This approach gave us a good starting point to model different aspects relevant for maritime system engineering. Based on the fact that the IALA standard mainly addresses Safety Applications we had to add relevant target characteristics related to uncooperative Target Types not covered by typical vessel traffic information systems.

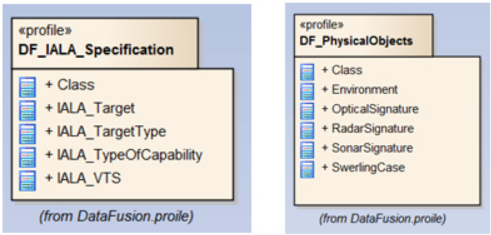


Fig. 5. sterotypes derrived from IALA specifications

Additional we added profiles to support radar system performance analysis and prediction as required to enable Radar simulation support [18] including environmental aspects to describe weather conditions in specific scenarios.

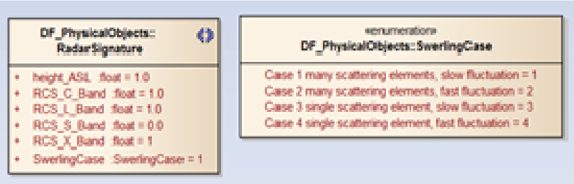

DF_PhysicalObjects::
RadarSignature
height_ASL :float = 1.0
RCS_C_Band :float = 1.0
RCS_L_Band :float = 1.0
RCS_S_Band :float = 0.0
RCS_X_Band :float = 1
SwerlingCase :SwerlingCase = 1
«enumeration»
DF_PhysicalObjects::SwerlingCase
Case 1 many scattering elements, slow fluctuation = 1
Case 2 many scattering elements, fast fluctuation = 2
Case 3 single scattering element, slow fluctuation = 3
Case 4 single scattering element, fast fluctuation = 4

Fig. 6. Details of radar signature model

An advantage of MBSE is the concept of one source for all system aspects. A next step in the planned roadmap is to export scenarios defined in our system model to the radar performance simulation tool we use in-house named ASIM/ASCAD.

4.2 EMSec specific

Within the initial Domain Specific Model derived from the IALA standard several aspects relevant for security scenarios have been missing, e.g. to describe target characteristics of asymmetric targets e.g. fast boats or skiffs. Also different environmental areas like had to be added. Another part which is not covered by the IALA platform is the characteristics of the platform carrying the sensor, for moving platforms like the earth observation satellites or maritime patrol aircrafts revisit times and waypoint plans are important system aspects for the validation of the system. In [18] the author guides though the operational concept for oil spill detection at the Brazilian coast. In this scenario an oil spill defense concept of operation is developed and the operational scenario is analyzed to derive technical requirements related to earth observation satellites with Synthetic Aperture Radar.

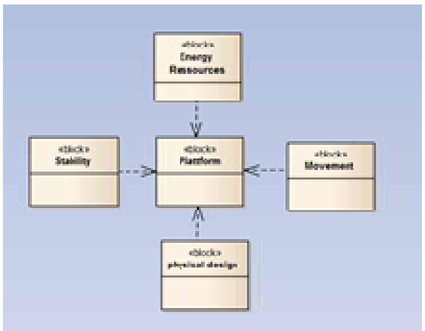


Fig. 7. Relavant Plattform aspects

As a result we added a profile to the engineering model to reflect platform aspects which influence the quality of the situational picture and additional workflow elements for analysis of functional workflows.

5 RESULTS AND FUTURE WORK

The EMSec project includes a bundle of different R&D activities with on common goal: to provide sound real time services for maritime security which close existing gaps in today's situational awareness. Three different levels of integration are addressed within the scope of the project: service integration and orchestration (RMSAS), user integration and support and a framework featuring model based system engineering to understand capabilities and limitations of the overall systems of systems.

REFERENCES

[1] Stefan Brüggemann, Sebastian Förster, "User requirements for real-time services for the maritime security" (ISIS2014)

[2] Stefan Brüggemann, Konstantina Bereta, Guohui Xiao, and Manolis Koubarakis, „Ontology-based Data Access for Maritime Security", 13th ESWC 2016, Create, Greece

[3] Heiko Borchert, “The Future of Maritime Surveillance in an Era of Contested Maritime Domains” (Lucerne: Sandfire AG, 2011).

[4] IMO, “AMENDMENTS IAMSAR MANUAL-Volume I”, MSC.1/Circ. 1367 Annex, page 1, 24 May 2010.

[5] European Commission / Joint Research Centre Ispra, Italy, “INTEGRATED MARITIME POLICY FOR THE EU Working Document III on MARITIME SURVEILLANCE SYSTEMS” 14 June 2008, Public .

[6] IALA, “Vessel Traffic Services Manual”, Edition 5, 2012

[7] Thomas Strasser, “Integrated Maritime Surveillance (IMS) – Common Information Sharing Environment (CISE)”, DG Mare, 22.11.2011

[8] COE CSW, CJOS COE, MARSEC COE, Beyond Border Consulting Ltd, NMIOTC, “Maritime Situational Awarness from fragmented sea surveillance to combined maritime situational awarness”, April 2015

[9] IALA Recommendation V-145, “On the Inter-VTS Exchange Format (IVEF) Service”, Edition 1June 2011

[10] INCOSE, “SYSTEMS ENGINEERING VISION 2020”, Revsion 2.03, September 2007, Doc-No: INCOSE-TP-2004-004-02

[11] Tim Weilkiens, “Systems Engineering mit SysML/UML”, dpunkt.verlag, 3. Auflage 2014, ISBN 978-3-86490-091-4

[12] OMG, „Shared Operational Picture Exchange Services (SOPES) Information Exchange Data Model (IEDM)“, Version 1.0, Date May 2011

[13] www.mise.mda.gov, “National Information Exchange Model – Maritime (NIEM-M) Domain”, NIEM V2.1, 18 December 2012

[14] EU R&D project CoopP, “Test Project on Cooperation in Execution of Various Maritime Functionalities at Sub-Regional or Sea-Basin Level in the Field of Integrated Maritime Surveillance (CoopP)-Final Rerport”, March 2014

[15] Fulya Tuncer Cetin, Burcu Yilmaz, Yildiray Kabak, Ju-Hwan Lee, Cengiz Erbas, Erdem Akagunduz, Sang-Jae Lee, “Increasing Maritime Situational Awarness with Interoperating Distributed Information Sources”, 18th ICCRTS, 2013

[16] Rommel N. Carvalho, Richard Haberlin, Pailo Cesar G. Costa, Kathryn B. Laskey, KC Chang, “Modelling a Probalistic Ontology for Maritime Domain Awarness”, Proceedings of the Fourteenth International Conference on Information Fusion, July 2011

[17] Fischer, Y, Beyer, J, “Ontologies for Probabilistic Situation Assessment in the Maritime Domain”, CogSIGMA 2013

[18] Skolnik, Merrill I., “Radar Handbook”, Mc Graw Hill, Second Edition, 1990, ISBN 0-07-057913-X (for Definition of Swerling Case, page 2.22)

[19] Moreno de Queiroz Figueiredo, “MONITORAMENTO DE DERRAMAMENTO DE ÓLEO NO MAR UTILIZANDO MÚLTIPLOS SATÉLITES SAR – O DESAFIO DO SISGAAZ Tempo de Revisita Desafio do SisGAAz Resultados Aluno”, 2012, https://prezi.com/psqcm2bk2dxy/gfhffh/

FROM MULTIFACETED INFORMATION TO COHERENT AND WELL-FOUNDED SUGGESTIONS FOR A LAND TRANSPORT SECURITY RESEARCH AGENDA: PROCEEDINGS AND RESULTS OF THE FP7 PROJECT CARONTE

Joachim Burbiel[1] and Sonja Grigoleit[2]

[1] *joachim.burbiel@dlr.de*
DLR Project Management Agency, European and international cooperation, Heinrich-Konen-Straße 1, 53227 Bonn (Germany)

[2] *sonja.grigoleit@int.fraunhofer.de*
Fraunhofer Institute for Technological Trend Analysis INT, Department for Technology Analysis and Strategic Planning, Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

The main aim of the CARONTE project (www.caronte-project.eu, September 2014 to February 2016) was to provide well founded input to strategic research planning in the domain of land transport security, especially on the European level. In order to achieve this goal, information from various sources was analysed. The project culminated in the prioritisation of possible research fields and the development of several sets of ideas for future research.

Keywords: land transport security, research agenda

1. INTRODUCTION

Europe’s prosperity relies on effective and safe transport systems. Any attacks or disturbances to land freight or passenger transport would have a major impact on economic growth, territorial cohesion, social development, and even on the life and health of European citizens. Unfortunately, there are weaknesses in Europe’s land transport security, and these issues are diverse and complex. Continuous and coordinated efforts are needed to address them.

For 18 months, the CARONTE project has been working on issues like “What are the security challenges to land transportation and how can a strategic research agenda for the EU efficiently help to find answers?” During this time the consortium has carried out analyses on: the state of the art in securing land transportation, the threats facing the sector, and the current gaps and requirements for future research. On the basis of these assessments CARONTE has defined a future research agenda for land transport security that focuses on the sector’s emerging risks while avoiding any doubling-up of research elsewhere. Special care has been taken to base the research agenda on the concept of fluent and efficient flow of passengers and goods, while bearing in mind the relevant ethical, societal and legal aspects.

Within this project “land transport” encompasses road, rail, and, to a lesser degree, inland waterway transportation, including the relevant interfaces. Both passenger and freight transportation were considered.

2. THE CARONTE APPROACH

Before any work was begun, the CARONTE consortium had to define common terms to forge a clear picture of their meanings in a land transport security context. Thus in the context of this project, the following terms were applied:

Need: A necessary requirement for the operability of land transport (e.g. secure critical infrastructures).

Solution: A technical or organisational measure to ensure that a need is met.

Gap: If the currently available solutions are not adequate to completely satisfy a need, there is a (capability) gap.

Threat: A potential event that challenges the functioning of transport systems. Countering a threat might be a "need" which requires "solutions".

In addition to that, a working definition of what "security" means had to be found to determine the scope of the project. From all conceivable security issues, the CARONTE project focussed on those that are caused by wilful acts of persons (mainly with criminal or terrorist intents). This definition of security is illustrated in Fig. 1.

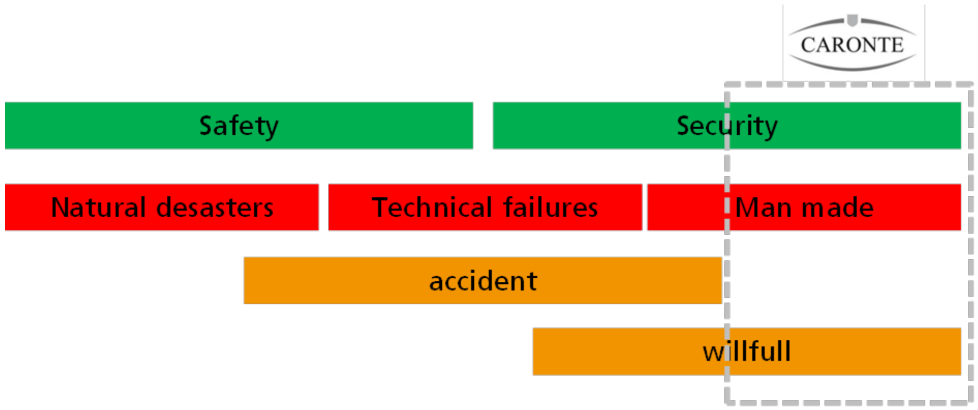


Figure 1: Defining the scope of the CARONTE project.

The sources of information used in the CARONTE project were manifold. More than a dozen meetings with internal and external experts ensured that as many voices as possible were heard. In this context, two meetings of the high level advisory board and two conferences with a total of more than 120 participants were of special importance. In addition to this, expert opinion was collected through questionnaires and structured interviews. The second important source of information was data on recently completed and on-going research projects relevant for the domains covered by the CARONTE project. More than 120 European and national research projects were evaluated in order to determine the state of the art, current research priorities, and existing research gaps. The third kind of sources were official policy papers, existing research programmes, and research agendas developed both by professional bodies and previous research projects.

2.1 Prioritisation of research issues

The information generated within the CARONTE project using the sources described above were collected, condensed and systematically sorted.

On this basis a longlist of "needs/requirements" for land transport security and corresponding "possible solutions" were generated and validated. The items on the longlist were further analysed systematically through a multi-criteria approach named "Weighted-Bit Assessment Table for Land Transport Problems and Solutions" (WBAT-LTPS).[1] In addition to this, more than one hundred research projects of relevance for land transport security were evaluated concerning their connection to the items on the longlist. Finally, existing policy papers, research programmes and strategies, and centres of excellence in land transport security were analysed.

As this longlist generated contained more than 30 “needs/requirements” and approx. 50 “possible solutions”, further prioritisations were necessary in order to develop a meaningful research agenda.

For the preparation of a useful roadmap the prioritisation was performed in three different classes (see Fig. 2).

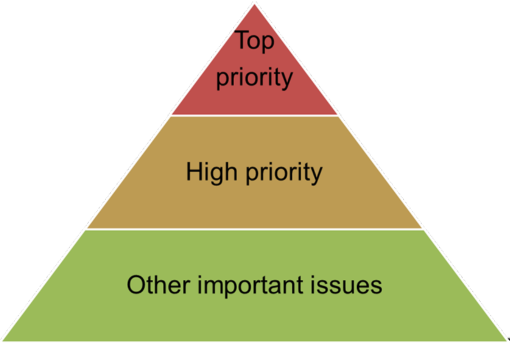


Figure 2: Prioritisation classes.

A set of seven criteria was developed to sort the issues of the longlist of “needs/requirements”. These criteria were designed to take into account as much of the information previously gathered as possible. By a deliberate choice, no “mathematical system” was devised to “calculate” a final priority score from the individual judgements, as this would only simulate calculability where in fact expert opinion is key.

These individual criteria are:

1 **Expert opinion** (stated during the CARONTE workshops and expert advisory groups)

2 Is this “need/requirement” a **burning issue** to be dealt with or is it less urgent or less important?

3 **Number of research projects** dealing with this “need/requirement” or providing solutions (is this issue already sufficiently addressed by current research work or are there only insufficient research projects dealing with this subject)

4 **Research is essential** for meeting the need or requirement (is research urgently needed or are there measures (e.g. new regulations, networking activities) other than research better suited to close the gap)

5 **Connection to land transport** (is this “need/requirement” a land transport issue or a more general problem and not specific for land transport)

6 General impression from the **WBAT-LTPS** (is there a serious lack of knowledge regarding the threat itself or is the threat well described, do affordable solutions exist to deal with the threat, is the information about possible solutions sufficiently disseminated among the people who need to know, are national or international standards and processes in place, do relevant authorities and first responders work successfully together)

7 **Connection to current policies** (is this “need/requirement” frequently mentioned in policy papers or is too new to be mentioned in policy papers or is it not considered to be a priority in policy papers)

On this basis a draft priority list was generated, discussed and agreed upon during a CARONTE workshop.

3. RESULTS AND GENERATION OF RESEARCH IDEAS

As a result of the process described above, the following priority lists were generated. The sequence of the items on the three individual lists is arbitrary.

Top priority issues:

- Staying operational in the event of a cyber-incident
- Timely and efficient threat detection (incl. Early threat detection in trains, stations and on track)
- Special security problems of railways as open systems

High priority issues:

- Balancing security requirements and privacy demands of passenger
- Security awareness of personnel and customers
- Crisis Management
- Security by design
- Security retrofit (ICT)
- Secure communication links for traffic control systems
- Protection of autonomous vehicles against cyber-attacks
- Secure critical infrastructures (cyber/road system)

Other important issues:

- Sharing of best practices among stakeholders
- Effective communication between companies, police and other administrations about threats
- Efficient security solutions (lifecycle costs)
- Sufficient financial support for the implementation of security measures
- Sufficient financial support for security research
- Applying the best security measures and technologies
- Securing legacy systems (physical)
- Secure critical infrastructures (especially tunnels and bridges)
- Data security / privacy
- User-friendliness of security systems
- Keeping pace with developing risks and threats
- Secure communication in freight transport chains
- Limiting damage in the case of an attack
- Professional security management
- Common standards and protocols for rail security
- Secure truck parking and protection of driving personnel
- Protection against inside threats
- Avoidance of dangerous routes or parking lots

The three top priorities and eight high priority issues were then analysed in more depth. For the remaining eighteen items classified to be important for land transportation security, short evaluations were generated.

These in-depth analyses of the 11 items identified to be of top or high priority was conducted in a five-step approach:

1. In a first step, **research projects** (with a focus on, but not limited to, European Framework Programmes) that had been identified to be connected to the individual topics were re-visited, and their relevance for a possible research agenda was thoroughly assessed.
2. In a second step, the research projects analysed were **clustered** to achieve a systematic overview of relevant research areas.
3. In the next step, available **research roadmaps and policy papers** and additional documents were analysed.
4. The fourth step compared the relevant **threats and gaps** of land transport (identified during the course of the CARONTE project) of this top or high priority area with the research activities and priorities identified in steps 1 to 3. Consequently, threats and gaps not sufficiently covered were identified.
5. The final step consisted in the description of **urgent research needs and possible approaches**, based on the information obtained in the previous steps.

Thus, the final output of this in-depth analysis is a list of research needs or research ideas how to overcome the security gaps identified in and around these 11 top and high priority areas described above. The last task of the CARONTE project was to sort these research ideas along the lines of the European security research programme. More than 20 research ideas are presented for the “Fight against Crime and Terrorism” (FCT) area, a total of 15 in the areas “Critical Infrastructure Protection” (CIP) and “Disaster-resilience: safeguarding and securing society” (DRS), and more than 20 ideas that address the “Digital Security Focus Area” (DS). A summary of these research ideas is presented in Fig. 3 to 5.

4. CONCLUSION

All in all, the CARONTE project has achieved its goal of providing input to strategic research planning in the domain of land transport security. Information from more than a hundred experts was collected through various methods, more than 120 ongoing and recently completed research projects were evaluated, and a large number of relevant policy papers and research programmes were analysed. This complex information was sorted and processed in a transparent way in order to obtain research ideas that are highly relevant for current and future strategic research planning. These ideas have been categorized and are presented in a way that allows an easy uptake in the strategic research planning processes of the European Commission and other authorities.

The CARONTE Consortium hopes that the work performed during this project will provide inspiration to all persons involved in security research planning, especially in the domain of land transportation.

REFERENCES

[1] Burbiel, J; Grigoleit, S.; Schulze, J. (2008) *The weighted- bit assessment table of hazardous chemicals.* Deutsche Pharmazeutische Gesellschaft (Jahrestagung 2008), Bonn, pp. 20.

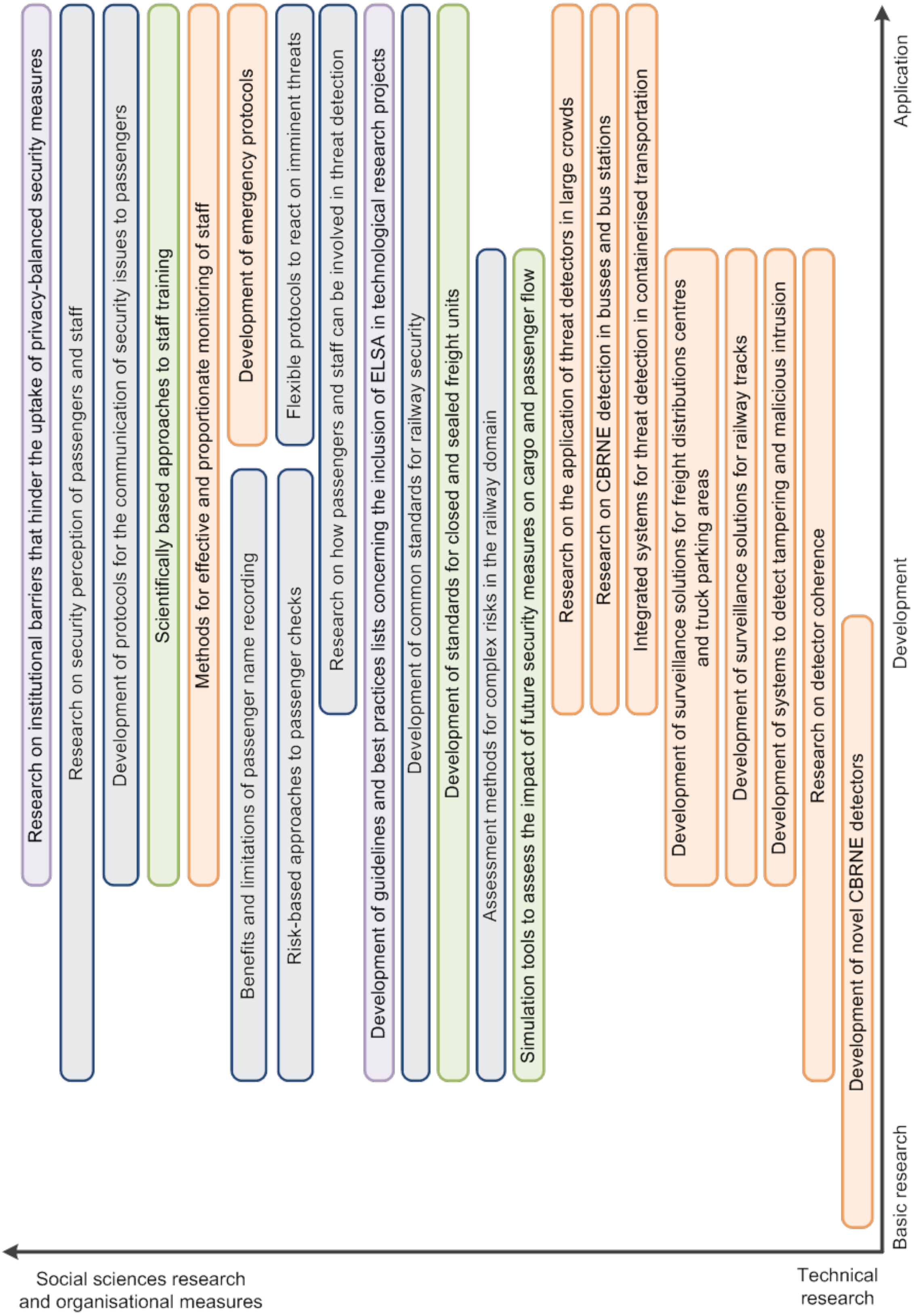

Research on institutional barriers that hinder the uptake of privacy-balanced security measures
Research on security perception of passengers and staff
Development of protocols for the communication of security issues to passengers
Scientifically based approaches to staff training
Methods for effective and proportionate monitoring of staff
Development of emergency protocols
Benefits and limitations of passenger name recording
Flexible protocols to react on imminent threats
Risk-based approaches to passenger checks
Research on how passengers and staff can be involved in threat detection
Development of guidelines and best practices lists concerning the inclusion of ELSA in technological research projects
Development of common standards for railway security
Development of standards for closed and sealed freight units
Assessment methods for complex risks in the railway domain
Simulation tools to assess the impact of future security measures on cargo and passenger flow
Research on the application of threat detectors in large crowds
Research on CBRNE detection in busses and bus stations
Integrated systems for threat detection in containerised transportation
Development of surveillance solutions for freight distributions centres and truck parking areas
Development of surveillance solutions for railway tracks
Development of systems to detect tampering and malicious intrusion
Research on detector coherence
Development of novel CBRNE detectors
Application
Development
Basic research
Social sciences research and organisational measures
Technical research

Figure 3: Tentative roadmap for "Fight Against Terrorism" (FCT) (the blue items relate to railway security, the orange items relate to threat detection, the purple items relate to balancing security and privacy, the green items relate to other domains)

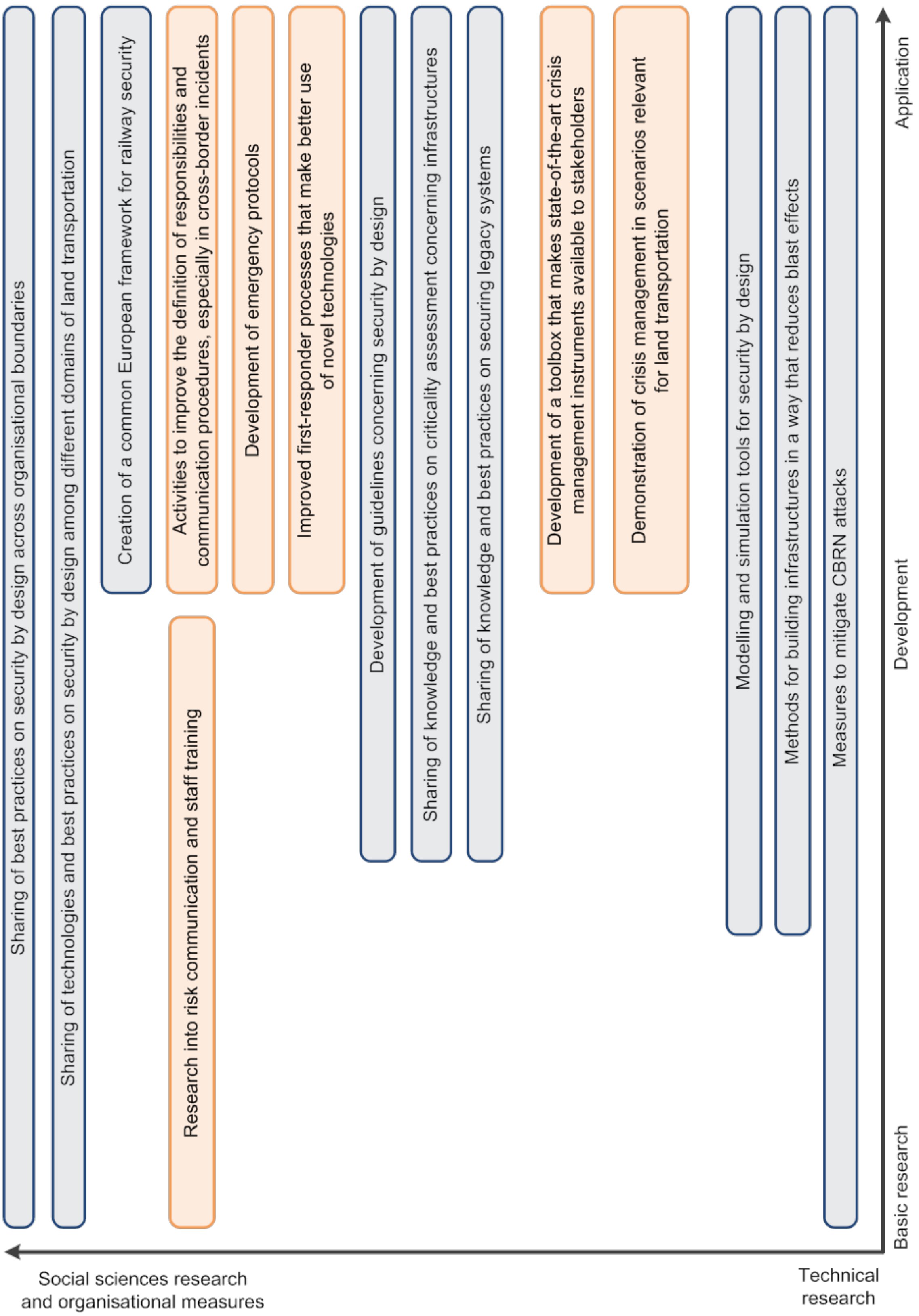

Sharing of best practices on security by design across organisational boundaries
Sharing of technologies and best practices on security by design among different domains of land transportation
Creation of a common European framework for railway security
Activities to improve the definition of responsibilities and communication procedures, especially in cross-border incidents
Research into risk communication and staff training
Development of emergency protocols
Improved first-responder processes that make better use of novel technologies
Development of guidelines concerning security by design
Sharing of knowledge and best practices on criticality assessment concerning infrastructures
Sharing of knowledge and best practices on securing legacy systems
Development of a toolbox that makes state-of-the-art crisis management instruments available to stakeholders
Demonstration of crisis management in scenarios relevant for land transportation
Modelling and simulation tools for security by design
Methods for building infrastructures in a way that reduces blast effects
Measures to mitigate CBRN attacks
Application
Development
Basic research
Social sciences research and organisational measures
Technical research

Figure 4: Tentative roadmap for “Critical Infrastructure Protection” (CIP) and “Disaster-resilience: safeguarding and security society” (DRS) (the blue items relate to incident prevention and threat mitigation, the orange items relate to crisis management)

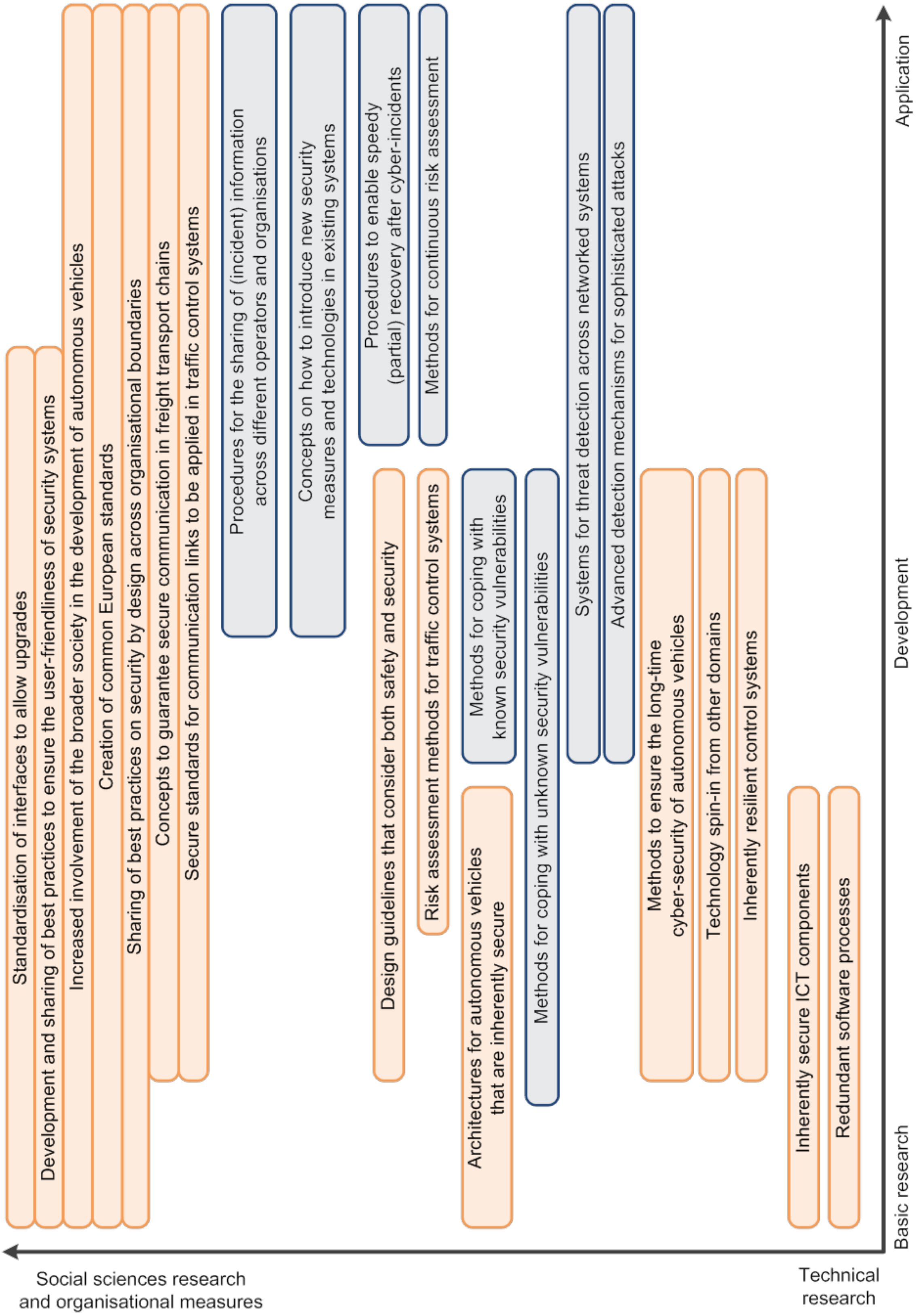

Standardisation of interfaces to allow upgrades
Development and sharing of best practices to ensure the user-friendliness of security systems
Increased involvement of the broader society in the development of autonomous vehicles
Creation of common European standards
Sharing of best practices on security by design across organisational boundaries
Concepts to guarantee secure communication in freight transport chains
Secure standards for communication links to be applied in traffic control systems
Procedures for the sharing of (incident) information across different operators and organisations
Concepts on how to introduce new security measures and technologies in existing systems
Procedures to enable speedy (partial) recovery after cyber-incidents
Methods for continuous risk assessment
Design guidelines that consider both safety and security
Risk assessment methods for traffic control systems
Methods for coping with known security vulnerabilities
Architectures for autonomous vehicles that are inherently secure
Methods for coping with unknown security vulnerabilities
Systems for threat detection across networked systems
Advanced detection mechanisms for sophisticated attacks
Methods to ensure the long-time cyber-security of autonomous vehicles
Technology spin-in from other domains
Inherently resilient control systems
Inherently secure ICT components
Redundant software processes
Application
Development
Basic research
Social sciences research and organisational measures
Technical research

Figure 5: Tentative roadmap for the “Digital Security Focus Area” (the blue items aim at securing existing systems, the orange items aim at securing future systems)

USING UNMANNED VEHICLES TO ENHANCE PORT FACILITY SECURITY - INTRODUCTORY FRAMEWORKS WITH REGARD TO THE ISPS-CODE AND OTHER REGULATIONS

Michael Weickhardt[1]

[1] michael.weickhardt@mgt.the-klu.org

Kühne Logistics University, Großer Grasbrook 17, 20457 Hamburg (Germany)

Abstract

Unmanned vehicles have evolved over the past decade in operational safety, usability and reduced costs wherefore implementation opportunities have increased significantly as a result of former military driven research and development now entering commercial /civil markets. Ports operate in a complex area and have advanced requirements on safety and security given their sensible infrastructure with multiple supply chains, especially after the 9/11 attacks have shown that attacks on transportation modes are no fiction. Those aspects create a natural demand for innovative approaches to improve or assist existing procedures in safety and security. The focus of this paper is to provide a general framework for drone usage in port operations and an analysis on proper integration of such technology in existing legal requirements. Although this paper is limited to ports its findings are applicable to other areas as well therefore providing a valuable content for operator of sensible logistic infrastructures in general.

Keywords: Port Safety, Port Security, Maritime Inspections, Sensible Infrastructure, Unmanned Aerial Vehicle (UAV). Remotely Operated Vehicle (ROV)

1 INTRODUCTION

During the last decades the technological advances of unmanned systems began establishing themselves in civil and commercial areas providing a valuable service to a multitude of customers through complex systems. Generally spoken, the difference between an unmanned aerial vehicle (UAV) and a simple model airplane are defined by the level of potential autonomy and the payload that is differentiated in four categories according to [11] namely sensors, relays, weapons, cargo. The major trade-off of payload on a UAV is flight durability and the different operation areas of civil/ commercial UAVs led to a multitude of different systems that entered the market in the most recent past. According to [14] the number of industrial produced systems has risen from 655 to 2.059 over the past decade. Other sources refer to higher global numbers of unmanned vehicle systems and considering the amount of self-build and upgraded systems it is likely that higher amounts of operated unmanned systems have entered the market. According to the European Commission (2007) for example the number of UAVs deployed globally on operations has increased from around 1,000 to 5,000 systems between 2004 and 2008 only. According to annual studies of [16] the global UAV market value has almost doubled from 55 billion USD in 2007 to 95 billion UAD in 2015 while global UAV expenditures rose from 3,4 billion USD to 10 billion USD p.a. over the same time, although these numbers vary among different sources. The main drivers of this rapid development (generally agreed upon among different sources) is the widespread availability of electronic sensors, GPS devices, Wi-Fi receivers, and smartphones that have reduced the overall cost of unmanned systems, enabling manufacturers to enter the market without worrying about the supply of components [4]. The lower cost-options of recent technologies already deliver a platform with easy-launch and recovery, integrated communications and sensors payloads, and user-friendly control station hardware for a relatively cheap price that allows small- and medium size companies to consider their use (see [17]). Unmanned aircraft will without doubt augment some manned flight operations

Table 1: Development of Industrial Produced RPAS Systems

RPAS Development Status	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Proof-of-concept demonstrator	85	150	230	217	266	240	236	184	184	191	171
Development continuing	310	333	470	589	697	702	773	560	586	628	650
Ordered as test/demo system	8	8	7	17	20	43	44	25	25	24	23
Ordered, entering services	29	38	45	49	60	15	22	18	19	19	21
In Inventory and/or in service	134	100	110	128	160	158	162	178	193	215	221
Developed and market ready	72	95	119	137	209	278	296	413	446	535	660
No longer in production or development	17	39	40	40	53	83	90	203	255	272	313
Total	**655**	**763**	**1.021**	**1.177**	**1.465**	**1.519**	**1.623**	**1.581**	**1.708**	**1.884**	**2.059**

Source: [14]

while displacing others as they generally require two to five times the weight of the pilot in specialized equipment needed to support him [15]. This paper focusses on the integration of unmanned systems in port facilities to assist and/or conduct legally required safety and security operations. Even when focusing on ports, the evaluated frameworks and findings of this paper can furthermore be applied to other related sensible infrastructures with an advances security demand that, however, cannot be evaluated in detail due to the limitations of this paper. When evaluating unmanned vehicles for the use in port facilities this paper not only focusses on unmanned aerial vehicles (UAV) but also on remotely operated vehicles (ROV) that can be applied below the water surface. The latter has been of a limited academic interest so far compared to UAVs but nonetheless the recent technological advance allows for a consideration of such technology in this paper's context as well and first studies already revealed successful operations using ROVs (see [12] [1]). Since this paper focusses on the use of both UAV and ROV it will continue with the term “unmanned vehicles” likewise accounting for both potential aerial and underwater operations. Due to the limitations of this paper towards civil/commercial uses of unmanned systems, the focus lies on classes between Nano and short range classification arguing that those classes provide cost efficient and reliable services for port facilities given the recent technological developments. This paper starts by providing a brief discussion of existing usage, classification and barriers towards unmanned systems usages that arose from this paper's literature review. Main aspects of the first chapter are two aspects. First, the theoretical introduction of a new unmanned system class – the operational UAV class – describing those systems that are of use for the majority of private companies dealing with sensible infrastructure on the one hand but on the other hand significantly vary from tactical classes in mass, endurance, altitude and range. Second, among the wide discussion of barriers and risk factors going along with unmanned systems this paper provides a framework of the most applicable factors for ports and other sensitive infrastructures. Chapter 2 introduces the legal background of port operations linking those to unmanned operation opportunities. Furthermore a port specific risk assessment framework for UAV and ROV is introduced.

1.1 Usage and classification of Unmanned Vehicles

UAVs present a viable alternative to manned vehicles, especially for deployment in dull, dirty, or inherently dangerous missions [15]. Potential uses of unmanned vehicles have long been evaluated among conducted studies (See [20] [6] [15] [7]). The classification of unmanned vehicles varies according to the underlying reference and specific countries or organizations. This paper follows the approach of [19] who differentiates 13 classes based on the factors of mass, range, altitude and endurance of the systems differentiating strategic operations (global, covering a large geographic area), tactical operations (regional, covering a small geographic area) and special tasks. Both the strategic aspect and special tasks can be accounted for in the military usage or advanced research operations while strategic operations follow a more commercial or civil usability. Micro and Mini classes in that respect were regarded separately compared to other approaches like [14]. This paper follows this approach arguing that those classes have benefitted from major developments within the past years, nowadays providing a cost efficient service for civil or commercial user but with less than tactical endurance or range achievements. This paper argues that technological advances within the past few years furthermore led to a new class of commercially/civil usable unmanned vehicles that need to be addressed as well – the Nano class (See also [14]). Due to limitations of Mini-, Micro- and Nano-class unmanned vehicles in range and endurance that differ significantly from other tactical systems, these classes are for the purpose of this paper described as “operational” vehicles that provide a local service covering a narrow geographic area.

Table 2: Unmanned Aerial Vehicle Classification Table

Class / Description	Mass (kg)	Range (km)	Flight alt. (m)	Endurance (h)
Operational***				
Nano**	<0,5 **	<2 **	150/250/300**	<1 **
Micro	<5	<10	150/250/300*	<1
Mini	<20/25/30/150*	<10	150/250/300*	<2
Tactical				
Close range (CR)	25–150	10–30	3,000	2–4
Short range (SR)	50–250	30–70	3,000	3–6
Medium range (MR)	150–500	70–200	5,000	6–10
Strategic				
Special task				

source: [5] referring to [19]

1.2 Barriers and Risk Factors

Integration of UAVs into civil airspace and their potential market success depends on a complex set of technical, economic, political, and legal factors. Unlike the early years of aviation, UAVs do not operate in empty skies and must contend with a mature civil aviation system—one filled with aircraft, controlled and monitored by complex systems, dominated by large commercial markets, saturated by interest groups, and governed by a voluminous regulatory structure [6]. In the example of a port maritime regulations include several areas in which existing regulations overlap or at least are interconnected to existing ones [13] [10]. Different sources already provided operative barrier analysis for unmanned systems as displayed in **Fehler! Verweisquelle konnte nicht gefunden werden.**. The most applicable aspects for unmanned port operations among these evaluations are highlighted and will briefly be explained.

1.2.1 Public Perception

Following the argumentation of [21] this paper agrees that the public perception dynamic presents several key issues on risk communication, or how to inform both the general public and users of the system that key risks have been considered and mitigated.

Table 3: Unmanned System Operation Barriers

Weibel and Hansmann (2005)	Dep. of Transportation (2003)	DeGarmo (2004)
Safety Requirements	Safety hazards	Safety Criticality
	Security concerns	
	Technology and reliability/maintainability barriers	Technical Complexity
Policy Process	Regulatory	Legal Complexity
	Liability issues	
	Privacy and civil right issues	
	Institutional relationships	
Public Perception	Public Perception	Socio-political Risk
Market Forces	Market and economic barriers	Economic Cost

Source: Weickhardt 2016 referring to [21] [17] [6]

[22] argued however that public perception of technological risks does not depend heavily on the actual risk,but depends largely on the perceived benefits of the technology, opinion of the

technology and other factors that are not generally termed as rational. Following the argumentation of [9] the interaction of different decision making bodies within a port and its hinterland connection will inevitably lead to situations where the overall benefit of one aspect may counteract with other single organizational or economic aspects. This factor puts a high importance to the general perception of stakeholders towards new technologies like unmanned systems.

1.2.2 Safety hazards and Security concerns

Security concerns derive from the fact that UAV platforms may serve research and public purposes, as well as terrorism or sabotage destructive ends. Remotely operated, radio controlled vehicles, especially if small and unobtrusive, can carry out nefarious surveillance missions, or even transport and deliver explosives, or biological-chemical- radiological-nuclear materials to vulnerable high value, critical infrastructure, or civilian population targets [17]. Safety hazards caused by unmanned systems are classified in ground impacts creating hazards for people on the ground when an unmanned aerial vehicle crashes down and midair collisions with a manned aircraft threatening the safety of the pilots or passengers aboard that aircraft. Both effects are critical system design drivers that have own implications for UAV operations and reliability requirement. From a port management perspective this paper follows the approach of [17] to separate safety and security issues since they fall under different legal requirements according to SOALS and ISPS requirements.

1.2.3 Technical Complexity

Improving unmanned systems reliability has been the focus of interest to overcome safety and perception barriers and provide a valuable service to the customers. According to [6]there are essentially two ways to improve reliability either by improving the integrity of components and systems and/or building in redundancy. The price of using highly reliable and certified aviation parts adds, however, to acquisition and maintenance costs. Therefore technology improvement must come at comparable or lower cost, if offered on a UAV payload and it must not overcome a single specific barrier, while exacerbating another that very likely is its technical complexity according to [17]. Recent technological developments have introduced a majority of fail-safe functions and other risk reducing factors of unmanned vehicles that should reduce general reluctance and provide a relatively safe and easy-to-use solution to commercial/civil user of unmanned vehicles.

1.2.4 Legal complexity

In line with [21] the emergence of UAS operations drives the need to generate applicable policies that, however, is rather difficult considering the wide variety of unmanned vehicles with multiple areas of usage. Additionally, the identification of the appropriate level of safety and regulation needed should rather be assessed according to the specific system and/or area of use. Basic risk identification and quantification of unmanned systems usage in the academia was shaped by contributions of [20 [21] that compare the risk associated with fatal hazards to definitions of the FAA's target level of safety in the national airspace of the US. Apart from providing a good basis for risk quantification, this model assumes a equal likelihood of encountering an aircraft in any region of the National Air Space at any time and the formulation only yields the probability of collision, assigning the same severity to the incident regardless of the collision momentum [15] that varies significantly with the different classes of unmanned systems. Also operational and small tactical systems according to Table 6 performing missions in urban regions like ports would not be expected to collide with manned aircrafts in low-height airspace of less than 150m. However, as of today only little has been implemented into actual legal frameworks forcing unmanned systems to be operated in very segregated areas and often not recognizing the reduced fatality risk of small UAV classes operated less populated areas.

1.2.5 Economic costs

Economic costs are perceived as one of the most obvious factors for the implementation and use of unmanned systems in a company's operations. If no clear economic advantages of the new technology over conventional methods can be recognized a company will hardly be willing to consider the above mentioned multitude of factors like safety, legal issues or external perception. This paper, however, argues that recent developments on the unmanned system's market have led to a decline in prices while constant technological evolvements have parallel increased operational opportunities and safety mechanisms that makes it very interesting for many companies to at least consider a possible integration of unmanned systems in (parts) of their operations.

2 BACKGROUND FOR UNMANNED SYSTEM USAGE IN PORTS

Ports are sensible infrastructures with an increased demand on security measurements that arose after the 9.11 attacks when the possibility of terrorists using modes of transportation to conduct attacks against civil infrastructures and humans went into the center of attraction. Maritime regulations include several areas in which existing regulations overlap or at least are interconnected to existing ones [13] [10]. This paper identified the following legal frameworks to directly interact with a potential use of unmanned systems in port operations and therefor providing a valuable framework: The International Convention for the Safety of Life at Sea 1974 (SOLAS), Chapter IX – International Safety Management Code 1994 (ISM), Chapter XI-2 International Ship and Port Facility Security Code 2002 (ISPS-Code), the International Convention for the Prevention of Pollution from Ships 1973/78 (MarPol),the Paris Memorandum of Understanding on Port State Control 1982 (Paris MOU) and the international Labor Organization Code of Practice on Safety and Health in Ports 2003 (ILO). Several operations exist within a port that can be conducted or assisted by the use of unmanned systems. These operations can broadly be differentiated in inspection purposes, management and other factors. A port's operation with its often multiple supply chains (rail, road, sea) takes place above the waterline wherefore UAVs find almost complete applicability in this context. ROVs, however, can provide valuable services below the surface where operations so far could only have been conducted via divers or not at all. It shall be mentioned, that the evaluated legal frameworks provide only a fraction of regulations that are applied in and around port facilities. It is likely that other sources provide additional legal content to this topic that could be addressed in future research. This paper follows the argumentation of [8] who argued that the majority of different stakeholders within a port and its hinterland connection makes it inevitable that safety and security aspects are embedded into everyday business processes and in collaboration among different stakeholders [3]. This aspect is of utmost importance to integrate new technologies like unmanned systems into ports without increasing any operation's complexity or costs that otherwise can and most likely will create reluctance of one or several stakeholders. This paper argues that port operator see themselves confronted with a high dependency on international trade flows and a considerable competition between other port operators. Following [2] the aspects of structural factors affecting long term economic performance as encapsulated in the concept of competitiveness lie in the areas of productivity, skills and innovation in an economy that for the sake of this argument can foster the implementation of unmanned systems. Furthermore, through their connection to hinterland supply chains a port's effectiveness also significantly affects regional economies (see [2]) that can positively affect the public perception aspect empathized in chapter 1.

Table 4: Unmanned System Port Operations and Legal Backgrounds

Category	Operation	UAV Operation	ROV Operation	ISPS-Code	Other
general				(A) Article 14.1	
	PFSA	Yes	Yes	(B) Article 15.3.1,2	
				(B) Article 15.14.1	
	Checking of cargo	Yes	No	(B) Article 16.33	
				(B) Article 16.36	
	Checking of Ship's stores	Yes	No	(B) Article 16.41	
				(B) Article 16.43	
	Monitoring Port Facility Security	Yes	No	(B) Article 16.49.2,3	
Inspection	Inspection of Quays	Yes	Yes	(B) Article 15.16.1,2	
	Inspection of Gear	Yes	Yes	(B) Article 15.7.2	ILO Chapter 5 Article 1.4.1.
	Inspection of facilities	Yes	No	(B) Article 15.7.6	
	Inspection of ship hulls	No	Yes	(B) Article 9.46.4	Paris MOU Annex 11 Article 11
				(B) Article 9.47.4	Paris MOU Annex 11 Article 12
				(B) Article 9.49.4,5	
Management	Traffic Control	Yes	No	(B) Article 16.20.3	
				(B) Article 16.27.6	
				(B) Article 16.27.7	
	Change Management	Yes	Yes	(A) Article 15.4.	ILO Chapter 11 Article 2.5.5.3
	Emergency guidance	Yes	Yes	(B) Article 16.20.7	ISM Part A Article1.2.3
					ILO Chapter 11 Article 2.5.4.1
	Dangerous goods Spill control	Yes	Yes		MarPol Annex I Chapter 4 Reg 15,34 Article 7
					ILO Chapter 11 Article 1.6.
other	patrol	Yes	Yes	(B) Article 16.20.4	
				(B) Article 16.27.6	
	First aid Emergency	Yes	Yes		ISM Part A Article1.4.5

Source: Weickhardt (2016)

2.1 Risk Factors of Port Related Unmanned Systems

Among the evaluated legal frameworks applicable for port operations the ILO code of Practice on Safety and Health in Ports provides a clear understanding about requirements on the implementation of innovative technologies demanding that technological or other innovations, and/or new work practices involving such innovations, introduced in ports can be done in a safe and proper manner and that safe working conditions are maintained (ILO (2005) Chapter 1 Article 1.4). As mentioned, ports operate among different supply chains and different stakeholder simultaneously in an area where efficiency, safety/security and costs are driving factors. In order to minimize risk associated with unmanned systems and mitigate those within unmanned operations (following [29 [21] the following table introduces port related factors and their impact on UAV/ROV operations and the overall planning of operation path that do not endanger any persons in or around a port facility.

Table 5: Unmanned Systems Operation- and Risk Assessment Variables

Category	Variable	UAV	ROV	Important for path planning
port structure	terminal operation	Yes	No	Yes
	external personal factor	Yes	No	Yes
	Facilities	Yes	No	Yes
	Sheltering factor	Yes	No	Yes
water	current	No	Yes	No
	depth	No	Yes	No
	visibility under water	No	Yes	No
weather	weather conditions	Yes	No	Yes
external	distance to civil areas	Yes	No	Yes
	surrounding area	Yes	Yes	Yes
operation	payload	Yes	No	No
	endurance	Yes	Yes	Yes
	emergency response operations	Yes	Yes	-

Source: Weickhardt (2016)

Given the different operative area of UAV above the surface and ROV below the waterline the underlying intensity of risk assessment factors varies considerably with the possible interference with port operations. ROV in that respect do not interfere with general port operations when a ship lies at a quay for loading/unloading purpose with deactivated propulsion and therefore do not require as much risk assessment factors as UAVs. Basic ROV operation consideration is the line of sight underwater (based on water quality, algae, fine particles etc.). Current, operative depth and endurance shall be considered for the use of a specific ROV and its specifications while the surrounding area must be considered for operative planning in order not to interfere with other waterborne movements. The majority of publicly available and affordable ROV use cable between the ROV and its controlling unit. This aspect is seen as a considerable fail-safe mode because it provides the operator with an opportunity to simply drag back the ROV in case of system failure. Using UAV in port operations requires a careful examination of different risk factors being integrated in the operative path planning of the UAV. Basic consideration of the operation of a UAV is the current weather and surrounding areas that might provide risk or might be negatively affected by UAVs (for example airports or military facilities in near location to a port) also including civil areas in case of events for example. Within the port several factors must be considered including existing facilities both fix (buildings) and moving (loading gear, cranes). Those structures provide a physical obstacle for UAV operations additional to port operations that the UAV must not endanger or otherwise interfere with. This paper argues that regularly UAV operations in ports will create a certain amount of awareness of port personnel towards unmanned systems reducing the potential distraction of unmanned operations. This might, however, not be the case for external personal entering the port facility (e.g. truck driver, external authorities, visitors etc.) which requires additional consideration. Using UAVs the operative payload required will also affect the path planning for increasing payloads lead to decreasing flight endurance and therefore minimizing the operative area. One positive aspect of integrating unmanned systems into ports is the opportunity of having the opportunity to provide surveillance in cases of accidents or fires for co-ordination of forces and authorities that, however, cannot be considered for path planning due to their unpredictable nature.

3 CONCLUSION

This paper contributed to the existing literature by providing a first framework for their application in port facilities under consideration of operational aspects as well as underlying legal frameworks. A general introduction of unmanned systems for the use in civil/commercial areas was made and existing operation barriers of general UAV operations have been introduced and discussed based on existing literature and considering a shore based maritime application. The majority of possible operations are based on safety and security issues were this paper sees the first important aspect of successful integration of unmanned systems into port facilities. Findings of this paper can be applied to other sensible infrastructure as well. Given that fact that (inter)national legal frameworks for the use of unmanned systems have not been introduced at the moment, the aspect of legal complexity as an operative barrier following [6] shall be subject to future research. This paper argues that the existing scope of unmanned system research (based on scientific and military applications) may not fit to the operation in civil/commercial areas were systems will most likely not be classified over “medium range” in order to provide a certain cost/benefit ratio. A proposal for a new classification of systems that are below tactical usability as “operational class” has therefore been introduced and should be analyzed in future evaluations.

REFERENCES

[1] Allotta, B.; Brandani, L. et al. (2015). Development of Nemo ROV For The Inspection Of The Costa Concordia Wreck, Proceedings Of The Institution Of Mechanical Engineers Part M Journal Of Engineering For The Maritime Environment

[2] BARNES, P.; Oloruntoba, R. 2005, assurance of security in maritime supply chains: conceptual issues of vulnerability and crisis management. Journal of International Management, 11(4). 519-540.

[3] BICHOU, K. 2005, maritime security: framework, methods and applications, report to UNCTAD, Geneva,

[4] CANIS, B. (2015). Unmanned Aircraft Systems (UAS). Commercial Outlook for a New Industry: Congressional Research Service.

[5] DALAMAGKIDIS, K. (2015). Classification of UAV, In: Valavanis and Vachtsevanos (2015) Handbook of Unmanned Aerial Vehicles, 1st edition, p.83-91

[6] DEGARMO, M.-T. (2004). Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace.

[7] EUROPEAN COMMISSION (EU 1) (2007). Study Analyzing the Current Activities in the Field of UAV.

[8] FRITTELLI, J.F. 2003, port and maritime security: background and issues for Congress, Congressional Research Service, (December 5) Report RL 31733.

[9] HECKER, J.Z. (2002). Port Security: Nation Faces Formidable Challenges In Making New Initiatives Successful, U.S. General Accounting Office August 1

[10] HELMICK, J.S. 2008, port and maritime security: a research perspective, in Journal of Transportation Security, 1(1). 15-28.

[11] OLIVER, B. (2009). Could UAVs improve New Zealands Maritime Security?, Massey University Centre for Defense Studies

[12] Osumi, H. (2014). Application of Robot Technologies to the Disaster Sites, The Japan Society of Mechanical Engineers, Report on the Great East Japan Earthquake Disaster

[13] PAPA, P. 2012, US and EU strategies for maritime transport security: A comparative perspective. Transport Policy, 28, 75-85

[14] RPAS YEARBOOK (2015). International Remotely Piloted Systems Information Source http://uvs-info.com/index.php/yearbooks/yearbook-2015/book/23?page=1 [accessed Mai 2016]

[15] SPRAGUE, K.-L. (2004). Civilian Applications and Policy Implications of Commercial Unmanned Aerial Vehicles. Master of Science in Technology and Policy. Massachusetts Institute of Technology.

[16] Teal Group Press releases (2007-2015) http://tealgroup.com/index.php/about-teal-group-corporation/press-releases [accessed Mai 2016]

[17] U.S. DEPARTMENT OF TRANSPORTATION (2003). A Roadmap For Deploying Unmanned Aerial Vehicles (UAVs) In Transportation.

[18] VALAVANIS, K.-P.; Vachtsevanos, G.J. (2015). Handbook of Unmanned Aerial Vehicles, 1st edition, Springer

[19] VAN BLYENBURGH, P. (2006). UAV systems: global review. Presented at the Avionics'06 conference, Amsterdam,

[20] WEIBEL, R.-E. (2002). Safety Considerations for Operation of Different Classes of Unmanned Aerial Vehicles in the National Airspace System, Massachusetts Institute Of Technology

[21] WEIBEL, R.-E.; Hansmann, J. (2005). An Integrated Approach to Evaluating Risk Mitigation Measures for UAV Operational Concepts in the NAS, Conference proceedings at Aerospace Conference. 26 - 29 September 2005. Arlington, VA.

[22] Slovic, P., et. al,(2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality, Risk Analysis, Vol. 24, No. 2, p. 311-322

EXPLORATION OF CONSEQUENCES OF POTENTIAL MALFUNCTIONS OF GLOBAL NAVIGATION SATELLITE SYSTEMS

Iztok Prezelj[1], Jelena Juvan[2], Erik Kopač[3] and Gerwin van der Meulen[4]

[1] iztok.prezelj@fdv.uni-lj.si

Chair of Defence Studies, Faculty of Social Sciences, University of Ljubljana, Kardeljeva ploscad 5, 1000 Ljubljana (Slovenia)

[2] jelena.juvan@fdv.uni-lj.si

Chair of Defence Studies, Faculty of Social Sciences, University of Ljubljana, Kardeljeva ploscad 5, 1000 Ljubljana (Slovenia)

[3]erik.kopac©fdv.uni-lj.si

Chair of Defence Studies, Faculty of Social Sciences, University of Ljubljana, Kardeljeva ploscad 5, 1000 Ljubljana (Slovenia)

[4]G.vanderMeulen@decisio.nl

Decisio, Valkenburgerstraat 212, 1011 ND Amsterdam

Abstract

European countries and numerous services have become increasingly dependent on the navigation support provided by the existing Global Navigation Satellite Systems – GNSS (predominantly GPS and supplementary systems such as EGNOS). The European navigation system GALILEO will likely to become fully operational in the near future. GNSS can be understood as a critical infrastructure in Europe because of our high and strategic dependence on its uninterrupted operation. Malfunction of GNSS can cause major direct and indirect consequences. There is a lack of clarity about the proportion and seriousness of such consequences for our societies. This paper presents results from research on the consequences of potential malfunctions of GNSS in Europe, done as part of EU-funded PROGRES research project[1]. Investigation in this direction will contribute to improvement of our preparedness and crisis management procedures in the unpredictable future

Keywords: GNSS, malfunction, crisis

1 INTRODUCTION

Global Navigation Satellite System (GNSS) is a term used to describe collectively all the planned and currently available satellite based navigation systems.. The main goal of GNSS technology is to provide users all over the globe the positioning, navigation and timing service (PNT). In brief, this is achieved through the line of sight view with minimum 4 GNSS satellites– through the means of the triangulation method.

[1] This paper shows some results from the project PROGRESS. PROGRESS has received funding from EU FP7 under grant agreement Contract No. 607679. The project started on 1st May 2014 and is due to be completed in 2017. The information appearing in this document has been prepared in good faith and represents the opinions of the authors. The authors are solely responsible for this publication and it does not represent the opinion of the European Commission. Neither the authors nor the European Commission are responsible or any use that might be made of data including opinions appearing herein.

In the framework of the project PROGRESS, we investigated the following possible effects of a potential complete malfunction of GNSS services in Europe (a low probability – high consequence scenario): direct societal consequences, such as casualties on the territory of EU, direct economic damage, and public effects (the number of affected end users, impact on public confidence/trust in the service providers, impact on public services, and impact on social order), and cross-sectoral consequences for other GNSS-dependent sectors (e.g. transport, electricity, ICT, etc.). These effects need to be explored in order to understand the pervasiveness of this technology in Europe and emerging strategic dependence of our societies. This paper aims to direct scientific discussions in the area of GNSS criticality for our societies.

2 APPLICATIONS OF GNSS

There are four different types of GNSS programmes. The first GNSS programmes were launched in the seventies: the GPS system from the US and the GLONASS system from Russia. Both systems were born in a Cold War context. Their main mission was to answer to military and strategic needs. Galileo is the European GNSS programme, and is currently managed by the European Commision, the European GNSS Agency (GSA) and the European Space Agency (ESA). The primary objectives of Galileo are to provide an alternative upon which European nations can rely, independent from systems like the Russian GLONASS and US GPS systems and to increase the availability through interoperability with these systems. In addition to these, the fourth global system due to be completed by 2020 is the Chinese Navigation Satellite System - Beidou. Other regional initiatives exist in Japan (QZSS system) and India (IRNSS system) (Jeffrey (2010).

The first applications of GNSS were developed for military use, surveying and mapping. Nowadays, GNSS applications are used by the transportation, land management, agriculture sectors as well as the energy and mining industry. Its ability to deliver accurate navigation data, makes GNSS trustworthy, especially for the aviation industry. GNSS can provide vertical guidance for safer landing, route optimisation, enabling fuel savings and CO2 emissions reductions, as well as cost reduction through the phasing out of current ground-based equipment. Also GNSS enabled opening of small airports in remote regions, increasing the prospects for regional integration and intercontinental air connection (Capacity4dev, 2012).

GNSS systems are composed by three segments:

- The Space Segment: ensure the range calculation between the user and the satellite and is used to broadcast the signal with key information (such as the position of the satellite, the time and several corrections).
- The Ground Segment: the Ground Control Center and the Ground Mission Segment is globally in charge of: monitoring the satellite constellation, estimating the satellites position and clock drift, and uploading the information to the satellite before it is broadcasted to the users.
- The User Segment: this segment uses the signal in space to compute the location, speed and time with two main categories of services, the Open Service (accessible free-of-charge to civil users) and the Control Access Service (for military or commercial purposes). Additionally, it provides users a new search and rescue (SAR) function part of the existing Cospas-Sarsat Programme giving users a feedback response and sending emergency beacons distress signals to the rescue coordination team.

The range of possible uses of GNSS is enormous, spanning many domains, both public and private. Numerous potential applications have already been identified, based on the quality and reliability of GNSS signals, but the list is certain to grow, limited only by the imaginations of innovative entrepreneurs and service providers. In this segment we present a number of services according to GSA (2014):

- Location-based services: GNSS enables the integration of accurate positioning signal receivers within mobile telephones, personal digital assistants (PDAs), mp3 players, portable computers, cameras and video devices.
- Emergency, security and humanitarian services: devices enable security-related applications, permitting the location of stolen property, for example, or lost pets or individuals. GNSS signals facilitate civil protection operations in harsh environments, speed up rescue operations for people in distress, and provide tools for coastguards and border control authorities.
- Science, environment, weather: GNSS services are used to carry out scientific research in meteorology and geology, in the field of geodesy, to track pollutants, dangerous goods and icebergs, to map the oceans, study tides, currents and sea levels. GNSS contribute through accurate timing/positioning. Galileo will allow improved monitoring of the atmosphere, of water vapour for weather forecasting and climate studies, and the ionosphere for radio communications, space science and earthquake prediction. It will also help to better understand the movements of populations of wild animals.
- Transport: satellite navigation can increase traffic safety and efficiency by improving the way we use vehicles. Highly accurate and reliable Galileo signals will serve fleet management, enabling the delivery of detailed maps or voice notifications to locate specific shipments and containers in road transport. It will deliver similar benefits in aviation, maritime and rail transport, and even for pedestrian traffic.
- Agriculture: by integrating GNSS signals with other technologies, the agriculture community can benefit from improved monitoring of the distribution and dilution of chemicals, improved parcel yield thanks to customised treatment and more efficient property management.
- Fisheries: the fishing industry benefits from more effective information exchange between vessels and stations and improved navigation aids for fishermen.
- Civil Engineering: combined with digital mapping, GNSS offers a powerful tool for decreasing cost and increasing productivity while maintaining the highest construction standards, from the planning of structures to the maintenance and surveillance of existing infrastructure.

3 CRITICAL INFRASTRUCTURE IN EUROPE AND GNSS

We firmly believe that GNSS has become or is becoming a critical infrastructure in European societies, perhaps for the entire EU as well. According to CIIP (2014): “The term “critical infrastructure” refers to assets of physical and computer-based systems that are essential to the minimum operations of an economy and its government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both government and private.”

Critical infrastructures have been defined as “fundamental capacities, technical systems and organizations that provide those capacities” (Schulman and Roe, 2006). These complex systems provide a permanent flow of services that are essential for the well-being and security of the population (Michel-Kerjan, 2003: 134). Society has become increasingly dependent on these infrastructures (Knight and Sullivan, 2000, Ellison et al., 1999), so that normal life can not exist anymore without their support (Koubatis and Schonberger, 2005). The complexity of critical infrastructures is high also due to increasing inter-connectedness of infrastructural sectors, a high share of private ownership, increasing dependency from ICT systems, increasing international role of infrastructures, etc. (Le Grand, Springinsfeld, and Riguidel, 2003).

EU defined the critical infrastructure as an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (EU, 2008).

Space infrastructure fits the above definition of critical infrastructure. Some of the consequences of malfunctioning can be easily predicted while some others can be unpredictable. Society and some commercial actors frequently underestimate the risk of significant disruption of satellite services. It can be noted that the threats, vulnerabilities and risks are increasing with the increase of societal reliance upon the satellite services and cross-sectoral interdependencies.

4 MALFUNCTIONING OF GNSS SYSTEMS

There has been little research on the scenarios of a collapse and failure of satellite infrastructure and related effects on other infrastructure and sectors. A simulation of propagation of a GPS service failure to the power grid, telecommunications and railway showed their instant or gradual reduction of operationality (Lupo, 2014).

Critical infrastructures have been exposed to a great number of threats' risks in the past. Le Grand et al. (2003) classified such events in three groups:

- Failures created due to internal system deficiencies;
- Accidents mainly due to external reasons, and
- Intentional attacks mostly by external actors.

Unintentional threats include natural, accidental and malicious threats that can have a physical and cyber character (Dunn, 2004). These threats are categorised as follows:

- Ground-based threats: natural terrestrial threats, such as earthquakes, floods, thunderstorms, lightning, dust storms, heavy snows, tropical storms, tornadoes, corrosive sea spray, salt air, terrestrial interference etc., and power outages;
- Space-based threats from space objects (including debris) and space environment (solar, cosmic radiation, temperature variations), and

Intentional threats include deliberate attacks, a natural disaster caused by human action, negligence, accidents, computer hacking, criminal activities or malicious behaviour.

Critical infrastructures have become a relatively easy target for attacks due to its prevalent wide geographic dispersion and, as Lewis (2006) noted, due to its scope and attractive low effort-high return ratio.

4 SOME CONCLUSIONS REACHED BY THE PROGRESS RESEARCHERS

The results of our research (gathered based on the workshop with GNSS stakeholders) show that complete interruption of GNSS can potentially cause human casualties early after interruption. It is also likely that the economic damage of a complete GNSS malfunction will be – instantly – very high. GNSS interruption has the potential to cause very high indirect economic effects in other GNSS depending sectors (e.g. telecommunications, electricity, transport…). Interruption of the GNSS signal will likely have various public effects:

- The majority of the end users could likely be affected immediately after such an interruption.
- Public confidence/trust in the service providers could likely not be highly affected in one hour after interruption due to the high uncertainty about what is going on. Later on, this effect will supposedly increase to a very high level and will probably be driven by media reports.
- The functionality of public services, such as state, regional and local administrative services, and emergency services (health, police and fire protection services), could be increasingly affected through time.
- Social order will not be impacted directly. Public protests and demonstrations are not likely to take place against the providers of the GNSS services (which are rather abstract for the population), but could most likely be against the indirectly affected GNSS dependent sectors which will not be able to provide their usual services.

Malfunctioning of GNSS will likely affect several other GNSS dependent sectors. Some of the proportions of these effects are imaginable and will be described in our presentation, but some are beyond our imagination (due to the extreme complexity of systems, interconnectedness, etc.).

The lesson of our work is that we need to invest more in our societies' resilience and preparedness for situations when the GNSS could fail to perform its expected service.

REFERENCES

[1] Jeffrey, C. (2010). An introduction to GNSS.

[2] Capacity4dev (2012). European Satellite Navigation Systems Could Foster Development in Africa. Available at: http://capacity4dev.ec.europa.eu/article/european-satellite-navigation-systems-could-foster-development-africa. Retrieved on June 1st 2016.

[3] GSA (2014), User Applications. Available at: http://www.gsc-europa.eu/gnss-markets/user-applications. Retrieved on July 9th 2014

[4] CIIP (2014), available at: http://cybersecuritykeeper.com/cip.html. Retrieved on June 1st 2016.

[5] Schulman, P. & Roe, E. (2006). Future Challenges for Crisis Management in Europe. Paper presented at the conference Protecting Critical Infrastructures: Vulnerable Systems, Modern Crises, and Institutional Design. Conference on Future Challenges for Crisis Management in Europe, 4-5 May, Stockholm.

[6] Michel-Kerjan, E. (2003). New Challenges in Critical Infrastructures: A US Perspective. Journal of Contingencies and Crisis Management 11(3).

[7] Knight, John & Sullivan, Kevin (2000). On the Definition of Survivability. Department of Computer Science, University of Virginia.

[8] Ellison, R., Fischer, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A. & Mead, N.R. (1999). Survivability: Protecting Your Critical Systems. Pittsburgh: CERT Coordination Center, Carnegie Mellon University. Retrieved on: February 10, 2006, from www.cert.org/archive/html/protect-critical-systems.html

[9] Koubatis, A. and J.Y. Schonberger (2005). Risk management of complex critical systems. International Journal of Critical Infrastructures 1(2/3): 195 - 215.

[10] Le Grand, G., Springinsfeld, F. & Riguidel, M. (2003). Policy Based Management for Critical Infrastructure Protection. ACIP Project funded by the European Commission, Paris: GET/Télécom Paris. Retrieved on: February 10, 2006, from www.tsi.enst.fr/publications/enst/inproceedings-2003-3517.pdf

[11] EU (2008). Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. Official Journal of the EU, December 23, Brussels. Retrieved on: January 2, 2009, from http://eur-lex.europa.eu.

[12] Lupo, Roberto (2014). *Space Awareness for Critical Infrastructure*. Final SPARC Workshop, 17.1. Telespazio, Rome.

[13] Le Grand, G., Springinsfeld, F. & Riguidel, M. (2003). Policy Based Management for Critical Infrastructure Protection. ACIP Project funded by the European Commission, Paris: GET/Télécom Paris. Retrieved on: February 10, 2006, from www.tsi.enst.fr/publications/enst/inproceedings-2003-3517.pdf

[14] Dunn, M. (2004). Analysis of Methods and Models for CII Assessment. In: M. Dunn & I. Wiegert (eds.) International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries. Zurich: ETH – Swiss Federal Institute of Technology. Retrieved on April 1, 2007 from: www.isn.ethz.ch.

[15] Lewis, T. (2006). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley Interscience, New Jersey.

CHALLENGES OF MANAGING IT-TRUST

Dr. Alexander Löw[1]

[1] *a.loew@dwh.info*
Data-Warehouse GmbH, Beethovenstr. 33-35, 85521 Ottobrunn (Germany)

Abstract

Certificates are issued by many places. For a certificate is considered as valid, anyone have to trust the Certificate issuing authority (CA). However, many of these companies and organizations are unknown to most users. The user delegated his confidence to the manufacturer of the software and it is even difficult to decide about the certificate, e.g how safe are the procedures used in its issuing and publication and if the certificate is at all suitable or intended for which applications. In complex network environments the assessment of certificate management becomes a real problem. This document tries to show best practices how to detect, identify, assess, exchange, automate X.509 certificates or keys and the regarding impacts to IT-trust, business continuity.

Keywords: IT-Trust, X.509 Management, Certificate Assessment, Certificate exchange

1 BACKGROUND TO X.509 AND IT-TRUST

Certificates are issued by many places. For a certificate is considered as valid, you have to trust the Certificate issuing authority (CA). In Web browsers, many certification authorities are classified as trustworthy by default for this reason. However, many of these companies and organizations are unknown to most users. The user delegated his confidence to the manufacturer of the software.

A second problem is that it is even difficult to decide about the certificate ,e.g how safe are the procedures used in its issuing and publication and if the certificate is at all suitable or intended for which applications. The user should read for the appropriate documentation of the CA, the certificate policy (CP) and the certification practice statement (CPS), whose contents are specified by RFC 3647 General. Qualified certificates can be used for high security requirements, whose Issuer are subject to legally prescribed safety standards and government supervision.

1.1 Misuse of trust relations

However, governmental organizations have to request certificates for their own purposes at the issuing offices. This would officialize any surveillance software and enable the silent installation by the countries officials (e.g North Korea against Sony®, China against US-military aircraft industry).
These problems were evident, for example, by an incident where VeriSign ® issued certificates to persons which claims incorrectly to work for the company Microsoft ®[1]. These certificates, the scammers had now apparently trusted evidence, that they were part of the company Microsoft. It would have been possible for example to sign program code, so that it would be installed by Windows operating systems without warning in the name of the Microsoft ®. Although these certificates have been revoked immediately after the error was noticed, but they were still a security risk, because the certificates contained no indication, where a possible withdrawal could be retrieved. Also Foxconn's® certificate was stolen and the base for the successful Kaspersky® Hack[2]. This case is a sign that you can't rely blind on

[1] Flame Virus

[2] Kaspersky Hack

the trustworthiness of certificates and the care of CA's provided by OS and other Software. In addition, press releases about misuse proof that also leading software manufacturer and experts are not yet been fully aware to the subject. The revocation of a certificate is only effective if current revocation information is available for examination. For this purpose, you can retrieve certificate revocation lists (CRL) and online checks (for example, OCSP). Every Browser, Operating System and Application uses a vendor dependent system for these Checks. No unified method is provided currently. Googles new approach about Certificate transparency (CT) is one of the first methods of the leading companies to manage the browser specific area of SSL/TLS.

1.2 Problem Description

Especially in complex network environments the issue about certificate management becomes a real problem. How to detect, identify, assess, exchange, automate X.509 certificates or keys. Certificates are stored in many Silos and Areas and contain no central managing area in none OS. Typical containers are (browser container in Firefox, Chrome, etc.), Registry, crypto-DLL’s and all code-signed files. Additional proprietary containers for SSL/SSH connections, encryption and other security functions raise the complexity of findings. All scanners and checking mechanisms (like CT) specialize to the SSL/SHH keys and certificates, so the APT prevention tools take care about this area. As SSH/SSL is less than 1% of the certificates inside IT-devices it is looking through a pinhole to discover the world. As critical infrastructures, high security areas and devices, IOT rely on the validity of the certificate infrastructure correctness this trusts needs to be monitored. Any disturbing of these trusted network could harm the whole system.

In addition to this e.g. military security requirements enforces a valid certificate management, but the diversification of products, vendors and IT-Systems generated several silos of certificate Management environments.

This results in a multi-trust-multi-trustees environment which could not be handled with current technologies.

2 SOLUTION APPROACH

To get an overview of the internal structure, there are two main approaches:

2.1 The user allows only trusted software to install and get an overview of the certificates by the manufacturer and vendors.

This approach would imply a close and strong connection of customer and vendors. As computer environments are diversified and complex no vendor is able to provide all the informations. We analysed Windows 10 with Microsoft Office infrastructure and had many findings in which the result will be that the vendors by themselves are not able to supervise their own products. As the main vendors have no supervision the problem complexity raises with the usage of different products from different vendors as these are merged into.

2.2 The user verifies the certificate landscape and defines its trust landscape itself.

This approach takes care about the current situation inside the customers environment, but the impacts and the possible changes in the state is more complex as there is no service from the vendor available to solve the findings. Only a third party service with a support in this environments or setting up a research team could improve the situations. The advantage of this approach is based on the independence from the customer to choose any product and environment which fits to the needed trust environment. Both approaches require a knowledge of the complete trust landscape.

2.2.1 Manual search and definition

Searching manually for Certificates might be a strategy in small environments. But for midsize or large enterprises or organisations it is nearly impossible to process this because of the vast number of devices, systems and software that would need to be searched through. Additionally, it is not transparent, where Certificates and Keys are located and the chances are high that a big part of the Certificates will not be found.
Estimated effords for a manual search and export is about 5 hours per device if most tasks could be supported by scripts. The collection and harmonisation into one database takes about 1 hour. Typical results are 600-700 certificates per device and most of the SSH/SSL keys are found.

2.2.2 Automated search and definition

Automated search is only available with self made toolsets and software. Only exception is currently Cert'n Key Scanner which uses several search engines to identify certificates due to the individual need. The Scanning engine could be fully customized to the areas of searching and the search depth. This automated search of Cert'n Key leads into up to 160.000 Certificates for one device.

3 EXISTING APPROACHES FOR MANAGEMENT OF TRUST ENVIRONMENTS

Most products available are silo oriented like PKI-Systems, SSH/SSL Detection and Managing Tools and so on.

The only holistic product for a silo independent trust management is provided by Data-Warehouse GmbH and is called Cert'n Key. The philosophy of gaining the overview of the complete trust management environment and the regarding keys and certificates is the starting point. With this all following processes could be implemented like, elimination of everlasting, weak and retiring certificates, elimination of self signed certificates outside of central management, strengthen of encryption, detection of unwanted trust anchors, deletion of unwanted trust relation, control and management of new trustpoints (like Trojans or other unwanted software), data exchange with siem and apt protection tools to identify unwanted network traffic.

Cert'n Key approach enables management of devices on your local network (or remote), to manually or automatically (serial or parallel) investigate and manage Certificates and Keys and generate a central repository. This repository provides a knowledge-supported assessment of certificates and the review of the chain of trust, removing unwanted trust relationships (manual (delete), or service-based), the identification of risks (manual (analysis and security) or service-based) and enforcement of corporate policies for the automated exchange of certificates. To manage complex networks automated ZoneServers can be used to support the collection and automated distribution of policies and results in extension to your end device (Remote). Alternatively, the information can be collected with automated software distribution processes from the devices. Through the encrypted local storage of the results in the Cert'n Key scan DB any business processes regarding the operation and software distribution can be supported. Should a company need any different process, adaptions can be made appropriate within the Cert'n Key process engine (driven by EBUS-J) definitions, so that it can be optimally integrated into the enterprise process landscape.

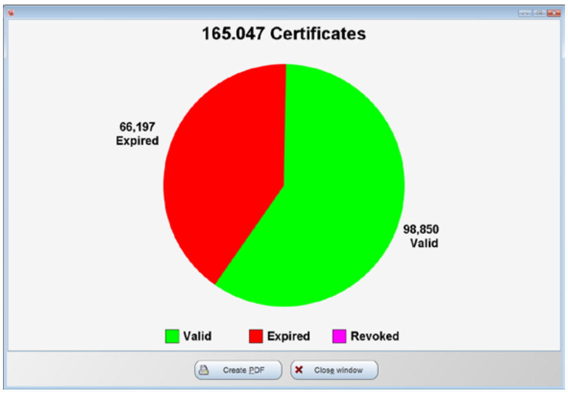
4 OUTLOOK

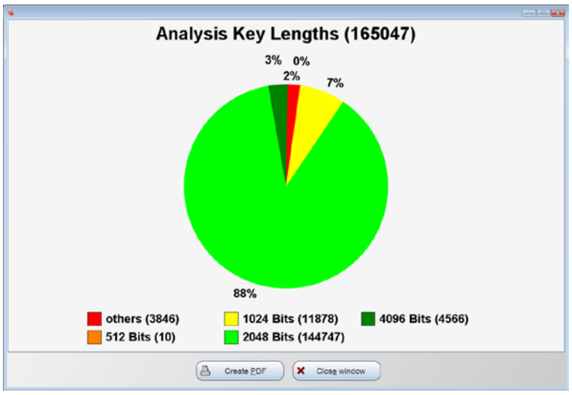
Next generation of trust management could lead into trusted code execution platforms in which the existing certificate and branch informations lead into a supervised code usage with a secure execution without attack possibilities. Current research activities are performed together with Fraunhofer Institute in Bonn.

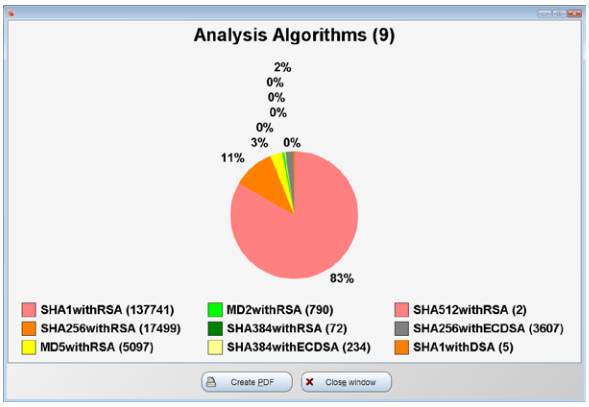
5 ENUMERATION

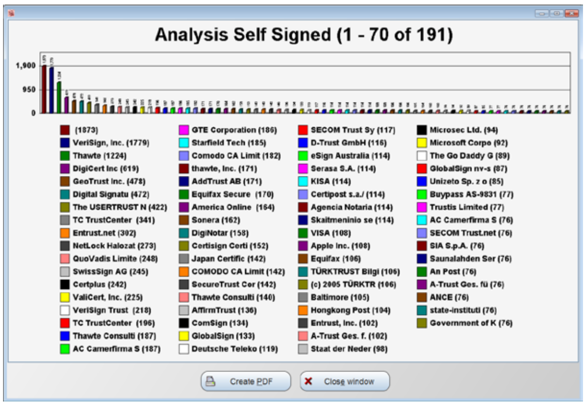
5.1 Windows PC

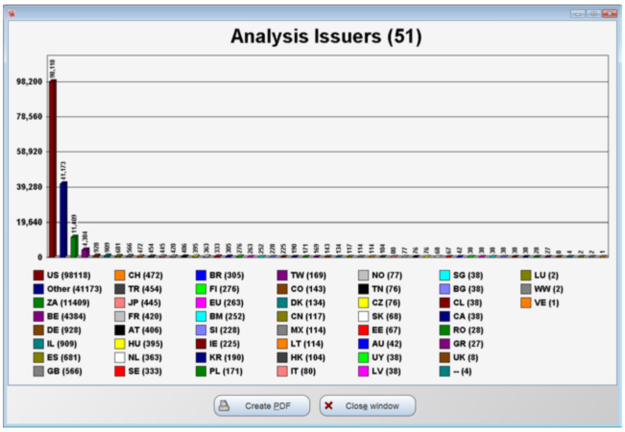
Cert'n key detects up to 165.047 certificates per Windows 7 PC, of these are 66.197 invalid. The Analysis give some overview about a Windows 7 X.509 Landscape:

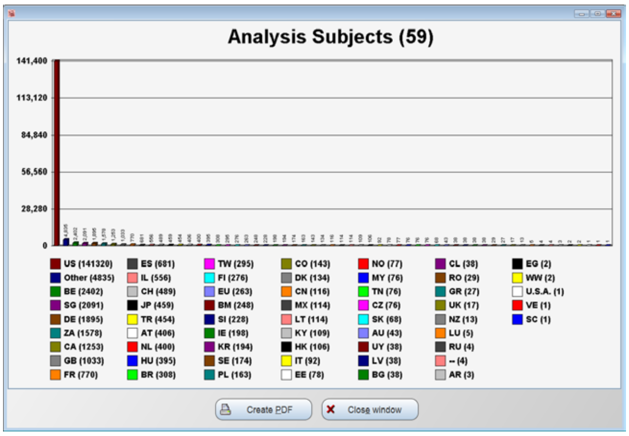


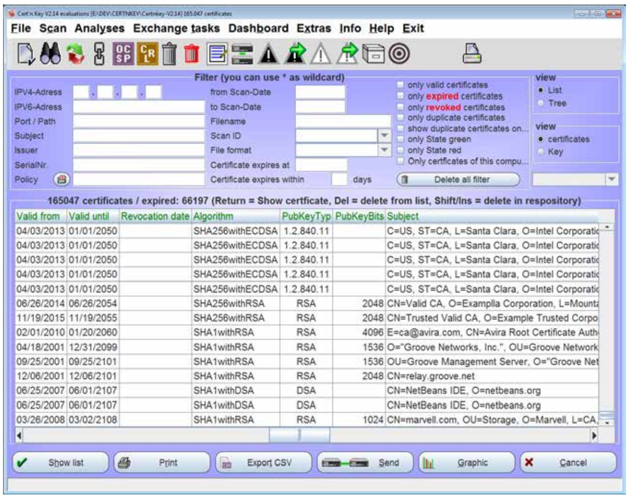






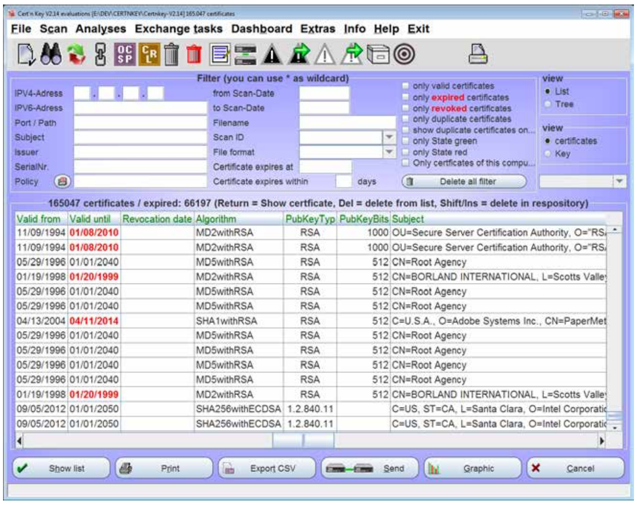





Cert'n Key V2.14 evaluations [E:\DEV\CERTNKEY\Certnkey-V2.14] 165.047 certificates
File Scan Analyses Exchange tasks Dashboard Extras Info Help Exit
Filter (you can use * as wildcard)
IPV4-Adress
IPV6-Adress
Port / Path
Subject
Issuer
SerialNr.
Policy
from Scan-Date
to Scan-Date
Filename
Scan ID
File format
Certificate expires at
Certificate expires within
days
□ only valid certificates
□ only expired certificates
□ only revoked certificates
□ only duplicate certificates
□ show duplicate certificates on...
□ only State green
□ only State red
□ Only certficates of this compu...
Delete all filter
view
● List
○ Tree
view
● certificates
○ Key
Show list
Print
Export CSV
Send
Graphic
Cancel

165047 certificates / expired: 66197 (Return = Show certficate, Del = delete from list, Shift/Ins = delete in respository)

Valid from	Valid until	Revocation date	Algorithm	PubKeyTyp	PubKeyBits	Subject
04/03/2013	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic
04/03/2013	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic
04/03/2013	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic
04/03/2013	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic
04/03/2013	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic
06/26/2014	06/26/2054		SHA256withRSA	RSA	2048	CN=Valid CA, O=Exampla Corporation, L=Mounta
11/19/2015	11/19/2055		SHA256withRSA	RSA	2048	CN=Trusted Valid CA, O=Example Trusted Corpo
02/01/2010	01/20/2060		SHA1withRSA	RSA	4096	E=ca@avira.com, CN=Avira Root Certificate Auth
04/18/2001	12/31/2099		SHA1withRSA	RSA	1536	O="Groove Networks, Inc.", OU=Groove Network
09/25/2001	09/25/2101		SHA1withRSA	RSA	1536	OU=Groove Management Server, O="Groove Net
12/06/2001	12/06/2101		SHA1withRSA	RSA	2048	CN=relay.groove.net
06/25/2007	06/01/2107		SHA1withDSA	DSA		CN=NetBeans IDE, O=netbeans.org
06/25/2007	06/01/2107		SHA1withDSA	DSA		CN=NetBeans IDE, O=netbeans.org
03/26/2008	03/02/2108		SHA1withRSA	RSA	1024	CN=marvell.com, OU=Storage, O=Marvell, L=CA,


Cert'n Key V2.14 evaluations [E:\DEV\CERTNKEY\Certnkey-V2.14] 165.047 certificates
File Scan Analyses Exchange tasks Dashboard Extras Info Help Exit
Filter (you can use * as wildcard)
IPV4-Adress
IPV6-Adress
Port / Path
Subject
Issuer
SerialNr.
Policy
from Scan-Date
to Scan-Date
Filename
Scan ID
File format
Certificate expires at
Certificate expires within
days
□ only valid certificates
□ only expired certificates
□ only revoked certificates
□ only duplicate certificates
□ show duplicate certificates on...
□ only State green
□ only State red
□ Only certficates of this compu...
Delete all filter
view
● List
○ Tree
view
● certificates
○ Key
Show list
Print
Export CSV
Send
Graphic
Cancel

165047 certificates / expired: 66197 (Return = Show certficate, Del = delete from list, Shift/Ins = delete in respository)

Valid from	Valid until	Revocation date	Algorithm	PubKeyTyp	PubKeyBits	Subject
11/09/1994	01/08/2010		MD2withRSA	RSA	1000	OU=Secure Server Certification Authority, O="RS
11/09/1994	01/08/2010		MD2withRSA	RSA	1000	OU=Secure Server Certification Authority, O="RS
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
01/19/1998	01/20/1999		MD2withRSA	RSA	512	CN=BORLAND INTERNATIONAL, L=Scotts Valley
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
04/13/2004	04/11/2014		SHA1withRSA	RSA	512	C=U.S.A., O=Adobe Systems Inc., CN=PaperMet
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
05/29/1996	01/01/2040		MD5withRSA	RSA	512	CN=Root Agency
01/19/1998	01/20/1999		MD2withRSA	RSA	512	CN=BORLAND INTERNATIONAL, L=Scotts Valley
09/05/2012	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic
09/05/2012	01/01/2050		SHA256withECDSA	1.2.840.11		C=US, ST=CA, L=Santa Clara, O=Intel Corporatic

5.2 Mac OS PC

Nearly same results but less certificates. Mac OS will provide up to 39.000 certificates and about 25% invalid.

5.3 Linux PC

Linux contains very diversified Trust structure depending on distribution and installed systems.

REFERENCES

[1] Cert'n Key Trust Management Platform – Data-Warehouse GmbH – www.certnkey.com

[2] ITU-T Recommendation X.509 (1997): Information technology – Open Systems Interconnection – The Directory: Authentication framework

[3] ITU-T Recommendation X.509 (2012): Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

[4] RFC 2818: "HTTP over TLS", Mai 2000.

[5] RFC 3729: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.

[6] RFC 4055: "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Juni 2005.

[7] RFC 4491: "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST 34.11-94 Algorithms with the Internet X.509 Public Key Infrastruture Certificate and CRL Profile", Mai 2006.

[8] RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Mai 2008.

[9] RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008.

[10] RFC 5750: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", Januar 2010.

[11] RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Message Specification", Januar 2010.

[12] RFC 6698: "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, August 2012.

[13] RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)", Oktober 2014.

[14] RFC 7469: "Public Key Pinning Extension for HTTP", April 2015.

[15] Draft: Using Secure DNS to Associate Certificates with Domain Names For S/MIME, August 2015, abrufbar unter https://tools.ietf.org/html/draft-ietf-dane-smime-09

[16] Technische Richtlinie TR-02102-1: Kryptographische Verfahren:

[17] Technische Richtlinie TR-03109: Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb.

[18] Technische Richtlinie TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme.

[19] Technische Richtlinie TR-03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 - Kommunikationsverfahren in Anwendungen

[20] C. Brubaker, S. Jana, B. Ray, S. Khurshid, V. Shmatikov: "Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations", Mai 2014, abrufbar unter **https://www.cs.utexas.edu/~shmat/shmat_oak14.pdf**

[21] A. Delignat-Lavaud, M. Abadi, A. Birell, I. Mironov, T. Wobber, Y. Xie: "Web PKI: Closing the Gap between Guidelines and Practices, Februar 2014.

[22] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, V.Shmatikov: "The most dangerous code in the world: Validating SSL certificates in non-browser software", in *Proceedings of the 2012 ACM Conference on Computer and Communication Security*.

[23] M. Malinspike: "Null Prefix Attacks Against SSL/TLS Certificates", September 2007, abrufbar unter http://www.toughtcrime.org/papers/null-prefix-attacks.pdf

[24] M. Malinspike: "Defeating OCSP With The Character '3' ", September 2007, abrufbar unter http://www.toughtcrime.org/papers/ocsp-attack.pdf

[25] Unterlage für Ausschreibung und Bewertung von IT-Leistungen, Version 2.0 vom 15.06.2010, Beschaffungsamt des BMI.

INTEGRATION MODEL OF SAFETY AND SECURITY AS A PART OF INTEGRATED SAFETY

Juraj Sinay[1] and Hana Pacaiova[2]

[1]*juraj.sinay@tuke.sk*
Technical University of Kosice, Mechanical Engineering Faculty, Safety and Production Quality Department, Letna 9, 042 00 Kosice (Slovak Republic)

[2] *hana.pacaiova@tuke.sk*
Technical University of Kosice, Mechanical Engineering Faculty, Safety and Production Quality Department, Letna 9, 042 00 Kosice (Slovak Republic)

Abstract

Integrated approach to the risk management in the man-machine-environment system is oriented towards all components of this system in the form of a generic principle application, i.e. there are defined conditions for the risk management of the individual system parts so that the mutual interrelations of these parts could be taken into consideration with regard to application of the Generic Risk Assessment Model (GRAM). The technical risks are relating to the area of machinery (or technical systems), while another area of the human risks occurring on a workplace is focused on the human aspect (Safety). Analyses of the risk consequences within the framework of a civic community belong to the area of Security. The developed risk management models are intended for application of integrated approach to the performed analyses, taking into consideration specific hazards arising in the individual phases of machinery technical life cycle installed in various industrial technologies.

Keywords: Risk management, risk-based-thinking, integration, effectivity.

1 MANAGEMENT EXPECTATION

The problems of effective risk management in technical practice require finding of such solutions that would make the investments in measures from which each has its own measure of effectiveness as effective as possible.

The requirements of industry are based on requirements of the customers, community and legislation that in certain way form a frame for doing business of the organization.. Sustainable competitiveness has its advantages [2] but it requires culture in risk management through the whole organization. The last economic crisis (2008-2010) had its negative impacts that pointed out shortcomings in management skills. These shortcomings resulted mainly from a wide range of business opportunities (globalization), increasing speed of information dissemination (IT – Information technology communication), legislative framework (environment, OH&S, effective use of energy and the like) and especially, public opinion. In the past, several approaches for improving the management existed, for example, a "resource-based view (RBV) with IT support [3]," business model "based on the value-based principles, [4]," enterprise risk management "[5], up to an " integrated sustainable management system "(ISO standard 26000) based on ethical behavior and overall respect.

In certain time and environment, all these approaches were based on the effort to create a balance between requirements of parties interested and possibilities (resources) to achieve the organization´s goals on a long-term basis. Nowadays, this balance can be managed only complexly, watching and managing all processes taking into account internal and external aspects affecting them.

Risk management is the only universal tool enabling on long-term basis and systematically to create an environment that is on one side prepared to minimize all impacts (threats) threatening the competitiveness but on the other side also to identify possibilities (opportunities) how to improve.

This tool requires some rules, such as:

- Knowledge and understanding of the risk management, requirement and their use in various management areas.
- Basic algorithm (steps) of the risk assessment, its importance in the risk management (proposed measures).
- Levels and specification of the risk management processes depending on its management areas.
- Methods and procedures „best suitable“for certain identified threats and subsequently analyzed and assessed risks.
- Relationship between the risks resulting from individual resources (areas) and their impact on goals set.
- An integrated approach at their complex management: transparency, communication skills, measurability and dynamics in view of the changes requirements.

Creation of a comprehensive system for risk management (hereinafter referred to as GRAM) was based on several years of research activities (for example, . 7PR „iNTnteg-Risk“) and practical experience at in implementing the requirements of legislation and practice (OH&S, Major Accident Risk Prevention – SEVESO III, Critical infrastructure, Pipeline integrity assessment) of a workplace.

2 MODEL STRUCTURE

Model parameters took into account the organization goals depending on its activity in a given business environment. In the first stage, it was a field of OH & S (Safety - SA), and security (Se) to which the areas of requirements for quality, environment, cost and more we assigned. Creation of criteria for hazard / threat identification, probability estimation included not only existing risks but also assessment of newly rising risks (new materials, technologies, an aging population and so on.). Description of the individual stages of solution was as follows:

1. Analysis of methods and processes for identifying new and emerging risks of industrial technology (object) in relation to Safety and Security in all stages of their life cycle.
2. Requirements for Risk Based Thinking as a new aspect of quality management system according to ISO 9001. The creation of algorithms for assessing the significance of the possible correlation of the individual areas (elements and criteria) in order to find common approaches to comprehensive risk management.
3. Creation of a comprehensive tool for measuring the performance of the integrated environment of management system (Key Performance Indicator - KPI).
4. Creation of risk management models, including the definition of the parameters stages of causal dependence, based on the principle of generic approach "Generic Risk Assessment Model" - GRAM.
5. Creation of a specific structure for measuring performance of these management processes, through effective indicators, the so called KPI (Key Performance Indicators).
6. Verification of the model and application development for the implementation of measures under the minimisation of risks in integrated risk management taking into account the requirements of comprehensive security (Sa&Se) for selected types of industrial technologies.

The relevant stages of solutions were scheduled over five years and required a detailed description of processes in order to conduct targeted analyses related to the areas of the solved issues. The basic scheme of the GRAM model was created continuously, its form originated in the early stages of research and it was gradually completed into the final-form with the aim of a more detailed elaboration in the form of algorithms (see Fig. 1).

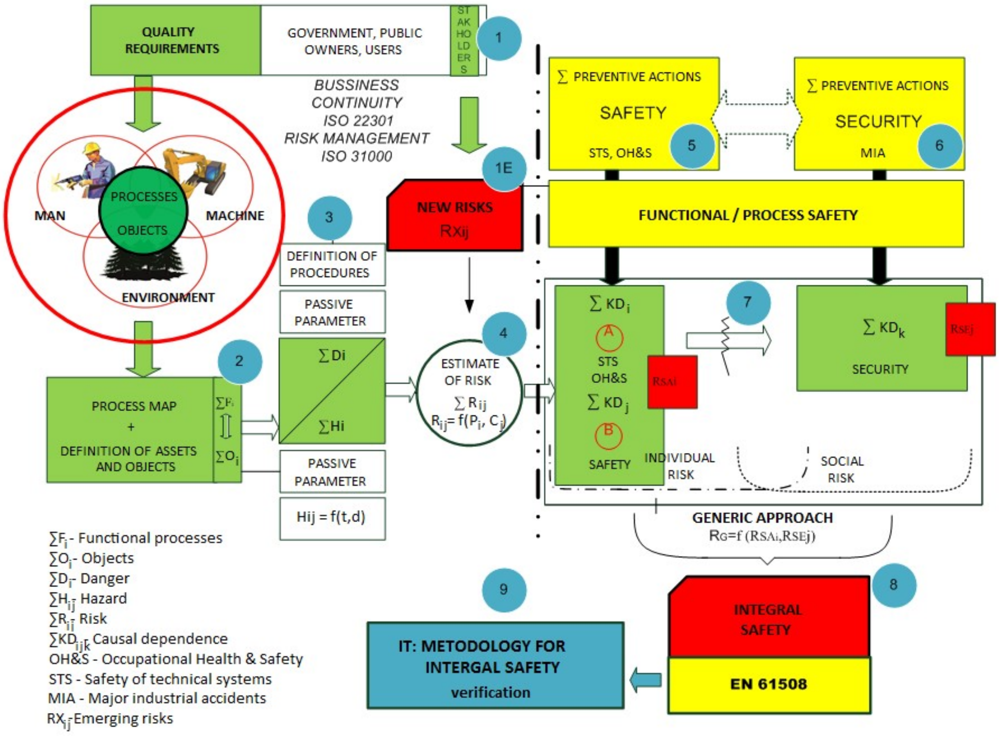


Fig. 1 Base structure of GRAM model

2.1.1 Steps of the GRAM building process

The first stage of the solution focused on analytical methods used in various risk assessment processes, without their interconnection. It was based on the legislative requirements in areas such as: security, environment, machinery safety, occupational health and safety, prevention of major industrial accidents.

When analysing the requirements in the field of civil security, areas such as critical infrastructure protection, civil protection, protection of classified information, information security, crime prevention and the like were explored.

The basic philosophy was based on the assumption that a comprehensive risk assessment must be based on the relation between probability and consequences, taking into account the so-called direct and indirect effects (see Fig. 2).

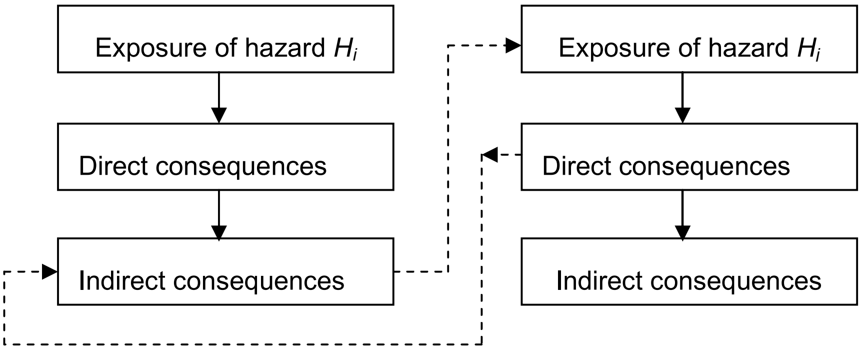


Fig. 2 Risk indicators and their relation

The aim was to describe the basic functional risk assessment for each observed group (hazards H_{ij}) and area according to the formula:

$$R = \sum_{i=1}^{n} P_i C_i \qquad (1)$$

Where: P_i is probability (or likelihood) of *i* – risk; C_i is consequence (effect, loss) the risk can cause.

While it was the search for mutual relations so as to express the risk parameters for the individual areas and their intersections, as well as the areas of Safety and Security [6] in the light of existing, new and emerging risks (*Em & Ex*) and the life cycle (*LC*) of the object.

$$R_{Sai} = \sum_{i=1}^{n} Psa_i Csa_i \quad \cap \quad R_{Sej} = \sum_{j=1}^{n} Pse_j Cse_j \qquad (2)$$

Analyses were based on the results of a research within the project iNTteg- Risk [7].

With regard to the effects of lifecycle based on the value of risk, the criteria for assessing the significance of the stage of the life cycle of an object on the basis of life cycle costs were determined. It was based on the prerequisite (Accordance Caisc Corporation study, [8]) that only 5% of the total cost could be affected by operation and maintenance.

The output from the first stage created the first filter for determining the criteria for Business Objectives identification and evaluation: Consequence (potential lost) categories and their severities (*CCS*).

The aim of the second stage was to identify the areas of possible correlations of individual processes in risk management processes by identifying critical objects.

Multi-criteria matrix to identify potential adverse impacts of CCS and their assessment was defined for the following areas [9], [10], (see Tab. 1, 2):

- Health and Safety (OH&S) - Safety - *CSa*;
- Environmental leaks and pollution - Environment - *CE*;
- Downtime - the duration of the service interruption - Downtime - *CD*;
- Quality - Customer Satisfaction - Quality - *CQ*;
- The cost of repairing the equipment - Repair Cost - *CR*;
- Financial losses and property losses - Financial loses / Property - *CF*.

Tab. 1 Multi-criteria matrix for each area of losses *CCS*

Category of losses – **CCS**		**Level of loss**							
		I. Negligible		II. Border		III. Critical		IV. Catastrophic	
CSa	OH&S	S1	No impact on human	S2	Injury or a partial harm to health	S3	Serious injury, significant damage to health	S4	Higher number of people affected, death
CE	Environment	E1	No damage (e.g. contamination)	E2	Damage/contamination in operation manageable by own resources	E3	Extent of damage/leakage in operation is serious, help is necessary during its removal	E4	Extent of damage/leakage is disastrous and has long-term impact on the area around the plant
CD	Operation (downtime)	D1	Operation downtime is negligible	D2	Operation downtime up to 2 hours.	D3	Operation downtime is from 2 hrs.	D4	Operation downtime is more than 24

							to 24 hrs.		hrs.
CQ	Quality	Q1	Product defect has no impact on the product quality	Q2	Product defect must be additionally removed	Q3	Product defect requires repeated production (recasting)	Q4	Product defect requires the change of technology. Dissatisfaction of customer
CR	Cost of repairs	R1	Repair will not exceed cost planning	R2	Repair cost exceeds 1000 EUR	R3	Repair cost is over 1000 and less than 5000 EUR	R4	Repair cost exceeds 5000 EUR
CF	Financial loss - property	F1	Minimal impact on the budget	F2	Higher energy consumption up to 5000 EUR	F3	Losses exceed 5000 Euro, less than 20000 EUR	F4	Losses are high and exceed 20000 EUR

CCS parameter is defined and assessed as a function of the severity of types (level of severity) of individual areas of losses for the *i*-component, determined on the basis of social perception in the current conditions (legislation, public, etc.).

Tab. 2 Multi-criteria matrix and its assessment

Criticality level *RK_i*	**Safety CSa**	**Environment CE**	**Operation CD**	**Quality CQ**	**Repair costs CR**	**Financial loss CF**
	V *4	V*3	V=1	V*2	V=1	V=1,5
A3: V = 8	32	24	8	16	8	12
A2: V = 7	28	21	7	14	7	10,5
A1: V = 6	24	18	6	12	6	9
B2: V = 5	20	15	5	10	5	7,5
B1: V = 4	16	12	4	8	4	6
C3: V = 3	12	9	3	6	3	4,5
C2: V = 2	8	6	2	4	2	3
C1: V = 1	4	3	1	2	1	1,5

Risk assessment of an object RK$_i$:
Very high risk VVR: points from 75 to 100; High risk VR: points from 41 to 74;
Medium risk SR: points from 28 to 41; Low risk NR: points to 27.

Remark: Weight of *RK$_i$* is related to the analysis of criticality of objects – category A, B, C. Probability is defined at max. 5 levels.

$$Cg_i = f(Sa_i, E_i, Q_i, D_i, R_i, F_i, IS_i) \qquad (3)$$

Where: $CSa_i, CE_i, CQ_i, CD_i, CR_i, CF_i$ - areas of loss CCS (parameter *RKI$_i$*); IS_i - factor taking into consideration the impact of loss in relation to individual and social risk.

Remark: The value of IS_is increases with the prerequisite of severity of social risk - IS_i = 1: individual risk, IS_i = points for the possibility of a major industrial accident, not exceeding corporate limits, IS_i = points for public intervention in the immediate vicinity of the plant, IS_i = 7 for the potential transboundary impacts, IS_i = 10 for threats to the region or the state economy as a result of CCS (e.g. as an element of critical infrastructure).

To determine the estimates of probability of the risks/threats, point scores were applied and divided into five levels. However, taking into account all aspects and impacts on the probability of a negative event) in the space of Sa&Se (risk and threat) led to modeling of probability taking into account the causality as follows:

$$Pg_i = f(Pa_i, Pe_i, LCm_i, Eu_i) \qquad (4)$$

Where: Pa_i – the probability of the i – risk (see Tab. 3); Pe_i – the probability of emergence of the i – risk (see Tab. 4); LCm_i – taking account the impact of life cycle stage; Eu_i – the impact of uncertainty as a factor in the type of risk.

Tab. 3 Safety: probability of hazard - *Psa*

Safety /hazards: probability - ***Psa***		
Level	Description	Assessment
I	Error/failure occurrence in a process is unlikely, the error is unplanned, inadvertent	od 0 po 3
II	Error/failure occurrence in a process is probable, the error is unplanned, inadvertent but its cause is clear	od 4 po 6
III	Error/failure occurrence in a process is very probable, the error is unplanned, inadvertent but its cause is clear and registered	od 6 po 8
IV	Error/failure occurrence in a process is almost sure, the error is clear, deliberate act without the aim of lose can not be excluded, elimination of the cause is necessary	od 8 po 10

Tab. 4 Security: probability of threats - *Pse*

Security /threats: probability – ***Pse***		
Level	Description	Assessment
I	Error/failure occurrence in a process is unlike, planned and intentional error is almost impossible, there is no immediate threat	od 0 po 3
II	Error/failure occurrence in a process is probable, planned and intentional error is almost possible, immediate threat can be registered	od 4 po 6
III	Error/failure occurrence in a process is very probable, planned and intentional error is possible, immediate threat can be registered and is a result of intent of a group of people	od 6 po 8
IV	Error/failure occurrence in a process is almost certain, planned error with malicious intent is possible, threat is clear and concrete and is a result of intent of a group of people	od 8 po 10

Addressing the **third stage** focused on the development of a model of risk management as part of integrated security systems (Sa&Se), hence creating a generic risk assessment model GRAM.

According to the results of previous analysis and modeling of CCS, a comprehensive GRAM model defined by the following parameters and their relation was created:

- ✓ description of causality in the field of Safety – Rsa_i *(Safety Risk)*,
- ✓ description of causality in the field of Security – Rse_i *(Security Risk)*,
- ✓ assignment LC measure parameter – *LCm (Life cycle measure)*,
- ✓ assignment of parameter reflecting the impact of uncertainty: risk type Rx_i - *Eu* (*Em emerging)*, *emerging progress* – *Ep*, existing – *Ex*,
- ✓ defining scales for determining the extent of the intersection between Sa&Se – *SSM - Sa & Se measure,*
- ✓ methodology for estimation and risk assessment – risk matrix ($Rg_i = f(Rsa_i, Rse_i)$),
- ✓ determining risk management parameters - the measure and its impact on the value of risk (measure parameters) - $M_{Sa\&Se}$,
- ✓ risk management efficiency parameter (KPI_i) - M_{KPIi}.

Matrix of risk generic risk assessment model GRAM was formed as an intersection of scores of probability Pg_i and consequence Cg_i (see Tab. 5).

Tab. 5 GRAM Risk matrix

Cg = Sa+E+Q+D+R+F+IS				
Pg = Pse+Psa+LCm+Eu	CI	CII	CIII	CIV
PI	22-39	29-58	48-74	64-115
PII	34-45	41-64	60-80	76-121
PIII	39-54	46-73	65-89	81-130
PIV	49-64	56-83	75-99	91-140

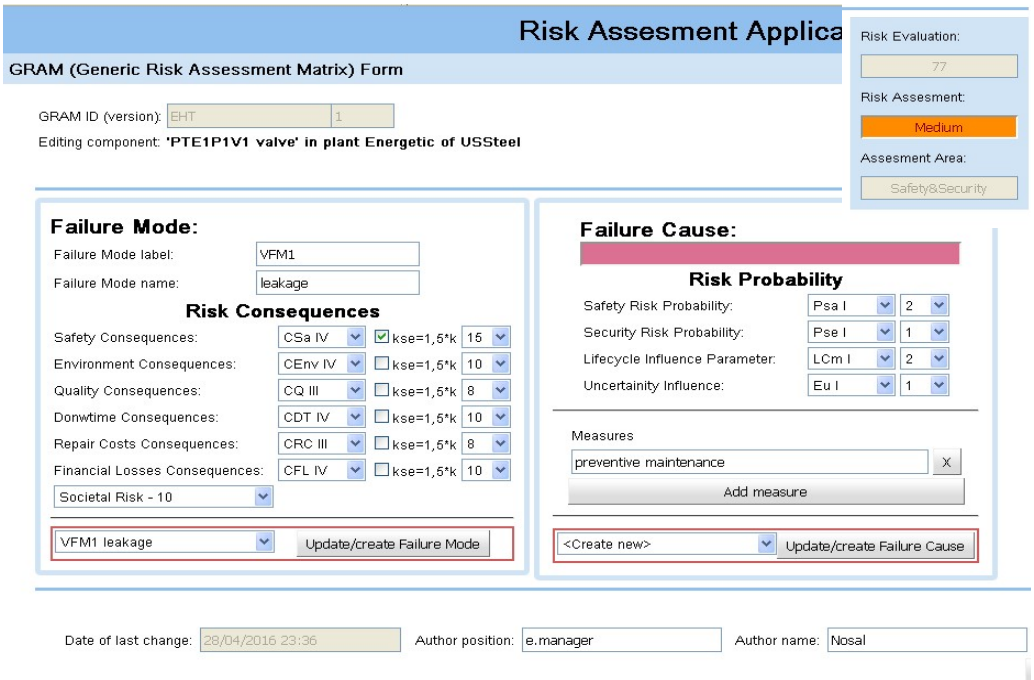
Low risk	(22 – 58)	There is no need to take action - residual risk
Middle risk	(59 – 83)	It is necessary to adopt measures - ALARP principle (As Low as Reasonable Possible)
High risk	(84 – 140)	It is necessary to investigate all the effects and take immediate action.

3 RESULTS

To verify the functionality of the proposed model a software application (see Fig. 3) was developed in cooperation with the Faculty of Electrical engineering. This application allows to verify reliability of the model and to assess whether the model parameters are set correctly.

The software structure is as follows:

- Basic data on the operation; Tree structure - plant - production unit - asset - physical asset; Assessor's data (team) - name, job title, date; Identification of risks – hazards /threats (failure mode); Assigning values *Pgi* and *Cgi* to every described cause; Risk evaluation – Risk matrix; Proposal of measures and their assessment (KPI, [9]).



Risk Assesment Applica

GRAM (Generic Risk Assessment Matrix) Form

GRAM ID (version): EHT 1

Editing component: **'PTE1P1V1 valve' in plant Energetic of USSteel**

Risk Evaluation: 77

Risk Assesment: Medium

Assesment Area: Safety&Security

Failure Mode:

Failure Mode label: VFM1

Failure Mode name: leakage

Risk Consequences

Safety Consequences:	CSa IV	☑ kse=1,5*k	15
Environment Consequences:	CEnv IV	☐ kse=1,5*k	10
Quality Consequences:	CQ III	☐ kse=1,5*k	8
Donwtime Consequences:	CDT IV	☐ kse=1,5*k	10
Repair Costs Consequences:	CRC III	☐ kse=1,5*k	8
Financial Losses Consequences:	CFL IV	☐ kse=1,5*k	10

Societal Risk - 10

VFM1 leakage

Failure Cause:

Risk Probability

Safety Risk Probability:	Psa I	2
Security Risk Probability:	Pse I	1
Lifecycle Influence Parameter:	LCm I	2
Uncertainity Influence:	Eu I	1

Measures

preventive maintenance

<Create new>

Date of last change: 28/04/2016 23:36 Author position: e.manager Author name: Nosal

Fig. 3 GRAM software application

4 CONCLUSION

The GRAM model in its current form creates a platform for possible upgrades or other extensions that take into account parameters such as from the area of OH & S: noise, vibrations, chemicals, human errors and the like. Qualitative approach applied in the methodology of the model can be changed to semi-qualitative in case of collection and evaluation of data from the operation providing so new possibility of the model extension. Research task of the risk assessment complexity brought during five years many questions. The research team tries now to standardize management and control of processes using the principles of the GRAM model to enable implementation of fully automated access on the basis of precise rules. Applied outputs of the GRAM model in industrial practice brought a positive response, especially in relation to the requirements of ISO 9001: 2015 for risk assessment as an integrating tool for meeting all the requirements of interested parties in the organization.

5 ACKNOWLEGMENT

This paper was developed within the project APVV - 0337-11. The research on new and emerging risks of industrial technologies within integrated security as a prerequisite for the management of sustainable development and also within the University Science Park TECHNICOM for Innovation Applications Supported by Knowledge Technology, ITMS: 26220220182, supported by the Research & Development Operational Program funded by the ERDF."

REFERENCES

[1] Faber, M.H., Stewart, M.G. (2003). *Risk assessment for civil engineering facilities: critical overview and discussion*. Reliability Engineering and System Safety 80, pp.173-184.

[2] Oliver, Ch. (1997). Sustainable Competitive Advantage: *Combining Institutional and resource-based views*. Strategic Management Journal, Vol. 18:9, pp. 697-713.

[3] Dehning, B., Stratopoulos, T. (2003). *Determinants of a sustainable competitive advantage due to an IT-enabled strategy*. Journal of Strategic Information Systems 12, pp. 7-28.

[4] Morris, M, Schindehutte, M., Allen, J. (2005). *The entrepreneur´s business model: toward a unified perspective*. Journal of Business Research 58, pp. 726-735.

[5] Brustbauer, J. (2014). *Enterprise risk management in SMEs: Towards a structural model*. International Small Business Journal, 34: pp.70-85.

[6] Vargová, S., Sinay, J. (2015). *Safety & Security Management System in Public Transport*. Security research conference 10th Future Security. – Stuttgart, Fraunhofer Verlag, pp. 477-480.

[7] Pacaiova, H. and col., Project 7RP: *iNTeg- Risk: Early Recognition, Monitoring and Integrated Management of Emerging, New Technology related Risk*. http://www.integrisk.eu-vri.eu.

[8] Durairaj, S. K, Ong, S.K., Nee A.Y.C., Tan, R.B.H. (2002). *Evaluation of Life Cycle Cost Analysis Methodologies*. Corporate Environmental strategy, vol. 9. Issue 1, pp. 30-39.

[9] Pacaiova, H., Namesanska, J. (2014). *Quality of maintenance as a part of production quality*. 17th QMOD-ICQSS: Quality Management and Organizational Development Conference: proceedings: Part 3: Annex 1: 3rd - 5th September 2014, Prague, Czech Republic. University Library Press, pp. 1-10.

AN APPROACH TO BALANCING OF SAFETY AND SECURITY REQUIREMENTS UNDER UNCERTAINTY

Daniel Lichte[1], Stefan Marchlewitz[2], Kai-Dietrich Wolf[3],

[1] *lichte.iss@uni-wuppertal.de*
[2]*marchlew@uni-wuppertal.de*
[3]*wolf.iss@uni-wuppertal.de*

Institut für Sicherungssysteme, Bergische Universität Wuppertal,
Talstr. 71, 42551 Velbert, Germany

Abstract

The assessment of measures to optimize and balance the quality regarding safety and security is difficult, as influencing factors may be subject to larger variations and uncertainties have to be considered.

This paper presents an approach to a comprehensive modeling of safety and security risks. It is based on the generalized definition of security risk as a function of threat, vulnerability and impact and uses probabilistic methods to model uncertainties. Risk thus becomes an interconnection of probability density functions rather than a product of discrete variables.

The presented approach enables a variance based sensitivity analysis of the overall risk assessment of safety and security contributions. In sensitivity analysis, the variance of the density function as a result of introduced uncertainties is taken as the basis for calculating a safety and security range. Simultaneous consideration of safety and security may serve as basis for well founded decisions for system optimization.

Keywords: risk assessment, variance based sensitivity analysis, safety and security range.

1 INDTRODUCTION

The development of safe and secure systems as well as facilities in (industrial) infrastructures is a major challenge, particularly because safety and security boundary conditions have to be considered simultaneously. For safety analysis of infrastructures and inherent technical systems, a wide range of quantitative methods exists. In these models, the safety level is often determined via probabilistic models that predict the failure rate of the system or of individual components. Besides the possibility to determine the safety on the logical and physical layer of the product, newer approaches focus on the performance of systems rather than components.

Both, safety and security risks can be described in terms of probability; a scheme for the analysis of interactions between safety and security functions of the system components has not yet been developed and there is still a lack regarding common methodologies for hazard and risk analysis allowing for an integrated consideration of both - safety and security.

Typically, the security assessment of such complex systems consisting of physical and IT-based subsystems requires different analytical methods. The majority of security analysis methods are based on qualitative or semi-quantitative approaches like attack trees. However, a few existing methods allow the description of security risks by probability functions. The advantage of the latter methods is the inclusion of uncertainties regarding different influencing factors.

This paper illustrates the approach based on a critical infrastructure example and the related scenarios which constitute different challenges regarding safety and security issues that are tackled.

2 STATE OF THE ART

So far, no comprehensive approaches emerged that consider safety and security aspects of a system simultaneously. At the same time, a number of methods exist to assess the differently defined risk of both aspects. In the following, the differing methods and risk definitions are outlined.

2.1 Safety Assessment and Technical Risk

Actually there is a wide range of existing methods for safety assessment. Ortmeier divided them into qualitative and quantitative methods of analysis [1]. In order to evaluate a product or system in terms of its safety, often a combination of methods is used. In most of the cases, it is not exactly safety which is determined. The assessment is either carried out using probabilistic models that predict the system failure behavior due to the failure rate of individual components or based on a risk assessment.

A risk assessment could describe the probability that the system assumes an unsafe condition or that a hazard results in an adverse event for an employee in the context of occasional safety. Both options require knowledge of a device structure, the environment and the behavior of components define a risk in detail. In this case the risk is defined by [2]:

$$Risk = Hazard\ Probability \times Consequence \tag{1}$$

In addition to allowing the determination of safety through logical and physical shape of the product or system, new approaches focus on its functions. These approaches rely on the identification and classification of threats with the subsequent derivation of safety objectives, i.e. in automotive industry [3], process engineering [4], nuclear power [5] or aerospace. However, with regard to the identification of interactions with security-related functions, present research yields insufficient practical approaches and concepts that could be applied in industry sectors [3].

2.2 Security Assessment

Security comprises a number of issues covering different fields of expertise; therefore a comprehensive view is needed for a holistic security assessment [6]. Physical security as a part deals with the protection of (critical) infrastructures from intentional physical attacks[7]. The aim of physical security measures is to prevent an attacker from reaching his goal by different means of protection, detection and intervention and also set up resilient structures to lower the consequences of successful attacks [8]. The corresponding risk definition can be defined as [9] [10]:

$$Risk = Threat \times Vulnerability \times Consequence \tag{2}$$

In security risk assessment this definition helps to combine quantitative consequences of attacks with probabilities of successful attacks. Inherent uncertainties regarding the three risk should be cautiously considered [11]. Approaches to security risk assessment may be divided into qualitative, quantitative and hybrid methods. Qualitative methods are mostly based on expert knowledge, while existing quantitative methods use discrete probabilities. Developed quantitative methods are aimed at cost-benefit considerations that wage between potential financial losses as attack results and the probability of occurrence of various attack scenarios and the vulnerability of the security system [12].

Quantitative vulnerability analysis (as part of the quantitative risk analysis methods) is mostly based on methods adapted from reliability as well as general risk analysis. Here, the considered security system is modeled dependent on given attack scenarios [13]. The vulnerability modeling approaches can be further split up into mainly analytical but also formal methods. An overview of approaches is given in [14]. In this context, Contini et al. introduce the integration of simple probability distributions to describe protection measures into attack trees [15] [9]. Hence, it is possible to analyze the security systems ability for an attack intervention by comparing the systems response probability distribution f_R and residual protection f_R.

$$P\{t > \tau\} = \int_{t_o}^{t_1} f_R(t) \int_{\tau_o}^{t} f_A(\tau) d\tau dt \tag{3}$$

This relation between protection and intervention is also described by Garcia [16]. The approach describes feasible barrier based attack paths as part of different attack scenarios. The model is time based and introduces the critical detection point outlining the latest effective possible point of detection.

2.3 Variance Sensitivity Analysis

The variance based sensitivity analysis has been applied in recent years in literature to various problems like the assessment of the reliability of adaptronic structure systems [17], the analysis of dynamic fault trees [18] or the analysis of nonlinear mathematical models [19]. The purpose of this analysis is to determine the influence of one or more parameters in a mathematical model and to identify the associated uncertainties. The respective parameters will be defined as stochastically independent random variables X_i, which can be expressed by the corresponding probability density function Y. Using a connection e.g. by an equation of the different parameters the model of a system can be described. In order to determine the influence of a parameter on the model output the first order effect is calculated by:

$$First\ Order = \frac{Var[E(Y|X_i)]}{Var[Y]} \tag{4}$$

By the consideration of the interactions between the parameters the total order that considers the sum of all partial sensitivity effects will be calculated by [20]:

$$Total\ Order = \frac{Var[E(Y|X_{-i})]}{Var[Y]} \tag{5}$$

The total order effect considers the sum of all partial sensitivity effects. In this case, X_{-i} refers to the amount of all input t variables excluding the i-th parameter. In a combined risk assessment, the interaction of the parameters with regard to the combined risk is important.

3 APPROACH

The article proposes a new approach to a general risk assessment by unifying the yet independent risk models of safety and security. Therefore a generalized risk formulation is introduced that covers both aspects and harmonizes the consideration of risks.

In order to be able to handle uncertainties inherent to safety and security and to analyse interactions between safety and security measures the model utilizes probability density functions (pdf) to describe the system's characteristics regarding both aspects. For analysis purposes, a variance based sensitivity analysis is proposed that helps to investigate the weight of input variables as well as the impact of uncertainties on the resulting general risk. This information helps to make well founded decisions regarding the system optimization.

After deriving the probabilistic model of generalized risk, it is applied to an example infrastructure of the chemical process industry; here a kerosene producing plant. The input parameters for safety and security and associated assumed pdf are derived and a possible interaction between safety and security measures is presented.

Finally, a variance based sensitivity analysis is conducted and the findings regarding uncertainties and safety-security interactions and resulting goal conflicts are discussed.

3.1 Merging Safety and Security

As shown in the state of the art, there are different approaches for safety and security analysis. The two fields are separately considered, as a joint risk assessment is not possible. To tackle this issue, the article proposes a new approach combining both, safety and security risks in a merged assessment that is based on the usage of probabilistic density functions (pdf).

Therefore the definition of safety and security risk is generalized in a unified expression based on the security risk. It is applicable to both fields.

$$R = T * V * C \tag{6}$$

Unlike the standard definition, safety risk is analogously to security risk defined as a product of a threat, the system's vulnerability and possible consequences. The newly introduced distinction between threat and vulnerability allows the description of possible triggers of system failures, such as accidental misuse or single subcomponent failures. Additionally, the introduction of vulnerability enables the description of technical and operational safety measures, including the manual intervention as a last resort. Fig. 1 shows the differing meanings in terms of introduced risk definition.

Safety	• Component Failure • Accidental Misuse • …	• Technical Safety • Manual Intervention	
$Risk = Threat * Vulnerability * Consequence$			
Security	• Sabotage • Terrorist Attack • …	• Asset Protection • Detection • Intervention	

Figure 1: Differing Impact Factors for Safety and Security Risk

The description of the single terms based on pdfs allows a computation of the resulting combined risk density function. Thus, a consideration of uncertainties related to the different safety and security risk elements is possible. Furthermore, existing inherent interactions between safety and security measures of the system which affect the overall risk can be included into the mathematical model. This allows a further analysis of these interactions and the impact of different measures intended to enhance either safety or security on the total risk, e.g. by a variance sensitivity analysis.

Following, both risk formulations and their elements are derived.

3.2 Safety Risk

The safety risk is, as above introduced, a combination of the three factors of threat T, vulnerability V and consequence C.

$$R_{safety} = T_{safety} * V_{safety}\left(P_{Safety}, I_{Safety}\right) * C_{safety} \tag{7}$$

As there are different possible threats that can lead to system failures the describing factor T_{Safety} can be shaped differently depending on the specific consideration. Possible impact factors for its shaping are for example the probability of accidental misuse, as well as failure probabilities of critical single system components. The consideration of the consequences C_{Safety} is based on company values and has to be estimated individually for considered infrastructures. The associated pdf describes the probability of occurrence related to the severity of the consequences. The vulnerability of the safety system V_{Safety} can be divided in two subcategories to assess the probability of system failures resulting in the considered threats.

Firstly, the technical protection of the system P_{Safety} to prevent system failures is considered. Hereby, the failure probability of the functional systemic interaction of common technical measures such as cold and hot redundancies or automatic emergency safety devices is described. Secondly, the manual intervention to reach a safe state I_{Safety} as a last resort to prevent critical failures contributes to the safety of the whole system. The conditional probability of the time needed for intervention $p_{i,Safety}(t)$ and the time-dependant probability of system failure p_{sf} as a result of failing technical protection (P_{Safety}) describes this measure:

$$P_{I,safety}(t) = \int_0^t p_{i,safety}(t) \left[\int_\tau^\infty p_{sf}(\tau) d\tau\right] dt \tag{8}$$

The safety related vulnerability is then derived by the following expression describing the subsequent failure of technical protection and manual intervention in case a threat is realised:

$$p_{V,safety}(t) = 1 - p_{P,safety} \left(1 - p_{P,safety}(t) \cdot P_{I,saftey}\right) \tag{9}$$

This yields to the resulting cumulated vulnerability of the safety system:

$$P_{V,safety}(t) = \int_0^t \left[1 - p_{P,safety} \left(1 - p_{P,safety}(t) \cdot P_{I,saftey}\right)\right] dt \tag{10}$$

3.3 Security Risk

Likewise the safety risk, the security risk is defined as a combination of threat, vulnerability and consequence. The definition corresponds to the classic security risk:

$$R_{security} = T_{security} * V_{security}(P, D, I) * C_{security} \tag{11}$$

The factor threat $T_{Security}$ and the associated pdf $p_{t,Security}(t)$ describe the probability of an occurring attack in dependence to time. Hereby, different characteristics of considered attack scenarios and infrastructures should be taken into account. The consequences of a possible attack $C_{Security}$ are equal to safety risk

The vulnerability $V_{Security}$ describes the probability of an attacker successfully reaching his goal, in this case a system failure. It is defined as the result of protection, detection and intervention measures. The provided protection of security measures and the time needed for intervention are considered as time-dependent pdf's:

$$p_{P,security}(t), p_{I,security}(t) \tag{12}$$

As a simplification, the time needed to detect an attacker t_D is assumed as a discrete value. Dependent on t_D the probability of a failed intervention can be formulated as the conditional probability that the attacker breaks through the system protection before an intervention stops him:

$$P_{I,security}(t_D) = \int_{t_D}^{\infty} p_{I,Security}(t_I - t_D) \cdot \left[\int_{t_I}^{\infty} p_{P,Security}(\tau + t_D)\, d\tau \right] dt_I \tag{13}$$

The combination of probability of a failed intervention on the one hand and given time slot inside which protection measures prevent the attacker from breaking through on the other hand describe the systems vulnerability.

$$P_{V,security}(t) = \int_{0}^{t} p_d(t_d) \cdot P_i(t_d)\, dt_d \tag{14}$$

3.4 Derivation of Combined Risk Function

The formulations for the safety and security risk function are now combined to a general risk density as a function of consequence severity for a chosen time interval from 0 to t:

$$\begin{aligned} R_{Combined}(t) &= P\left(r_{Safety}(t)\right) \cup P\left(r_{Security}(t)\right) \\ &= (R_{Safety}(t) + R_{Security}(t) - \left(R_{Safety}(t) \cdot R_{Security}(t)\right) \end{aligned} \tag{15}$$

3.5 Scenario description

For further explanation a part of a process plant is selected. Depending on the type of plant there are different hazards; like fire, explosion, leakage of toxic substances or sabotage. All these hazards will be expressed by T_{safety} and $T_{security}$. The consequences will be summarized by $C_{safety} = C_{security} = C$ based on the assumption that the consequences are stochastically independent.

The vulnerability which describes the system characteristics will be defined by $p_{V,safety}(t)$ and $P_{V,security}(t)$. The safety vulnerability interacts with security protection measures $p_{p,security}(t)$, as the measures possibly hinder a manual intervention. This is considered by the simplified equation for normalized total intervention time:

$$p_{i,total,safety}(t) = \frac{p_{i,safety}(t) + 0.2 \cdot p_{p,security}(t)}{P_{i,total,safety}} \tag{16}$$

For specific calculation the following tab. 1 shows the assumed values of the input parameters:

tab. 1: Input Values of Used Variables

Variable	Probability Distribution	Parameter First Run	Parameter Second Run
$p_{p,safety}(t)$	exponential distribution	$\lambda = 1.6 \cdot 10^{-1}$	$\lambda = 1.6 \cdot 10^{-1}$
$p_{p,security}(t)$	normal distribution	$\mu = 180\ \sigma = 30$	$\mu = 360\ \sigma = 120$
$p_{i,security}(t)$	normal distribution	$\mu = 300\ \sigma = 70$	$\mu = 300\ \sigma = 70$
$p_{i,safety}(t)$	normal distribution	$\mu = 180\ \sigma = 30$	$\mu = 180\ \sigma = 30$
$p_{sf}(t)$	normal distribution	$\mu = 200\ \sigma = 50$	$\mu = 200\ \sigma = 30$

The safety and security of the system are related by $R_{Combined}(t)$. Here, the risk of a serious consequence for a period of two years is calculated. In order to evaluate the influence of each variable on the combined risk, a variance sensitivity analysis is performed using the software Simlab. In this example 24 576 samples with the sample method Sobol were generated to calculate the first order and total order effects. Fig. 1 shows the first and total order in a pie chart.

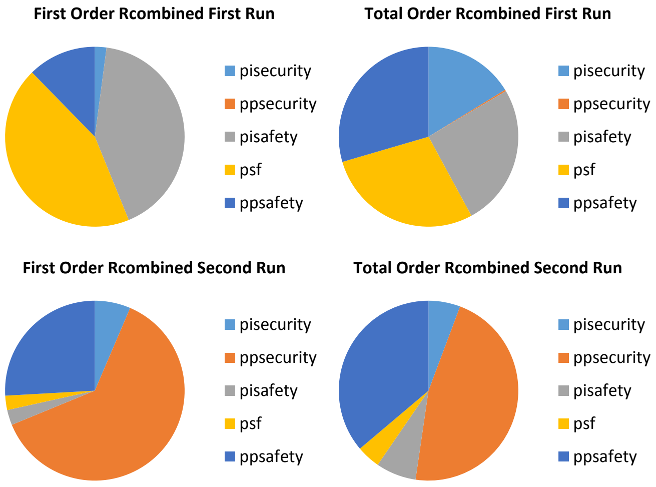


fig. 1: Impact of Input Values on Combined Risk

However, the greatest impact in the first run by total order is caused by the safety protection $p_{p,safety}(t)$ and by $p_{sf}(t)$ for the first order. Increasing physical security by corresponding measures in the second run noticeably influences the uncertainty of the combined risk in this configuration, because of increases standard deviation. While the second configuration has a higher margin of safety, it contains a higher variance. This result is derived by the uncertainty analysis because the discrete value $R_{Combined}$ reduces only by 4% regarding to the simultaneous risk of safety and security.

$$R_{Combined,first\ run} = 0.12 \tag{17}$$

$$R_{Combined,second\ run} = 0.079 \tag{18}$$

4. Conclusion and Outlook

Setting up a common model of risk assessment for safety and security opens the possibility to balance impact of security protection devices on safety installations. The variance based sensitivity analysis supports the decision making by visualizing the resulting uncertainty of a security measure. Although a structural security measure in principle provides greater security, however by a high variance proportion an adverse effect on the overall risk could be possible and the safety could be affected by a higher resulting uncertainty. For further investigation it will be interesting to verify particular inherent trade-offs between safety and security. Likewise, a simplification of the model seems to be of particular interest to promote its practical use.

REFERENCES

[1] F. Ortmeier, *Formale Sicherheitsanalyse*. Berlin: Logos Verlag, 2006.

[2] “BS OHSAS 18001:2007 - Arbeits und Gesundheitsschutz - Managementsysteme - Anforderungen.” Beuth Verlag, 2007.

[3] “ISO/CD 26262 - Road Vehicles - Functional Safety. Februar 2008.” Beuth Verlag, 2008.

[4] “BS IEC 61882:2001-08-28-Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP) - Leitfaden.” Beuth Verlag, 2001.

[5] “DIN EN 61508-1:2011-02-Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.” Beuth Verlag, 2011.

[6] Harnser Group, Ed., “A Reference Security Management Plan for Energy Infrastructure.” European Commission, 2010.

[7] J. Beyerer, J. Geisler, A. Dahlem, and P. Winzer, “Sicherheit: Systemanalyse und Design,” in *Sicherheitsforschung - Chancen und Perspektiven*, Berlin: Springer, 2010, pp. 39–72.

[8] M. L. Garcia, *The Design and Evaluation of Physical Protection Systems*, 2nd ed. Burlington, MA, USA: Butterworth-Heinemann, 2008.

[9] S. Contini, L. Fabbri, V. Matuzas, and Cojazzi, Giacomo, “Protection of Multiple Assets to Intentional Attacks: A Methodological Framework,” in *Probalistic Safety Assessment. International. 11th 2012*, Helsinki, Finnland, 2012, vol. 6, pp. 4343–4352.

[10] W. L. McGill, B. M. Ayyub, and M. Kaminskiy, “Risk Analysis for Critical Asset Protection: Risk Analysis for Critical Asset Protection,” *Risk Analysis*, vol. 27, no. 5, pp. 1265–1281, 2007.

[11] J. W. Meritt, “A Method for Quantitative Risk Analysis,” in *Proceedings of the 22nd National Information Systems Security Conference*, Arlington, VA, USA, 2008.

[12] P. L. Campbell and J. E. Stamp, “A Classification Scheme for Risk Assessment Methods,” Sandia National Laboratories, Albuquerque, NM, USA, SAND2004-4233, 2004.

[13] C. A. Roper, *Risk Management for Security Professionals*. Burlington, MA, USA: Butterworth-Heinemann, 1999.

[14] D. J. Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2011.

[15] S. Contini, G. G. M. Cojazzi, and G. Renda, “On the use of non-coherent fault trees in safety and security studies,” *Reliability Engineering and System Safety*, vol. 93, no. 12, pp. 1886–1895, 2008.

[16] M. L. Garcia, *Vulnerability Assessment of Physical Protection Systems*. Burlington, MA, USA: Butterworth-Heinemann, 2006.

[17] S.-O. Han, “Varianzbasierte Sensitivitätsanalyse als Beitrag zur Bewertung der Zuverlässigkeit adaptronischer Struktursysteme,” TU Darmstadt, Darmstadt, 2011.

[18] Y. Ou and J. B. Dugan, “Sensitivity analysis of modular dynamic fault trees,” in *Computer Performance and Dependability Symposium, 2000. IPDS 2000. Proceedings. IEEE International*, 2000, pp. 35–43.

[19] T. Henkel, H. Wilson, and W. Krug, “Global sensitivity analysis of nonlinear mathematical models-an implementation of two complementing variance-based algorithms,” in *Proceedings of the Winter Simulation Conference*, 2012, p. 154.

[20] A. Saltelli, S. Tarantola, F. Campolongo, and M. Ratto, *Sensitivity Analysis in Practice - A Guide to Assessing Scientific Models*. Chichester, England: John Wiley & Sons, 2007.

EVADEX - METHODS FOR STANDARDIZED EVALUATION OF EXPLOSIVE TRACE DETECTION SYSTEMS

D. Röseling[1], F. Schnürer[1], C. Ulrich[1], M. Wittek[1], H. Krause[1]

[1] *dirk.roeseling@ict.fraunhofer.de*
Fraunhofer Institute for Chemical Technologie ICT, Dept. Energetic Materials, Joseph-von-Fraunhofer Strasse 7, 76327 Pfinztal (Germany)

Abstract

The worldwide number of terroristic attacks has been increasing throughout the last years inside the aviation sector as well as in the non-aviation sector. The implementation of new innovative explosives trace detection systems can prevent bomb attacks and consequently save lives. The proper choice of the right detection method strongly depends on the field of application. Existing regulations and criteria are different when it comes to person controls compared to cargo inspection. Currently there are no generalized and standardized certification test methods available covering more than one field of application. This output is essentially required as guideline for end users to make the proper decision which type of detection system fits to their desired use.

Keywords: standardisation, explosive traces, detection, research project.

1 OBJECTIVE OF EVADEX

In the context of the tender for „Zivile Sicherheit – Schutz vor Explosionsgefahren und Chemieunfällen“ of the German Federal Ministry of Education and Research (BMBF) the research project EVADEX has started in November 2014 aiming at developing evaluation strategies and methods that enable a direct performance comparison of explosive trace detection systems. The new, innovative test methods as well as the new developed test samples allow a characterization of the detection systems against standardized criteria. The end-user will be able to choose detection equipment from a comparable variety specific to his intended application. It is worthwhile to mention that a specific scenario is explicitly linked to a unique requirements profile such as environmental conditions, expected threat materials and a scenario based set of interferents and background materials.

Explosive detection dogs, on the other hand, are representing a proven and well established detection method for some application scenarios. Hence, the olfactory functionality of dogs will be examined on a very fundamental level to find out if they are able to sense the pure explosive compounds or more the odour cocktail of an explosive formulation. The outcome of the research will be transferred into operational guidelines for detection dogs.

Overall, the project results shall be translated into a DIN specification. As innovative approach the consortium has chosen a comprehensive (figure 1) one which beyond the pure technological challenges as described above also includes the research of sociological and legal aspects directly related the explosive trace detection technologies as well as their use in field e.g. acceptance of a certain inspection measure for both the security inspector on the one hand as well as the person that is checked.

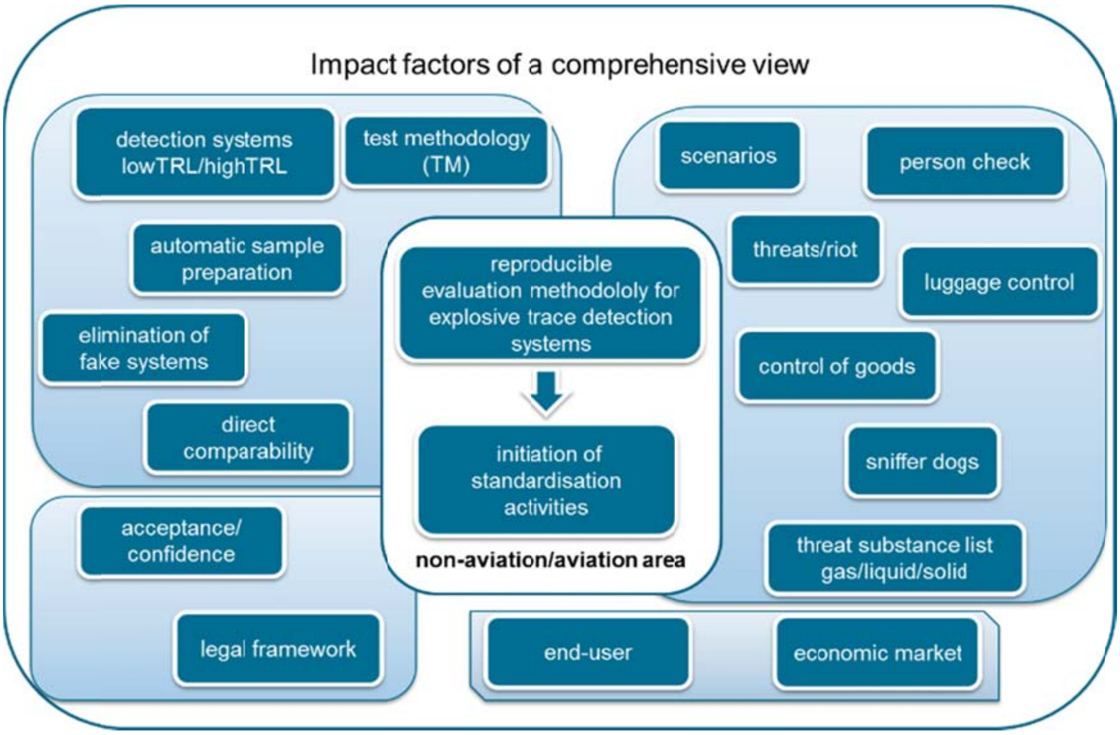

Impact factors of a comprehensive view
detection systems lowTRL/highTRL
test methodology (TM)
automatic sample preparation
elimination of fake systems
direct comparability
acceptance/ confidence
legal framework
reproducible evaluation methodoloy for explosive trace detection systems
initiation of standardisation activities
non-aviation/aviation area
scenarios
person check
threats/riot
luggage control
control of goods
sniffer dogs
threat substance list gas/liquid/solid
end-user
economic market

Figure 1: Impact factors and parameters of security equipment from evaluation to application in the field

1.1 Consortium partners and their roles

The consortium within the research project EVADEX contains overall six partners:

- Albert-Ludwigs-Universität Freiburg (center for security and society)
- Bundespolizei (Forschungs- und Erprobungsstelle Lübeck, Ref. 65)
- DIN e.V. (Deutsches Institut für Normung e.V., Berlin)
- Fraunhofer ICT (department for energetic materials, Pfinztal)
- GeSiM mbH (Gesellschaft für Silizium-Mikrosysteme mbH, Großerkmannsdorf)
- IAS GmbH (Inspire Analytical Systems, Oberursel)

Fraunhofer ICT as coordinator is responsible for providing the knowledge and scientific background of handling and preparing explosive materials. Furthermore, Fraunhofer ICT brings in its experience as official test centre explosive detection systems within the ECAC regime and on national level. The role of the participants of the Albert-Ludwig-University of Freiburg is twofold, on the one hand they are investigating the sociological aspects related to security inspections as a whole as well as the legal framework e.g. what is a security officer allowed to do within a given control situation and what are the rights of the person that are investigated. Bundespolizei represents on major end-user in the field of security equipment and supposed to feed in their experience regarding application scenarios of security measures, common threats as well as providing their sniffer dog team. The important role of DIN within EVADEX is to guide and contribute the proposed work toward a concept that is eligible to be transferred into a so called DIN SPEC (preliminary step of a standard). One major issue known within the evaluation of explosive trace detection system is the sample preparation on a level down to nanogramms. The quality management will be tremendously increased by implementing GeSiM as partner with the intention to transfer manually handling steps to an automatically process of liquid, gels and solid explosive traces. IAS as an expert in the field of inventing gas generators will develop a system capable of generating define gas concentration in the expected realistic range that can be found in the field for both the detection systems and the sniffer dogs.

2 RESEARCH AND METHODOLOGIES

2.1 Framework of EVADEX

The first goal of the project was to define the framework for the work to be followed. In collaboration of Bundespolizei and Fraunhofer ICT the threat and interferent substance list has been defined. As a matter of fact, the threat substances that are commonly used within incidents are more or less independent to security related scenarios. On the other hand, the so called interferent substances are directly related to a scenario in terms of appearance and furthermore may have a different impact on the various detecting methods of security equipment. In addition, common surfaces have been defined due to the fact that most of the commercially available trace detection systems are using a swabbing technique to take up a sample. Since the above mentioned information are classified no further details will be mentioned.

2.2 Application scenarios as basis for generic scenarios

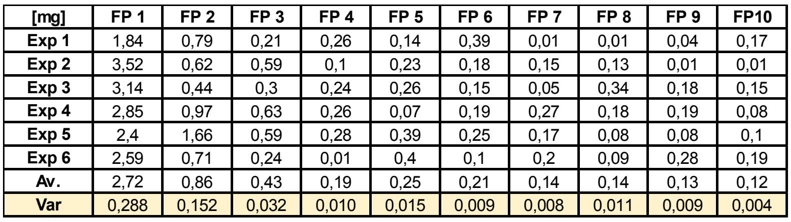
The objective of EVADEX is to develop some type of standardised evaluation test method for explosive trace detection systems guiding and contributing to the decision of end-user to assess either the best application scenario or to find the best system for a given application. The second case represents the current state of the art. E.g. ECAC has released a common test methodology in 2014 that is used to evaluate the performance of particle trace detection systems for the use within security checkpoint at the airports. It is worthwhile to mention that a system has only a chance to enter the market if it has passed this certification test. Beside the aviation sector with its checkpoint security scenario there are plenty of application scenarios each with slight differences that would result to quite a large number of tailored certification test methods. A manufacturer would have to pay each test enabling to enter the market. The innovative concept within EVADEX is to gather the information for a large number of application scenarios, identify the common similarities and create a generic baseline for a comprehensive evaluation test methodology. In case a system passes this evaluation the output would be that it is eligible or unqualified for a number of various scenarios. The scenarios have been determined by the Bundespolizei (e.g. security within mass transportation (Bundesbahn), secure critical infrastructure etc.) as well as in interviews with private security providers (Securitas, Kötter).

2.3 From manual sample preparation to automation

The relevance of a certification evaluation methodology as entry criteria for the security market has been sufficiently explained. Hence, the result needs a robust and reliable statistic leading in most of the cases to a high number of repetitions of explosive trace samples. These samples imply a high reproducibility in the range of nanogramm contaminations with almost no error margins. The quality assurance process has to check the parameter that the amount that has been applied on a surface is the exact mass and to ensure after the transfer via swab has taken place if still residues are left on the sample.

2.3.1 Dry transfer vs. liquid transfer

It is nearly impossible to use a dry transfer method to apply e.g. 50 ng of a crystalline substance onto a glass slide. There are impact parameters such as electrostatic charge, no balance available to measure the weight difference as well as a broad distribution of the particle size etc. With a simple macroscopic experiment using a silicon finger simulating finger prints TNT (mean particle diameter 85µm) has been transferred onto aluminium foil (figure 2).



[mg]	FP 1	FP 2	FP 3	FP 4	FP 5	FP 6	FP 7	FP 8	FP 9	FP10
Exp 1	1,84	0,79	0,21	0,26	0,14	0,39	0,01	0,01	0,04	0,17
Exp 2	3,52	0,62	0,59	0,1	0,23	0,18	0,15	0,13	0,01	0,01
Exp 3	3,14	0,44	0,3	0,24	0,26	0,15	0,05	0,34	0,18	0,15
Exp 4	2,85	0,97	0,63	0,26	0,07	0,19	0,27	0,18	0,19	0,08
Exp 5	2,4	1,66	0,59	0,28	0,39	0,25	0,17	0,08	0,08	0,1
Exp 6	2,59	0,71	0,24	0,01	0,4	0,1	0,2	0,09	0,28	0,19
Av.	2,72	0,86	0,43	0,19	0,25	0,21	0,14	0,14	0,13	0,12
Var	0,288	0,152	0,032	0,010	0,015	0,009	0,008	0,011	0,009	0,004

Figure 2: TNT Fingerprints with 10 repetitions

Even after the tenth finger print the resulting weight difference is in the range of 4µg while the system can measure down to 1ng for some common military explosives. The only manual transfer method that imply both a defined small scale and a low error margin is the so called Bytac transfer method. This method simply makes advantage of a standard solution which can be prepared with high precision and subsequently applied to a transfer surface by using a high precision pipette such as the eVol (1 µl +/- 2.7%) – figure 3. The transfer surface is actually the Bytac foil containing a compound of Teflon and polyethylene. The applied solution will be dried under standard environmental conditions and then transferred on the destination surface. This prepared sample is then ready for being swabbed and tested with the explosive detection system.

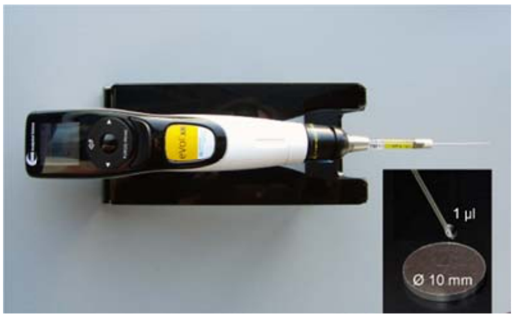


Fig. 3: eVol pipette

The investigation of the recovery rate is strongly depending on the surface material as well as the explosive substance itself (figure 4).

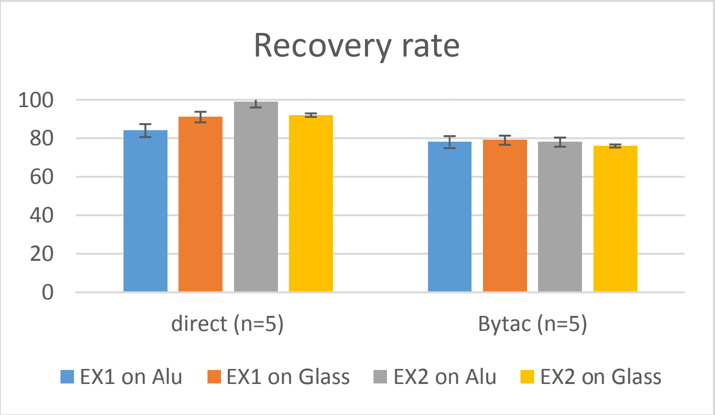
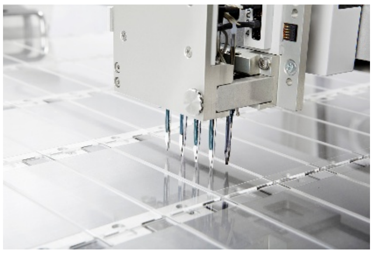


Fig. 4: Recovery rate of explosive (compared direct deposition vs. Bytac transfer)

The conclusion of this manual transfer method is that even the recovery rate is reproducible low at 78% the resulting error margin is acceptable and robust.

GeSiM has modified an automatic liquid dispenser that is able to replicate the manual Bytac process for a variety of organic solvents (figure 5).



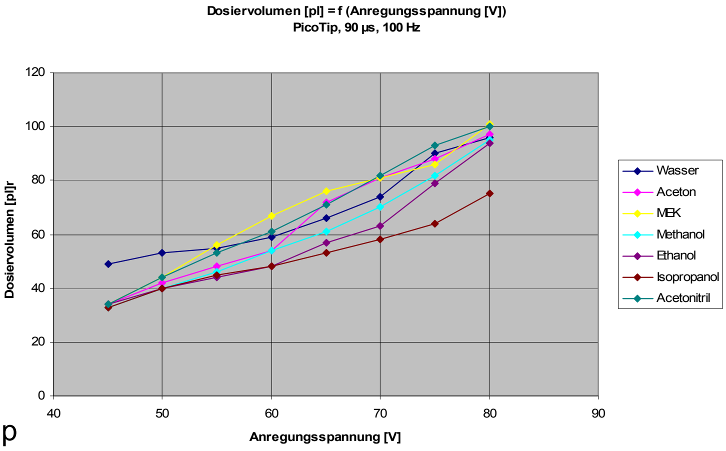


Fig. 5: Nano-Plotter 2.1 with pico-tip

In the second half of the project the nano-plotter will be transferred to ICT for a direct investigation using real explosives.

Using in principle the same platform GeSiM has also modified the tip into a direct solid dispenser. At this stage only some very promising preliminary results can be presented in figure 6. The principle is to aspirate particles eliminate the exceeding particles and apply the monolayer of particles onto the target surface.

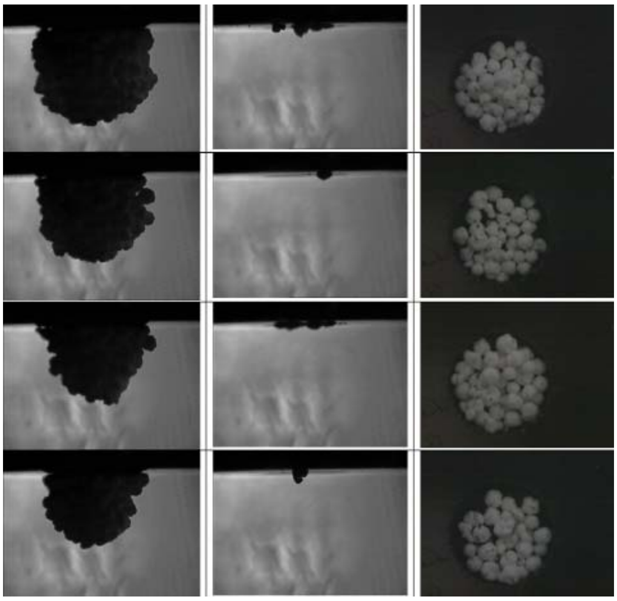


Fig. 6: Aspiration and deposition procedure with mono modal test particle (30 µm (span 90/10 - 0,18))

2.4 Gas generator for explosive substances

One of the most challenging task at the moment seems to be creating a gas generator for most of the military and civil explosives. As shown in figure 7 most of the explosives have a very low vapour pressure. Realistic vapour concentrations under given environmental condition to be detected by the explosive vapour detection system are in the range of 0.1 ppq (10^-16; SEDET explosive vapour detection system).

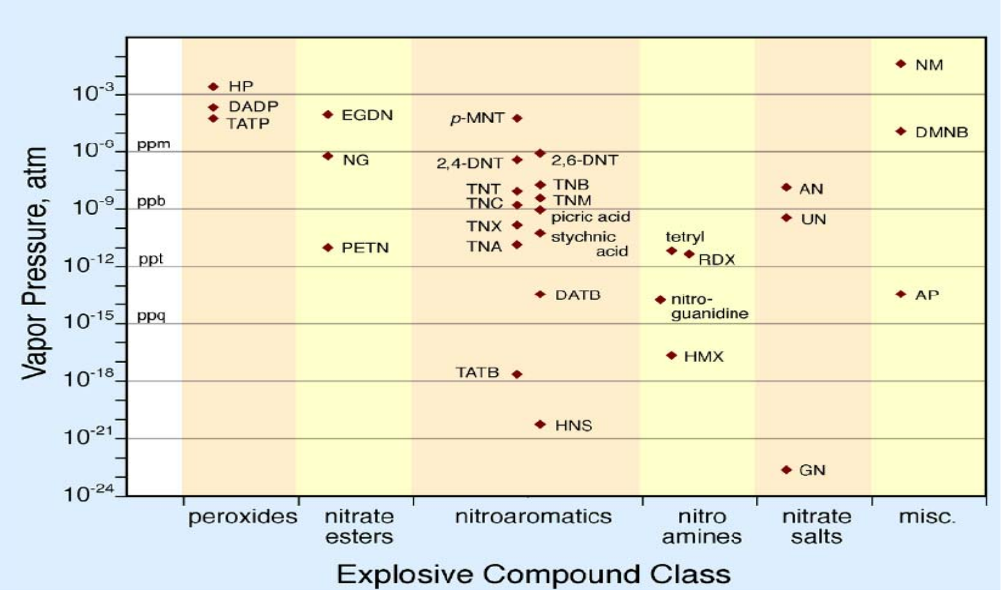


Fig. 7: Vapour pressure of common explosives

IAS is currently developing a gas generator with two different approaches:

a. In synergy with GeSiM incorporating the pico dispenser into their gas generator
b. With a promising pulsed gas generator eliminating the “dead volume” error

Fraunhofer ICT in parallel is working on the basic understanding of all possible effects dealing with explosive vapour detection that can depending on the concentration either be direct meaning a given equilibrium pressure with a net amount of explosive above the detection limit is directly analysed or the other principle putting an enrichment step in front of the detection. E.g. a high volume sampler that collects the particle containing in a large amount of air onto a filter with subsequently releases the joined amount within a thermodesorber into a detection system. All work is currently done using a sample environment (150 L tank, figure 8) with several inlets combined to a GC/MS and investigation the diffusion of various explosives.

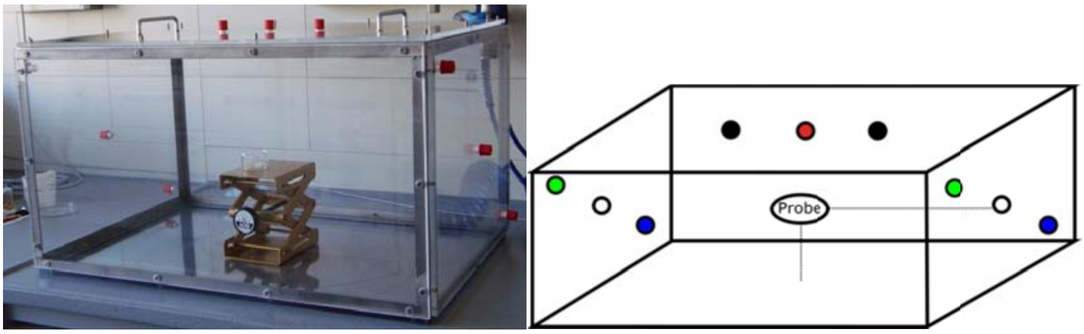


Fig. 8: Test tank (150L) and schematic structure for diffusion trials

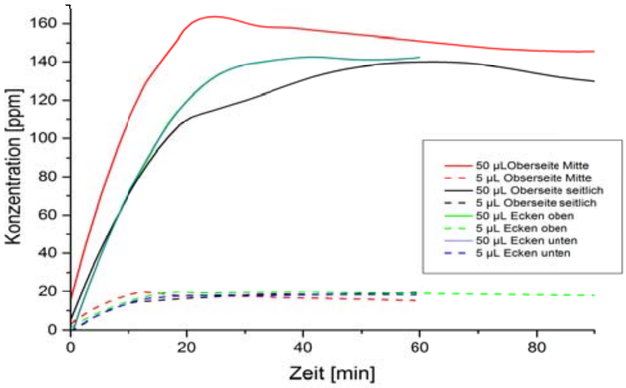


Fig. 9: Diffusion times of trial substances.

The resulting model will be used and transferred to the field environment such as LD3 container etc. Additional parameters that will be tremendously important when creating a test methodology for "pre-concentration" units are the whole convection, ad/absorption processes, diffusion, equilibrium time, turbulences etc. It is already obvious that this won't be possible within the given project time.

2.5 Legal and sociological aspects of security measures

The legal aspects are limited to national German regulation based on the nature as national research project. At this point of time within the project only a small essay can be presented. E.g. aspects related to the police authorisation baselines given in the § 43 Abs. 1 Nr. 2 BPolG states that at least that the circumstances must be reasonable and limited to concrete person to allow a security measure not just based on a common suspicion. Other aspects are also highlighted who is liable for compensating disadvantaged as a matter of a security measure.

The focus of the sociological research which is a combined study of empirical, literature and interview data is set on the acceptance per se. It includes several aspects and views from both the security personnel as well as the persons that undergo a certain security measure. Figure 10 and 11 are trying to illustrate the complexity of the task.

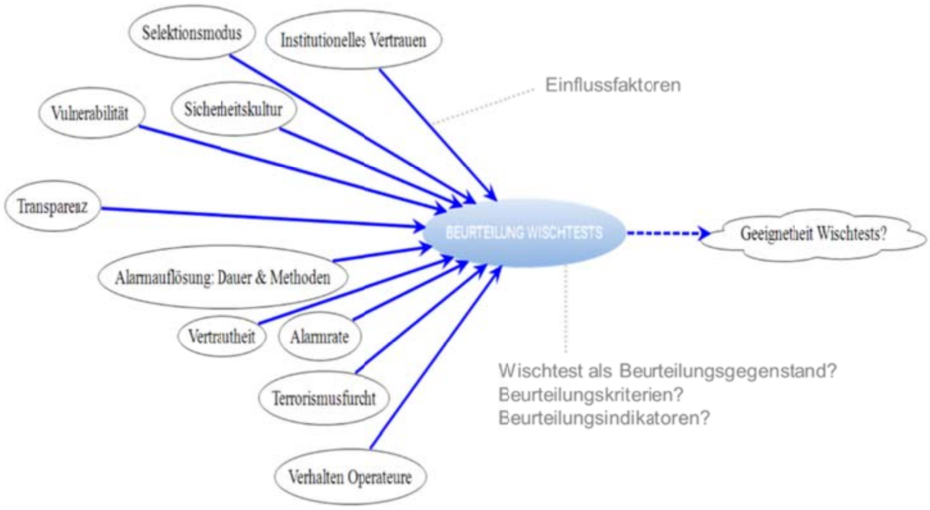


Fig. 10: Acceptance impact factors of a person undergoing a security measure

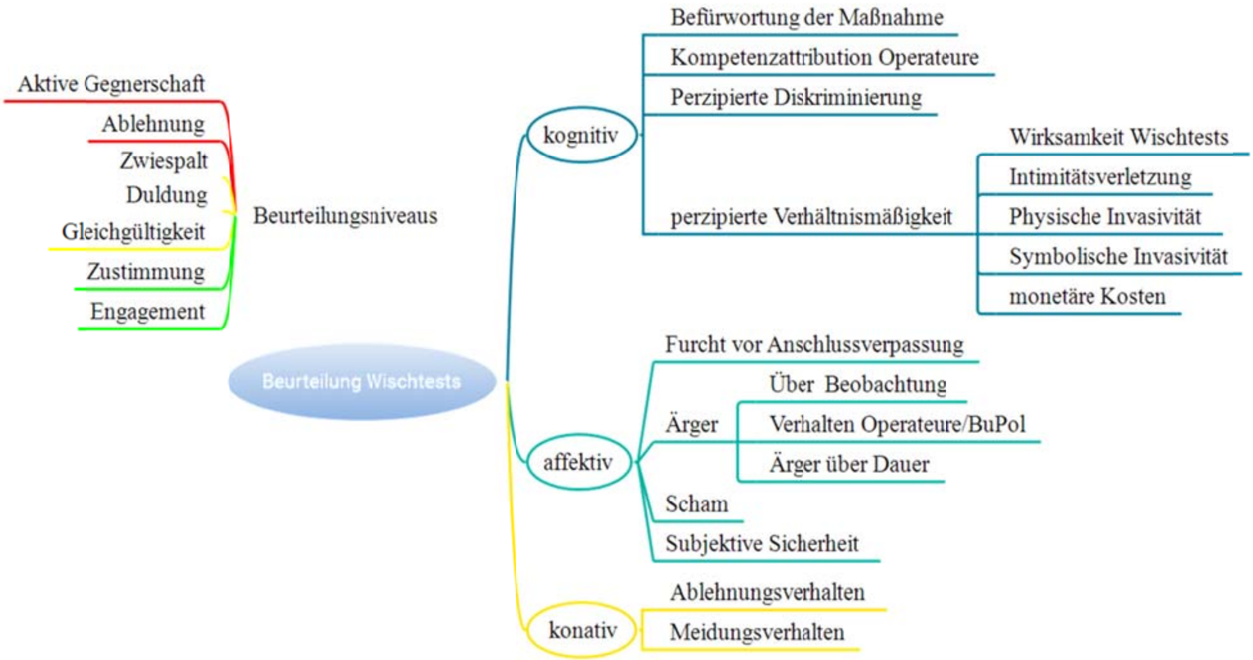


Fig. 11: Systematic categorisation of the subjective experience made within a security measure

3 CONCLUSIONS

The summary of the comprehensive approach towards a possible standardised evaluation methodology for explosive trace detection systems has highlighted the scientific, technical problems as well as the sociological and legal significance. The development phase has been accomplished, basic results such as defining the framework of threat/interferent substances, highly likely surfaces, application scenarios have been done. The concept for initiating the standardisation activities under the guidelines of DIN are on its way. The challenges for the second half of the project on the technical side will be further investigations to provide highly modified explosive material that enables the automatic dry transfer of masses down to nanogramm range as well as further improvement in understanding and assign all impact factor on the field of vapour detection. Furthermore, the so called sniffer dogs will be investigated but it is important to mention already at this stage that there won't be any direct compare between canine and technological performance.

THE NEED FOR SENSORS AND EARLY WARNING DURING ACCIDENTS WITH HAZARDOUS MATERIALS

Inge Trijssenaar[1] and Ingrid Raben[2]

[1] *Inge.Trijssenaar@tno.nl and* [2] *Ingrid.Raben@tno.nl*
Netherlands organization for applied scientific research (TNO),
Princetonlaan 6, 3584 CB Utrecht (the Netherlands)

Abstract

Human behaviour and protective measures during a large-scale chemical release can make the difference between life and death.

In the Netherlands it generally takes 45 minutes to 2 hours before a generic alarm signal is given to citizens due to the need to send out fire brigade measurement teams and the decision making procedures applied. This time duration could significantly be reduced by making use of innovative technologies such as sensors.

This paper describes the research on self-rescue and protective measures showing the need for early warning combined with a concrete action perspective in order to protect citizens from injury. A possible option to enable early warning is the use of sensor systems in combination with real-time modelling of chemical release, dispersion and real-time modelling of the best measure for self-rescue and protection of citizens.

Keywords: early warning, self-rescue, protective measures, e-nose, chemical release, fire, explosion, toxic release.

1 INTRODUCTION

The Self Rescue Model (SeReMo) has been developed to estimate the consequences of human behaviour and protective measures for hazardous material scenarios [7, 10,11]. Scenarios included in SeReMo are fires, explosions and toxic releases. Although developed for accidental hazardous material (haz mat) scenarios, such events may also be caused deliberately. SeReMo consists of dynamic injury models and a set of safety measure models. SeReMo includes human behaviour intended to rescue oneself, Fig. 1 shows the five main strategies for self-rescue behaviour [3]: (1) shelter, (2) take shelter, (3) Flee, (4) Evacuate building and flee (5) Hide behind obstacle or building.

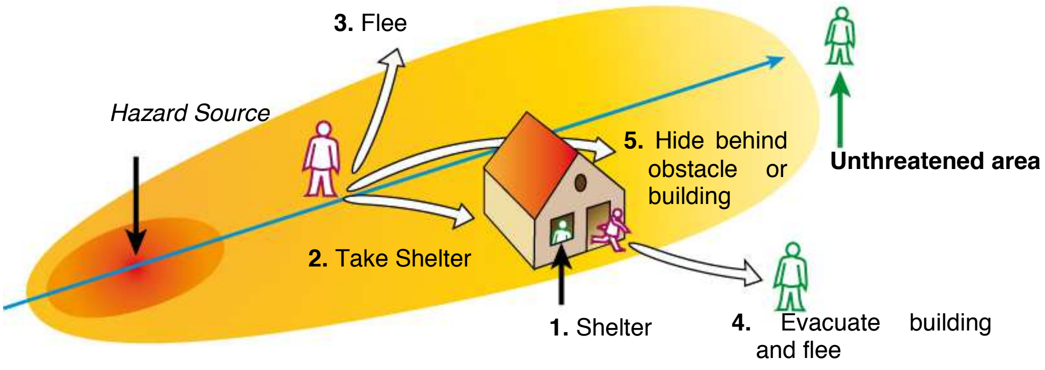

3. Flee
Hazard Source
5. Hide behind obstacle or building
Unthreatened area
2. Take Shelter
1. Shelter
4. Evacuate building and flee

Figure 1: Five main strategies for self-rescue behaviour

Each of the strategies can be complemented with additional protective measures. The strategy ‘shelter’ can for instance be complemented with closing windows and doors, shutdown of the ventilation system, and vertical evacuation inside a building. The strategy ‘flee’ can be complemented by a crosswind or downwind direction and by using a wet cloth as breathing protection. For several years SeReMo has been applied in cooperation with (a.o.) Dutch emergency response (Safety Regions). The effect of self-rescue behaviour and protective measures on lethal and sub-lethal injuries are illustrated in several projects for accidental haz mat releases [1, 5, 6, 9, 13].

The general objective for the application of SeReMo is to determine a sensible self-rescue strategy and effective additional safety measures for specified haz mat scenarios. The emergency response services include the project results in their preparation for possible scenarios [14,15].

2 EFFECT OF SAFETY MEASURES

Fig. 2 shows how SeReMo is applied to determine the effect of safety measures (self-rescue and protective measures) within a haz mat scenario. SeReMo integrates the safety measures with physical effect models for toxic dose, concentrations of toxic or flammable compounds, heat radiation and overpressures of the scenarios. The physical effects are influenced by e.g. release rate, weather conditions. The Yellow Book [12] contains physical effect models, which have been implemented in the software EFFECTS. SeReMo includes models for safety measures as well as injury models [7] for incapacitation or inhibited walking velocity in EFFECTS. A person that flees will be ‘tracked’ until he reaches a shelter or safe location. SeReMo enables to dynamically determine the effects of safety measures.

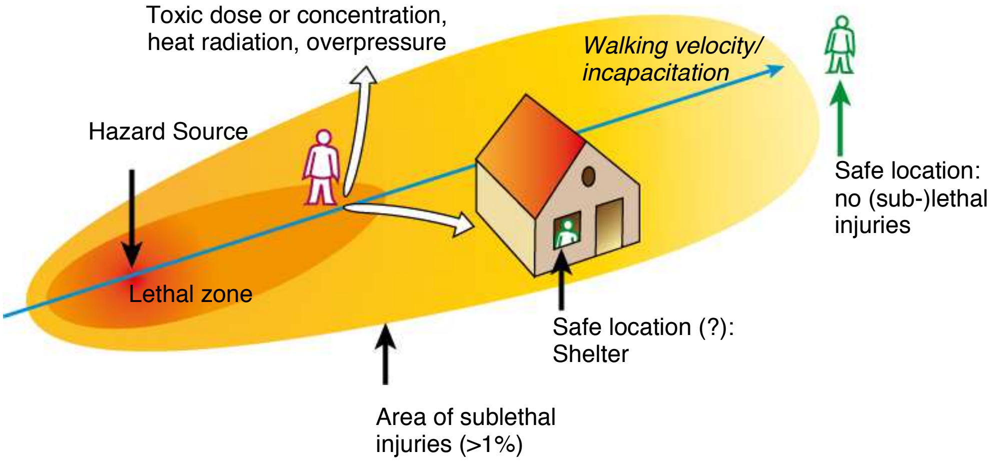

Toxic dose or concentration, heat radiation, overpressure
Walking velocity/ incapacitation
Hazard Source
Safe location: no (sub-)lethal injuries
Lethal zone
Safe location (?): Shelter
Area of sublethal injuries (>1%)

Figure 2. Self-Rescue Model for human behaviour and protective measures

The Required Time is the time needed for a person to reach a safe location, from its starting position and includes the time for detection of the scenario, the time to raise alarm, pre-movement time and the time for self-rescue [8]. The distribution of the Required Time is analogue to the time distribution used for the Required Safe Egress Time (RSET) which is well-known in fire safety engineering [4]. Where RSET involves egress only, the actions for haz mat scenarios include all actions related to the self-rescue strategies shown in Fig.1. The value that is assigned for the preparation time required for detection, alarm and pre-movement depends on the detectability and perception of the scenario involved. A scenario with clear alarming signals, such as noise, odour and visible effects (fire, cloud) will result in a larger sense of urgency compared to a scenario which is not easily observed. The self-rescue time also depends on the scenario since the walking velocity can be inhibited in toxic scenarios or encouraged in fire scenarios.

2.1 Flash fire scenarios

2.1.1 What happens in a flash fire scenario?

An incident with flammable gas, e.g. LPG, may be caused by a hole in the tank by which an amount of gas is released during a certain period. Another conceivable scenario is failure of the tank by which the entire contents is released instantaneously. In both cases, it is possible that the gas is ignited immediately or only after some time (delayed ignition). In case of delayed ignition a gas cloud is formed and, when ignited, can cause a flash fire or a vapour cloud explosion. In case of a flash fire, injuries among persons present in the vicinity may be caused by direct flame contact, as well as secondary fires in buildings.

The effect of the self-rescue measures not only depends on the Required Time to apply the self-rescue measures as well as the characteristics of the scenario. An important parameter for a flash fire is the ignition time, which in its turn depends on the population density or 'ignition source density' of the area. The calculation method will be described in more detail in future publications.

2.1.2 Self-rescue measures

The following self-rescue measures are selected in cooperation with the emergency response organisation [6]: For a person that is initially inside: (a) Do nothing, (b) Close windows and doors, shutdown ventilation system, (c) Open windows and doors widely. For a person that is initially outside: (d) Do nothing, (e) Flee alongwind, (f) Flee crosswind.

2.1.3 Results

Fig. 3 depicts the total number of victims for various self-rescue measures in an urban area [6]. The left bars show the results for a person which is initially inside. The right bars show the results for a person initially outside. For each set of results (indoors vs outdoor) the left column represents the situation where no action is taken. It can be concluded from the figure that the best measure is to flee in crosswind direction (0 victims when fleeing in crosswind direction). Residing outdoors while doing nothing is the worst option (34 victims).

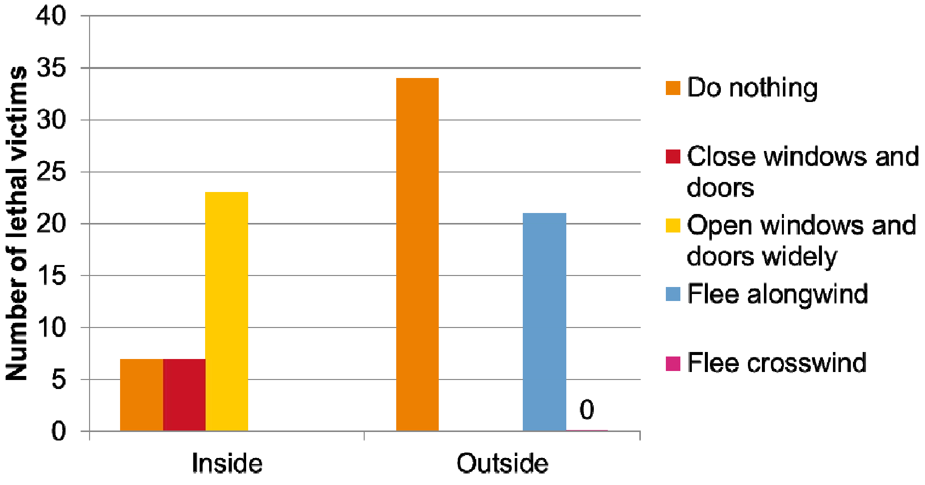


Figure 3. Number of victims for various self-rescue measures in urban area [6]

Furthermore, Fig. 3 shows that residing indoors while opening the windows and doors results in more victims (23 fatalities) compared to doing nothing. Closing of doors and windows has no beneficial effect on the number of victims (7 victims for residing indoors and doing nothing or closing the doors and windows).

The flee direction is of major importance when residing outdoors. If it is unclear where the wind comes from, it is advisable to go indoors, as the number of victims indoors is much lower compared to fleeing in the wrong direction (7 resp. 21 victims).

2.2 Toxic cloud scenarios

2.2.1 What happens in a toxic cloud scenario?

Toxic clouds can occur after the releases of a toxic gas or liquid. Well-known examples of toxic gases are ammonia and chlorine. A release of a toxic gas will result in the dispersion of a toxic cloud and may cause injury to persons due to exposure to the toxic gas. Examples of toxic liquids are acrylonitrile and acrolein. In case of toxic liquids a pool is formed. After evaporation a toxic cloud is formed. Exposure to this gas cloud, depending on exposure time and concentration, may cause lethal injury. For both gas and liquid scenarios, time elapses between the start of the release and the occurrence of injuries. Atmospheric conditions play an important role in the severity of the consequences.

2.2.2 Self-rescue measures

Toxic cloud scenarios are investigated in [5] and [13]. Results of [5] for a toxic liquid release of acrylonitrile are shown below. The following self-rescue measures are selected in cooperation with the emergency response organisation [5]: for a person that is initially inside: (a) do nothing, (b) Close windows and doors, shutdown ventilation system. For a person that is initially outside: (a) Do nothing, (d) Flee alongwind. The research [5] also includes other self-rescue measures. In this paper the results are shown for preparation time of 100 seconds, 15 minutes, 30 minutes.

2.2.3 Results

Fig. 4 shows the results for the selected self-rescue measures and preparation times for an acrylonitrile scenario [5].

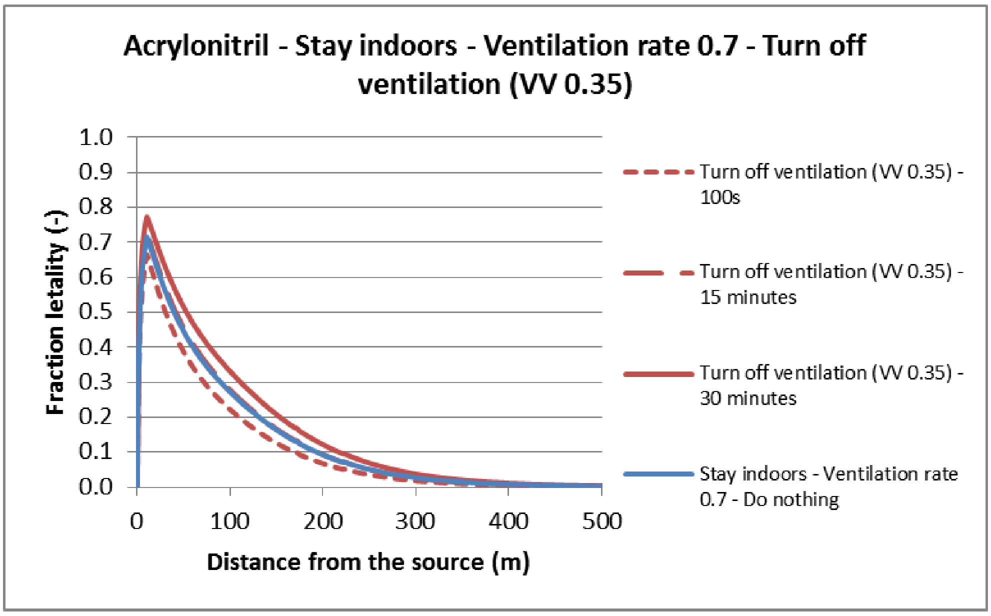


Figure 4. Lethality fraction vs. distance for various self-rescue measures and preparation times

Fig. 4 shows that turning off ventilation and closing of windows and doors only results in a positive effect (lower lethality) if this is done quickly. For this specific scenario closure of windows and doors and shutting down the ventilation system after 15 minutes can even result in no or a negative effect compared to doing nothing. Taking the measure after 15 minutes can trap the hazardous material in the building, while the outside atmosphere already contains fresh air without hazardous materials.

In Fig. 5 the results for fleeing along wind are presented [5]. The curves for 15 and 30 minutes (partially) overlap the stay outdoors- do nothing curve. The figure clearly shows that fleeing within a short period of time after the incident (in this case within 100 seconds) has a positive effect on the level of lethality. Especially beyond approximately 25 meter the lethality is strongly reduced, even to reach 0% lethality beyond 50 meter. When more time is needed to start fleeing (15 minutes) a positive effect is only observed at larger distance from the incident (> 220 meter).

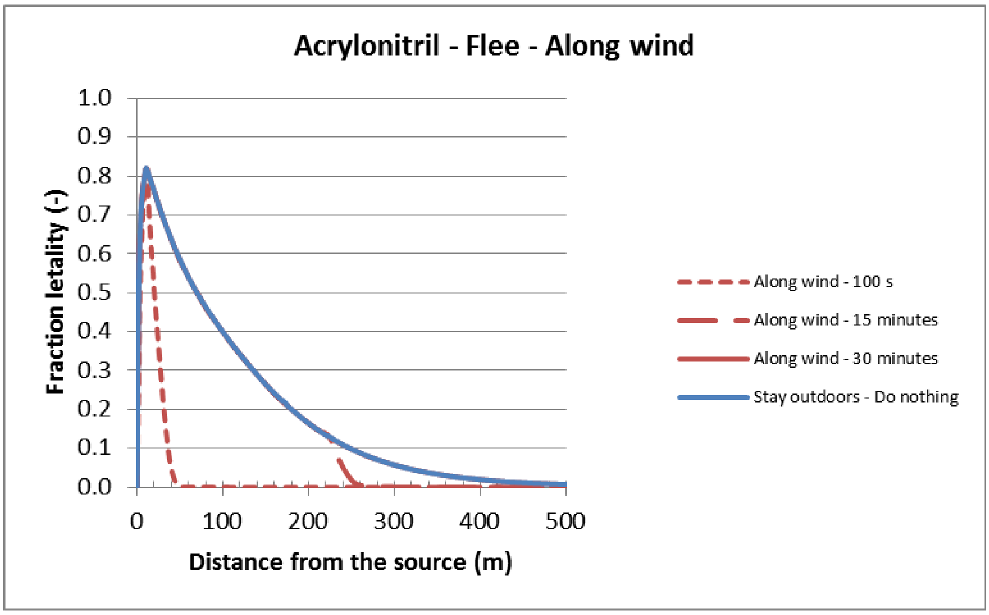


Figure 5. Fraction of lethality versus distance for various self-rescue measures and preparation times in a toxic cloud

2.3 Boiling Liquid Expanding Vapour Explosion (BLEVE)

2.3.1 What happens in a BLEVE scenario?

In the event of a liquefied flammable gas, such as LPG, an instantaneous release is followed by an instantaneous evaporation and a physical explosion, called Boiling Liquid Expanding Vapour Explosion (BLEVE), often the gas cloud is ignited resulting in a fireball. In this paper a so-called ‘warm’ BLEVE scenario of a tank car is considered, results are reported in more detail in [6]. A warm BLEVE is a BLEVE arising from a fire near the tank with flammable liquefied gas. The heat radiation of the fire heats up the contents of the (liquefied) gas tanker and the pressure in the gas tanker rises. When the wall temperature at the top (gas side) reaches above 500°C, the steel tank wall will weaken and collapse. Injuries among persons present in the vicinity may be caused by direct flame contact or by heat radiation at a larger distance from the fire.

2.3.2 Self-rescue measures

The following self-rescue measures are selected in cooperation with the emergency response organisation [6]: For a person that is initially inside: (a) Do nothing, (b) Open windows and doors widely, (c) evacuate the building and flee – dwelling, (d) evacuate the building and flee – office. For a person that is initially outside: (a) Do nothing, (b) flee. For the Required Time a probability density function is used, based on estimations for the various time elements mentioned at the start of the chapter. Also for the time available to rescue oneself an estimation is made for the probability density function.

2.3.3 Results

Fig. 6 shows the percentage of lethal victims for various self-rescue measures for persons within 90 meters from the incident [6]. For persons initially inside the best self-rescue measure is to evacuate and flee (for a dwelling and an office this results in 7% and 4% respectively). Opening windows and doors widely results in the largest probability of injury (100%). Stay inside and do nothing results in a probability of 10%. For persons initially outside, doing nothing results in 100% lethal injury, while the lethal injury can be reduced to 12% by fleeing.

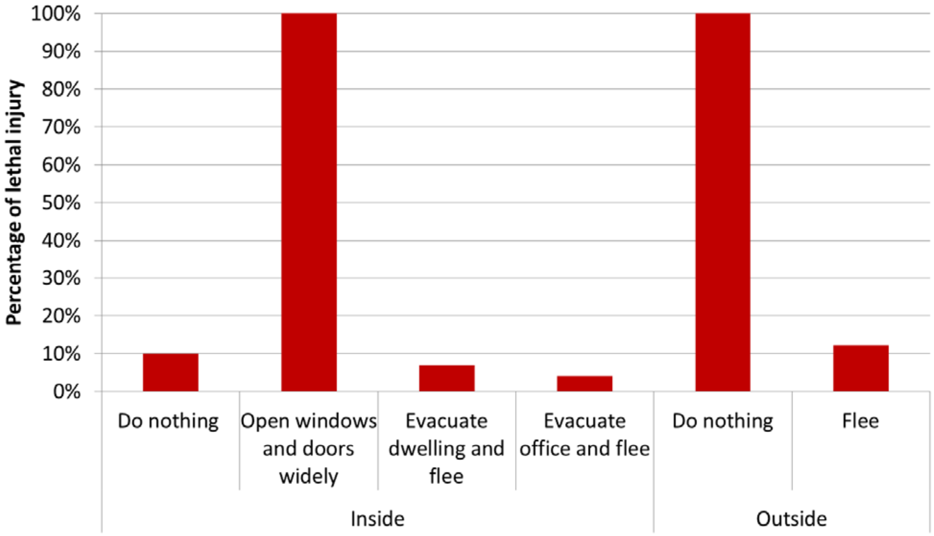


Figure 6. Percentage of lethal victims for various self-rescue measures for persons within 90 meters from the incident [6].

3 THE NEED FOR SENSORS AND EARLY WARNING

3.1 Alarm techniques

Research by Raben [5] showed that it generally takes 45 minutes to 2 hours before a generic alarm signal is given to citizens. This time duration could significantly be reduced by making use of innovative technologies such as sensors. Generally applied alarm techniques are sirens or cell broadcasting (NL-alert in the Netherlands).

3.2 Emergency response procedures and real incidents

During a real haz mat incident, the emergency response requires time for image forming, judgement and decision-making. The total required time depends on (1) the time required for gathering information; (2) quality and reliability of the information provided; (3) emergency response procedures followed.

In general, the first emergency responders arriving on the incident location are non-specialists [2]. Depending on the regional procedures, the specialist (haz mat advisor, AGS) can arrive at the incident location within either 30 minutes or 1 hour. In urgent cases where citizens need to be informed and alarmed immediately, there is no time to wait until the haz mat specialist is present or even until a measuring team has collected data. In order to quickly respond to the haz mat incident, the emergency response services need information that is easy to interpret by a non–specialist in cooperation with a specialist, the latter not being present at the incident location. Sensors can provide the specialist with information to judge the situation at distance and therewith reduce the time required for gathering information as well as the quality and reliability of the information provided.

3.3 Sensors in chemical industry

The use of sensor systems in areas with chemical industry increases rapidly. Apart from on-site detection systems, e-nose networks are available in e.g. the port of Rotterdam. This development gives opportunities for enabling early warning of citizens.

The ideal sensor enables to quickly recognize every compound released and any incident developing, can quantify the concentration, as well as the source location. The ideal sensor does not exist.

There are general sensors, such as e-noses, which are able to recognize a broad spectrum of compounds. Their sensitivity varies between chemical compounds however quantification of the order of magnitude of the concentration is possible. On the other hand very specific sensors are available, such as sensors for ammonia or carbon monoxide. These are able to recognize and sometimes quantify the concentration of a single compound. Analytic instruments based on gas chromatography are able to quantitatively measure a broad spectrum of compounds, however these instruments are too large and expensive to put it on ‘every corner of the street’ and therefore are only applied by the measuring teams in case of an incident.

A sensor network could be used to follow a release in time and place for various wind directions and conditions in order to (roughly) determine the source location. Dispersion models are required in order to estimate the source strength. To estimate the source location one needs either these models and/or information about possible sources. The influence of obstacles, such as buildings, should not be underestimated (e.g. COSTaction ES1006). This issue could perhaps be solved by using more sophisticated models that include the influence of built environment on air flow. The sensitivity of the sensor network is another important characteristic. This depends on the sensitivity of the sensors as well as the sensor density of the network. The sensor network should be designed in such a way that major hazards can be (easily) detected, while the summer barbeque or a normal hearth fire can be held undisturbed. This might be a challenge, but hopes are on that it will be more easy to detect major hazards, compared to relatively small incidents. The strategy is to start with detecting the worst case scenarios and - when experience increases - also smaller incidents can be judged and detected.

4 CONCLUSIONS

A recurring conclusion is that the time available for citizens to take effective actions is limited, generally less than 15 minutes, and for various haz mat scenarios even less than several minutes. In addition, the research shows that lives can be saved by the combination of early warning in combination with self-rescue behaviour. In order to enable early warning, a combination is recommended of sensor systems and (real-time) modelling of dispersion as well as safety measures.

REFERENCES

[1] Bekker-Grob, E.W. de, Bergstra, A.D., Bliemer, M.C.J., Trijssenaar-Buhre, I.J.M., Burdorf, A. (2015).*Protective Behaviour of Citizens to Transport Accidents Involving Hazardous Materials:A Discrete Choice Experiment Applied to Populated Areas nearby Waterways.* PLOS ONE, 10.1371/journal.pone.0142507

[2] Leidraad voor ongevalsbestrijding gevaarlijke stoffen (2001).

[3] Oberijé, N. (2006).*Beoordelings- en selectiemethodiek technische en organisatorische maatregelen ter ondersteuning van zelfredzaamheid.* Tijdschrift voor Veiligheid, 2006 (5) 1, p.39-66.

[4] Purser. (2003). *Data benefits.* Fire Engineers Journal & Fire Protection. p. 21-24.

[5] Raben I., Trijssenaar I., Sterkenburg R., Thijssen C. (2015). *Bevorderen zelfredzaamheid spoorzone 'Roosendaal-Halderberge-Moerdijk*, TNO-rapport R11622.

[6] Trijssenaar I. (2016). *Methodieken voor bepalen handelingsperspectieven en schade bij ongevallen met gevaarlijke stoffen, Methodiekontwikkeling ten behoeve van het Scenarioboek Externe Veiligheid*, to be published.

[7] Trijssenaar, I.J.M., van der Horst, M.J., Simons M. & Sterkenburg, R.P. (2013). *Self Rescue Model-SeReMo-a model to determine the effects of human behaviour and safety measures on the consequences of a hazardous material release-development of the new triage injury model and self-rescue for fire and explosion accidents.* Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds), London, ISBN 978-1-138-00123-7, pp 483-489.

[8] Trijssenaar, I. , C. Thijssen, R. Sterkenburg, I. Raben, M. Kobes (2013), *Kwantificering van de effectiviteit van maatregelen voor ongevallen met gevaarlijke stoffen, Fase 2*, TNO-rapport R11365.

[9] Rosmuller N.,Trijssenaar I.,Reinders J.,Blokker P.(2012).*Quantification of the number of injured people due to hazardous material accidents*. Int.J.Emergency Management,Vol. 8,No. 4, p. 308-331.

[10] Trijssenaar, I.J.M. & Sterkenburg R.P. (2009). *Self-rescue in quantitative risk-analysis, modeling and case studies for accidental toxic releases*. Proceedings of the European Safety and Reliability Conference 2009, ESREL 2009, Reliability, Risk and Safety: Theory and Applications, pp. Briš, Guedes Soares & Martorell (eds), ISBN 978-0-415-55509-8, pp 1163 – 1169.

[11] Trijssenaar, I.J.M. & Raben, I.M.E. & Wiersma, T.& Wijnant, S.I. (2007). *Self-rescue in quantitative risk-analysis*. Proceedings of the European Safety and Reliability Conference 2007, ESREL 2007 - Risk, Reliability and Societal Safety, 2, pp. 1541-1546.

[12] Yellow Book. (2005). *Methods for the calculation of physical effects – due to releases of hazardous materials (liquids and gases)*, CPR14E, PGS2.

[13] ZonMW. (2013). I. Trijssenaar, I. Raben, I. Heidebrink, *Kijk uit op de Westerschelde - slachtofferberekeningen*, TNO-rapport R12066.

[14] *Scenarioboek Externe Veiligheid*. (2015). www.scenarioboekev.nl

[15] *CBIS* (2015), CBIS website and E-learning module, http://www.cbismoerdijk.nl/

TRACE DETECTION OF EXPLOSIVES WITH HANDHELD RAMAN USING SPUTTERED SERS SUBSTRATES

Anne-Marie Dowgiallo* and Derek Guenther

*anne-marie.dowgiallo@oceanoptics.com
Ocean Optics, Inc., 830 Douglas Ave., Dunedin, FL 34698, USA

Abstract

Detection of trace levels of explosives using portable devices is of crucial interest for national security. Surface enhanced Raman spectroscopy (SERS) is a unique tool that offers high sensitivity, high specificity, fast response time, and low limits of detection for various explosives such as TNT, RDX, and PETN. Newly developed SERS substrates increase the Raman signal of explosives by orders of magnitude compared to today's state-of-the-art SERS substrates. These substrates lower the detection limit for common explosives with a pocket-size, battery-powered Raman instrument to tens of picograms using safe laser power levels (20 mW at 638 nm) with a 10-second measurement time. Additional experiments are underway to test the specificity and sensitivity of these SERS substrates for chemical warfare agents.

Keywords: SERS, Raman, explosives, detection, sensitivity.

1 INTRODUCTION

Ocean Optics offers a range of Raman detection systems in both modular and handheld form factors, and in the last two years we have also begun offering surface enhanced Raman substrates to couple with these systems for trace level detection of analytes.

1.1 Paper-based substrates

The current Ocean Optics market-available SERS substrates utilize quartz paper embedded with a proprietary gold or silver nanoparticle ink, which when cured leaves metallic nanoparticles dispersed throughout the fiber structure of the quartz matrix (Figure 1) based on the method by Hoppmann *et al.*[1]

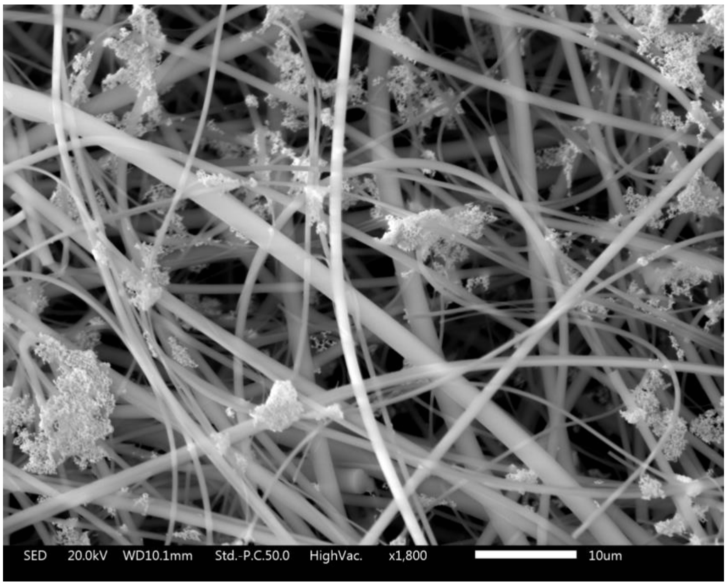


Figure 1: Scanning Electron Micoscopy (SEM) image of paper-based Surface Enhanced Raman Spectroscopy (SERS) substrates

This material is then affixed to a glass slide, which is a form factor that can be easily used with modular and portable Raman systems (Figures 2).

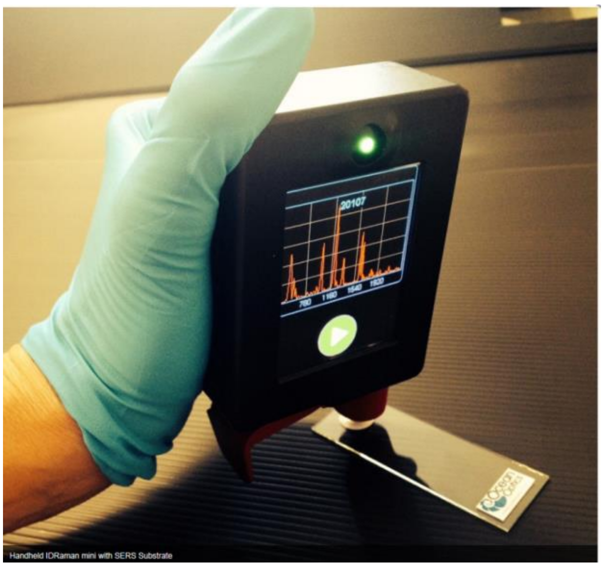


Figure 2: Handheld SERS measurement

1.2 Nanosponge on glass substrate

While the gold or silver nanoparticle paper-based technology is effective for the detection of fuel markers, anti-fungal dyes, food contaminants, and other important species, they do not offer enough enhancements to detect trace levels of explosives and chemical weapons. As security becomes more and more of a concern across the globe, the ability to detect such species at trace levels is crucial to averting deadly attacks. Ocean Optics has developed a new technology based on plasma-phase deposition of a gold-silver alloy onto a unique glass surface. By optimizing the working gas pressure in the millitorr regime, we are able to deposit an alloy with a nanosponge structure (Figure 3). This nanoporous material is able to bind with Raman analytes and has shown exceptional performance with species that are typically near impossible to detect. This report will show the ability of this new technology to detect trace levels of chemicals that play a core role in today's defense and security efforts.

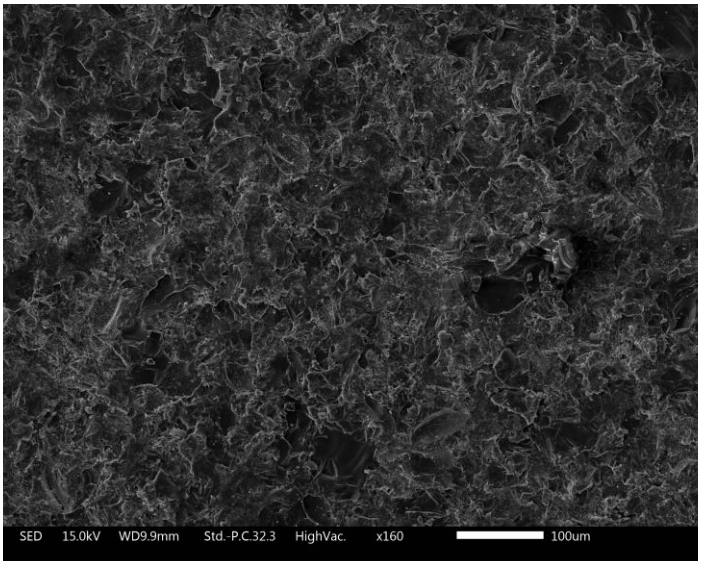


Figure 3: SEM image of nanosponge alloy

2 MATERIALS AND METHODS

Roughened borosilicate glass slides were purchased from Sigma-Aldrich and were diced to ~4 x 4 mm squares. These substrates were cleaned prior to metal deposition by sonicating in separate baths of acetone and isopropyl alcohol. Thin films were deposited using a CRC sputter coater with 300 W DC power supply using low pressures ≥6 mtorr. A thin film of chromium (~5 nm) was first deposited, followed by a ~200 nm film of Au-Ag alloy. Solutions of PETN and RDX were prepared in acetone with concentrations of 100 and 1000 ppm. The same concentrations were made for solutions of ammonium nitrate in water. Then, 10 uL of each solution was deposited on several different nanosponge substrates. Raman experiments were performed using a Snowy Range Sierra Raman reader for use with a 638 nm laser. The laser power was typically 22 mW with 10 seconds integration time. The spot size of the focused laser was approximately 25 µm. A typical Raman measurement involved collecting the spectrum of the blank substrate first, subtracting this data out to get a flat baseline, and then measuring the substrate after the analyte of interest had been added and dried in air. This background subtraction method ensures that we only see peaks from analyte of interest. The amount of material detected was calculated based on the spot size of the laser and area of the substrate. For example, 10 µL of 100 ppm analyte deposited on a 4.35 x 4.4 mm substrate using a 25 µm laser spot corresponds to ~25 pg of analyte detected in the laser beam area.

3 RESULTS

3.1 Ammonium Nitrate

Figure 4 shows the surface enhanced Raman spectrum of ammonium nitrate at two concentration levels, demonstrating that the technology is able to give a detectable signal at concentrations that differ even by an order of magnitude.

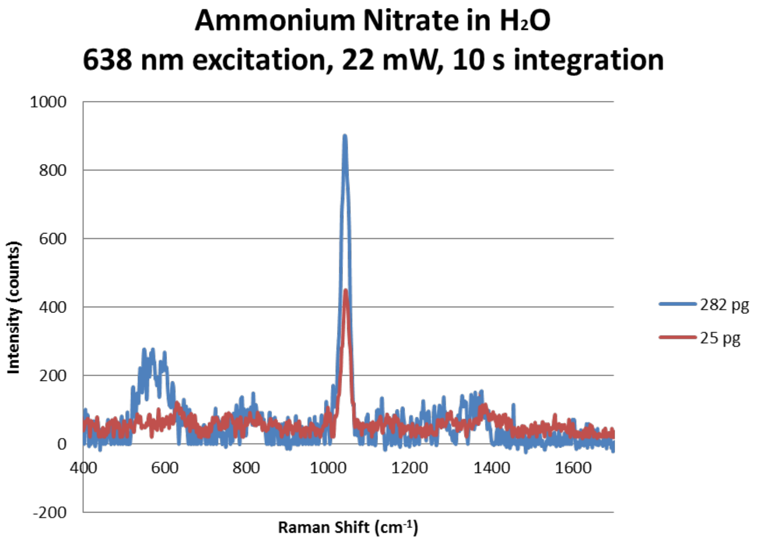


Figure 4: Raman spectrum of ammonium nitrate at two different concentrations on nanosponge SERS substrate.

PETN is often considered one of the most difficult explosives to detect because its structure does not lend itself to the necessary binding towards surface enhanced Raman chemistries. Nonetheless, this new technology gives the three key analytical peaks that are signature to this compound, even down to picogram levels (Figure 5).

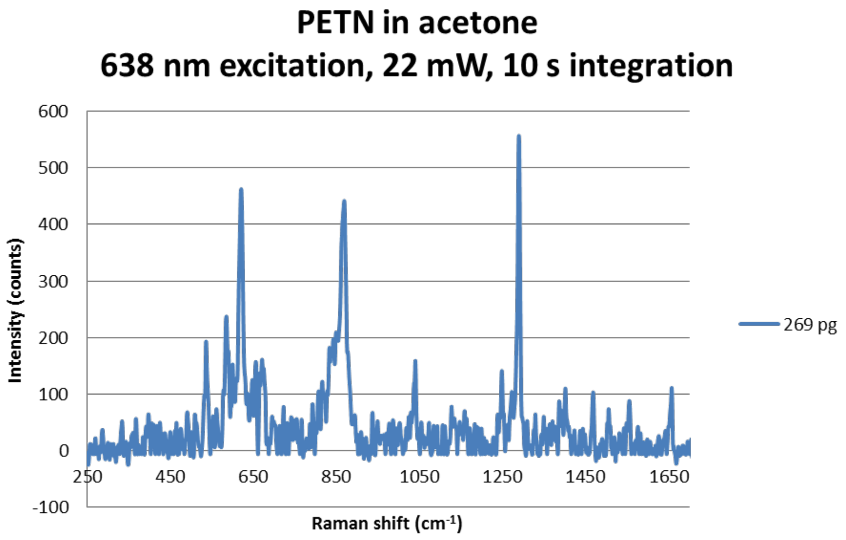


Figure 5: Raman spectrum of PETN explosive on nanosponge SERS substrate

3.2 RDX

Similarly, RDX is another explosive which is known to be rather difficult to detect. Figure 6 shows analytical peaks being registered by the device down to tens-of-picograms levels.

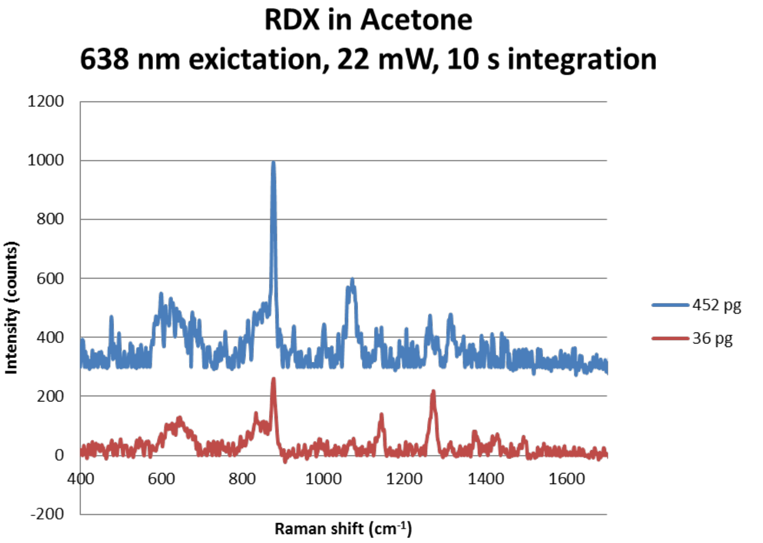


Figure 6: Raman spectrum of RDX explosive at two different concentrations on nanosponge SERS substrate

4 DISCUSSION

4.1 Comparison to Klarite

Figure 7 shows SERS spectra of the explosive RDX after being deposited on Klarite substrates by Botti *et al.*[2] These were obtained using the same integration time of 10 seconds, though it should be noted that the power used in those experiments was much higher at 180mW. Ocean Optics substrates were able to generate comparable limits of detection for RDX at one-eighth of the laser power used with the Klarite substrates. The spectra in Figure 7 represent probed masses of (a) 80 pg, (b) 200 pg and (c) 3 µg.

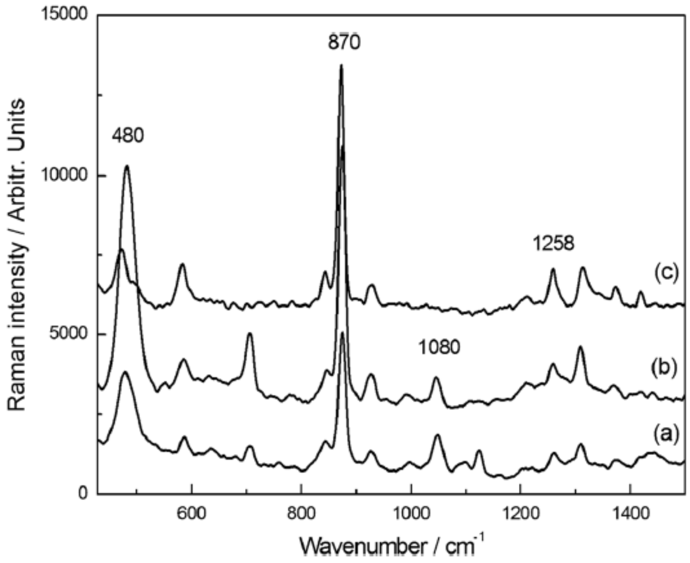


Figure 7: Raman spectrum of RDX on Klarite substrate

4.2 Optimum Laser Wavelength

Ongoing work includes optimizing the roughness of the glass surface, adjusting the ratio of gold to silver based on wavelength and analyte used, and modifying the porosity of the nanosponge structure by altering the working gas pressure. As these optimizations continue and the observed signals become stronger and more well-defined, the analytical software used to correlate peaks to analytes will become more reliable and consistent. All reported measurements were done using a 638 nm laser, as this wavelength shows the most regular and stable SERS response using the new sputter-based technology. Other wavelengths such a 785 nm and 532 nm also work with this technology, but the SERS intensity using 638 nm is the highest for most of the analytes examined. Table 1 shows the optimal wavelength per analyte for the three SERS technologies we can offer. Note that this does not mean they do not work with other wavelengths; these are merely configurations that gave the greatest peak intensity, even if only by a small amount.

Table 1: Optimum combination of SERS Substrates and Raman Wavelength

Substrate	**Sputtered Nanosponge**			**Gold Paper**			**Silver Paper**		
Wavelength (nm)	**532**	**638**	**785**	**532**	**638**	**785**	**532**	**638**	**785**
Analyte	BPE	Melamine			Malachite Green	Thiram	Rhodamine 6G	Malachite Green	Thiram
	Rhodamine B	Malachite Green			Rhodamine B	Melamine	Crystal Violet	Rhodamine B	Melamine
	Crystal Violet	Thiram			Rhodamine 6G	TNT			TNT
					Crystal Violet	BPE			BPE

Due to the strong performance with the sputtered technology we are set to release 638 nm systems in both modular and hand-held form factors. The hand-held system of course lends itself to field use and roadside-type applications, which would most likely utilize a swab form factor. Some preliminary studies have been performed using a swab approach, specifically looking at pesticide contamination on crops.

5 CONCLUSIONS

We present a novel surface enhanced Raman substrate consisting of a gold and silver alloy film to detect trace levels of explosive materials. The analyte of interest was drop-casted onto the substrate and measured using a benchtop Raman system. The current technique can detect several different explosives down to picogram levels. More work will be performed on this approach using explosives, as well as other types of chemical weapons. Several governments are actively testing these substrates using bioweapons such as Sarin and mustard gas with very promising initial results, which will be presented publically when ready. Ocean Optics will also be looking into how a field-ready procedure may look when using the sputter-based technology. This may include having a separate non-SERS swab overly wetted with solvent, and then squeezing a drop of this solvent on to the sputtered substrate after exposure to the test sample. We look forward to these types of developments as well as new form factors such as microtiter plates. This nanosponge alloy technology has the potential to be the most attractive SERS platform on the market due to its nearly unrivaled performance and low cost.

6 REFERENCES

1. E.P. Hoppmann, W.W. Yu, I.M. White, Highly sensitive and flexible inkjet printed SERS sensors on paper. *Methods,* **2013**, *63*, 219–224.
2. S. Botti, S. Almaviva, L. Cantarini, A. Palucci, A. Puiu, A. Rufoloni, Trace level detection and identification of nitro-based explosives by surface-enhanced Raman spectroscopy. *J. Raman Spectrosc.*, **2013**, *44*, 463-468.

APPLICATION OF STANDOFF LIF TO LIVING AND INACTIVATED BACTERIA SAMPLES

Arne Walter[1], Frank Duschek[1], Lea Fellner[1], Karin Grünewald[1], Herbert Tomaso[2], Jürgen Handke[1]

[1] *arne.walter@dlr.de*
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*

Abstract

To minimize the impact of an airborne bio-agent output, sensitive, specific and swift detection and identification are essential. A single method can hardly meet all of these requirements. Point sensors allow highly sensitive and specific identification but are localized and comparatively slow. Most laser-based standoff systems lack selectivity and specificity but provide real-time detection and classification in a wide region with additional information about location and propagation. A combination of both methods allows benefiting from their complementary assets and may be a promising solution to optimize detection and identification of hazardous substances.

Here, we present progress for an outdoor bio-detector based on laser-induced fluorescence (LIF) developed at the DLR Lampoldshausen. After excitation at 280 and 355 nm, bacteria species express unique fluorescence spectra. Upon deactivation, the spectral features change depending on the applied method.

Keywords: Bacteria; Fluorescence, laser induced; Spectroscopy; Standoff detection; Biological sensing and sensors; Hazardous material; Biological agent

1 INTRODUCTION

Terrorist attacks with bio-agents like e.g. the release of the neurotoxin sarin in the Tokyo subway in 1995 [10] and anthrax letters in 2001 [3] or accidental shipment of anthrax contaminated material in 2015 show the importance of effective detection of potentially hazardous substances. Most bio-agents are inexpensive and easy to obtain, grow and deploy. Due to a potential delay between infection and symptoms and the possibility of person-to-person spread, fast detection, localization and identification are crucial for immediate safety and containment measures.

Laser-based detection of hazardous material can be performed from safe distances up to the kilometre range and monitor wide areas in real-time. Operating an outdoor detection system is challenging because environmental material e.g. pollen, dust and diesel in the have to be taken into account. Fog, rain and snow affect laser propagation and stray light while incident sun- and ambient light interfere with the measurement. Furthermore, for use in inhabited areas, the laser radiation has to be eye safe.

1.1 Laser Induced Fluorescence

Established standoff detection techniques detect either plasma emission (Laser induced plasma spectroscopy, LIBS [5, 11]), inelastic scattered light (Raman spectroscopy [11]) or laser induced fluorescence (LIF [6, 11]). LIF spectroscopy yields a higher response signal than Raman spectroscopy and does not need as high excitation energies as LIBS. On the downside the obtained spectral features are limited. Deployment of multiple excitation wavelengths and time-resolved measurements provide additional information and, combined with sophisticated data analysis, significantly improves discrimination. However, LIF-based identification of bacteria has not yet been achieved. Here, we present and discuss promising data for further differentiation of bacterial species. To date, the combination of fast LIF-based detection, classification and localization and a subsequent directed acquisition and identification of a potentially hazardous sample with point sensors seems to be the most promising solution.

1.2 Bacteria fluorescence

Compared to chemical solutions, spectroscopy on bacteria is more complex. Bacteria differ in size and shapes and occur as single cells or may form clusters, chains or microfilms. They adapt to environmental conditions like nutrient supply and change their metabolic activity to these effects [1]. When exposed to stress, some bacteria, like *Bacillus anthracis*, can reversibly form endospores, dormant structures of high durability and changed constituent composition [8].

Observed bacteria fluorescence is a superposition of several contributing molecules absorbing at the respective excitation wavelengths. For *Escherichia coli (E. coli)*, fifteen potential contributors have been described [7]. Table 1 shows the most contributing fluorophores together with relevant absorption coefficients, mass fractions and estimated fluorescence quantum yields as well as calculated contributions to overall fluorescence at excitation wavelengths of 280 and 355 nm.

Substance	ε(280 nm) l mol^{-1} cm^{-1}	ε(355 nm) l mol^{-1} cm^{-1}	Mass fraction g / g dry weight (%)	Fluorescence		
				Quantum Yield	Calculated contribution at 280 nm (%)*	Calculated contribution at 355 nm (%)*
Tryptophan	5800	0	1.1 (4.0)	0.12	95.9	0.0
Tyrosine	1400	0	2.3 (3.5)	0.003	1.4	0.0
NADH + NADPH	2500	5200	0.048 (0.058)	0.04	0.2	27.1
Riboflavin + FMN	5000	9000	0.011 (0.01)	0.13	0.5	58.6
FAD	30000	9000	0.045 (0.045)	0.013	0.6	11.7
Pyridoxal derivates (unbound)	1000-2200	0-800	0.012 (0.012)	0.01-0.14	0.1	2.6
Ubiquinol	40000	0	0.003 (0.0)	0.018	0.1	0.0
Menaquinol	2700	6000	0.001 (0.003)	0.27	0.0	0.10

Table 1: Overview of the main fluorescing compounds for *E.coli* with spectral characteristics summarized from the work of Hill et al. [7]. Additionally, resulting estimated contribution to the overall fluorescence are displayed. Mass fractions for a mixture of closely related species from the genus *Bacillus* are set in parenthesis for comparison. ε is the decadic molar attenuation coefficient. Note that quantum yields are highly dependent on the local environment of a fluorophore and may vary in magnitudes. *calculated from given values

Since attenuation-coefficient ratios at these wavelengths differ significantly for most specified molecules, different sets of molecules will be probed and may lead to characteristic fluorescence spectra. Promising results of a first advance in bacteria LIF spectroscopy are presented in Ref. [4] and [12].

Upon excitation at 280 nm, *Bacillus thuringiensis* (*B. thuringiensis*) and *E. coli* have shown clearly distinguishable fluorescence spectra [4], as presented in Figure 1. As can be seen from Table 1, below 500 nm, dominant fluorophores should be mainly tryptophan (emission spectrum shown as dashed grey line) and some tyrosine (dash-dotted grey line) whereas the spectra above 500 nm coincide with NADH fluorescence (dotted grey line). The sum of these three fluorophores (solid grey line) was plotted to fit *B. thuringiensis'* fluorescence (solid blue line) with surprising agreement. Excitation at 355 nm produced similar fluorescence spectra which are in good agreement with NADH fluorescence for wavelengths greater than 500 nm. Note that measured bacteria spectra will rarely be just the sum of their components' spectra. Only few molecules within a bacterium contribute to fluorescence, others will reabsorb. Another issue is each molecule's fluorescence quantum yield, which can vary by several magnitudes depending on the local environment. The quantum yields found for molecules in solution can be a hint at best [9].

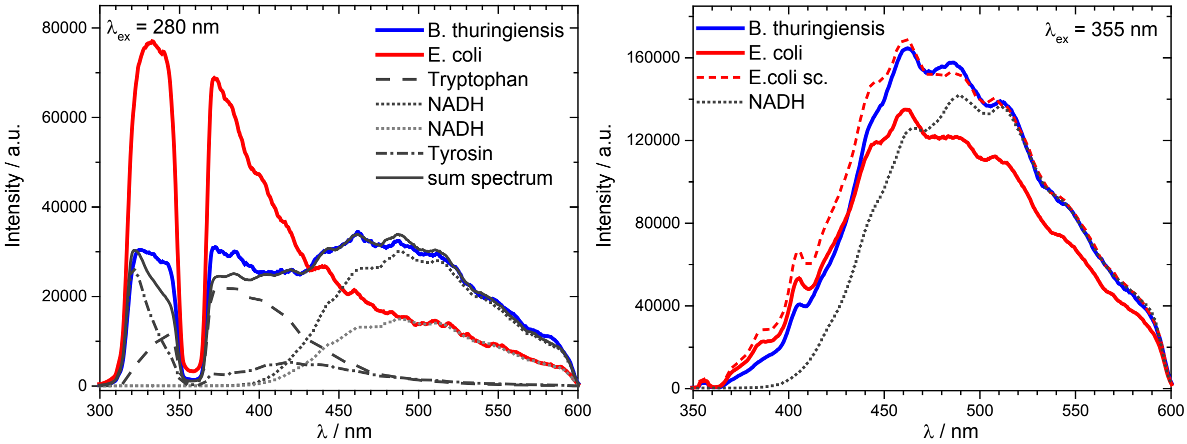


Figure 1: LIF spectra of *B. thuringiensis* (10^7 CFU/ml in PBS) and *E.coli* (10^9 CFU/ml in PBS) upon excitation at 280 nm (left) and 355 nm (right) [4, 12]. E. coli spectrum at 355 nm is scaled for comparison (dashed red line). On the left panel, fluorescence spectra of tryptophan, NADH and tyrosine and the sum of those spectra are plotted (dashed, dotted, dash-dotted and solid grey line), scaled to tentatively fit *B.thuringiensis*. On the right panel, only NADH is plotted (dotted grey line). All spectra are corrected for solvent-contributions.

While *E.coli* and *B. thuringiensis* are distant relatives in the domain of bacteria, the closely related members of the *Bacillus (B.)* genus, *B. subtilis*, *B. atrophaeus* and *B. thuringiensis* can also be distinguished by their characteristic fluorescence [12], as shown in Figure 2.

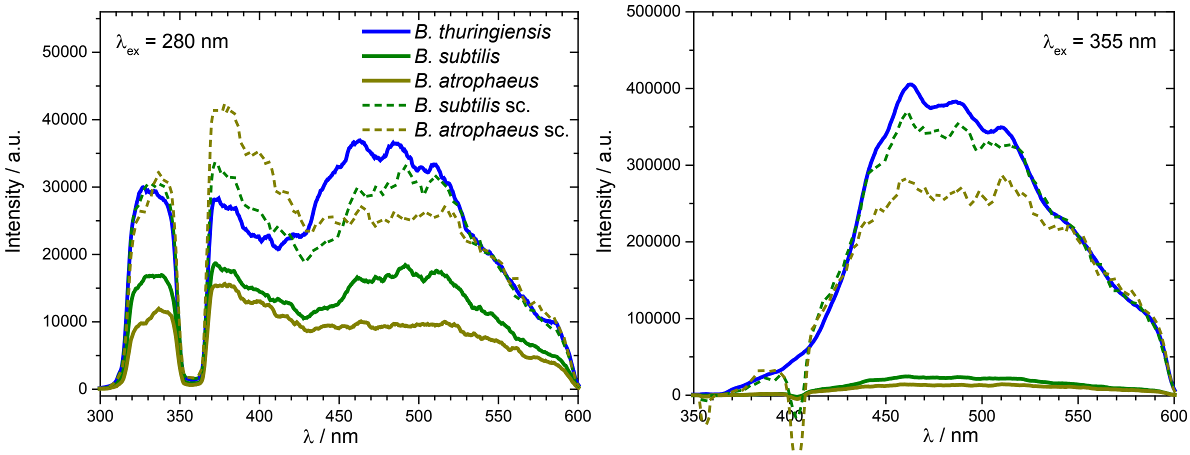


Figure 2: Fluorescence spectra of *B. thuringiensis, B. subtilis* and *B. atrophaeus* (10^8 CFU/ml in PBS) upon excitation at 280 nm (left) and 355 nm (right) [12]. Dashed curves are scaled to match the signal strength of *B. thuringiensis* on the red flank for comparison. Spectra are smoothed and corrected for solvent-interactions.

For proof of principle, LIF standoff detection for classification and identification of bacteria was evaluated using non-hazardous bacterial species as place holder for pathogenic bacteria. Future evaluations will have to be also performed with hazardous species in aerosol chambers at biosafety level 2 and 3 conditions to create a database that will allow differentiation among bacteria genera or even species. In this work, we investigate the influence of deactivation on the fluorescence spectra. Application of inactivated bacteria would facilitate the experimental approach since time consuming and potentially dangerous work with highly pathogenic bacteria could be reduced or completely avoided and data for classification could be gathered conveniently.

2 EXPERIMENTAL SETUP

2.1 Optical setup

To meet the challenges of outdoor detection, the standoff LIF detection system used for the conducted measurements is operated on a free space optical test range at the German Aerospace Center at Lampoldshausen. Chemical, biological and explosive (CBE) substances can be measured at distances from 20 to 135 m under different weather conditions. Laser and detection system are located in an open laboratory whereas the target is positioned outdoors. While experiments can be carried out with both aerosols and liquid phase in a cuvette at a range of distances, all data shown here were collected for suspensions at a distance of 22 m.

Eye safe laser pulses at 280 nm and 355 nm are used to excite the sample. Time-resolved spectra are captured by a gated iCCD camera. The detection system is prepared for background correction and trained pattern recognition software that classifies the sample into coarse classes. The schematic setup of the detection system is shown in Fig. 3.

A Nd:YAG laser supplies pulses of 7 ns pulse length at 355 nm with a repetition rate of 10 Hz. Each second pulse is frequency converted to 280 nm, resulting in an effective repetition rate of 5 Hz with pulse energies of about 10 mJ for each wavelength. Both wavelengths are directed onto the target substance. Fluorescence light is collected by a Newton telescope with an optical diameter of 400 mm. The collected light is split, spectrally filtered to suppress the laser lines and coupled into two optical fibers. One fraction is detected by a photomultiplier tube (PMT) providing information on the wavelength-independent temporal signal of the fluorescence. The other fraction is analyzed by a spectrometer with a resolution of 1 nm spanning a spectral range of 300 – 600 nm and detected by a gated iCCD camera. Time resolved spectra are obtained by a combination of

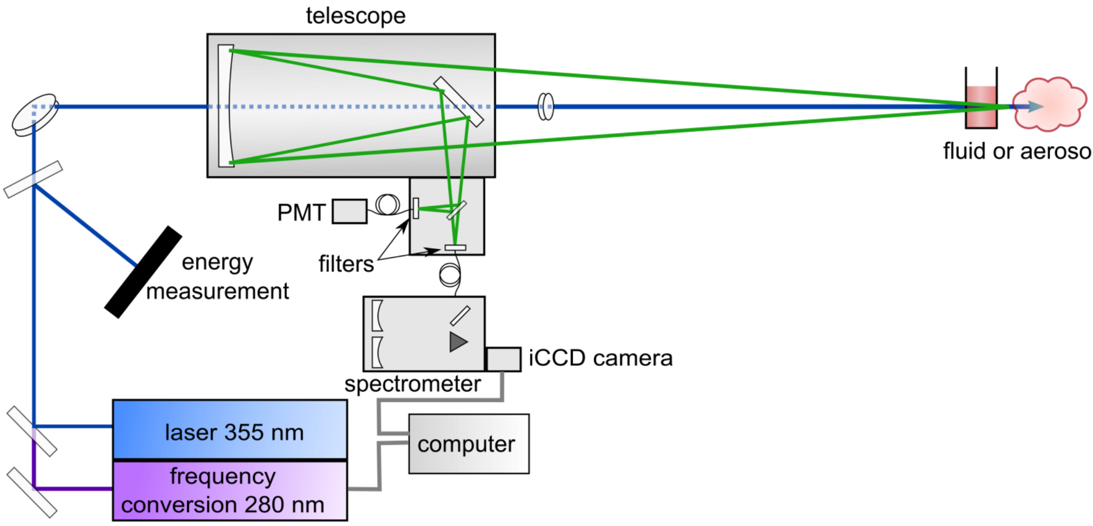


Figure 3: Schematic draft of the optical setup

several consecutive measurements with camera gates delayed relative to the laser pulse. 50 ms after each laser pulse, a background spectrum is recorded to compensate for fluctuations in background radiation and to make measurements more independent from weather conditions. A detailed description of the optical and electronical setup and on data acquisition and processing is given in Ref [6].

2.2 Cultivation and Sample preparation

Bacterial strains: *Bacillus thuringiensis* var. kurstaki strain HD-1 (isolated from insecticide DIPEL), *Escherichia coli* K12[2], *Bacillus atrophaeus* Nakamura 1989 (DSM 7264) and *Bacillus subtilis* (DSM 1970).

Cultivation of the bacteria species was carried out on blood agar plates (nutrient agar 1 obtained by Sifin, Berlin, Germany) supplemented with 7.5 % cattle or sheep blood at 37 °C for 24 h. Colony material was harvested and suspended in phosphate buffered saline (PBS) and stored at 4 °C. The concentration of colony forming units (CFU) per ml was determined by cultivation of 100 µl serially diluted solution in PBS with 0.4 % agar on agar plates at identical conditions. Bacterial suspensions were diluted with PBS to the concentrations measured. Chemical samples (NADH, amino acids) were solved in deionized water, stirred for 1 h and stored at 4 °C over night. Deactivation of bacteria was carried out either by heating at 95 °C for 10 min, autoclaving at 134 °C for 30 min, dilution in Ethanol and gamma radiation at 30 kGy +/- 10 % (done by Synergy Health Radeberg GmbH, Radeberg, Germany).

3 RESULTS

Samples of *B. thuringiensis* [12] and *E.coli* were deactivated by different treatments. The corresponding LIF spectra are presented in Fig. 4. Relative changes of fluorescence intensity calculated from the LIF spectra of Fig. 4 are illustrated in Fig. 5. Exited at 280 nm, fluorescence of *B. thuringiensis* (Fig. 4a) shows minor spectral changes after heating to 95 °C, namely a decrease in fluorescence below and a minor increase above 350 nm (see Fig. 5a). The 355 nm spectrum (Fig. 4b) remains almost unchanged (Fig. 5e). For the autoclaved samples, the spectra show similar changes with a larger increase in overall fluorescence intensity (Figs. 5b,f). Treated with ethanol, the 280 nm spectrum remains unchanged above 400 nm but fluorescence below significantly increases (Fig. 5c). The 355 nm spectrum also expresses an increase for wavelengths below 500 nm (Fig. 5g). Irradiation with gamma rays results in the most drastic changes of the fluorescence spectra. Excitation at 280 nm induces less fluorescence below 350 nm but an increased emission for longer wavelengths (Fig. 5d). Excited at 355 nm, fluorescence is increased for all observed wavelengths, especially below 450 nm (Fig. 5h).

Exited at 280 nm, fluorescence of *E. coli* (Fig. 4c) shows more significant spectral changes than *B. thuringiensis.* After heating to 95 °C, fluorescence decreases below 400 nm and significantly increases above (see Fig. 5a). The 355 nm spectrum (Fig. 4d) shows roughly the same behavior with almost doubled fluorescence intensity between 450 and 500 nm compared to the active sample (Fig. 5e). Autoclaved, the spectra show similar changes as for *B. thuringiensis* but with decreased fluorescence intensity below 400 nm (Figs. 5b,f). After being treated with ethanol, the 280 nm spectrum remains largely unchanged above 450 nm but fluorescence below increases (Fig. 5c). For 355 nm, fluorescence increases for wavelengths below 500 nm (Fig. 5g). Note that upon treatment with ethanol, the spectral changes for *B. thuringiensis* and *E. coli* at 355 nm coincide in shape, while less pronounced for *E.coli*. As for *B. thuringiensis*, irradiation with gamma rays results in the most drastic changes in the fluorescence spectra of *E. coli*. Excitation at 280 nm induces less fluorescence below 350 nm but increased emission for longer wavelengths (Fig. 5d). Excited at 355 nm, fluorescence is increased for all observed wavelengths but especially below 450 nm, just like for *B. thuringiensis* (Fig. 5h).

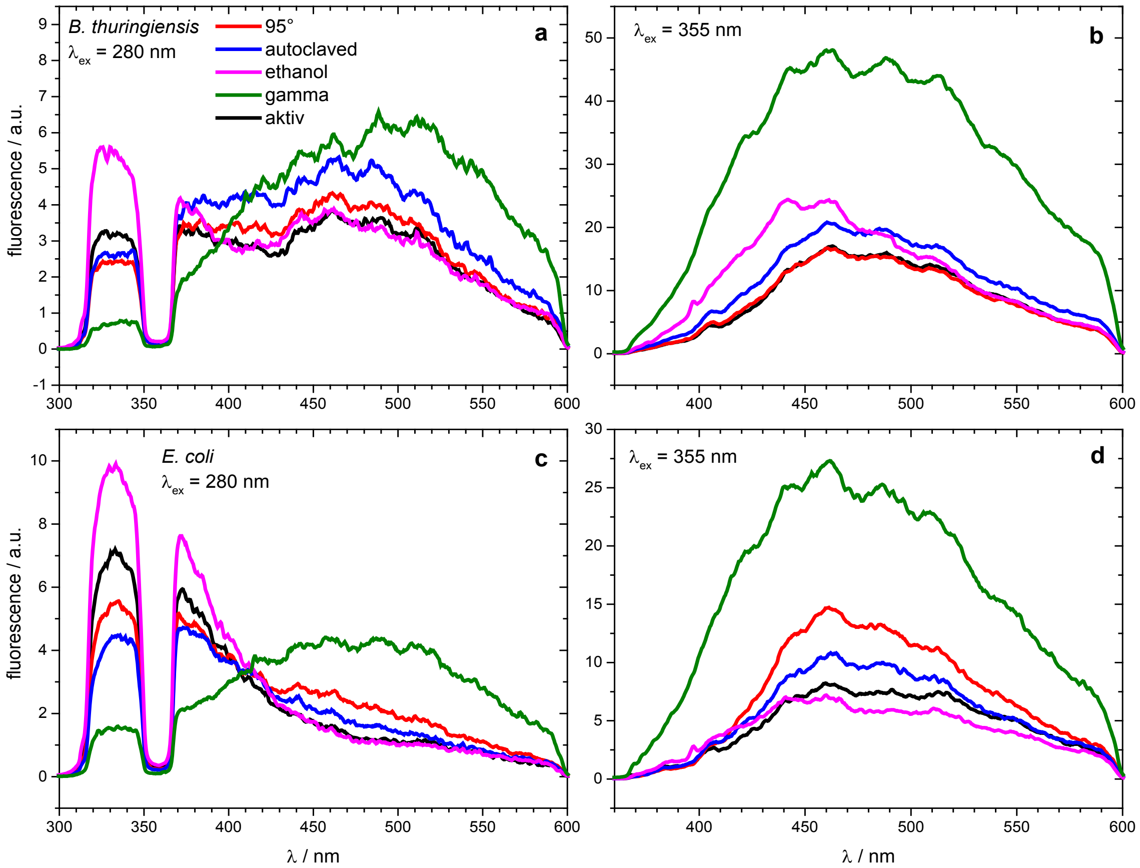


Figure 4: LIF spectra of *B. thuringiensis* (a,b -10^7 CFU/ml in PBS) and *E. coli* (c,d - 10^9 CFU/ml in PBS) excited at different wavelengths after deactivation by different methods

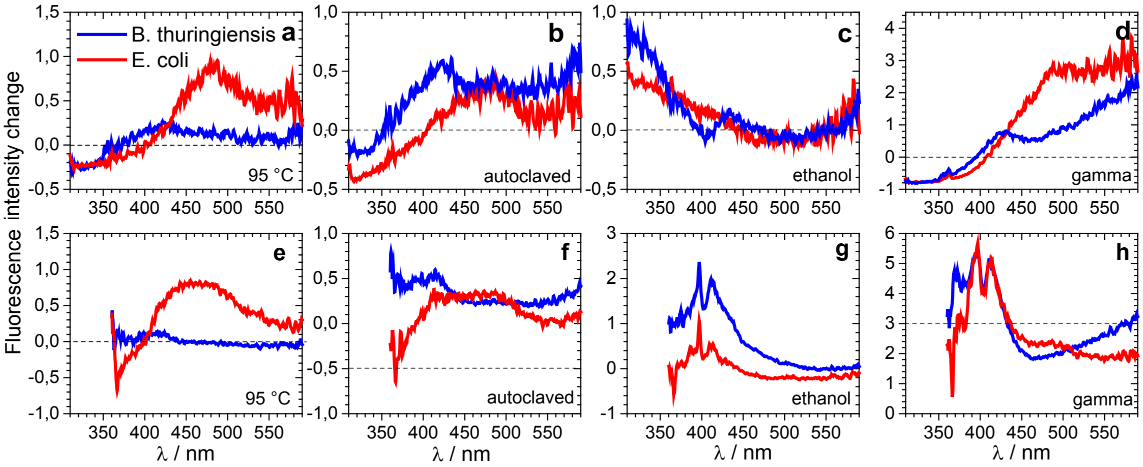


Figure 5: Relative changes in LIF spectra of *B. thuringiensis* and *E. coli* induced by different methods of deactivation excited at 280 nm (a-d) and 355 nm (e-f), calculated from LIF spectra in Fig. 4.

Most methods of deactivation shown here change the fluorescence spectra significantly both in amplitude and in shape. While heating to 95 °C seems quite promising for *B. thuringiensis* since it causes only minor spectral changes at both wavelengths, fluorescence drastically changes for *E. coli.* So far, deactivation does not generally seem feasible to produce optical facsimiles for pathogen bacteria. It may be that certain species respond well to certain treatments. Comparisons of the presented methods indicate a similar spectral respond of different bacteria on some treatments, e.g. deactivation by ethanol (see Figs. 5c,g). If this indication can be confirmed for further species and can be utilized has yet to be tested.

4 CONCLUSION AND OUTLOOK

Hyperspectral LIF standoff spectra of very distant relatives of bacteria as well as of closely related species have been shown for UV excitation wavelengths. The spectral diversity even within three species of a genus was proven to be high enough for safe distinction. Spectral accordance of some fluorophores with parts of the bacteria spectra has been illustrated. It was shown that inactivation methods can have influences on the spectra of *B. thuringiensis* and *E. coli.* While so far no tested method of deactivation can be generally applied, some treatments may work for selected bacteria.

As an outlook, an extension of the classifier for more distinct classification up to identification on the species level is desirable and in perspective, the spectral database [4, 6] will be extended. Investigations in more detailed classification will be carried out. The use of inactivated bacteria for safe handling of hazardous species will be investigated further by applying more deactivation methods on a wide range of species. Furthermore, a more detailed investigation of the spectral contributions of bacteria fluorophores will be performed.

REFERENCES

[1] Abee, T. and Wouters, J.A. (1999). *Microbial stress response in minimal processing.* International Journal of Food Microbiology. 50, 1-2, pp. 65–91.

[2] Clowes, R.C. and Hayes, W. (1968). *Experiments in microbial genetics*. Blackwell Scientific Publications.

[3] Council, N.R. (2011). *Review of the Scientific Approaches Used During the FBItextquotesingles Investigation of the 2001 Anthrax Letters*. The National Academies Press.

[4] Duschek, F. et al. (2015). A fast Hyperspectral Laser Induced Fluorescence application for standoff detection and online classification of biological hazardous materials. *10th Future Security 2015. Security Research Conference. Proceedings* (Berlin, 2015), pp. 97–104.

[5] Duschek, F. et al. (2010). Stand-off detection at the DLR laser test range applying laser-induced breakdown spectroscopy. *Optics and Photonics for Counterterrorism and Crime Fighting VI and Optical Materials in Defence Systems Technology VII*. SPIE-Intl Soc Optical Eng.

[6] Fischbach, T. et al. (2015). Standoff detection and classification procedure for bioorganic compounds by hyperspectral laser-induced fluorescence. *Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XVI*. SPIE-Intl Soc Optical Eng.

[7] Hill, S.C. et al. (2013). Fluorescence of bioaerosols: mathematical model including primary fluorescing and absorbing molecules in bacteria. *Opt. Express*. The Optical Society.

[8] Koehler, T.M. (2009). Bacillus anthracis physiology and genetics. *Molecular Aspects of Medicine*. 30, 6 (Dec. 2009), pp. 386–396.

[9] Pan, C.-P. and Barkley, M.D. (2004). Conformational Effects on Tryptophan Fluorescence in Cyclic Hexapeptides. *Biophysical Journal*. 86, 6, pp. 3828–3835.

[10] Tu, A.T. (1999). Overview of Sarin Terrorist Attacks in Japan. *ACS Symposium Series*. A.T. Tu and W. Gaffield, eds. American Chemical Society (ACS). pp. 304–317.

[11] Wallin, S. et al. (2009). Laser-based standoff detection of explosives: a critical review. *Anal Bioanal Chem*. 395, 2, pp. 259–274.

[12] Walter, A. et al. (2016). Stand-off detection: distinction of bacteria by hyperspectral laser induced fluorescence. *Proc. SPIE 9824*.

COMPLEX SYSTEM ANALYSIS USING GRAPH THEORY - IDENTIFYING CRITICALITY IN TRANSPORTATION NETWORKS

Martin Zsifkovits, Zhonglin Wang, Marian Sorin Nistor, Stefan Pickl

martin.zsifkovits@unibw.de, zhonglin.wang@unibw.de, sorin.nistor@unibw.de, stefan.pickl@unibw.de
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85577 Neubiberg (Germany)

Abstract

The aim of this paper is a deeper understanding of the behaviour of a critical infrastructure and its vulnerabilities. One example for such a vulnerable system is the German high-speed train system (ICE). The system can be seen as an individual network that might allow for various security installations and measures, regardless the policies of other public transport systems. We propose graph theoretic measures to analyse the system in detail, where we concentrate on centrality and efficiency measures. This is to detect the most vulnerable spots that demand for special treatment in terms of protection and the overall robustness of the system. The representation of result is based on visual analytics, which play a major role in managerial decision support.

Keywords: Transportation Systems, Vulnerability Analysis, Network Analysis, Graph Theory.

1 INTRODUCTION

The protection of critical infrastructures is essential for state and society [1]. As their functioning is a basis for our daily lives, critical infrastructures are a major target for terroristic attacks. Such attacks seem to be planned and organized in order to strike the most critical spots for harming the system strongly. One example for such a vulnerable system is the rail bound public transport, being represented by underground train systems and trains (both, regional and long distance). In order to protect such a system better, several security technologies can be seen as promising solutions in the future. However, before security measures can be implemented, decision makers need to deeply understand the systems' behaviour and its vulnerabilities.

The paper at hand focuses on the German high-speed train system (ICE) [2]. Quantitative graph theoretic measures [3] are proposed to analyse the ICE system, being represented as a distance-weighted and undirected graph. This is not only to detect the most vulnerable stations, but also to evaluate the overall robustness of the system. On this note, classical centrality measures [4-14] are applied to identify the most critical stations. Among these measures, degree centrality [5], closeness centrality [5], eigenvector centrality [6] and betweenness centrality [9] are considered. Furthermore, the nodal efficiency measure [15] and its improved version, the flow-weighted efficiency measure [15] are implemented to discern the crucial stations.

The reminder of this paper is organized as follows. In Section 2, the ICE network is constructed as a graph. Quantitative graph measures in terms of centrality and efficiency are introduced in detail. In Section 3, the network analysis on the ICE graph is applied using the measures described in the previous section and graphically represented using visual analytics techniques. In the last section, important conclusions are drawn and potential for future research is presented.

2 MODELS AND METHODS

In this section, based on the map of the Germany high speed train system (ICE) [2], the ICE network as an exemplary system is introduced in detail. The network measures of the centrality and efficiency are presented in this section as basis of the network analysis on the ICE network. Among the centrality measures in literature [12], four indices are considered in this paper: degree centrality [6], closeness centrality [11], eigenvector centrality [6], and betweenness centrality [14]. Additionally, the classical network nodal efficiency [16] and its improved version, the flow-weighted network nodal efficiency [15] will be described.

It is known that the ICE train network, as any other railway transportation system, is composed of stations (nodes) and their connections (edges). The German ICE network, being analysed in this paper, consists of 121 nodes and 168 edges. In this paper, the network is abstracted as an undirected weighted graph $G(V,E)$, where $V=\{v_i \mid i=1,2,3,...,\mathrm{n}\}$ represents the set of nodes and $E=\{e_{ij} \mid v_i,v_j \in V\}$ the set of edges of the network. $A=[a_{ij}]_{\mathrm{n}\times n}$ is the weighted adjacency matrix, where $a_{ij}=\omega_{ij}$ when $(v_i,v_j)\in E$, otherwise, $a_{ij}=0$. Here, n denotes the number of nodes in a graph, and ω_{ij} the distance length between every pair of adjacent nodes with the unit of 100 km. In order to compute the flow-weighted efficiency measure applied on the ICE network, another weighted adjacency matrix is considered. We define $B=[b_{ij}]_{n\times n}$, where $b_{ij}=\varpi_{ij}$ when there is at least one train passing the edge between the adjacent nodes v_i and v_j, otherwise, $b_{ij}=0$. Here, ϖ_{ij} represents the train flow defined as the number of trains passing through the edge between the adjacent nodes v_i and v_j in a day.

2.1 Centrality measures

The indicators of various centrality measures can be used to detect the vulnerable nodes in a graph. Many centrality measures exist that have been studied in prior publications [5, 8, 10, 12, 14]. In this paper, four of the most relevant existing centrality measures are implemented. This are the degree centrality measure, the closeness centrality measure, the eigenvector centrality measure, and the betweenness centrality measure.

2.1.1 Degree Centrality Measure

The degree centrality measure [5] is defined as the number of edges that one node shares with the others. This is a simple indicator of whether one node is very connected (hub node) in a network or not. According to [5] the formula $C_d(v_i)$ of the degree centrality of one node v_i is defined as $C_d(v_i)=|N(v_i)|/(n-1)$ [13], where $N(v_i)$ is the set of adjacent nodes of v_i.

2.1.2 Closeness Centrality Measure

The closeness centrality [5] can be used to measure how close one node is to all the other nodes along the shortest paths. This can also reflect the accessibility of a given node in a graph. This measure is defined as the reciprocal of average distance from a given node v_i to all other nodes. As shown in [13], the formula of the closeness centrality $C_c(v_i)$ of one node v_i is defined as $C_c(v_i)=(n-1)\big/\sum_{j=i}^{n} d(v_i,v_j)$. Here, $d(v_i,v_j)$ is the distance length (unit of 100 km) of the shortest path between node v_i and node v_j.

2.1.3 Eigenvector Centrality Measure

The influence of a node in a network can be measured with the help of the eigenvector centrality measure [6]. However, the influence of a central node not only depends on the number of its neighbours, but also the influence of its neighbours. The eigenvector centrality $C_e(v_i)$ for a node v_i is defined as $C_e(v_i)=(1/\lambda)\sum_{v_j\in N(v_i)} a_{ji}\times C_e(v_j)$ [13]. Here, $N(v_i)$ is the set of nodes connected to v_i, and λ is the maximum eigenvalue of the adjacency matrix.

2.1.4 Betweenness Centrality Measure

The betweenness centrality measure [5] quantifies the number of the shortest paths between all the other pairs of nodes passing through a given node in a graph. A node tends to be crucial, if it lies on the shortest paths connecting large pairs of nodes. Moreover, the nodal betweenness centrality reflects the transitivity of a given node in a network. The formula of the betweenness centrality $C_b(v_k)$ for a node v_k is defined as $C_b(v_k)=(2/(n^2-3n+2))\sum_{i\neq k}^{n}\sum_{j\neq i\neq k}^{n}\sigma_{ij}(v_k)/\sigma_{ij}$ [13]. Here, σ_{ij} is the number of shortest paths between the nodes v_i and v_j, and $\sigma_{ij}(v_k)$ is the number of the shortest paths between the nodes v_i and v_j passing through node v_k.

2.2 Efficiency measures

Whether the information can be exchanged efficiently from one node to the rest of the network can be characterized with the support of efficiency measures. In this section, two types of efficiency measures are presented. These are the classical efficiency measure, and its variation, the flow-weighted efficiency measure which computes in addition the flow information between the nodes of a network.

2.2.1 Classical Efficiency Measure

According to [15], the classical efficiency measure computes the distance length of the shortest paths from a given node to all the others. Its formula for a node v_i in the graph G, $E_{V(G)}(v_i)$ is defined as $E_{V(G)}(v_i)=(1/(n-1))\sum_{j\neq i}^{n}1/d(v_i,v_j)$ [15]. Here, $d(v_i,v_j)$ is defined as the distance length (unit of 100 km) of the shortest path between node v_i and node v_j.

2.2.2 Flow-weighted Efficiency Measure

The flow-weighted efficiency measure [15] considers not only the distance length of the shortest paths but also the train flow information between the nodes of a network. This measure $E_{F\_V(G)}(v_i)$ for a node v_i is defined as $E_{F\_V(G)}(v_i)=(1/(n-1))\sum_{j\neq i}^{n}w(v_i,v_j)/d(v_i,v_j)$. Here, $w(v_i,v_j)$ represents the lowest train flow of all edges along the shortest path between the nodes v_i and v_j defined as $w(v_i,v_j)=\min_{(v_k,v_l)\in P_{ij}}\varpi_{kl}$ [15]. P_{ij} represents the set of edges on the shortest path from node v_i to node v_j, and ϖ_{kl} denotes the train flow between the connected nodes v_i and v_j.

3 RESULTS

So far, the network to be analysed was constructed, and an important list of measures was introduced in order to conduct an extensive network analysis. Now, these measures are applied. The centrality and efficiency measures are applied to detect the hubs and the most efficient nodes of the ICE network. In order to determine the flow-weighted efficiency measure, the train flow on the *Tuesday to Thursday* schedule (May 24 – 26 2016) is considered exemplary.

A comparison among the nodal centrality measures and the nodal efficiency measures is presented in Table 1. Here, according to the node degree centrality measure, the most central stations are *Frankfurt(M) Flughafen Fernbf* and *Mannheim Hbf.* Furthermore, we found that the station *Frankfurt(M) Flughafen Fernbf* can be also identified among the top five important stations according to centrality measures like closeness, eigenvector and betweenness. On another note, the station *Mannheim Hbf* appears among the top five station only for the eigenvector centrality measure.

Table 1. Top five critical stations of ICE network.

Ranking based on node degree centrality			Ranking based on node closeness centrality		
ID	Name	Values	ID	Name	Values
2	Frankfurt(M) Flughafen Fernbf	0.075	1	Frankfurt(Main)Hbf	0.293106
4	Mannheim Hbf	0.075	2	Frankfurt(M) Flughafen Fernbf	0.289831
1	Frankfurt(Main)Hbf	0.066667	23	Hanau Hbf	0.288122
41	Köln Hbf	0.066667	26	Fulda	0.286137
82	Hannover Hbf	0.058333	27	Kassel-Wilhelmshöhe	0.277216
Ranking based on node eigenvector centrality			Ranking based on node betweenness centrality		
ID	Name	Values	ID	Name	Values
2	Frankfurt(M) Flughafen Fernbf	0.445345	1	Frankfurt(Main)Hbf	0.284034
4	Mannheim Hbf	0.340208	103	Berlin Hbf	0.280392
41	Köln Hbf	0.318321	22	Nürnberg Hbf	0.201961
1	Frankfurt(Main)Hbf	0.318158	2	Frankfurt(M) Flughafen Fernbf	0.196779
50	Köln Messe/Deutz Gl.11-12	0.259669	82	Hannover Hbf	0.181653
Ranking based on node efficiency measure			Ranking based on node flow-weighted efficiency measure		
ID	Name	Values	ID	Name	Values
103	Berlin Hbf	1.00782	92	Hamburg Dammtor	25.74423
106	Berlin Ostbahnhof	0.850841	91	Hamburg Hbf	25.59645
41	Köln Hbf	0.829973	103	Berlin Hbf	21.96745
50	Köln Messe/Deutz Gl.11-12	0.827539	107	Berlin Gesundbrunnen	15.5683
91	Hamburg Hbf	0.811662	104	Berlin Südkreuz	10.74468

According to the node closeness centrality measure, station *Frankfurt(Main)Hbf* is highlighted as the closest station to all the other stations along the shortest paths. Other measures find this station important too. For instance, it can be also found on the first position for the betweenness centrality, the degree centrality on the third position, and the eigenvector centrality on the fourth.

Based on the node eigenvector centrality measure, as it was shown by the node degree centrality measure, the station *Frankfurt(M) Flughafen Fernbf* is confirmed as the most central station with the largest influence, as its neighbouring stations *Mannheim Hbf*, *Frankfurt(Main)Hbf*, and *Köln Hbf* have not only a higher number of neighbours according to degree centrality measure, but also larger influences according to eigenvector centrality measure.

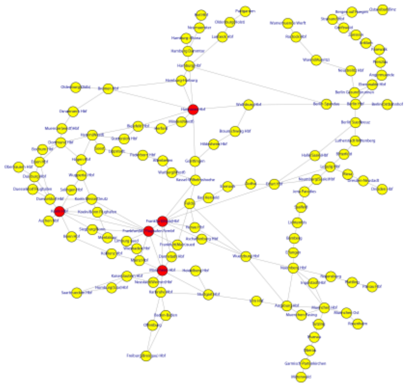
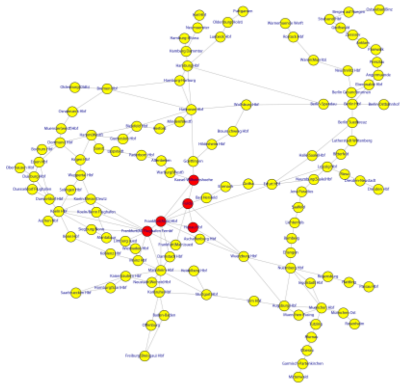
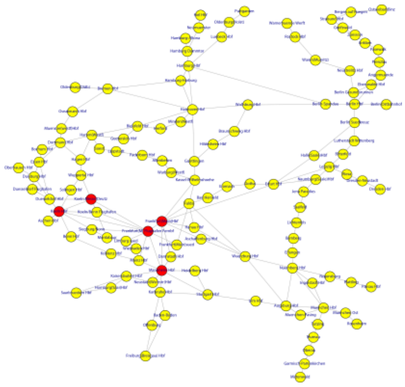
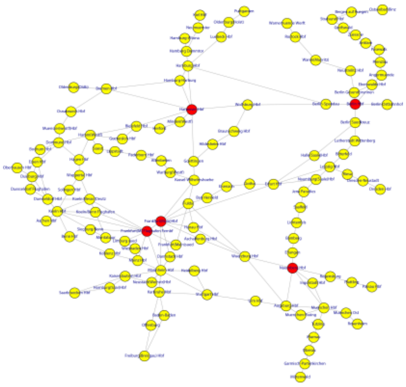
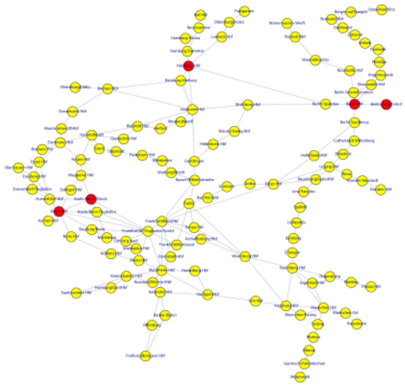
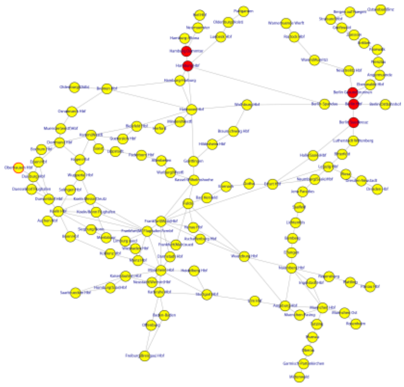
On the basis of the node betweenness centrality measure, the station *Frankfurt(Main)Hbf* can be identified as the most transmissible station based on how often the shortest paths would pass through the given station, as it was detected by the node closeness centrality measure.

The node efficiency measure finds the station *Berlin Hbf* as the most efficient station of the network based on its shortest paths in reaching any other station. This station is found important also by the node flow-weighted efficiency measure.

The node flow-weighted efficiency measure identifies the station *Hamburg Dammtor* as the most efficient station based on its shortest paths in reaching any other station of the network. This measure considers also in the same time the minimum train flow available on each route.

In a further step, visual analytics are applied to the results in order to represent the numerical results graphically. The exemplary representation of the results highlight the stations with highest degrees in red.

Table 2. Visual Analytics Applied to conducted results

	
Degree Centrality	***Closeness Centrality***
	
Eigenvector Centrality	***Betweenness Centrality***
	
Efficiency Measure	***Flow-Weighted Efficiency Measure***

4 CONCLUSIONS

In this paper, quantitative network analysis is conducted on the German ICE network. Through the results achieved by the measures applied, one can get a feeling for the most critical stations in terms of serviceability in the German ICE system. Concretely, the stations *Frankfurt(M) Flughafen Fernbf, Frankfurt(Main)Hbf, Berlin Hbf, Köln Hbf,* and *Mannheim Hbf* seem to be especially critical and therefore demand for special treatment in terms of safety and security. The visual representation of results gives an intuitive picture of the situation and allows for further conclusions. Interestingly, results in Table 1 do not show a single station being important for all the applied measures. Therefore, the idea of a network of networks (NON) should be applied in future research in order to get a more global picture of the network. Such a global measure would allow for combining all parameters in a single analysis. Furthermore, the tested measures should be compared to vulnerability measures. This might even sharpen the overall picture of the network in terms of criticality.

REFERENCES

[1] Rinaldi, S. M. (2004). *Modeling and simulating critical infrastructures and their interdependencies*. In System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on IEEE. pp. 8-pp

[2] Deutsche Bahn. (2016). *Geman ice-netz 2016*. Technical report, Herausgeber: Deutsche Bahn, https://www.bahn.de/p/view/mdb/bahnintern/fahrplan und buchung/reiseauskunftsmedien/fahrplanmediendownload/2016/mdb 213351 ice liniennetz 2016.pdf.

[3] Dehmer, M., Emmert-Streib, F. (Eds.). (2014). *Quantitative Graph Theory: Mathematical Foundations and Applications*. CRC Press.

[4] Dehmer M, Emmert-Streib F, Pickl S. (2015). *Computational network theory: Theoretical foundations and applications*. Wiley-VCH Verlang GmbH & Co. KGaA, Weinheim.

[5] Freeman, L. C. (1978). *Centrality in social networks conceptual clarification.* Social networks, 1(3), pp. 215-239.

[6] Maharani, W., Gozali, A. A. (2014). *Degree centrality and eigenvector centrality in twitter*. In Telecommunication Systems Services and Applications (TSSA), 2014 8th International Conference on IEEE, pp. 1-5.

[7] Emmert-Streib, F. and Dehmer, M., (2011). *Networks for systems biology: conceptual connection of data and function*. Systems Biology, IET, 5(3), pp.185-207.

[8] Ruhnau, B. (2000). *Eigenvector-centrality—a node-centrality?*. Social networks, 22(4), pp. 357-365.

[9] Newman, M. E. (2008). *The mathematics of networks*. The new palgrave encyclopedia of economics, 2(2008), pp. 1-12.

[10] Wang, J., Mo, H., Wang, F., Jin, F. (2011). *Exploring the network structure and nodal centrality of China's air transport network: A complex network approach*. Journal of Transport Geography, 19(4), pp. 712-721.

[11] Derrible, S. (2012). *Network centrality of metro systems*. PloS one, 7(7), pp. e40575.

[12] Gómez, D., Figueira, J. R., Eusébio, A. (2013). *Modeling centrality measures in social network analysis using bi-criteria network flow optimization problems*. European Journal of Operational Research, 226(2), pp. 354-365.

[13] Boudin, F. (2013). *A comparison of centrality measures for graph-based keyphrase extraction*. In International Joint Conference on Natural Language Processing (IJCNLP), pp. 834-838.

[14] Tsiotas, D., Polyzos, S. (2015). *Introducing a new centrality measure from the transportation network analysis in Greece*. Annals of Operations Research, 227(1), pp. 93-117.

[15] Nistor, M. S., Pickl, S., Raap, M., Zsifkovits, M. (2016*). Network Efficiency and Vulnerability Analysis using the Flow-weighted Efficiency Measure*. EMNet-Book: Management and Governance of Networks. Forthcoming.

[16] Latora, V., Marchiori, M. (2003). *Economic small-world behavior in weighted networks*. The European Physical Journal B-Condensed Matter and Complex Systems, 32(2), 249-263.

A QUANTITATIVE APPROACH TO VULNERABILITY ASSESSMENT OF CRITICAL INFRASTRUCTURES WITH RESPECT TO MULTIPLE PHYSICAL ATTACK SCENARIOS

Daniel Lichte[1], Stefan Marchlewitz[2] and Kai-Dietrich Wolf[3]

[1] *lichte@iss.uni-wuppertal.de*

[2] *marchlew@uni-wuppertal.de*

[3] *wolf@iss.uni-wuppertal.de*
Bergische Universität Wuppertal, Institut für Sicherungssysteme, Talstrasse 71,
42551 Velbert (Germany)

Abstract

Due to the growing threat of attacks, the security of critical infrastructures increasingly gets in the center of interest of society and research. Different emerged approaches propose a holistic security risk management and assessment including a scenario dependent vulnerability analysis. So far, there is no comprehensive method to gain scenario spanning vulnerability results or to consider uncertainties regarding the capability of security equipment. The article focuses on these challenges and provides an analytic modeling approach, which allows for a quantitative and scenario spanning vulnerability assessment. Probability density functions are used to describe the parameters protection, detection and intervention as security system capabilities. It is shown that a scenario spanning assessment and the consideration of uncertainties in the description of the system is feasible. A vulnerability computation with alternative example configurations illustrates the implementation of the modeling assumptions into the proposed modeling approach. Conclusive, a critical discussion of the analytical model is given.

Keywords: critical infrastructure protection, CIP, vulnerability assessment, physical security, probability functions, probabilistic modeling, analytical modeling, risk analysis.

1 INTRODUCTION

Due to a growing threat of attacks, physical security and protection of critical infrastructures has become an increasingly important topic in society and research in recent years. Critical infrastructures are distributed networks and facilities, which are considered essential for security, economy, public and health services [1].

Several governments created research and political programs dealing with the protection of critical infrastructures, e.g. the USA [2] or the EU and also Germany [3]. These programs partly address the development of methods for a security oriented risk analysis, leading to a more intensive examination and new approaches of critical infrastructure protection. The analysis of these proposed approaches shows that further research is needed for several reasons. Firstly, the resilience of critical infrastructures in case of successful attacks is a main topic of research, while the prevention of attacks via physical security is hardly considered. Secondly, the developed approaches for security risk analysis and vulnerability assessment are based on scenario analysis. Additionally, assessment and analysis operate with discrete probabilities. As a result, the uncertainties regarding the capabilities of components in current infrastructure security systems with increasing complexity are not taken into account for vulnerability and overall risk assessment. At the same time, existing methods are not capable of a scenario spanning modelling and quantification of vulnerability, as the employed methods are mostly qualitative and based on expert knowledge.

By outlining the state of art, the above mentioned shortcomings are further explained. Following, an analytical approach for vulnerability assessment is proposed, where the main goal is to establish a model of the security system that enables the treatment of uncertainties and also a scenario spanning assessment. This is achieved by applying probability density functions (pdf) as a description of the fundamental parameters of the security system. The general procedure is then illustrated by the assessment of an example configuration.

2 STATE OF THE ART

Security comprises a number of issues covering different fields of expertise; therefore a comprehensive view is needed for a holistic security assessment [4]. Physical security as a part deals with the protection of (critical) infrastructures from intentional physical attacks [5]. The aim of physical security measures is to prevent an attacker from reaching his goal by different means of protection, detection and intervention and also set up resilient structures to lower the consequences of successful attacks [6].

The corresponding risk definition can be defined as [7] [8]:

$$Risk = Threat \times Vulnerability \times Consequence \tag{1}$$

This definition combines in a quantitative manner consequences of attacks and probabilities of threat scenarios with the risk of individual attacks being successful, defined as vulnerability. The above quantitative formulation of risk may help to deduce acceptable risks and necessary measures to reduce risks [9]. Inherent uncertainties regarding the three risk factors should be cautiously considered [10].

Various approaches to security risk assessment have been developed, which may be divided into qualitative, quantitative and hybrid methods [11]. Qualitative methods are mostly based on expert knowledge, while existing quantitative methods use discrete probabilities. The former are more widespread because of their ease of use, while at the same time the usage of expert knowledge can lead to inaccurate or even wrong results [12]. Additionally, some quantitative methods aiming at cost-benefit analysis have been developed. Typically, cost-benefit analysis of security measures would account for potential financial losses as result of an attack, the probability of occurrence of various attack scenarios and the vulnerability of the security system [13]. This analysis yields accurate results but raises the complexity compared to qualitative methods [12].

Quantitative vulnerability analysis as part of the quantitative risk analysis methods is mostly based on methods adapted from reliability and general risk analysis. Here, the considered model is dependent on given attack scenarios [14]. This dependency is detrimental to a comprehensive analysis as knowledge about the behavior of a potential attacker may be insufficient [15]. The different modeling approaches can be further split up into mainly analytical but also formal methods. An overview of approaches is given in [16]. Analytical methods are often based on attack trees, which can be seen as a derivative of the fault trees known from reliability analysis. Attack trees were first used by Schneier [17] for IT security analysis and since have been further developed by different authors, summarized e.g. in [18].

Contini et al. have introduced incoherent attack trees to characterize the dynamic behavior of the considered system [19]. Additionally, they integrated simple probability distributions for protection into attack trees to investigate the chronologic sequence of attacks. Hence, it is possible to analyze the security system's ability for an attack intervention by comparing the probabilities of residual protection and system response [7].

Garcia describes this relation in [6], where feasible attack paths as part of different attack scenarios and corresponding barriers are used. The model is time based and introduces the critical detection point, which is the latest possible point of detection that ensures a successful intervention.

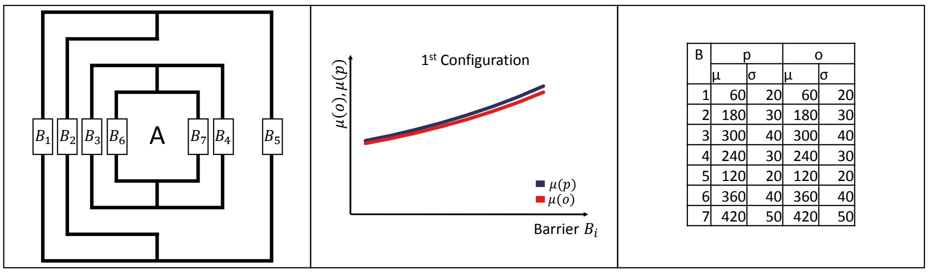
Overall, the different existing approaches to analytical modeling and analysis of vulnerability are lacking the consideration of uncertainties in the system parameters and overall behavior. Additionally, these approaches do not allow a scenario spanning analysis of the whole security system, as the analysis depends on specific scenarios.

3 APPROACH

In the following, the analytical modeling approach is introduced. It is based on the assumptions made by Contini et al. and Garcia and uses probability density functions (pdf) to describe the characteristics of security system components for protection, detection and intervention. The Parameter observation is introduced as the system description is limited to the technical abilities of the inherent components: detection is then regarded as a combination of protection and observation to reflect the circumstance that detecting an attack through observation is a time dependent process. The aim here is to consider uncertainties and establish a scenario spanning view of the whole system when determining its vulnerability.

In a first step, four fundamental assumptions about the system behavior and the relations between the system components are made. Following these assumptions, the model is developed in corresponding steps. The steps are gradually applied to an example system configuration (see fig. 1), in which the components are characterized using normal distributions (pdf). Finally, a comparison with a second configuration is drawn.

The model depicted on the left in fig. 1 (onion layer model) represents the structure and feasible attack paths by means of barriers. Four individual attack paths lead to the asset A via barriers B_1-B_7.



B	p		o	
	μ	σ	μ	σ
1	60	20	60	20
2	180	30	180	30
3	300	40	300	40
4	240	30	240	30
5	120	20	120	20
6	360	40	360	40
7	420	50	420	50

fig. 1: Example System

The chosen configuration of individual protection and observation pdf at barriers B_1-B_7 (fig. 1, right) may be resulting from a general strategy for protection and detection ability along possible attack paths (fig. 1, center). Here, protection at the outer barriers grows stronger on the way to the asset while bigger efforts are made at the perimeter to gain a low observation time.

3.1 Basic Assumptions

The most relevant behavior of a security system can be characterized by four basic assumptions about dependencies and relations between its components:

1. The weakest path of the security system determines the system's vulnerability, as the way of the attacker is uncertain.

2. The combination of protection and observation at barriers is necessary as an attacker is always able to break through a barrier given infinite time without being detected.
3. The detection of an attack is possible only if the protection is sufficient to prevent a break-through until detection.
4. After detection, an attack can be stopped only, if the residual protection along the remaining attack path lasts long enough to keep the attacker from reaching the asset until intervention is completed.

Following these assumptions, the analytic modeling approach can now be derived.

3.2 Step 1: Topological Modeling

In a first step, the topological and physical relations in the security system of a considered infrastructure are modeled. Following the first assumption, all attack paths of a system should be considered, as the unknown weakest path determines the system's vulnerability. Thus, all feasible attack paths of an infrastructure are extracted into a path based model. fig. 2 shows the result of the extraction of the example models attack paths. The path model includes all four attack paths directed towards the asset.

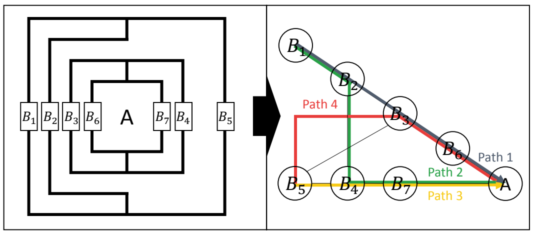


fig. 2: Path-based Model of Example System

3.3 Step 2: Attack Path Detailing

In accordance with the second assumption, the model for the single attack paths is further detailed in step 2. Therefore, the detailed model of the attack paths comprises protection and observation components at the barriers connected in sequence. Additionally, an intervention option is added to the model at every barrier because of its direct dependency on the interaction between protection and observation components. The attack path is detailed as exemplarily shown in fig. 3 for the first path of the example system and displays the different components at the involved barriers.

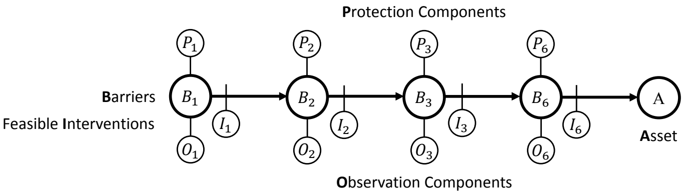


fig. 3: Detailed Attack Path 1 of Example System

3.4 Step 3: Barrier Oriented Probability of Detection

The third assumption implies that detection at a barrier occurs with the probability that protection is holding back the attacker long enough until the point of detection is reached. The conditional probability for detection D gives:

$$D = P(t_p > t_o)$$

fig. 4 shows the relation between observation and protection for the time of an attack t. The pdf for detection results from the area where detection potentially occurs.

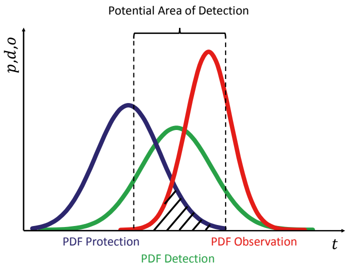


fig. 4: Area of Potential Detection

The resulting cumulated detection probability function $D(t)$ can be interpreted as the technical ability to detect an attack combining components for protection and observation. In terms of probability it can be described with the following expression:

$$D(t) = \int_0^t o(t_o) \cdot \left[\int_{t_o}^{\infty} p(\tau) d\tau \right] dt_o \tag{2}$$

3.5 Step 4: Timely Intervention on Attack Path

In accordance with the fourth assumption an intervention is always needed to stop an attack. Therefore, the timely intervention on an attack path is derived. Intervention is defined as a pdf that depicts the time dependent probability of a successful intervention. As described by Garcia, for a timely intervention the required time for intervention t_I has to be shorter than the time the attacker needs to break through the residual protection on the considered attack path [6] (see fig. 5).

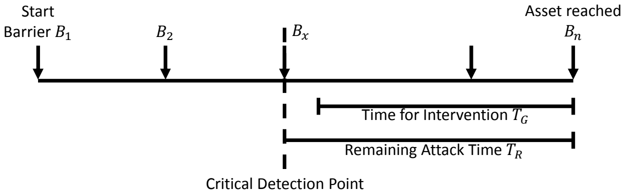


fig. 5: Critical Detection Point

Then, the simplified relation for a barrier B_x on an attack path with n barriers is:

$$t_I < \sum_{x+1}^{n} t_{p,i} \tag{3}$$

By analogy with Contini et al. in [7], the description by probability distributions results in the conditional probability of the needed intervention time t_I being shorter than the residual protection on the path t_x (see fig. 5):

$$T = P(t_x > t_I) \tag{4}$$

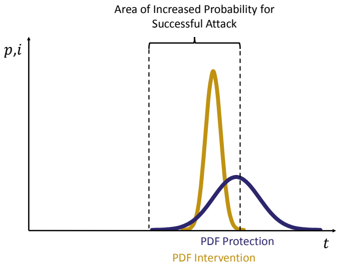


fig. 6: Timely Intervention

Further, the residual protection probability can be calculated by convolution of the pdfs for protection of the remaining barriers of the attack path. For barrier B_x on the attack path:

$$p_{Path,x}(t) = p_{x+1}(t) * \dots * p_n(t) \tag{5}$$

The cumulated conditional probability for timely intervention $T(t)$ can then be derived by combining the pdfs for intervention and residual protection:

$$T(t) = \int_0^t i(t_I) \cdot \left[\int_t^\infty p_{Path,x}(\tau) d\tau \right] dt_I \tag{6}$$

Now, the vulnerability of every barrier V_i can be calculated by means of absolute detection ability D_i and the barriers overall probability of a timely intervention T_i. Both values are derived by calculating the corresponding cumulated probabilities for $t \to \infty$. In this way, all feasible points of detected break through and timely intervention are considered. Therefore the strength of a barrier S_i is described as the probability of preventing the attacker from reaching the asset by detection and timely intervention. The vulnerability is the strength complement:

$$V_i = 1 - S_i = 1 - D_i \cdot T_i \tag{7}$$

As the attacker can only be detected once on the attack path, the absolute detection rate is decreasing over an attack path. This is reflected in the serial connection of the barriers on an attack path and leads to the calculation of the vulnerability $V_{Path,j}$ for path j as a product of the barriers vulnerabilities:

$$V_{Path,j} = \prod_{i=1}^{n} V_i \tag{8}$$

The resulting path vulnerability is applicable to all kinds of attack paths in security systems. For path 1 of the example system (see fig. 1) this yields:

$$V_{Path,1} = V_1 \cdot V_2 \cdot V_3 \cdot V_6 = 0{,}1309 \tag{9}$$

3.6 Comparison of Configurations

After having deduced the system description, the example security system introduced above is compared to a second configuration that only differs in the positioning of the security system's components. The characteristics of the components remain unchanged. The comparison illustrates the behavior of the proposed model.

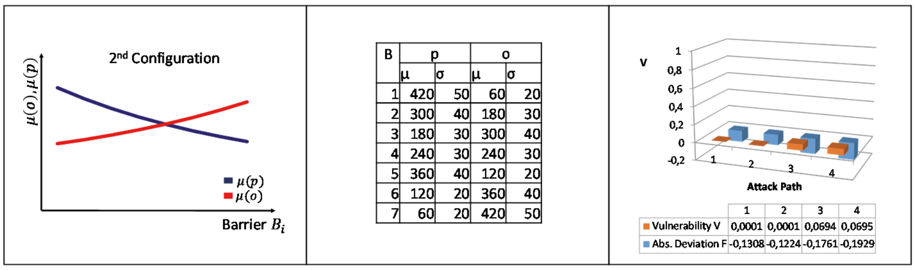
As the vulnerability of path 1 has already been determined for the first configuration, the remaining paths of the example system are calculated. The results of all paths are summarized in tab. 1

tab. 1: Path Vulnerability for Configuration 1

Path	1	2	3	4
Vulnerability V	0.1309	0.1225	0.2455	0.2624

Apparently, results depend on the length of the attack path. Path 1 and 2 consist of four barriers, while the asset can be reached by breaking through three barriers on the paths 3 and 4 and a timely intervention is less probable on these paths. This leads to a potentially higher vulnerability.

In an alternate configuration 2, the perimeter is strongly protected, descending towards the asset, while detection components and intervention possibilities are not changed. The principle configuration and the computational results are shown in fig. 7.



B	p		o	
	μ	σ	μ	σ
1	420	50	60	20
2	300	40	180	30
3	180	30	300	40
4	240	30	240	30
5	360	40	120	20
6	120	20	360	40
7	60	20	420	50

	1	2	3	4
🟧 Vulnerability V	0,0001	0,0001	0,0694	0,0695
🟦 Abs. Deviation F	-0,1308	-0,1224	-0,1761	-0,1929

fig. 7: Values and Results of Configuration 2

The results for configuration 2 are similar to the first ones, although the level of vulnerability is lower for all paths of the system. This results from the maximized strength of the outer barriers ensuring a high detection ability in the early stage of an attack. Due to the more likely early detection, the probability of a timely intervention is high albeit the falling protection level.

The comparison of the configurations shows that the basic assumptions regarding the behavior of a security system are considered in the presented modeling approach. Most important for vulnerability is the probability to detect an attack and the residual protection on the path to allow a timely intervention.

4 CONCLUSION

By outlining the state of art, the paper reveals shortcomings in current physical security and vulnerability analyses, notably regarding the consideration of existing uncertainties in current approaches. Starting from this, an analytic model based on the probabilistic description of the characteristic parameters protection, observation and intervention as well as on the principle of the weakest path is proposed.

The approach is then further detailed in four steps according to presumed basic assumptions. The first step develops the model by describing the topological relations of a security system. Individual attack paths are detailed in step 2 by combining the basic parameters at every barrier. Based on the 2nd step, the description for detection is illustrated. In step 4, the probabilistic relation for timely intervention is deduced. Thus, the path vulnerability is composed. All steps of the proposed approach are applied to an example security system, and a comparison with a second configuration is conducted.

The proposed analytic approach shows that vulnerability modeling based on probabilistic methods allows the treatment of the system's inherent uncertainties in assessment. Additionally, the approach theoretically enables a scenario spanning system analysis by using the method of the weakest path and therefore considering the whole system. Going beyond existing methods, this model is suitable for vulnerability optimization, which is subject of our ongoing work.

Nevertheless, the approach should be enhanced further for application. As the input parameters of protection, observation and intervention are not discussed yet, they need to be detailed. It should be investigated how an aggregation of these parameters would be possible and to which extent they are dependent on the risk factor threat. Furthermore, there is more evaluation needed to verify the models consistency, possibly by a variance based sensitivity analysis to further understand the model's behavior. After successful evaluation the model could be the basis for the optimization of vulnerability under constraints, e.g. cost restrictions.

REFERENCES

[1] C. Alcaraz and S. Zeadally, “Critical infrastructure protection: Requirements and challenges for the 21st century,” *International Journal of Critical Infrastructure Protection*, 2014.

[2] The White House, “Presidential Policy Directive -- Critical Infrastructure Security and Resilience,” The White House, Washington, DC, USA, Presidential Policy Directive PPD-21, 2013.

[3] Bundesministerium des Innern, “Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie).” Bundesministerium des Innern, 2009.

[4] Harnser Group, Ed., “A Reference Security Management Plan for Energy Infrastructure.” European Commission, 2010.

[5] J. Beyerer, J. Geisler, A. Dahlem, and P. Winzer, “Sicherheit: Systemanalyse und Design,” in *Sicherheitsforschung - Chancen und Perspektiven*, Berlin: Springer, 2010, pp. 39–72.

[6] M. L. Garcia, *The Design and Evaluation of Physical Protection Systems*, 2nd ed. Burlington, MA, USA: Butterworth-Heinemann, 2008.

[7] S. Contini, L. Fabbri, V. Matuzas, and Cojazzi, Giacomo, “Protection of Multiple Assets to Intentional Attacks: A Methodological Framework,” in *Probalistic Safety Assessment. International. 11th 2012*, Helsinki, Finnland, 2012, vol. 6, pp. 4343–4352.

[8] W. L. McGill, B. M. Ayyub, and M. Kaminskiy, “Risk Analysis for Critical Asset Protection: Risk Analysis for Critical Asset Protection,” *Risk Analysis*, vol. 27, no. 5, pp. 1265–1281, 2007.

[9] J. F. Broder and E. Tucker, *Risk Analysis and the Security Survey*, 4th ed. Waltham, MA, USA: Butterworth-Heinemann, 2012.

[10] P. L. Campbell and J. E. Stamp, “A Classification Scheme for Risk Assessment Methods,” Sandia National Laboratories, Albuquerque, NM, USA, SAND2004-4233, 2004.

[11] J. W. Meritt, “A Method for Quantitative Risk Analysis,” in *Proceedings of the 22nd National Information Systems Security Conference*, Arlington, VA, USA, 2008.

[12] D. J. Landoll, *The Security Risk Assessment Handbook: AComplete Guide for Performing Security Risk Assessments*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2011.

[13] F. Flammini, A. Gaglione, N. Mazzocca, and C. Pragliola, “Quantitative security risk assessment and management for railway transportation infrastructures,” in *Critical Information Infrastructure Security*, Springer, 2009, pp. 180–189.

[14] G. S. French and D. Gootzit, “Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack,” in *Vulnerability, Unvertainty and Risk: Analysis, Modeling and Management*, Hyattsville, ML, USA, 2011, pp. 782–789.

[15] L. A. (Tony) Cox, Jr., *Risk Analysis of Complex and Uncertain Systems*. New York, NY, USA: Springer, 2009.

[16] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, “Model-based evaluation: from dependability to security,” *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 48–65, 2004.

[17] B. Schneier, “Attack Trees,” *Dr. Dobbs Journal*, vol. 24, no. 12, pp. 21–29, 1999.

[18] Z. Vintr, D. Valis, and J. Malach, “Attack tree-based evaluation of physical protection systems vulnerability,” presented at the 2012 IEEE International Carnahan Conference on Security Technology (ICCST), 2012, pp. 59–65.

[19] S. Contini, G. G. M. Cojazzi, and G. Renda, “On the use of non-coherent fault trees in safety and security studies,” *Reliability Engineering and System Safety*, vol. 93, no. 12, pp. 1886–1895, 2008.

DEFAULT RISK OF SATELLITE BASED CRITICAL INFRASTRUCTURE

Harald Opitz[1, 2]

[1] *hopitzu@web.de*
University of Bonn, Faculty of Mathematics and Natural Sciences,
Department of Geography, Meckenheimer Allee 166, 53115 Bonn (Germany)

[2]Fraunhofer Institute for Technological Trend Analysis INT,
Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

Satellite based services and applications have moved into the focus of the European Critical Infrastructure Protection (ECIP) latest when the Galileo program [1] came into its action phase in 2012, and the Copernicus program [2] was physically launched by the European Space Agency (ESA) in 2014. A decade before, the US Government Accountability Office brought up questions on commercial satellite security [3] while warning: Loss of capabilities by failure of satellite data (systems) inevitably lead to severe implications in economic and social life [4]. Analysing critical infrastructure in these terms raises further questions of interdependencies between satellite based CI branches. Satellite systems are already being integrated into infrastructure operations to discover new resources in nature, compensate for capacity limitations in telecommunication, increase efficiency in logistics, transportation, navigation and traffic, and protection against natural hazards as well as accidental risks by early warning systems. In brief, satellite systems can make or break civil infrastructure. A survey on satellite based CIP, recently done by the author (2015/16), provides answers to ‘what is critical about satellite based CI, from both users’ and providers’ perspective. Highlighting a dozen CI-branches, it analyses aspects of threat awareness from cyberattacks to space weather, examines failure types, questions enterprises’ response behaviour as well as impacts expected on possible breakdowns caused by interruption of satellite data flow.

Keywords: Critical Infrastructure Protection, Satellite Applications, Risk Management.

ACKNOWLEDGEMENTS

For their strong support of the entire study, many thanks to: ATG Europe (NL), Bundeswehr Office for Defence Planning; Centre of Satellite Navigation Hesse (cesah); European Space Agency (ESA); Federal Office of Civil Protection and Disaster Assistance (BBK); Forum for Satellite Navigation, Fraunhofer Institute for Technological Trend Analysis INT; German Aerospace Center (DLR).

1 INTRODUCTION

Space, while politically looked upon as an individual CI sector by leading space nations [4, 5], encompasses a variety of unique satellite capacities and therewith holding some keys to the future of man-made problems on Earth. However, there are different points of view to ’what is satellite based CI’, what it does or does not include and who is in charge in case of emergency. While up to now, satellite based CI in Germany is subsumed under ’Information and Telecommunication branch’ [5, 6], the European decree on CI [8] issues distinctive satellite based applications as original and essential CIs (e.g. Galileo, Eurocontrol). Moreover, satellite systems are used by EU for boarder control (Frontex) and further security issues (e.g. maritime surveillance) [9].

Over the last decade Global Navigation Satellite Systems (GNSS) have been developed by several nations in different approaches (Russia, Glonass 2011; China Compass/Beidou, 2011; India, IRNSS 2016; Japan, QZNSS 2018; Europe, Galileo fully operational in 2018). Beyond geo-political and strategic purpose, national autonomy (independence from GPS), GNSS increasingly have become an overall security factor in economies running CIs. Thus, the question of 'dual use' [10] has widened its focus. Now, including security matters within the civilian environment of populations' everyday life such as process control of power and resources supply, public transport, finance transfer, navigation et al.

1.1 Interdependency of satellite based critical infrastructure

Satellite systems as for Earth observation, surveillance, navigation and telecommunication are equipped with specialised capabilities which makes them irreplaceable for the operation of other complex CI systems. Fig. 1 shows the complex interdependencies between 9 basic functions of existence connected to their data sources provided by satellite systems from CI Space sector and to Information Communication Technology CI sector (ICT) [11]. Each of these two sectors provides immense capacity of digital data capturing, storage, processing, en-/decoding and accelerated laser data transport which makes their combined interaction via ground segments interdependent. A possible shortfall of either CI system would lead to inoperability while satellite based services would be lost.

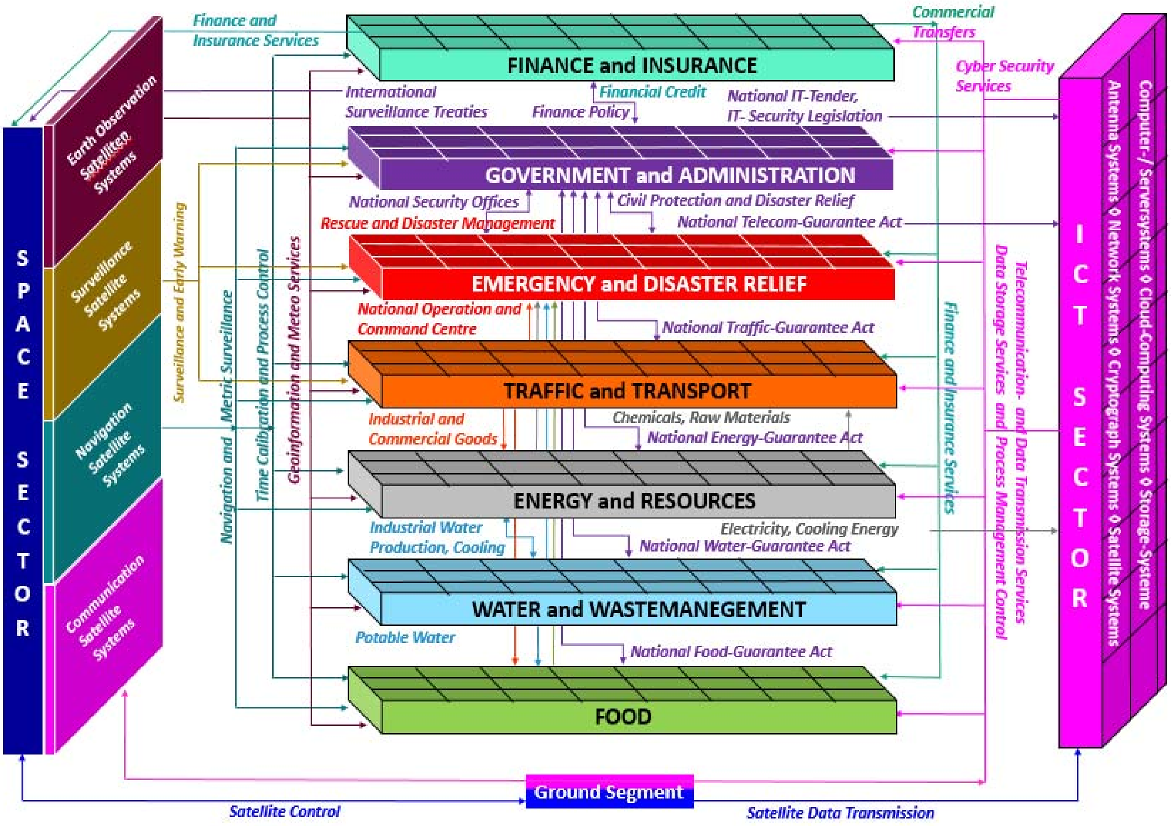

SPACE SECTOR
Earth Observation Satellites Systems
Surveillance Satellite Systems
Navigation Satellite Systems
Communication Satellite Systems
Finance and Insurance Services
Surveillance and Early Warning
Navigation and Metric Surveillance
Time Calibration and Process Control
Geoinformation and Meteo Services
FINANCE and INSURANCE
International Surveillance Treaties
Financial Credit
Finance Policy
National IT-Tender, IT- Security Legislation
GOVERNMENT and ADMINISTRATION
National Security Offices
Rescue and Disaster Management
Civil Protection and Disaster Relief
National Telecom-Guarantee Act
EMERGENCY and DISASTER RELIEF
National Operation and Command Centre
National Traffic-Guarantee Act
TRAFFIC and TRANSPORT
Industrial and Commercial Goods
Chemicals, Raw Materials
National Energy-Guarantee Act
ENERGY and RESOURCES
Industrial Water Production, Cooling
Electricity, Cooling Energy
National Water-Guarantee Act
WATER and WASTEMANEGEMENT
Potable Water
National Food-Guarantee Act
FOOD
Commercial Transfers
Cyber Security Services
Finance and Insurance Services
Telecommunication- and Data Transmission Services
Data Storage Services and Process Management Control
ICT SECTOR
Antenna Systems ◊ Network Systems ◊ Cryptograph Systems ◊ Satellite Systems
Computer-/ Serversystems ◊ Cloud-Computing Systems ◊ Storage-Systeme
Ground Segment
Satellite Control
Satellite Data Transmission

Fig. 1: Interdependencies of satellite based CIs (source: HELLER [12], own adaption)

As a consequence, an even temporary loss of satellite services will lead to CI cascading effects [13, 14] mostly risking economic cycle, foremost by miss-navigation, traffic collapse, communication breakdown, and financial transfer crash [15]. But also long term observation would be affected by satellite outage, implying the shortfall of suitable foundation for assessing space weather phenomena [16, 17] concerning military and civil electronic facilities, up to missing ecological data determining environment factors as for crop prediction et al [3, 18, 19] Finally, with regard to natural hazards and human catastrophes, satellite assets are essential for disaster forecast, damage assessment and situational follow up when global emergency services are required.

2 APPROACH AND METHODOLOGY

Main effort of the study was to bring up attention to satellite based CI in order to be recognized as an individual CI branch with manifold valuable, critical services in todays' economy and society. Therefore, a survey was designed with criteria extracted from the expert conference 'Global Navigation meets Geoinformation 2015', at the European Space Operation Centre (ESOC), organized by cesah [20]. Using 'Risk Analysis and Horizon Scanning' digital tool (RAHS) a broad variety of 150 manufacturers, providers and users of satellite based CI were addressed, which of the answers of 42 multi structured enterprises and institutions are represented 105 times in more than 20 CI-branches featured in Fig. 1. As far as to the knowledge of the author, this survey was done for the first time, and therefore decided to apply mixed method research [21] combined with grounded theory [22]. Analysis were done entirely by quantitative calculation; while some expert opinions were blended into the risk assessment, in order to sustain some of their arguments which are discussed in the main body of the study. Not least, the author contributed some observations from his years of experience as a team member of the security and the communication department at ESOC, participating in several missions (MSG-3, SWARM, Sentinel1-A, GALILEO, ROSETTA).

3 SURVEY RESULTS

Due to the limited space granted here, the visualized results of the survey are followed directly by the author's interpretation. While satellite data for navigation, telecommunication, and optical vision are the most permanently used applications, the survey results (Fig. 2) showed the strongest increase of satellite based services for telematics (esp. home services), and security applications (e.g. observation of pipelines et al facilities worth protecting) [2]. With 3.3 million downloads from Sentinel portal open to public [23], the usage of radar and optical vision raised significantly for spatial and environment data. More than 22.500 registered users hinting to the growing interest for satellite products and increasing privatization of this market. Moreover, 41% of internet data flow is covered by satellite service, with growth aspired up to 70% within the next years.

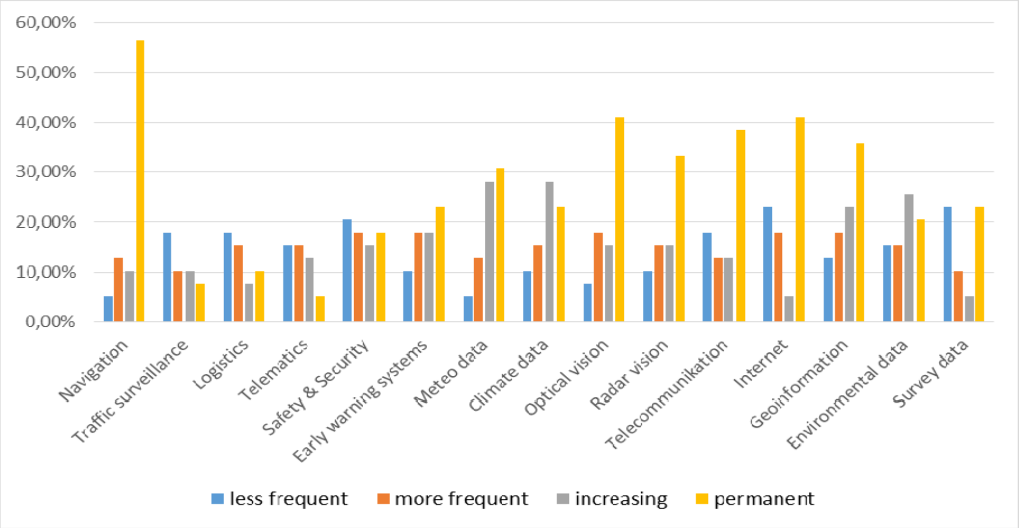


Fig. 2: Application and usage intensity of satellite data

Even though the risk for most hazards was rated low (Fig. 3), it indicates a generally high awareness level concerning the subject. 71% of survey participants confirmed to having a strong risk awareness when using satellite based data. The most common hazards are held most likely for realistic: Such as weather extremes same as human or technical failure, which can be interpreted as risk events that did take place more often in the own facility, already.

So space phenomena, including space debris, cyber war, and acts of terror being imaginable, they were esteemed being at the very end of hazard events risking satellite data. In opposition to this, experts on space phenomena and security matters on satellite operations consider exactly these hazards as high risk elements. Even though having occurred rather seldom, there is a growing tendency to these threats being imminent. Some reasons for this are the increasing knowledge distribution on high-end programming, signal manipulation, software spread on the private satellite market, and attempts of hacking satellites or satellite controls by hired groups of obscure origin [5, 24].

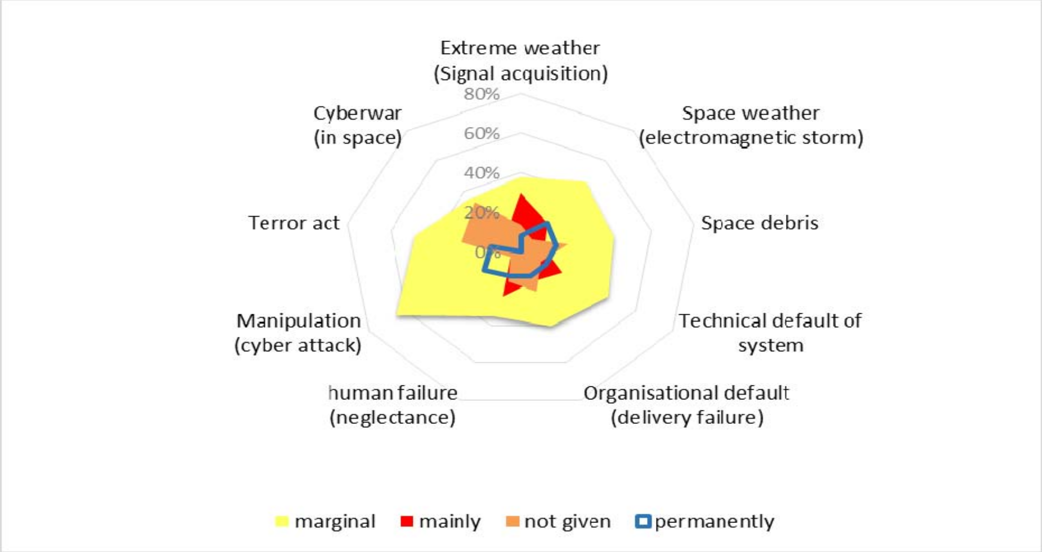


Fig. 3: Risk esteem on application of satellite data due to various hazards

Asked for only true satellite data failure occurrences, in Fig. 4 cyberattacks were confirmed with less than 10 per year by 12% of survey participants. This matches with the low data rate provided for the ‘permanently’ given risk in Fig. 3, delivering trustworthy statements. As well,

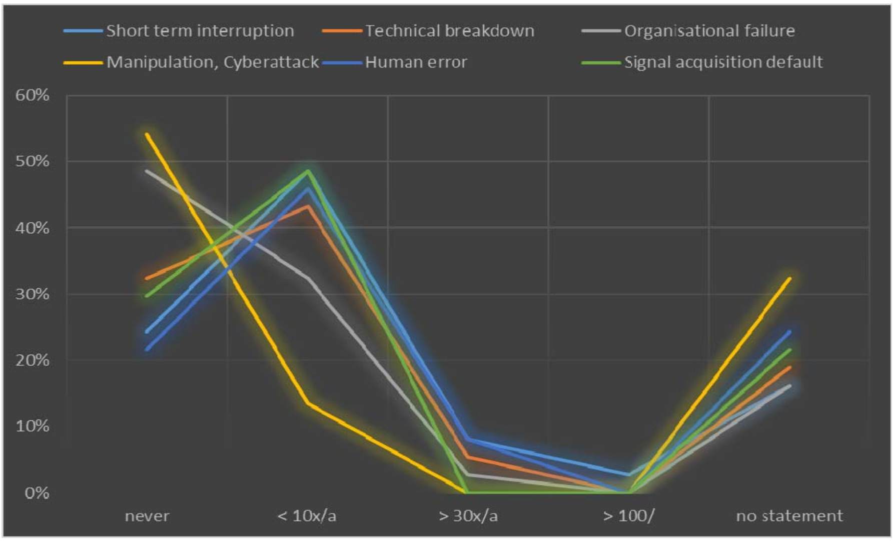


Fig. 4: Average shortfall of satellite data per year caused by various failures

these graphs showing also the highest discrepancy between answers not given or stating neither failures ever happened, while the other half of survey participants admitted all other kind of failure reason did occur by <10 times per year. Interpretation: Sensitive questions on company security not answered do either show a strong understanding of the same or might be a hint to a significant dark figure.

Taking suitable precautions against a possible interruption of satellite based data was deemed not being necessary by more than one third of the survey participants in Fig. 5, no matter how long a shortfall would last. This maybe either owed to the rather vague certainty that ‘everything is secured’ within the own facility, or risk awareness is lowered when measures may afford further investment. In latter case, means of choice are redundant systems and/or switch to other satellite systems. For this, Galileo and partly Glonass were named most frequently by on fifth of the participating enterprises and institutions.

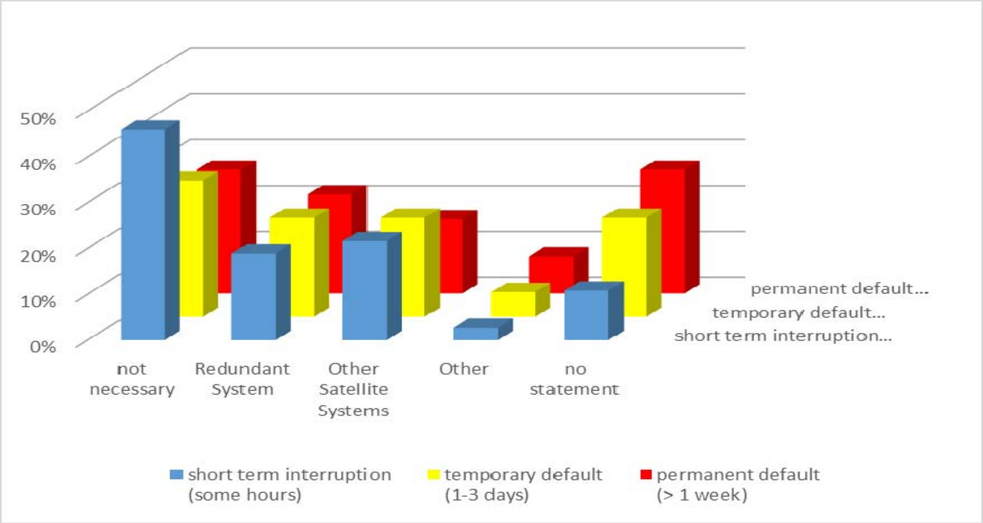


Fig. 5: Applied countermeasures against satellite data failure

The occurrence of a possible damage caused by satellite based services and its impact on CI was difficult to calculate, as the data base would have afforded deeper insight into the companies’ and institutions’ risk management structures. However, all statements showed an

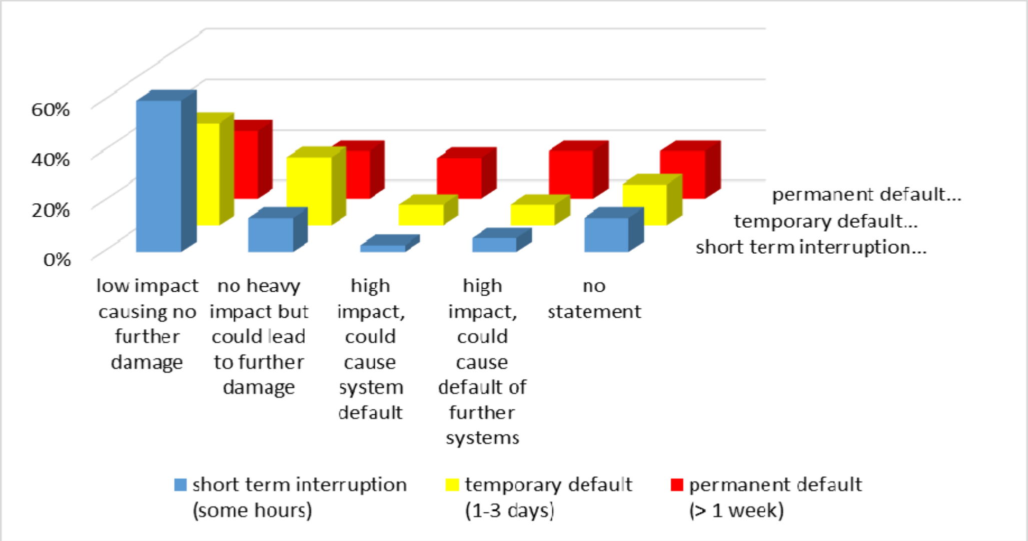


Fig. 6: Loss estimation and exposure in case of satellite data failure

average high degree of certainty (1.83, with minimum certainty = 4). Most likely taken into account are low impacts with no further consequence for own systems (Fig. 4). High impacts with damage rate increasing for own and further systems was admitted by one fifth of enterprises when falling together with permanent default for more than a week. Whether short or long term absence of satellite data flow may cause higher or even irreversible impacts to a designated CI branch, is due to transaction speed of its business operations, and buffer time for activating means of resilience [8, 15]. According to experts, three time categories can be assigned to CI damages with high impact when caused by unbuffered breakdown of satellite data: (i) Instant damage will affect public traffic (esp. aviation, metro, railway) and communication within 1-2 hours, including emergency and financial transfer systems; (ii) mid-term, logistics and transport will be concerned within 2 days (esp. port handling and connected systems); (iii) for long-term, all satellite based observation systems (e.g. climate and maritime programs) will be involved while no exact time line can be estimated, as some alternative solutions can be activated meanwhile. When bringing in alternative solutions, it has to be considered that this again causes downgrading effects.

4 RISK DEFENSE ARCHITECTURE FOR SATELLITE BASED CIP

An interface analysis extracted from the different target group interviews, provides a model for an idealized risk defense architecture (Fig. 7). The general idea is to integrate the existing responsibilities and individual interests of each action group into a communicative structure in order to create an overall satellite based CIP awareness. Interactive and transparent, satellite data user and CIP advisors shall participate in a common risk assessment process to provide propositions on expert level. All of the reflected concerns and inputs from users', providers' and manufacturers' side shall be considered by the ESA Council and the EC [25]. Corresponding to decree ECIP 2013 this defense architecture is to build up and strengthen resilience against any risks of satellite based data failure.

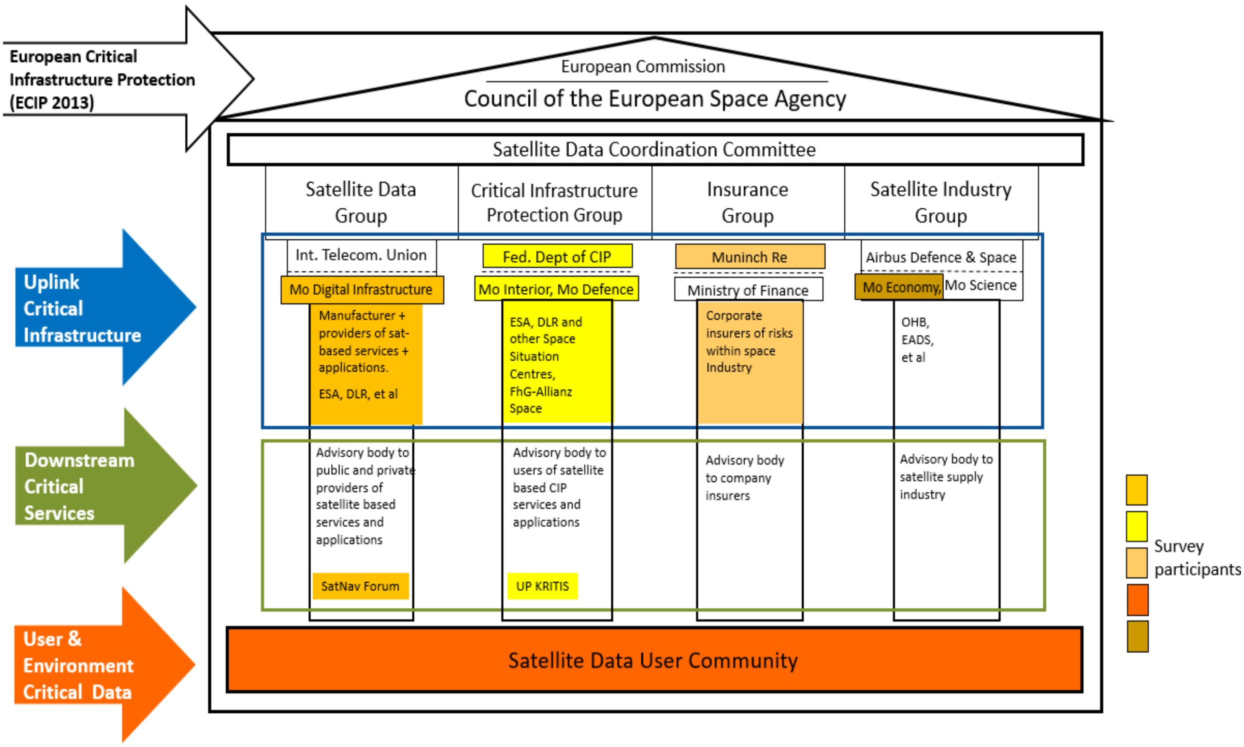

European Critical Infrastructure Protection (ECIP 2013)
European Commission
Council of the European Space Agency
Satellite Data Coordination Committee
Satellite Data Group
Critical Infrastructure Protection Group
Insurance Group
Satellite Industry Group
Int. Telecom. Union
Mo Digital Infrastructure
Manufacturer + providers of sat-based services + applications.
ESA, DLR, et al
Fed. Dept of CIP
Mo Interior, Mo Defence
ESA, DLR and other Space Situation Centres, FhG-Allianz Space
Muninch Re
Ministry of Finance
Corporate insurers of risks within space Industry
Airbus Defence & Space
Mo Economy, Mo Science
OHB, EADS, et al
Uplink Critical Infrastructure
Downstream Critical Services
User & Environment Critical Data
Advisory body to public and private providers of satellite based services and applications
SatNav Forum
Advisory body to users of satellite based CIP services and applications
UP KRITIS
Advisory body to company insurers
Advisory body to satellite supply industry
Satellite Data User Community
Survey participants

Fig. 7: Model for a risk defense architecture designed for satellite based CIP

5 CONCLUSIONS, TRENDS, RISKS

Examining satellite based CIs, the author supports an area-related and action-related scientific approach. The rather futile discussion to either approve satellite systems to CI Space sector or to CI Information Communication Technology sector (ICT) is settled by the fact that satellite systems are space bound which marks them as a spatially unique resource. The same argument applies to all other ICT-using CI-sectors, whether it concerns aviation (controlled airspace), media (public space) or ICT itself (virtual space).

With regard to the variety of active players concerned, there are multiple perspectives to be taken into account in order to build up comprehensive resilience: Daily users of applications, service providers, controllers and watch keepers in operation centres et al are located on different action levels but do have a common understanding for the subject examined here.

Dependency from satellite data in case of a shortfall means loss of timing and accuracy with massive impact possible: Overflow and blockage of trading centres and reloading points, followed by further spatial problems such as waste removal. Especially mass emergencies in metropoles do afford extraordinary means and capabilities for crisis management which generate additional costs to economy and society.

Last, some economic trends and risk assessments gained from the survey:

- Commercialization of satellite based CI is seen as a trend by 77% of the survey participants.
- 50% of those questioned, do see an increasing risk along with the growth rate of satellite based data applications for critical infrastructure.
- 85% of companies and institutions are depending from satellite based data, while
- 71% will need equivalent substitute in case of a shortfall of satellite based data.
- 74% of companies confirm downgrading in production numbers and quality if satellite data applications were not available.

REFERENCES

[1] European GNSS Agency (2015). *Market Report.* Available at: http://www.gsa.europa.eu/system/files/reports/GNSS-Market-Report-2015-issue4_0.pdf

[2] ESA (2015). *Earth Observation Market Development.* Available at: http://www.amsat.it/ESA_ESRIN_Earth_Obser.pdf

[3] GAO (2008). *United Sates Government Accountability Office, Environmental Satellites: Polar-orbiting Satellite Acquisition Faces Delays: Decision Needed on Whether and How to Ensure Climate Data Continuity.*

[4] GAO (2002). *United Sates Government Accountability Office, Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed.*

[5] Enderle, W., ESA (2015). *Satellitennavigation - Kritische Infrastruktur von morgen?* Fachvortrag zum Kongress global Navigation meets Geoinformation, Mai 2015. Available at: http://www.cesah.com/fileadmin/Dokumente/Vortr%C3%A4ge_GNmGI_2015/1_-_Werner_Enderle.pdf

[6] BMI (2009). *Bundesministerium des Inneren Nationale Strategie zum Schutz kritischer Infrastrukturen (KRITIS-Strategie).*

[7] Lenz, S. (2009). *Vulnerabilität kritischer Infrastrukturen.*

[8] EUROPEAN COMMISSION (2013). *Commission Staff Working Document on new approach to the European Program for Critical Infrastructure Protection Making European Critical Infrastructure more secure.* SWD, 2013 318 final.

[9] Remuss, N.-L. (2011). *The Use of Space Resources in the Fight against Piracy.* European Journal of Navigation 9(1), pp. 19 - 26.

[10] Mutscheler, M. (2013). *Risiken für die Weltraumnutzung.* Stiftung Wissenschaft und Politik Transatlantische Risikogovernance.

[11] BSI **(**2015). *Bundesamt für Sicherheit in der Informationstechnik KRITIS-Sektorstudie Informationstechnik und Telekommunikationstechnik (IKT).* Öffentliche Version - Revisionsstand 5. Februar 2015.

[12] Heller, M. (2002). *Interdependencies in Civil Infrastructure Systems.*

[13] Kotzanikolaou, P. (2013). *Cascading Effects of Common-Cause Failures on Critical Infrastructures.*

[14] Nieuwenhuijs, A., Luiijf, E. und Klaver, M., (2008). *Modelling critical infrastructure dependencies*.

[15] EUROPEAN COMMISSION (2014). *Joint Working Centre, Space Weather and Financial Systems: Findings and Outlook.*

[16] Royal Academy of Engineering (2005). *Extreme space weather: impacts on engineered systems and infrastructure.*

[17] International Space University & University of South Australia (2014). *The 2014 Southern Hemisphere Summer Space Program.*

[18] OECD (2014). Space 2030 – *Exploring the Future of Space Applications.*

[19] OECD (2011). *The Space Economy at a Glance.*

[20] cesah (2015). *Centrum für Satellitennavigation Hessen*. Available at: www.cesah.com

[21] Creswell, J., u. Clark, P. (2007). *Designing and Conducting Mixed Methods Research.*

[22] Strauss, A., Corbin, J.M. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.*

[23] ESA (2016). *Data User Element.* Available at: http://dup.esrin.esa.it/

[24] Wood, P. (2012). *Cyber Attacks: An Emerging Threat to Satellites.* Available at:
https://www.youtube.com/watch?v=ta8hydqBYzw
http://flightsoftware.jhuapl.edu/files/2012/FSW12_Wood.pdf

[25] Hobe, S. (2006). *Die sicherheitspolitische Dimension der Raumfahrt. The EC/EU in Space, Cooperation between ESA and EC**:** The cases of Galileo and GMES.*

TOWARDS MEASURING THE LINKAGE RISK IN INFORMATION FLOWS

Christoph Bier[1] and Jürgen Beyerer[2]

[1] *christoph.bier@iosb.fraunhofer.de* [2] *juergen.beyerer@iosb.fraunhofer.de*
Fraunhofer IOSB, Fraunhoferstraße 1, 76131 Karlsruhe, Germany

Abstract

Information is becoming one of the most important assets in our modern world. It must be protected in industry, infrastructures, government, and armed forces. Classified information can handled according to well-established access control models. However, the free flow of information is a precondition for decision-making and efficient processes in many cases. Hence, lots of information is not classified by default or on such a low classification level that many people and systems have access to it. Due to sophisticated analysis methods, this poses risks.

We present a set of unlinkability metrics to determine the overall linkage risk of a collection of information processes. The metrics cover the linkage of storage location, of information flows, of sensitive data, and of sensitive data with (intelligence) sources. We developed a process simulator that allows comparing different process designs a priori and at runtime.

Keywords: Unlinkability; information flow; risk measurement; data protection; classified information.

1 INTRODUCTION

Information is becoming one of the most important assets in our modern world. It must be protected in industry, infrastructures, government, and armed forces.

Classified information can be handled according to well-established access control models. For instance, the Bell-LaPadula model [1] defines two major rules: no read-up and no write-down. Hardware based approaches are available as well. Red-black networks restrict the information flow to flows from the black to the red segment.

However, the free flow of information is a precondition for decision-making and efficient processes in many cases. Hence, lots of information is not classified by default or on such a low classification level that many people and systems have access to it. Due to sophisticated analysis methods, this poses risks. Valuable information can be derived by linking low classified and unclassified information.

The propagation of higher classifications is no solution as well. If more information is highly classified, more people need the clearance for these classification levels. Sometimes people get access to lots of top secret information without any obvious need (e.g., in the Snowden case). Therefore, the aggregation of information in systems and roles must be reduced.

We present a set of unlinkability metrics to determine the overall linkage risk of a collection of information processes. The metrics cover the linkage of storage location, the linkage of information sharing and transfer, the linkage of pre-defined sensitive data, and the linkage of sensitive data with (intelligence) sources. Different process designs can be compared a-priori and at runtime. The most unlinkable one can be selected. Others can be ruled out if necessary.

The metrics are based on an analysis of information flows. Therefore, we developed a simulator for exemplary process instantiations. This simulator can easily be fed with all aspects of the unlinkability model. On top, we present a visualization tool to make the most risky information flows visible to human decision makers.

The remaining part of the paper is structured as follows: In Sec. 2, we discuss existing approaches on measuring unlinkability. In Sec. 3, we present generalized and flexible metric for unlinkability, especially for the linkage risk between systems, sensitive data and (intelligence) sources. We discuss how to determine information flow entropy in Sec. 4. Hereafter, we introduce our simulator for information flows in Sec. 5. This simulator is used for the visualization presented in Sec. 6. In the final section, we conclude with some remarks on future work.

2 RELATED WORK

A reference work on terminology for unlinkability is the continuous updated publication by Pfitzmann and Hansen [2]. Bohli and Pashalidis [3] formalised a hierarchy of unlinkability notions based on a model similar to IND-CPA. They define unlinkability on equivalence relations only.

The concept to describe anonymity based on information theory was brought up by Serjanov and Danezis [4]. Dias et al. [5] added the normalization of the anonymity metric. Steinbrecher and Köpsel [6] transferred the concept to unlinkability. Pashalidis [7] generalised the notion from equivalence relations to arbitrary binary relations.

3 A METRIC FOR UNLINKABILITY

Requirement for the definition of unlinkability is a model of the part of the reality, for which we want to measure unlinkability. In particular, the entities E, their relations R have to be defined. The attacker, from whose perspective unlinkability is dermined, must be described.

The linkage of entities can be defined over any mathematical relation R. A linkage relation R is a subset of the cartesian product of $n \geq 2$ subsets $E_1, \dots, E_n \subseteq E$ of the set of all entities E. It is common to choose the entity sets of the entity classes.

Unlinkability can be defined in an absolute or relative way. Absolute unlinkablity of two or more entities means that from an attackers perspective, the attacker cannot distinguish if the entities are in a certain relation to each other or not [2]. In situations where a certain degree of linkability is unavoidable but minimization of linkability is of interest, this kind of metric does not help.

Relative unlinkability compares the uncertainty of the attacker A regarding the true linkage relation R_τ after interaction with the system Σ^{A} with the uncertainty before the interaction. The uncertainty before the interaction depends on the *background knowledge* (*a priori knowledge*) of the attacker. The attacker can make *observations* I during the interaction with Σ^{A}. The union of background knowledge and observations is the a *posteriori knowledge*.

Entropy together with Bayesian probability (probability as *degree of belief*) has been established as the state of the art to measure relative unlinkability. Be X a random variable over the set of candidate relations $\mathcal{R}$. The attacker assigns a probability $P(X = R)$ to every candidate relation $R \in \mathcal{R}$ before and after interaction with Σ^{A}. $P(X = R)$ is the assumed probability that R is the true linkage relation R_τ between $E_1, \dots, E_n$.

Therefore, the entropy of the a priori as well as the a-posteriori knowledge of the attacker is given as:

$$H(X) = -\sum_{R \in \mathrm{R}} P(X = R) \log_2 P(X = R) \qquad [\mathit{bit}]$$

under the assumption that $P(X = R) \log_2 P(X = R) = 0$ for $P(X = R) = 0$.

The degree of unlinkability is the ratio between the a priori and the a posteriori entropy, given the observation I:

$$\Delta(X, I) = \frac{H(X \mid I)}{H(X)}$$

As we want to compare different process designs, the background knowledge is set to the observations I_{Ref} an attacker can make when interacting with the reference system, resulting in $H(X|I_{Ref})$ in the denominator and $H(X|I_{Ref}, I)$ in the numerator. As the a posteriori observations might even out the assumed probability distribution, this may result in $\Delta(X, I) > 1$ which is undesirable for a well-defined unlinkability metric. Hence, we define the normalized degree of unlinkability.

The normalized degree of unlinkability considers all possible attackers. As it is always possible to come up with an attacker with no background knowledge, even given the reference system, who can also not observe anything in the considered system, the normalized degree of unlinkability is

$$\left||\Delta|\right| = \min_{A}(\{\Delta(X_A, I_A)\}) \in [0; 1]$$

The set of relevant attackers depend on the given scenario. In most cases, it includes the systems taking part in data processing and/or the operators controlling them. Their background knowledge is often defined by the information flows through the respective system based on the reference processes as well as on common knowledge on process design.

We identified the following four relations as most relevant for measuring unlinkability in the setting of classified information:

- The identification relation $R^{ID} \subseteq D \times O$, which expresses if sensitive data $d \in D$ is linked to a particular (intelligence) source $o \in O$.
- The equivalence relation $R^{EQ} \subseteq D \times D$, which expresses if two pieces of sensitive data $d_1, d_2 \in D$ are related to the same (intelligence) source or other relevant attribute.
- The storage relation $R^{SG} \subseteq S \times D$, which characterizes for all systems $s \in S$ if they have processed and/or stored a certain sensitive data $d \in D$.
- The flow relation $R^{FW} \subseteq S \times S \times D$, which represents for two systems $s_1, s_2 \in S$ if they have shared a certain sensitive data $d \in D$.

The last relation is especially important to derive to which degree a given process design supports the separation of concerns when handling classified data.

4 DETERMINING INFORMATION FLOW ENTROPY

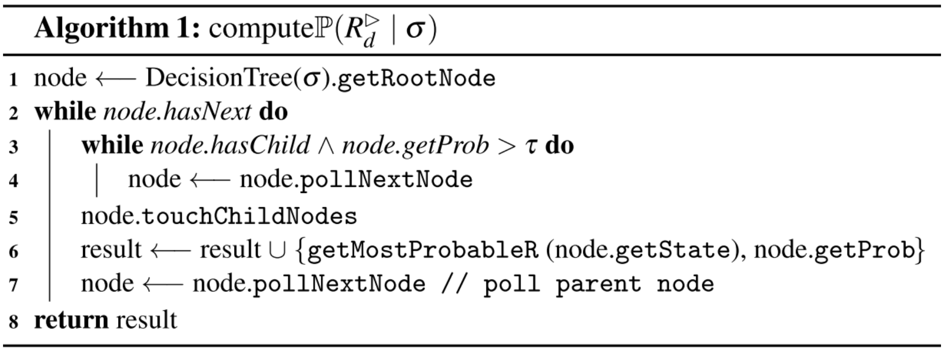
The calculation of all possible probabilities $P(X = R)$ is, similar to the interference in Bayesian networks, NP-hard. In worst case, the computational complexity of calculating all probabilities of a binary relation $R \subseteq S \times S$ is in $O\left(2^{|S| \cdot |S|}\right)$. For the ternary flow relation, the situation is even worse.

To cope with the ternary flow relation, the assumption of independent data flows helps. We assume that any flow of data from one system to another is independent from the flow of other data. In reality, this might not always be the case. Nevertheless, as it is possible to aggregate highly correlated data in one $d \in D$ by definition, the assumption is justifiable. Entropy is additive for independent subsystems. Therefore, we can calculate the total degree of unlinkability of R^{FW} based on the degree of unlinkability per data:

$$H(X^{FW}) = \sum_{d \in D} H(X_d^{FW})$$

Still, we cannot compute $H(X_d^{FW})$ within reasonable time. Fortunately, a heuristic solution is possible, if we add one additional assumption: All data has exactly one source. This assumption is reasonable. If one would collect data from different sources, we would simply not consider it as the same data, either because of the lack of knowledge or because of the different meta-properties of the data. Given this assumption, we can compute the probabilities along the decision tree up to a certain threshold τ. The data source is the root node. The threshold defines the minimum probability taken into account.

Algorithm 1 (Fig. 1) shows how depth-first search in the decision tree works. The tree is traversed until the probability falls below the threshold (line 3). If the the current node no leaf, the remaining subtree will not be searched further (line 5). The probability looked for is directly given by the probability of the subtree. Subsequently, the relation with the highest probability is selected as the representative of the subtree (line 6).



Algorithm 1: compute$\mathbb{P}(R_d^{\triangleright} \mid \sigma)$

```
1 node ⟵ DecisionTree(σ).getRootNode
2 while node.hasNext do
3     while node.hasChild ∧ node.getProb > τ do
4         node ⟵ node.pollNextNode
5     node.touchChildNodes
6     result ⟵ result ∪ {getMostProbableR (node.getState), node.getProb}
7     node ⟵ node.pollNextNode // poll parent node
8 return result
```

Figure 1 Traversing the Decision Tree

We found out that is approach is feasible, depending on the number of systems, up to a threshold of 10^{-6}. As the heuristic systematically underestimates the real entropy, we can provide a guaranteed unlinkability. For small system sets the underestimation is well below 0,01.

5 SIMULATING INFORMATION FLOWS

We need to define and simulate prototypical processes to compare different process designs a priori and at runtime. Input data for a simulation are the sets of the model (data, systems, and (intelligence) sources) and a description of possible information flows. Our simulator reads all these inputs as csv-files (lists of comma-separated values). Afterwards, the process is simulated and the linkage risk for the respective instantiation is measured. The syntax to describe information flows is as follows:

Line = DataInitLine | FlowLine | ClearLine | TimeLine ;

DataInitLine = “d”, Number, { “,”, Number }, “>”, Number ;

FlowLine = Number, { “,”, Number }, “>”, Number ;

ClearLine = “c”, Number ;

TimeLine = “t”, Number ;

Number = DigitNotNull, { Digit } ;

Digit = “0” | DigitNotNull ;

DigitNotNull = "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9" .

A DataInitLine defines which data is collected by which system, a FlowLine describes the information flows between systems, while a ClearLine states that data must be deleted from a certain system, resulting in a posteriori gaps in the processing chain. A TimeLine changes the internal clock of the simulator by designating a UNIX time stamp. All data numbers and system numbers used in the flow definition, must also be defined in the respective set files.

The more scenarios are simulated, the better is the validity and the significance of the unlinkability determined. If the results differ from scenario to scenario, the scenarios have to be weighted according to their relevance. As the unlinkability metric is ordinal, one has to be careful not to simply add up the results of different scenarios.

6 VISUALIZING PROCESSES FOR DECISION MAKERS

For simulations, but especially at runtime, it is helpful to visualize information flows to increase the understanding of decision makers towards unlinkability metrics. We developed a web application to inspect the information flows (Fig. 2).

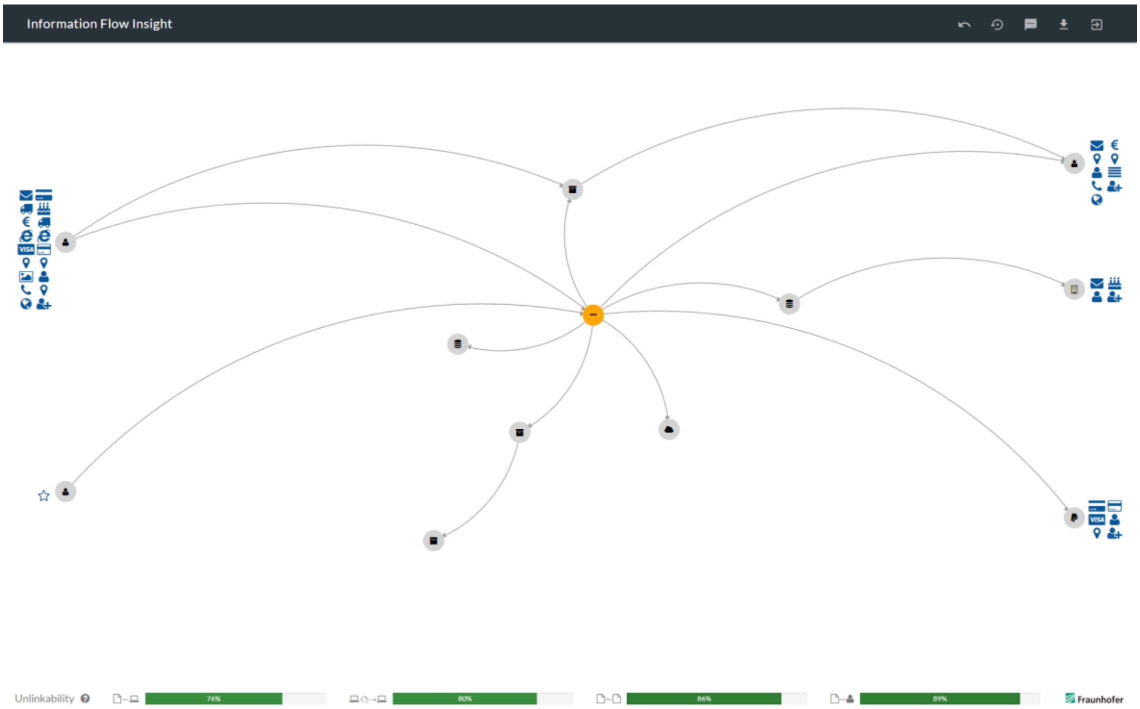


Figure 2 Information Flow Visualization

On the left hand side, one can see the (intelligence) sources. In the middle, the information flows within the organization are visualized. On the right hand side, other organizations or departments, where data has been transferred to, are listed. At the bottom, the unlinkability metrics for the current process design are presented.

7 CONCLUSION

We described an unlinkability metric for the linkage of storage locations, of information flows, of sensitive data, and of sensitive data with (intelligence) sources based on information theory. These metrics were formally introduced. An implementation for information flows, including a simulator and visualizations was presented. These metrics, especially when easily accessible via the web application, allow the improvement of handling of sensitive data in various domains.

REFERENCES

[1] Bell, D. Elliot; La Padula, Leonard J. (1973). *Secure Computer Systems: Mathematical Foundations.* MITRE Technical Report 2547(I).

[2] A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, v0.34.

[3] Bohli, Jens-Matthias; Pashalidis, Andreas (2011). *Relations among privacy notions.* ACM Transactions on Information and System Security, 14(1), p. 1–24.

[4] Serjantov, Andrei; Danezis, George (2003). *Towards an Information Theoretic Metric for Anonymity*. In: Proceedings of the 2nd international conference on Privacy enhancing technologies. LNCS, p. 41–53.

[5] Díaz, Claudia; Seys, Stefaan; Claessens, Joris; Preneel, Bart (2003). *Towards Measuring Anonymity.* In (Dingledine, Roger; Syverson, Paul, Hrsg.): 2nd International Workshop on Privacy Enhancing Technologies (PET 2002). Springer Berlin Heidelberg, p. 54–68.

[6] Steinbrecher, Sandra; Köpsell, Stefan (2003). *Modelling Unlinkability*. In: 3rd International Workshop on Privacy Enhancing Technologies (PET 2003). Springer, p. 32–47.

[7] Pashalidis, Andreas (2008). *Measuring the Effectiveness and the Fairness of Relation Hiding Systems*. In: Proceedings of the Asia-Pacific Services Computing Conference (APSCC ’08). p. 1387–1394.

SANDBOX EVASION THE EASY WAY - EVADING MAJOR COMMERCIAL SANDBOXES

Martin Clauß and Raphael Ernst

{martin.clauss,raphael.ernst}@fkie.fraunhofer.de
Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Fraunhoferstr. 20, 53343 Wachtberg-Werthhoven

Abstract

Sandboxes execute malware in an isolated environment and decide, based the samples behavior and metadata, whether it is malicious or benign. Sandbox evasion techniques can be found in many current malware samples. As a response to that fact, security vendors include techniques to detect evasive behavior in their sandbox products. In this paper we investigate sandboxes with respect to their capabilities to analyze malware with evasive behavior. Our results show shortcomings in all tested sandboxes with different evasion techniques and simple implementations.

Keywords: Sandbox Evasion, Evasive Malware

1 INTRODUCTION

Malware has evolved dramatically in recent years. Although “Love Letter” and “Code Red” infected a huge amount of computers (in 2000 and 2001 respectively) when they were released, their infection and spreading techniques were simple and easy to detect. Nowadays malware uses sophisticated approaches to overcome a variety of anti-malware techniques. Packers hide the actual program code such that static analysis becomes more complicated, polymorphic malware weakens the effectiveness of signature based approaches, and professional attackers buy zero-day-exploits for well-known software. Consequently, the security industry addressed these problems with a new approach: Sandboxes. These dedicated security appliances run potential malware, analyze its behavior and classify a potential malware sample based on the observations. Attackers quickly adapted and tried to evade these systems causing an arms-race between sandbox developers and malware authors. This arms-race lead to impressive sandbox technologies allowing solutions to run non-executed code branches, live patching of several functions, and almost fully transparent sandboxes. However, reports from security vendors show that sandboxes are still evaded and malware implements such features on a regular basis [1-5].

This paper presents test methods that can be used to investigate the sandbox analysis performance and shows attack vectors which may be used to evade a sandbox. These methods were tested against several commercial products. However, all products quickly evolve over time, so this work is just a snapshot of the current state of the art and should not be used as an indicator whether a certain product is “secure” or not. The primary goal of this paper is to create awareness of the possibility to evade sandboxes. Our study was organized two folded: We first analyzed the capabilities of available sandboxes as described by the vendors and picked five representatives for further analysis. Three of them were analyzed in greater detail.

The remainder of this paper is organized as follows: Section 2 gives a brief overview about the different sandbox types, followed by evasion techniques commonly used in

Section 3. Our experiment setup and the results are given in Sections 4 and 5 before the paper is concluded.

2 SANDBOXES

Sandboxes evolved over time and several different types exist. Although, they are not limited to certain operating systems (OS), we focus on sandboxes providing a Microsoft Windows environment due to its widespread use. The decision whether a sample is good- or malware depends on the monitored behavior like system calls, access to files or network resources, and what the sample does with the acquired data. This information can be monitored on different levels and different ways. Early sandboxes emulated calls to the Windows API. They were limited in their ability to execute samples and easily to detect as they only provided a subset of the API. Furthermore, they had no information about data processing between API calls. Sandboxes hooking system functions could run much more samples as they run a full OS but keep their limited vision as they monitor only a subset of the available functions [6, 7]. A very similar approach uses kernel level hooks. As the malware have to run in kernel space to detect those hooks (i.e. the privilege to read kernel memory) it is harder to detect such sandboxes. However, all mentioned sandboxes run inside or as part of the OS, are easy to detect, and limited in their monitoring capabilities [8]. Therefore, some recent sandboxes stepped outside of the OS. Instead they run an unmodified a fully emulated or virtualized guest and monitor processor instructions as well as memory access, making such sandboxes almost fully transparent [8-10]. This technique is far more complex as it cannot rely on OS functions but has to translate memory access and processor instructions to events in the OS, e.g., file access. This problem is called the semantic gap [8, 11].

3 EVASION TECHNIQUES

Previous works on evasion techniques focus on ways to prevent evasions. Therefore, evasions are typically the motivation in these works and we identified five main categories: (1) stalling, (2) sandbox detection, (3) system virtualization detection, (4) human being detection, and (5) multi stage attacks. Related topics (not covered in this paper) are obfuscation and anti-debugging techniques [12].

Stalling is an old approach to evade sandboxes. The idea is to postpone the malicious code execution until the sandbox terminates [8, 13]. This means that malware can either wait or execute unsuspicious computations. We name the first variant sleep evasion and the second busy code evasion. A simple example for the sleep evasion is a call to an OS sleep function (e.g. Sleep() from kernel32.dll in Windows). Instead of calling sleep() once with a duration of k time units we can call sleep() multiple times so that the sum of the shorter durations equals to k (e.g., calling sleep(1) twice instead of calling sleep(2)). Modern sandboxes can shorten the real time that elapses when a sleep() function is called. However, some sandboxes define a lower bound l for the duration k of the sleep() function that should be shortened. In this case the analysis can be evaded by calling sleep(m) multiple times with m < l. Although, it looks as if sandbox vendors can fix this problem by a simple summation of the sleep time, it is much more complicated in real world scenarios. Attackers might add arbitrary code between two sleep calls or cause (intentional) runtime exceptions when sleeps are shorter than expected. Another way to postpone the execution of malicious code is to wait for an OS event like a process creation (e.g., like starting a program). Targeted attacks might further optimize this attack by combining events specific for the targeted victim, e.g., uncommon programs. Therefore, sandboxes need some fine tuning for the specific environment.

Another stalling technique to evade analysis is the busy code evasion. For that technique we first add some code that does legitimate and unsuspicious computations before executing malicious code. As an example we implemented the Slow Sort algorithm [14] for the busy code part of the program. Sometimes malware uses remote services on the Internet (e.g. an attacker-controlled web service) to query when to start malicious actions. A discussion about challenges from a sandboxes' perspective is given in [15].

Malware with **sandbox detection** checks if it is executed in a sandbox environment. If a sandbox is detected benign code is executed or the sample terminates. The prevalent detection mechanisms vary greatly, such that some malware samples search for particular Windows licenses, drivers, API hooks, processes, files and directories, or system configurations identifying the system as a sandbox [16, 17]. Tools like Anticuckoo [18], Pafish [19], and sems [20] demonstrate some of those techniques. Those techniques can be summarized under the term fingerprinting.

Closely related to sandbox detection is the system **virtualization detection** [17, 21-24]. Both share the same idea. However, system virtualization detection tries to detect virtualized systems as they are commonly used in sandboxes. Due to the increasing use of virtualization it is likely to expect to see less malware implementing those techniques as valuable targets might be omitted.

Human being detection tries to distinguish analysis systems from target machines by monitoring human behavior like mouse movement and keyboard input. If those human interaction signs are missing, no malicious code gets executed. [1] shows some of these approaches seen in 2014.

Multi stage attacks pass through multiple steps before they execute the malicious code. One common way keeps the malware dormant until the next reboot. In this case the sample adds itself to the Autorun. After the reboot it starts the malicious part of the program code. Another approach downloads the malicious code from a remote server. Therefore, the authors can prevent known analysis systems from getting the sample and offer benign code instead. Those benign programs are often called downloaders.

4 EXPERIMENTS

For the majority of tests we wrote Visual Basic Scripts (VBS) that we converted to PE (Portable Executable) files using the commercial tool ScriptCryptor [25]. The remaining tests were written in C/C++ and C#. After submitting our test programs to the sandbox we used the sandbox's report (including screenshots) and the output files which our programs created to analyze the success or failure of our evasion. The following tests were executed:

Driver fingerprinting: We iterated through all drivers using WMI ("SELECT * FROM Win32_PnPSignedDriver") and looked for indicators such as the name of the sandbox's vendor. This test fails if sandbox drivers are found.

Directory and file fingerprinting: In this test we iterated recursively over directories such as C:\Windows including C:\Windows\System32 and the user's private folders (Downloads, Pictures, Documents etc.) looking for suspicious file or directory names. A focus was on driver files and Python files that could be an indicator for in-guest agents used by the sandbox to record execution data or simulate user behavior. This test fails if directories or files are found that allow an identification of the sandbox.

Named pipes fingerprinting: Some sandboxes create named pipes to communicate with the host OS (e.g., to save recorded data, cf. Cuckoo sandbox in early versions). In this test we enumerated all named pipes and did a manual analysis to find indicators of a sandbox. This test fails if named pipes are found allowing an identification of the sandbox.

Sandbox process fingerprinting: Sandboxes often use in-guest agents to monitor the API calls or to simulate user behavior (moving the mouse, clicking, scrolling, pressing keys and so on). Those agents (e.g., Python scripts or ordinary executables) can be detected during the analysis when iterating over all running processes. We dumped all processes into a file and analyzed it after the analysis was completed. This test fails if a process is found that allows an identification of the sandbox.

Virtualization/Emulation fingerprinting: For this test we tried to find indicators for a virtualized or emulated environment such as virtualized hardware components (e.g., network cards, hard disks etc.), BIOS information, registry keys and so on. This test fails if a virtual environment is detected.

Micro-sleep evasion: In this test we used a loop to execute multiple calls to Sleep() with a duration of 1 second. This test fails if the code after the sleep call(s) is not executed during the analysis.

```
' simple call to Sleep(), sleep for 60 seconds
WScript.Sleep(60 * 1000)

' multiple shorter calls to Sleep(), sleep for 60 seconds in total
For i = 1 To 1000
      ' Sleep for 60 milliseconds
      WScript.Sleep(60)
Next
```

Busy code evasion: For this test we implemented the Slow Sort algorithm. The code after this algorithm was used to indicate that the sandbox was able to detect the busy code and also able to skip that part of the code. This test fails if the code after the busy code is not executed during the analysis.

Create-process-event evasion: Here we used the script shown in listing below to wait for a web browser to be opened by the sandbox. We also searched the reports for indicators that the stalling was detected. This test fails if the code after the event-creation code is not executed during the analysis and the stalling is not mentioned.

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" & "\\" & strComputer &
"\root\cimv2")

strQuery = "SELECT * FROM __InstanceCreationEvent " & " WITHIN 1 WHERE
TargetInstance ISA 'Win32_Process'"
Set colMonitoredProcesses =
objWMIService.ExecNotificationQuery(strQuery)
```

```
' Wait for a new web browser (modify for arbitrary processes)
Do
      Set objLatestProcess = colMonitoredProcesses.NextEvent

      If (objLatestProcess.TargetInstance.Name = "chrome.exe" Or _
          objLatestProcess.TargetInstance.Name = "firefox.exe" Or _
          objLatestProcess.TargetInstance.Name = "iexplore.exe") Then
            ' Malicious activities here
            WScript.Quit(0)
      End If
Loop
```

Conditional evasion: Some sandboxes have a feature that allows them to analyze alternative branches when encountering a conditional branch based on environment information. For example, if the sample executes on a specific date the alternative branch would be all dates that are not equal to this specific date:

```
if today == 2016-12-24
      do_mailicious_actions()
else
      do_nothing_or_benign_actions()
```

Sandboxes with an alternative branch exploration feature are able to execute the code of the else branch despite that today is not equal to 2016-12-24. This allows the sandboxes to detect evasive behavior. The concrete test was a simple script that downloads a file and executes that file only after a specific date in the future. This means that the download should not happen but with an alternative branch exploration feature there should be a hint in the report that the download and the execution of the downloaded file would be executed after a specific date has been reached. This test fails if the malicious branch is not analyzed.

Reboot evasion: In this test we wrote a script that adds itself to the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run registry key. And only starts its activities after a reboot. This test fails if the sandbox does not reboot and continues the analysis.

In general it has to be mentioned that those test are easy to implement and not very sophisticated.

5 RESULTS

Test	Sandbox 1	Sandbox 2	Sandbox 3
Driver fingerprinting	failed	passed	passed
Directory and file fingerprinting	failed	passed	passed
Named pipes fingerprinting	failed	passed	passed
Sandbox process fingerprinting	failed	passed	passed
Virtualization/Emulation fingerprinting	failed	failed	failed
Busy code evasion	failed	failed	failed
Micro-sleep evasion	failed	failed	failed
Create-process-event evasion	failed	failed	failed
Conditional evasion	failed	failed	failed
Reboot evasion*	failed	failed	failed

* Reboot evasion has been addressed by multiple vendors since our first research.

6 CONCLUSION

In this paper we investigated major sandboxes with respect to sandbox evasion techniques. We wrote test programs implementing common evasion techniques and tested them against the sandboxes under investigation. The results show that it is possible to run a targeted attack using simple evasion techniques and evade the sandbox detection.

REFERENCES

[1] Sai Omkar Vashisht and Abhishek Singh. (2014, June) Turing Test in Reverse: New Sandbox-Evasion Techniques Seek Human Interaction. [Online]. https://www.fireeye.com/blog/threat-research/2014/06/turing-test-in-reverse-new-sandbox-evasion-techniques-seek-human-interaction.html

[2] JoeSecurity. (2016, April) Nymaim - Evading Sandboxes with API Hammering. [Online]. http://joe4security.blogspot.de/2016/04/nymaim-evading-sandboxes-with-api.html

[3] VMRay. (2015, September) Sandbox Evasion with COM by Malware in-the-wild. [Online]. https://www.vmray.com/sandbox-evasion-with-com-by-malware-in-the-wild

[4] Michael Rosen. (2016, March) Malware Sandbox Evasion Tactics and Countermeasures – Part 1. [Online]. https://www.bluecoat.com/company-blog/2016-05-03/malware-sandbox-evasion-tactics-part-1

[5] Joe Giron. (2015, Mai) Exposing Rombertik - Turning the Tables on Evasive Malware. [Online]. http://labs.lastline.com/exposing-rombertik-turning-the-tables-

on-evasive-malware

[6] Cuckoo, Cuckoo Sandbox Workshop on Blackhat US 2013: Cuckoo Sandbox, 2013.

[7] Thomas Mandl, Ulrich Bayer, and Florian Nentwich, Presentation on Virus Bulletin Conference: ANUBIS, 2009.

[8] Chrisopther Kruegel, Blackhat US: Full System Emulation: Achieving Successful Automated Dynamic Analysis of Evasive Malware, 2014.

[9] Carsten Willems, Ralf Hund, and Thorsten Holz, Technical Report TR-HGI-2012-002: CXPInsepector: Hypervisor-Based, Hardware-Assisted System Monitoring, 2012.

[10] Tamas K. Lengyel, Steve Maresca, and Bryan D. Payne, Proc. of the Computer Security Application Conference: Scalability, Fidelity and Stealth in the DRAKVUF Dynamic, 2014.

[11] Ulrich Bayer, Christopher Kruegel, and Engin Kirda, TTAnalyze: A Tool for Analyzing Malware, 2006.

[12] Peter Ferrie. (2011, May) The “Ultimate” Anti-Debugging Reference. [Online]. http://anti-reversing.com/Downloads/Anti-Reversing/The_Ultimate_Anti-Reversing_Reference.pdf

[13] Inoue Daisuke, Proc. Communications (ICC): Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware's Network Activity, 2008.

[14] Andrei Broder and Jorge Stolfi, Proc. SIAGACT: Pessimal Algorithms and Simplexity Analysis, 1984.

[15] Arunpreet Singh. (2014, November) Not so Fast my Friend - Using Inverted Timing Attacks to Bypass Dynamic Analysis. [Online]. http://labs.lastline.com/not-so-fast-my-friend-using-inverted-timing-attacks-to-bypass-dynamic-analysis

[16] Ulrich Bayer, Imam Habibi, Davide Balzarotti, Engin Kirda, and Christopher Kruegel, Proc. of Workshop on Large-Scale Exploits and Emergent Threats (LEET): A View on Current Malware Behaviors, 2009.

[17] Timothy Vidas and Nicolas Christin, Proc. of the Symposium on Information, Computer and Communications Security (ASIA CSS): Evading Android Runtime Analysis via Sandbox Detection, 2014.

[18] Github-User: David-Reguera-Garcia-Dreg. (2016, June) anticuckoo. [Online]. https://github.com/David-Reguera-Garcia-Dreg/anticuckoo

[19] Github-User: a0rtega. (2016, June) pafish. [Online]. https://github.com/a0rtega/pafish

[20] Github-User: AlicanAkyol. (2016, June) sems. [Online].

https://github.com/AlicanAkyol/sems

[21] Roberto Paleari, Lorenzo Martignoni, Giampaolo Fresi Roglia, and Danilo Bruschi, Proc. of the USENIX Conference on Offensive technologies (WOOT): A Fistful of Red-Pills: How to Automatically Generate Procedures to Detect CPU Emulators, 2009.

[22] Boris Lau and Vanja Svajcer, Journal in Computer Virology: Measuring virtual Machine Detection in Malware Using DSD Tracer, 2010.

[23] Peter Ferrie, Attacks on Virtual Machine Emulators.

[24] Xu Chen, Jon Andersen, Z. Morely Mao, Michael Bailey, and Jose Nazario, Proc. of Conference on Dependable Systems and Networks with FTCS and DCC (DSN): Towards an Understanding of Anti-Virtualization and Anti-Debugging Behavior in Modern Malware, 2008.

[25] Abyssmedia. (2016, June) ScriptCryptor Compiler. [Online]. http://www.abyssmedia.com/scriptcryptor/

MEASURING THE EFFECT OF HIDING MESSAGES IN JPEG FILES

Jonathan P. Chapman[1], Daniel Schmitz[2] and Elmar Gerhards-Padilla[3]

[1] *jonathan.chapman@fkie.fraunhofer.de*
[2] daniel.schmitz@fkie.fraunhofer.de
[3] elmar.gerhards-padilla@fkie.fraunhofer.de
Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE,
Cyber Analysis & Defense Dept., Zanderstr. 5, 53121 Bonn (Germany)

Abstract

In this paper, we provide an overview to our analysis of the effect of steganographically embedding messages in JPEG files. For our evaluation, we used a set of over 13000 images in different sizes that were subsequently converted into JPEG files with different quality settings. Our analysis shows that images containing messages embedded using the F5 and Outguess algorithms may be detected by observing the coefficient distribution for the respective image files. For the Steghide algorithm however, this may be difficult to achieve.

Keywords: steganography, JPEG.

1 INTRODUCTION

Targeted malware like Duqu [1] but also more general purpose malware like ZeusVM [2] or an unnamed malware discovered on compromised servers [3] hide their communications with their command and control servers by embedding messages in JPEG files. Hence, being able to detect such channels is no longer only a requirement to prevent data exfiltration from high security facilities but should concern all operators of computing infrastructure targeted by the named malware. With respect to the banking Trojan ZeusVM, this includes all end user PCs.

In this work, we lay the foundations for developing efficient methods to detect steganographic message exchanges in JPEG images. We evaluated the effect of embedding messages with three popular algorithms on a large database of JPEG images, including different sizes and quality settings. Our analysis shows paths towards efficient methods for detecting the presence of embedded messages but also shows the limitations of the approach.

The remainder of this paper is organised as follows: In section 2, we describe the required fundamentals of JPEG compression, it’s file format and some basic effects of JPEG compression. The following section provides a brief overview to the steganographic algorithms we used for our evaluation. We then go on to discuss our data set and finally the effect of embedding messages in JPEG files in section 4. The paper closes with a brief summary of our conclusions.

2 BACKGROUND

In this section, we briefly introduce the JPEG file format and compression standards. We deliberately omit details that may be important for general purposes but are not required to follow the analysis presented in this paper.

2.1 The JPEG File Format

The JPEG File Interchange Format (JFIF, commonly referred to as JPEG) is a file format designed to allow efficiently storing continuous-tone still images. This refers in particular to photographs. Here, JPEG files often require only a fraction of the bytes needed to store a bitmap representation of the same photograph while compression artefacts remain difficult to be seen. Additionally, users can decide to trade-off between file size and image quality by choosing an appropriate configuration when encoding their photographs. [4]

2.2 JPEG Compression Fundamentals

The JPEG compression's first step is to transform an image given in an arbitrary colour space into the three-channel YC_bC_r space. The Y or luma channel encodes the intensity or brightness of each pixel while the C_b and C_r or chroma channels carry the pixels' colour information. Monochromatic images only use the luma channel.

The picture is then split into discrete blocks of 8 by 8 pixels each. For each of these blocks and for each channel, the discrete cosine transform (DCT) yields a series of 64 coefficients. The first or DC coefficient stores the base colour for each pixel in the block. The remaining 63 coefficients, also referred to as AC coefficients, reflect the intensity of a cosine component each. When organising the coefficients in a matrix the entries on the left refer to components with a low horizontal frequency and the component's horizontal frequency increases as we move to the right. Similarly, the top row refers to a low vertical frequency component and the frequency increases as we move to the bottom of the matrix. Hence, as we move left to right and top to bottom in the matrix, the frequency represented by the respective AC coefficient increases. It is important to note that while changes in low frequency components are easy to see, the higher the respective frequency, the less obvious the change becomes to the human eye.

This is exploited by the following quantisation step. Using the quantisation table (DQT) stored in the JPEG file's header, each coefficient is divided by the respective entry in the quantisation table and then rounded to the nearest integer. When the respective entry in the DQT is 1, the coefficient is only rounded but as the value of the DQT entry increases, the granularity for the respective frequency component's coefficients becomes more and more coarse. Since JPEG is designed for continuous-tone images and the AC coefficients only store an offset to the base colour for the given block, large entries in the DQT usually result in most of the respective coefficients being rounded to zero.

2.3 Encoding

As described in section 2.2, each block is encoded as a matrix of integers. These matrices are converted into a stream of coefficients, storing the elements in the order reflected by Table 1. Then, run-length encoding is applied on this vector. Since the process discussed in section 2.2 results – for appropriately chosen values in the DQT – in long sequences of similar values for most blocks, this can significantly reduce the size of the image. As a last step however, Huffman coding is applied globally, possibly yielding an even smaller size for the image file.

2.4 Overview to the Effect of JPEG Compression on Their Coefficients

Table 1. Ordering of JPEG coefficients.

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

In this section, we briefly describe how the different JPEG compression settings discussed above affect the distribution of an image's coefficient values. As an example, we will use the picture shown on the left of Figure 2 – a photograph of a landscape taken with a high resolution (16 megapixels) camera and lossless format. In the centre of Figure 2, we see a 32 by 32 pixel excerpt from the image at its full resolution. The excerpt on the right hand side of the figure shows roughly the same region of the photograph but at about one tenth of the original resolution. Obviously, the low resolution excerpt is more diverse, showing not only sky and a larger part of a tree but also wheat. This illustrates a less intuitive effect of JPEG compression: When an image is reduced in size, the diversity in the blocks used for the discrete cosine transform increases. Hence, generally blocks from a low resolution image require more disk space than those of a high resolution image. However, a high resolution image file contains a significantly larger count of blocks and hence the size of the respective file will still be much larger than that of a low resolution version of the same image.

Figure 1 shows how lowering the quality setting for the JPEG compression of the 1.6 megapixel photograph discussed above affects the reproduction of the original image. The two excerpts on the left, from the original and the 100% quality JPEGs, are practically indistinguishable. The centre picture (75%) already shows visible artefacts while most details are lost in the excerpts on the right hand side, which were extracted from 50% and 25% quality JPEG files.

Figure 3 indicates how these changes affect the underlying coefficient distributions. It shows the coefficient distribution at offset 1, i.e. for the first AC coefficient, of our sample image in qualities 100% and 75%. Non-surprisingly, while the mode for both distributions is zero, it makes up for only about 10% of the values for the high quality image while 40% of the lower quality's coefficients were rounded down to zero. Also, the high quality image covers a much larger part of the spectrum.

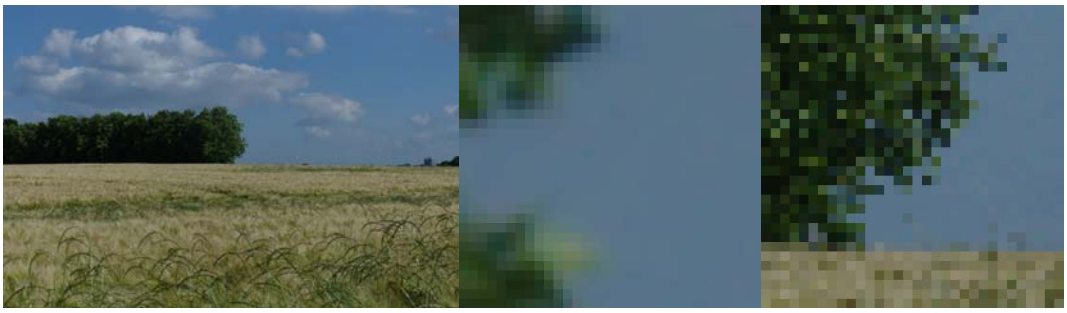


Figure 2. A photograph of a landscape (left) and two 32x32 pixel excerpts from the

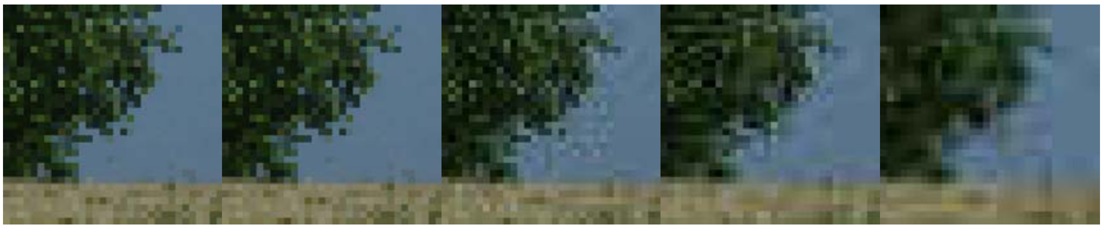


Figure 1. The same 32x32 pixel excerpt from a photograph across different JPEG quality levels.

3 STEGANOGRAPHIC METHODS FOR EMBEDDING MESSAGES IN JPEG FILES

There are several approaches which may be followed to embed messages in JPEG files. A simple one would be to add messages after the end of image marker indicating the end of the JPEG file. While decoders generally ignore this data, this approach would be straightforward to detect. This is the method used by ZeusVM [2].

Another method would be to exchange messages through EXIF metadata tags that may be included in JPEG files, like the malware described by Cid [3]. To hinder detection, these would have to replicate the data used for legitimate purposes, resulting in a very low bit rate per file exchanged. This could trigger a detection mechanism designed to identify unusually large volumes of data exchanges.

Hence, our work focuses on approaches that embed messages in the AC coefficients stored in JPEG files. While giving a detailed description of the approaches considered below, we briefly describe their commonalities in this paragraph. Since modifying the DC coefficients would have a particularly significant impact on the decoded images, all approaches restrict themselves to the AC coefficients. For the same reasons, the algorithms usually just add or subtract a value of one from a given coefficient.

While low frequency AC components may also have a strong impact on the decoded image, there are limitations with respect to avoiding them for the embedding. E.g. for a low quality image, most coefficients and in particular those corresponding to high frequency components are zero, hence here only low frequency AC coefficients can be used without creating a very suspicious pattern in the encoded file. In the following sections, we briefly describe three algorithms we considered for the study presented in this paper.

3.1 F5

The F5 algorithm [5] embeds messages in the quantised coefficients of a JPEG file. First, they use a password to derive a pseudo-random sequence traversing the coefficients. Hence, the coefficients that will subsequently be modified will not occur in a sequence but will be spread randomly across the image. Second, they use the matrix encoding scheme. This allows them to store several bits of a message by modifying only a small number of bits in the image. These bits however need to be part of a larger group of modifiable bits in the image, i.e. they trade capacity for secrecy. For the coefficients that need to be modified, the value of the least significant bit (LSB) is inspected and modified, if it does not correspond to the value needed to encode the message. Here, a zero in a message is stored as an even number (LSB is zero) and a one as an odd number (LSB is one) for positive coefficients. For negative coefficients, this relationship is reversed, i.e. an odd LSB refers to a zero in the hidden message.

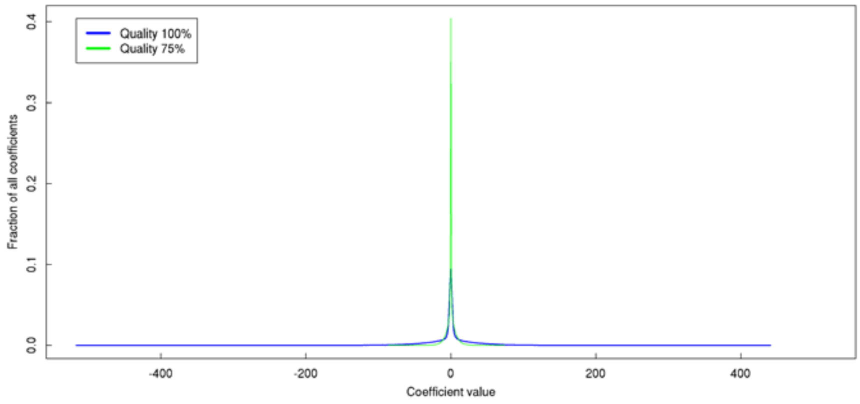


Figure 3. A comparison of coefficient distributions for different JPEG qualities.

3.2 Outguess

The Outguess algorithm [6] first embeds a 32 bit configuration vector in the cover medium, choosing non-zero offsets between its bits pseudo-randomly. To encode the message, again offsets are chosen at random. However, this time the offsets are chosen in relation to the number of remaining message bits and using only up to 50% of the bits that can be used for the embedding. Hence, the message bits are roughly evenly distributed across the medium and at least as many bits may be changed as already have been changed in the embedding.

With respect to JPEG images, the latter fact is used by Outguess to counteract the changes in the distribution of the coefficients inflicted by embedding the message. For every LSB changed, an adjacent bit is flipped into the other direction. I.e. when an odd coefficient is changed into an even one, a nearby even coefficient that was not used for embedding a message bit is changed into an odd one.

3.3 Steghide

Finally, Steghide [7] maps the cover medium onto a graph where each vertex of the graph corresponds to several samples of the cover medium which need to be changed to embed the message. These vertices are connected with edges, if their sample values can be exchanged to obtain the necessary changes to the cover medium to embed the respective message. For the vertices for which such a matching cannot be achieved, a single sample in the cover medium is changed to achieve a matching. In the data used for the evaluation presented in [7], this occurred only for 3% of the vertices.

4 ANALYSIS OF THE EFFECT OF STEGANOGRAPHICALLY EMBEDDING MESSAGES IN JPEG FILES

4.1 Data Set

The configuration of the JPEG compression used to store an image has a significant impact on the coefficient distribution of the encoded image, as discussed in section 2.4. Hence, we gathered a large data of high resolution photographs which were provided in a lossless data format like DNG, NEF, TIFF or PPM. We then converted these images into JPEG files with different configurations for the compression.

Our initial source data set consists of 5921 files. We separated these into three classes. “Large” includes all files with a resolution above 10 megapixels and contains 2109 files. The “medium” files have a resolution between 2 and 10 megapixels. In addition to the 3171 files that were already provided in a corresponding resolution, we resized the 2109 images in the “large” class to fit into this set, adding up to a total of 5280 files. Finally, only 641 images of the source set provided in a 2 megapixel or less resolution. Hence, we resized images from the other two sets to fit into this class, yielding the same count of files as in the source data set. To avoid introducing any biases, we drew the width and height for the resized images from a large set of JPEG files retrieved through search engines for images and cropped the source images to the respective aspect ratio, if necessary. All classes combined, our data set includes 13310 images.

We converted these images into sets of JPEG files with their quality set to 100%, i.e. with a DQT only consisting of ones, 90%, 80% and 70% respectively. Additionally, we used a setting of 75% to provide a base for comparing Outguess images against their cover media since its reference implementation only supports this quality setting.

4.2 Measuring the Effect of Embedding Messages

In this section, we discuss the effect of embedding messages in JPEG files for different algorithms. For each file in the cover set and for each algorithm, we embedded a message with a length of 0.2 bits per non-zero bit in the cover file. To illustrate the effect, we designed a plot which we will refer to as “centre of mass plot” or mass plot for short. Figure 4 shows two mass plots for comparing the coefficient distributions for JPEG files before and after embedding messages with the F5 algorithm. For a given value, the plot reflects the fraction that value takes up of all coefficients at a given offset. It shows the median for that fraction over all images in the respective data set as a dashed line. Solid lines indicate the border between the first and second or third and fourth quartile. Thus, in a centre of mass plot, we can easily see in which range the fraction for 50% of the image files lies (between the solid lines) and also where to expect the upper and lower 25% of those fractions (above or below the solid lines).

In the following sections, we will discuss the main findings for the individual algorithms, starting with F5. The next section describes the results for embedding messages with Outguess and finally, we take a brief look at the effect of doing so with Steghide.

4.2.1 F5

Figure 4 shows mass plots for the luma channel of the “large” data set with a quality of 100% before and after embedding a message with the F5 algorithm. The graph on the left of Figure 4 illustrates how aggressively F5 embeds messages. Even at the first and second offsets, which have the largest impact on the decoded image, almost half the images have an unusually high fraction of zeros with respect to the distribution derived from the original images. Since F5 modifies the least significant bits for arbitrary coefficient values, the effect observed for coefficient values of one, as shown on the right hand side of Figure 4, is much smaller. We can use this insight as shown on the left hand side of Figure 5. Here, for the same data set, we considered the fractions of the non-zero coefficients with a non-zero modulo 2 remainder. With a few exceptions, the centre of mass for the original cover media is around 0.5. For images containing F5-messages however, at almost all offsets, more than 75% of the images exhibit a fraction well below the reference set’s Q1/Q2 border.

While the above observation looks very promising for a straightforward detection method, the effect is significantly attenuated when using lower quality images. On the right hand side of Figure 5, we see the non-zero remainder distribution for the “large” data set but with a quality of 70%. Here, the median and quartile ranges are still visibly lower but much less so than for the full quality images. We observed this effect across all channels and image sizes.

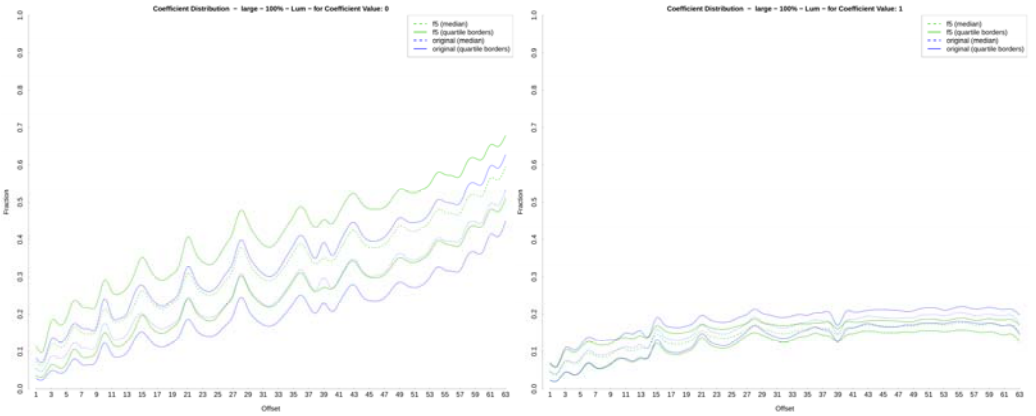


Figure 4. Distributions for the coefficient values 0 and 1 for images with and without messages embedded with the F5 algorithm.

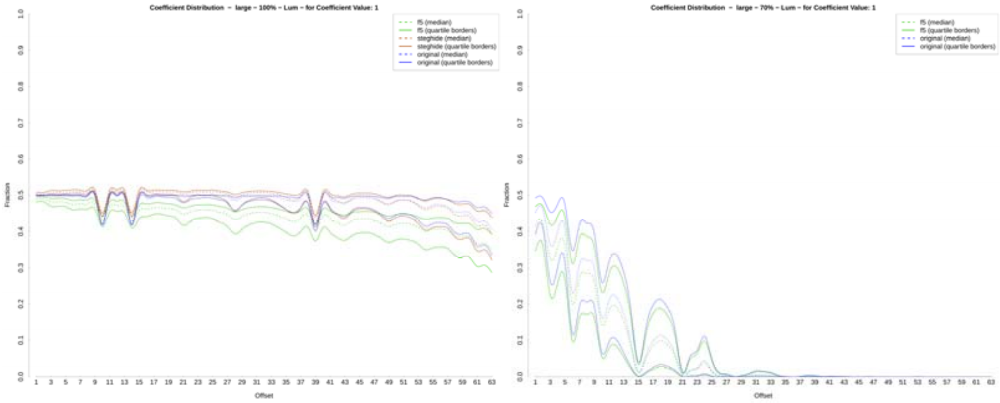


Figure 5. Distributions for the non-zero modulo 2 remainders before and after embedding messages with the F5 and Steghide algorithms.

4.2.2 Outguess

For Outguess, which only embeds messages in JPEG files with 75% quality, we observe a similar effect like for F5. As reflected by the left mass plot in Figure 6 however, showing the coefficient distribution for the “large” data set’s luma channel, Outguess significantly reduces the fraction of zeros in comparison to the original files, with a median close to the Q1/Q2 border of the original distribution. The effect of embedding messages is even stronger than for F5 when embedding in images with 70% quality, as shown on the right hand side of Figure 6. While embedding messages with Outguess has only a small effect on the chroma channels by comparison, the described significant impact on the luma channel may make it easier to detect than F5.

4.2.3 Steghide

Finally, we take a look at Steghide. Our analysis reveals, that – other than for the approaches discussed above – this embedding seems not to be applied by flipping the least significant bit to zero or one. Instead, we were able to observe that a coefficient value of -2 is slightly more likely and a value of -1 slightly less likely to occur in an image with an embedded message. The same relationship holds for values of 2 and 1.

As briefly discussed in section 3.3, Steghide aims to achieve an embedding by exchanging rather than modifying JPEG blocks. When merely exchanging blocks, there is no effect on the global distribution of the coefficients in the respective JPEG file. Hence, only blocks for which Steghide was unable to find a match have an impact on the distribution. This can be observed in the mass plot for the non-zero modulo 2 remainders shown on the left hand side of Figure 5. While the distribution for Steghide deviates – with respect to their inter-quartile ranges (IQR) – significantly from the original files in the low offsets, they increasingly overlap on the high frequency offsets. While we see a similar effect for the medium-sized 100% quality images, the distributions are difficult to distinguish for the “small” data set even when considering

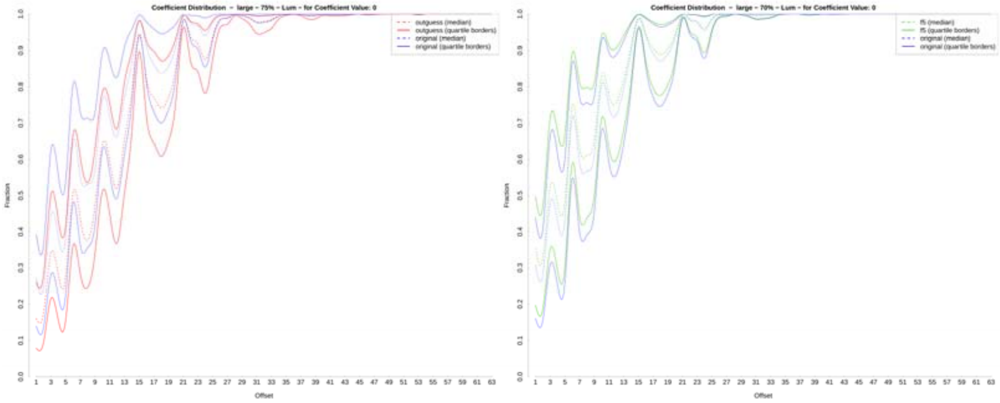


Figure 6. A comparison of coefficient value 0 distributions for Outguess and F5.

100% quality images. As we decrease the quality, the IQR of the original data sets increase and the distributions become increasingly difficult to distinguish. Hence, we conclude that identifying JPEG images carrying steganographic messages embedded with Steghide through their coefficient distribution poses the toughest among the algorithms we considered in this analysis.

5 CONCLUSIONS

In this paper, we provided an overview to the JPEG compression and file format. We explained how differences in size and quality affect the distribution of the underlying coefficients and subsequently the decoded image. Algorithms like F5, Outguess and Steghide modify these coefficients to secretly transfer messages. However, even when embedding messages with a very conservative rate of 0.2 bits per non-zero bit in the cover image, all of these algorithms have a measurable effect on the coefficient distribution. We measured this effect using a total of 13310 images in different sizes which were converted into sets of JPEG files with different quality levels. Generally, the effect of the embedding is more obvious for large high quality images where reducing the quality of images has a more significant effect than reducing their size. However, one should take into account that this will also reduce the effective data rate obtained through the steganographic channel.

Our detailed analysis shows that when comparing images with embedded messages against their counterparts without a message, most algorithms produced a significant change in the distribution of the non-zero modulo 2 remainders. Hence, we suggest that a detection method should take these into account. With respect to our analysis, Outguess had the strongest effect on the distribution, followed by F5. Steghide on the other hand produced only minor changes on the global distribution and may thus be difficult to detect reliably using global coefficient distributions.

REFERENCES

[1] Symantec, „W32.Duqu: The precursor to the next Stuxnet, Version 1.4," 2011.

[2] J. Segura, „Malwarebytes Labs: Hiding in plain sight: A story about a sneaky banking Trojan," 17 2 2014. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/. [Accessed on 22 June 2016].

[3] D. Cid, „Sucuri Blog: Malware Hidden Inside JPG EXIF Headers," 16 7 2013. [Online]. Available: https://blog.sucuri.net/2013/07/malware-hidden-inside-jpg-exif-headers.html. [Accessed on 22 June 2016].

[4] G. K. Wallace, „The JPEG still picture compression standard," *Communications of the ACM - Special issue on digital multimedia systems,* April 1991.

[5] A. Westfeld, „F5 - A Steganographic Algorithm," *Lecture Notes in Computer Science 2137: Information Hiding,* 2001.

[6] N. Provos, „Defending against statistical steganalysis," *Proceedings of the 10th conference on USENIX Security Symposium,* 2001.

[7] S. Hetzl und P. Mutzel, „A Graph Theoretic Approach to Steganography," *Lecture Notes in Computer Science 3677: Communications and Multimedia Security,* 2005.

WORKING AND LIVING IN INTERACTIVE ENVIRONMENTS – REQUIREMENTS FOR SECURITY AND PRIVACY

Erik Krempel[1], Pascal Birnstill[1] and Jürgen Beyerer[1,2]

[1] *{erik.krempel|pascal.birnstill|juergen.beyerer}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and
Image Exploitation IOSB, Karlsruhe, Germany
[2] Vision and Fusion Laboratory, Karlsruhe Institute of Technology, Karlsruhe, Germany

Abstract

Interactive assistance systems collect, process, and produce personal data of its users. Such systems have in common that they infer the current state of a given task from multi-sensor exploitation of a scene, which is matched with static model knowledge and learned characteristics of the users. Another typical property is, that the users have only limited control over the data processing. In a smart home the user needs to trust in services providers, which are operated in the cloud. Interactive environments at the workplace are deployed and maintained by the employer. In this paper we analyze assistance systems from an IT security as well as from a data protection perspective to document similarities in different scenarios. The goal is to show how threats to the security of personal data can be minimized and how data protection principles can be operationalized in such systems to bring the user in control of data access and usage.

Keywords: Interactive assistance, security, privacy, data protection, trusted computing

1 INTRODUCTION

When looking at recent research projects in the area of human-machine interaction, we observe a trend towards interactive assistance at the workplace; be it industrial production, operating rooms in hospitals, or security control centers. In addition, our homes and cars have started to perceive our behavior to enable smarter heating and facilitate the operation of entertainment electronics. Interactive assistance should be appropriate to the current situation and to individual users' needs and preferences. For this, persons, tools, objects, and environmental parameters are observed by a multitude of sensors (in the following we will refer to this data as live data). Live data is evaluated and interpreted to infer the current situation or work step by matching the observations with model knowledge, which enables interactive assistance systems to point users to problems before they become critical, to suggest possible solutions, or to intervene autonomously in specific cases.

User-specific interaction requires attentive assistance systems to know certain characteristics of individual users. Thus, available data source are also exploited to obtain and refine user profiles. By this means they are able to adjust the frequency and kind of provided assistance so as to find an adequate trade-off between supporting and disturbing the user. If we think, for instance, about assistance during surgical interventions we may want to adjust assistance to the stress level of the surgeon, his experience, and the observed progress of the intervention. Only little assistance is needed as long as the surgeon is relaxed and no complications or deviations from the expected workflow have been observed. For estimating the stress level we may observe and interpret concrete actions, facial expressions, and vital parameters. However, the significance of a particular indicator strongly varies between individuals. In most cases, such characteristics are partly determined by using machine learning algorithms and partly provided by the users themselves. In any case, these characteristics have to be persisted in user profiles.

From a security and privacy engineering perspective, live data sources and user profiles must be analyzed with respect to misuse potentials. At the workplace, user profiles and live data can be misused for performance monitoring of employees. At home, data can be misused for surveillance of family members or flat mates and invade individuals' privacy. Once more data becomes available, more business and misuse cases will emerge. Some insurance companies already give incentives for tracking car speed and movement. In the future, they may demand access to data concerning the drivers' attention and refuse cover if a driver was distracted.

Simply stopping the collection and storage of personal data would result in poor performance or complete deactivation of assistance services. Designers thus have to integrate security mechanisms that allow services to process required personal data, while at the same time effectively preventing misuse and ensuring compliance with applicable (data protection) law.

Research and own experiences have shown that security- and privacy related requirements have to be considered from the beginning of the design process as the integration of security mechanisms becomes more expensive and more complex at later stages. We therefore tackle the following problems in this paper: (i) Based on a generic system model we analyze interactive assistance systems with respect to specific assets and according protection goals as well as specific attackers and their intentions. (ii) We outline how security mechanisms from the domains of authentication, trusted computing, and usage control have to be combined so as to realize trustworthy and tamper-resistant interactive assistance system as well as portable and controllable user profiles.

This paper is structured as follows. After discussing related work in Section 2, we define our system model in Section 3. In Sections 4 and 5 we introduce protection goals and attackers. We extend the system model with security mechanisms in Section 6, analyze the fulfillment of the protection goals in Section 7 and conclude in Section 8.

2 RELATED WORK

In 2002, Marc Langheinreich presented recognized work on privacy in ubiquitous environments [5]. He developed a concept where privacy proxies and the users' mobile devices interact to enable user awareness and relies on social norm, cooperative operators and legal regulations to protect privacy. He argues that technical protection by encryption and anonymization will be hardly achievable. We see his point and believe that privacy needs social and legal control. Nonetheless we see high potential for technical data protection by recent developments.

Recent work for security and privacy in assistance environments is limited and highly domain specific, most of it done for smart home scenarios. Islam et al. [3] look into the security and privacy challenges of wireless sensor networks commonly found in smart home environments. Theoharidou et al. focus on the privacy aspects of smart homes for the elderly [1]. The Sentry@Home [4] project incorporates a privacy aware proxy that filters and controls private information that is shared outside of the home. While this approach provides means for protection against outside attackers, only limited protection against internal attacks is given.

3 SYSTEM MODEL

In our system model of interactive assistance systems we distinguish between **live data** and **user profile** data.

Adequately assisting users during their daily tasks requires assistance systems to know or to learn the users' characteristics and preferences. This information is stored persistently in a **user profile**. As an example consider assistance in a smart home. To automatically adapt the heating when a resident enters a room or to play his favorite kind of music, systems need to learn his preferences as well as some means to identify individuals. While these profiles might be non-critical in many cases, even certain smart home scenarios may require sensitive information. As a rule of thumb it can be assumed that the higher the level of details stored in a user profile the more importance should be attributed to accurate user identification and authentication.

Live data includes all data collected to infer the current situation in the assistance environment. This may include video streams, microphones, or any other sensor that contributes parameters for situation recognition. We assume that live data is only processed in real time, but not stored persistently.

We further assume that usage of interactive assistance systems proceed as follows: In the first step the system detects a user and tries to identify him. For this, systems typically rely on biometric identification or radio signals, e.g., from RFID-transponders or smartphones carried by the users. Once a user is identified, assistance systems exploit collected live data and interpret the results given the recognized user's profile stored in the system so as to adapt assistance to his characteristics and preferences. During usage an assistance system may also update users' profiles, e.g., musical preferences have changed or assistance information should be displayed using another modality. While in some cases a user can access his profile when interacting with an assistance system, he has little to no control over its usage.

4 PROTECTION GOALS

We need to consider protections goals with respect to assistance systems themselves and with respect to the classes of data processed by such systems, i.e., user profile data as well as live data.

Naturally, availability and integrity of assistance systems are fundamental goals. Assistance systems being unavailable may only be inconvenient in smart home scenarios, but dangerous when considering car assistance. While availability is important from an IT security perspective in the first place, integrity it is equally important from a data protection perspective. When a system is tampered with, no guarantees about data protection properties or the application of privacy enhancing technologies (PETs) can be given.

For both, user profile data and live data, confidentiality is the most important protection goal. Third parties outside the assistance environment should not be able to gain access to neither class of data. While raw live data already poses a substantial threat to users' privacy, illegitimate access to processed data, e.g., live data interpreted given user profiles and thus revealing the user's stress level, would have a devastating impact on privacy. Ideally raw sensor data should either not leave the assistance environment at all or get pseudonymized/anonymized beforehand by means of appropriate PETs. Processed data should by no means leave the system.

We add authenticity as an additional important component for the security of assistance environments. By this we mean, that a system is able to identify a user (or a group of users) and an attacker is not able to fake this allocation and therefore cannot claim to be another person.

5 ATTACKER MODELS AND THREATS

In their highly recognized publication “Security and privacy in sensor networks” Chan and Perrig point out why large scale sensor networks, i.e., assistance environments, change the privacy problem [2]. One might argue, that if you would not mind a random person observing you, then you should not mind a random system observing the same data. We believe that this is not true, because a single attacker might use several systems to spy on different remote places and sources simultaneously and thus multiplying privacy impact in an unforeseen way. This should change our perception as every bit of information an attacker might be able to gain access to should be evaluated for potential risks.

While the list of possible attackers in assistance environments strongly depends on the scenario, we can still to identify the following generic attackers and their intentions:

- **Privacy attacker**: The privacy attacker wants to access personal data stored or processed in the assistance environment, i.e., break the confidentiality of user profiles or live data. Exemplary intentions of the privacy attacker could be as follows. In a smart home, residents might try to misuse the system to monitor from afar if and when other residents leave the house or come back home. At the work place the privacy attacker may be a supervisor whose intention may be illegitimate performance monitoring of employees. This is particularly worrisome, as upcoming assistance environments often estimate stress levels of users during certain work steps, which may reveal information concerning a user's health status.
- **Sabotage attacker**: The sabotage attacker tries to prevent the system from providing assistance in the intended way. He either degrades or the quality of assistance or completely deactivates it. To do so, he needs to attack the integrity of the system itself or the integrity of processed data. Manipulating or deleting live data or persisted user profiles can degrade assistance functionality, but also denial of service-attacks against particular services could serve for this purpose. While not all cases of sabotage can be prevented, i.e., an attacker might destroy sensors, it is still important to detect and this kind of sabotage and to notify a responsible technician.
- **Impersonation attacker**: The impersonation attacker tricks the system into taking him for a regular user, i.e., he aims to violate an authentication method provided by the system. His intention might be gaining access to privileged or restricted functionality or areas, e.g., a smart home that automatically opens the door to residents. Another incentive for the impersonation attacker might be, that once the system recognizes him as a regular user he might be able access the otherwise protected user profile for his profit.

6 GIVING CONTROL TO THE USER

In the subsequent paragraphs we discuss concepts and mechanisms that should be combined so as to give the control of data usage back to the user. For this, we modify the system model of Section 3 such that usages of interactive assistance systems proceed as follows: The system detects an individual, whom it can either directly identify or from whom it requests an authentication. Whether or not a cryptographic authentication is required will also depend on the sensitivity of the attributes stored in user profiles. If the user considers this data as uncritical, he may allow the system to store it persistently. In case certain attributes are considered sensitive, e.g., attributes that reveal his medical condition, he may demand a strong cryptographic authentication as well as to remain in control over access to his user profile. A reliable authentication method could also be mandatory if it is of high importance that certain parameters observed by the system are interpreted correctly and where this interpretation requires knowledge stored in the user profile. Thus, the overarching aim of our approach is that users should be in control over stored user profiles. This enables them to decide if and under which circumstances they are willing to share them with an assistance system.

Before sharing data, we first of all need to make sure that a given system is trustworthy and will treat provided data according to our security demands, which comprises four aspect: (i) the security of the system has been approved, (ii) the system has not been tampered with after its deployment, (iii) we can negotiate security mechanisms for our data with the system, and (iv) we are able to manage and exchange user profiles with the system. In the following we will assume (i) as given, i.e., the considered system's security has been confirmed by some certification body or, as envisioned for the future, verified using formal methods [6]. Concerning (ii) we will discuss how trust anchors such as trusted platform modules (TPM) can be used to validate the integrity of the considered system. We propose to implement (iii) by means of deploying usage control technology [7, 8]. Usage control provides a framework for specifying and enforcing security- and privacy-related mechanisms in policies, which are attached to data. Regarding (iv) we will assume that individuals manage their profiles via a dedicated application for mobile devices, which also provides communication interfaces for exchanging user profiles and associated policies with the considered system, e.g., Bluetooth.

6.1 Assumptions of Trustworthiness

As discussed before, we assume that the system is trustworthy with respect to user profile data (and live data) at the time of deployment. This means that it has been shown that the system does not leak provided user profile data to its operating organization and also that it will enforce specific security mechanisms users may demand in addition before transferring the user profile. A user may, for instance, want to specify for which purposes a particular attribute of his user profile should be used or must not be used, or that a particular attribute may leave the system if has been anonymized before. We will discuss specification and enforcement of such security- and privacy-related requirements in 6.4.

6.2 Trust Anchors for System Integrity

Given that the considered system is trustworthy at the time of we need to make sure that the system has not been tampered with after it was put into operation. *Trusted platform modules (TPM)* [9, 10] are unforgeable cryptoprocessors microchips that can serve as trust anchors for this kind of integrity checks. A TPM can calculate and sign hashes over a system's hard- and software configuration, which can be validated by third parties so as to verify that software has not been manipulated (to actually prevent manipulation TPMs can also be employed for hard disk encryption and trusted boot). As TPMs are equipped with a unique RSA key, the so-called *endorsement key (EK)*, they can also be used by software components to verify the hardware platform. For attestation of integrity (also denoted as *remote attestation*), i.e., for signing integrity checksums, so-called *attestation identity keys (AIK)* are used, which are essentially pseudonyms of the EK. Since the EK pair is globally unique, its usage for such purposes would lead to further privacy issues.

To enable a user to make sure that a system beyond his control has not been tampered with, the system must provide a recent attestation of its integrity. For verifying this attestation, the authenticity of the used AIK is crucial: How can the user know that the AIK used for the signature belongs to the TPM of the system he wants to use? If we assume that we can trust in the vendor of the system, but not in the operator, AIKs could be authenticated by vendors. This means, however, that a public key infrastructure (PKI) or some decentralized secure register for authenticated AIKs is needed so as to enable users to verify the authenticity of a given AIK.

6.3 Controlling User Profiles with Usage Control

After a user successfully validated that the considered system has not been tampered with, we assume that it is essentially trusted by the user. This includes that the system provides reliable protection mechanisms the user can negotiate for (specific parts of) his user profile so as to stay in control of the usages of his data after the initial access has been granted. By this means we are able to give individuals more. For this purpose usage control frameworks have been introduced by Sandhu [7] and Pretschner [8]. Usage control requirements such as “Do not redistribute my data”, “Use my data for statistical purposes only“, “Store my data only in anonymized form”, and “Delete my data after 24 hours” are typically specified in usage control policies. Thus, usage control enables users to define permitted respectively forbidden usages or processing purposes on fine-grained level, i.e., on the level of particular attributes of their user profiles. Given that the usage control infrastructure (as part of the considered system) is implemented correctly, is free of bugs, and has not been tampered with, it will be monitoring received data continuously so that it can be guaranteed that personal data is processed in compliance with the policy the user attached to it. Note that this requires that usage control is augmented with data flow tracking technology as explained in [11].

6.4 Securing User Profiles

As already discussed, we consider persistent storage of user profiles in smart environment systems an undesirable risk unless they are encrypted with cryptographic key material owned by the user. We therefore assume that user profiles are managed (this includes editing of usage control policies for the user profiles) and stored on a mobile device owned by the user. But also on the user’s own smart phone user profiles should be protected using encryption. And then again we need to protect the key material. This could of course be done by encrypting the secret or private key using a passphrase. However, a higher level of security can be achieved using smart cards or similar cryptographic tokens for encryption and decryption. Such devices are also available in microSD format and are therefore usable in many mobile devices. By this means cryptographic keys are only stored within the tamper-resistant secure file system of the smart card. If a user profile is additionally stored in a smart environment system, the smart card can also be used for encryption and decryption. If contactless smart cards are used, these cryptographic procedures could even be executed without involving the user’s smart phone.

7 SECURITY ANALYSIS

After this brief outline on security mechanisms for interactive assistance systems and their interplay, we need to go back to the attackers of Section 4 again. In the following we analyze to what extent the described mechanisms increase the system’s robustness against the particular attackers.

First of all we need to discuss the fact that we delegate the responsibility to users to specify appropriate privacy policies for their user profiles. While this gives the maximum level of control to the users, it might lead to adverse situations. If you imagine a near future, where assistance systems in the workplace store and process users’ personal data that allow for performance monitoring, an employer might urge his employees to share it. A similar case is insurance companies seducing insured persons with lower fares if they agree to share certain data. This already became reality with so-called telemetry contract offered by automobile insurers.

A public discourse is needed to figure out whether individuals should actually be able to share anything with any party or whether the minimum privacy standards have to be demanded as mandatory and to be enforced by according systems. While from a technical point of view both options are available society will have to decide which one should be preferred as we will not be able to have both at the same time.

Given that the system did not have vulnerabilities to be exploited by privacy attackers at the time of deployment, a positive integrity validation based on trusted computing confirms that (i) we can trust in the system not to leak data and that (ii) provided user profiles are processed in compliance with the users' requirements specified in usage control policies. Particularly if a user specifies that a given interactive assistance system must only store his user profile data encrypted with key material under his control, the **privacy attacker** will not be able to break confidentiality so as to obtain illegitimate access to the users personal data, even in case he broke authentication.

The **impersonation attacker** must break the system's authentication scheme if he wants to obtain the usage privileges of a regular user. Again, if the system was trustworthy at the time of deployment and we positively validated that it has not been tampered with, then it will provide strong cryptographic authentication schemes. However, we cannot ultimately relieve the users from the responsibility to actually request strong authentication. Users have to be careful about trade-offs between security and convenience. One may, for instance, reject the inconvenience of strong authentication schemes with services inside one's smart home, but not at the front door. Then such trade-offs of course depend on the sensitivity of data stored in the user profile for a specific system, whereas also the amount of personal data attributes indicates that one should not opt for convenience.

The measures against the privacy attacker and the impersonation attacker are also necessary to avert the **sabotage attacker**. They will however not prevent him from physically damaging the system to degrade its services. They will also not prevent him from attacking the system's availability, e.g., by means of denial-of-service and related attacks on the infrastructure level. However, a large fraction of such attacks can be prevented if vendors and integrators adhere to best practices and established guidelines such as Common Criteria [12] or IT Grundschutz [13].

8 CONCLUSION

This paper takes a generic look at assistance environments and what kind of IT security and privacy challenges are present. After defining a generic system model we describe protection goals valid in common assistance systems. The description of a privacy, sabotage and impersonation attacker completes the description of current and future systems. We present a combination of mechanisms that allow developers to build secure and privacy-aware systems where users are in control over their data. One question that cannot be answered today is whether users should have ultimate control over their data or not. Do we want to allow users to share any of their data, even if it might be due to external pressure and in their disadvantage or do we build systems that decide what kind of data users are allowed to share?

REFERENCES

[1] Theoharidou, M., Tsalis, N., & Gritzalis, D. (2014). Smart Home Solutions: Privacy Issues.

[2] Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. Computer, 36(10), 103-105.

[3] Islam, K., Shen, W., & Wang, X. (2012). Security and privacy considerations for wireless sensor networks in smart home environments. In Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on (pp. 626-633). IEEE.

[4] Bagüés, S. A., Zeidler, A., Valdivielso, C. F., & Matias, I. R. (2007). Sentry@ Home-Leveraging the smart home for privacy in pervasive computing. International Journal of smart home, 1(2), 129-145.

[5] Langheinrich, M. (2002). A privacy awareness system for ubiquitous computing environments. In *UbiComp 2002: Ubiquitous Computing* (pp. 237-245). Springer Berlin Heidelberg.

[6] Böhl, F., Greiner, S., & Scheidecker, P. (2014). Proving correctness and security of two-party computation implemented in Java in presence of a semi-honest sender. In Cryptology and Network Security (pp. 175-190). Springer International Publishing.

[7] Park, J., & Sandhu, R. (2004). The UCON ABC usage control model. *ACM Transactions on Information and System Security (TISSEC)*, *7*(1), 128-174.

[8] Pretschner, A., Hilty, M., & Basin, D. (2006). Distributed usage control.*Communications of the ACM*, *49*(9), 39-44.

[9] http://www.trustedcomputinggroup.org/tpm_2-0_mobile_common_profile_v2r31/

[10] Sandhu, R., Ranganathan, K., & Zhang, X. (2006, March). Secure information sharing enabled by trusted computing and PEI models. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security* (pp. 2-12). ACM.

[11] Harvan, M., & Pretschner, A. (2009, October). State-based usage control enforcement with data flow tracking using system call interposition. In *Network and System Security, 2009. NSS'09. Third International Conference on* (pp. 373-380). IEEE.

[12] https://www.commoncriteriaportal.org/

[13] BSI, B. (2008). Standard 100-2: IT-Grundschutz-Vorgehensweise. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

ELICITING AND REFINING REQUIREMENTS FOR COMPREHENSIBLE SECURITY

Brandon Broadnax,[1] Pascal Birnstill, [2] Jörn Müller-Quade[1] and Jürgen Beyerer[2]

[1] *{brandon.broadnax|mueller-quade}@kit.edu*
Karlsruhe Institute of Technology, Germany

[2] *{pascal.birnstill|juergen.beyerer}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and
Image Exploitation IOSB, Karlsruhe, Germany

Abstract

In this work we introduce the principle of comprehensible security, which demands that the security of an IT system is understandable for stakeholders. In particular, all assumptions made for the security mechanisms of an IT system ought to be well-documented. Based on this principle, we propose a conceptual framework that facilitates communication between developers and stakeholders. Our framework uses a goal-oriented approach where requirements are gradually refined. Each refinement corresponds to a specific stage of the development process. In addition, requirements originating from legal constraints are also considered in our framework, because it is indispensable to consider applicable law when developing an IT system. Furthermore, since designing secure IT systems is an interdisciplinary challenge, our framework was also developed to facilitate collaboration between experts of different subfields of computer science. To this end, our framework provides a method for decomposing security requirements into tasks addressed within specific subfields.

Keywords: Information security, security requirements, comprehensible security

1 INTRODUCTION

Security of a system is often blindly trusted - with disastrous consequences. As a result, confidential data of users or entire companies may become disclosed or large networks may suffer DDOS attacks. Typically, it is only stated that the system uses some security mechanisms. However, these much-touted security mechanisms are black boxes to users. They may be outdated and therefore completely insecure. Moreover, the security of a system is generally based on unproven assumptions that are not documented. This is a huge problem as these assumptions may, for instance, hold only for a certain period of time, making the system insecure in the future.

Security that is not comprehensible should not be trusted at all. We therefore put forward the principle of comprehensible security which demands that the security of an IT system is understandable for stakeholders. In particular, all assumptions made during security analysis have to be well-documented and open to public inspection. Consequently, when discussing the security of a software project with stakeholders, one should be able to explain why, how, and under which assumptions the specification, design, and implementation ensure the security-related requirements. In the following we mention various problems that have to be tackled in order to achieve comprehensible security in requirements engineering.

First of all, security-related requirements are introduced on different levels of abstraction. Stakeholder requirements are typically phrased in an informal language in a rather ambiguous manner. This is in parts due to the fact that stakeholders are typically technical laymen that cannot express their needs in a precise way. On a lower level of abstraction, security mechanisms and the guarantees they provide are specified in a very technical language, however. If one wants to be able to explain security to the stakeholders, one must find a way to bridge this gap between the informal requirements of stakeholders and the specification of the final implementation of the system.

Furthermore, security issues have to be tackled in an interdisciplinary context. Naturally, aspects of security are addressed by various subfields of computer science such as cryptography, access and usage control, network security, software engineering, software verification, compiler construction, etc. Overcoming patchwork security however requires that the security mechanisms of these subfields are combined in a reasonable way. In particular, this combination of methods should be done in such a way that security of the system is comprehensible to the developers of the system. Hence, a method that facilitates collaboration between experts of different subfields of computer science is needed. Additionally, all assumptions made by the various domain experts for the security of their mechanisms have to be documented in a way that is comprehensible for stakeholders.

Additional complexity comes from conflicts between different security-related requirements and also between security-related requirements and other functional or non-functional requirements. These conflicts can reveal themselves at different stages of a development process. For instance, although we can already point out during requirements elicitation that there is a trade-off relationship between confidentiality, integrity, and availability, the extent to which we will be able to meet a specific requirement in terms of latency depends on the concrete choices of mechanisms for ensuring confidentiality and integrity during system design or implementation. In order to be able to solve such conflicts along the way, requirements have to be annotated with priorities. In addition, conflicts with legal requirements constitute a special case. As they are non-negotiable, they override conflicting requirements. Handling such cases necessarily requires an additional consultation of requirements engineers and stakeholders.

Our contribution is a conceptual framework, which (i) refines security-related requirements of stakeholders in a way that is understandable for stakeholders (ii) facilitates collaboration between experts of different subfields of computer science (iii) provides means for recognizing and resolving conflicts at each stage of the development process. Throughout this paper, we assume non-security-related requirements to be known, i.e., they have already been elicited.

2 RELATED WORK

Requirements engineering (RE), established in the mid-1970s, is the process of identifying, analyzing, documenting and maintaining requirements. It can be roughly broken down into four activities (cf. [15]): *requirements elicitation*, *requirements* analysis & negotiation, *requirements specification*, and *requirements validation*. Requirements elicitation (also called "‘requirement gathering"’) is the practice of collecting the requirements of a system from stakeholders. The objective of requirements analysis and negotiation is to check requirements and resolve conflicts among the elicited requirements of the system. The result of requirements specification is a description of all the functional and non-functional requirements of a system under development, possibly including a set of use cases. Finally, requirements validation involves checking that the documented requirements actually meet stakeholder needs.

Goal modeling is a modeling type in RE were security requirements are represented in the form of stakeholder goals. A goal-oriented approach in RE can have many advantages (cf. [20]). Eliciting goals naturally leads to the questions "why", "how" and "how else". This way, it is less likely to miss stakeholder requirements or to over-specify them. Furthermore, alternative design options are revealed in the process thus preventing premature design decisions. Modeling requirements as goals can also help to cope with complex requirements as large goals can be decomposed into smaller goals that are easier to realize. Moreover, goals can facilitate identifying conflicts, as typically meeting one goal can complicate or even make it impossible to meet other goals. The various trade-offs between requirements that arise can be resolved more easily with goals. Finally, goal modeling enables to measure requirement completeness by defining requirements to be complete if they fulfill all elicited goals.

Goal modeling has been proposed in literature at various stages of RE. For instance, goals are used for requirements elicitation by the frameworks GOMS [3], ORDIT [5], Ellis'94 [9], i* [21, 22], ISAC [13], F^3 [2]. Goals can also be found in the context of requirements negotiation in the frameworks SIBYL [11], REMAP [17], Duffy'95 [6] or the Reasoning Loop Model [12]. The frameworks KAOS [4], GBRAM [1], and NFR [14] use goals at the requirements specification level. Finally, a goal-oriented approach for requirements validation was adopted for the frameworks GSN [19] and GQM [18]. Goal modeling has been proposed as a strategy for analyzing security trade-offs in [7]. This approach has been developed further in [8] where the authors propose to employ goal modeling to systematically analyze the vulnerabilities of a system design and their effects.

3 FUZZINESS OF SECURITY REQUIREMENTS

We chose the modeling type “goal modeling” for identifying and analyzing security requirements. This model type was chosen for the reason that goals can be expressed by the stakeholders from their individual perspectives. Therefore, goals are a natural representation of security requirements in the context of comprehensible security. Furthermore, we have also adopted the notions “soft goal” and “hard goal” from the i*-framework ([21, 22]) as these notions are suitable tools for decomposing security requirements in a judicious and comprehensible manner.

As stated above, we assume throughout this paper that the functional requirements have already been elicited. We call the class of all users as well as the set of all elicited functional requirements a scenario. Starting from a scenario, the developers elicit the security requirements by interacting with the stakeholders. In general, the requirements that are expressed by the stakeholders are not precise enough for a technical implementation. Therefore, a framework was developed for describing the process from the security requirements of the stakeholders to the technical requirements of the system under development. In this framework, one starts from the assets of a stakeholder. Assets are resources that are of some particular (tangible or intangible) value for a stakeholder. A stakeholder's assets can be potentially harmed by the system under development. This leads to the notion of soft goals. On the level of abstraction of stakeholder requirements, soft goals specify which property of a particular asset must be preserved. For instance, a stakeholder can demand that his personal data are “kept secret”, his reputation remains “undamaged” or that his money is “used moderately”. The notion of soft goals is used to model the phase of requirements elicitation, where the various security requirements of the stakeholders are iden- tied. Here, it is assumed that stakeholders, being technical laymen, can express their requirements only in the form of soft goals, i.e., in the form

“Property Y of asset X must be preserved!”

Note that soft goals are expressed without referring to any functional requirements of the system under development. As soft goals are expressed using an informal language, it is difficult to directly implement them in a technical system. For that reason, the notion of hard goals was introduced. Hard goals are defined as necessary conditions for fulfilling the elicited soft goals in the system under development. They contribute to the abstraction level of the system's specification. Unlike soft goals, hard goals always refer to some functional requirement that is part of the system under consideration. The syntax for hard goals is expressed along the lines of the following phrase:

"<Functional requirement> must not conflict <soft goal>!"

For example, the requirement "Data must be exchanged confidentially!" is a hard goal with respect to the soft goal "Data must be kept secret!" and with respect to the mechanism "Data transmission" that belongs to the functional requirements of the system under development. Since hard goals are expressed as more concrete requirements for a system under development, they are easier to implement and verify. Moreover, since hard goals are still expressed in a non-technical language and since they are directly related to a specific soft goal, they are comprehensible for a stakeholder. The rationale behind this is that a developer, after refining the various soft goals into hard goals, can present these hard goals to a stakeholder, who can then get an overview of the necessary things that have to be done in to fulfill his requirements.

The aforementioned refinement constitutes only the first step in our framework. Hard goals that were derived from soft goals will be further refined into smaller problems that can be tackled by mechanisms within specific fields of computer science (cf. 4).

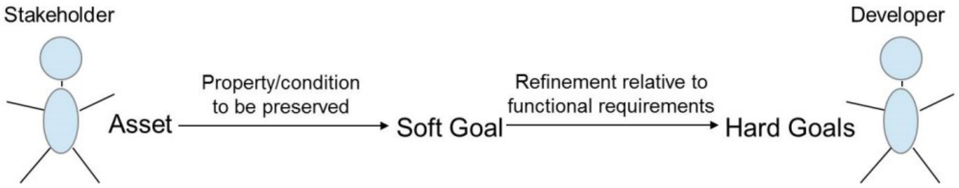

Stakeholder
Developer
Asset
Property/condition to be preserved
Soft Goal
Refinement relative to functional requirements
Hard Goals

Figure 1: Refining soft goals into hard goals

4 INTERDISCIPLINARY DECOMPOSITION

Security of IT systems is an interdisciplinary challenge which requires that mechanisms of various subfields of computer science complement each other. In the following, we show how this can be done in accordance with the principle of comprehensible security. On the level of abstraction of hard goals, we introduce the notion of so-called black box mechanisms. A black box mechanism is a place holder for a class of mechanisms satisfying the considered hard goal. These mechanisms are provided by a particular subfield of computer science. Which specific mechanism is eventually used is a question that is addressed on a lower level of abstraction (cf. 5). Black box mechanisms are chosen on the abstraction level of system design. More specifically, design decisions between black box mechanisms are allowed in case a hard goal can be fulfilled by different black box mechanisms.

The applicability and security of black box mechanisms typically rely on specific abstract assumptions. These assumptions are characteristic of the subfield from which a black box mechanism is provided. In our framework, these assumptions are called separating assumptions. Separating assumptions define the boundaries between subfields. They describe questions which a subfield factors out, passing them to the field of research of another subfield. As separating assumptions rely on the existence and security of mechanisms of other subfields, they can be considered as hard goals addressed by other subfields. In our framework, separating assumptions are expressed in terms of the properties or tasks that are fulfilled for a specific black box mechanism:

"<Property or task> is fulfilled for <black box mechanism>!"

When developing a secure system one should address as many separating assumptions as possible. This leads to an iterative refinement process for hard goals, where the separating assumptions made for the security of a black box mechanism imply hard goals that are fulfilled by other black box mechanisms. In more detail, one proceeds as follows. By rephrasing separating assumptions of a black box mechanism as hard goals, we obtain further hard goals that are tackled by mechanisms of other subfields. These mechanisms give rise to further separating assumptions and so on. This way, one can systematically identify further hard goals until one eventually reaches separating assumptions that one cannot verify, e.g., one has to rely on the correctness of a component or of the operating system because one do not have access to its source code. In our conceptual framework, these unverified assumptions are the trust anchors of the developed system. We call the described iterative process a decomposition of hard goals, which results in a tree structure beneath each hard goal that was derived from a specific soft goal. Usually, the security of a system will depend on several trust anchors. This is because when decomposing a hard goal, one may end up with several separating assumptions that cannot be verified. Furthermore, one normally needs to decompose multiple hard goals, which do not necessarily lead to the same unverifiable separating assumptions. The principle of comprehensible security demands that every separating assumption and trust anchor is explicitly documented in order to make the security of a system as transparent as possible.

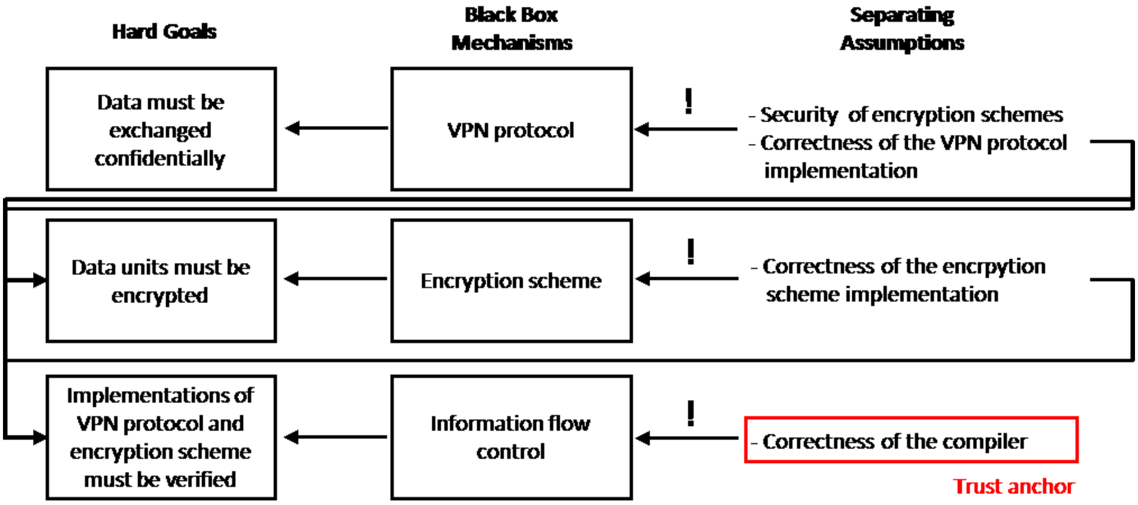

Hard Goals
Black Box Mechanisms
Separating Assumptions
Data must be exchanged confidentially
VPN protocol
!
- Security of encryption schemes
- Correctness of the VPN protocol implementation
Data units must be encrypted
Encryption scheme
!
- Correctness of the encrpytion scheme implementation
Implementations of VPN protocol and encryption scheme must be verified
Information flow control
!
- Correctness of the compiler
Trust anchor

Figure 2: Example for the decomposition of a hard goal

Fig. 2 illustrates the decomposition of hard goals through the example of the hard goal *data must be exchanged confidentially*. The black box mechanism *virtual private network (VPN) protocol* fulfills the hard goal under the sep. assump. *security of encryption schemes*, which is addressed by cryptography, and *correctness of the VPN protocol implementation*, which is addressed by software verification. This implies the hard goal *data units must be encrypted*, which leads to the black box mechanism *encryption scheme*. In addition, cryptography also assumes the *correctness of the encryption scheme implementation*. Correctness of the VPN protocol and encryption scheme can be achieved using the black box mechanism information flow control, which assumes the *correctness of the compiler*. Finally, since correctness of the compiler has not been verified in this example, it is a trust anchor of the system.

5 SUBFIELD-SPECIFIC LEVEL

On a more detailed level of abstraction, more precisely when the system design is realized in the system's implementation, black box mechanisms are instantiated by concrete mechanisms, which are called white box mechanisms. White box mechanisms provide the necessary conditions for fulfilling a hard goal. These are called guarantees in our framework (cf. Figure 3).

Guarantees usually cannot be given unconditionally. Rather, specific assumptions have to be made. At the white box level of abstraction, these assumptions are called fundamental assumptions in our framework. Fundamental assumptions comprise subfield-specific foundations. Going back to the example introduced above, assume that we have decided to realize the black box mechanism encryption scheme using (a specific variant of) the RSA cryptosystem. The RSA cryptosystem can be shown to be secure under the fundamental assumption that no efficient algorithm exists to solve the problem of factoring large numbers. Guarantees given by different mechanisms and subfields vary substantially regarding the degree of precision and formalization. Typically, the white box level of abstraction has to be considered when one wants to resolve trade-offs, as concrete mechanisms have to be analyzed for this purpose. We elaborate on this issue in the next section.

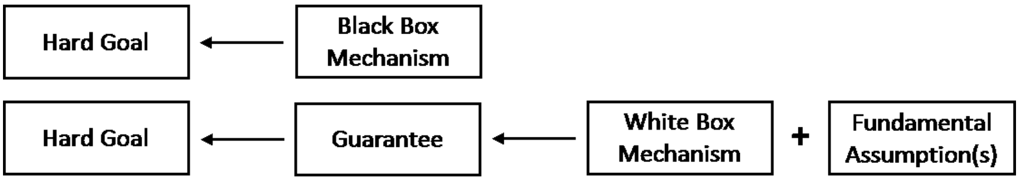


Figure 3: Black box mechanisms are instantiated by white box mechanisms

6 RECOGNIZING AND RESOLVING CONFLICTS

Ambiguity of soft goals isn't the only problem a developer faces during requirements analysis. There can also be conflicts among the various requirements elicited. These conflicts can reveal themselves on various levels of refinement. Conflicts can reveal themselves already during the requirements elicitation phase if there is an inherent trade-off relationship between soft goals (*inherent conflicts*). Conflicts may also emerge as a consequence of using a specific black box mechanism (*derived conflicts*).

The best known inherent conflict is the trade-off relationship between soft goals concerning confidentiality, integrity, and availability, which cannot be maximized at the same time and thus have to be balanced to achieve adequate security. If, for instance, confidentiality is implemented via an encryption scheme and availability is realized via a replication scheme, integrity is hard to preserve since replicates have to be kept synchronized, which introduces additional overhead in terms of encryption, which in turn affects availability.

Although derived conflicts may seem less common, they do emerge when trying to ensure that critical software systems are operated within a secure environment: When realizing a secure environment, we may want to apply black box mechanisms such as deep packet inspection (DPI) on gateways and firewalls for early detection of malware, viruses, or attacks. This requires that payloads of network packets are inspected, which interferes with the goal of exchanging data via confidential communication channels realized via black box mechanisms like VPN protocols that encrypt payloads.

The various trade-offs that might arise through these conflicts have to be identified and discussed with the stakeholder. For this to be possible there has to be a feedback loop to the stakeholders at any level of refinement. In order to cope with these conflicts, soft goals have to be annotated with priorities. These annotations can then help the developer during the development process, e.g., when there are several options for black box mechanisms.

Many conflicts can only be resolved at the white box level of abstraction, as concrete mechanisms are considered at this level of abstraction only. As an example of a conflict to be addressed on the white box level, consider the problem of secure database outsourcing: A database containing confidential data is to be outsourced to a cloud storage provider. Services built on this database have to be able to compute specific queries with a specific upper bound concerning latency. The black box mechanism addressing this problem is confidentiality-preserving indexing (CPI), which can be instantiated by deterministic indexes, order-preserving encryption, or searchable encryption on the white box level. When deciding for a concrete white box mechanism, the type of queries that are to be executed on the database may rule out some candidates for white box mechanisms. In the second step, a white box mechanism with low communication and computation overhead will be chosen in order to minimize latency. In case it turns out that the latency requirements of the stakeholders still cannot be met, latency or security requirements are either relaxed according to given priorities or in consultation with the stakeholders. More details on resolving trade-offs in the context of secure database outsourcing can be found in [10].

6.1 Legal Requirements

Legal requirements are important to consider because even an ideally secure implementation is useless if it does not adhere to applicable law. However, legal requirements are not necessarily implied by the other (non-legal) requirements. This is due to the fact that soft goals are expressed from a stakeholder's individual perspective and stakeholders are typically not only layman with respect to technical issues but also with respect to legal issues. Moreover, legal requirements may even be at odds with other requirements.

Consider the example of video surveillance in subway trains, which help counter acts of violence and vandalism. The large amounts of video data could be pre-evaluated using activity recognition algorithms that automatically alert the police. However, European data protection law prohibits automated individual decisions entailing legal or other adverse consequences for the person(s) affected. Instead, situations have to be assessed by a human operator before any countermeasures are initiated. This legal constraint has to be considered when designing the workflow of the system.

To incorporate requirements originating from legal issues, our framework formally considers the legislator as an additional stakeholder who introduces legal requirements. A common base for soft goals and laws is provided by the notion of assets mentioned above. Like soft goals, laws also originate from specific assets that are to be protected. Unlike soft goals, however, laws cannot be modified so as to resolve conflicts with other soft goals. For this reason, the notion of obligations was introduced. Obligations are non-negotiable requirements that are defined on the same level of abstraction as soft goals. Laws imply obligations. For instance, § 6a of the German Energy Economy Law demands that economically sensitive data such as consumption data of individual households is to be treated as confidential.

7 CONCLUSION

In this paper we have presented a new conceptual framework for requirements engineering. This framework helps a developer during the entire development phase of a system, starting with requirements elicitation. Our framework is tailored in such a way as to make the security of a system under development as comprehensible as possible for a stakeholder. Additionally, our framework facilitates collaboration between developers coming from different fields of computer science by means of an iterative delegation process. Moreover, legal requirements are also considered in our framework because an IT system must adhere to applicable law.

REFERENCES

[1] A. Antón et al. Goal-based requirements analysis. In Requirements Engineering, Proceedings of the 2nd Int. Conf. on, pp. 136-144, IEEE, 1996.

[2] J. Bubenko et al. Objectives driven capture of business rules and of information systems requirements. In Systems, Man and Cybernetics, 'Systems Engineering in the Service of Humans', Proc. of the Int. Conf. on, pp. 670-677, IEEE, 1993.

[3] S. K. Card et al. The psychology of human-computer interaction, 1983.

[4] A. Dardenne et. al. Goal-directed requirements acquisition. Science of computer programming, 20(1):3-50, 1993.

[5] J. Dobson et al. The ordit approach to organisational requirements. In Requirements engineering, pages 87-106. Academic Press Professional, 1994.

[6] D. Duffy et al. A framework for requirements analysis using automated reasoning. In Advanced Information Systems Engineering, pp. 68-81. Springer, 1995.

[7] G. Elahi and E. Yu. A goal oriented approach for modeling and analyzing security trade-offs. In Conceptual Modeling-ER, pp. 375-390, 2007.

[8] G. Elahi et al. A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. Requirements Engineering 15.1: pp. 41-62, 2010.

[9] C. Ellis and J. Wainer. A conceptual model of groupware. In Proc. of the ACM Conf. on Computer Supported Cooperative Work, pp. 79-88. ACM, 1994.

[10] J. Köhler. Tunable Security for Deployable Data Outsourcing. Karlsruher Institut für Technologie, 2015.

[11] J. Lee and K.-Y. Lai. What's in design rationale? Human-Computer Interaction, 6(3-4):251-280, 1991.

[12] P. Louridas and P. Loucopoulos. A generic model for reflective design. ACM Trans. on Software Engineering and Methodology (TOSEM), 9(2):199-237, 2000.

[13] M. Lundeberg. The isac approach to specification of information systems and its application to the organization of an ifip working conference. In Information systems design methodologies: A comparative review, pp. 173-234. The Netherlands: North-Holland, 1982.

[14] J. Mylopoulos et al. Representing and using nonfunctional requirements: A process-oriented approach. Software Engineering, IEEE Trans. on, 18(6):483-497, 1992.

[15] K. Pohl. Requirements engineering: An overview. RWTH, Fachgruppe Informatik, 1996.

[16] A. Pretschner et al. Distributed usage control. Commun. ACM, 49(9):39-44, 2006.

[17] B. Ramesh and V. Dhar. Supporting systems development by capturing deliberations during requirements engineering. Software Engineering, IEEE Trans. on, 18(6):498-510, 1992.

[18] R. Van Solingen et al. Goal question metric (gqm) approach. Encyclopedia of Software Engineering, 2002.

[19] S. Wilson et al. Safety case development: Current practice, future prospects. In Safety and Reliability of Software Based Systems, pp. 135-156. Springer, 1997.

[20] E. Yu and J. Mylopoulos. Why goal-oriented requirements engineering. In Proc. of the 4th Int. Workshop on Requirements Engineering: Foundations of Software Quality, volume 15, 1998.

[21] E. S. Yu. Towards modelling and reasoning support for early-phase requirements engineering. In Requirements Engineering, Proc. of the 3rd IEEE Int. Symposium on, pp. 226-235. IEEE, 1997.

[22] E. S. Yu and J. Mylopoulos. Understanding "why" in software process modelling, analysis, and design. In Proc. of the 16th int. conf. on Software engineering, pp. 159-168. IEEE Computer Society Press, 1994.

DETECTION OF CONSPICUOUS BEHAVIOR IN STREET TRAFFIC BY USING B-SPLINES AS FEATURE VECTOR

Mathias Anneken[1], Yvonne Fischer[1] and Jürgen Beyerer[1, 2]

[1] *{mathias.anneken, yvonne.fischer, juergen.beyerer}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB),
Interactive Analysis and Diagnosis, Fraunhoferstr. 1, 76137 Karlsruhe (Germany)

[2] *Karlsruhe Institute of Technology (KIT), Vision and Fusion Laboratory,*
Adenauerring 4, 76131 Karlsruhe (Germany)

Abstract

Due to the increasing amount of data, a human operator might not be able to identify the important situations accurately. In order to improve the situation awareness of human operators in surveillance tasks, decision support systems need to direct the focus of the operators on situations of interests. These situations are often deviations from the typical patterns. Therefore, outliers and novelties have to be identified. In this paper, a data-driven algorithm for the detection of anomalies in trajectories based on b-splines is used to detect abnormal behavior in street traffic. The control points of a b-spline interpolation representing a trajectory are used as feature vector for anomaly detection algorithms. For the evaluation, two datasets of street traffic in cities are analyzed. In order to detect outlier in the datasets, the local outlier factor and the feature-bagging for outlier detection algorithm are used.

Keywords: anomaly detection, traffic surveillance, b-spline interpolation, local outlier factor, feature-bagging for outlier detection

1 INTRODUCTION

The amount of data recorded by surveillance system is steadily increasing, resulting in an information overload for the operators of these systems. Therefore, an automatic system for the identification of unusual behavior of specific prior defined situations is needed. Such a system have to be able to evaluate and asses a situation based on the incoming data as well as on the expert knowledge given by domain experts. For the former, anomaly detection algorithms are used. These algorithms identify deviations from the recorded typical behavior.

As surveillance tasks arise in different application domains, e.g., maritime surveillance or traffic surveillance, it is important, that such systems can be adapted to a new domain with ease. Hence, it is from utter importance to evaluate an algorithm with different datasets recorded in different domains. Further, the adaption of the algorithms has to be feasible. As the annotation of data is time consuming and expansive, an unsupervised algorithm is preferable.

Anneken et al. [1] present an algorithm based on b-spline to detect anomalies. For the evaluation an annotated dataset from the maritime domain is used. Here, this algorithm is adapted by using the local outlier factor and the feature-bagging for outlier detection as unsupervised anomaly detection algorithms. For the evaluation, a dataset of street traffic is utilized.

2 RELATED WORK

A survey on anomaly detection is given by Chandola et al. [2]. They give an overview about the variety of approaches for anomaly detection and different application domains anomaly detection is used in like video surveillance and cyber security. The different algorithm are divided by their principle approach, e.g., cluster-based or nearest neighbor based.

Piciarelli et al. [3] detect anomalies in video sequences. Thus, the main idea is to identify deviation from typical patterns. They utilize a single-class support vector machine as anomaly detection algorithm. The identification of anomalies without a priori information on the distribution of anomalies is one of the major topics in their work.

By using the piecewise liner segmentation algorithm, de Vries and van Someren [4] divide trajectories in smaller segments. Afterwards, these segments are clustered and kernel methods are used for the anomaly detection. For the evaluation, real data from the Netherlands' coast near Rotterdam is used.

Amongst others, Janssens [5] compares different outlier detection algorithms by using 24 different real-world datasets. As outlier detection algorithms, k-nearest neighbor data description, parzen window data description, support vector data description, local outlier factor, and local correlation integral are used. The best performance is achieved by using the local outlier factor and the support vector data description.

Fischer et al. [6] use dynamic Bayesian networks to model specific situations. Each situation is subdivided into elementary and abstract situations. During this process, expert domain knowledge about the specific situation is embedded in the model. The model is evaluated by using an example from the maritime domain, namely for an incoming suspicious smuggling vessel. In order to build this model, several parameters have to be estimated. Therefore, Fischer et al. introduce an automatic approach for the parameter estimation.

Anneken et al. [7] model the vessel traffic in the maritime domain as probability density functions. These functions are estimated by using Gaussian mixture models and kernel density estimation. As input data, an annotated dataset of cargo and tanker vessels is used. An anomaly is identified by evaluating the probability density function. If the value is lower than a prior defined threshold, the incoming data will be considered as anomaly.

3 DATASET

The dataset used in the evaluation was recorded by the Federal Highway Administration (FHWA) for the Next Generation Simulation (NGSIM) program [8]. The goal of NGSIM is to develop algorithm to support traffic simulations. In order to evaluate these algorithms different traffic situations were recorded and made publicly available for further research. In section 5 two of these datasets are used. The first one was recorded in Peachtree St., Atlanta, Georgia, USA the second one in Lankershim Blvd., Los Angeles, California, USA. Both datasets contain traffic data of different vehicle types on both lanes in a timespan of half an hour. The recorded data is shown in Fig. 1. Outliers and anomalies in these recordings are, e.g., U-turns at traffic lights or turns in directions, which are not allowed.

4 ALGORITHM

The challenge in comparing two trajectories with each other, arises due to different sample rates, lengths and number of points in each trajectory. In order to compare two arbitrary trajectories, different approaches are introduced in literature. E.g. the Hausdorff metric can be used to calculate the distance between two sets of points as described by Laxhammar et al. [9] or dynamic time warping as described by Vakanski and Mantegh [10] can be used to determine the difference between two time-series. Here, the idea to represent a trajectory by using the control points of a b-spline interpolation as introduced by Anneken et al. [1] is used. Compared to the work by Anneken et al., the complete dataset is unlabeled. Thus, instead of supervised learning approaches like support vector

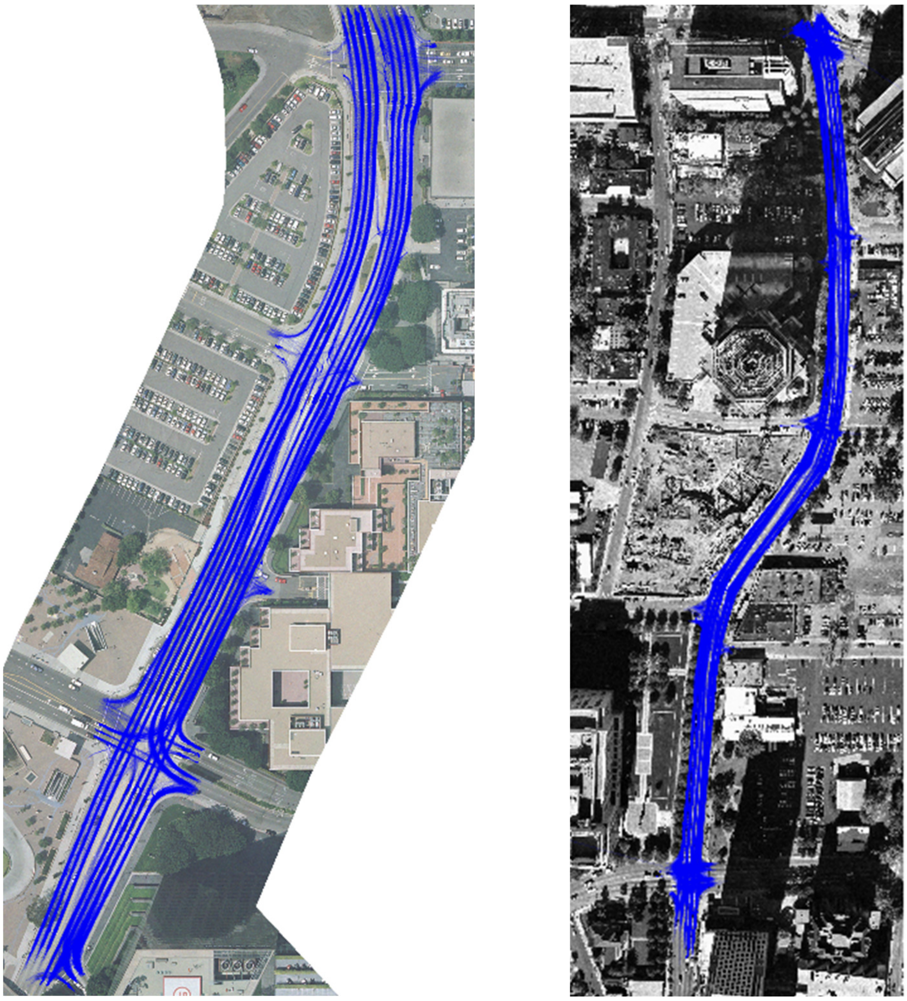


Fig. 1: The street traffic datasets used for the evaluation. The trajectories of the vehicles are drawn in blue. On the left side, the Lankershim dataset is shown; on the right the Peachtree dataset is shown.

machines, the local outlier factor and the feature bagging for outlier detection algorithms are used to determine anomalies in the dataset.

Each datum in the dataset has at least a position in longitude and latitude and an identifier for the trajectory the datum is part of. Hence, the trajectory T consists of n_T points $p_i = (p_{lon}, p_{lat})$ with $i = 1, \dots, n_T$. As n_T may vary for each trajectory, the idea is to transform the trajectory by using a b-spline interpolation. The resulting control points, which define the b-spline, are then used as feature vector representing the whole trajectory T.

4.1 Local outlier factor

The local outlier factor (LOF) is introduced by Breunig et el. [11]. The idea is to detect outliers by analyzing and comparing the local density of a datum with its neighborhood. If the local density is small compared to the density of the neighboring data, the datum will be considered an outlier. Otherwise, the datum is member of a cluster.

First of all, let $d_k(A)$ be the distance from A to the k-th nearest neighbor. The set of all k-nearest neighbors is denoted as $N_k(A)$. Thus, the reachability distance can be defined as

$$d_{r,k}(A, B) = \max\{d_k(B), d(A, B)\}.$$

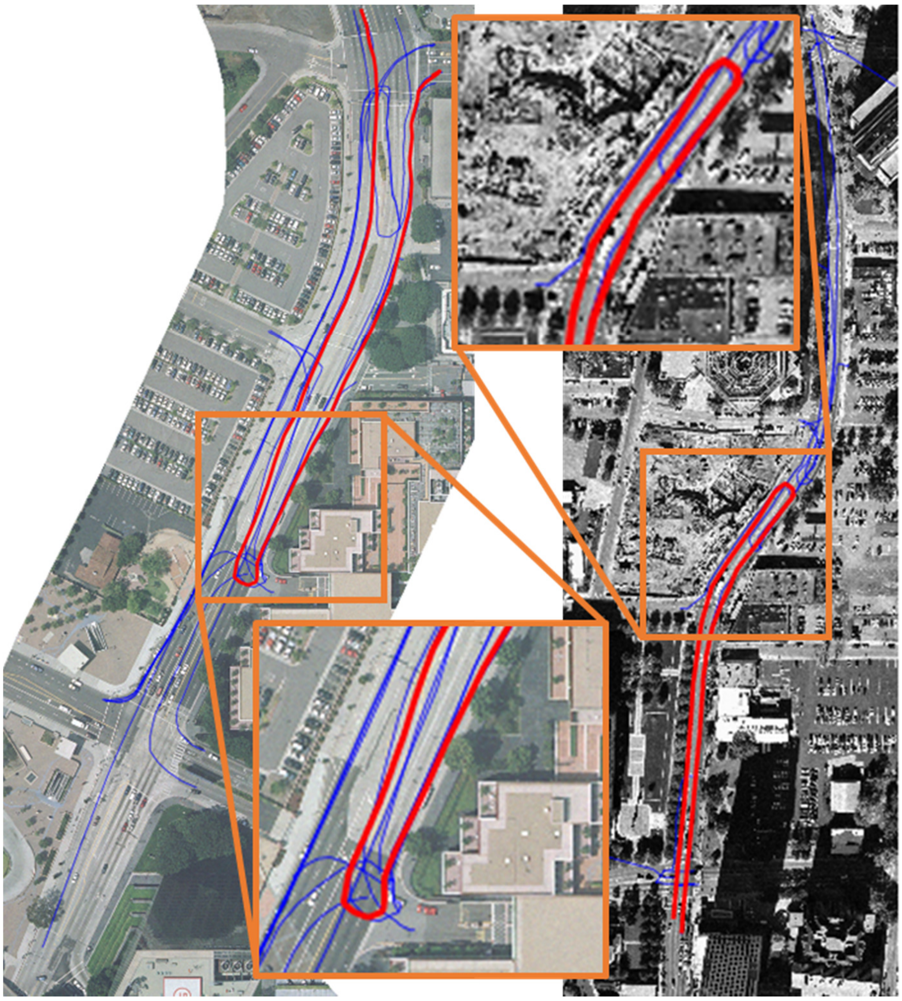


Fig. 2: Example anomalies in the two datasets as detected by both algorithms.

I.e., the reachability distance will be either the distance between the two objects or at least the $d_k(B)$.

The local reachability density is then defined as

$$lrd(A) \;=\; 1/(\frac{\sum_{B\in N_k(A)} d_{r,k}(A,B)}{|N_k(A)|}).$$

The local outlier factor is then given by

$$LOF_k(A) = \frac{\sum_{B\in N_k(A)} \frac{lrd(B)}{lrd(A)}}{|N_k(A)|}.$$

A LOF smaller than 1 indicates a denser region, while a value significantly higher than 1 indicates an outlier.

4.2 Feature-bagging for outlier detection

The feature-bagging for outlier detection (FBOD) is introduced by Lazarevic and Kumar [12] as an extension to the LOF. The algorithm uses multiple projections of the dataset for multiple instances of the LOF algorithm. After estimating the LOF for each datum of these projections, the individual results are combined. The intention is to improve the detection quality for higher dimensional input data. It can be considered an ensemble method.

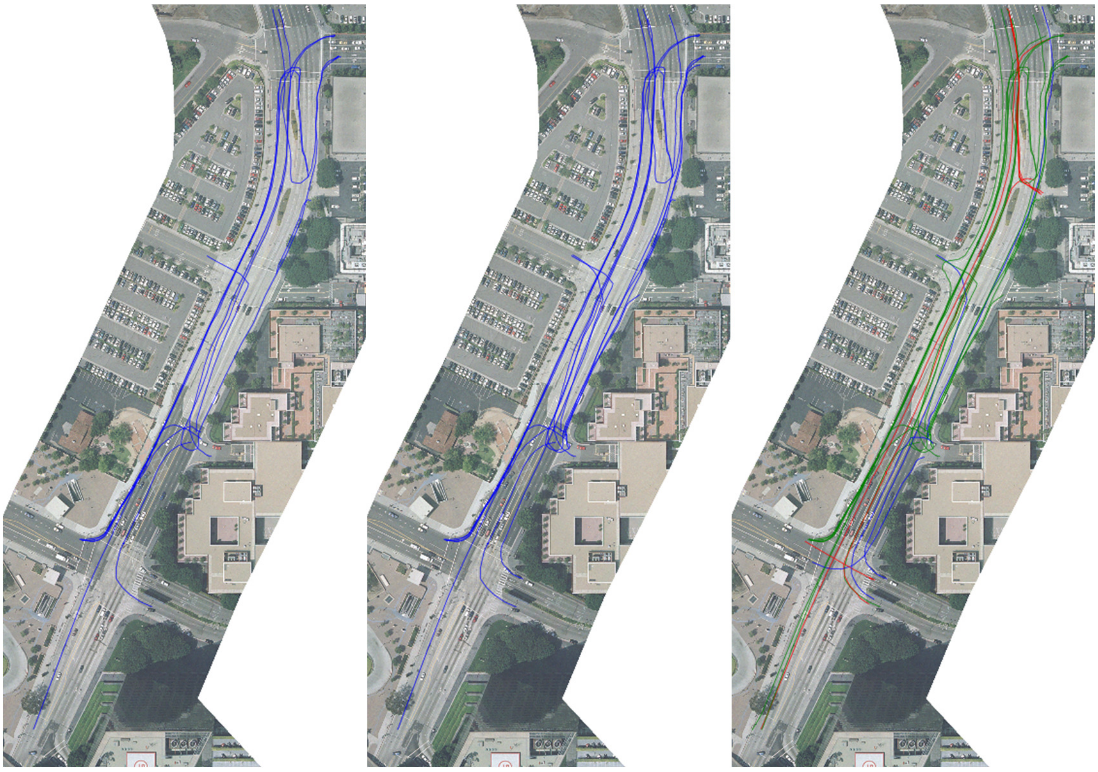


Fig. 3: The results of the anomaly detection in the Lankershim dataset. From left to right: LOF, FBOD and a comparison of the two algorithms. The blue trajectories in the left and middle figure are abnormal trajectories detected by the algorithm. In the right figure, green trajectories are the ones detected by both algorithms. Red trajectories are detected by LOF and blue ones are detected by FBOD.

5 EVALUATION

For the evaluation, the two datasets are used. For each dataset the number of nearest neighbors k has to be estimated. Further, a threshold for both algorithms independently has to be determined, as the result for both is a floating number which only indicates high density if the number is smaller or equal 1. Only if the number is significantly larger than 1, the datum is considered an anomaly. Therefore, for each dataset a threshold is identified. The threshold is chosen, so that the 20 trajectories with the highest outlier factor are considered an anomaly.

In Fig. 2, some examples of conspicuous behavior detected by the algorithms for both areas are shown. In both cases U-turns are performed by the vehicles at crossings, where this is not allowed.

In Fig. 3 and Fig. 4, results of both algorithms are compared to each other. In Fig. 3, the results for the Lankershim dataset are shown. For each algorithm, a single subfigure depicts the 20 most abnormal trajectories. Furthermore, a figure to compare the two algorithms is given. In Fig. 4, the two algorithms are just compared with each other. The results for the algorithms differ only slightly.

6 CONCLUSION

In the given datasets conspicuous behavior of some participants in the recorded traffic could be detected. This behavior includes U-turns and turns in general at crossing, where this behavior is not allowed. The falsely classified anomalies are mostly vehicles driving on routes with low density, i.e., vehicle are driving from smaller side streets on the

Lankershim Blvd. or the Peachtree St. and take a turn again on a smaller side street. As not many drivers take this route, these are outliers in the dataset, even though the behavior is not conspicuous.

7 FUTURE WORK

As the evaluation yields only qualitative results, a next step should be the qualitative assessment of the proposed algorithms with the given dataset. Furthermore, other dataset from different domains should be included to obtain more reliable results.

The algorithm can only be used for offline analyses. For a real time analysis, changes to the algorithm have to be made. One possibility could be using sliding windows with different window sizes. Another one could be the segmentation of the trajectory based, e.g., on the piecewise linear segmentation algorithm.

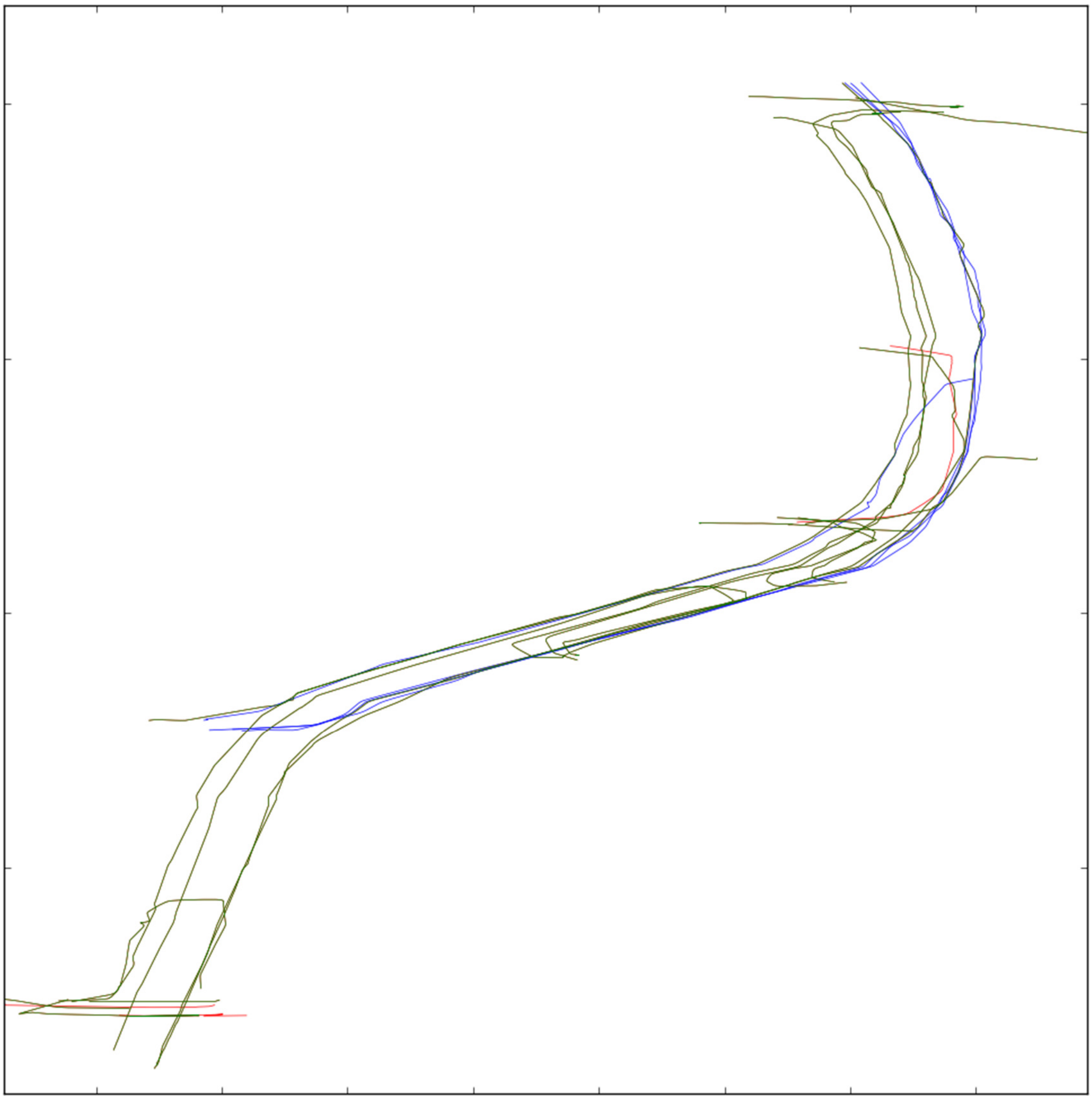


Fig. 4: A comparison of the two algorithms in the Peachtree dataset. Green trajectories are detected by both algorithms, red only by LOF and blue by FBOD.

REFERENCES

[1] Anneken, M.; Fischer, Y. & Beyerer, J. (2016), *Anomaly Detection using B-spline Control Points as Feature Space in Annotated Trajectory Data from the Maritime Domain*, Proceedings of the 8th International Conference on Agents and Artificial Intelligence, pp. 250-257

[2] Chandola, V.; Banerjee, A. & Kumar, V. (2009), *Anomaly Detection: A Survey*, ACM Computing Surveys, ACM, 15:1-15:58

[3] Piciarelli, C.; Micheloni, C. & Foresti, G. (2008), Trajectory-Based Anomalous Event Detection Circuits and Systems for Video Technology, IEEE Transactions on, pp. 1544-1554

[4] de Vries, G. K. D. & van Someren, M. (2012), *Machine learning for vessel trajectories using compression, alignments and domain knowledge*, Expert Systems with Applications, pp. 13426 - 13439

[5] Janssens, J. H. M (2013). *Outlier Selection and One-Class Classification*, Tilburg University

[6] Fischer, Y.; Reiswich, A. & Beyerer, J. (2014), *Modeling and recognizing situations of interest in surveillance applications*, Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2014 IEEE International Inter-Disciplinary Conference on, pp. 209-215

[7] Anneken, M.; Fischer, Y. & Beyerer, J. (2015), *Evaluation and comparison of anomaly detection algorithms in annotated datasets from the maritime domain*, Proceedings of 2015 SAI Intelligent Systems Conference (IntelliSys)

[8] Federal Highway Administration (2007), NGSIM – Next Generation Simulation, Retrieved May 20, 2016 from: http://www.fhwa.dot.gov/publications/research/operations/its/06135/index.cfm

[9] Laxhammar, R. & Falkman, G. (2011), *Sequential Conformal Anomaly Detection in trajectories based on Hausdorff distance*, 14th International Conference on Information Fusion (FUSION)

[10] Vakanski, A.; Mantegh, I.; Irish, A. & Janabi-Sharifi, F. (2012), *Trajectory Learning for Robot Programming by Demonstration Using Hidden Markov Model and Dynamic Time Warping*, Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, pp. 1039-1052

[11] Breunig, M. M.; Kriegel, H.-P.; Ng, R. T. & Sander (2000), J. *LOF: Identifying Density-based Local Outliers,* Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, ACM, pp. 93-104

[12] Lazarevic, A. & Kumar, V. (2005), *Feature Bagging for Outlier Detection*, Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining, ACM, pp. 157-166

REAL-TIME IMAGE PROCESSING BASED DEFLAGRATION DETECTION AND LOCALISATION

Tobias Ernst[1], Alexander Fay[2], Felix Kümmerlen[3]

[1] *tobias.ernst@hsu-hh.de*
Helmut Schmidt University / University of the Federal Armed Forces Hamburg, Institute of Automation Technology, Holstenhofweg 85, 22043 Hamburg (Germany)

[2] *alexander.fay@hsu-hh.de*
Helmut Schmidt University / University of the Federal Armed Forces Hamburg, Institute of Automation Technology, Holstenhofweg 85, 22043 Hamburg (Germany)

[3] *FelixKuemmerlen@bundeswehr.org*
Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS), Humboldtstrasse 100, 29633 Munster (Germany)

Abstract

The topic of fire and smoke detection has been extensively examined already. But the detection of faster combustion processes like deflagrations, which are also called flash fires, is only rarely investigated, although deflagrations are more dangerous than static fires and they are harder to detect because they spread much faster. This paper is based on a deflagration detection algorithm which was first fully published in [1]. The algorithm was a novelty as it enables cameras to detect deflagrations. But three main concerns remained open in [1]: the lack of real-time capability, the liability for false alarms, and the missing but essential localisation of a detected deflagration. Within this paper, we report how these three deficiencies have been overcome.

Keywords: Deflagration detection, real-time, parallel processing, stereo camera

1 INTRODUCTION

In the domain of fire and smoke detection, several approaches exist which investigate in camera systems and algorithms ([2], [3], [4]). Beside reducing the vulnerability to false alarms and increasing the detection ratio, the ability to calculate the result in real-time receives increasing attention ([5], [6], [7]). Most fire-like combustion processes occur within seconds or minutes. Therefore the detection systems need to compute the underlying algorithms within a few seconds. Usually, surveillance cameras are used for the detection, thus the algorithms are considered to be “real-time capable” if they can be evaluated within the frame rate of the utilized cameras, which is usually 30 frames per second (FPS), which results in a computation time of about 33 ms per frame.

Especially in military vehicles but also in chemical test stations and mills, deflagrations, which are in the focus of our research, represent a tremendous safety hazard. They develop much faster. In order to protect the crew of a military vehicle or any person which is located in a danger zone from the worst injuries, deflagrations have to be detected within 15 ms to start countermeasures in time. For the whole extinguishing process a time of 250 ms is declared [8]. This is the reason why simple but quick optical sensors have been used for the detection of deflagrations in the past. These sensors are able to detect deflagrations within the required 15 ms but are not able to provide any further information regarding the combustion process [9]. Furthermore they are vulnerable to nuisance alarms. To simultaneously detect, locate and acquire more information about a deflagration, we propose to apply cameras with a higher frame rate than those of typical surveillance cameras. With an increased frame rate and the need to detect deflagrations within less than 15 ms [9], the computing time of the detection algorithms is crucial. Thus, in this paper, at first the requirements regarding a real-time deflagration detection algorithm and camera system are being discussed. Afterwards it will be examined how the algorithm published by *Schröder* in [1] fulfills these needs. The paper will discuss which parts of the algorithm are (time-) critical and will present solutions to improve the real-time performance of the identified parts. Afterwards the algorithm has been implemented to compute a 200 FPS video stream for real-time detection of deflagrations. Furthermore it has been enhanced to make the detection more robust by using features which have originally been used for flame detection. Also an adaptive background segmentation has been implemented to further improve the robustness. To locate deflagrations within the field of view of two cameras, the detection results are triangulated. The whole detection and localization has been tested regarding the performance and detection ratio on artificial created deflagrations on a testing bench.

2 REAL-TIME DEFLAGRATION DETECTION

2.1 Requirements

As stated above, the sensors already in use need about 15 ms for the detection. Thus any newer system should also detect deflagrations within 15 ms. As the algorithm needs at least 3 frames (images) of a developing deflagration, the frame rate of the camera has to be at least 200 FPS (1).

$$\frac{\mathbf{1}}{\frac{\mathbf{15\,ms}}{\mathbf{3}}} = \mathbf{200\ Hz} \tag{1}$$

This results in the requirement that the processing time of each frame should be faster than 5 ms. In fact the processing time has to be even faster to acquire the image and to perform some additional calculations such as to locate the deflagration. The localisation of the deflagration is necessary to properly suppress it, as the extinguishing agent should be applied at its optimal position. To locate a deflagration, however, the frames of at least two cameras have to be analysed and the results have to be triangulated. Since the detection system has to work autonomous and cannot wait for human confirmation of an eventually detected deflagration and because of the reason that the extinguishing process might be quite uncomfortable in the narrowness of a military vehicle, the detection should be robust to false alarms. Reasons for false alarms can be for example sunlight, muzzle flash, rotating lights or other fire coloured objects.

2.2 Detection Algorithm

The sequence of the algorithm developed by Schröder is outlined in Fig. 1. In the first step the intensity, the high pass filtered intensity and the red-blue ratio is calculated for each pixel

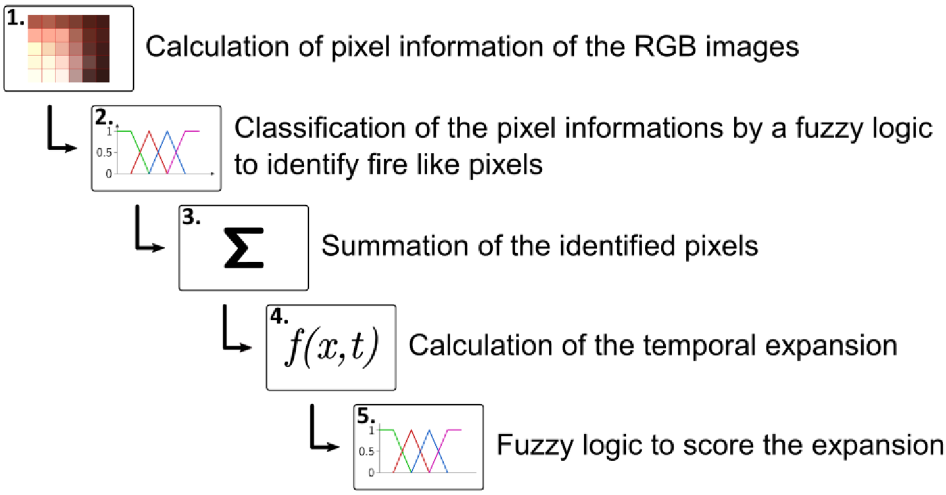

1.
Calculation of pixel information of the RGB images
2.
1
0.5
0
Classification of the pixel informations by a fuzzy logic to identify fire like pixels
3.
Σ
Summation of the identified pixels
4.
f(x,t)
Calculation of the temporal expansion
5.
1
0.5
0
Fuzzy logic to score the expansion

Fig. 1: Sequence of Schröders algorithm to detect deflagrations

of a frame. In the second step this information is used by a fuzzy logic to decide if the pixel seems to be fire-like. Afterwards – in the third step – the sum of all fire-like pixels is calculated. In step four, the spatial expansion parameter (SEP) is calculated. At the end (in step five) another fuzzy logic calculates the membership of the frame to a deflagration by the sum of fire-like pixels and the SEP. Especially step one and two are quite time consuming as they have to be done pixel by pixel. But also the summation within step three is slow as a large array has to be summed. The time needed for these 3 steps highly depends on the resolution of the camera image. But decreasing the resolution is not a good option as this will lead to a poorer precision of the detection and an eventually performed localisation.

Due to the fact that some operations are done pixel by pixel, the algorithm is highly qualified to be parallelized. The sequence of the parallelized algorithm is shown in Fig. 2. The steps are the same but the first two steps (the calculation of pixel information and their fuzzification) can be done in one processing step. By doing this in parallel for every pixel, a significant speedup of the detection algorithm should be achievable. Furthermore it is taken into account that an image taken by a camera is not a RGB image. Normally the image sensor chip of a camera takes Bayer coded images. This means that coloured glass is placed in front of each photosensor. Usually 50 % of them are green and respectively 25 % are red and blue. With an interpolation step (demosaicing) the colour information is reconstructed to generate an image that is suited for the human eye, as we understand colours as a mixture of green, blue and red. But for the detection algorithm the demosaicing does not produce any additional information. To the contrary it produces additional data that has to be analysed. The needed colour information is well represented in the Bayer coded (raw) image. Therefore not every pixel has to be analysed but only every tuple of two green, one red and one blue pixel. As a consequence the amount of processing steps is reduced by the factor of 1/4.

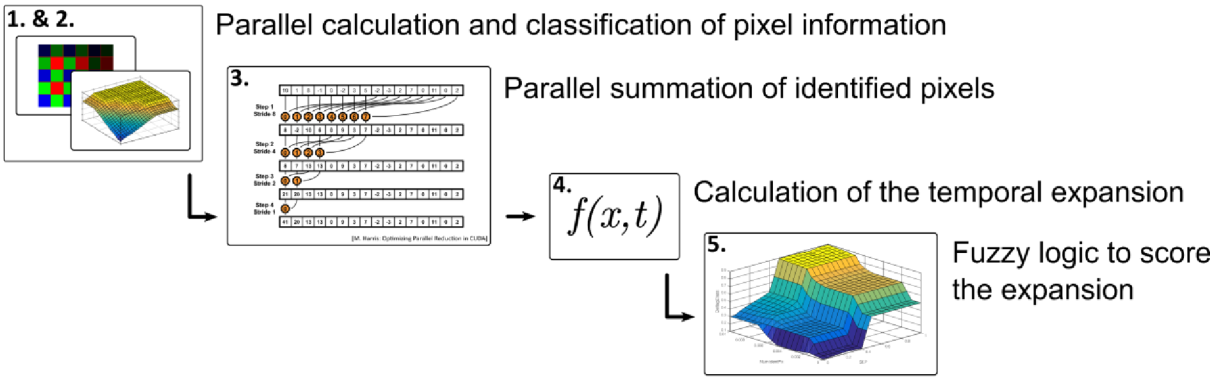

1. & 2.
Parallel calculation and classification of pixel information
3.
Parallel summation of identified pixels
[M. Harris: Optimizing Parallel Reduction in CUDA]
4.
$f(x,t)$
Calculation of the temporal expansion
5.
Fuzzy logic to score the expansion

Fig. 2: Parallelized algorithm

After step one and two, the sum of all fire-like pixels is calculated during step three. Naturally this has to be done sequentially. But with parallel reduction the time complexity of the summation can be reduced from $\mathcal{O}(n)$ for the sequential summing of n elements to $\mathcal{O}(n/p + \log(n))$ for the parallel summing with p processors [10]. After that the SEP is calculated in step four. With the algorithm of Schröder the absolute amount of pixels is taken into account. But as the resolution of the utilised camera might change it is more universal not to use the sum m but the ratio r_m of identified pixels, which is described by (2), to calculate the SEP.

$$r_m = \frac{m}{image_{rows} \cdot image_{columns}} \qquad (2)$$

As this assumption also applies to the last step, a new fuzzy logic has been designed. This fuzzy logic uses the SEP and r_m instead of m to classify if the image contains a deflagration or not. The membership functions and the output functions are shown in Fig. 3 and the rules are listed in Tab. 1. With these improvements it is possible to speed up the calculation of the algorithm from 56 ms per frame of the Matlab implementation (run on an i7-3610QM

@ 2.3 GHz) to 1.1 ms of an implementation where the main processing is done on the graphics card of a PC (NVS 5400M).

These results seem to be sufficient for the algorithm to be called real-time capable. But by now it had only been tested under laboratory conditions with black background and no other light sources. In order to harden the deflagration detection to more realistic conditions, some improvements have been implemented, which are outlined in the following section.

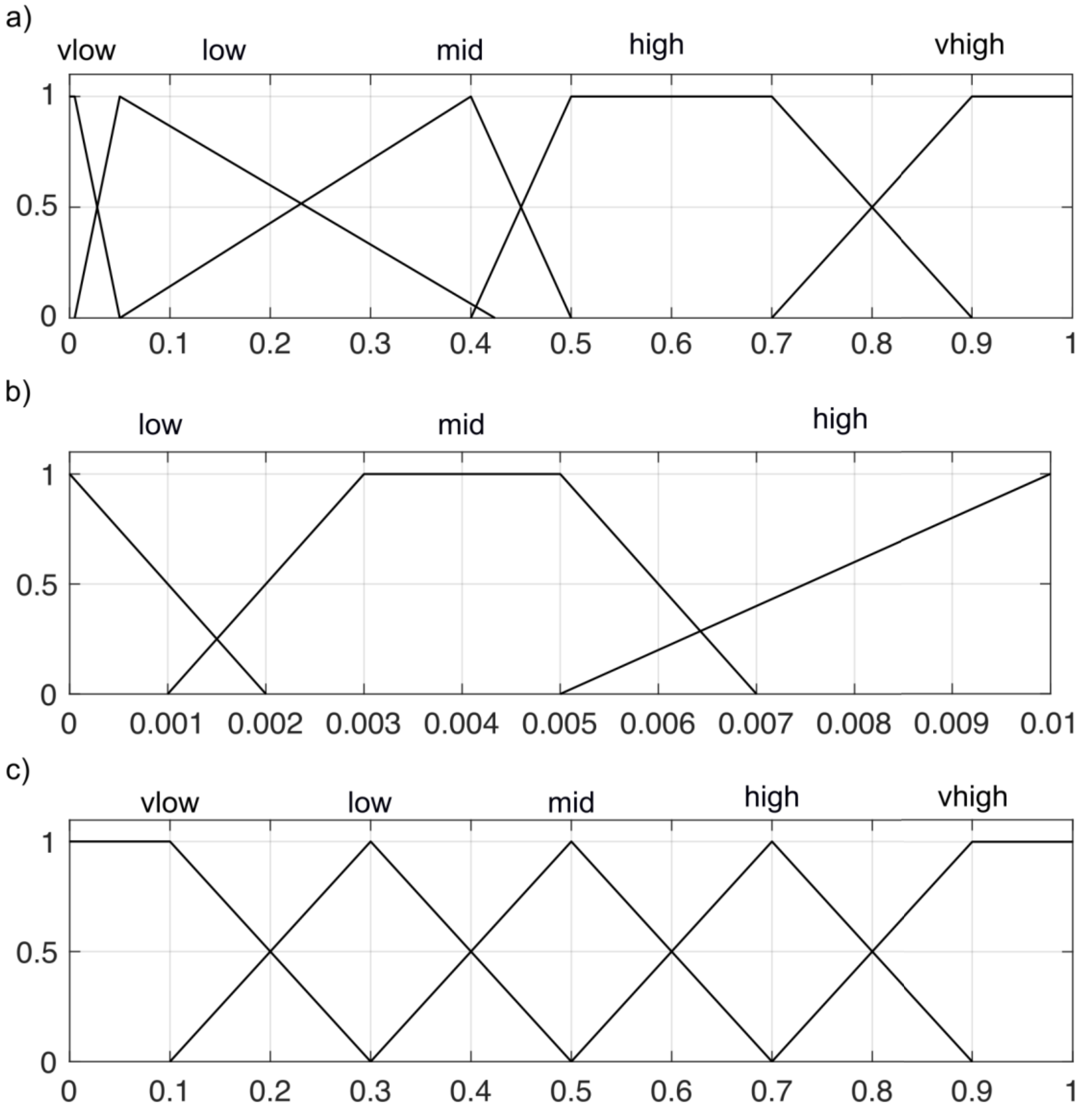


Fig. 3: a) Membership functions for SEP, b) Membership functions for r_m, c) Membership function for deflagration classification

Tab. 1: Rules of the fuzzy logic to classify for a deflagration

AND				SEP		
		vlow	low	Mid	high	vhigh
r_m	low	vlow	vlow	Vlow	mid	mid
	mid	vlow	low	Low	high	high
	high	low	low	Mid	vhigh	vhigh

2.3 Improvements

2.3.1 Background segmentation

As the algorithm seems to perform well by detecting deflagrations on black background, these are not very realistic circumstances. Under real conditions the background will be coloured and inhomogeneous. Furthermore it might contain fire coloured objects which by now will also be taken into account and therefore sophisticate the results of the deflagration detection. For background segmentation the algorithm developed by Jiang in [11] is used. It segments the foreground pixels not by a fixed threshold but accordingly to the intensity of the image.

The segmentation to compute the binary image G, which marks every foreground pixel with 1 (or true) and every background pixel with 0 (or false), is done in two steps and performed pixel by pixel. At first the value of each pixel of the frame I is compared to the value of a background image B, which is initialized with the first frame taken. During the comparison of each pixel in row m and column n $B_{m,n}$ is incremented if $I_{m,n} > B_{m,n}$ or decremented if $I_{m,n} < B_{m,n}$. In the second step the value $I_{m,n}$ is compared to two predefined threshold values T_i, which separate the values of I into 3 portions. Together with these threshold values the foreground image G is calculated by comparing the difference between $I_{m,n}$ and $B_{m,n}$ to the thresholds D_i. The pseudocode of this algorithm is shown in Fig. 4.

```
foreach pixel in I
   if(I[m,n] > B[m,n]): B[m,n]++
   else if(I[m,n] < B[m,n]): B[m,n]--

   if(I[m,n] > T[1]): if(abs(I[m,n]-B[m,n])>D[2]): G[m,n]=1
                      else: G[m,n]=0
   elseif(I[m,n] > T[0]): if(abs(I[m,n]-B[m,n])>D[1]): G[m,n]=1
                          else: G[m,n]=0
   else: if(abs(I[m,n]-B[m,n])>D[0]): G[m,n]=1
         else: G[m,n]=0
```

Fig. 4: Pseudocode of the background segmentation

2.3.2 Colour segmentation of fire-like pixels

To further improve the segmentation and to reduce false alarms, the colour features developed by Seo in [12] are used. They use the YCbCr colour space to distinguish between fire-like and non fire-like pixels, as the YCbCr colour space offers a better separation of chrominance and luminance information. Especially the chrominance information can be used to classify fire-like pixels. [12]

After converting the Bayer coded (BG) greyscale image I of the size s to an YCbCr image $J = [Y, Cb, Cr]^T$ of size $s/4$ by (3), the binary image F is calculated by (4). In F every pixel marked by 1 (or true) is likely to belong to a fire [12]. Therefore this information can be used to depict fire-like pixels more robustly.

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0{,}2568 & 0{,}2521 & 0{,}0979 \\ -0{,}1482 & -0{,}1455 & 0{,}4392 \\ 0{,}4392 & -0{,}1839 & -0{,}0714 \end{bmatrix} \cdot \begin{bmatrix} I(2{:}2{:}end, 2{:}2{:}end) \\ I(1{:}2{:}end, 2{:}2{:}end) + I(2{:}2{:}end, 1{:}2{:}end) \\ I(1{:}2{:}end, 1{:}2{:}end) \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \qquad (3)$$

$$F(m,n) = \begin{cases} 1, & if\ Y(m,n) > Y_{mean} \wedge Cb(m,n) < Cb_{mean} \wedge Cr(m,n) > Cr_{mean} \\ 0, & otherwise \end{cases} \qquad (4)$$

2.3.3 *Combining foreground, colour segmentation and deflagration detection*

The background segmentation of 2.3.1 and the colour segmentation of 2.3.2 have to be done previously to step one and two of the deflagration detection algorithm described in 2.2. So only pixels which are segmented as foreground (i.e. $G(m,n) = 1$) and whose colours are fire-like (i.e. $F(m,n) = 1$) are considered for the detection. Both the background and the colour segmentation need approximately 1.1 ms per frame (on the same hardware as used in 2.2) and are also mainly computed on the graphics card. Together with the detection algorithm of section 2.2 this results in a calculation time of approximately 3.4 ms per frame, which is still under the demanded 5 ms.

3 LOCALISATION

To locate the deflagration it has to be detected by at least two cameras. Afterwards the position of the detected deflagration has to be determined in each camera image (frame). Then these two 2D positions can be triangulated to one 3D position by the algorithm described in [13].

For the localisation two cameras are used, which are positioned approximately 1 m apart from each other. Their different view of the setting can be seen in Fig. 5 and the rotation and transformation matrices R and t from camera 2 to camera 1 are stated in (5) and (6). The position of the deflagration in each frame is determined by its centre of mass in the binary image that points out fire-like pixels and is calculated during step two of the algorithm described in 2.2. In Fig. 6 the determined positions of a deflagration in the images of camera 1 and 2 are shown. As each camera has a different point of view of the scenario, it might detect the deflagration at a different time. But this is no drawback for the localisation as long as the detection times are not to different (more than 10 ms). Of course the localisation becomes inaccurate by that but as long as the position is within the area where the extinguishing agent is or will be applied, the position can be assumed as precise enough.

$$R = \begin{bmatrix} 0.7727 & -0.0151 & -0.6346 \\ 0.0208 & 0.9998 & 0.0016 \\ 0.6344 & -0.0144 & 0.7728 \end{bmatrix} \tag{5}$$

$$t = \begin{bmatrix} 1031.9 \\ 25.2 \\ 94.0 \end{bmatrix} \tag{6}$$

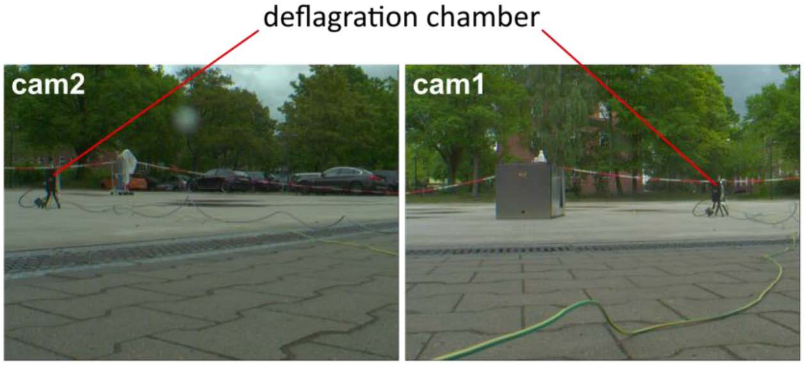


Fig. 5: Views of camera 1 and 2 at the setting

The calculation of the 3D position X is done by the algorithm described in [13], which is presented in Fig. 7. It uses the 2D coordinates X_1 and X_2 of the deflagration in the frames of camera 1 and 2 and the camera matrices P_1 and P_2 which are calculated according to (7) and (8) together with the matrices of the intrinsic camera parameters I_{c1} and I_{c2}. The 3D position X can then be determined relatively to camera 1.

$$P_1 = I_{c1} \cdot \left[\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right] \tag{7}$$

$$P_2 = I_{c2} \cdot [R, t] \tag{8}$$

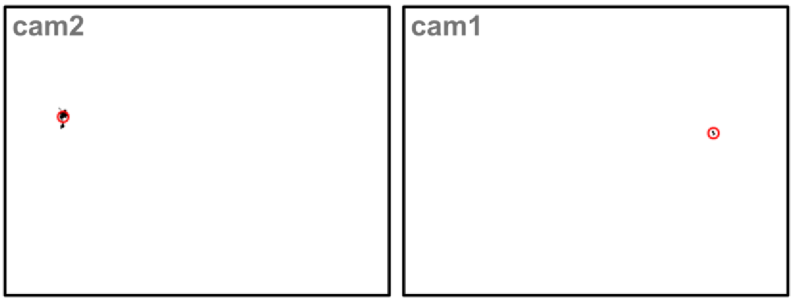


Fig. 6: Detected deflagration (black) and its position (red) in camera 1 and 2

For these first tests two separate deflagrations have been recorded. The first has been recorded by camera 1 and the second by camera 2. The position of the deflagration chamber stayed the same for both deflagrations. Afterwards the recorded images were processed to detect and localize the deflagration. Even with this very suboptimal setting, where two different deflagrations on the same position have been recorded, the position of them was calculated with a horizontal deviation of 12.4 mm, a vertical deviation of 18.4 mm and a depth deviation of 92.9 mm. With the previously measured distance of 5.1 m the horizontal and vertical precision of the system is 4.7 mm, the depth precision – as it is square dependant to the distance – is 23.3 mm. The results are therefore outside of the expected localisation tolerance of the stereoscopic system. But as a deflagration is a very inhomogeneous object it is not possible to detect the exact same point in each camera view. The results are therefore within the expected tolerance to detect a deflagration of a size of about 100x100x100 mm during their emergence phase.

```
A = 4x4 Matrix
A[1, 1:4] = X1[1]*P1[3, 1:4] - P1[1,1:4]
A[2, 1:4] = X1[2]*P1[3, 1:4] - P1[2,1:4]
A[3, 1:4] = X2[1]*P2[3, 1:4] - P2[1,1:4]
A[4, 1:4] = X2[2]*P2[3, 1:4] - P2[1,1:4]

[U,S,V] = svd(A) // singular value decomposition
X = V[1:4,4]
X = X / X[4]
```

Fig. 7: Pseudocode to triangulate two 2D positions X_1 and X_2 to one 3D position X

4 SUMMARY AND OUTLOOK

In 2.2 the deflagration detection algorithm of Schröder has been adjusted to the requirements depicted in 2.1. Furthermore it was extended by a background segmentation and an additional colour segmentation to increase the robustness of the algorithm. Together with these extra features the algorithm can still be computed in less than 5 ms, which is a requirement for the real-time capability. To achieve this, the processing and the structure of the algorithm have been parallelized, and it was implemented on the graphics card of a PC. Additionally the calculation of the location of a detected deflagration has been added. In a first test it could be shown that the determined position should be precise enough for an extinguishing system.

To prove the robustness of the detection it should be tested under more circumstances and also the false alarm rate should be examined. Furthermore the localisation should be tested with a number of deflagrations seen in different perspectives. To improve the localisation and the detection, more cameras could be added. Therefore a fusion algorithm has to be developed in order to compute one 3D position out of several detected 2D positions. This will also enable the system to detect and locate a deflagration if one or more cameras are covered or out of order.

REFERENCES

[1] T. Schröder, K. Krüger, F. Kümmerlen: *Image processing based deflagration detection using fuzzy logic classification*. In: Fire Safety Journal. 65, pp. 1-18, 2014.

[2] T. Celik, H. Ozkaramanli, H. Demirel: *Fire pixel classification using fuzzy logic and statistical color model*. In: IEEE International Conference on Acoustics, Speech and Signal Processing. pp. 1205-1208, 2007.

[3] W.-B. Horng, J.-W. Peng: *A Fast Image-Based Fire Flame Detection Method Using Color Analysis*. In: Tamkang Journal of Science and Engineering. 11(3), pp. 273-285, 2008.

[4] H.-S. Chu et al.: *Method and system for detecting flame*. US Patent 0142822 A1, 2010.

[5] L.-H. Chen, W.-C. Huang: *Fire Detection Using Spatial-temporal Analysis*. In: Proceedings of the World Congress on Engineering. 3, 2013.

[6] L. Song et al.: *The Research of Real-Time Forest Fire Alarm Algorithm Based on Video*. In: Sixth International Conference on Intelligent Human-Machine Systems and Cybernetics. pp. 106-109, 2014.

[7] B. Jiang et al.: *Towards a solid solution of real-time fire and flame detection*. In: Multimedia Tools and Applications. S. 689-705, 2014.

[8] *NATO STANAG 4317*, 02.08.1986. STANAG 4317 – Specification of common characteristics for fire detection and fire fighting systems for future main battle tanks.

[9] T. Schröder, K. Krüger, F. Kümmerlen: *Image processing based deflagration detection using within crew compartments of armored vehicles*. In: Proceedings of the 13th International Conference on Fire Science and Engineering. 2013.

[10] M. Harris: *Optimizing Cuda.* In: Supercomputing 2007, S05, 2007.

[11] B. Jiang, Y. Lu, X. Li, L. Lin: *Towards a solid solution of real-time fire and flame detection.* In: Multimedia Tools and Applications. pp. 689-705, Springer, 2014.

[12] J. Seo, M. Kang, C. H. Kim, J.-M. Kim: *An optimal many-core model-based supercomputing for accelerating video-equipped fire detection*. In: The Journal of Supercomputing. Vol. 71, Nr. 6, pp. 2275-2308, 2015.

[13] R. Hartley, A. Zisserman: *Multiple View Geometry in computer vision.* 2. Edition, Cambridge University Press, New York, 2003.

SHIP CLASSIFICATION IN HIGH AND VERY HIGH RESOLUTION SATELLITE SAR IMAGERY

Virginia Fernandez Arguedas[1] Domenico Velotto[2], Björn Tings[2],
Harm Greidanus[1] and Carlos Bentes[2]

[1] *harm.greidanus@jrc.ec.europa.eu*
European Commission - Joint Research Centre (JRC),
Via E. Fermi 2749, 21027 Ispra (Italy)

[2] *domenico.velotto@dlr.de*
Maritime Safety and Security Lab, Remote Sensing Technology Institute,
German Aerospace Center (DLR), Henrich-Focke-Str. 4, 28199, Bremen (Germany)

Abstract

To serve the security of the maritime domain, ship self-reporting systems provide information on the cooperative vessels. However, non-reporting ships should be also monitored. Satellite images can be used to detect and classify non-reporting ships. Synthetic Aperture Radar (SAR) offers monitoring capabilities regardless of clouds or daylight, and hence it is used for satellite global monitoring. Different satellite SAR systems are deployed, from European ones such as Sentinel-1, to national ones such as TerraSAR-X, presenting very diverse characteristics from their coverage to their image resolution. In this paper, two ship classification methods are presented, a method developed for use on high (20 m) resolution SAR images (Sentinel-1 dataset), and a method developed for use on very high (3 m) resolution ones (TerraSAR-X dataset). In a cross-application experiment, both methods are evaluated on both datasets. The exercise quantifies the methods' performance across resolutions, highlighting their pros and cons in this challenging application.

Keywords: Maritime Surveillance, Ship Classification, Synthetic Aperture Radar.

1 INTRODUCTION

To ensure adequate security of the maritime domain, including the maritime borders, it is necessary to be aware of the shipping activities in the relevant areas of sea. Some areas are covered by shore-based monitoring and observation systems, but for those that are not, satellite-based systems are an efficient alternative. The two main tools for satellite-based maritime surveillance are (a) automatic ship reporting systems and (b) imaging systems. Automatic ship reporting systems such as AIS (Automatic Identification System), LRIT (Long Range Identification and Tracking) or VMS (Vessel Monitoring System) let ships report their identity and position on a regular basis, and are mandated for certain classes of ships by specific (national or international) regulations [e.g., 1]. LRIT and VMS are restricted to government use, while satellite AIS is more widely available on a commercial basis. Data from these systems, and in particular from AIS that covers most ships in the world of 300 gross tonnes and up, enable the tracking of most of the medium and large ships globally. However, not all the AIS-carrying ships are successfully seen by satellite due to noise and interference problems, and ships engaged in irregular activities might turn off their AIS to avoid attention. Moreover, most of the smaller ships do not use automatic ship reporting systems.

In order to also find non-reporting ships out of coastal sensor range, satellite imaging is used, in optical or radar frequencies. The first step in analysing such images for maritime surveillance is ship detection (finding the ships), the second step is ship classification (establishing the type of ship). Although optical images are more readily interpreted for classification, they are hampered by clouds and are not available at night. Radar performs regardless of clouds or daylight and is therefore often preferred for maritime surveillance. Synthetic Aperture Radar (SAR) is the type of radar used from satellite, synthesising the radar image during the few seconds that the satellite illuminates the target.

The signature of a ship in a SAR image is, however, not easily interpreted, making classification difficult. It depends on the detailed shape of the metal structures on the ship, appearing differently depending on viewing geometry. The ship's signature can merge with radar backscatter from the ship's immediate surroundings, and its motions on the waves during the radar illumination time can introduce a blurring. Therefore, classification based on the ship's signature in SAR images is a challenge.

Satellite SAR systems can provide images with a range of spatial resolutions, from over 100 meter to below 1 meter. While the high resolutions are obviously preferred for their better classification power, the image sizes are inversely proportional to resolutions, low resolution images covering up to 450 km as opposed to only 5 km at the very high resolution end. Wide-area maritime surveillance can therefore not be done at very high resolution.

Europe has several satellite SAR systems in operation. Among those, the European Union's Copernicus program offers the Sentinel-1 SAR [2], which provides daily routine coverage of many maritime areas including the European seas. The most frequently produced image type, suitable for maritime surveillance, is the Interferometric Wide (IW) mode Ground Range Detected High resolution (GRDH) product that has 250 km swath width at 20 m resolution.

Among the national systems, the German TerraSAR-X [3] can produce images on demand with swaths between 270 km and 5 km and resolutions, respectively, between 40 m and 0.25 m. A good compromise between coverage and resolution is achieved by the Stripmap imaging mode with a 30 km swath and 3 m resolution (Multi-look Ground range Detected, MGD, product).

This paper discusses approaches to classify ship signatures in images from these two SARs. Although the minimum detectable ship size is an ill defined concept because it depends very strongly on ship type, radar parameters, viewing geometry and ambient conditions, as a rough indicator half of the resolution can be taken. In relation to the use of AIS, the 300 tonnes limit very roughly corresponds to 45 m ship length. For Sentinel-1 (IW-GRDH product), the size ranges of relevance are therefore (a) 10 m to 45 m, for the smaller ships that are still detectable but do mostly not report on AIS; and (b) 45-400 m, for the medium and large ships that are subject to the use of AIS. At 20 m resolution, however, even the large ships do not show much detail. It is therefore too much asked to do a classification into all relevant ship types, which would include passenger ship, tanker, container, bulk carrier, fishing ship, patrol ship, tug, etc. Instead, the ambition to perform classification into any possible ship type is reduced to a classification problem into a restricted set of classes. In many maritime areas of interest, the most frequently occurring types are tanker and cargo. It is still useful to be able to distinguish between those two. The ship reporting data contains the ship type (cargo or tanker), so a disambiguation between those two types in the SAR targets allows deciding on a probable association between a known reporting ship and a target found in the SAR image. Therefore, the classification problem for the Sentinel-1 images is here reduced to a disambiguation between two ship types, cargo and tanker.

For TerraSAR-X, having more resolving power, the classification problem is generalised to maritime object classification adding three further classes of maritime targets: offshore platform, offshore wind turbine and harbour structure.

Having available the two classification schemes, the 2-class disambiguation developed for the lower resolution Sentinel-1 images and the 5-class classification developed for the higher resolution TerraSAR-X images, it is also attempted to do a cross-application. The paper will present results of applying each of the two algorithms to each of the two data sets.

2 DATA

2.1 Sentinel-1 and related reference data

Four Sentinel-1 IW-GRDH images over the Western Indian Ocean were obtained during a period where also AIS data from up to 17 satellites operated by four providers were collected. The providers were exactEarth, SpaceQuest, ORBCOMM/LuxSpace and the Norwegian Coastal Administration. The SAR images were subjected to ship detection with JRC's SUMO detector, which uses a Constant False Alarm Rate (CFAR) algorithm, resulting in a total of 146 targets. Only co-pol (HH and VV) channels were used, without making a distinction between the two. After visual verification of the targets, correlation with AIS ship positions, and selecting only those AIS ships that were unambiguously tankers and cargo ships, a total of 100 targets were retained, 71 cargo ships and 29 tankers. Image chips of 140x140 pixels were extracted around the targets for the classification, and spatially upsampled by a factor of two, to 5 m pixel spacing.

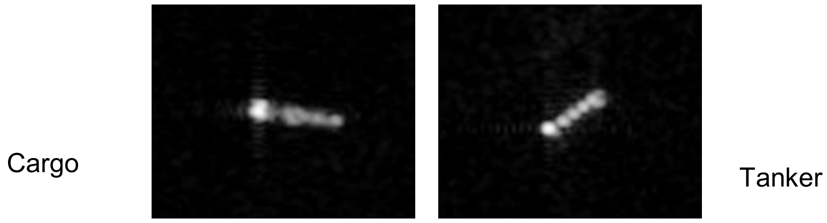


Figure 1. Examples of cargo and tanker classes from the Sentinel-1 dataset.

2.2 TerraSAR-X and related reference data

A total of 75 TerraSAR-X Stripmap MGD images, mostly over the North and Baltic Seas, were acquired in areas that were covered by terrestrial AIS and where known clusters of platforms and wind parks exist. As for the Sentinel-1 data, only co-pol channels were used without distinction. While the full range of incidence angles accessible to the TerraSAR-X Stripmap mode is 20° to 45°, a single such image covers a much smaller range of incidence angles that a single Sentinel-1 IW image. The relatively high number of acquisitions was necessary to capture the variations over incidence angle and marine conditions. The ship detector used for the SAR image dataset was DLR's SAINT detector, also of the CFAR type. The detected targets are automatically collocated with AIS and platform / wind park position databases. If no match has been found, the SAR detected target is discarded from the classification dataset. At the end of this process a total of 683 targets were extracted, representing the 5 classes of interest, see Fig. 2 [4].

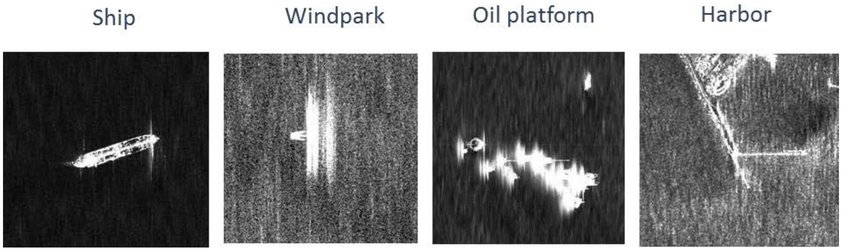


Figure 2. Examples of target classes form the very high resolution TerraSAR-X data set.

Additionally, a subset containing 185 cargo and tanker ship type (distribution 135 cargo and 50 tankers) was extracted to pursue the disambiguation problem. Image chips of 128 x 128 pixels were extracted around the targets and resampled to a common 2.5 m pixel spacing.

3 CLASSIFICATION METHOD

Two different methods for classification were applied to the data; one that was designed for the lower resolution Sentinel-1 data, and one that was designed for the very high resolution TerraSAR-X data.

3.1 Classification method designed for Sentinel-1 images

The image chips around the SAR signatures are first subjected to pre-processing to separate the (brighter) ship signature from the surrounding (darker) background. This consists of edge detection and morphological operations to delineate a contiguous signature outline while discarding isolated bright pixels. The image chip is then rotated so that the signature outline long axis points horizontally, and all pixels outside the smallest rectangular box that contains the signature outline are removed. The result is a reduced, rectangular, horizontal image chip that just fits the ship signature. The reduced chip is split lengthwise into three parts that represent bow, middle and stern.

Two texture measures are computed, Local Binary Patterns (LBP) and Histogram of Gradients (HOG). LBP analyses the immediate neighbours of each pixel, considering local spatial patterns and grey scale contrast [5, 6]. LBP is computed for the entire reduced chip and also for the bow, middle and stern parts separately. HOG calculates the distribution of intensity gradients or edge directions [7]. HOG is computed only for the entire reduced chip.

The classification has two phases, training and testing. In the training phase, a training dataset is analysed to build up a dictionary composed of a representative set of feature samples from each of the two vessel classes, tanker and cargo ship, based on Bag of Visual Words [8]. In the testing phase, the extracted features for each sample are compared with the built-in dictionary to determine the vessel class by finding the nearest neighbour. The general structure of the system is based on the work presented in [9,10]. For each of the two ship types, 15 samples were used for the training. All 100 samples were used for testing.

Each of the classifiers (LBP overall, LBP bow, LBP middle, LBP stern, HOG overall) gives a certain percentage result for correct disambiguation between the two classes cargo ship and tanker. The disambiguation result can be further improved by combining several classifiers. Several combinations using major voting as fusion method were tried out to find the best combination.

3.2 Classification method designed for TerraSAR-X images

Also here, the image chips extracted from the satellite images are first subjected to some pre-processing steps. The details can be found in [4] and consist in radiometric calibration, removing the ocean clutter signature, isolating the target of interest in the chip and normalising the intensity of the target’s signal response. The classification dataset is artificially enlarged performing a set of label-preserving transformations. The resulting augmented dataset is composed of 500 samples per class providing a more balanced classification dataset. For the training step 90% of the data are used and the remaining 10% are used for testing.

The classification model proposed here is based on Deep Neural Network (DNN). In [4] different DNN architectures have been analysed and the initial results encourages the use of Convolutional Neural Network (CNN) for the maritime object classification problem. The initial results obtained using high resolution TerraSAR-X images show that with an ensemble of CNN models an average f1-score of 93% for the considered 5 classes of maritime objects is achieved [4]. The advantage of DNN classifiers is the possibility to learn complex non-linear problems without the need of extracting handcrafted class features. However, the training process might be computationally expensive and an optimal network setting needs to be found. Here we briefly introduce to the final model architecture and topology developed in [4].

Fig. 3 shows the graph representation of the CNN model used. The input fed to the network is the SAR image chip obtained after pre-processing. The connections between neurons inside the network are achieved by a convolution operator and optimised to work with images. The proposed CNN topology is composed of two convolutional layers, alternated by pooling layers in order to reduce the dimensionality, and a fully connected dense (D) layer followed by a softmax (S) layer with dimensions provided in Fig. 3.

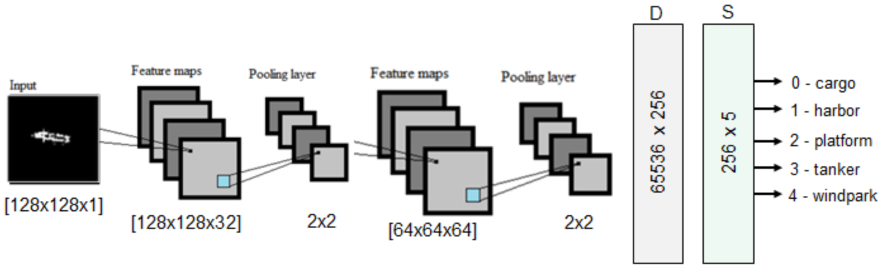


Figure 3. CNN architecture. The input is the chip obtained after pre-processing. The output is the class labels.

4 RESULTS

The classification performances are reported in terms of precision, recall and f1-score.

4.1 Classification results for the Sentinel-1 method

4.1.1 Sentinel-1 method on Sentinel-1 data

A pool of features was proposed to perform ship classification (disambiguation) for Sentinel-1 data in Section 3.1. Averaged over the testing dataset, the five individual classifiers (LBP overall, bow, middle, and stern, and HOG overall) scored 83 % in precision, 69 % in recall and 75 % in f1 for cargo, while for tanker the classifiers decreased their performance achieving 51 % in precision, 70 % in recall and 59 % in f1. The outperforming features were LBP bow, BP stern and HOG. When evaluated separately for cargo ships and for tankers, the scores differ by between 1 to 11 percentage points.

Table 1 summarises the results for combined classifiers. Three combinations are used, being equally-weighted linear combinations of: (1) General LBP, LBP Bow, LBP Middle and LBP Stern; (2) General LBP and HOG; and (3) LBP Bow, LBP Middle, LBP Stern and HOG. As shown in the table, the results obtained by the combined classifiers clearly exceed the individual classifiers, maximising the individual classifiers' complementary information. The results show that Combination 3 gives the best results achieving a 79.0 % in precision, a 77.9 % in recall and a 78.4 % in f1.

4.1.2 Sentinel-1 method on TerraSAR-X data

The same methodology presented in Section 3.1 is applied to TerraSAR-dataset. The underlying idea is to study the performance of the Sentinel-1 method on a more detailed dataset. The method, built for the analysis of low-resolution images, exploits mainly the texture characteristics of the targets since such features tend to be present in low resolution images. However, it neglects local features or key points detectors since such characteristics are not likely to be present in low resolution images.

Table 1. Sentinel-1 method on Sentinel-1 data.

	Combination 1 %			Combination 2 %			Combination 3 %		
	Precision	Recall	f1	Precision	Recall	f1	Precision	Recall	f1
Cargo	85.0	76.1	80.3	80.9	82.1	81.5	85.5	88.1	86.8
Tanker	57.9	71.0	63.8	60.0	58.1	59.0	72.4	67.7	70.0
Avg/Total	71.5	73.5	72.0	70.4	70.1	70.3	79.0	77.9	78.4

Averaged over the testing dataset, the five individual classifiers scored 76 % in precision, 73 % in recall and 77 % in f1 for cargo, while for tanker the classifiers decreased their performance achieving 35 % in precision, 39 % in recall and 36 % in f1. Amongst all individual classifiers, the feature that outperforms the others is HOG achieving 74 % and 43 % in f1 for cargo and tanker respectively. Comparing HOG performance in Sentinel-1 and TerraSAR-X datasets, its performance clearly improves for TerraSAR-X dataset, obtaining the highest tanker representativity.

Table 2 summarises the results for the Sentinel-1 method on the TerraSAR-X dataset. As in the results obtained in Section 4.1.1, Combination 3 presents a good performance when compared with the individual classifiers. However, for TerraSAR-X data, Combination 1 and 2 outperform Combination 3.

Table 2. Sentinel-1 method on TerraSAR-X data.

	Combination 1 %			Combination 2 %			Combination 3 %		
	Precision	Recall	f1	Precision	Recall	f1	Precision	Recall	f1
Cargo	79.2	84.4	81.7	78.1	92.6	84.8	75.8	90.4	82.4
Tanker	48.8	40.0	44.0	60.0	30.0	40.0	45.8	22.0	29.7
Avg/Total	64.0	62.2	62.8	69.1	61.3	62.4	60.8	56.2	56.1

The obtained results reveal that the selected features performed better on the Sentinel-1 dataset, maintaining performance on the TerraSAR-X dataset for the cargo class but presenting a performance drop on the tanker class. The features selected for the Sentinel-1 method neglect details and representative points due to absence of those in the Sentinel-1 dataset and focus on general appearance, texture and edges. Considering the obtained results, other features focusing more on key points and local information might perform better on higher resolution TerraSAR-X data. This could be further addressed in the future.

4.2 Classification result for TerraSAR-X method

4.2.1 TerraSAR-X method on TerraSAR-X data

Table 3 summarises the results for the 5-class problem obtained by an ensemble model built training CNN architectures in Fig. 3 with input SAR image chips at different pixel spacing. It is important to note that the scores have been obtained using only the test dataset (10% of the overall classification dataset) in order to have more reliable performance estimation.

Table 3. CNN model on TerraSAR-X data. Score obtained for each class.

	Precision %	Recall %	f1-score %
Cargo	100	92	96
Harbor	81	90	85
Platform	97	100	98
Tanker	98	97	97
Windpark	89	85	87
avg / total	93	93	93

4.2.2 *TerraSAR-X method on Sentinel-1data*

Table 4 summarises the results for the disambiguation problem (cargo ship - tanker differentiation) using the CNN model on Sentinel-1.

Table 4. CNN model on Sentinel-1 data. Score obtained for the disambiguation classes.

	Precision %	Recall %	f1-score %
Cargo	86	62	72
Tanker	45	76	56
avg / total	74	66	68

These results have been obtained using the Sentinel-1 dataset described in the section 2.1 directly as test set to the model previously trained on TerraSAR-X images. In this sense can be thought as an experiment of “Transfer Learning”. The option to train a model using only Sentinel-1 data will be conducted when a larger classification dataset will be collected and is therefore left for future work.

5 SUMMARY AND CONCLUSION

In this paper, two ship classification methods were presented and evaluated over two datasets with different image resolutions. One method is feature-based, developed on the lower resolution (20 m) Sentinel-1 IW images; the other is image-based, developed on the higher resolution (3 m) TerraSAR-X Stripmap images. The Sentinel-1 method exploits general appearance features, texture and edges, neglecting local features and details. The TerraSAR-X method uses CNN for the classification, avoiding the extraction of handcrafted class features and building the model directly from the images. In a cross-application test for the sub-problem of disambiguation between cargo ship or tanker (two-class classification), it was found that each method performs best on the data for which it was designed. This is attributed to the fact that they exploit their inherent benefits, i.e., the TerraSAR-X method was trained directly on its images, which is possible due to their high quality, while the Sentinel-1 method uses feature-based analysis to compensate for the lower image resolution. However, both methods present promising results in this preliminary experiment.

The cargo-tanker disambiguation with Sentinel-1 data is successful, despite the fact that the Sentinel-1 SAR IW signatures for cargo and tanker ships look quite similar by eye. Nonetheless, the TerraSAR-X data have much more potential for classification than the Sentinel-1 data. A classification into 5 classes that is possible with TerraSAR-X was not attempted with Sentinel-1.

In the future, a larger image dataset will be built and further experiments will be conducted. Moreover, multi-class ship classifiers will be targeted in an attempt to contribute to increased security in the maritime domain.

ACKNOWLEDGMENTS

Sentinel-1 data are © Copernicus 2014-2016.

TerraSAR-X data were provided by the German Aerospace Center (DLR) via AO accounts OCE2917 and OCE1045.

AIS data from Norwegian satellites were obtained courtesy of the Norwegian Defence Research establishment (FFI) and the Norwegian Coastal Administration under the PMAR project.

REFERENCES

[1] Greidanus, H., Vespe, M. and Alvarez, M. (2016). *Detection of anomalous behaviour in ship reporting data for improved maritime security*. Proc. 11th Future Security Conference, Berlin, 13-14 Sep 2016, Fraunhofer Group for Defence and Security VVS (these proceedings).

[2] European Space Agency (2013). *Sentinel-1 User Handbook*. GMES-S1OP-EOPG-TN-13-0001, 1 Sep 2013.

[3] Eineder, M., Fritz, T., Mittermayer, J., Roth, A., Boerner, E., and Breit, H. (2008). *TerraSAR-X Ground Segment, Basic Product Specification Document*. Cluster Applied Remote Sensing (CAF), Oberpfaffenhofen, Germany. Report No. TX-GS-DD-3302.

[4] Bentes, C. Velotto, D. and Lehner, S. (2015). *Target classification in oceanographic SAR images with deep neural networks: Architecture and initial results*. Proc. IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Milan, 26-31 Jul 2015, pp. 3703-3706.

[5] Ojala, T., Pietikäinen, M. and Harwood D. (1994). *Performance evaluation of texture measures with classification based on Kullback discrimination of distributions*. Proc. 12th IAPR International Conference on Pattern Recognition, Jerusalem, 9-13 Oct 1994, Vol. 1, pp. 582-585.

[6] Ojala, T., Pietikäinen, M. and Harwood D. (1996). *A Comparative Study of Texture Measures with Classification Based on Featured Distributions*. Pattern Recognition, Vol. 29, pp. 51-59.

[7] Dalal, N. and Triggs, B. (2005). *Histograms of Oriented Gradients for Human Detection*. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Diego, 20-25 Jun 2005, Vol. 1, pp. 886-893.

[8] Sivic, J. and Zisserman, A. (2003). *Video Google: A text retrieval approach to object matching in videos*. Proc. 9th IEEE International Conference on Computer Vision, Nice, 13-16 Oct 2003.

[9] Fernandez Arguedas, V. (2015). *Texture-based vessels classifier for electro-optical satellite imagery*. Proc. IEEE International Conference on Image Processing (ICIP), Quebec, 27-30 Sep 2015.

[10] Santamaria, C., Stasolla, M., Fernandez Arguedas, V., Argentieri, P., Alvarez, M. and Greidanus, H. (2015). *Sentinel-1 Maritime Surveillance: Testing and Experiences with Long-term Monitoring*. JRC98532, EUR 27591 EN, ISBN 978-92-79-53960-2 (PDF), ISSN 1831-9424 (online), doi: 10.2788/090400, Luxembourg: Publications Office of the European Union.

AUTOMATED BORDER CONTROL WITH A HARMONIZED MODULAR REFERENCE SYSTEM
-
EXPERIENCES IN THE EU RESEARCH PROJECT FASTPASS

Gunther Grasemann[1], Mario Kaufmann[1] and Elisabeth Peinsipp-Byma[1]

[1] *{gunther.grasemann, mario.kaufmann, 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 as well as 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 of the EU have been supported by automated border control systems (ABC) during the last years. The FP 7 EU project “FastPass” defines a European reference architecture for ABC systems relating to air, sea and land borders. The main objectives are lower cost, higher security for the border guards and increased acceptance for the travelers, authorities, politicians and the public. The FastPass consortium is a balanced mixture from industry, research and authorities/users of ABC systems with 27 partners from 9 countries (Austria, Germany, Finland, UK etc. like the Austrian AIT (coordinator), the Finish VTT and the German Fraunhofer Society.

The main objectives are derived from the following motivating challenges: increased passenger flows, increased spoofing attacks, increased security requirements. They are higher process speeds, anti-spoofing measures, system risk assessment, harmonization, variety in usage, better usability and acceptance.

1 INTRODUCTION

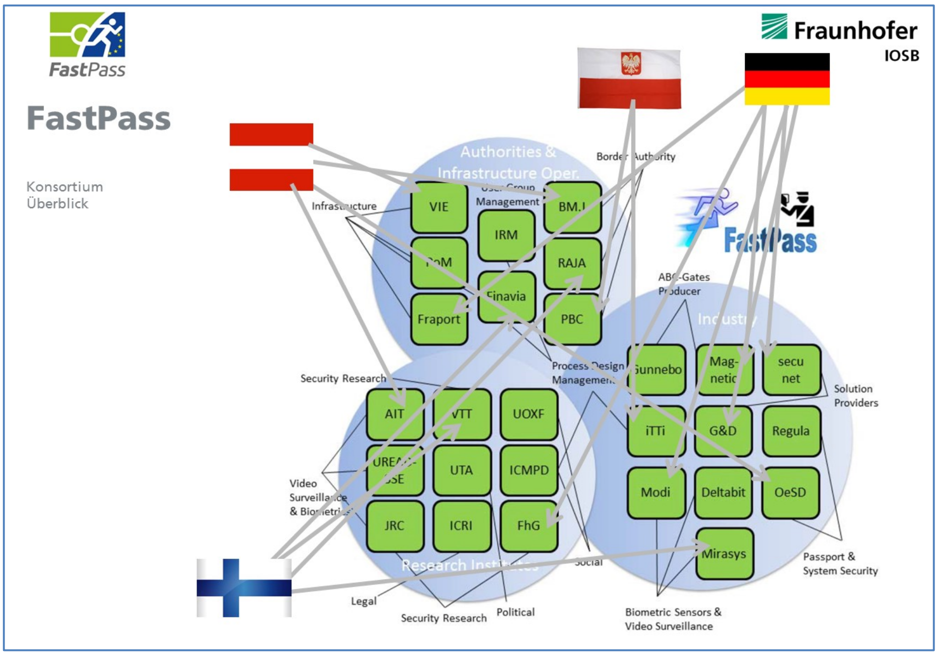


Figure 1: FastPass Consortium

In the last years, ABC systems have been introduced in several countries in Europe and other countries like Canada, Hong-Kong and the USA, in order to encounter the rapidly increasing amount of travelers. A lot of experiences have been gathered, many problems have been solved and many advantages discovered. However, there are still problems in the range of spoofing, missing usability and acceptance, operation failures and many more (comp. [1], [2], [5], [10]).

The FP7 IP FastPass has been set up to define a reference system architecture for European ABC systems and increase usability and acceptance and define the legal framework with respect to privacy and data protection([10], [3]).

2 PROJECT OVERVIEW AND OBECTIVES

The overall objectives of FastPass are shown in Figure 2: After the definition of conceptual items like border crossing concepts for the respective border types and architecture definitions, the focus lies on the integration into present concepts and installation in cooperation with the European authorities and the facilities. Furthermore, acceptance and usability tests shall be performed and lead to an over-all evaluation with lots of requirements and criteria defined in an evaluation framework that will perform data based automatic evaluation loops generating special views for the interpretation and discussion of the results (comp. [7]).

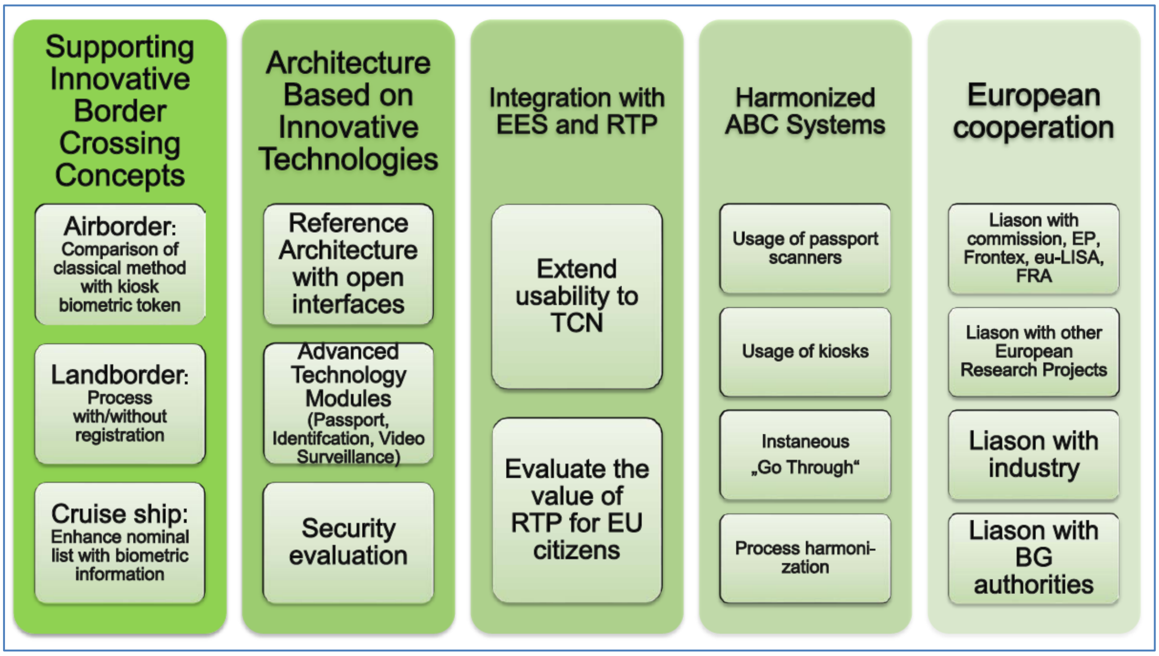

Supporting Innovative Border Crossing Concepts
Airborder: Comparison of classical method with kiosk biometric token
Landborder: Process with/without registration
Cruise ship: Enhance nominal list with biometric information
Architecture Based on Innovative Technologies
Reference Architecture with open interfaces
Advanced Technology Modules (Passport, Identifcation, Video Surveillance)
Security evaluation
Integration with EES and RTP
Extend usability to TCN
Evaluate the value of RTP for EU citizens
Harmonized ABC Systems
Usage of passport scanners
Usage of kiosks
Instaneous „Go Through“
Process harmoni-zation
European cooperation
Liason with commission, EP, Frontex, eu-LISA, FRA
Liason with other European Research Projects
Liason with industry
Liason with BG authorities

Figure 2: Objectives of FastPass

The requirements for the reference architecture are innovative border crossing concepts, the next-generation sensors, novel frameworks, software and algorithms, on-the-move biometric identification, speed, quality, reduced intrusiveness, counter spoofing and costs. Three typical installations at the different border types air, sea and land are currently being installed, tested, demonstrated and evaluated. They realize several air border scenarios with different paradigmatic concepts in Vienna, a cruise-ship scenario with special document handling at the port of Piraeus, a land border scenario with travelers remaining in the cars what is solved by moveable terminals, ANPR for the detection of the vehicle and driver and co-driver check at Moravita in Romania.

All scenarios are evaluated using a comprehensive framework with requirements, criteria, measurement descriptions, a methodology for a holistic risk and security assessment, a collection of threats (with type, impact, exploitability and mitigation strategy) and a collection of advanced tools for the evaluation processes.

The architecture concepts for all border types are based on innovative technologies with new biometric sensors, advanced video detection for the control of the passenger's behavior, queue length optimization module for the optimized balancing between the different lines and kiosk concept for the optimization of the complete process at air borders.

The results of FastPass will lead to reference architecture with increased security, with resistance to attacks on the document scanner, with resistance to biometric spoofing, with a risk and security assessment by dedicated methodology, a user interface developed with extensive feedback from the border guards, processes developed with extensive evaluation from traveler groups and privacy and data protection.

3 DEVELOPMENTS

In addition to the architecture, several developments have been performed in the range of FastPass in order to improve the control process. Especially, the problem of spoofing has been encountered by several by several improvements in the biometric process like substantiated face recognition, a new iris scanner system and a fusion algorithm that compares and combines biometric information on a symbolic level.

For the effectiveness of the process, several measures have been added to the over-all process like queue length calculation and optimization, the providence of kiosk systems for the document reading.

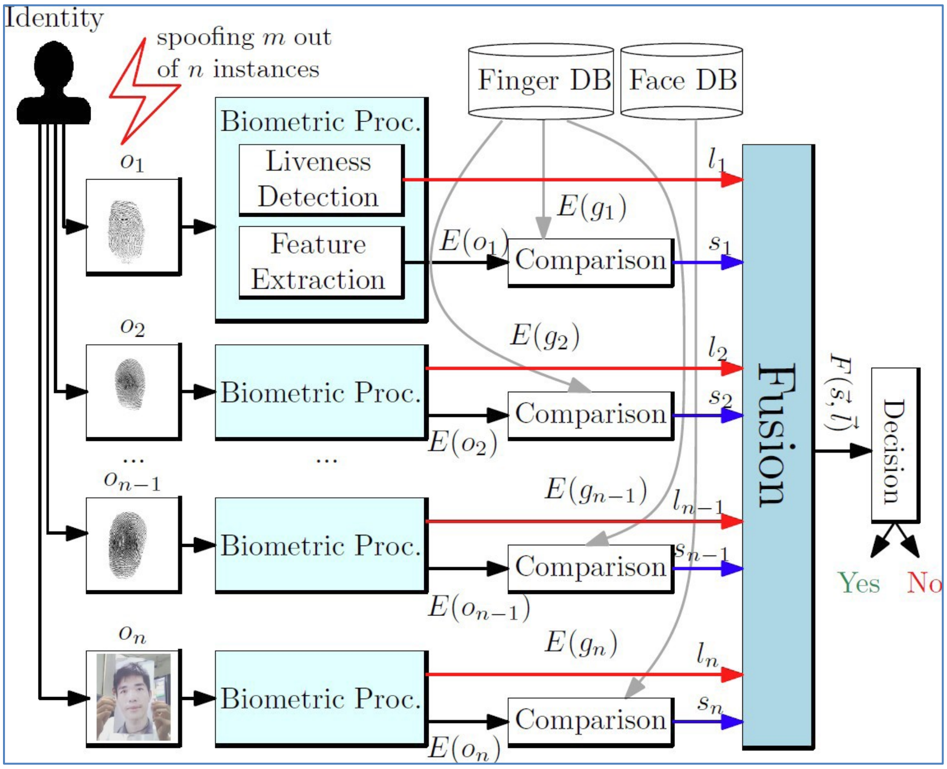


Figure 3: Schematic paradigm for counter spoofing fusion

4 SCENARIOS

For testing, demonstration and evaluation of the reference system, three installations have been developed and realized for the three border types air, sea and land in Vienna (Schwechat airport), the port of Piraeus in Greece and at the land border between Romania and Serbia in Moravita. All generic features of the systems are mainly equal, only in the special properties for the respective border type are differences.

At the air border, special tests with the usage of kiosk systems have been performed. To accelerate the complete process, it has been divided into two steps: the document reading process of the electronic part of the passport and the biometric measurement. The electronic document reading is performed by kiosk systems (comp. Figure 4). For the appointment to the second step of the process, the biometric detection and authentication, a token is required that is reliable enough for a unique appointment of the traveler. In a first step, this is the passport number which can be read optically in the beginning of the second phase in order to increase the speed. In a second step, the face of the traveler will be used as a token for the resume of the process at the mantrap.

For the optimization of the queuing process, there has been a development by AIT for the video based determination of the queue length (comp. Figure 5) and a queue balancing system developed by Fraunhofer IOSB to optimize the distribution between the single queues with an estimation of the respective duration at the single gates.

The installations at the sea border (Piraeus) and the land border (Moravita, Romania) are shown in Figure 6 and Figure 7.

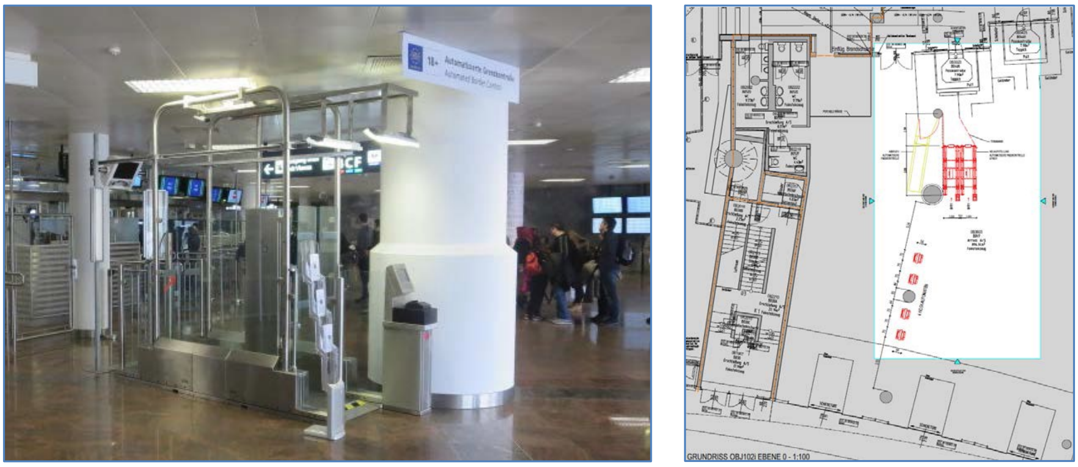


Figure 4: Air border installation at Schwechat airport

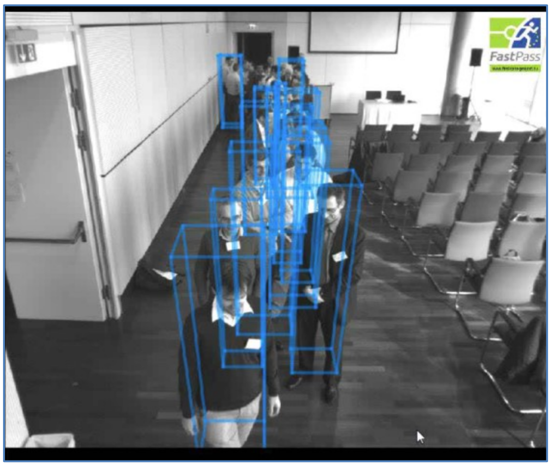


Figure 5: Queue Length Detection and Measurement

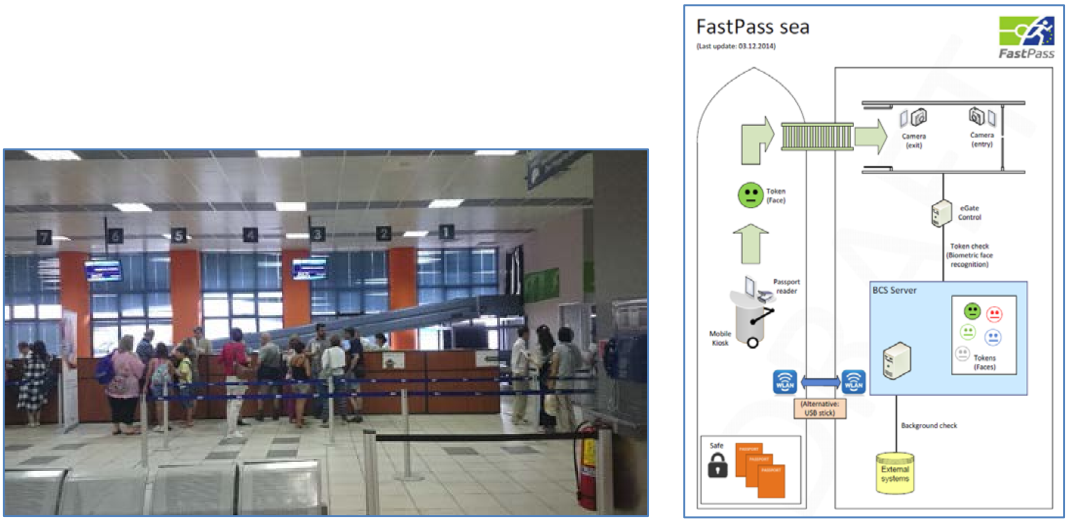


Figure 6: Sea border installation at the port of Piraeus

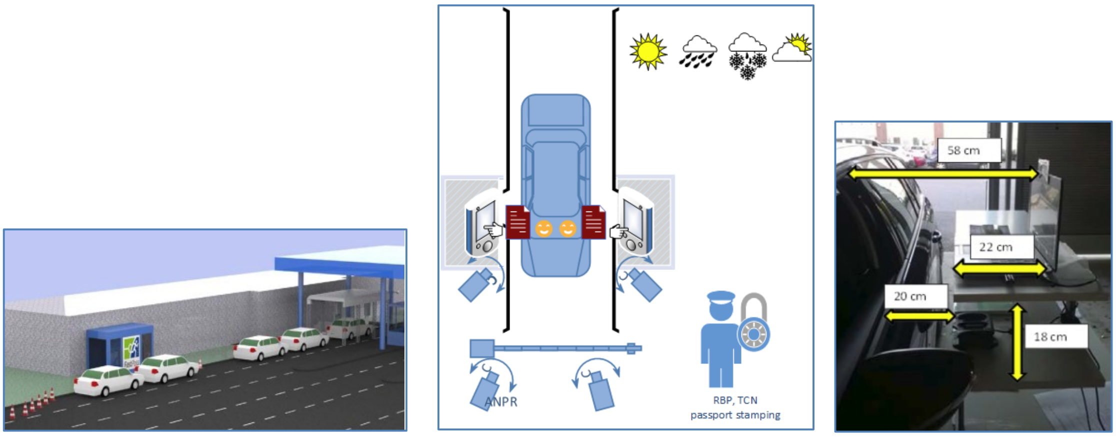


Figure 7: Land border installation in Moravita (Romania)

5 CONCLUSION

For the border 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] ABC4EU
Automated Border Control Gates for Europe
abc4eu.com/docs/Abc4eu_leaflet_19102015.pdf

[2] BAA 2009
Automated Border Control (ABC) Trial Stansted Airport 2008-9 - Summary Report
https://www.accenture.com/t20150523T054056__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_2/Accenture-ABC-Trial-Summary-Report.pdf

[3] Dimitrova, D.
Automated Border Control (ABC) in the EU: Legal Aspects: Legality, Privacy and Data Protection
https://www.fastpass-project.eu/sites/default/files/ABC_Legal.pdf

[4] 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.

[5] FRONTEX
Best Practice Operational Guidelines for Automated Border Control (ABC) Systems Research and Development Unit
frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_for_Automated_Border_Control.pdf

[6] Gorodnichy, D. O. et al.
Automated Border Control systems as part of e-border crossing process
biometrics.nist.gov/cs_links/ibpc2014/presentations/14-NIST-ABC-eBorder-Gorodnichy.P.pdf

[7] Keim, D. et al.
Mastering the Information Age Solving Problems with Visual Analytics
ISBN 978-3-905673-77-7, http://diglib.eg.org

[8] Koole, G.
Optimization of Business Processes: An Introduction to Applied Stochastic Modeling
Department of Mathematics, VU University Amsterdam, March 30, 2010

[9] Liu, H. X. et al.
Real-time queue length estimation for congested signalized intersections
Transportation Research Part C 17 (2009), 412-427

[10] Oostveen, A.-M., Kaufmann, M., Krempel, E. , Grasemann, G.
AUTOMATED BORDER CONTROL: A COMPARATIVE USABILITY STUDY AT TWO EUROPEAN AIRPORTS
https://www.fastpass-project.eu/sites/default/files/IHCI.pdf

[11] Vester, F.
Die Kunst vernetzt zu denken - Ideen und Werkzeuge für einen neuen Umgang mit Komplexität
München: Deutscher Taschenbuch Verlag, 2002.

[12] 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)

VIDEO-BASED LOG GENERATION FOR SECURITY SYSTEMS IN INDOOR SURVEILLANCE SCENARIOS.

David Münch, Stefan Becker, Hilke Kieritz,
Wolfgang Hübner, and Michael Arens

david.muench@iosb.fraunhofer.de
Fraunhofer IOSB, 76275 Ettlingen (Germany)

Abstract

In the EU FP7-SEC-2012-1-313034 project SAWSOC (Situation AWare Security Operations Center) the objective is to achieve “the convergence of physical and logical security technologies, particularly improving correlation techniques across existing technology silos (video surveillance, access control, network monitoring, etc.)”.

In this paper two use cases developed in SAWSOC are presented in the perspective of video-based log generation. The first is a critical infrastructure where we log visual observable occurrences in a critical server room. The second is a soccer stadium environment where we log the patrol path of guards and ensure the correct handling of each checkpoint of their patrol path.

Our approach consists of several generic computer vision modules and spatio-temporal data fusion using scene dependent knowledge. Each component of its own does not allow to make any statements about the current situation in the observed area. Instead, the sum of all components has to be considered.

Keywords: SAWSOC, visual log-file generation, security system, indoor visual surveillance.

1 INTRODUCTION

Security services in the physical and in the logical domain have been undergone much progress in the last decades. Services in the physical domain are e.g. video surveillance or identity and credential management software systems. Whereas monitoring network traffic and logging (computer) systems’ events are to be considered in the logical domain. Both, the physical and the logical services are stable and mature. Unfortunately, they have been developed independently of each other and do not make use of each other. All of these services are monitored in Security Operation Centers (SOC). Up to now, SOCs have been created for diversified and tailored needs, with independent approaches for physical and logical security purposes.

1.1 The SAWSOC project

In the EU FP7-SEC-2012-1-313034 project SAWSOC (Situation AWare Security Operations Center) the objective is to overcome these disadvantages mentioned above. The main objective is to “identify, implement, and validate techniques for achieving the convergence of physical and logical security technologies, particularly improving correlation techniques across existing technology silos (video surveillance, access control, biometrics, security information and event management (SIEM), network monitoring, Business Activity Monitoring and Business Process Monitoring, etc.)”. The SAWSOC project started on 1st November 2013 and will ended on 30th April 2016. The consortium consists of different companies and research institutions from Italy, Finland, Germany, Ireland, Israel, Poland, and the UK.

1.2 Use cases

Three prototypical use cases have been defined. The first one is a critical infrastructure for air traffic management in Italy. There, SAWSOC will protect the air traffic control infrastructure from malicious attacks. Additionally, inside jobs from companies' employees will be considered, too. The second use case is a critical infrastructure for energy production and distribution in Israel. There, SAWSOC will be applied on top of Supervisory Control and Data Acquisition (SCADA) systems. Last, a soccer stadium in Krakow, Poland, will be protected.

1.3 Summary and contribution

As a partner of the SAWSOC project, we provide video surveillance modules. They are more than basic image processing methods; they are context sensitive video analysis comprising of different levels from image processing, to scene understanding, and up to using background knowledge.

In this paper we present the advanced video surveillance modules for the SAWSOC project; in detail these are person detection and tracking, change detection, and skin detection as basis for information fusion applied in the scenario of infrastructure manipulation detection and in the scenario of the soccer stadium.

1.4 Related work

The survey papers [1-5] address the detection of meaningful events and situations in video surveillance. We can distinguish between two different strategies in extracting semantic information from raw videos. One kind are direct approaches. They use massive training data and methods from machine learning. They work as black box approaches: As input data the videos are fed in and the recognized events and situations are the results. The detailed comprehension of the underlying decision function is difficult. Nevertheless, direct approaches are powerful if there is enough training data. The other kind of approaches are hierarchical approaches, where the problem is partitioned into different layers in which different subproblems are addressed. The underlying formal model in hierarchical approaches goes from probabilistic graphical models to formal grammar and finally to description-based approaches such as higher order formal logic. Probabilistic graphical models are powerful but inference is complex, formal grammars are less flexible but easy to model. In contrast to these complex approaches, it is often handy to use established and easier usable methods, such as modelling background knowledge using a basic deterministic finite automaton.

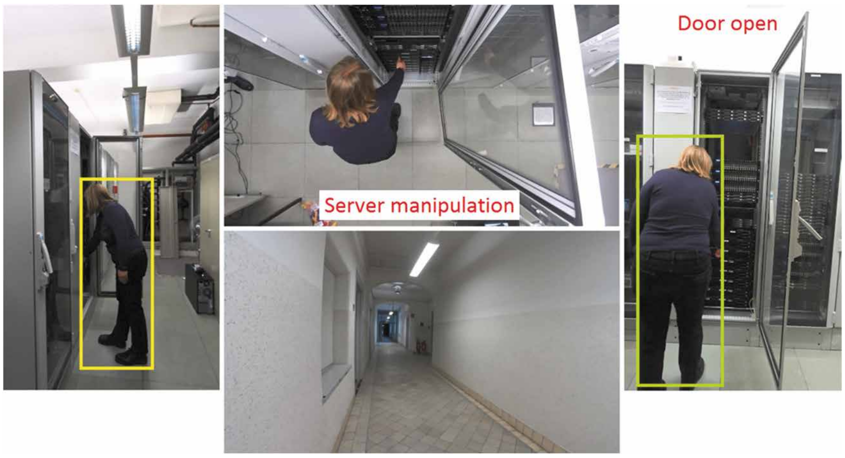


Fig. 1. Example views from the first sequence of the infrastructure manipulation use case. Each camera has a different view, which allows the detection of different events in each view.

2 VIDEO SURVEILLANCE MODULES

As physical manipulation of infrastructure is assumed to be done by people, the core component is a person detector and tracker. This component is based on offline learning of a general person model and online learning of the individual person's model [7]. A second component is a modified version of an abandoned object detection method to detect physical changes in the environment caused by a present person. We use the approach of Becker [8] with an IMM filter setup as presented in [9]. Finally, basic skin detection or door-status detection methods support the visual observable events. The video surveillance modules are described in detail in [10].

3 USE CASES

In this section two use cases from the SAWSOC project are addressed in the perspective of video-based log generation.

3.1 Infrastructure manipulation

In this section, a prototypical infrastructure manipulation setting – one of SAWSOC's use cases – is described. When running a critical infrastructure, special attention is needed to log the panned maintenance or to detect suspicious events. To provide data for this use case, we recorded four different scenes with four different persons using four synchronized cameras in a critical server room environment.

Each person is performing all or some of the subsequent five basic events:

1. Enter server room.

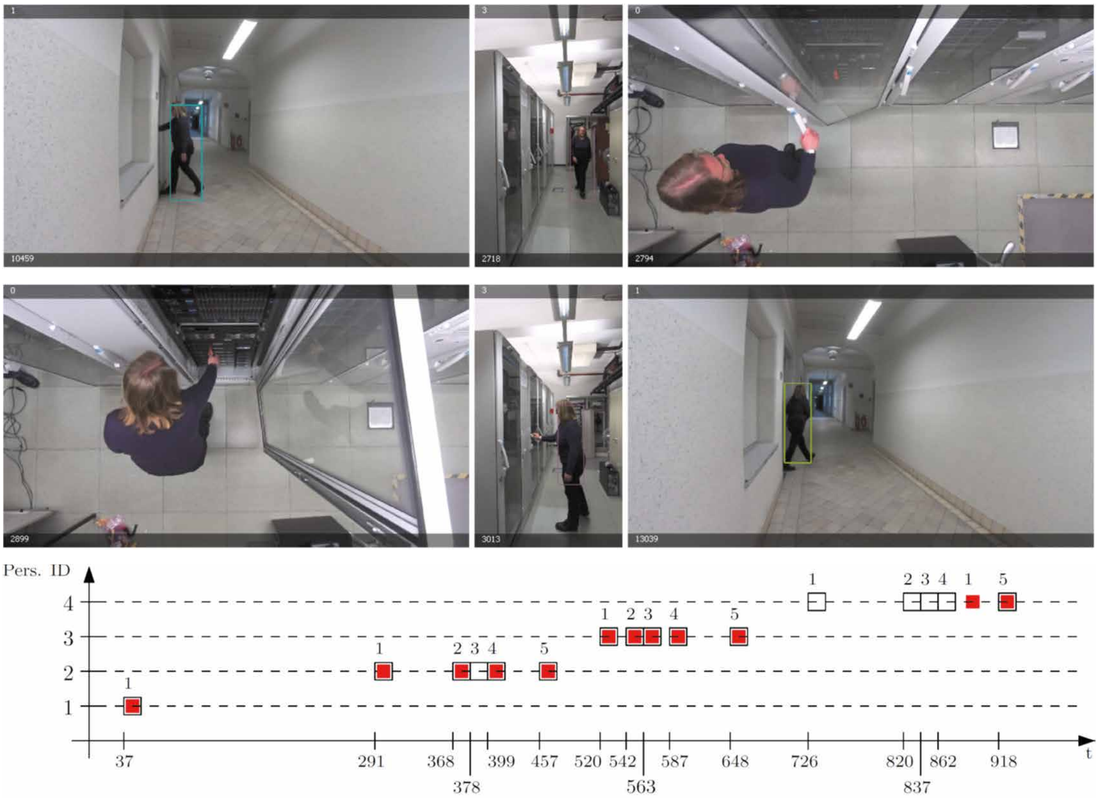


Fig. 2. Qualitative (top) and quantitative (bottom) evaluation in the first scene. The images show the events "enter the server room", "open server door", "server manipulation", "close server door", and "exit server room". Unfilled square stands for groundtruth, a filled square represents a detection. From [6].

2. Open server door.
3. Server manipulation.
4. Close server door.
5. Exit server room.

In Figure 1 some snapshots of the first sequence of our recordings are shown. The four cameras have different views, one is in the aisle in front of the server room, one is on the ceiling, one is in front of the servers, and one is parallel according to the servers. The precise evaluation of this use case can be found in [6]. The deterministic finite automaton (see Figure 5, [6]) is applied on top of the video surveillance events. In Figure 2 the results of the first scenes are shown. It can be seen that each time the person enters the server room again, it gets assigned a new person ID. Because no person identification is done, it is valid that the tracker assigns a new person ID for every new person track. At time 378 the server manipulation event was missed. This was due to only opening the server door very little, so that the cameras could see only the server door there. Later, at time 726 ff., the person was missed by the person detector, thus, all modules building upon this information will fail, too. In conclusion it can be said, that the sum of video surveillance events and moderate knowledge encoded in a deterministic finite automaton allows generating more complex events.

3.2 Security guard patrol

In this section the SAWSOC use case in the soccer stadium is addressed. To ensure security, guards have to walk designated patrol paths in the inside of the stadium. In this use case we log the patrol path of a guard and ensure the correct handling of each checkpoint of the patrol path. The soccer stadium's camera coverage is huge, but not every area is covered in detail. Thus we use the person detector and tracker mentioned above to find persons in the different cameras' images and then use additional scene information to detect the guards in the checkpoint regions. The positions of each guard during its patrol path are logged and deviations are reported. Background knowledge about the ground plane is added to improve the runtime of the person detector and tracker.

The soccer stadium dataset was recorded between 11/2015 and 02/2016 in the Cracovia stadium with cooperation of the Cracovia Football Club and Comarch (T. Grabowski, J. Szczebak). The dataset consists of video recordings with fourteen cameras covering security guards patrol path through the hallway inside the stadium. The entire dataset covers six different scenes, in which the security guards act differently. Figure 3 depicts a security guard (orange) together with an ordinary person.

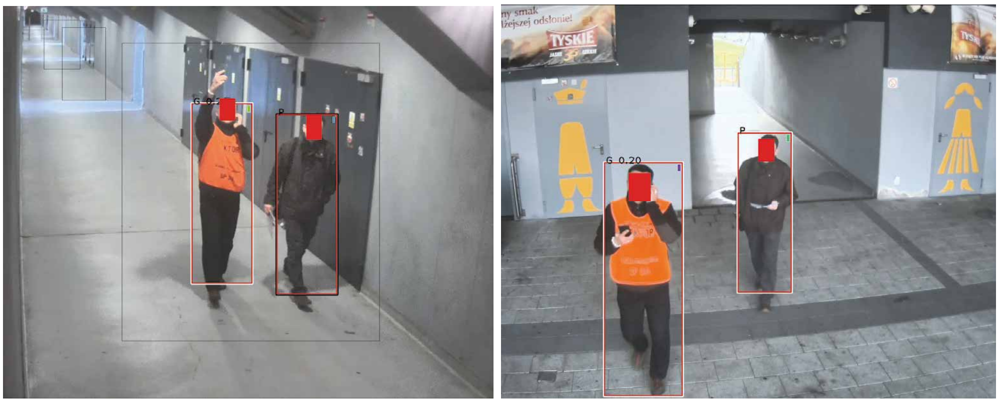


Fig. 3. A security guard and an ordinary person are walking along the hallside inside the soccer stadium. The guard is detected as guard and its position gets logged.

4 CONCLUSION

In this paper, we summarized in short the SAWSOC project and its main goals. Then, we addressed the video surveillance modules as generic and specific building block. Finally, all the modules were put together to show their strength in two use cases: In the infrastructure manipulation use case and in the security guard use case. We used existing technologies to build more complex systems and the results show that the whole is more than the sum of its parts. Future work after the end of the SAWSOC project is the integration of the video surveillance modules into the products enabled by SAWSOC.

ACKNOWLEDGMENTS

This work is supported in part by the European Unions Seventh Framework Programme for research, technological development and demonstration under grant agreement FP7-SEC-2012-1-313034 (SAWSOC-Project).

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] Münch, D., B. Hilsenbeck, H. Kieritz, S. Becker, A.-K. Grosselfinger, W. Hübner, M. Arens. (2016) Detection of infrastructure manipulation with knowledge-based video surveillance. Proc. of the Security and Defence Conference SPIE 2016, Edinburgh, UK.

[7] 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.

[8] Becker, S., D. Münch, H. Kieritz, W. Hübner, and M. Arens (2015). Detecting Abandoned Objects using Interacting Multiple Models. Proc. SPIE Volume 9652 Optics and Photonics for Counterterrorism, Crime Fighting, and Defence.

[9] Becker, S., H. Kieritz, W. Hübner, and M. Arens (2016). On the benefit of state separation for tracking in image space with an Interacting Multiple Model Filter. Prof. of 7th International Conference on Image and Signal Processing (ICISP), Trois-Rivières, QC, Canada.

[10] Münch, D., S. Becker, H. Kieritz, W. Hübner, M. Arens (2015). Knowledge-based Situational Analysis of Unusial Events in Public Places. Proc. of the 10th Future Security Research Conference, Berlin, Germany.

INTEGRATED OBJECT TRACKING AND OBJECT RE-IDENTIFICATION IN INTELLIGENT VIDEO SURVEILLANCE SYSTEMS

Andrew Spence, Vit Libal [1], Artem Rozantsev [2]

[1] {andrew.spence,vit.libal }@honeywell.com
Honeywell ACS Global Research Labs Prague Prague

[2] artem.rozantsev@epfl.ch
School of Computer & Communication Science, Ecole Polytechnique Fédérale de Lausanne

Abstract

This paper presents a novel approach to object tracking in multi-camera video surveillance systems. Most currently deployed video surveillance systems display the information in a “camera-centric” way where the security system operator(s) viewing several or several tens of camera views and it takes significant efforts and skills to establish the correspondence of the camera views in a monitored space. Understanding the actors and activities in the space or searching for an important event therefore is highly demanding work in terms of mental effort. An alternative way of monitoring the secured space is the “actor-centric” approach whereby the operator observes reliable trajectories of actors suitably represented e.g. by augmenting a plan view schematic. This approach offers the security operator effortless situation awareness and efficiency when performing off-line tasks such as searches for any security-related event or information. However, in surveillance systems with large numbers of overlapping and non-overlapping camera views, and with significant object traffic, the actor trajectories must be extracted reliably and accurately to realize a dependable “actor-centric” monitoring system. Object tracking and re-identification are techniques which can be used to address this problem. While the two have been the subject of study of numerous technical papers5-8, they have always been treated independently. Furthermore, their quality was measured using metrics wholly unrelated to the purpose of the automated/semi-automated video surveillance systems. In this paper, we describe how the top state of the art object tracking [1], [2] and re-identification [3], [4] techniques can be combined to maximize the benefit to the security operator. We also establish new metrics that quantify this benefit in a meaningful, practical way and utilise them to demonstrate how well the tracking and re-identification techniques perform individually and the advantage of combining them together.

Keywords: Multi-camera video surveillance system, person tracking and re-identification, integrated security, situation awareness, operator efficiency.

1 INTRODUCTION

Person tracking and person re-identification techniques hold high potential for creation of novel tools that assist operators of multi-camera security video surveillance systems. Person tracking enables the operator to quickly establish and easily maintain his situation awareness – it allows an instant overview of positions and motion of people in the monitored space and serves as a first step towards security decision making. The potential contribution of tracking to security is remarkable in the multi-camera scenarios, where the operator has to follow a high amount of static camera views to maintain his situation awareness. Each camera presents a partial view of a monitored environment that is highly influenced by the camera’s position, viewing angle, available lighting etc. The person tracking techniques allow information from various camera views to be combined into a global representation understandable to the operator.

The state of the art for multiple camera, multiple object tracking algorithms is comprehensively outlined in [9]. For purposes of this work, we have selected method described in [1], [2]. It consists of a background subtraction based object detection step, computationally efficient combination of detections from multiple camera views, and track forming based on optimal graph path search. Clear and efficient handling of the multiple camera views integration problem, overall computational efficiency and a straightforward means of integration of additional input features were among the reasons for choosing this approach. The output of the tracking algorithm takes the form of a trajectory represented as a sequence of points in the global coordinate system. The track of each object is then presented to the operator as a point representing the estimate of the current object's position and a curve representing the most recent part of object's trajectory, both overlaid on the image of map/floorplan of the monitored space.

The person re-identification aims to find re-appearance(s) of the same person/object in available camera views and hence is helpful in maintaining immediate situation awareness in scenarios with coverage gaps (by bridging the track over the gaps) or in analyzing recordings from the multi-camera video surveillance system in forensic search, for example, facilitating rapid discovery of the re-appearance or co-occurrences of specific persons. The re-identification techniques consist of a signature building step – each person's signature is built based on appearance descriptors derived from single or multiple images of the person. Then, in the matching step, each signature of interest is compared against the pool of other signatures collected from the data of interest.

An overview of the state of the art in the field of person re-identification is given in [5]. In our work, we use the re-identification method of Bak et al described in [3], [4]. This method uses covariance descriptors as features, extracted from the body region of the detected person and builds the signature from multiple subsequent detections of the person.

While, in the prevailing technical literature, the object tracking and person re-identification technologies are developed and evaluated separately, they have potential to complement each other and work as a part of the same tool/service in the two above named tasks – in establishing and maintaining situation awareness and in forensic search, which are central to the operator's goals. For the situation awareness, the person re-identification needs to be integrated on top of the tracking to help the operator to cover gaps in the camera coverage. For forensic search, the tracking may be added on top of the re-identification algorithm so that it reduces the search space by applying the spatio-temporal constraints for the signature correspondences.

Figures 1 and 2 depict an example of a simple space monitored by six fixed cameras. The floorplan is approximately rectangular. The field of view (FOV) of each surveillance camera is indicated by a coloured spaces in the figure 2. The right side of the floorplan is covered by five cameras with partially overlapping FOVs. Each camera is viewing a different important part/element of the space creating partial gaps among the FOVs. The rightmost part of the floor is covered by a single camera viewing the entrance door. This configuration also creates a large gap between the FOV of the rightmost camera and the other cameras. While this example was specifically designed for purposes of this work, incomplete coverage is a common case in video surveillance systems – the cameras are usually placed at the most important places only leaving gaps of various sizes between the camera's FOVs. If the object tracking system is employed to assist the operator to monitor such a space, the track of a person can only be captured within a FOV or across connected FOVs; as the person leaves the boundary of a camera FOV, the computed track terminates as there are no data. If the same person reappears in another camera's FOV after "crossing the coverage gap", which of course happens after some time, the operator will have to expend effort to recognize it is the same person. Obviously, if the re-identification technique is used to complement the tracking in a similar scenario, it may spare the operator this effort and enable him to effortlessly maintain his situation awareness.

Similarly, in the case of forensic search, when the operator seeks when/where a certain subject reappeared in the recordings previously acquired by a video surveillance system like the one in our example, the re-identification technology is used to help the operator to identify and rank possible matches. Here, the available tracking information, i.e. knowledge of position and motion of this subject and of other potentially matching subjects identified by the re-identification may be used to guide the re-identification, possibly to exclude unfeasible subjects from the set of possible matches reducing the search space and helping the operator to find the true matches with higher efficiency.

The following text builds on knowledge of the operator's work and proposes approach how the object tracking and person re-identification may be integrated and jointly evaluated.

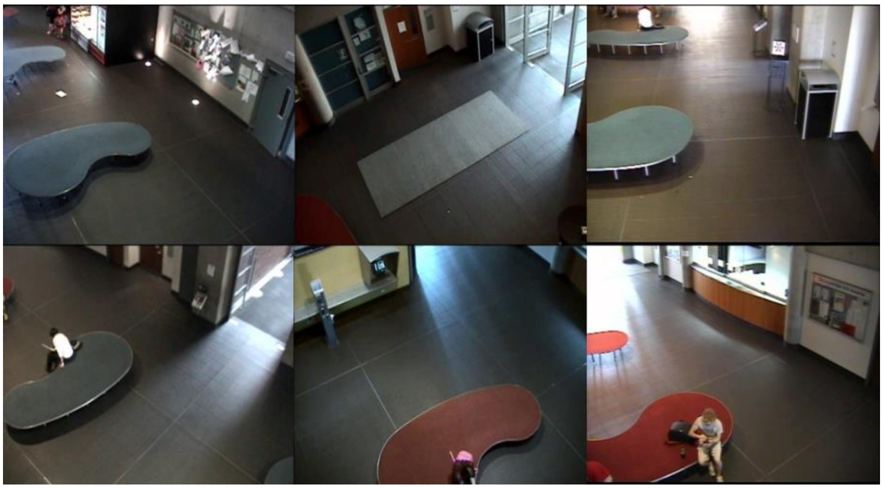


Figure 1: Bank of screens displaying video feeds from monitored area.

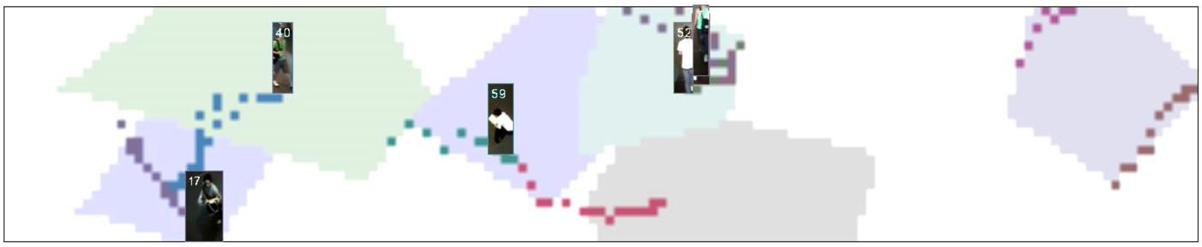


Figure 2: Plan view presentation provides instant overview; trajectories constructed with tracking and re-identification algorithms.

2 NEEDS OF THE OPERATOR OF THE SECURITY VIDEO SURVEILLANCE SYSTEMS

2.1 Situation awareness

The primary task of the operator of the security system is to maintain situational awareness across the monitored area so he can perform further analysis in case of any deviation from the normal situation. The operator's situational awareness consists of:

1. instantaneous knowledge of where each person is located.
2. instantaneous overview of the motion of each person – direction, speed, consistency, duration of stops.
3. instantaneous knowledge of mutual spatial and motion relations of the persons within the monitored space.
4. further details on a person's activity appearance etc.

The points 1-3 in the above list may be achieved with the help of video object tracking technology. Point 4 is achievable using the data from the video camera as well, but either requires operator's focus on a view of selected camera, or it requires further analysis by other intelligent software than object tracking. Still, the object tracking may be used to suggest an appropriate camera view for operator's best judgment.

The state of the art multi-camera, multi-object tracking algorithms provide, at each sampling time of the video surveillance system, the estimate of current position, speed and direction of each person within the covered area. The position estimate is provided in global coordinates. Since the 2D homography is used to map image positions to the global coordination system, 2D coordinates are provided. This is completely sufficient as the most efficient and understandable way to display the person's position in the monitored space is as a point, or an appropriately sized icon, overlaid on the map/floorplan of the monitored space. The speed and direction estimates of each person's motion may be indicated either by an appropriately positioned and sized arrow or by the "trail" – the most recent part of each person's track as provided by the object tracking tool. In this case, the speed may be indicated by the colour/shade of the person's trail and the direction of the motion by the tangent of the trail curve at the point of the current position. Figure 2, a snapshot of output of our intelligent video surveillance system, shows simplified example of the operator's display with indication of persons' positions within the monitored space, represented by their image from the most relevant camera view cropped by the bounding box of the person's detection. The most recent path of each person is indicated as the dotted "trail" understandably showing the person's speed and direction. Since the image of the person is taken from the camera providing the best view of the person, the operator, in one look at the floorplan can see all information required for his situation awareness and may quickly, with no additional effort, decide and act in the case that the situation deviates from normal.

This camera view display arrangement that uses object tracking technology to efficiently represent the situation and that allows the operator to focus and effortlessly follow each person can be called "actor centric" and significantly differs from the "camera view" centric arrangement of current surveillance systems where the operator needs to exercise significant effort to link the information from individual camera views in order to gain a coherent picture. However, because of the involvement of automated tools, there is an increased chance of introduction of errors into the information representation that the operator receives. Therefore, it is important to focus on additional requirements that enable measurement of how well the capability of the automated tools was translated to an efficient surveillance system fitting operator needs:

1. Tracking accuracy: All persons present within monitored space must be represented by a track and amount of false detections/tracks due to noise or distortions must be minimal. There must be zero or minimal amount of identity swaps – e.g. situations when a single track is constructed based on positions from two or more different persons (who e.g. might have passed near each other). Every missed person, false track or swapped identity may confuse the operator who may then misjudge the developing situation.

2. Tracking precision: The error of the person's position estimate must be minimal or within a reasonable tolerance. Too large a position error may also cause confusion to the operator and results in a loss of situation awareness.
3. Effort/time needed by the operator to fully comprehend the situation and gain high level understanding

Each error in terms of the tracking accuracy and tracking precision adds time and effort needed by the operator. If the two requirements 1 and 2 were 100% satisfied, the effort/time needed by the operator to comprehend the situation is minimal and will depend only on complexity of surveillance system (layout of the monitored space, number and placement of cameras)[1].

2.2 Forensic Search

Forensic search is performed by the security operator or analyst each time an incident occurs and it needs to be explained and analysed retrospectively. Various details then need to be viewed in the video surveillance recording, including activities of the incident actors before and after the incident. Because of the vast amount of video data (e.g. several hours or days' worth video footage from tens or hundreds of cameras) possibly featuring numerous incident actors and many irrelevant people, forensic search is usually a tedious, time consuming task. The use of re-identification tools rapidly speeds up the search by finding and ranking possible matches of candidates for re-appearance.

In the case of forensic search, the operator's needs are very simply expressed in the efficiency of the search. Therefore all that matters is how much time is needed by the operator/analyst to perform it.

3 INTEGRATION OF TRACKING AND RE-IDENTIFICATION

We have integrated tracking and re-identification algorithms into a single framework which can be used with video surveillance systems composed of cameras with overlapping and non-overlapping fields of view (Fig 3). Tracking involves a number of pre-processing steps such as image segmentation, homography mapping and object detection [1]. Once the foreground objects have been identified and their position in the global coordination system in the monitored area is known, tracks are formed by linking the detections of same object from frame to frame. In the case of overlapping views this task is significantly easier as consistency of the object's local motion can be assumed and spatio-temporal cues are then used to construct a trajectory [2]. Appearance cues are relied upon for non-overlapping views. In this case a signature is constructed for each trajectory produced by the tracking algorithm. A signature is a simple statistical model built by summing up values of occurrences of selected feature descriptors. Covariance descriptors build on the top of appearance related features such as histogram and histogram of gradients are used in our system as they exhibit best performance and invariance towards the inter-camera appearance variability. A trajectory signature is compared against a database of signatures, some of which may correspond to objects observed in other camera views, in order to detect a subject's re-appearance in a non-overlapping field of view.

The signature comparison is performed each time a new track is initialized, by the object tracking algorithm, at/near the edge of the coverage area. A pool of candidate signatures for the match consists of all signatures from the tracks previously terminated

[1] Note that we do not consider in this work aspects related to human factors, e.g. type of the GUI elements used to represent the floorplan/position/tracks. While the human factors are key elements of the security system design, they are out of the scope of this paper and we solely focus on the technology/functional aspects of the problem.

at/near the edge of coverage area. The pool is further limited to those signatures that origin from the tracks that are feasible matches with respect to spatio-temporal constraints. The spatio-temporal constraints are a set of rules such as the exclusion of a match of signatures between two displaced tracks that overlap in time etc. A candidate signature with maximum re-identification score is chosen as the match. If there are multiple signatures to be matched and the same candidate is best match for both, the maximum re-identification score rule is used again to select the match. To the operator, the matched tracks are indicated by showing the dotted line link between the matched tracks if the time interval elapsed until the reappearance of the person was not too long. Otherwise, the link between the partial tracks is kept in the database and shown only on operator's demand. The low score matches are not linked together and remain as independent appearances/disappearances of a person.

In the case of forensic search, the results of the online surveillance data processing are taken into account. The tracks, including the re-identification matches described above, are stored in a database and enable a fast search for re-appearance where short-term re-identification matches are considered i.e. those matches where there was a relatively short interval, e.g. up to tens of minutes, between the matching candidates. For longer term matches, no spatio-temporal constraints may be applied and hence the re-identification algorithm is used alone to find probable re-appearances of a subject of interest.

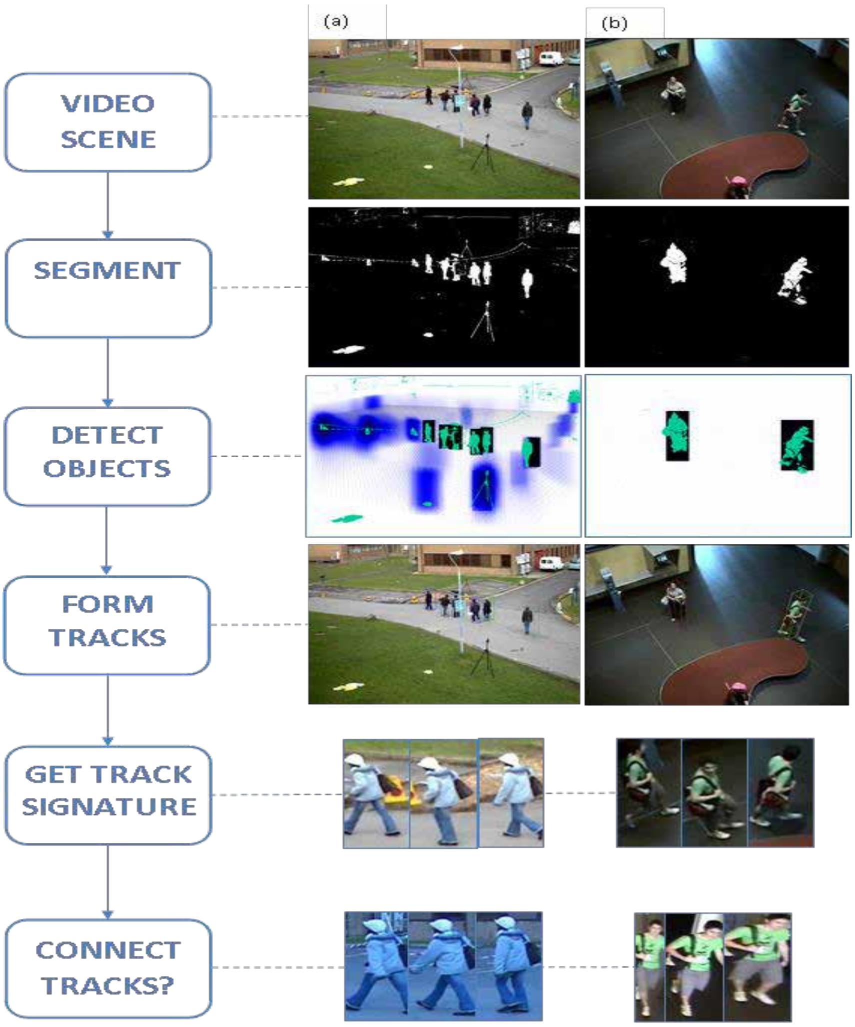


Figure 3: Framework integrating tracking and re-identification with examples from datasets (a) PETS, (b) SAIVT-SoftBio.

4 METRICS FOR THE ASSESSMENT OF INTELLIGENT VIDEO SURVEILLANCE SYSTEMS

In our work we have adopted the Multiple Object Tracking (MOT) based metrics [10] for the purpose of evaluation of the intelligent tools assisting the operator in the situation awareness scenario. MOT metrics are widely used for measuring the performance of the object tracking algorithms. According to the operator's needs stated in previous sections, the MOTA (MOT Accuracy) metrics directly relates to the tracking accuracy and MOTP (MOT Precision) describes the tracking precision. We have joined the two metrics together so that the tolerance parameter of the MOTP is fixed to a reasonable value and every occurrence of the tracking precision error then adds to the MOTA score. This in effect says that the position error larger than some predefined tolerance is going to confuse the operator (and cost him additional effort/time) compared to a lost track or a false track error.

An important difference of approach lies in the process how we define the ground truth and how we compare it to actual outcomes of the tools. Since our surveillance tool is capable of joining displaced tracks of a single person using re-identification, for our testing data we produced ground truth that connects the tracks across the coverage gaps – same person means a single track. This approach allows us to unify the tracking and re-identification evaluation: any re-identification error then actually causes identity swap and must be counted as the tracking accuracy error. This makes good sense from the perspective of the operator – since he will have to analyze the details in the case of the identity switch type of error, it will likely cost him a similar amount of confusion/effort/time disregarding whether the error occurs at the edge of the coverage area or in the middle. In summary, for the situation awareness type of task, we use modified MOT metrics which elegantly combine all the above stated operator's requirements and give a single evaluation number which enables a comparison of intelligent surveillance tools combining object tracking and person re-identification. This number expresses the ability/effort/time of the operator to establish/maintain the situation awareness.

As for the forensic search, we have adopted the averaged cumulative matching characteristic (CMC) widely used for the purposes of evaluation of re-identification algorithms [11]. It represents the expectation of finding the true match in the top N returned match candidates which is roughly inversely proportional to the time/effort that the security operator/analyst would need to perform the forensic search for a person's re-appearance in the data. Let's say, if we choose 10 as the number of signatures returned by the re-identification tool as the match candidates, the CMC value tells us how likely it is that the true match is within these 10 signatures. This corresponds to how much time, on average, the operator/analyst will need to spend searching the candidates beyond the returned candidate pool. Since the integrated tool for tracking and re-identification in the case of forensic search still returns the ranked pool of match candidates, no further changes of the metrics are needed and we have adopted the CRC characteristic as is.

5 CONCLUSION

We have presented a novel approach to the integration of object tracking and re-identification in multi-camera video surveillance systems. We have also shown how the resulting intelligent video surveillance tool may be used in the "actor centric" approach so it gives the security operator the benefit of effortless establishment and maintenance of his situation awareness. We have also proposed the unified evaluation metrics (unified in the sense that it does not make a distinction between tracking and re-identification) that reflect the needs of the two most important tasks that the security operator needs to perform. Use of these metrics will lead to effective comparison and selection of intelligent video surveillance systems in terms of the value that is being offered as opposed to the commonly used approach that only reflects partial capabilities of the systems. We have used these metrics for evaluation of our framework integrating the object tracking and re-identification, but the results were not available at the time of the submission of the paper.

In our future work, we aim to further extend how the object tracking and re-identification technologies are integrated and evaluate the framework on available data.

REFERENCES

[1] Fleuret F., Berclaz J., Lengagne R., Fua P., Multi-Camera People Tracking with a Probabilistic Occupancy Map, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 30, Nr. 2, pp. 267 - 282, February 2008.

[2] Berclaz J., Fleuret F., Türetken E., Fua P., Multiple Object Tracking using K-Shortest Paths Optimization, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011.

[3] Bak S., et al. "Retrieval system for person re-identification."*Computer Vision Theory and Applications (VISAPP), 2014 International Conference on*. Vol. 2. IEEE, 2014.

[4] Bąk S., et al. "Learning to match appearances by correlations in a covariance metric space." *Computer Vision–ECCV 2012*. Springer Berlin Heidelberg, 2012. 806-820.

[5] Bedagkar-Gala, A., and Shah S.K., "A survey of approaches and trends in person re-identification." *Image and Vision Computing* 32.4 (2014): 270-286.

[6] Li, Xi, et al. "A survey of appearance models in visual object tracking." *ACM transactions on Intelligent Systems and Technology (TIST)* 4.4 (2013): 58.

[7] Tomasi, Carlo, and Takeo Kanade. *Detection and tracking of point features*. Pittsburgh: School of Computer Science, Carnegie Mellon Univ., 1991.

[8] Zimmermann K., Matas J., Svoboda T. "Tracking by an optimal sequence of linear predictors." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 31.4 (2009): 677-692.

[9] Wang X. "Intelligent multi-camera video surveillance: A review", Pattern Recognition Letters 34 (2013) 3–19

[10] Bernardin K., Stiefelhagen R., "Evaluating Multiple Object Tracking Performance: the Clear Mot Metrics". EURASIP Journal on Image and Video Processing, 2008.

[11] Gray, D., Brennan, S., and Tao, H. (2007). Evaluating Appearance Models for Recognition, Reacquisition, and Tracking. PETS.

DETECTION OF SMALL UAVS - PROJECT OASYS²

Martin Laurenzis, Sébastien Hengy, Lionel Merlat, Rüdiger Schmitt, Vadim Allheilly, Pierre Naz, Frank Christnacher, Bernd Michael Fischer[1]

[1] *bernd.fischer@isl.eu*
French-German Research Institute of Saint-Louis (ISL)
BP 70034, 68301 SAINT-LOUIS, (France)

Abstract

In the frame of the OASyS² project, we are developing technology bricks for counter UAV systems which can be combined with various different technologies and sub-systems. ISL is investigating detection, identification and neutralization of small unmanned aerial vehicles on fundamental laboratory level as well as in field trials. Detection of UAVs is realized by a distributed acoustical sensor network with range of up to 300m. A combination of passive and active optical sensing channels is used for identification of UAVs. By a fusion of passive colour vision and active SWIR laser gated viewing, ISL has demonstrated an optical sensing close to natural human perception and an increase of the object-to-background contrast. Neutralization of UAVs is investigated in systematic laser material interaction studies of critical UAV construction elements. These studies help to limit high power laser irradiation to a scaled and well-balanced countermeasure to reduced collateral damages.

Keywords: Innovation, technology, research projects

1 INTRODUCTION

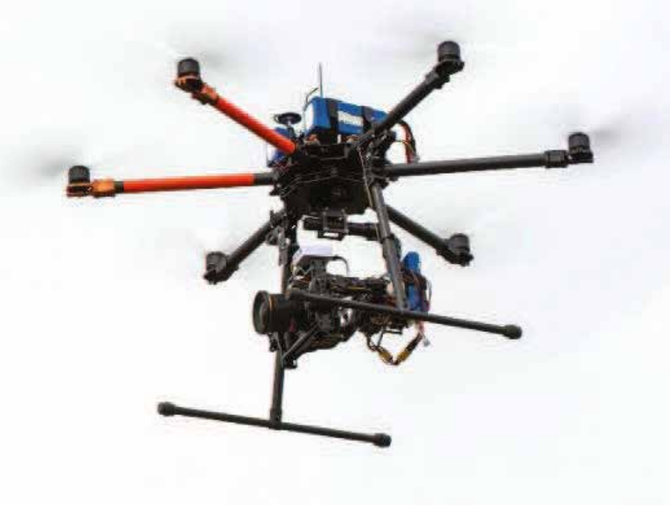


Figure 1: Unmanned Aerial Vehicle for professional application of an airborne camera system.

Small unmanned aerial vehicles (UAVs) are becoming increasingly popular and affordable the last years for professional applications as well as for the private consumer market, with varied capacities and performances. Recent events showed that illicit or hostile uses are possible and constitute an emergent, quickly evolutionary threat [1][2][3][4], which is not or very partially solved by the current anti-intrusions systems dealing with ground or air threats. Recent developments in UAV technologies tend to bring autonomous, highly agile and capable unmanned aerial vehicles to the market (Fig. 1). These UAVs can be used for spying operations (data collection for mission planning or infringing the sphere of privacy) as well as for transporting illicit or hazardous material (smuggling, flying improvised explosive devices).

At the French-German Research Institute of Saint-Louis (ISL), the IMOTEP project [5][6][7][8] has demonstrated the detection of sniper attacks and shots by gun fire acoustic signatures and the identification of shooters by active imaging. The expertise gained on this previous project is used to develop the necessary technological bricks for detection, localization, and identification of small unmanned aerial vehicles. The scenario of interest concerns the protection of sensitive zones (military or industrials) and individuals against the potential threat constituted by small drones.

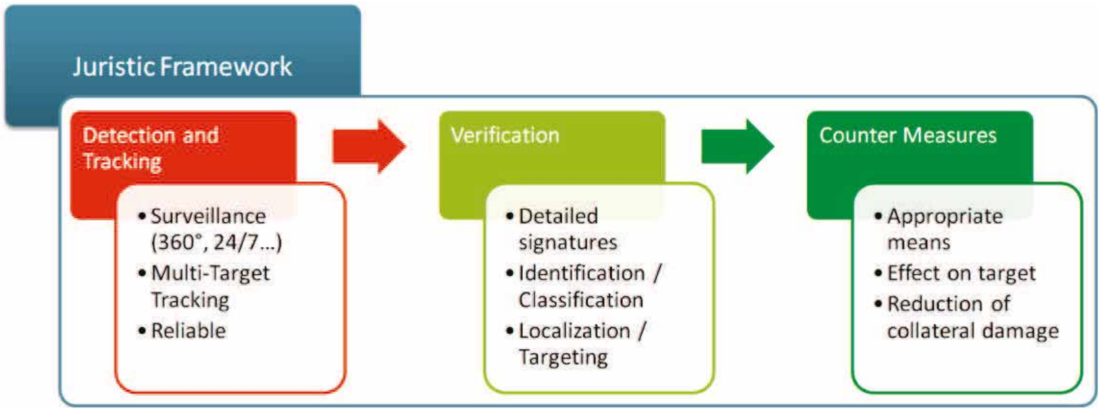
On the other hand, laser terminal effects have been extensively studies for more than 35 years. Those studies were tied with laser sources development in the mid-60s, mainly for specific metrology of fast phenomena. Nowadays, laser matter interaction can be viewed as the terminal ballistics of conventional weapons, with the unique capability of laser beams to carry energy at light velocity over large ranges. An on-going intern project aims to understand key factors of the degradation process of FRP and polymers leading to structural weaknesses.

2 THE OASYS² PROJECT

The project "Optical and Acoustic System for Security and Surveillance (OASyS²)" is an ISL internal project aiming to coordinate and to cross-connect the research activities of different ISL groups in the fields of sensor technologies, surveillance and countermeasures. The OASyS² project focuses on the detection, localization and identification of small unmanned aerial vehicles (UAVs) as well as on the investigation of countermeasures for their neutralization. The project includes a link between the detection / localization phase and countermeasures based on High Energy Lasers.

As illustrated in figure 2, the defense against UAV attacks has to follow a chain of different actions and reactions. In a first phase, small unmanned aerial vehicles have to be detected and their path has to be tracked by a reliable surveillance system. Then, the detected object has to be identified and threat has to be verified. Finally, after a precise localization, a countermeasure can be used to fight the threat.

At ISL, these three steps of action are investigated by acoustic detection and passive and active optical identification in field trials and countermeasures are studied by laser material interaction in the laboratory. Further, the OASyS² project covers the possibility to integrate alternative sensors (e.g. RADAR, thermal imaging …) and to use these information with in a sensor network.



Juristic Framework

Detection and Tracking
- Surveillance (360°, 24/7...)
- Multi-Target Tracking
- Reliable

Verification
- Detailed signatures
- Identification / Classification
- Localization / Targeting

Counter Measures
- Appropriate means
- Effect on target
- Reduction of collateral damage

Figure 2: Framework of the OASyS² project to develop technology bricks for detection verification and countermeasure.

2.1 Acoustic Detection Technology

ISL developed a compact microphone array in order to be able to detect and localize various types of UAVs. The first prototype that has been developed is constituted with four microphones in a 10 centimetres width tetrahedral shape. This allows real-time estimation of the azimuth and the elevation of the detected source using standard beam forming.

This first prototype has been deployed during a field trial organized in Todendorf, Germany. Real-time detection and localization of moving UAVs has been possible, and a rough estimation of the detection performance has been measured. Depending on the type of drone that has been used, the typical detection range varied from 100 meters for stealth UAVs (Mikado) to 300 meters for commercial drones (DJI Phantom Drone).

These first results are promising and optimised detection, localization and classification algorithms are now being developed in collaboration with the CNAM/LMSSC in parallel with a novel type of compact microphone arrays based on MEMs microphones [9].

Each individual acoustic array estimates the azimuth and the elevation of the detected event in real time (figure 3) and may transfer this information:

- to a central PC for a triangulation phase between the data provided by sensor modules which are distributed over the area.

- to the optical system which rotates in the direction of the threat and acquires images for identification,

At this stage we have one estimate of the position (direction and distance). The tracking of the threat during the flight is then possible by the acquisition and filtering of the successive positions of the detected object.

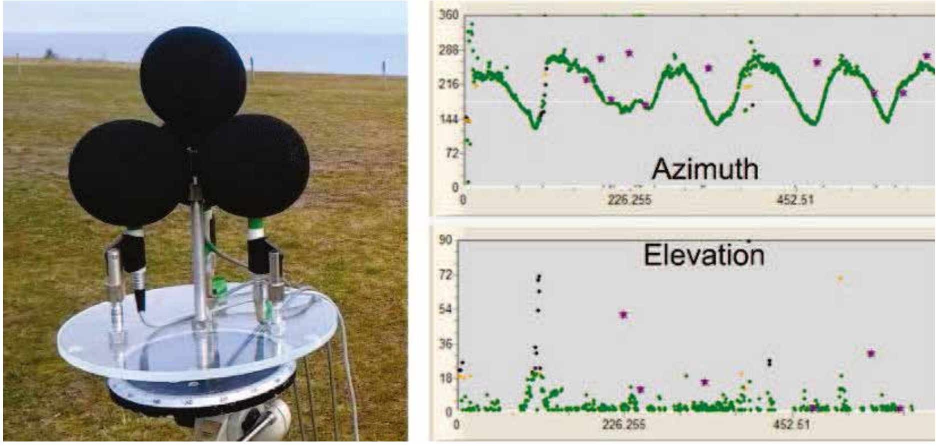


Figure 3: View of the first acoustic-array prototype deployed in the Todendorf field experiment and plots of the azimuth and elevation estimates as a function of time.

2.2 Passive and active optical identification

Optical identification of small unmanned aerial vehicles is investigated by an optical sensor system mounted on a motorized pan-&-tilt head.[10] The sensor system contains a passive and an active optical imaging channel. The passive imaging is based on a high resolution digital colour video camera equipped with commercial zoom optics. This sensor is used to record and present images to the user close to the natural human optical perception and orientation.

Further, an active sensing channel based on a shortwave infrared (SWIR) laser gated viewing system is used to record images of an active illuminated scenario. The illumination of the scene is realized by an eye-safe SWIR laser illuminator. Laser gated viewing is used to record imaged view high optical contrast even in hash environment (by gating out the background and the back-scattering), on the one hand, and to increase the optical contrast in the colour video by synthetic image fusion, on the other hand. Finally, laser gated viewing is used for ranging and precise localization of UAVs in 3D space.

In figure 4, the optical sensor system is depicted. Further, some results show the potential use of the combination of passive and active sensing channels for the identification and localization of small flying objects.

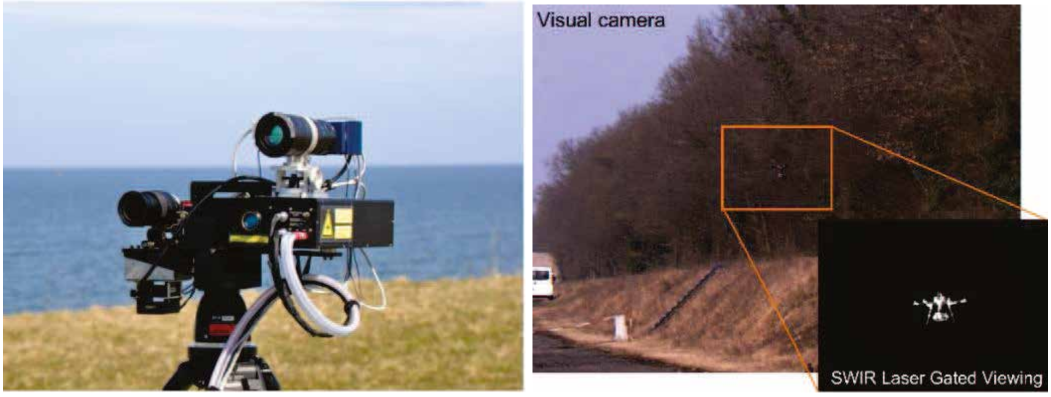


Figure 4: Optical sensor unit for the identification and localization of small unmanned aerial vehicles.

2.3 Investigation of Laser material interaction countermeasures

Laser matter interaction applications cover OCM (optical countermeasures) leading to optronic sensors dazzling, jamming or destruction, and up to hard kill of targets without any optical devices, such as landmines, IEDs, artillery shells or UAVs mainly due to strong thermal effects.

In the last years, a strong focus was made at ISL on the interaction process of laser radiation with metal targets such as artillery shells [11][12]. Due to the absorbed laser radiation an encased explosive charge can be initiated resulting in deflagration or even detonation of the projectile in flight.

As shown by experimental studies at ISL [13] the heating process can positively be impacted by material ablation and aero dynamical conditions. Other factors studied at ISL relate to rotation or imperfect overlap of different laser beams as it could be the case in realistic scenarios. Theoretical models have been developed for analytical and numerical calculations. The heating process can be simulated including ablation and the release of chemical energy in the explosive thanks to an in-house FEM code. Those simulations show the important influence of latent heat and material removal and are in good agreement with experimental results. Such a simulation outcome is shown in figure 5.

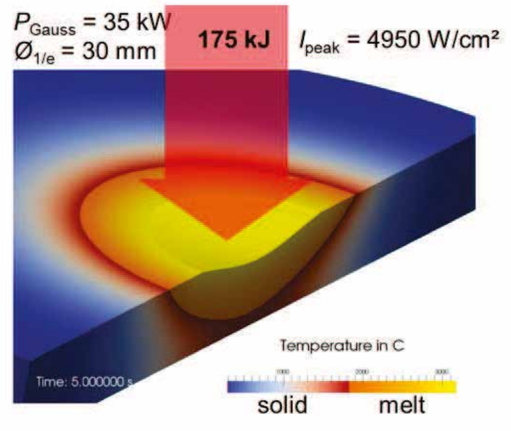


Figure 5: Simulated ablation of a low carbon steel irradiated by a 35 kW 30 mm Ø industry laser wavelength.

Drones and UAVs are of outmost interests in modern warfare. Understanding their laser vulnerabilities allows on the one hand to drive the future laser weapon technical requirements, and on the over hand to drive the development of new protective materials. Those aerial systems are usually made up of epoxy-based composite materials.

Such materials have strongly dissimilar optical, thermal and mechanical properties. The epoxy matrix is semi-transparent in the near infrared and burns at low temperature (i.e. ~270 °C) whereas carbon fibres are opaque and sustain more than 3000 °C. In addition, resin's additives properties are more sensitive to temperature. For example, an ebullition can be induced inside the composite material during the thermal front propagation, leading to an overpressure and speeding up the delamination process.

It has been demonstrated that despise the resistance of the carbon fibre to a direct laser illumination, the carbon composite Young modulus decreases linearly with the laser fluence. The thermal front still progresses inside the composite seconds after the end of the laser illumination and can thus induce mechanical failures while the shot is over. Such phenomena have been characterized by illumination of composite targets under mechanical stress with complete thermal observations.

Structural damages of lightweight drones by high energy laser result from the absorption of the beam energy by the structure material [14], mainly polymer-based. A wide spectrum of terminal effects can be addressed, ranging from pure mechanical weakness, to material removal, with the objective that the drone loses its flight capability. All those effects are investigated in laboratory conditions with the objective to build up a laser vulnerability model, taking into account:

- Laser-matter interaction: the trigger point of the laminate weakening phenomena is the coupling of the laser beam with itself. It is also from prior manner to define the energy absorption of light within the material. Because of the more complex optical behaviour of GFRP, the work focused on that type of laminate.
- Thermo-dynamical behaviour: once energy has been absorbed by the laminate, the thermodynamic law governs the heat propagation within the sample.
- Mechanical characterization: the ultimate goal is the determination of the mechanical response of the sample.

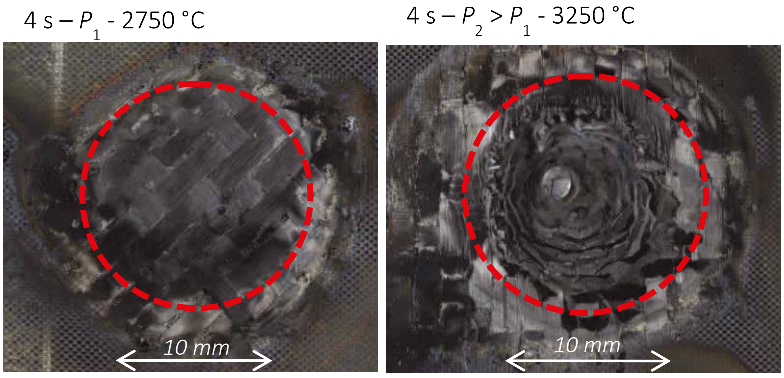


Figure 6: Final effect of a 10 cm Ø 4 s laser impact with 2 different powers on a CFRP. (Left) the matrix has been pyrolysed but the carbon fibers remains. (Right) the final temperature is high enough to lead to a carbon melting, leading to a bulk crater.

Because the material reaches very high temperatures when subjected to a HEL irradiation, the degradation kinetic of each phase according to the temperature and its consequences on the above-mentioned topics must be characterized too. The dynamical behavior of the material according to the temperature concerns each of the above aspects and is one of the key point of the study, whereas it can be very complex to achieve. Figure 6 shows the effect on a Carbon-Fiber Reinforced Plastic (CFRP).

3 CONCLUSION

In the frame of the OASyS² project, ISL is developing technology bricks for counter UAV systems which can be combined with various different technologies and sub-systems. ISL is investigating detection, identification and neutralization of small unmanned aerial vehicles on fundamental laboratory level as well as in field trials.

Detection of UAVs and surveillance of an area can be realized by a distributed acoustical sensor network. ISL has demonstrated detection of various UAVs in field trials up to a range of 300m.

Identification of UAVs can be realized by a combination of passive and active optical sensing channels. ISL has demonstrated that an optical sensing close to natural human perception and an increase of the object-to-background optical contrast can be reached by a fusion of passive colour vision and active SWIR laser gated viewing.

Neutralization of UAVs is investigated in systematic laser material interaction studies of critical UAV construction elements. These studies help to limit high power laser irradiation to a scaled and well-balanced countermeasure to reduced collateral damages.

REFERENCES

[1] Gallagher, S. "German chancellor’s drone “attack” shows the threat of weaponized UAVs." ARS Technica (2013).

[2] Sathyamoorthy, D., "A Review of Security Threats of Unmanned Aerial Vechicles and Mitigation Steps.”

[3] Wallace, R. J., Loffi, J. M. "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis." International Journal of Aviation, Aeronautics, and Aerospace 2.4 (2015): 1.

[4] Luxhoj, J. T. "System Safety Modeling of Alternative Geofencing Configurations for small UAS." International Journal of Aviation, Aeronautics, and Aerospace 3.1 (2016): 2.

[5] 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.

[6] 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.

[7] Hengy S., Laurenzis M., Fischer B.M., Naz P., Zimpfer V., Improvement of optical and acoustical technologies for the protection of camps or mobile troops: Poject IMOTEP, 10th Security Research Conference: Future Security, Berlin, DE, September 15-17, 2015

[8] Hengy, S., Laurenzis, M., Schneider, A., Acoustical sensors and a range-gated imaging system in a self-routing network for advanced threat analysis, GI-Edition Lecture Notes in Informatics (2011)

[9] Ramamonjy, A., Bavu, E., Garcia A., Hengy, S., Détection, classification et suivi de trajectoire de sources acoustiques par captation pression-vitesse sur capteurs MEMS numériques, CFA/VISHNO, Avril 2016.

[10] Laurenzis, M., Christnacher, F., 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), 397-405 (2014)

[11] R. Schmitt, “Analysis of Laser Effects in CRAM”, Directed Energy Systems 2015, London, Feb. 11-12, 2015

[12] R. Schmitt, “Use of Laser Weapons for Counter in Air Defense – Scientific Insights for a Better Understanding and Optimization”, Directed Energy Systems 2016, London, Feb. 24.-25, 2016

[13] V. Allheilly, F. Lacroix, AL. Eichhorn, L. Merlat, G. L’Hostis, B. Durand, An experimental method to assess the thermo-mechanical damage of CFRP subjected to a highly energetic 1.07 mm-wavelength laser irradiation, Composites Part B 92 (2016) 326-331

[14] V. Allheily, L. Merlat, F. Lacroix, A. Eichhorn, G. L’Hostis, The behavior of translucent composite laminates under highly energetic laser irradiations, to be presented at LANE 2016, Fürth, Germany, 19-22/09.

ON MULTIPLE SENSOR UAS SECURITY

RESEARCH ASPECTS AND FIRST EXPERIMENTAL RESULTS

Wolfgang Koch

wolfgang.koch@fkie.fraunhofer.de
Fraunhofer FKIE, Dept Sensor Data and Information Fusion
Fraunhoferstrße 20, D-53343 Wachtberg (Germany)

Abstract

Unmanned Aerial Systems UAS, also called *drones*, revolutionize the market for mobility based services and enable more efficient defence and police operations. A new generation of SME founders opens up innovative products and business models with barely foreseeable consequences for the everyday life of people. Also this rapidly developing technology, however, proves to be Janus-faced. Despite their unquestionable benefits, UAS increasingly pose serious safety and security threats. In this paper, we wish to identity relevant research questions to be answered before any effective drone threat recognition and countering system can be developed. First experimental results illustrate the key role of multiple sensor data fusion algorithms for detecting, tracking and classifying UAS.

Keywords: unmanned aerial system UAS, UAS detection / tracking / classification, multiple sensor data fusion, heterogeneous sensors, electronic counter measures.

1 SAFETY AND SECURITY ISSUES OF DRONES

Protection against any undesired use of drones is not only demanded in the interest of public safety and security, but is also an increasingly important requirement for protecting military and police forces in their challenging missions, which in turn leads to innovative product ideas. Evidently, systems for protecting against threats and risks related to drones play a crucial role for enabling socially accepted, legally regulated and commercially viable drone applications and to develop the huge market potential for new mobility services made technologically possible by drones [1].

The photo showing a popular toy drone hovering before the amused Chancellor Angela Merkel and her frightened minister of interior affairs, also responsible for Merkel's security, was distributed around the world. Its payload could easily have been an explosive device. Security specialists have for a long time been concerned about "Airborne Improvised Explosive Devices" that can be easily deployed by "everyday drones". A simple Google search reveals the global dimension of this new threat: "Drone Causes Power Cut in San Francisco", "Flight delayed at Heathrow When Drone Flies Over One of its Runways", "Drone Used to Smuggle Drugs into Prison", "A Drone Rattles the White House". Drones have also been used spying on industrial plants, product prototypes under development and critical infrastructures, such as nuclear power plants. Another abuse has been for covert recording of sensitive conversations by flying directional microphone drones.

Protection against drones, however, must not hinder their intended use. In the public domain, the safety and security issues should be harmonized with the social and economic opportunities presented by this new dimension of mobility. In dealing with the risks related to automobile mobility, a triple strategy is likely to be successfully utilized here: Any mobility related safety and security concept is expected to be based on a legal framework, on appropriate insurance products and on safety and security technologies, which need to be investigated and developed by research institutions and industry.

Fig. 1 shows a schematic view of a modular and scalable sensor data fusion architecture with standardized interfaces for drone reconnaissance. It is the very basis of any technical counter UAS system. The multiple sensor data fusion algorithms needed for this new application are available and need only to be appropriately adapted. See [2], for example, as a reference.

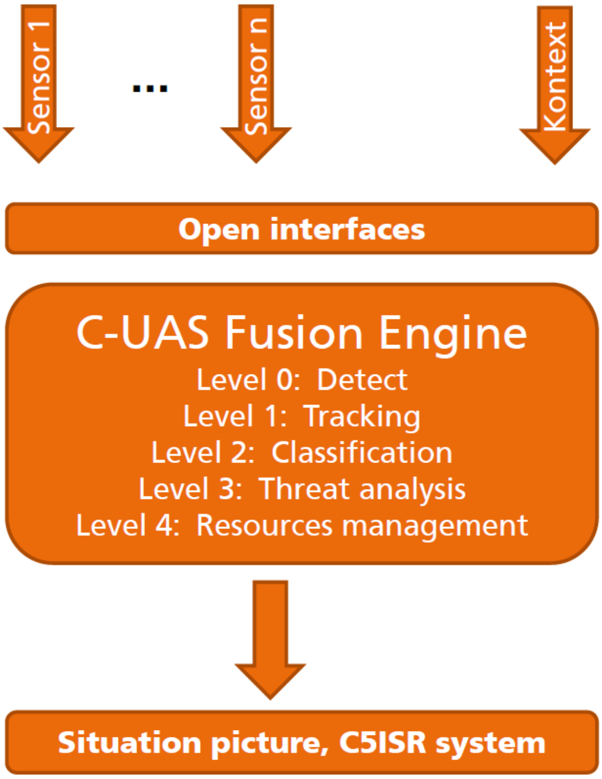


Fig. 1: Schematic view of a modular and scalable fusion architecture for Counter UAS with standardized interfaces.

For this reason, an electronic labeling requirement similar to car license plate is foreseeable for drones as well, which is based on transponder technologies used in air traffic control. Under discussion are “drone pilot’s licenses” and “electronic ignition keys". By automated drone identification systems, registered drone traffic can be observed and identified, as such, at any time. This would also indicate whether there is any non-cooperative and potentially threatening use of drones. In addition, geo-fencing is a viable option in establishing "no-fly zones" using geographic information systems. Since financial risks related to drone-based mobility services may easily exceed the resources of private individuals or companies, a new line of drone-related insurance products is likely to be developed. See reference [3] for a comparable discussion of socially, legally and ethically relevant issues in security assistance systems.

Which technology is to be chosen? What is to be protected against drone threats and by whom? Under consideration are especially low-signature Unmanned Aerial Systems, which are popular and their distribution is difficult to control. Because they can operate in a highly agile manner and achieve high speeds, the response times for any countermeasures are short.

2 MULTIPLE SENSOR DRONE THREAT ASSESSMENT

In order to detect drone threats quickly and reliably, we first need high performance sensors capable of detecting complementary characteristics of approaching drones. By utilizing efficient algorithms of multiple sensor data fusion, a suit of heterogeneous sensors can be integrated into a drone detection system. Fig. 2 illustrates the experimental setup of a measurement campaign for counter UAS at Fraunhofer FKIE in September 2015, where E/O, IR, acoustic and passive radar sensors have been used, their data fused and the results evaluated. Further research and experimentation is in progress with industrial partners. Fig. 3 shows two readily available drones from different weight classes and with different sensor signatures.

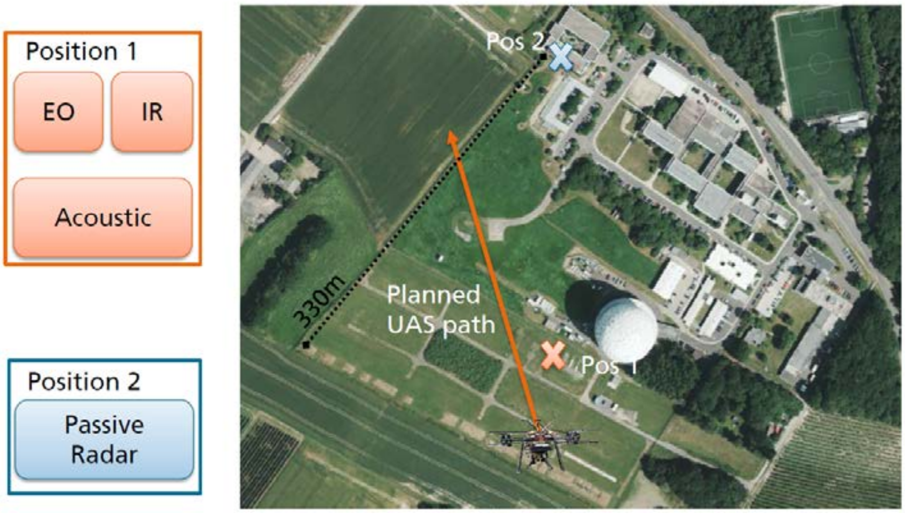


Fig. 2: Experimental Setup of a measurement and data fusion campaign counter UAS at Fraunhofer FKIE (September 2015) exploiting E/O, IR, acoustic and passive radar.

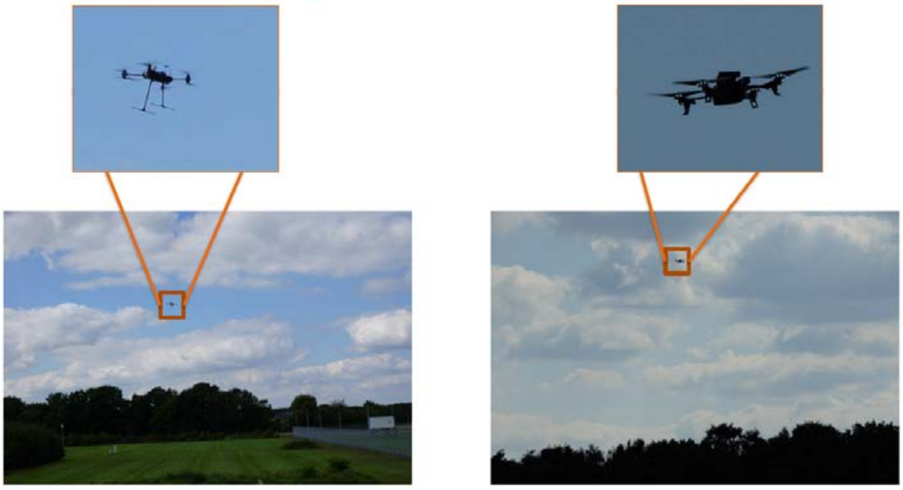


Fig. 3: UAS used for multiple sensor experimentation – weight > 8 kg and < 0.4 kg

Because of its range and all-weather capability, radar optimized for drone detection is the backbone sensor. Radar systems send signals either themselves or use existing "electro smog" as a source of illumination. Echoes reflected from drones are analyzed to estimate position and velocity, as well as to provide clues for classification. Passive radar uses radiation from mobile phone base stations for illumination, e.g. Since transmission permits for active radar operation are rarely granted, passive radar enables surveillance wherever mobile phones are working, and illuminate the airspace predominantly used by drones without any emission load. Fig. 4 shows an experimental passive radar system developed by Fraunhofer FKIE which exploits electromagnetic illumination provided by the broadcast signals of GSM mobile phone base stations. In the experiment, six illuminating GSM base stations have been used.

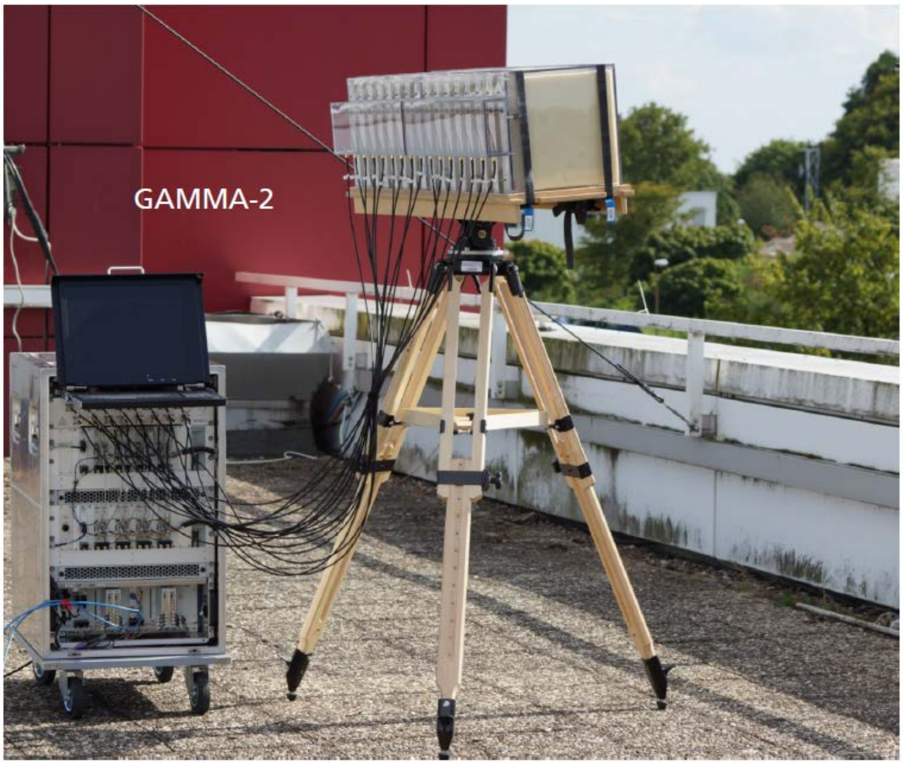


Fig. 4: Experimental passive radar exploiting six illuminating GSM base stations. In the measurement campaign, GPS-loggers provided the ground truth.

Overall design principles of GSM passive radar and experimental results related to security applications are discussed in reference [4]. For a comprehensive introduction into multistatic tracking see reference [5]. Fig. 5 shows a range-Doppler diagram where the expected Doppler frequency of the reflections caused by a drone according to ground truth is indicated over time. The comparison clearly indicates the suitability of GSM passive radar for drone detection applications in general.

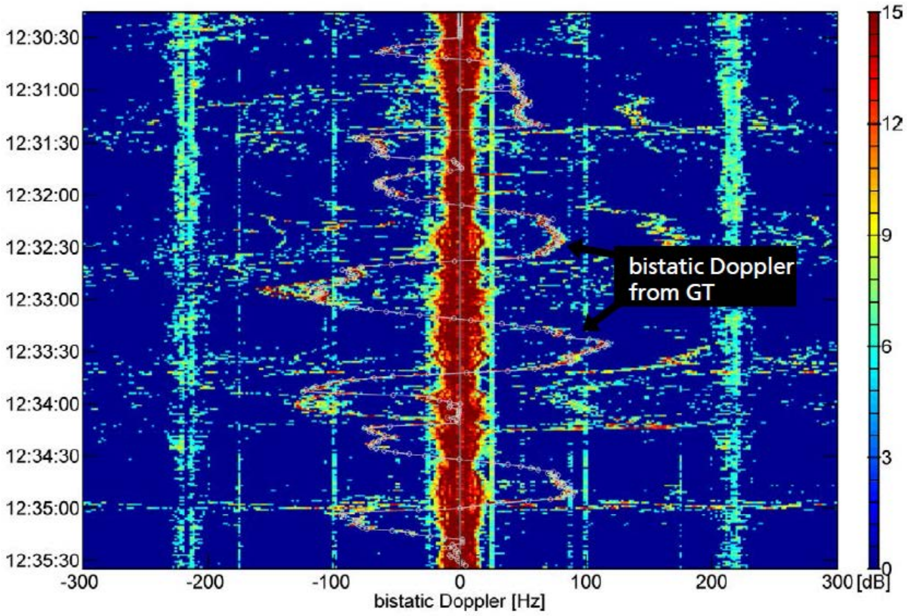


Fig. 5: Range-Doppler diagram with expected Doppler frequency according to ground truth over time. This provides a first confirmation of successful UAV detection.

In figures Fig. 6 and 7, preliminary results on solving illuminator-to-drone association problems are illustrated. These results are basic for ongoing work on developing and evaluating appropriate track-before-detect and drone tracking algorithms. Fig. 6 shows the number of correctly associated signal processing results to the ground truth whenever the estimation error of kinematic parameters (bistatic range, bistatic Doppler, azimuth) are below a certain threshold. The number of correct associations over the actual flight path of the UAS is illustrated in Fig. 7.

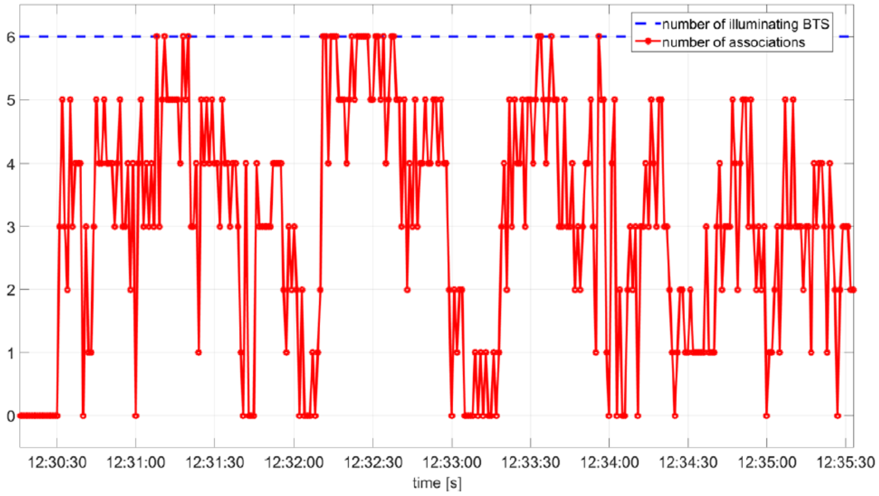


Fig. 6: Association of signal processing results to the ground truth wherever the estimation error of kinematic parameters are below a certain threshold.

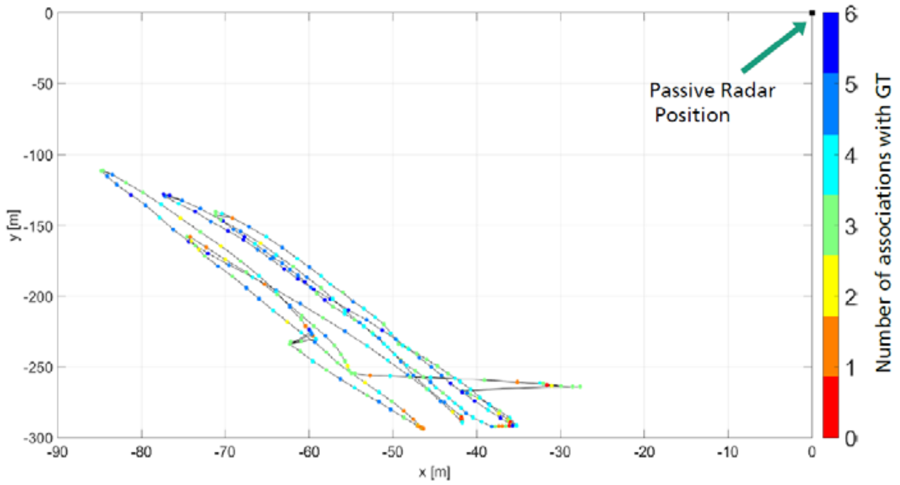


Fig. 7: The number of associations over the flight path illustrates the suitability of GSM passive radar for detecting and tracking UAS.

Radar data are to be fused with data streams provided by imaging sensors, typically covering several spectral regions [6]. Although they usually achieve lower ranges than radar sensors and are relying on weather conditions and the time of day, their resolution capabilities may well facilitate the target classification task and further reduce false alarm rates by using multiple sensor data fusion. Track-before-detect algorithms based on inhomogeneous Poisson point processes have been proven to provide a powerful methodology [7, 8]. Fig. 8 illustrates the chosen sensor data fusion approach.

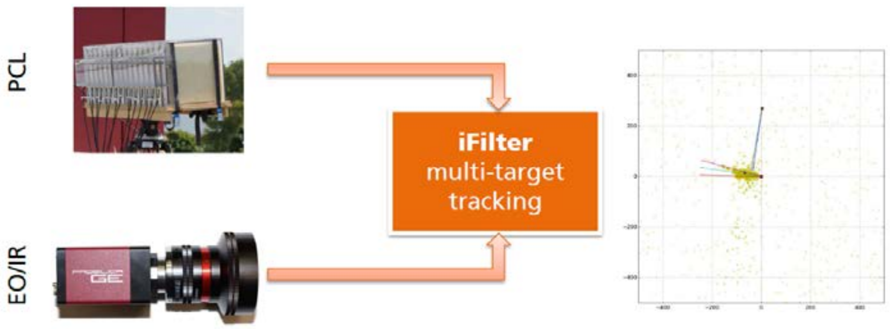


Fig. 8: Fusing GSM passive radar results with E/O-IR using intensity filtering.

Furthermore, emissions produced by the drones themselves enable drone detection, for example, emissions due to remote control. For details see reference [9]. Using appropriate data exploitations algorithms, a drone and its pilot can be localized. Also autonomously operating drones build up intermittent data links. Encouraging results have been obtained from acoustic emissions, which are detected by microphone networks. Therefore, array signal processing techniques are important [10].

The relevance of multiple sensor data fusion is thus evident. For sensor and resources management, however, game theoretical methods are required that enable robust system solutions.

3 REMARKS ON COUNTERMEASURES

Although their threat potential is high, “everyday drones" have the advantage of offering little electronic self-protection measures due to payload limitations. "Soft kill" measures may, therefore, limit their functionality. "Hard kill" measures, for example projectiles, laser, or high energy electromagnetic pulses, are excluded here because one wishes to avoid crashes with incalculable consequences in view of the chemical, biological, radioactive and explosive payloads that are possibly to be taken into account. The assessment and minimization of collateral damage must therefore accompany any discussion of done countermeasures.

To a certain extent, known methods of electronic warfare can be used to “hijack” the remote control of a drone. This is actually rather simple in the case of WLAN-based approaches. For more demanding, but increasingly common communication links the challenges are much larger. If a drone operates autonomously, the jamming or deception of satellite navigation can be appropriate (navigation warfare). The extent to which this is possible in a civil environment and the assurance that only potentially threatening drones are affected raise many research questions.

Whenever a drone is used for spying purposes, the data downlink or the sensors used can be disrupted by electromagnetic countermeasures. In a spying operation, where the sensor data is collected on board the drone and is not transmitted, the drone operator would be forced to bring the drone back into his possession. As a countermeasure, the drone would be tracked to lead directly to the perpetrators.

Whenever kamikaze drones are to be expected, intercept drones are an option that try to neutralize the undesirable drone by a network and transport it to a safe destination. It does not seem necessary to emphasize the great challenges in platform, sensor and control technologies that are implied by this approach.

Also, the problem of counter drone defense has to be considered: What can be done to ensure the use of drones in presence of counter drone technologies used by potential adversaries?

4 CONCLUSIONS

Advanced algorithms of multiple sensor data fusion and management of sensors play a key role in designing counter drone systems. In the context of C5ISR systems (Command, Control, Communications, Computer, Cyber, Intelligence, Surveillance and Reconnaissance), the technological challenges can be met, but require close cooperation between the military and police forces, research institutes and the relevant industries. In the protection of stationary equipment and mobile units in urban or open terrain, the integration of drone detection / tracking / classification in decision support systems is crucial.

REFERENCES

[1] W. Koch. *Multisensorielle UAS-Abwehr - Forschungsaspekte einer technologischen Herausforderung*. DWT Symposium „Angewandte Forschung für Verteidigung und Sicherheit in Deutschland“, Februar 2016, Bonn.

[2] W. Koch. *Tracking and Sensor Data Fusion – Methodological Framework and Selected Applications*. Springer Mathematical Engineering Series. 2014.

[3] W. Koch. *The Role of Context in Multiple Sensor Systems for Civil Security*. Chapter 5 in: L. Snidaro, J. Garcia, J. Llinas, E. Blasch (Eds.). *Context Enhanced Information Fusion – Improving Real World Performance with Domain Knowledge*. Springer Series on Advances in Computer Vision and Pattern Recognition (2016).

[4] M. Broetje, B. Knoedler, W. Koch. *Evaluation of GSM Passive Radar Data and Its Use in Multistatic Tracking*. 19th International Conference on Information Fusion (FUSION), Heidelberg, Germany, 2016.

[5] M. Daun, U. Nickel, W. Koch. *Tracking in multistatic passive radar systems using DAB/DVB-T illumination*. In: EURASIP Signal Processing, Vol. 92, Nr. 6, pp. 1365–1386 (2012).

[6] W. Koch. *Situationsanalyse durch multispektrale Sensordatenfusion – Architekturen und Experimente*. DWT Symposium „Angewandte Forschung für Verteidigung und Sicherheit in Deutschland“, Februar 2016, Bonn.

[7] M. Schikora, W. Koch, R.L. Streit, D. Cremers. *Sequential Monte Carlo method for the iFilter*. 14th International Conference on Information Fusion (FUSION), 2011.

[8] M. Schikora, D. Bender, W. Koch. *Airborne emitter tracking by fusing heterogeneous bearing data*. In: 17th International Conference on Information Fusion (FUSION), 2014.

[9] D. Musicki, R. Kaune, W. Koch. *Mobile emitter geolocation and tracking using TDOA and FDOA measurements*. In: IEEE Transactions on Signal Processing, vol. 58, nr. 3, pp. 1863-1874 (2010).

[10] M. Häge, W. Koch. *Threat Recognition with Various Distributed Sensors*. In: NATO IST-SET-126 Symposium on “Information Fusion (Hard and Soft) for ISR”, May 2015.

HIGH ENERGY LASER WEAPON DEMONSTRATORS FOR C-UAS APPLICATIONS

K. Ludewigt, Th. Baumgärtel, Th. Riesbeck, J. Schmitz, A. Graf and M. Jung

markus.jung@rheinmetall.com
Rheinmetall Waffe Munition GmbH
Heinrich-Erhardt-Str. 2, 29245 Unterlüß (Germany)

Abstract

Rheinmetall Waffe Munition has been working over 30 years in the area of High Energy Laser (HEL) for defence applications. In the last decade, Rheinmetall Waffe Munition switched to diode pumped solid state laser (DPSSL) and has successfully developed, realised and tested a variety of HEL weapon demonstrators for air- and ground-defence scenarios like countering rocket, artillery, mortar, missile (C-RAMM), countering unmanned aerial systems (C-UAS), unexploded ordnance (UXO) clearing based on this technology. By employing beam superimposition technology and a modular laser weapon concept, the total optical power has been successively increased. This contribution gives an overview over the stationary and mobile HEL weapon Demonstrators recently developed by Rheinmetall Waffe Munition. We will give an overview of the capabilities of these demonstrators against different potential targets and as a highlight, we will show the capability of the 30 kW stationary Laser Weapon Demonstrator integrated into an existing GBAD (ground based air defence system) to defeat saturated attacks of RAMM and UAS targets.

Keywords: High energy laser weapon, demonstrator, scenario, C-RAMM, C-UAS.

1 INTRODUCTION

In recent years the threat caused by UAS on our public security increased dramatically. this threat got visible at several incidents around the world from overflying nuclear power plants, crashing into the lawn of the White House [1], colliding with aircrafts landing at Heathrow [2], flying around the Eiffel Tower [3], or landing in front of the German chancellor Mrs. Merkel during an election campaign in Germany [4]. As semi-autonomous and easily operable UAS became available on a mass market with steadily growing quantities ("toy" drones), there is no question that the number of such incidents will increase. It is only a matter of time until UAS are used for terrorist attacks.

High Energy Laser (HEL) effectors are highly suitable to handle this threat. They have many advantages compared to conventional weapon systems and other kind of effectors. They can operate with a high precision, without practical time lag (speed of light) at large distances and are capable of downscaled escalation.

Fibre lasers, as a special type of diode pumped solid state lasers (DPSSL), have recently experienced huge advancements regarding output power, beam quality and electrical-to-optical efficiency. Thus, they have become suitable for security applications and are already used as laser sources in Laser Weapon Demonstrator programs by different nations [5], [6].

High power fibre lasers are available as COTS (commercial-off-the-shelf) products. Their main advantageous properties are short start-up time, deep magazine and they possess exceptionally low costs per engagement. In 2012, we demonstrated the integration of our fibre laser weapon system into different stationary air-defence platforms [6]. The modular concept of beam superimposing of several identical Laser Weapon Modules (LWMs), each consisting of a 10 kW fibre laser connected to a Beam Forming Unit (BFU), proved to be reliable and effective against generic mortar targets, unmanned aerial systems (UASs) and stationary structures. The complete engagement process from detecting, coarse tracking, fine tracking and interaction was demonstrated for realistic scenarios.

As a next stage, we will prove the scalability and flexibility of our laser weapon concept by integrating them into different platforms, either stationary or mobile. Mobile platforms show limitations according to size, weight and power (SWaP). The integration of specialised LWMs into different vehicles and into a GBAD weapon station will be shown. Typical C-UAS scenarios like dazzling UAS cameras, destroying single and multiple UAS equipped with explosive payloads will be shown.

2 HEL EFFECTORS

2.1 Basic Laser Weapon Module

The general setup of the employed HEL effectors is based on our successful experiments with generic multi-10-kW laser weapon demonstrators in 2011 [7] and 2012 [6]. By using beam superimposing technique and our modular LWM concept based on COTS high power fibre lasers it is possible to provide an adaptable and scalable solution to equip laser weapons to various platforms. A conceptual overview of the general HEL effector setup is shown in Fig. 1.

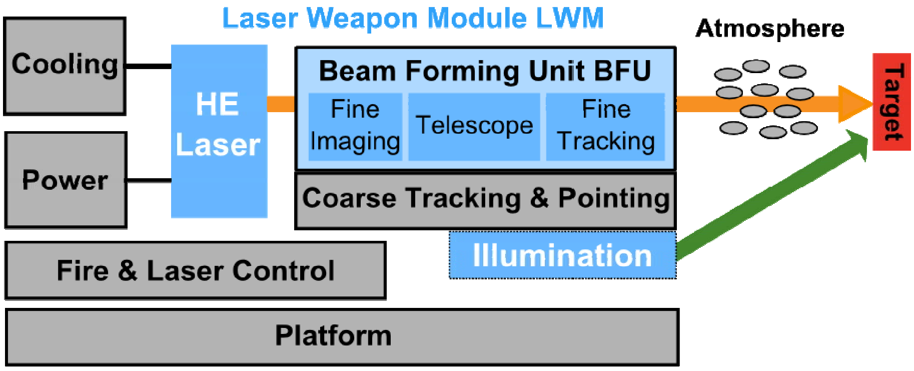


Fig. 1: General HEL effector setup with basic components.

The primary item of each HEL effector is at least one laser weapon module. Each module consists of a high energy (HE) fibre laser and a beam forming unit. The BFU is used to image the target with a high magnification, to track vulnerable points with a high precision and to focus the laser beam on such a point. The BFU can be divided into three parts: fine imaging, fine tracking and telescope. In order to increase the precision and the speed of the fine tracking system, the target may be illuminated by a narrow-band light source (e. g. a laser). The optical components of the BFU are designed and constructed to ensure a diffraction limited beam. Depending on the type and the later operation of the platform, peripheral components such as cooling and power supply for the HEL, coarse tracking and pointing as well as fire and laser control can either be integrated in the platform or provided externally. The available total laser power can be altered by using different types (5 kW, 10 kW, 20 kW) or different numbers of LWMs. Within the last years Rheinmetall developed stationary and mobile demonstrators for land and sea applications with power level from 5 kW up to 50 kW.

2.2 Mobile Demonstrators

From 2011 on Rheinmetall has extended the experience of the stationary HEL Demonstrators by mobile HEL demonstrators and integrated Laser Weapon Modules into mobile platforms like the TM-170, M113 (Mobile Effector Track), IFV (Infantry Fighting Vehicle) Boxer up to containerized solution for military trucks (see Fig. 2).

For down-scalable UXO (Unexploded Ordnance) and obstruction clearing scenarios with a limited range, a 1 kW fibre laser is fully integrated into the TM-170 and M113 [8]. The LWM on the M1113 uses a single BFU which is mounted on an armour-cased remote weapon station supplied by RUAG, Switzerland. The aperture of the BFU optics is minimized in order to reduce the influence of shockwaves from exploding objects. The cooling and power supply are integrated into the M113 platform which allows for an autarkic operation. The “Mobile Effector Track V” marks the first HEL effector integrated and tested on a tracked platform.

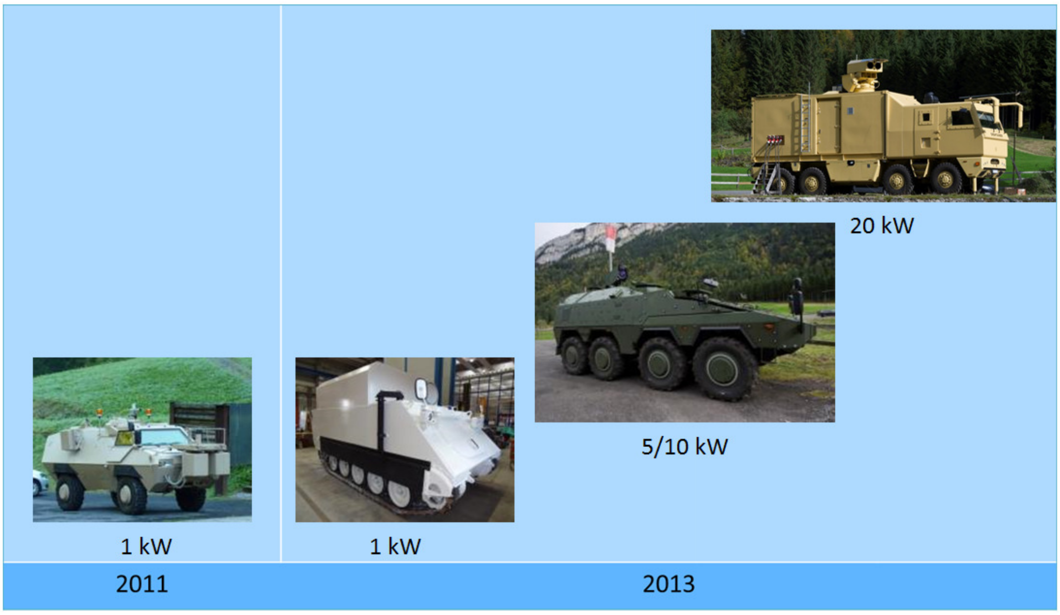


Fig. 2: Mobile HEL demonstrators.

In the 20 kW class, the “Mobile Effector Wheel XX” is designed for maximum mobility and based on an 8x8 IFV Boxer multirole armoured vehicle. A 5 kW fibre laser as well as power supply, energy storage and cooling system are integrated into a modified ambulance module. The LWM consists of a single BFU mounted on an agile remote weapon station. This can be operated manually or automatically with a coarse tracker. In contrast to the “Mobile Effector Track V”, the BFU has a larger aperture in order to ensure higher engagement distances. The BFU is equipped with a fine tracking system that allows platform vibration compensation. Thus, a stable pointing of the HEL beam can be ensured at large distances even with the motor of the drive module running. The operator stations for the HEL as well as both trackers are also incorporated in the module.

The 50-kW-class-system “Mobile Effector Container L” featured two LWMs, each with an optical power of 10 kW. The HEL effector is integrated in a ballistically protected standard 20 feet ISO container. The two 10 kW high energy lasers as well as the cooling unit are located inside of the container, while the BFUs are installed on a remote weapon station on top. Both BFUs feature an independent fine tracking system including an illumination laser. The operator station for the HEL as well as fine and coarse tracking is also embedded in the container which was carried by a protected Tatra T-815/7 8x8 truck supplied by DREHTAINER, Germany. The power supply for the HEL effector is provided externally. The container is an ideal component for a very flexible and modular system concept. One or more HEL effector containers can be transported and deployed easily in different configurations.

2.3 Stationary Demonstrator

The basic design of the stationary effector is identical to the 30 kW laser weapon station introduced by Rheinmetall in 2012 [6]. Three 10 kW LWMs are integrated in a modified MG 10 Skyshield Gun Turret by removing the gun and adapting the BFUs to the gun cradle. The high energy lasers are placed in a ten feet sea container below. The stationary 30 kW laser weapon station is shown in Figure 3. Both energy supply and cooling unit are provided externally. To demonstrate the full integration capability of the laser weapon station into an established ground based air-defence (GBAD) system, the coarse tracking of the MG-10 turret is guided by a Skyguard sensor platform using radar and electro-optic sensors. The sensor platform is modified by the installation of an illumination laser in order to increase the range and speed of the fine tracking system. The stationary effector is able to engage fast moving and agile aerial targets. A separate command and control centre is used to accommodate the operators for HEL firing, coarse and fine tracking which are integrated in the security loop of the GBAD system.

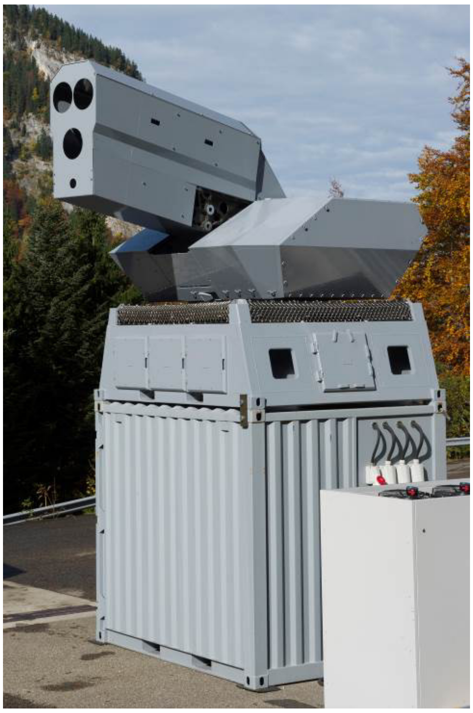


Fig. 3: Stationary demonstrator with 30 kW optical output power.

3 C-UAS TEST RESULTS

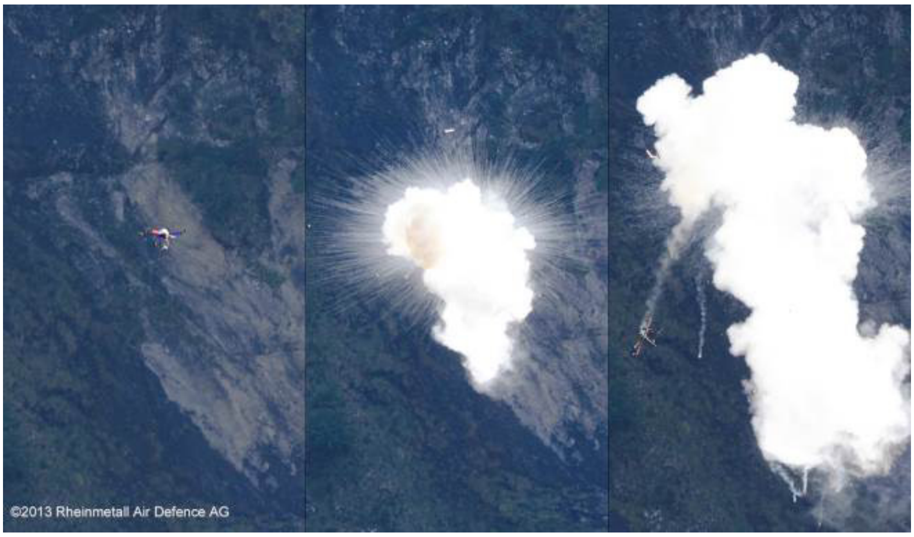
Most of the HEL effectors were operated on the Rheinmetall owned proving ground in Switzerland under conditions that are as realistic as possible. The following sections will briefly describe two countering UAS scenarios and their results.

3.1 Rogue rotary winged vertical take-off UAS with an explosive payload

The test scenarios for the Mobile Effector Wheel XX are focused on dynamic targets. The HEL effector is able to rapidly deflagrate a single round in the ammunition belt of a heavy machine gun which is mounted to a car passing by at distances above 100 m.

This requires a very precise and stable pointing of the HEL beam which is possible due to a well-tuned fine and coarse tracking system.

Another dynamic scenario that proved the stability and accuracy of the tracking systems is the successful engagement of an approaching vertical take-off unmanned aerial system (VTUAS). The VTUAS may be GPS-guided and carries a generic low explosive payload on a predetermined path. Using the 5 kW high energy laser of the Mobile Effector Wheel XX, the aerial thread could be neutralized by ignition of the payload, which resulted in the destruction of the VTUAS (series of three frames in the right part of Figure 4). If the VTUAS does not carry an explosive payload, a hardkill of the vehicle can be easily achieved by destruction the frame, motors or control electronics. Another downscaled option, e.g. for reconnaissance VTUAS, is to induce a mission kill by permanently or temporarily dazzling the optical sensors.



©2013 Rheinmetall Air Defence AG

Fig. 4: Engaging a UAS with by the Mobile Effector Wheel XX. Frame series show the destruction of a VTUAS with an explosive payload.

3.2 Swarm attack by fixed-wing UAS with an explosive payload

A UAS swarm attack with fixed-wing UAS describes a scenario which is allocated to the 30 kW GBAB weapon station described above.

For the UAS swarm attack, three jet-driven drones, based on a commercial available kit JT-240 (Figure 5), are modified according to the scenario specifications. They were auto-piloted by GPS to approach the HEL effector from a distance of about 4 km. The time interval between two subsequent UASs was chosen to about 20 s. Typical ground velocities during the approach were about 50 m/s with partially intense turbulence due to strong wind shear. After radar lock-on and coarse tracking, the UASs were illuminated and the fine tracking system of each BFU was set to track the same point on the target. In principle it is possible that each BFU tracks and fires at a different point. To maximize the effective range of the HEL-effector all three BFUs have been superimposed on the same point of interest. Two types of UAS hardkill approaches were tested: critical destruction of the UAS frame/control electronics and laser-induced detonation of an explosive payload similar to the VTUAS scenario. With a well-tuned and smoothly interacting coarse and fine tracking system, both approaches lead to the successful hardkill of the UAS within the limited time frame at distances of several kilometres (Figure 6). A swarm of three attacking UASs were successfully downed by a single HEL effector with 30 kW even under adverse weather conditions.

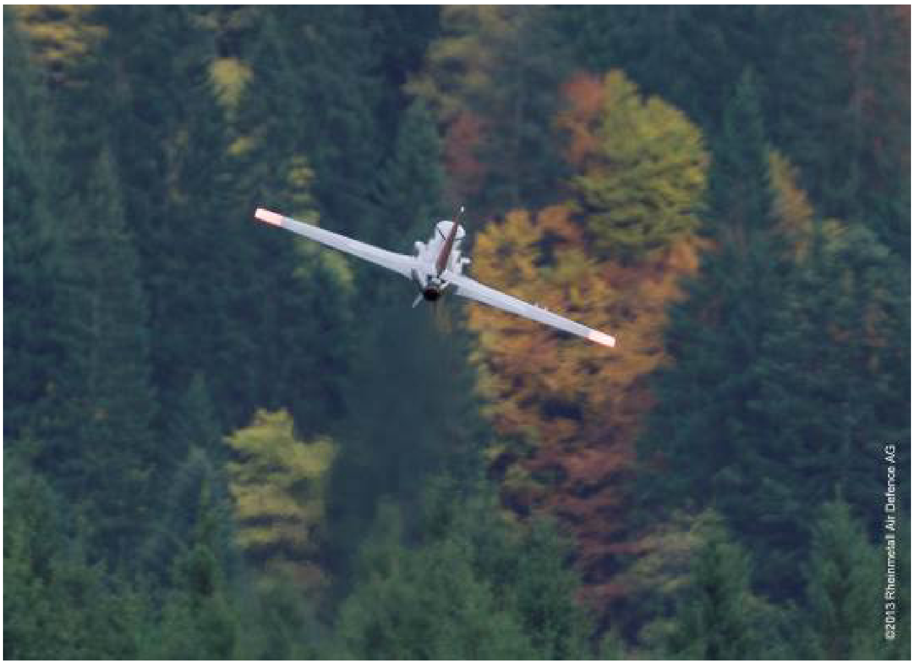


Fig. 5: Jet-driven UAS JT-240.

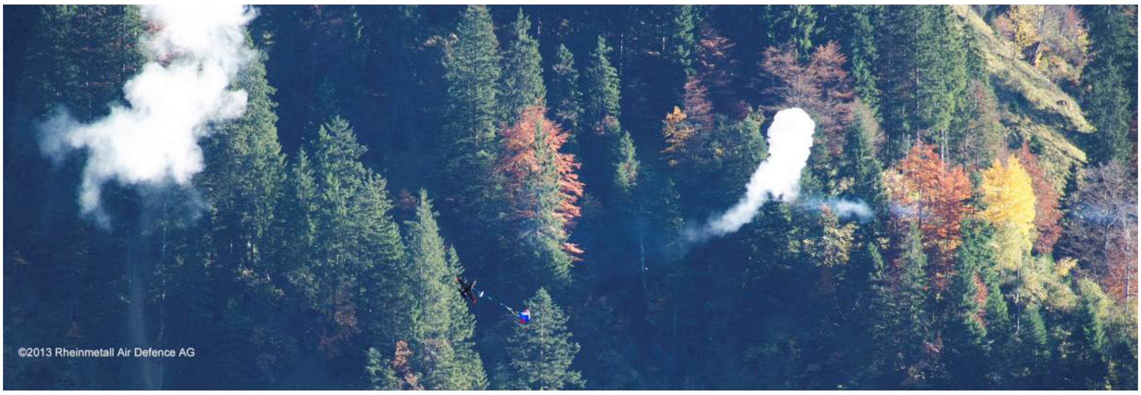


Fig. 6: UASs engaged by the Stationary Effector 30 kW. Top: a single JT-240 UAS. Bottom: downed UAS with rescue parachute (middle) with smoke from the target-laser-interaction (right). The smoke in the left part of the image originates from the hardkill of the previous UAS in the series.

4 CONCLUSIONS

The paper shows that Rheinmetalls modular high energy laser concept is well-suitable for integration of high energy laser weapons into a variety of platforms. The laser power and tracking modes can be tuned according to the mission profile and the available space of the platform. This ranges from completely autonomous tracked or wheeled vehicles (Mobile Effector Track V and Mobile Effector Wheel XX) to more powerful and complex laser effectors that are e.g. able to serve as components of a joint system (Mobile Effector Container L and Stationary Effector 30 kW). The capability of these effectors has been successfully tested by many different ground and air-defence scenarios covering EO sensor dazzling, VTUAS neutralization as well as the interception and neutralisation/defeat of UAS swarm attacks. All tests show that the theoretical advantages of HEL weapons such as high precision, scalability and reliability can be put into practice and are suitable for the use in the field by an appropriate system design. Future developments will concentrate on a further downsizing of the HEL components as well as even stronger system integration and networking in order to reach the full potential of high energy laser weapons.

5 ACKNOWLEDGEMENTS

The work was partly supported by the German Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAIN Bw).

REFERENCES

[1] Jansen, B. (2015). Small drone crashes near White House despite ban against flights in D.C. USA Today, http://www.usatoday.com/story/news/2015/10/09/drone-crash-white-house-ellipse-us-park-police-federal-aviation-administration/73641812/

[2] BBC: 'Drone' hits British Airways plane approaching Heathrow Airport. 17.04.2016, http://www.bbc.com/news/uk-36067591

[3] Mulholland, R. (2015). Paris seen from a drone – illegal but spectacular. 25.02.2015, The Telegraph, http://www.telegraph.co.uk/news/worldnews/europe/france/11434555/Paris-seen-from-a-drone-illegal-but-spectacular.html

[4] Heine, F. (2013). Merkel Buzzed by Mini-Drone at Campaign Event. SpiegelOnline, 16.09.2013, http://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html

[5] Pawlak, R. (2012). Recent Development and Near Term Directions for Navy laser Weapon System (LaWS) Testbed. Proc. SPIE 8547, Security and Defence, 2012.

[6] Ludewigt, K, Riesbeck, T, Graf, A., Jung, M. (2013). 50 kW laser weapon demonstrator of Rheinmetall Waffe Munition. Proc. SPIE 8898, 88980N, 2013.

[7] Ludewigt, K., Riesbeck, Th., Jung, M., et. al. Overview of the Laser Activities at Rheinmetall Waffe Munition. Proc. SPIE 8547, Security and Defence, 2012.

[8] Graf, A. (2012). High power fiber lasers for special applications. 15th International Conference on Laser Optics, St. Petersburg, June 25-29, 2012.

EMERGING THREAT; LOW SLOW AND SMALL UAVs & HOW TO DEFEAT THEM AT RURAL AREAS

Mustafa Ayazoğlu[1], Faruk Soykan[2], Fikri Dikmen[3], Meysun Avcı Özgün[4]

[1] *mayazoglu@aselsan.com.tr*
ASELSAN, Defense System Technologies Division –C2 Systems Engineering Dept., Macunköy, Ankara (Turkey)

[2] *fsoykan@aselsan.com.tr*
ASELSAN, Defense System Technologies Division –Air and Missile Defense Systems Dept., Macunköy, Ankara (Turkey)

[3] *fdikmen@aselsan.com.tr*
ASELSAN, Defense System Technologies Division –C2 Systems Engineering Dept., Macunköy, Ankara (Turkey)

[4] *avci@aselsan.com.tr*
ASELSAN, Defense System Technologies Division –Ballistic Missile Defense Systems Dept., Macunköy, Ankara (Turkey)

Abstract

Mini and Micro UAV arena witnessed a great advancement during the last couple of years. This advancement, different than many of the technologies in the past, is not only supported by commercial companies but also by the public interest. The immense technology advancement in the UAV arena leads to vast number of different commercial products with pretty advanced capabilities as well as an open source community custom building these units.

Unfortunately, these commercial products and the open source information are also accessible by the illegal parties, making mini and micro UAVs, especially drones as the number one offence instruments. These devices has many illegal uses in urban and rural environments. Since from the countering perspective rural and urban areas has very different constraints to be considered, in this paper we will focus on threats by these units in rural areas and how to counter them.

Keywords: drone, uav, countering, rural, anti-drone, terror.

1 INTRODUCTION

Mini and Micro UAVs, especially drones, are becoming more and more popular among hobbyist and unfortunately criminals/terrorists. This is due to the fact that they have high potential, are easily accessible and easily customizable. Many different illegal uses of these units both in urban and rural environments have been noted in the past. Example of these uses are reconnaissance [1], drug smuggling [7, 8], endangering airplanes and helicopters [4, 5], ISTAR [1] etc. To be able to efficiently counter these threats, many factors needs to be considered. These factors can be summarized as;

- Potential uses of UAVs

  - Types of UAVs and their limitations
- Threat environment
  - Urban
  - Rural
- Technical limitations

In this paper, we first focus on the potential illegal uses of mini and micro UAVs, then consider the environment focusing on rural environment constraints together with technical limitations and lastly we will try to come up with a general system architecture for rural environment UAV countering system.

2 POTENTIAL ILLEGAL USES OF MINI AND MICRO UAVS

To be able to understand the potential illegal uses of mini and micro UAVs, we first need to understand the potentials of these flying platforms. Broadly mini and micro UAVs can be classified into two main categories;

- Fixed Wing UAVs (Planes)
- Rotary Wing UAVs (Helicopters, Drones)

The UAVs in each of these categories have their own advantages and limitations. Table 1 summarizes the advantages and limitations of these categories.

Type	Advantages	Disadvantages
Fixed Wing UAVs	• Longer Range • More Stable (due to aerodynamics) • Higher Pay Load	• Larger • Low positional precision • Harder to fly • Harder to take off • Cannot Hover
Rotary Wing UAVs	• Smaller • High positional precision • Hovering • Easier to fly • Easier to take off • Agile	• Shorter Range • More Fragile (due to aerodynamics) • Limited Pay Load

Table 1: UAV Types and Their Advantages and Disadvantages

Keeping Table 1 in mind we can now focus on the previous illegal uses of UAVs and come up with a framework, which will help us to understand their illegal usage potential.

These units have been reported to be involved in the following illegal acts. The features of the mini and micro UAVs that suit the misuse are also added following the respective item.

- Illegal reconnaissance

  For a UAV to be used in reconnaissance, it should be carrying a camera that streams video to the ground station or saves it to a memory space. If it could hover at a certain altitude the mission might be conducted with higher success rate. Additionally it should also be noted that if the reconnaissance is done real-time because of the downlink and RC ranges the ground station cannot be further away that about 5kms (assuming commercial RF links)

- Drug smuggling

  The UAVs used for drug smuggling should be able to carry additional pay load, on the other hand a UAV with GPS is also required since the remote controller range for most of the UAVs are limited to 5kms additionally manual use of the drone may not be possible around the border where ground forces limit accessing certain areas around it.

- ISTAR

  This is very similar to the illegal reconnaissance offence, except it is mostly done in rural areas where the offender’s main aim is to use an explosive weapon where the UAVs are used for giving instantaneous feedback. This is done through the video streaming back to the ground station. Additionally a UAV equipped with GPS is also useful from the point of the view of the offender.

- Endangering airplanes and helicopters

  Unlike the threats above the UAVs themselves may create trouble for the air vehicles without even carrying an explosive device. If the UAV has the potential of hovering at high altitudes this may also create additional trouble for the air vehicles.

As it can be noted from the previous discussion, the main characteristics of mini and micro UAVs that make them possible terrorist tool are;

- They can carry some pay load
- They have a camera with downlink/with memory
- Some can hover or move quickly without being spotted
- Some may have a GPS for precise positioning

So any illegal act requiring these characteristics can be done using mini and micro UAVs.

We can now make the connections between the terrorist acts and the type of the UAVs and can have some educated guesses. For example if a terrorist act requires a very heavy explosive carrying we can assume that the attack might be done using a fixed wing UAV. If it requires precise surveillance it can be done using a rotary wing UAV since they can hover. If the terrorist act requires sneaking into a base it can be done using a drone since they can follow the terrain with ease and avoid obstacles since they are agile.

3 THREAT ENVIRONMENT AND ASSOCIATED TECHNICAL LIMITATIONS

After reviewing the potential of mini and micro UAVs we can now consider the effects of the environment. The environment both changes the types of attacks and threats as well as the countering methods and the way of surveillance. The following list indicates the associated problems in rural areas and presents a solution to each of them. Note that the list is not exhaustive.

Mini and micro UAV countering at rural areas

- **Problems regarding to Line-Of-Sight (LOS):** Especially for low flying drones LOS can be a problem creating fragmented tracks in the radar and in EO. Fragmented tracks may result in short tracking times which may not be enough for identifying the target and shorten the reaction time.

  Solutions for this might be;
  - Using different sensors at different points. Although it may not be possible for urban anti-LSS systems to spread around too much for rural environments the deployment options are a lot more.
  - Mixing and matching with different type of sensors which may not require line of sight (e.g. Acoustics)
  - Using elevated sensors. Using elevated sensors will be more advantageous in terms of LOS, however there is an additional complexity involved with this solution which is for some of the sensors (e.g. Radars) the sensor should be looking downwards creating limitations on the maximum possible range.

- **Problems regarding to C2 Network:** Unlike urban environment, for the rural environment there might not be a readily usable high bandwidth communication infrastructure. In these areas for the system installation the communication back bone should also be created which might be a limiting factor for deployment and hence the solution of distributing the sensors to different locations to solve LOS issues might not be possible in some cases

  Solutions for this might be;
  - Using wireless connections, however using wireless connection requires special attention depending on the system's effector. For example if the effector is a jammer careful frequency planning is required which complicates the system solution.

- **Problems regarding to High Altitude Attacks:** This is a shared problem with the urban environment case, when a UAV is flying very high above while approaching the defended asset it might not be detectable after a certain range. The problem happens because with most of the sensors, dome coverage is not possible (e.g. Radars, EO, etc.) and most of the sensors cannot see what is on top of them creating a blind region.

Solutions for this might be;

- Using a different sensor of the same kind with a different viewing angle
- Using a completely different sensor with dome coverage (e.g. Acoustics) Note that although using an acoustic sensor for rural environment case is possible, this might not be a feasible solution for most of the urban environment cases due to high ambient noise. Also note that using a sole acoustic sensor has its own disadvantages such as their limited range.

- **Problems regarding to Hovering Targets:** This type of attacks can be used for surveillance type of threats, where the objective of the offender is to gather as much as information as possible about the defended asset before a main stream attack starts. Using the terrains roughness the offender can come close enough to a distance where surveillance is possible and hovers at a certain altitude. Although the motion of the drone from behind of the obstacle to hovering altitude might provide some detectable cues for some sensors the duration of this motion is usually is not long enough to detect the target. Once it is in the hovering state, the drone might be completely undetectable for some of the sensors.

  Solution for this might be;

  - Using the micro doppler effect for some radars. However the micro doppler effect would only be observable after a certain range.
  - Using the constant or slowly changing background assumption for EO and learning the background adaptively. However background adaptation should be adjusted carefully otherwise the drone might be blended to the background. Note that while this is easy for fixed asset protection it is harder to implement for mobile asset protection.
  - Using the acoustic sensors for “listening” how the motors sound, however to be able to distinguish the hovering motor’s sound from the noise, a large database is required.

- **Problems regarding to Effectors:** Once the threat has been detected and identified, the only thing is left to negate the threat. This can be done in two ways these are soft kill which only stops the UAV doing its mission (jam, spoof, blind, etc.) and hard kill which stops the UAV itself (guns, missiles, laser, etc.). The choice of kill depends on the environment and the mission of the UAV, unfortunately detecting the UAV’s mission is not an easy task and special intelligence should be involved in the task. If the UAV’s mission is known the operational concept might first require a soft kill and if the soft kill is not successful a hard kill method might come into the place. Note that for urban case hard kill methods may not be feasible. On the other hand unfortunately for most of the cases soft kill and hard kill weapons are completely different and there is no single sensor capable of both (except lasers). Since this is the case a method for choosing most suitable weapon is required.

  Solution for this might be;

  - Using command and control (C2) system with threat evaluation and weapon assignment (TEWA) tools.

4 PROPOSED SYSTEM ARCHITECTURE

As it can be noted from the previous section, the following properties of the system should be shared by most of the counter mini and micro UAV systems. These are;

The system should have

- Multiple different type of sensors
- Multiple different type of effectors
- A C2 system with fusion and TEWA capabilities tailored for the case

Given these facts we propose the following general system architecture

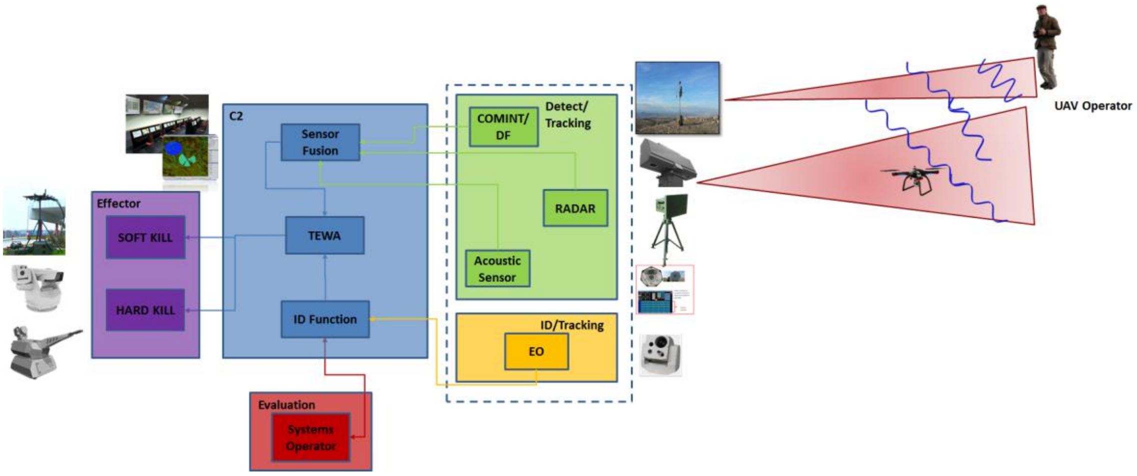


Figure 1: General System Architecture

Note that the system splits the division of workload among different type of system units. This way each of the system's sub units' weaknesses are covered by some other unit/s in the system. Since no single sensor or effector is perfect for mini and micro UAV countering purposes.

5 CONCLUSION

In conclusion, since mini and micro UAV attacks change from environment to environment, it can be said that no single sensor of effector is perfect for this case every sensor and effector has its own advantages and disadvantages. Sensors and effectors should be used in combination with the help of a command and control system to get the maximum benefit out of them. It should also be noted that any solution is environment specific and while one solution is perfect in one case it may completely fail in another environment. So the systems should be crafted carefully for the specific case.

REFERENCES

[1] http://www.theguardian.com/uk-news/2016/jan/11/drones-terrorist-attacks-security-thinktank

[2] http://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office

[3] https://www.theguardian.com/football/2014/oct/14/serbia-albania-euro-2016-flag-halted

[4] http://www.theguardian.com/world/2013/apr/25/israeli-aeroplane-shoots-down-drone

[5] http://www.dailymail.co.uk/news/article-3184023/Department-Homeland-Security-issues-terrorist-warning-three-drones-spotted-three-days-flying-dangerously-close-planes-landing-JFK-airport.html

[6] http://www.dailymail.co.uk/news/article-2814363/Drones-carrying-explosives-number-one-terror-threat-say-NYPD.html

[7] http://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268

[8] http://www.independent.co.uk/news/uk/crime/criminal-gangs-using-drones-to-deliver-legal-highs-to-prisons-a6791191.html

COMBINED TRANSIENT EFFECTS OF THERMAL AND MECHANICAL STRESS ON MATERIAL

Berthold Roemer

bertholdroemer@bundeswehr.org
Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS),
Humboldtstrasse 100, 29633 Munster (Germany)

Abstract

Nuclear weapons still exist and protection of today's and future critical infrastructure and defence material should be considered. This paper presents an alternative approach to determine combined thermal heat flash and blast effects. The idea is twofold. Instead of using very expensive experimental simulators the investigation of combined effects could be done with numerical simulation. The numerical simulation of a coupled thermal and mechanical interaction has to be validated by experiments. This leads to the need, to determine the effects of combined interaction with a combination of simultaneously measurements of mechanical and thermal stress.

As an example, the paper will show the determination of material stiffness change by ultrasonic pulse-echo techniques during thermal flash on homogeneous material (e.g. PVC).

Keywords: Nuclear weapon – thermal radiation - elastic modulus – mechanical properties - ultrasonic

1 OBJECTIVES

The importance of combined thermal heat flash and blast effects is increasing, because new material will be used more and more to build critical infrastructure or defense material. Especially, synthetic material like plastics, carbon fiber or insulation materials are more common. These materials have typically very low thermal conductivity that can lead to a higher temperature stress. Therefore, a thermal heat flash can change the material properties of synthetic materials seriously. A blast will hit this changed environment typically few seconds after the heat flash. This will lead to synergistic or combined thermal blast effects that could not neglected if the damage on these material is assessed. Although, the experimental possibilities to investigate combined effects are decreased.

The intention of this paper is to show that a mixture of experimental tests and numerical simulations can be used to estimate the importance of combined thermal heat flash and blast effects. A method will be presented to validate numerical codes that shall compute combined thermal and mechanical stress.

1.1 Nuclear Heat Flash and Blast Characteristics

The heat flash and blast characteristics of nuclear weapons are scenario dependent [1]. Special environmental conditions can be simulated, separately or combined.

1.1.1 Heat Flash Simulation

Heat flash simulation capabilities exists for example at WIS [2].

Here is available an indoor and an outdoor facility.

The indoor facility uses pulsed Xenon-lamps (about 6000 K blackbody radiation) that offers a maximum irradiance of about 400 W/cm^2 with user defined pulse shapes (for example nuclear pulse shapes – 1./2. pulse) for small surface exposure (ca. 25 cm^2).

The outdoor facility uses 4 burner units (about 2600 K blackbody radiation) that offers a maximum irradiance of about 200 W/cm^2 with trapezoidal pulse shapes for surface exposure up to about 10 m^2).

Établissement Technique Central de l'Armement (ETCA) offers a Solar Furnace [2].

1.1.2 Blast Simulation

The assessment of the effects of nuclear blast waves on infrastructure or military equipment relies to a large extent on numerical simulations and experimental investigations in specialized blast simulation facilities, such as the LBS 501 operated by the Armed Forces Technical Center WTD 52. Facilities of this type can generate blast waves with positive durations in the order of several hundred milliseconds and amplitudes of up to or more than 100 kPa at a scale appropriate for testing armored vehicles of small aircrafts [3].

1.1.3 Simulation of Combined Effects of Thermal Radiation and Blast

The Large Blast and Thermal Simulator at White Sands Missile Range (WSMR), New Mexico is operated and maintained by the Defense Threat Reduction Agency. The simulator includes a 165 m tunnel with a semi-circular cross section with a radius of 10 m. This facility can be used for the survivability testing of Department of Defense equipment to the combined effects of thermal radiation and blast from low height-of-burst nuclear detonations [4].

1.2 Typical Parameters in Heat Flash and Blast Experiments

In general, measurements in Heat Flash and Blast experiments are time responses of the incident stress on a Device under Test (DUT) and the response of a DUT to the incident stress. The response of a DUT will be observed with sensors and photographic means.

1.2.1 Parameters in Heat Flash Experiments

In Heat Flash Experiments the incident stress is the irradiance that is linked to a total thermal fluence [J/m^2] and an energy delivering time that represents for example 90 % of the incident energy. The determined response parameters of a DUT depend on the characteristics of a DUT: Parameters are temperature, transmission-/emission spectra, weight, development of flames and smoke, distortions, ablations.

1.2.2 Parameters in Blast Experiments

In Blast Experiments the incident stress is the atmospheric pressure that is linked to an incident peak static over pressure, peak dynamic pressure, positive phase duration, static overpressure and dynamic pressure impulse. The determined response parameters are e.g. accelerations, strains, distortions, ablations, crack gross and turn over.

1.3 Necessary Parameters to Validate a Numerical Code that shall Simulate Combined Transient Effects of Thermal and Mechanical Stress on Material

The observed trend in numerical simulation is to link all necessary or possible physical interactions of matter in to one code. The validation of the code will be worked out systematically: First step, validate each interaction separately. Second step, validate meaningful combinations of interactions. Last step, validate every combination of interactions. The validation will be accepted if a well-defined real world experiment can be transferred successfully to the virtual world. The set-up of that a real world experiment has to be well defined (as exactly as necessary). In detail the input parameters and the underlying physical theory are sufficient known. Additional, the algorithms has to be suitable.

1.3.1 Necessary Parameters in Heat Flash and Blast Effect Simulation

It is quite obvious that all mentioned parameters in chapters 1.2.1 and 1.2.2 should be reproduced by computing a virtual world experiment. But, a numerical simulation that is based on a fundamental theory and not only on mathematical fits of special experimental results needs additional input.

The following parameters are fundamental to determine thermo-mechanical effects on material/systems:

- elastic modulus
- strain curve
- pressure on contact junctions between different material
- rigidity modulus
- reactivity

There exist data in the literature that could be used as input. For example see Fig. 1 that shows the thermal dependence of the elastic modulus from temperature.

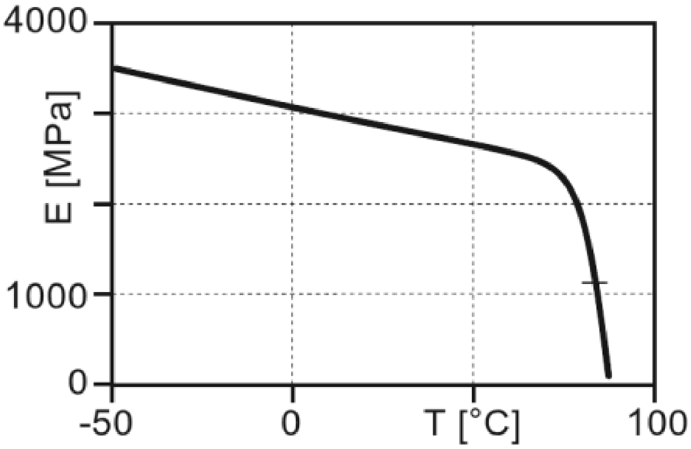


Figure 1: Elastic modulus of Polyvinyl Chloride, PVC (unplasticized) as function from temperature [5]

Typically, data are not available in the extent that is required. If the data are available, input it has to be checked, what is the origin of these data and whether these data are accurate enough to represent transient stress and not only quasi steady state simulations.

1.3.2 Additional Parameters in Combined Heat Flash and Blast Effect Simulation

Other parameters could be necessary to determine the blast interaction with the reactivity of DUT material. For example, an ignited fire could be spread out or extinguished.

2 METHODOLOGY

The basic method is to determine with a heat flash experiment all necessary parameters that are needed as input for a numerical simulation of blast effects. There will be of cause some parameters that cannot be determined with a heat flash experiment (see 1.3.2). How these parameters could be determined with a blast experiment will not be discussed in this paper.

A heat flash experiment offers the possibility to measure parameters that are needed to understand combined thermal and blast effects on material (see 1.3.1).

The measurement of thermal and mechanical material properties during a heat flash experiment provides the possibility to determine the coupling between thermal and mechanical interaction.

This is needed to validate a numerical code that should couple thermal and mechanical stress on material.

An example of a combined measurement technique will be presented in 2.1.

2.1 Determination of material stiffness change by ultrasonic pulse-echo techniques during thermal flash on homogeneous material

The term stiffness describes the resistance against elastic deformation. Therefore, stiffness is related to the elastic modulus E. E is linked to the sound velocity c and the density ρ of the material. Formula (1) shows the relation between c and E, if the transverse contraction μ is included [6]:

$$c = (E\,(1 - \mu) / (\rho\,(1 + \mu)\,(1 - 2\,\mu))^{-1/2} \qquad (1)$$

WIS investigated the change of sound velocity in unplasticized PVC during a heat flash of a Xenon (XE)-Lamp (50 W/cm^2), with trapezoidal pulse shape [7]. Energy of about 75 J/cm^2 was transferred onto the surface of a PVC plate, dimensions 6 cm x 6 cm x 0.4 cm, in two seconds.

Fig. 2 shows the ultrasonic pulse-echo measurement, done with ultrasonic pulse-echo tool USD 10 of Krautkramer using their probe H10M (10 MHz).

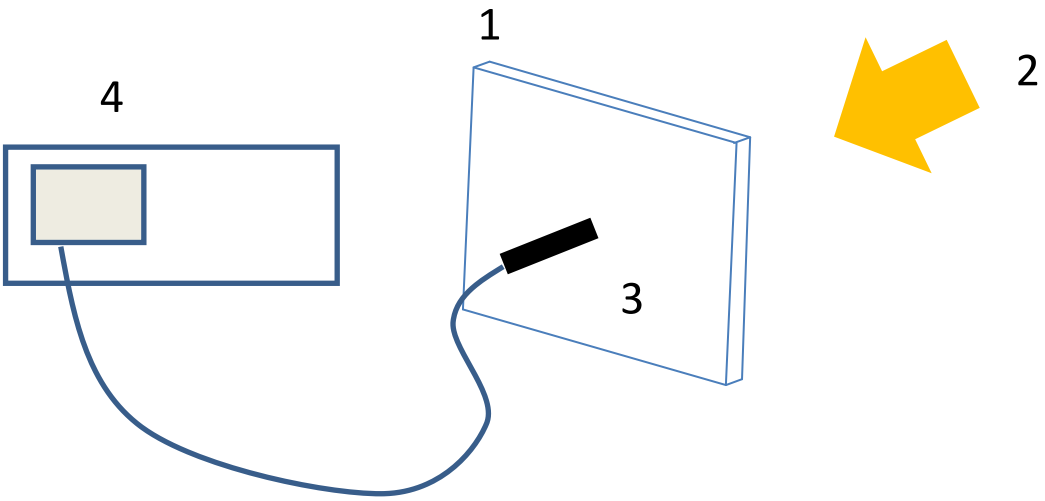


Figure 2: Sketch of a heat flash experiment on unplasticized PVC: (1) PVC plate, (2) XE-Flash, (3) ultrasonic probe, (4) ultrasonic pulse-echo tool.

The display of the USD 10 was recorded with a video camera. The time relation to the heat flash was not recorded.

Selected video pictures with relative equal time steps were done, Fig.3.

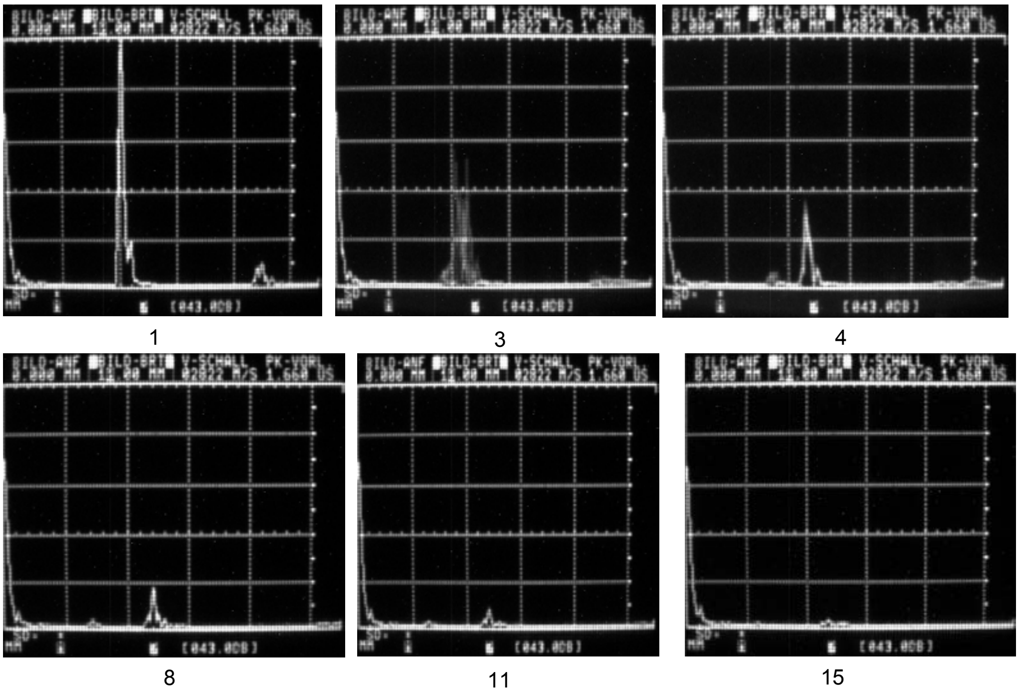


BILD-ANF BILD-BRT V-SCHALL PK-VORL
0.000 MM 14.00 MM 02822 M/S 1.660 US
1
3
4
8
11
15

Figure 3: Numbered video pictures of the display of ultrasonic pulse-echo tool

Fig. 4 shows the outcome of the video pictures.

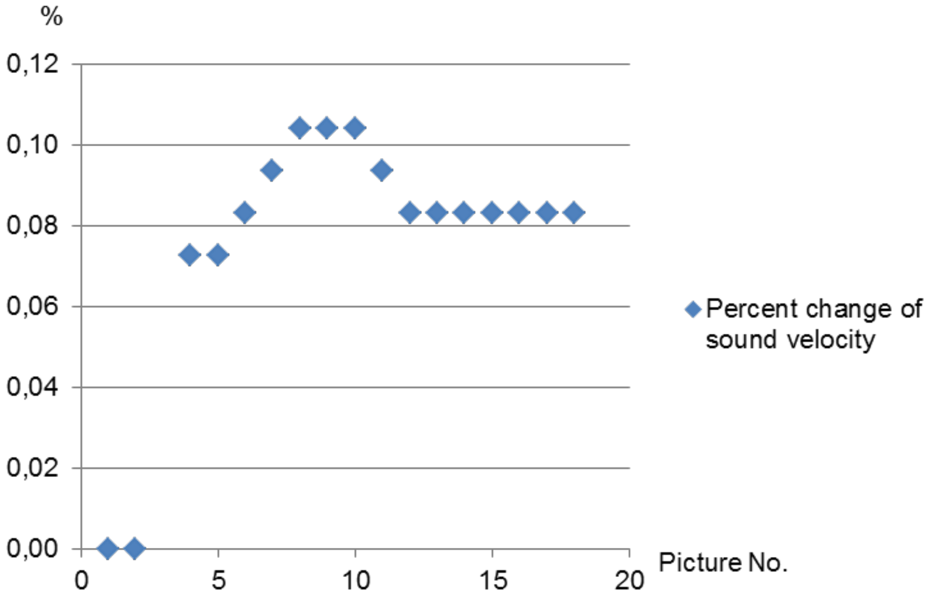


Figure 4: Determined relative change of ultra sound velocity

The front and back temperatures were measured with pyrometers (Optron IN 30 and Bartec R301). The maximum front temperature was about 630 °C. To determine the cooling effect of the ultrasonic probe, the back temperature was once measured without probe and with probe. The difference was about 30 %. The maximum back temperature was about 60 °C without probe and it was about 40 °C with probe. Therefore, the influence of the ultrasonic probe on the back temperature has to be pay attention. Obviously, it has to be considered for times after the incident temperature arrived at the back of the DUT.

An coarse approach indicated that a velocity change for unplasticized PVC would be expected in the order of about 6 %, if a core temperature increased from 20°C up to 75 °C (steady state). This can be estimated, using formula (1) with the parameters shown in Fig.1 and assuming a transverse contraction of 0.43.

At present, the ultrasonic pulse-echo technique will be optimized with respect to time correlation of heat flash, frequency of measurement and dynamic of measurement.

Finally, a numerical simulation of the experiment is planned.

The assumption is that a comparable result of experiment and computation could validate the experiment and the thermal mechanical code.

3 RESULTS

A validation of computing combined thermal and mechanical stress on material needs additional measurements. Especially, mechanical properties of material during thermal stress could provide the necessary information. In case of transient stress, these measurements are not yet common.

The example “stiffness change during heat flash” shows that this quantity can be measured for homogeneous material like PVC. But, the technique has to be improved.

4 CONCLUSIONS

WIS would like to improve its combined thermal and mechanical measurement to increase the possibilities of nuclear protection of todays and future critical infrastructure.

We believe that new combinations of measurement techniques are the right choice to validate the necessary multiphysics codes for this task.

REFERENCES [Arial, 12-point, bold, left alignment]

[1] Glasstone, S., Dolan, P. J. (1977). The Effects of Nuclear Weapons, United States Department of Defense and the Energy Research and Development Administration

[2] Simon, K., Wenig, P., Serra, J.-J. (2008). Reproducibility of Flux and Fluence Levels in Nuclear Thermal Testing, MABS20

[3] Klomfass, A.,van Keuk, J., Simon K. (2010). Extension of Ansys-Autodyn^{TM} for the Simulation of Nuclear and Conventional Blast Waves, MABS21

[4] Verma, A., Renon, G. (2008). Large Blast and Thermal Simulator (LBTS), MABS 20

[5] Ehrenstein, G.W.,Riedel, G.,Trawiel, P. (2012).Thermal Analysis of Plastics: Theory and Practice, ISBN 3-446-22673-7, p. 355

[6] Demtröder, W. (2015). Experimentalphysik 1: Mechanik und Wärme, ISBN 978-3-662-46414-4, p. 353

[7] Römer, B., Hübers, T. (2014). Ultrasonic pulse-echo investigation on PVC, internal documentation WIS Branch 310

SOTRA SAFETY IMPROVEMENT ON MOTORWAYS BY MEASURING WIDTH OF SPECIAL TRANSPORTS

Rigobert Opitz[1], Martin Gam[2] and Ichrak Ketata[3]

[1] *Rigobert.Opitz@rocgmbh.com*
ROC Systemtechnik GmbH, Raiffeisenstrasse 214, A-8041 Graz

[2] *Martin.Gam@asfinag.at*
ASFINAG SERVICE GmbH, Verkehrsmanagement, Sondertransportkoordination
Klingerstrasse 10, A-1230 WIEN

[3] *Ichrak.Ketata@rocgmbh.com*
ROC Systemtechnik GmbH, Raiffeisenstrasse 214, A-8041 Graz

Keywords

3D Vehicle contour measurement, exceptional transports on roads, road safety improvement, vehicle weight and dimension control, weigh in motion (WIM) systems

ABSTARCT

Guarantying a high standard of safety and security in the area of transport of goods and mobility on roads is an important challenge for the future. Avoiding blocking of motorways and tunnels especially by abnormal loads and transports not following regulations, in time and dimensions, is a precondition for safety on roads and traffic flow.
Innovative developments have been achieved by the SOTRA ("Sonder Transporte") Project for measuring and monitoring exceptional transports on motorways and sensing their compliancy with state regulations. The system consists of 3D Profile Laser scanners that automatically measure the width of the vehicles at high speed combined with automatic license plate recognition thereby in future allowing violation enforcement.

In Austria there are timely restrictions for special Transports starting with 3,51m width. The SOTRA System is also a response for the upcoming EU Directive 2015/719 concerning "Weight and Dimensions" in Europe.

1.0 OVERVIEW

In Austria vehicles and driving on highways are classified into 4 classes with defined driving times, based on their load width, starting from a width of 3,51m. Vehicles with higher widths like 4,5m or more have stronger restrictions and are the ones that cause the most trouble.

In fact, special transports on motorways and tunnels that are too wide and which do not drive during their designated time frames (usually night) can cause substantial traffic hold-up. Moreover, an abnormal road transport could not only hinder other traffic but also can considerably affect road safety.

Therefore, it is needed to ensure road and road users safety, to implement a system that can detect violating vehicles and is prepared to be used as a possible enforcement system in the future.

In the section 2 SOTRA Goals and Requirements are presented, Section 3 highlights the System Concept, followed by Section 4 summarizing the proof of Concept and concluded by Future Control Stations in Section 5

2.0 SOTRA Goals and Requirements

The Goals of the Projects were to detect and determine the width of special Transports through Scanner/Sensors at Highway speeds. By doing this, the compliance with the timely restrictions can be verified and enforce the law on offenders. Furthermore, using this intelligent sensing technology, it can be ensured that drivers and passengers are provided with highly safer travel.

At the end of the project, the following requirements were fulfilled:

1. The minimum width value used to define the limit for control and enforcement should be editable and can be changed easily
2. It should be possible to control and edit the time slot for the hold off period of the different vehicle classes (for example vehicles with a width value between 4,5m and 5m should not drive on the motorway between 06:00 – 08:00 and between 16:00 – 19:00)
3. Each control site can add its own exception rules regarding the hold off period of the different vehicle classes
4. Detection of vehicles and the delivered output should guarantee and ensure a clear and unique identification of the vehicles that can be used to enforce the violating ones.
5. Accurate width vehicle measuring on motorways while driving with high speed

3.0 SYSTEM Concept

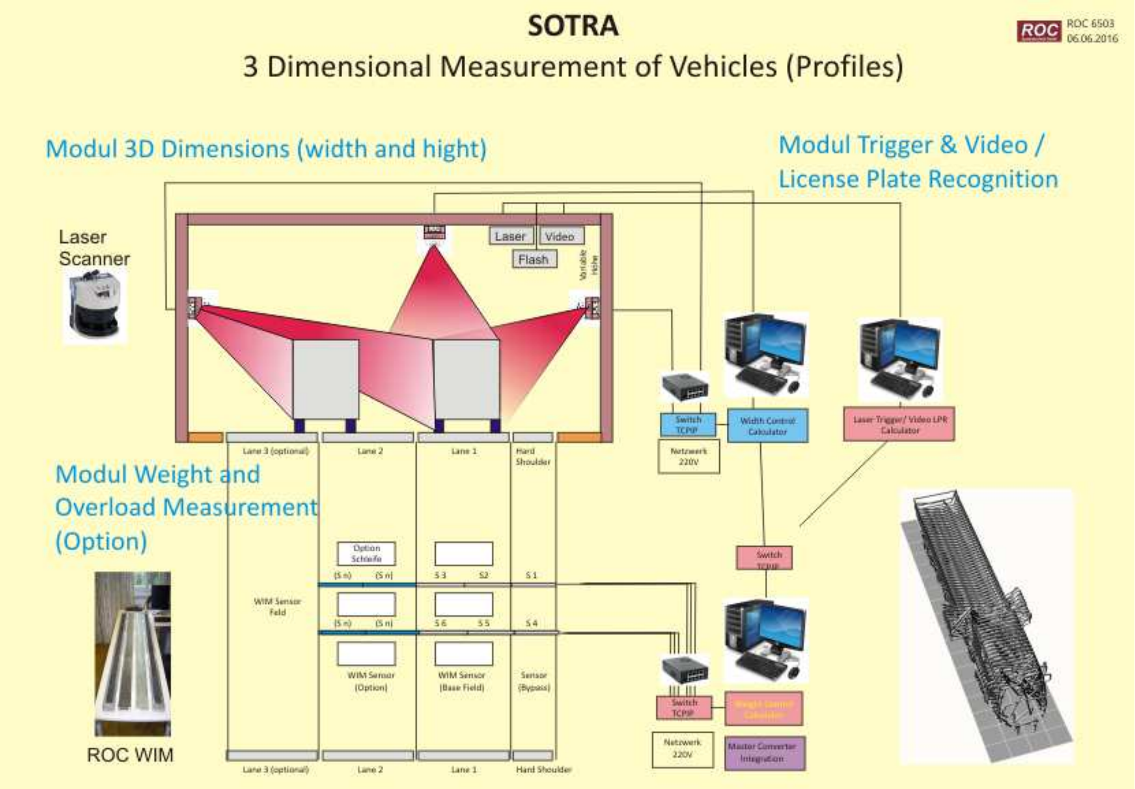
3.1 Width Measurement

Different technologies for width measurement where compared and the best solution was chosen. The width measurement is done trough three Laser Scanners that are positioned over the highway. The Sensors create a 3D Profile of the Vehicle. Through this height and can be measured exactly.

Three laser scanners were fixed on the gantry and deliver data to the measurement system that gives as a base for further calculation and consideration of different parameters.

Through the Laser Trigger and Camera, front picture of the vehicle is taken, and the License Plate Number is computed.(*Relevant data protection aspects were considered).*

The output from those two modules is integrated and saved into the database as a part of the preparation for future use for enforcement.



SOTRA

3 Dimensional Measurement of Vehicles (Profiles)

ROC 6503
06.06.2016

Modul 3D Dimensions (width and hight)

Modul Trigger & Video / License Plate Recognition

Modul Weight and Overload Measurement (Option)

Figure 1

The system is prepared to be extended with a new generation of HS WIM sensors for weight measuring to combine top down and bottom up measurements of the vehicles. (*Relevant data protection aspects will be considered).*

3.2 3D Vehicle Contour Profiling

The basic element of the system is an arrangement of 3 synchronized Laserscanners, one from both sides and one from the top on a gantry.

The sensors are positioned to cover the section of the road to be monitored.

This disposition allows a vehicle contour profiling and vehicle width measurement.

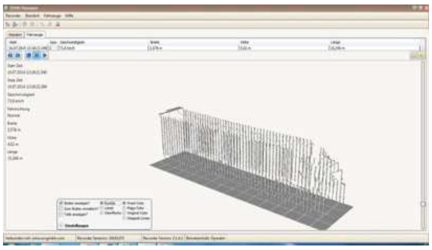
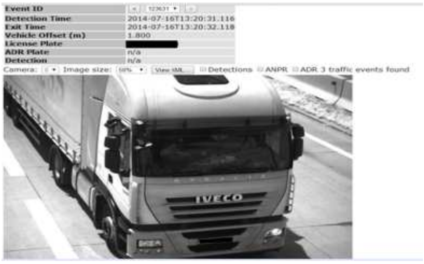


Figure 2

3.3 Number plate recognition

With the camera System, a picture of every special transport is recorded. By using special software the Number plate as well as the EU dangerous goods plate (ADR) are recognized. This picture associated with the License Plate Number and the ADR are associated with the vehicle contour profile and stored in the Database. (*Relevant data protection aspects were considered).*



Event ID	123631
Detection Time	2014-07-16T13:20:31.116
Exit Time	2014-07-16T13:20:32.118
Vehicle Offset (m)	1.800
License Plate	[redacted]
ADR Plate	n/a
Detection	n/a

Camera: Image size: 50% View XML □ Detections □ ANPR □ ADR 3 traffic events found

Figure 3

3.4 Integration

Systems for width measurement, image capture, number plate recognition and preparation for HS WIM were integrated. By doing this, several challenges where overcome: Reading & Synchronization of Data, Managing of Data, configuration of Laser scanners.

3.5 Graphical User Interface

The Graphical user interface that was implemented is composed of two parts: settings interface and displays. The interface allows checking Vehicles wider than a selectable width, which can be edited. The temporal restrictions can be also changed to fit individual needs (Default: Restrictions for the whole of Austria).

In the display part, vehicles that are wider than the defined minimum width are shown to the user. Vehicles that violate the restrictions are highlighted with yellow color.

4.0 PROOF of Concept

Prof-of-Concept through implementation of Sensors, Adapters, Cameras, Number plate recognition, software, integration of components, data transfer and graphical user interface was done and verified by test measurements.

The width measurement of special vehicles wider than 4.5m is possible and was tested. The tests were done with a special test vehicle at 2.8m, 3m, 4m and 5m widths and promise an accuracy of around ±10cm.

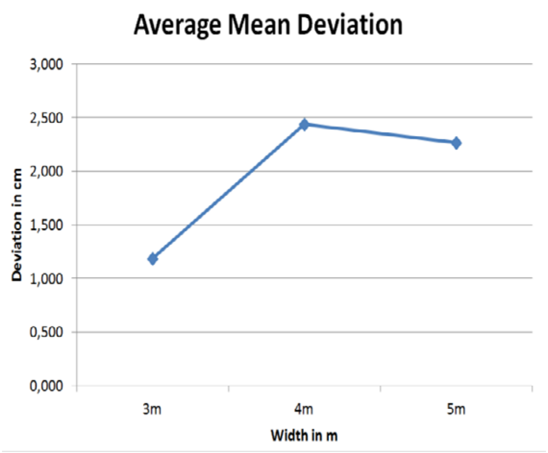


Figure 4

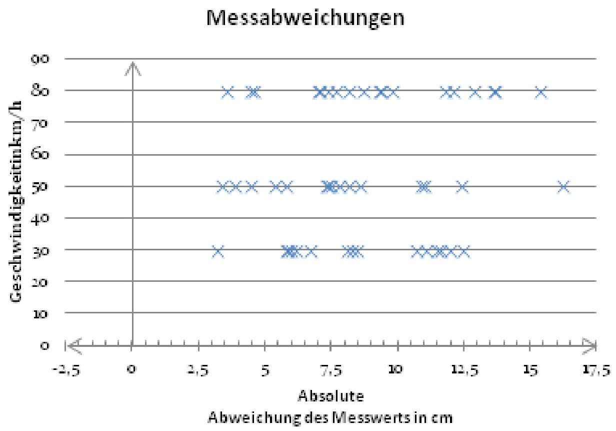


Figure 5

4.1 Variable width thresholds

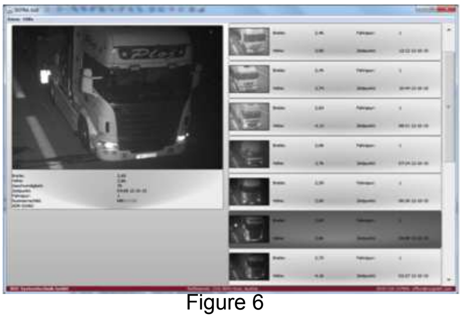


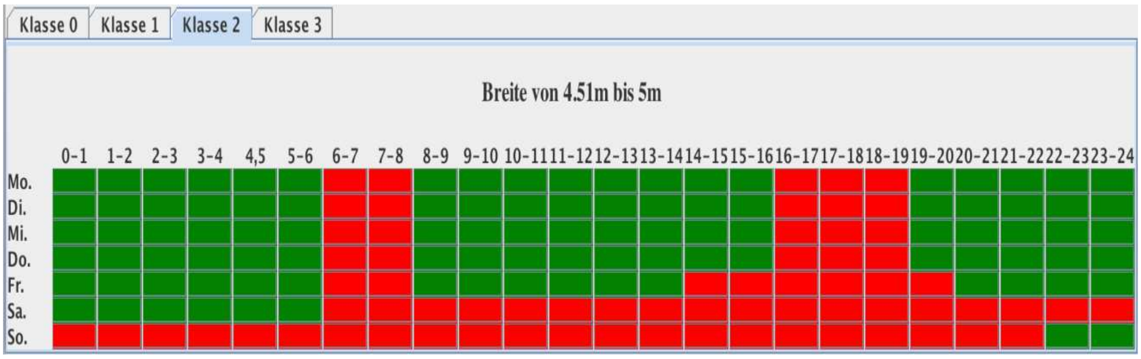
Figure 6

Vehicles that are wider than the defined with threshold are displayed in the graphical interface. In the right side of the GUI a list of a vehicle is displayed. Once one of them is selected, it will be shown in the left side with bigger pictures.

The Vehicle parameters width, height, speed, timestamp, lane, image and number plate are displayed. If available also the ADR plate data is displayed.

4.2 Variable temporal restrictions

Every installation of the graphical user interface can be configured individually. Both the minimal threshold as well as the temporal restrictions for the different special transport classes can be defined individually.



Breite von 4.51m bis 5m

	0-1	1-2	2-3	3-4	4,5	5-6	6-7	7-8	8-9	9-10	10-11	11-12	12-13	13-14	14-15	15-16	16-17	17-18	18-19	19-20	20-21	21-22	22-23	23-24
Mo.	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩
Di.	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩
Mi.	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩
Do.	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩
Fr.	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩
Sa.	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
So.	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩

Figure 7

The table in the original software was specified for a vehicle width of 4.5 to 5 m for the different days and hours of the day.

The different classes are represented in different tables. For example vehicle of the Class 2 are those with a width value between 4,5m and 5m.

Red color represents the hold off time. For example all vehicles within the Class 2 are allowed to drive on Sunday only between 22:00 and 24:00

4.3 Calibration (gauge) ability of the system

Next step will be a project to get the official calibration or official certification of the system.

For the future official gauging of the System several steps are planned, e.g.: Picture of full vehicle (legal reasoning) and ensuring the coverage of corner cases.

During the SOTRA project it was proven that, although the high speed with which the vehicles were driving in the motorway, a high accuracy was achieved measuring the vehicle widths, which should be usable for direct enforcement.

5.0 FUTURE Weight and Dimension Control Station

The development of the specification for the system for width measurement of special transports at highway speeds includes the holistic approach for future „Multi-Purpose control stations“. These stations should measure weight and dimensions while allowing for multi-lane-free-flow.

Preparation of new HS-WIM with new sensors developed is an innovative method to capture weights of wheels, axles, axle groups and gross weight and tire footprints of trucks

At the moment the new WIM sensors are in developed (Optimsation), with the following features: Inline technology, internal data processing within Sensor, 80 measurement points per Sensor, creation of Multi-Sensor-Arrays. The sensors are calibrated statically in advance and can be placed in the road within 15 minutes. These Sensors allow for True multi lane free flow.

Next step is the preparation to gauge the System for enforcement together with local authorities (Federal Office of Metrology and Surveying). The System arrives at a critical time as the EU directive concerning “Weight and Dimensions” has to be fulfilled in the coming years.

The integrated concept of SOTRA and WIM envisions “Multi-Purpose control stations” for the future, measuring weight, dimensions, speed and other vehicle parameters at the same time.

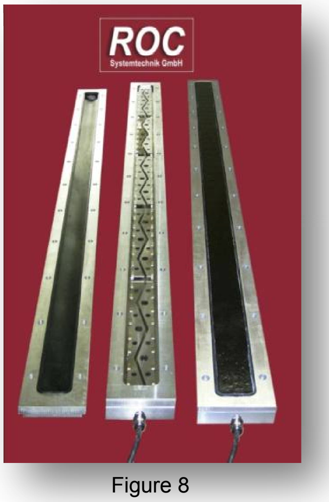
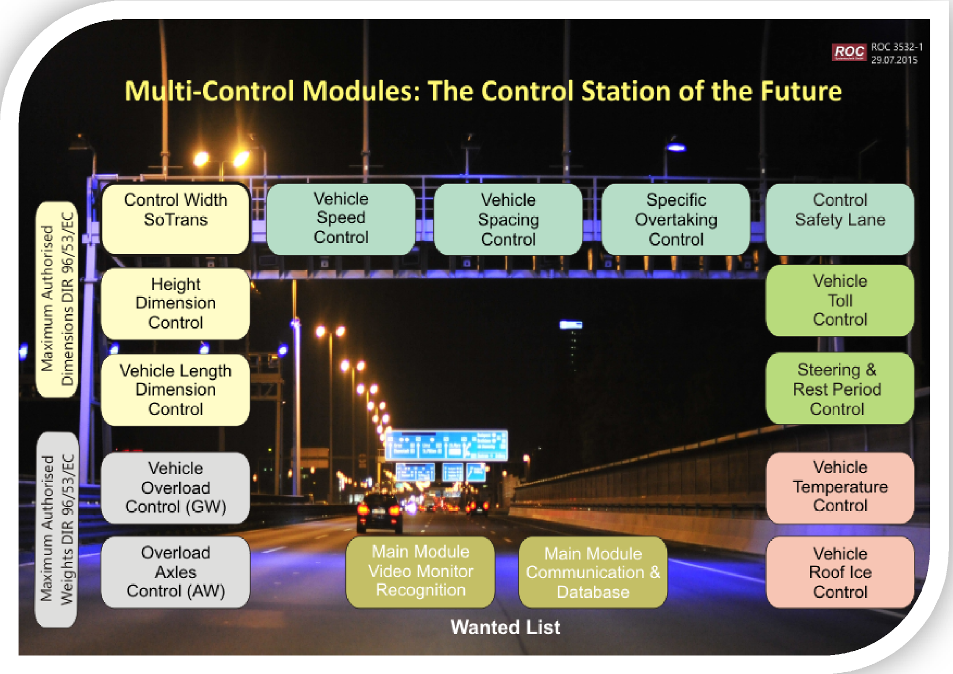


Figure 8



Multi-Control Modules: The Control Station of the Future

Maximum Authorised Dimensions DIR 96/53/EC

Maximum Authorised Weights DIR 96/53/EC

Control Width SoTrans

Vehicle Speed Control

Vehicle Spacing Control

Specific Overtaking Control

Control Safety Lane

Height Dimension Control

Vehicle Toll Control

Vehicle Length Dimension Control

Steering & Rest Period Control

Vehicle Overload Control (GW)

Vehicle Temperature Control

Overload Axles Control (AW)

Main Module Video Monitor Recognition

Main Module Communication & Database

Vehicle Roof Ice Control

Wanted List

Figure 9

DEVELOPMENT OF A WIRELESS LOW-POWER SENSOR NODE FOR LOW LATENCY SENSOR NETWORKS USING WAKE-UP RECEIVERS

T. Kumberg[1], J. Kokert[2], R. Tannhäuser[3], M. Schink[4] and L.M. Reindl[5]

[1]timo.kumberg@imtek.uni-freiburg.de

[2]jan.kokert@imtek.uni-freiburg.de

[3]robert.tannhaeuser@imtek.uni-freiburg.de

[4]marc.schink@saturn.uni-freiburg.de

[5]leonhard.reindl@imtek.uni-freiburg.de

University of Freiburg Department of Microsystems Engineering – IMTEK
Laboratory for Electrical Instrumentation Georges-Köhler-Allee 106, 79110
Freiburg, Germany

Abstract

Wireless sensor networks still suffer from short lifetimes originating from limited energy sources. Due to their low-power consumption and on-demand communication ability, wake-up receivers represent an energy efficient and simple enhancement to wireless sensor nodes and wireless sensor network protocols that have the ability to increase network lifetime. Here, we analyse a simple and energy efficient cross-layer routing protocol for wireless sensor nodes that include a wake-up receiver. The protocol makes use of shorter and larger transmission ranges of wake-up and main radios to safe energy by crossing several nodes during data transfer. In respect to energy consumption and latency, it outperforms existing protocols in many scenarios. In this article, we present a wireless sensor node utilizing the wake-up transceiver. We demonstrate and analyse the multi-hop protocol in a laboratory test setup. To further increase lifetime and reliability of sensor networks, we present methods to safe energy at the node by means of an energy sub-system.

Keywords: cross-layer routing protocol, wake-up receiver, energy-aware routing.

1 INTRODUCTION

Supervisory control and data acquisition (SCADA) systems are commonly used to continuously monitor and control for example critical infrastructures, such as pipelines or power grid lines in real-time [1, 2, 3]. According to [1], a SCADA system consists of a SCADA centre which does the main data processing, storage and visualization and provides process control functionality. Linked to the SCADA centre are remote terminal units which act as gateways to connected sensors. Wireless sensor networks play a more and more important role for example to replace wired remote terminal units, to connect wireless sensors to them or to extend existing SCADA systems at low costs, with respect to installation and maintenance [1, 3]. In addition, wireless sensor networks provide in-situ data access to local operators who can carry out their tasks based on current data [2].

But wireless sensor networks also impose new challenges, as they usually have higher latencies compared to wired networks. Wireless sensor nodes (WSN) have limited energy resources or are powered by fluctuating sources. As a consequence, wireless sensor nodes may fail in certain scenarios. Failing can lead to data losses at the sensor node and, more severe to the whole network, leads to connection losses between sensors in the field or to the base station. If the power on a node falls below a certain level, critical tasks such as sending of alarm signals cannot be performed.

Adjusting the duty cycle based on the available energy is method commonly used in sensor nodes. The authors of [4] separate a system in a wireless sensor node under test and an energy sub-system. The execution of different application tasks based on battery voltage is shown in [5].

In this paper we introduce a low power wake-up sensor node. We present a simple cross-layer routing protocol that can be used to transmit data with low latencies and show the efficiency of the protocol based on its overhead ratio. In the second part, we introduce an energy monitoring sub-system to create energy awareness on the node and to prevent node failures caused by energy insufficiencies.

2 HARDWARE AND SOFTWARE

2.1 Wireless Sensor Node

The wireless nodes used in this work are based on the sensor node introduced by [6] and further developed in [7, 8]. The microcontroller utilized on the nodes is a 32 bit EFM32 Gecko family device by SiliconLabs. It provides up to 128 kB RAM and 1024 kB flash memory and several low power states to reduce the overall energy consumption. With activated realtime clock the EFM32GG for example can be configured to draw only 1.1 µA.

For long-range data communication, a CC1101 radio is used that has a current consumption of 30 mA when transmitting at 10 dBm output power at 868 MHz and around 17 mA transmitting at 0 dBm. Its sensitivity depends on the communication data rate, at 38.4 kbaud it is around -104 dBm. The 125 kHz wake-up receiver (AS3932) from austriamicrosystems 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 [6,7] and an total energy consumption of around 9 µW in listening mode. To store incoming and outgoing data, the sensor nodes can be equipped with a MicroSD card that provides several GB of storage. A software ringbuffer provides flexibility and logging functionality to prevent data losses in case of network outages.

The embedded software is realized as a state machine. An integrated watchdog timer provides additional security and is able to reset the microcontroller in case of unintended software loops or other errors.

To test the cross-layer protocol and the energy sub-system, the wireless sensor node is equipped with a piezoresistive sensor (MPL3115A2) by Freescale. The sensor has an integrated 24-bit ADC to provide digitally temperature, humidity and air-pressure readings. In standby mode, the sensor draws around 2 µA. To reduce output noise the sensor is able to oversample readings in the range of 1 to 128 oversamples. Increasing the number of oversamples increases resolution and power consumption.

2.2 Routing Protocol

The sensitivity of the wake-up receiver is lower than the sensitivity of the communication radio, thus data can be sent over greater distances than wake-up messages. The routing protocol depicted in Fig. 1 and introduced in [8], makes use of this behavior: 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. 1 for example node 13 sends a wake-up signal to node 12, which forwards the wake-up to node 11 that itself wakes node 10. Data communication may now be done to one of the woken nodes 10, 11 or 12. As communication radios have high energy requirements in the range of 50 – 100 mW during communication, significant amounts of energy can be saved by using this approach.

As introduced in [8], the node that initiates a communication (node 13) sends a routing request to the first woken node (node 12). This node forwards the routing request to its next neighbour (node 11) and answers the initial request by sending a route request acknowledge to the initiating node (node 13). Similar to this, each woken node (nodes 11 and 10) sends a route request acknowledge to the node that started the communication (node 13) to show their presence and to provide status information.

Status information can be free data slots (at receiver) and hop distance from the starting node. Further parameters like link quality, receiver signal strength and information of the energy sub-system like harvested and remaining energy can be included to increase the stability of the network. By using the energy parameters, an energy aware routing can be realized that is able to enhance significantly the network lifetime. The source (node 13) decides to which node the data will be sent based on this status information.

Once the communication link to a node is established, up to 64 data packets (with up to 256 bytes size each) can be transmitted subsequently. After transmission, the link is closed and the participating nodes go back to sleep again.

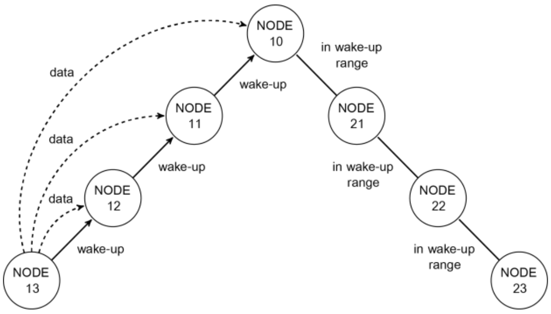


Fig. 1: Schematic of the wake-up multi-hop routing protocol [8].

2.3 Energy Awareness

Keeping in mind that the energy source for each node is limited, the only way to save energy is to prioritize tasks. This may result in skipping or postpone regular low-priority tasks to guarantee a failsafe operation of sporadic high priority tasks. This results in an asynchronous data transfer that can be accomplished with a constantly listening data sink or by means of a wake-up receiver as in our case.

To increase the reliability of the network and to guarantee sufficient power levels on each node, we present a strategy for energy management and preservation. We divide the system into a wireless sensor node (WSN) under test and the power management (PM) as shown in Fig. 2. The wireless sensor node comprises the µC, sensors and the radio. The PM consists of the energy harvester (not shown), energy storage, a dc/dc regulator and monitoring capabilities which are built-up on a modular platform, described in [9].

By using the monitoring capabilities of the PM the WSN-µC can decide which task needs to be postponed. In particular the decision is based on the amount of energy currently produced (input power, P_{in}) and the stored energy E_{store}. The additional PM-µC and the communication via UART1 is used to log the data in a convenient way. In a final deployed system the sensors attached to the PM will be read-out by the WSN-µC directly. The difference in current consumption (UART vs. I2C) is 40 µA and can be neglected due to the very short on time of <10 us per second.

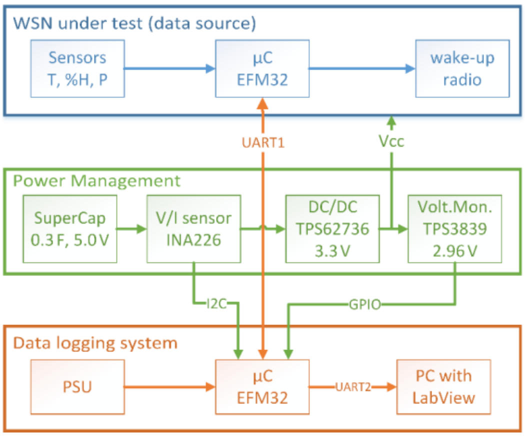


Fig. 2: Schematic drawings of wireless sensor node (WSN), power management and data logging system. Arrows indicate the communication between the different blocks.

3 EXPERIMENTAL ANALYSIS

This section introduces the various experimental setups that were used to analyse the concepts introduced in Section 2. At first, we investigate the performance of the proposed cross-layer routing protocol as introduced in Section 2, with respect to its latency and efficiency. Further we characterized the power consumption of the node. At the end of Section 3 we present a test setup where the duty cycle is based on the energy available and on asynchronous data transmissions.

3.1 Routing Protocol Performance

According to [10], the performance of any routing protocol can be evaluated by using different types of metrics, like route acquisition time t_{RA}, and the control-overhead ratio O_{CD}. The latter is defined in [10] as the ratio of control bits sent (CB_s) over data bits delivered (DB_D), that is $O_{CD} = CB_S/DB_D$. The route acquisition time t_{RA} is defined as the time required until a route is established after it was requested [10].

To test the performance of the proposed routing protocol we used a test setup similar to the topology presented in Fig. 1. Fig. 3 shows the setup consisting of three relay nodes, a source and a sink. Data was sent at a rate of 38.4 kbit/s. For the tests it is assumed that only neighbouring nodes are in wake-up range, for example the source can only wake up relay node 1. It is further assumed that all nodes are in communication range, which means that data may be transmitted directly between nodes. For example the source can transmit directly to the sink due to the superior communication radio range compared to the wake-up radio efficiency.

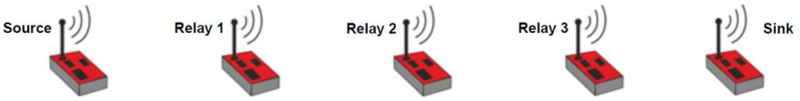


Fig. 3: Test setup consisting of source node, sink node and three relay nodes. Wake-up is only possible for neighbouring nodes, data transmission is possible directly from source to sink.

3.1.1 Route acquisition time

In our proposed algorithm we assume that the route is established after the node sends back the route request acknowledge. To measure the route acquisition time t_{RA} we send data from the source to relay-node 1, secondly from source to relay node 3 and finally from source to sink. Since only neighbouring nodes are in wake-up range, wake-up calls needs to be forwarded in second and third cases. Table 1 shows t_{RA} and the resulting cross data rate in kbits/s. It can be seen that t_{RA} equals 26 ms for single-hop communication, and t_{RA} = 33 ms in cases of forwarding wake-up packets. t_{RA} is required by the protocol to send wake-up calls and to perform the corresponding protocol handshakes. Due to the additional protocol overhead, the cross data rate decreases in case of multiple hops.

Table 1: t_{RA}: Time required to established a route for different numbers of hops

	single hop	three hops	four hops
t_{RA} in ms	26	92	125
Data rate in kbps	32.4	31.8	31.5

Fig. 4 shows on the left side the times required to wake up a one-, three- and four-hop distant node and subsequently send up to 16 kB data to it using the proposed protocol. Fig. 4 on the right side shows the number of hops plotted against the time required to wake up and subsequently send up to 16 kB data to one-, three- and four-hop distant nodes. Table 1 and Fig. 4 show the low latency of the protocol even when communicating to distant nodes.

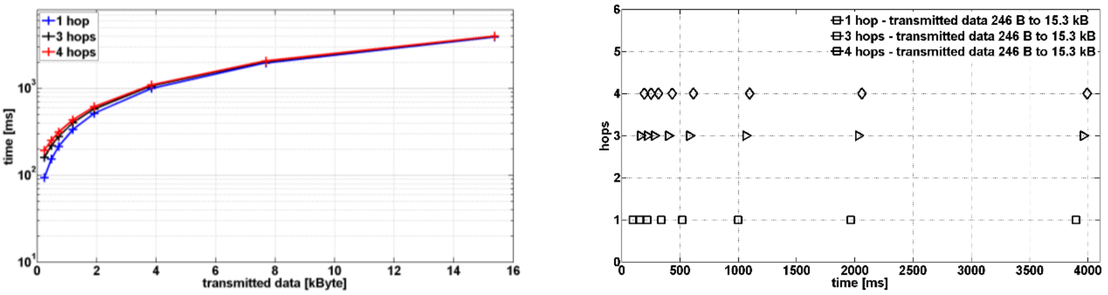


Fig. 4: (left) Time required to wake-up and sent data over one-, three- and four-hops. (right) time required to wake-up and sent data over one-, three- and four-hops.

3.1.2 *Control Overhead*

To determine the control-overhead ratio O_{CD} of the protocol we used the same test setup as mentioned above. We analysed the proposed cross-layer protocol with respect to protocol overhead which is directly related to the efficiency of the protocol.

Fig. 5 (left) shows O_{CD} over sent data-bytes when transmitting one data packet. It can be seen that in the beginning the overhead dominates due to the large amount of bytes required for the wake-up call (158 bytes). The red line shows the equilibrium between sent control-bytes and sent data-bytes, which is located at 180 bytes. Fitting the curve by an equation of the form $y(x) = b*x^m$ reveals the relation between data and control bytes. Here, b = 180 and m = -1 which means that sending one data packet requires 180 control bytes.

On the right side, Fig. 5 shows O_{CD} plotted against the number of sent packets, where one packet consists of 246 bytes. In this case O_{CD} can be fitted by using a function of the form $y(x) = a + b*x^m$, with a = 0,0285, b = 173 and m = -1, which means that the weight of the control bits decreased from 180 to 173 due to the fact that in-between data packets require almost no further control bits. The receiver sends a 3 byte long acknowledgement upon reception of a data packet and each data packet contains 4 byte routing information. Thus, with increasing number of data packets, O_{CD} tends asymptotically to 7 control bytes (O_{CD} = 0.03) which is indicated by the red dashed line in Fig. 5 right.

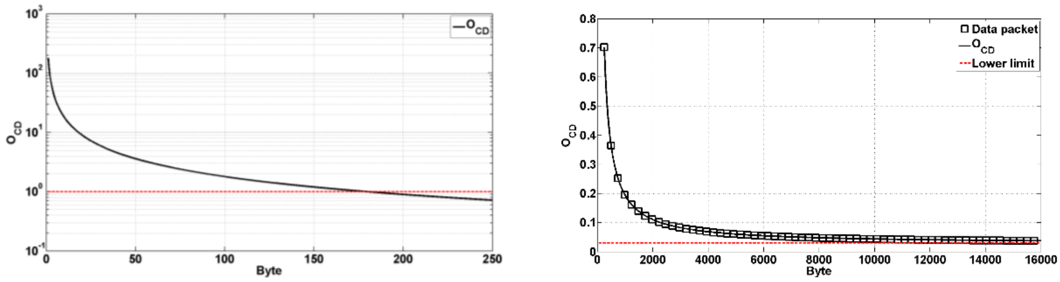


Fig. 5: O_{CD} versus number of transmitted bytes when sending one data packet (left) and up to 64 data packets (right). The red line on the left figure shows when O_{CD} = 1. On the right side, the red line indicates the theoretical minimum of O_{CD} using the proposed protocol.

From Fig. 5 it becomes clear that the routing protocol is more efficient and requires less energy per data byte, when sending larger data packets compared to small data packets. Sending of large packets can easily be achieved by accumulation of sensor data on the sensor node.

3.2 Energy Awareness

To evaluate the concept introduced in Section 2.3, we compare two setups. In the first setup (I) the duty cycle is fixed and calculated on a rough estimate based on the power available. In the second setup (II) the knowledge of P_{in} and E_{store} is used to skip tasks and thus adjust the duty cycle.

The scenario is the following: We assume a simple case where a sensor node measures regularly (every 10 s) data of its surrounding like humidity, air pressure and temperature very precisely with oversampling of the sensor. Further an alarm signal may be triggered when one of the values exceeds a threshold which is checked by a single-sample measurement every second. Both information are transmitted from the sensor node to a base station.

The highest priority for the system is that the storage has always a certain minimum energy level E_{min} which is needed to carry out the single-sample sensor reading. If there is excess energy available, the oversampled measurement can be carried out. Transmission of data requires most energy and consequently energy can be saved if several sensor readings are accumulated and transmitted in one larger data packet. The drawback is an increase of latency.

We simulate by experiment a complete energy black-out by charging the supercapacitor to 5 V and connect it to the wireless sensor node at t = 0 s. In literature supercapacitors are often suspected to have a high leakage current. In fact charge-redistribution effects with a time constant of several hours influence the terminal voltage [11]. To mitigate these non-idealities, the supercapacitor was charged for over one hour at 5 V. As a side effect, the effective capacity C_{eff} increases from 0.3 F to about 0.5 F. The usable energy in the voltage range from 5 V down to 3 V is calculated by $E_0 = \frac{1}{2} C_{\mathrm{eff}} \left(V_{\mathrm{high}}^2 - V_{\mathrm{low}}^2 \right)$ to 4 J.

Depending on the energy level of the storage, tasks with different energy requirements are executed by the wireless sensor node according to Table 2. The experimental results of both systems (I) and (II) are shown in Fig. 6.

Table 2: Overview of measurement and transmission tasks performed on the energy aware sensor node related to energy condition. Further the calculated average energy consumption and remaining runtime is shown.

State	Measurement every 670 ms	Transmission at …	Required energy level	Avg. energy consumption	Remaining runtime
3	oversampled	each meas.	> 2.0 J	22 mW	90 s
2	single	each meas.	> 1.0 J	6.5 mW	155 s
1	single	every 10th meas.	> 0.33 J	1.6 mW	420 s
0	single	(no Tx)	<= 0.33 J	106 µW	3800 s

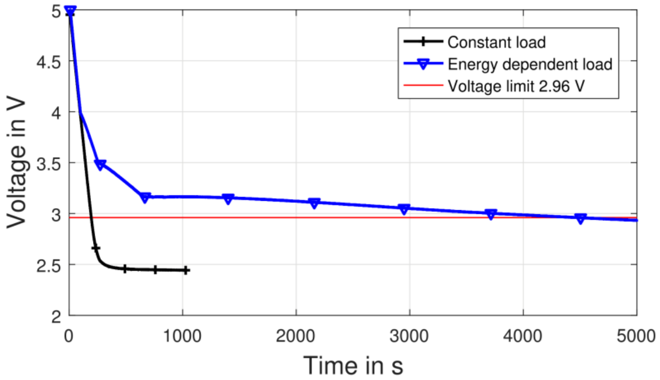


Fig. 6: Input voltage at the wireless sensor node plotted versus time. The black curve (crosses) shows case (I) where the sensor nodes performs a constant task and is unaware of its available energy. The blue curve (triangles) shows case (II) where the node adjusts its task to the available energy.

Further, the average energy in each period and the remaining runtime (based on E_0 = 4 J) for setup II is shown in Table 2. The energy for one cycle in state 3 and state 0 calculates to 14.7 mJ and 71 µJ respectively. These values are in good accordance (rel. error +5% and +1.4%) with the characterizations performed of the sensor using oversampling and single measurement modes, as shown in Fig. 7.

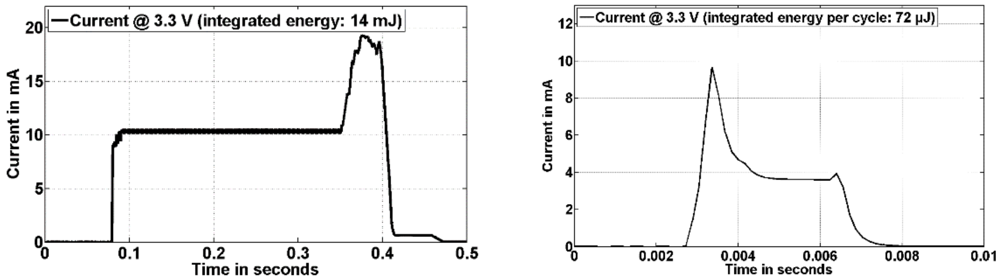


Fig. 7: (left) Current of the sensor in oversampling mode and data transmission (peak at the end). (right) Current of the sensor node without oversampling (no data transmission).

4 CONCLUSIONS

In this paper, we introduced a wireless sensor node that includes a wake-up receiver to realize low-power consumption and asynchronous communication capability. We presented and analysed a static and simple multi-hop wake-up routing protocol that significantly reduces the energy consumption compared to single-hop communication. Having a route acquisition time of approximately only 33 ms per node, the protocol exhibits low communication latencies even when using multiple wake-up calls. By analysing the protocol overhead ratio we demonstrated the efficiency of the cross-layer routing protocol especially for larger data packets. The second part of this work, presented a power management sub-system that creates energy awareness on the wireless sensor node. Two tests were carried out, to analyse the effect of adjusting the load in dependence on the energy available. During the tests we examined the lifetime with and without energy awareness. The results show that the energy aware node survives up to four times longer than the unaware node, although the sub-system itself requires additional energy.

REFERENCES

[1] Alcaraz, C., Lopez, J., Zhou, J., & Roman, R. (2011). Secure SCADA framework for the protection of energy control systems. Concurrency and Computation: Practice and Experience, 23(12), 1431-1442.

[2] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International journal of critical infrastructure protection, 8, 53-66.

[3] Shinozuka, M., Papakonstantinou, K. G., Torbol, M., & Kim, S. (2015). Real-time remote monitoring: the DuraMote platform and experiments towards future, advanced, large-scale SCADA systems. Structure and Infrastructure Engineering, 11(4), 588-603.

[4] Magno, M., Marinkovic, S., Brunelli, D., Popovici, E., O'Flynn, B., & Benini, L. (2012). Smart power unit with ultra low power radio trigger capabilities for wireless sensor networks. *2012 Design, Automation & Test in Europe Conference & Exhibition (DATE)*

[5] Oletic, D., Razov, T., & Bilas, V. (2011). Extending lifetime of battery operated wireless sensor node with DC-DC switching converter. In *Instrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE* (pp. 1–5).

[6] 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.

[7] Kumberg, T., Tannhaeuser, R., Gamm, G. U., & Reindl, L. M. (2014, June). Energy improved wake-up strategy for wireless sensor networks. In *Sensors and Measuring Systems 2014; 17. ITG/GMA Symposium; Proceedings of* (pp. 1-6). VDE.

[8] Kumberg, T., Tannhaeuser, R., Schink, M., Schneid, S., König, S., Schindelhauer, C., & Reindl, L. M. WIRELESS WAKE-UP SENSOR NETWORK FOR STRUCTURAL HEALTH MONITORING OF LARGE-SCALE HIGHWAY BRIDGES.

[9] Kokert, J., Beckedahl, T., Reindl, L.M., (2016). Development and Evaluation of a Modular Energy Management Construction Kit, Proceedings 18. GMA-ITG-Fachtagung, Nürnberg, Germany, 2016.

[10] Bansal, M., Rajput, R., & Gupta, G. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. The internet society.

[11] Merrett, G. V., & Weddell, A. S. (2012, June). Supercapacitor leakage in energy-harvesting sensor nodes: Fact or fiction?. In *Networked Sensing Systems (INSS), 2012 Ninth International Conference on* (pp. 1-5). IEEE.

CONCEPTS OF SENSOR SYSTEMS FOR OBJECT SECURITY AND ENTRANCE CONTROL AS WELL AS FOR DRONE DEFENCE

Roland Seibert[1] and Dr. Michael Groß[2]

[1] *roland.seibert@diehl-bgt-defence.de*
Diehl BGT Defence GmbH & Co. KG (DBD), Alte Nussdorferstr. 13, 88662 Überlingen (Germany)

[2] *michael.gross@diehl-bgt-defence.de*
Diehl BGT Defence GmbH & Co. KG (DBD), Alte Nussdorferstr. 13, 88662 Überlingen (Germany)

Abstract

On the basis of current samples, trials and studies, possible approaches for object security, entrance control for facilities and field camps (recognition, identification and tracking of persons) as well as for drone defence will be presented. The used sensor systems and concepts will be explained by selected samples of drone defence trials and a biometrical study dealing with person detection and face recognition on large distances (e.g. for field camp security). Possibilities, approaches as well as limits will be shown.

Keywords: Sensor systems, security concepts, face detection, entrance control, drones, drone defence

1 OBJECT SECURITY AND ENTRANCE CONTROL

1.1 Overview

Object security and entrance control for facilities and field camps require among system adapted sensors a sophisticated system concept taking into account not only the sensors and the algorithms but also the data processing capabilities, multi sensor systems, networking and other requirements.

In the case of object security and entrance control where persons are surveyed and re-recognized one must distinguish between scenarios on which one has to deal with cooperative persons (the person knows how to behave) and non-cooperative people (the person doesn't know who to behave, is not willing to do so and / or is part of a large group). Especially at public scenarios and non-cooperate persons one has also to distinguish between large and near distances between the person and the control station.

This paper covers the case of non-cooperate persons to be detected and identified at large distances. Examples are the observation of a market place, the entrance of an airport as well as a field camp with a long access path. Incoming persons must be detected and tracked by person detection algorithms as well as identified by face detection and recognition. The complexity of suitable sensors in combination with algorithms and processing will be illustrated.

During the R&D project "Biometrische Sensorik" [1] founded by WTD 91, GF 500/100 (3/2013 to 11/2015) under the lead of the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) in cooperation with Diehl BGT Defence (DBD), Videmo, Airbus Defence & Space (ADS) a demonstrator system was built up to acquire the requirements for the sensors as well as to demonstrate person detection and face recognition in real scenarios. The results and solutions covered herein, are based mainly on that study.

1.2 Sensor system selection

For identification of a person’s face detection algorithms are needed. To do face detection one need a high resolution on faces. At least the eye distance (one of the main classification properties) in the image must be greater than about 20-30 pixels. Different light situations especially in uncontrolled scenarios (day light dependent outside scenarios) must also be taken into account like different aspect angles and partly hidden areas of a face (e.g. using sun glasses or side views).

On the other hand, the requirement to observe a large area like a market place or airport areas requires a wide field of view for the sensors or a combination of several sensors working together to cover the wide field of view.

1.2.1 Considerations for camera selection

Cameras for person and face detection can work in different spectral ranges: visual (VIS), near infrared (NIR) and the thermal infrared (midwave IR, MWIR or longwave IR, LWIR). In general, the IR wavelength domain promise more robustness against light situations and changes compared to the visible waveband. The reason for this is, that VIS and NIR cameras need active illumination (natural or artificial) while on the other hand MWIR and LWIR use self-radiation of a warm object. On the other hand, SWIR cameras are capable to look through goggles or sun glasses.

Exemplary studies [1] were made using different camera systems. As can be seen in Figure 1, existing face detection algorithms work well in the VIS and NIR waveband while on the other hand they don’t work without special adaptations in the thermal wavebands. Also details disappear more and more in thermal spectral range which makes detections more difficult or nearly impossible.

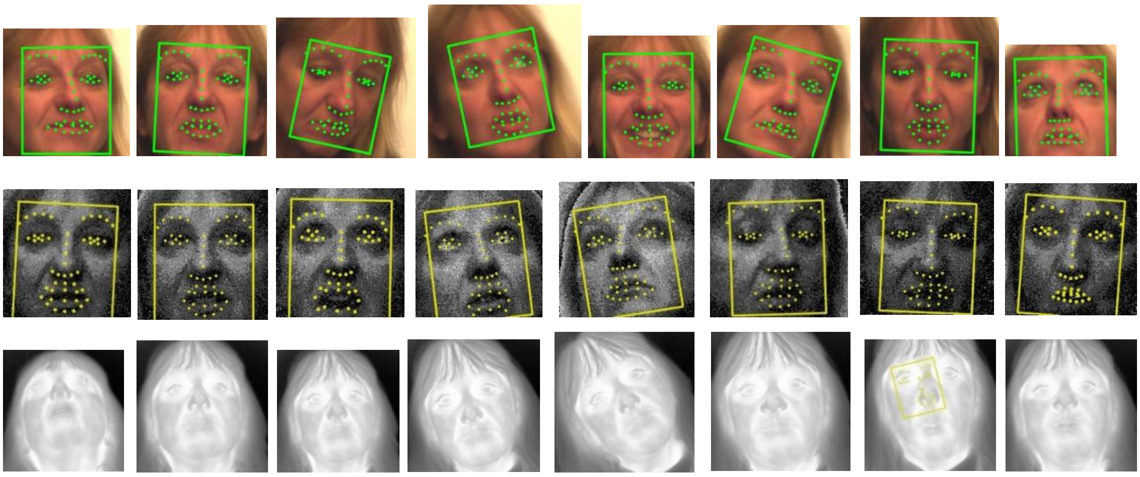


Figure 1: Face detection using visual, near infrared and thermal infrared cameras

Another aspect concerning the usage of NIR, MWIR and LWIR is the fact, that there is mostly no reference material available in order for compare infrared images of faces to the visual spectral range. So the assignment to known persons is difficult or not possible.

Actually only visible sensors are the favorite because they provide much details (in contrast to IR sensors were a face shows only little or no distinctive details), high resolution cameras are available and they are cheap compared to other types of sensors.

1.2.2 Optics and sensor size

To cover a wide field of view (FoV) using high resolution either multiple sensors with moderate number of pixels using small FoVs or one large sensor using wide FoV optics can be employed. Multiple sensors require not only multiple cameras (sensors and optics) but in most cases multiple processing units and internetworking between them. Therefore, the approach to use only one sensor seems to be attractive.

In the said project the professional RED EPIC Dragon 6k camera was chosen (see Figure 2). This camera uses a high resolution monochrome sensor consisting of 19,4 Mega Pixel. The currently used algorithms for person detection and face detection don’t need color information so the monochrome version is sufficient. So this guarantees best sharpness and resolution.

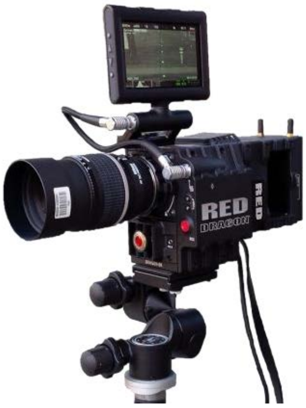


Figure 2: High resolution 6k camera - RED EPIC® Dragon – used in lab demonstration

The high pixel number of this camera type allows to use wide angle optics to cover the required FoV without losing resolution for details.

One of the main criteria for selection of the right optical system are in addition to the resolution, the depth of field and the horizontal field of view. These requirements disagree partially. Face detection and recognition need a good sharpness, whereas the requirement at wide field applications is the area in depth.

Actually the usage of a focal length of 135 mm at $f^{\#}$ 8 and an object distance of about 20 m leads to a depth of field of about 8 m and a horizontal FoV of about 5 m. This is suitable for surveillance of some smaller entrance areas (e.g. escalator access) but not for larger public places.

An additional aspect is the position of the camera. To detect faces, the camera look direction has to be flat horizontal. On top views, faces can’t be seen normally. This leads in addition to the depth of field problematic to occlusions.

1.3 Signal processing

In the said project [1] a client server architecture between camera and signal processing system was used for the demonstrator. Camera data is transferred via TCP/IP to the signal processing. This allows the most flexibility in the design and architecture of the system as well as for load distribution. Standard face detection and recognition algorithms developed by the company Videmo [2] are used in addition with person detection and tracking algorithms developed by Fraunhofer IOSB.

The algorithms work very well. The main challenge here is the enormous data rate to process. For the currently chosen camera system (37 MB per frame) the nominal data rate would be about 7,4 GBit/sec for a 25 Hz framerate. This is nearly impossible to process using standard available components of the stock. Also recording and replay, storing capacities are complex and costly, therefore one need specialized solutions out of commercial stock. Low cost solutions don't exist.

The currently build up demonstrator consists of a server computer controlling the camera, providing image data by TCP/IP and providing record and replay functions. An additional client computer (modern i7 or XEON multicore) acts as the signal processing unit running the face detection and recognition algorithms by Videmo as well as the person detection, tracking and fusion algorithms by IOSB. Everything integrated in one user interface developed by DBD. With this configuration a frame rate of only about 1 Hz could be realized. Possible solutions for future optimization of the processing performance were identified.

The following sample (Figure 3) shows a screen shot of the demonstrator system.

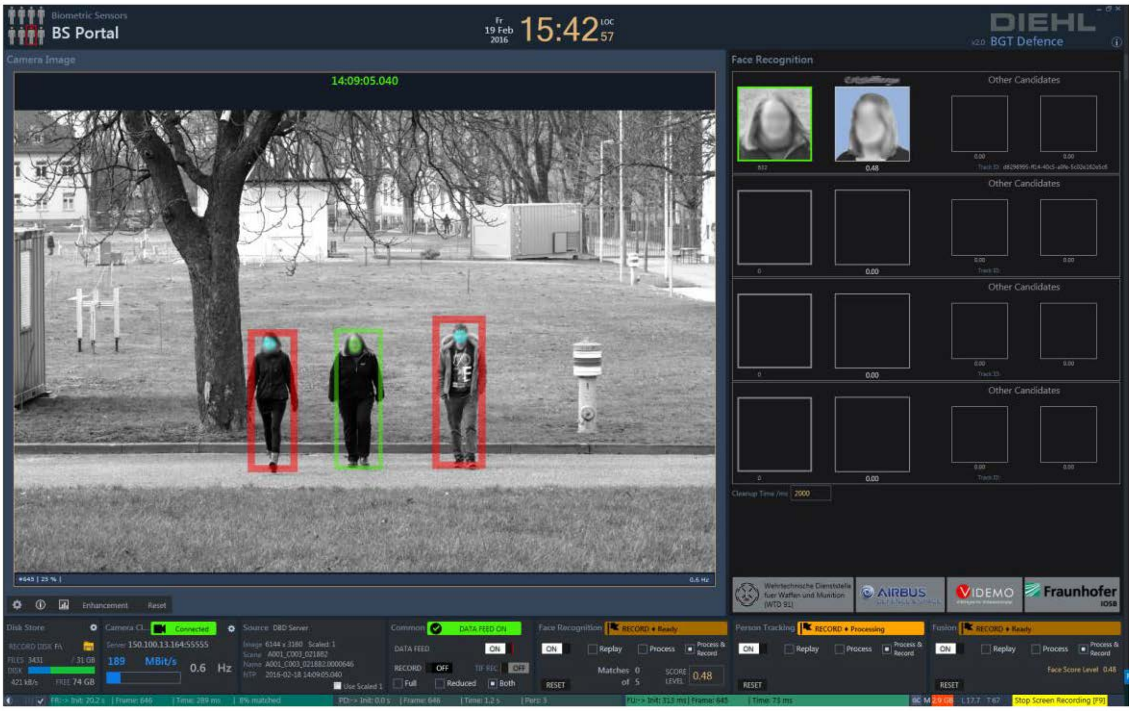


Figure 3: Screen sample of person & face detection in a graphical user interface

Three incoming persons were detected and tracked while one person could be identified by face detection and recognition (green).

1.4 Conclusion

Security applications for object security and entrance control especially for large areas and at great distances require a very well selected sensor concept in combination with high performance computing and infra structure.

The processing and display of extremely large images requires in terms of data transfer, preprocessing and algorithmics an extremely efficient infrastructure (network, hard drives, etc.) and hardware (computing capacity).

One solution could be to split the sensor into several small commercial ones (smaller sensor size and therefore smaller FoV) each supplied by one computational unit. The algorithms in conjunction with each other and with the user interface should be optimised using lossless image compression and perhaps specialized preprocessing FPGAs (Field Programmable Gate Arrays). Such a solution would be modular adaptive to the actual requirement and cost effective. Other applications like using action cams for mobile security personal could then be easily adapted.

2 SECURITY-SENSOR ASPECTS IN µ-DRONE THREAT-SCENARIOS

Small UAVs often classified as LSS (Low-Slow-Small) are more and more discerned as potential threat in civil and military security relevant scenarios.

Small drones especially multicopter types are characterized by specific flight qualities which make them sometimes spontaneous with respect to their appearance and therefore time critical for detection. Low signatures in all spectral bands and similarity to natural objects in the environment e.g. birds usually complicate the object detection or - more precise - the classification process.

With respect to an assumed defence action in threat scenarios with µ-drones a positive recognition or identification of the drone is required before defence measures are to be initiated. Thus the sensor to shooter process is in either case time sensitive which increases the demands on the acquisition sensor system.

Typical flight performances of small drones in terms of speed and manoeuvrability also lead to time sensitive detection and defence measures, and low signatures of these drones in real background clutter will generally cause difficult detection conditions. Even multicopter drones can approach close to the ground exploiting masking by terrain or ground objects like forest ore buildings. Thus their exposition will often be spontaneously and in proximity to the area to be defended. The task of detection has then to be performed without delay and high reliability.

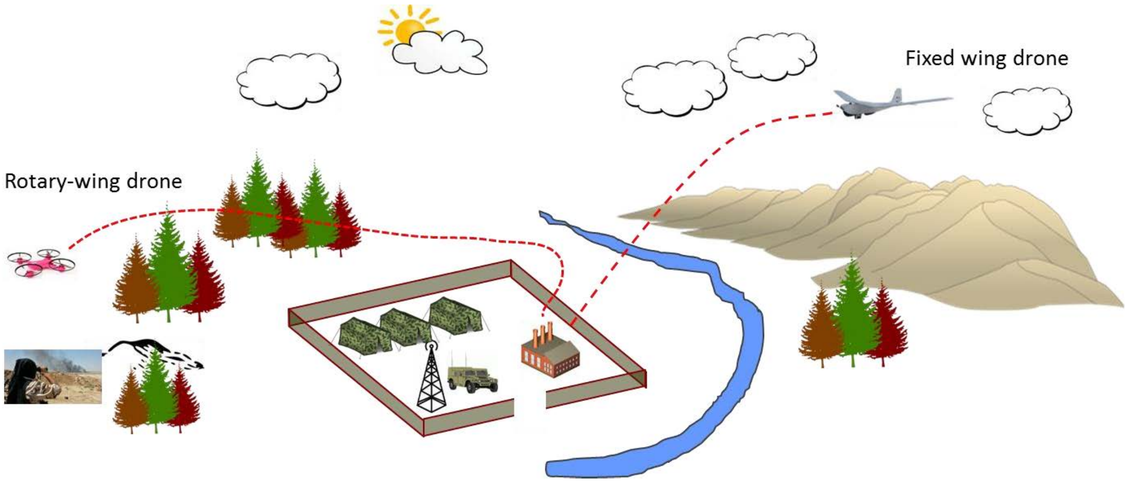


Figure 4: Typical drone scenario

Due to environmental clutter conditions the sensor system should work with multiple sensor principles i.e. complementary extracting the major features which characterize a small drone.

LSS-drones are characterized by their HF-Emission, Infrared and visible signature, acoustic signature, Radar-Backscattering and motion features.

In real scenarios every one of the afore mentioned features can but must not appear simultaneously, making a multisensory approach with data fusion more reliable as a single sensor system.

One of the primary sensor in a multisensory network could be an optronic sensor system comprising a imaging sensor in the infrared and visible spectral band. This is due to the necessity of an imaging technique for object recognition and identification.

Simultaneously the imaging sensors can cover a large surveillance sector in azimuth (at least 360 degree) and elevation (up to 80 degree) with high resolution and required sampling rate (> 10 Hz). Figure 5 shows examples of the infrared signature of small drones recorded with a high resolution optronical tracking system after primary detection.

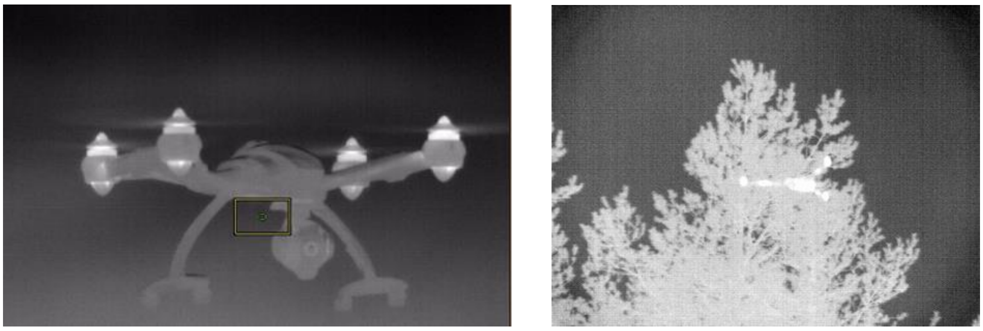


Figure 5: High resolution Infrared image of LSS drones with and without background clutter

The primary optronical sensor is usually a wide angular range covering surveillance sensor with high spatial resolution. Reasonably it comprises a multi-camera system working in a longwave infrared and a visual spectral band simultaneously in order to analyse heat and color features (signature) as well as motion behaviour.

Wide area surveillance can be realized with either sector-scanner or monolithic panoramic sensors. The first type has the advantage that the singe sector sensors can be placed at strategic points in the area where obscuration by terrain or foreground objects are negligible. The sensors work together in a network at which each of them provides own processing capacity for independent reconnaissance and alarming. Surveillance results and alarm indications are transmitted to the central control centre for further coordination and threat evaluation.

To work with distributed sensors has advantages even in the case of protecting larger areas as e.g. military camps, airports, congress hotel districts and others. Due to the limited Acquisition range of optronical surveillance sensors (500 m) and the blind angle problem of distributed sensors, each of the sub-sensors must cover a larger angular field-of-regard (compare Figure 6).

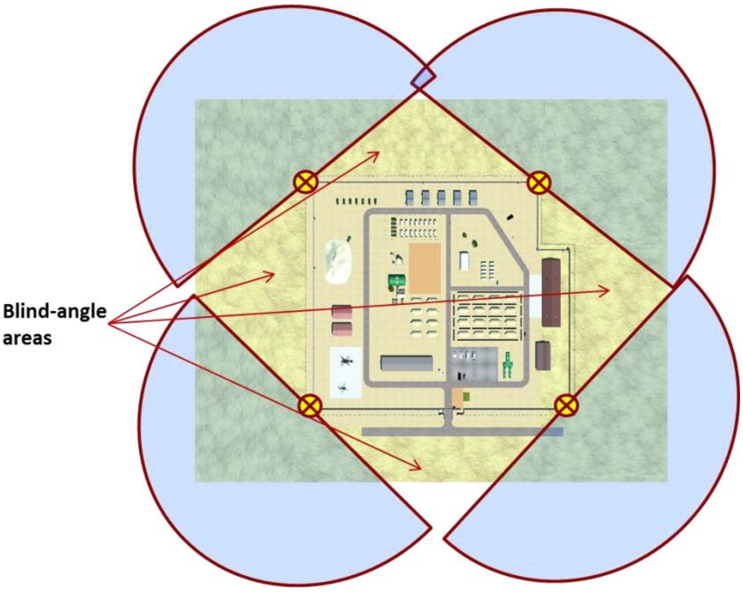


Figure 6: Example of a 360° coverage of a camp with 4 wide angle surveillance sensors

The angular coverage regarding elevation is also critical. Due to actual flight performances even of rotary wing drones which can achieve altitudes of up to 3000 m and more a surveillance sensor system must secure at least the entire hemisphere.

All these requirements lead to a sensor system with extremely demanding layout with respect to pixel format and frame rate. Nevertheless, these types of sensors can technically be realized with independent multi-camera devices with inherent image-processing capability.

Such devices were approved last year during a security mission for an international meeting of politicians in the south of Germany as well as during own company trials and at trials in cooperation with BAAINBw (Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr).

REFERENCES

[1] Hübner, W. Dr. rer. nat. (2015). *Final Report „F&E Studie Biometrische Sensorik“* for the R&D project of WTD 91 – 500/100, Contract E/E 91 S/CC031/CF186, Fraunhofer IOSB, OBJ 2015/07

[2] Videmo Intelligente Videoanalyse GmbH & Co. KG, Web: www.videmo.de, Karlsruhe (Germany)

ACXIS – AUTOMATED COMPARISON OF X-RAY IMAGES FOR CARGO SCANNING

Alexander Flisch[1], Thomas Lüthi[2], Mathieu Plamondon[3], Stefan Hartmann[4], Wicher Visser[5], Adrian Schwaninger[6], Diana Hardmeier[7], Marius Costin[8], Caroline Vienne[9], Frank Sukowski[10], Ulf Haßler[11], Irène Dorion[12], Andrea Canonica[13], Eric Rochat[14], Ger Koomen[15], Micha Slegt[16]

[1] alexander.flisch@empa.ch, [2] thomas.luethi@empa.ch,
[3]mathieu.plamondon@empa.ch, [4]stefan.hartmann@empa.ch
EMPA. Swiss Federal Laboratories for Materials Science and Technology, Center for X-ray Analytics, Überlandstrasse 129, 8600 Dübendorf (Switzerland)

[5] wicher.visser@casra.ch, [6]adrian.schwaninger@casra.ch, [7]diana.hardmeier@casra.ch
Center of Adaptive Security Research and Applications (CASRA),
Thurgauerstrasse 39, 8050 Zürich (Switzerland)

[8] marius.costin@cea.fr, [9] caroline.vienne@cea.fr
CEA LIST, Department of Imaging & Simulation for Non-Destructive Testing,
91191 Gif sur Yvette (France)

[10] frank.sukowski@iis.fraunhofer.de, [11] ulf.hassler@iis.fraunhofer.de
Fraunhofer Institute for Integrated Circuits IIS, Development Center for X-ray Technology EZRT, Flugplatzstrasse 75, 90768 Fürth (Germany)

[12] irene.dorion@smithsdetection.com
Smiths Heimann S.A.S. (SH), 36, rue Charles Heller, 94405 Vitry sur Seine (France)

[13] andrea.canonica@ezv.admin.ch, [14] eric.rochat@ezv.admin.ch
Swiss federal Customs Administration (FCA), Montbijoustrasse 40, 3003 Bern (Switzerland)

[15] gcm.koomen@belastingsdienst.nl, [16] m.slegt@belastingsdienst.nl
Dutch Tax and Customs Administration, Dutch Customs Laboratory (DTCA),
PO Box 3070, 6401 DN Heerlen (Netherlands)

Abstract

The ongoing FP7 project “ACXIS - Automated Comparison of X-ray Images for cargo Scanning” delivers enhanced inspection procedures for customs. A manufacturer independent reference data base for X-ray images of illegal and legitimate cargo is developed. One of the X-ray image recording work flow is to use 3D-CT data of illegal cargo mockups and to artificially generate arbitrary X-ray projections. By merging these X-ray projections and radiographic images of cargo freight containers with legitimate goods a high number of reference images can be obtained in a very efficient way. Based on these images an analysis system is developed consisting of image pre-processing methods as well as automated target recognition (ATR) algorithms supporting the inspection officer by identifying threat items automatically and highlighting them in the X-ray image.

Keywords: Cargo screening, ATR, X-ray, imaging, image processing,

1 INTRODUCTION

Government and citizens expect the customs authorities both to impede the import of goods that endanger public safety and to prevent import tax evasion [1],[2]. The predicament of the customs administrations will soon be aggravated by both the increase of global trade and the trend towards 100% screening [3]. Therefore, a significant increase of the cargo inspection capabilities is essential for Europe to keep its position in the global trading and transportation network. It is therefore a goal to develop new inspection concepts to enable faster cargo handling at customs.

A viable solution for more efficient and effective cargo screening is an automated analysis system for the X-ray images supporting the inspection officer with automated illegal cargo and threat detection. To implement the adjustability on the local context as well as the activities to fight organised crime, a data base system has to be established in which X-ray images and meta-information of both historic detection and mock-up cargo are stored and exchanged between customs organisations. Given the variety of systems currently installed at European customs offices, the new automated detection system improves the current detection capabilities if it operates manufacturer-independently and provides a reliable detection for different scanner types and application fields.

Different scenarios for the support of the inspection officer are conceivable. First, images of historic detections based on the cargo declaration are displayed alongside the current cargo image to facilitate a direct comparison. Second, the system automatically analyses the image and highlights in the image presented to the inspection officer regions of interest where a closer inspection is required. Third, in a future development step, the system will independently inspect uncritical cargo, i.e. empty containers, and forward the inspection task to a human operator only in case of ambiguous results. Current training consists in the identification of a small set of critical cargo elements superimposed on historic images of the inspection system. A drawback of this system is the adaption of the inspection officer to the small set of training images that are usually limited due to factors like confidentiality of the image data. The set of training images is significantly enhanced if artificial cargo image can be generated with arbitrary positioning of objects in the image data base.

In this project, a risk analysis will be conducted in close collaboration between end users (customs organizations), scientists and security experts in order to define threats to be detected in different cargo screening scenarios. A large and representative data base containing cargo X-ray images will be developed. Modern image and signal processing algorithms will be applied and further developed for automated detection of threats in X-ray images using different signatures based on material, structure and shape information. Applied visual cognition research will be used to identify how expert screeners recognize threats in order to further enhance automated detection and screener assist technology. The highly innovative system will be implemented using a simulator to be used in the field by end users in order to ensure operational relevance, practical evaluation and further refinement of the system.

2 IMPROVED INSPECTION PROCEDURES

In the scope of ACXIS, automated target recognition (ATR) functions are developed to analyse images issued from X-ray scans of cargo shipments inspected at land, air or sea border crossing points. With the new procedures proposed by the ACXIS project, the Customs officers will carry out the inspection helped by ATR functions available on-demand. They will be able to annotate the results and to share them with other agencies through a secure system. The X-ray data will be converted into a standardized format and stored in a database along with the results of the ATRs and other annotations (Figure 1). This standardization allows comparison between scans from X-ray machines of different manufacturers and models. The database is loaded with a large array of reference material and new scans are continuously integrated.

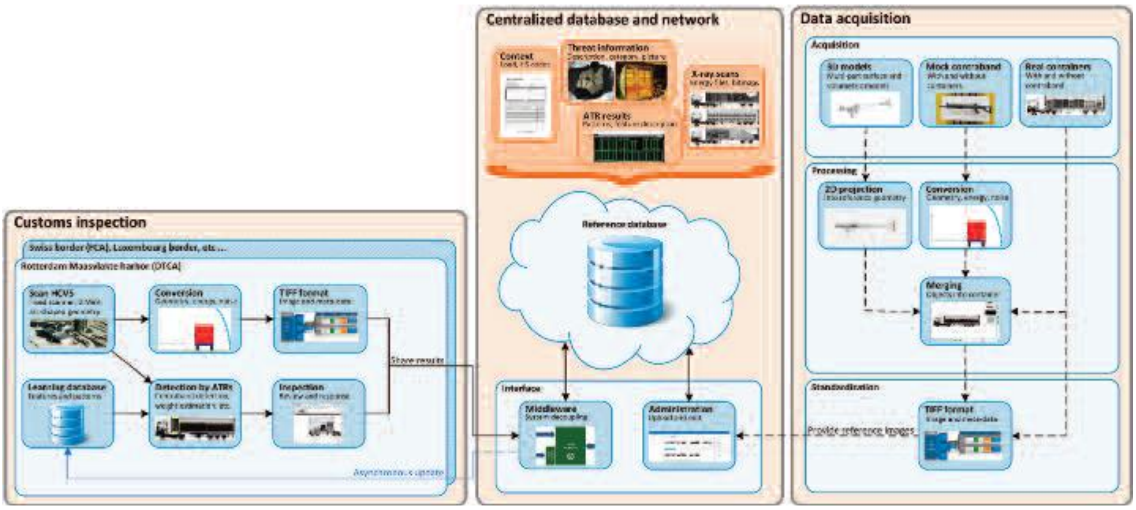


Figure 1: X-ray inspection procedure for border controls with automated target recognition functions based on a centralized database

3 REFERENCE DATABASE

Based on risk analysis conducted by the Customs administrations, threat objects and their locations in the container were identified. Following their recommendations, a set of mock-ups was created with real threat items and simulants, combined with common goods (Figure 2).

These were scanned using laboratory systems, and some with a cargo scanner, chosen as reference. The main objective of these mock-up scans was to enlarge the variety of threat images. For the same purpose, simulation tools were also used in order to generate X-ray images from 3D models of various types of threat items (e.g. weapons).

Between all classes of threats, few more details are given on two items. Tobacco products are principally legal, but with a fairly high taxation on them. Therefore it can be interesting to bring untaxed cigarettes in large amounts to the black market. Due to the relatively low density, the cigarettes themselves are hardly visible behind more massive materials; however, their packaging has a certain texture that can be detected. Another class of risk items if the shielding containers of radioactive Gamma-ray sources, used generally in the field of non-destructive testing (NDT). The transport of such containers is legal, but needs an adequately equipped and identified vehicle as well as specially trained drivers. The heavy shielding necessary for such sources is made from lead or depleted uranium and therefore, creates opaque regions on the X-ray image because of the high attenuation of the beam. These areas are visually analyzed, but automatic algorithms could also be employed.

All the images from the database and especially the ones containing threat items will provide a large basis for training of screening officers and also for machine learning methods in automated detection algorithms.

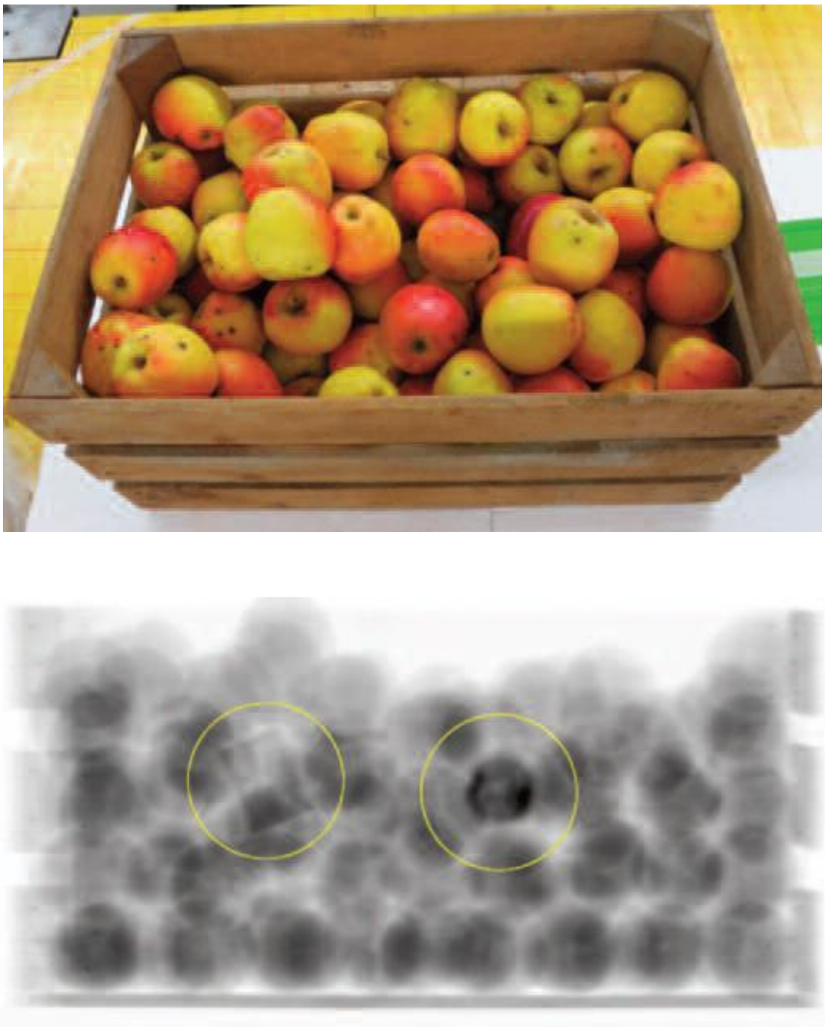


Figure 2: Example of images containing threats. Plastex and hand grenade hidden between apples. Photo (top) and X-ray image (bottom)

4 IMAGE UNIFICATION

When analysing X-ray images, the human brain easily adapts to other different systems, regardless the possible geometric deformations, various textures and different levels of contrast or noise, which is not the case for automatic algorithms. Since a large variety of X-ray scanners are installed at border checkpoints, the analysed images need to be similar in terms of the aforementioned parameters. Standardising these images is a preparation step and is mandatory for good detection performances.

Physical processes involved in digital X-ray imaging were studied and accurate models were developed in order to take into account the differences between the various X-ray scanners. Geometric adaption is perhaps the most challenging since projecting a complex load from distant view angles generates different distortions in the resulting image. However, an approach which selects the most similar ray paths and makes use of the standardised container dimensions gives satisfactory conversion results as shown in Figure 3. The example shows a conversion of a Euromax image (top) to a SH-HCVS image appearance (middle) that looks very similar to a genuinely obtained SH-HCVS image (bottom).

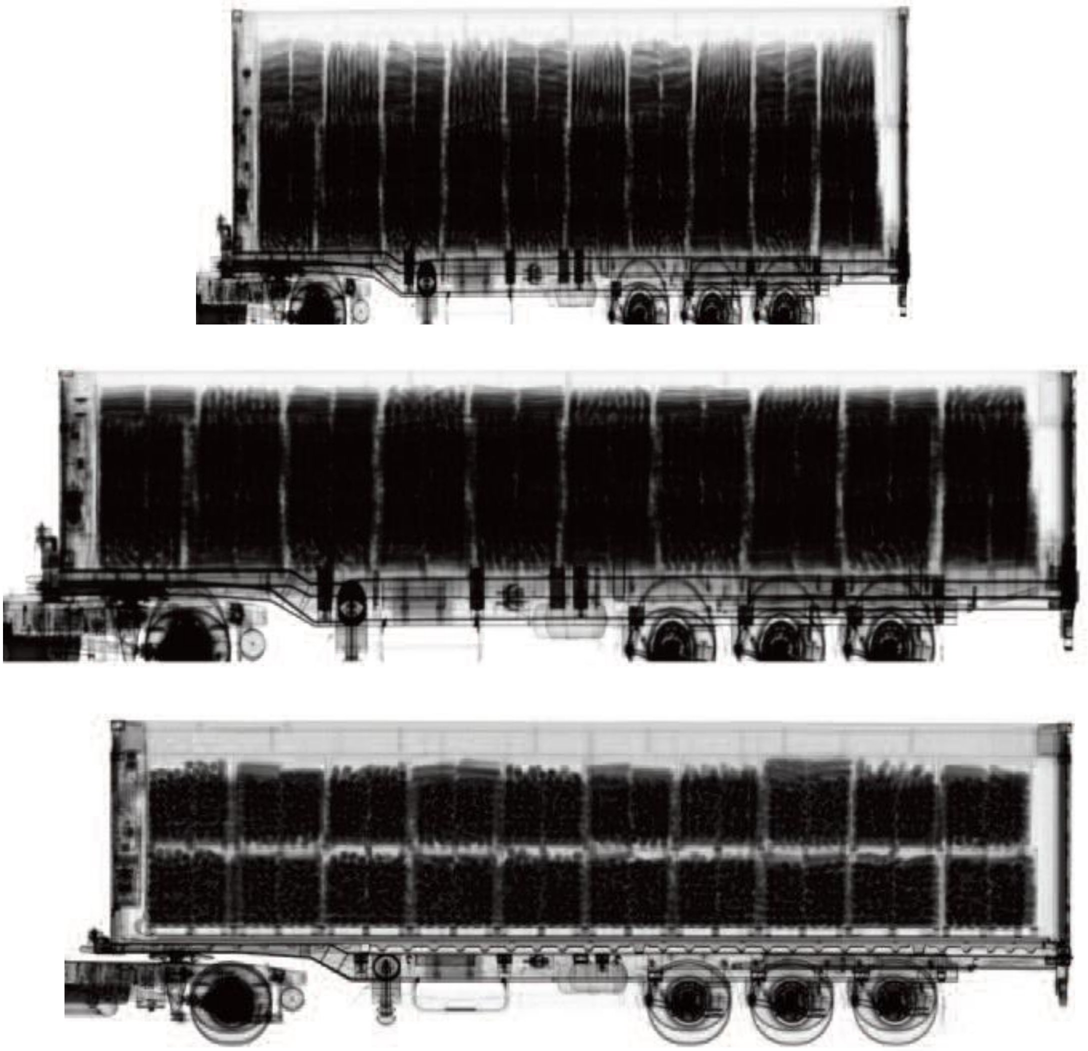


Figure 3: Real container scan with Euromax (top) and SH-HCVS (bottom) scanners. The Euromax scan was converted to the SH-HCVS format (middle)

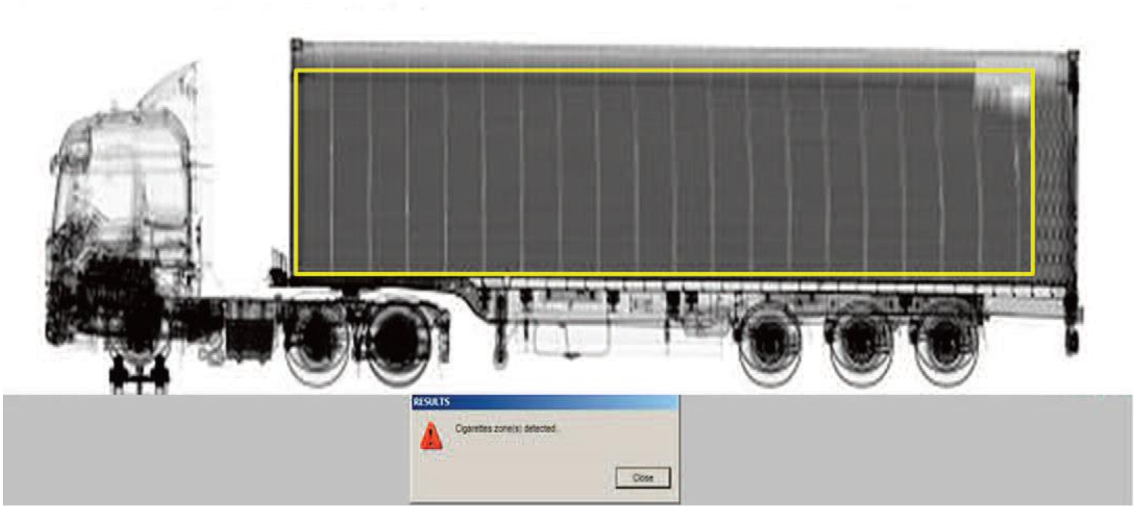
Contrast corrections take into account the source spectra and typical phantoms are used to estimate several attenuation points, which are then fitted in order to use the obtained curves for adjustments of grey level values. Several noise reduction algorithms [4],[5],[6],[7] were evaluated in order to select the best one to reduce the noise to the level of the reference scanner, without affecting the image quality (e.g. the texture of the sharpness).

5 AUTOMATED TARGET RECOGNITION

The ultimate goal is to provide assisted / automated detection techniques of threats through dedicated algorithms. Several illicit goods detection scenarios were selected and prioritized. Several approaches of complementary assisted / automated detection techniques have been investigated according to the various envisioned scenarios, such as image comparison, load characterization and direct target recognition.

5.1 Automated Detection of Cigarettes

Methods for cigarettes detection based on texture analysis are being developed and show promising results. For instance the load in Figure 4 is automatically identified as cigarettes packs and a warning is displayed to the screening officer.



Cigarettes zone(s) detected.

Figure 4: Example of automated detection of cigarettes

5.2 Weight Estimation

A tool to help the operators to analyze the load of a cargo container is the weight estimation. In the process of analyzing the load, it is often helpful to match areas on the X-ray image of the load with the goods marked on the waybill. This software tool will give an indication of the actual weight to be compared with the declarations, as shown in Figure 5

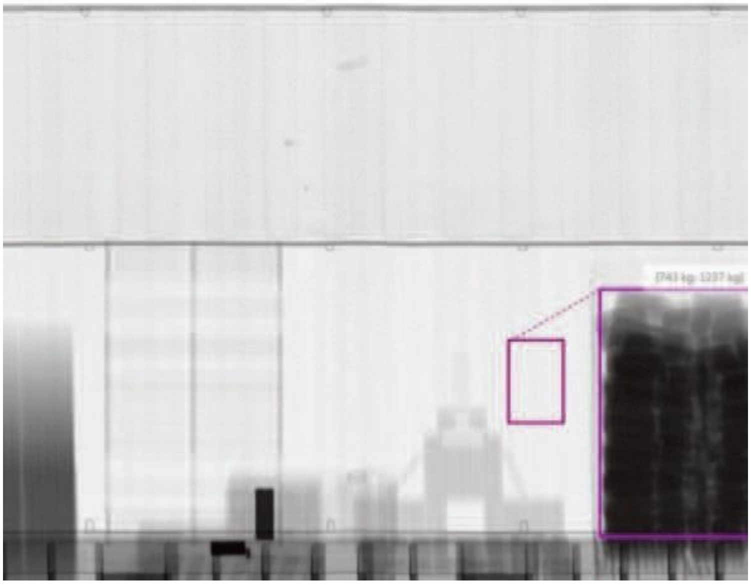


Figure 5: Tool for weight estimation of loads in a cargo container

5.3 Image Irregularity Detection

Instead of searching to detect specific threats which might be missed because of their large variety, a very helpful approach is to detect irregularities. A tool has been developed which will point out areas showing irregularities which will then be analysed in detail by the screening officer. Through advanced image processing algorithms employing registration techniques, a difference image with respect to a reference will give indications of irregularities, a indicated in Figure 6.

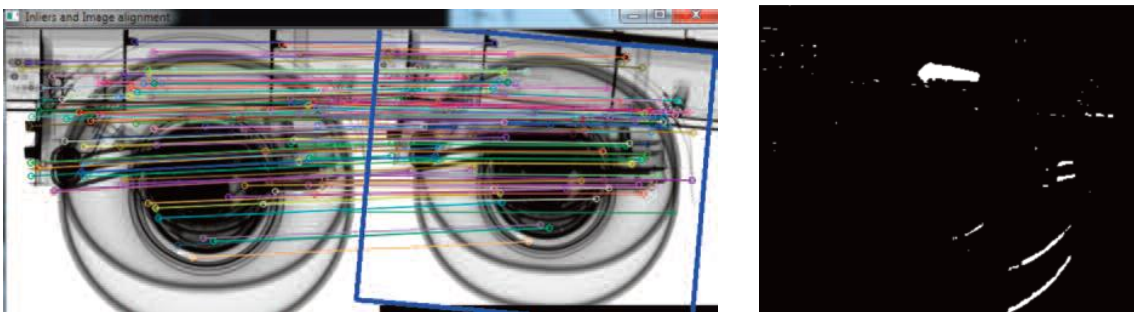


Figure 6: Automatic detection of an irregularity by comparison with reference image: registration process and indication on a difference image

6 TRAINING THE CUSTOMS OFFICERS AND VALIDATION

A software application is developed to provide focused training on X-ray image interpretation and decision making, and to periodically evaluate the performance of Customs officers (Figure 7). The user interface is carefully designed to resemble various X-ray scanning systems, and includes the most important support functions, such as zooming, image filters and enhancements. The behaviour of the ATR functions are simulated with the placement of coloured frames in the image that indicate the possible existence of suspicious goods. The user receives feedback upon making decision whether the cargo should be subject to further inspection, informing him whether his answer was correct and which suspicious goods are part of the cargo.

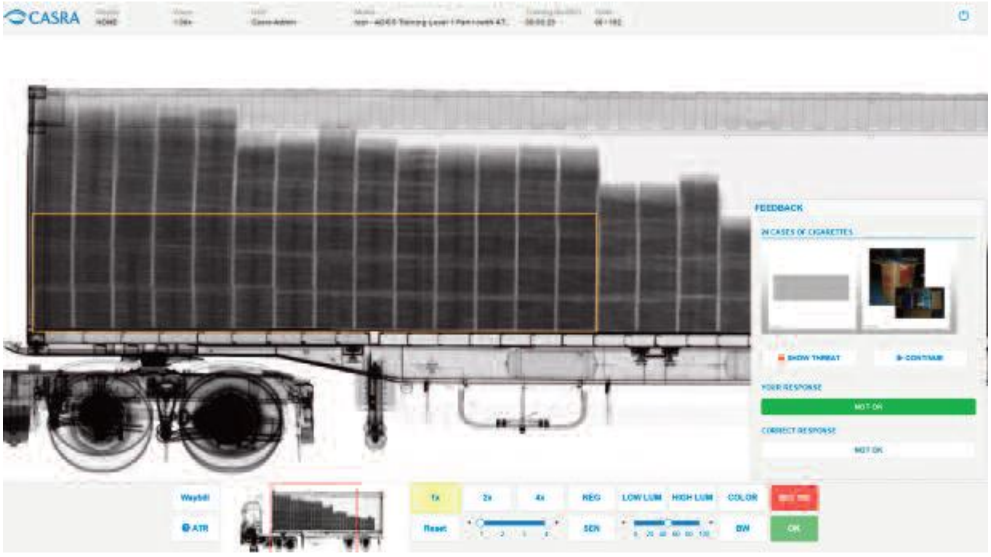


Figure 7: Educating the experts: training with the simulator

The impact of the ATRs on the performance of Customs officers is evaluated through a validation study. A group of operators is selected for training during which they are presented with simulations of X-ray scans of shipments that are annotated with the detection results of the ATRs. The performance of these participants are compared against a control group.

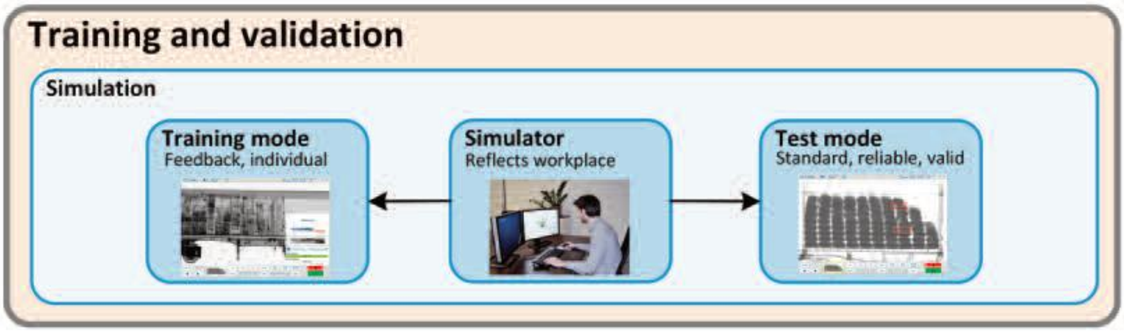


Figure 8: The simulation software provides X-ray interpretation training and tests for customs officers

Training and test modules have been developed for the simulation software (Figure 8). The training modules automatically adjust the training difficulty to the level of expertise of the user. Supervised learning is guaranteed by providing the user with feedback after each image. The test modules are standardized packages that enable reliable and valid means to carry out initial and recurrent evaluation of Customs officers. These methodologies are rooted in behavioral psychology and have been applied to airport security personnel for many years with great success [8], [9].

REFERENCES

[1] Customs in the 21st Century; Enhancing Growth and Development through Trade Facilitation and Border Security, Annex II to Doc. SC0090E1a, World Customs Organization, 2008.

[2] Article 2 “Mission of customs authorities”, Regulation (EC) No 450/2008 of the European Parliament and of the Council

[3] G. Chen, P. Bjorkholm, T. R. Fox, Z. Wilson, X. Bonsergent (2009), *X-Ray Cargo Inspecion: Status and Trends,* AIP Conf. Proc. 1099, 570-573

[4] Guidotti, Patrick (2009). *Some Anisotropic Diffusions.* University of California. Irvine, CA 92697

[5] Rudin et al. (1992). *Nonlinear total variation based noise removal algorithms.* Santa Monica, CA 90405, USA, S. 259-268

[6] Dabov et al. (2006). *Image denoising with block-matching and 3D filtering.* San Jose, California, USA

[7] Buades et al. (2011), *Non-Local Means Denoising*

[8] D. Hardmeier, A. Schwaninger (2008), *Visual cognition abilities in X-ray screening.* Proceedings of the 3rd International Conference on Research in Air Transportation, ICRAT 2008, Fairfax, Virginia, USA, 311-316

[9] A. Schwaninger, A. Bolfing, T. Halbherr, S. Helman, A. Belyavin, L. Hay (2008), *The impact of image based factors and training on threat detection performance in X-ray screening.* Proceedings of the 3rd International Conference on Research in Air Transportation, ICRAT 2008, Fairfax, Virginia, USA, 317-324

ACKNOWLEDGEMENTS

The project AXCIS – Automated comparison of X-ray images for cargo scanning was funded by European Union under the 7th Framework Programme

IMPROVING ROBUSTNESS FOR SEVERE WEATHER CONDITIONS IN AIRPORT ENVIRONMENTS BY PROCESS MONITORING AND COMMON SITUATIONAL AWARENESS

Arne Schwarze

arne.schwarze@fkie.fraunhofer.de
Fraunhofer Institute for Communication, Information Processing and Ergonomics,
Fraunhoferstr. 20, 53343 Wachtberg (Germany)

Abstract

Prevention of critical situations is very much about monitoring different parameters, aggregating information to higher class situation assessment and starting the right measures at an early point in time – maybe under stressful conditions. Technical systems can support users in complex process environments and thus can be a key factor in establishing robustness against external influences. To support decision makers in such environments, knowledge about their process responsibilities and information needs is essential. If one has deep knowledge about the processes, their interdependencies, their critical resources and the responsible actors, it is possible to establish a process monitoring and common situational awareness. The Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) developed a software tool to enable this for airports, especially for severe weather in winter.

Keywords: airport operations, crisis management, early warning, process monitoring, situational awareness, winter services

1 INTRODUCTION

Airports comprise a complex process landscape with various operation centres (airport operator, air traffic control, airlines, etc.). Detection of precarious developments is difficult, as each operation centre only knows some fragments of the whole situation picture. Making things worse, external factors like weather conditions, air traffic flow and capacity of nearby airports have high impact on airport operations. One widely known example are the volcanic activities in Iceland in March and April 2010 that led to reduced airspace capacity and thus to airplanes without permission for lift-off as well as redirected incoming aircrafts that originally were planned for other destinations.

Especially winter operations during bad weather conditions are challenging for airports as they have to deal with reduced capacity, scarce resources and delayed flights as well as they have to ensure the de-icing of airport surfaces and airplanes.

A common operation picture of airport processes enables acting in advance by predicting possible bottlenecks. In particular when high workload scenarios occur, an intelligent assistance system takes workload from the users and supports them in fulfilling their key tasks.

2 PROJECT SETTING AND COURSE OF ACTION

The solution described in this paper was developed and tested at Cologne Bonn Airport (CGN), where operation runs day and night (“24/7”). There are established processes and systems that build the pre-setting of the optimisation efforts. To take this into account, the following basic principles for project execution were formulated:

- No existing systems will be substituted.

- Only processes that are in scope of the project are optimized. Process out of project scope will not be touched.
- Dependencies and interfaces to other processes will not be changed. This also means that communication connections from/to processes that are out of scope stay the same (e.g. digital form send via email).

The scope of the project was defined as supporting winter services operation, which is responsible for minimising the negative impact of the weather situation on airport operations.

2.1 Project setting

Winter services operation is a critical success factor for airport operation during winter conditions. Negative impacts of winter conditions are:

- Air traffic network may have reduced capacity, which results in delayed or diverted flights. The impact on airport operation is reduced predictability of required resources which results in decreasing ability of planning staff and resource allocation to processes.
- Nearby airports may have limited capacity or even have interrupted their operation, which also results in diverted flights.
- Local capacity may be reduced as airport infrastructure is impacted by weather influences, for example runway capacity maybe reduced as snow removal requires temporal interruption of runway usage.
- Additional tasks are required, for example de-icing of airplanes, continuous monitoring of weather development, additional communication for coordination with other stakeholders (air traffic control, airline, ground handler, etc.). This results in increasing workload for airport employees.
- Other stakeholders at the airport (control tower operator, airline, ground handler, etc.) also suffer from additional workload and reduced predictability. This leads again to less predictability for the airport as well as more communication overhead.

Factors like air traffic network capacity, other airports capacity the local weather development cannot be influenced by the airport. So the possibilities for local mitigation of influences by bad weather situations are limited. Nevertheless improving these possibilities could result optimisation of resource allocation und thereby in less impact of the external factors on airport operations. The negative impacts listed above already show two starting points for improvement: targeted distribution of relevant information to stakeholders (reduction of communication overhead) and predictability. Both require an overview of the current situation.

2.1.1 Scope of support for winter services operation

Motivated by hard winter 2010/11 in Germany, CGN not only increased its amount of technical winter services equipment, but also established the described project with Fraunhofer FKIE by end of 2012 to achieve the following main goals

- getting a common operational picture of the overall winter services situation at the airport
- enabling early detection and warning for potentially hazardous developments
- targeted information distribution to relevant stakeholders
- initiating counter measures and keeping the operators in the loop to monitor progress and effect of measures

Another important aspect is documentation. All actions taken should be documented as in case of an aircraft accident investigation, for example by German Bundesstelle für Flugunfalluntersuchung (BFU), the compliance with all regulations has to be proven.

2.1.2 System landscape

As important example for airport IT systems, the Airport Operational Database (AODB) should be mentioned. The AODB contains data about flight planning and operational flight information. In addition there are some systems that are specific for winter services use, for example sensor-based surface monitoring system on runways and weather forecasts system, hosted by external weather office. Additionally there are systems that are used for a wide range of airport operations like dispatching system for task assignment.

As these systems are usually implemented as stovepipe systems, dedicated to serve a single purpose, so users with coordinating tasks have to switch between a notable number of systems. For operational winter services coordination there are six main systems that are relevant: AODB, sensor-based surface monitoring system (runway conditions), weather forecast system, resource monitoring system (filling level of de-icing fluid), dispatching system (assignment of winter services tasks) and equipment management system (especially for vehicle availability monitoring).

2.1.3 Organisational landscape

The operational part of winter services at an airport at minimum consists of a central coordination instance and an executing part out in the fields. The coordinating instance has various information interfaces, as one can see in fig. 1. The described solution was supposed to support in particular the coordinating part of winter services operation.

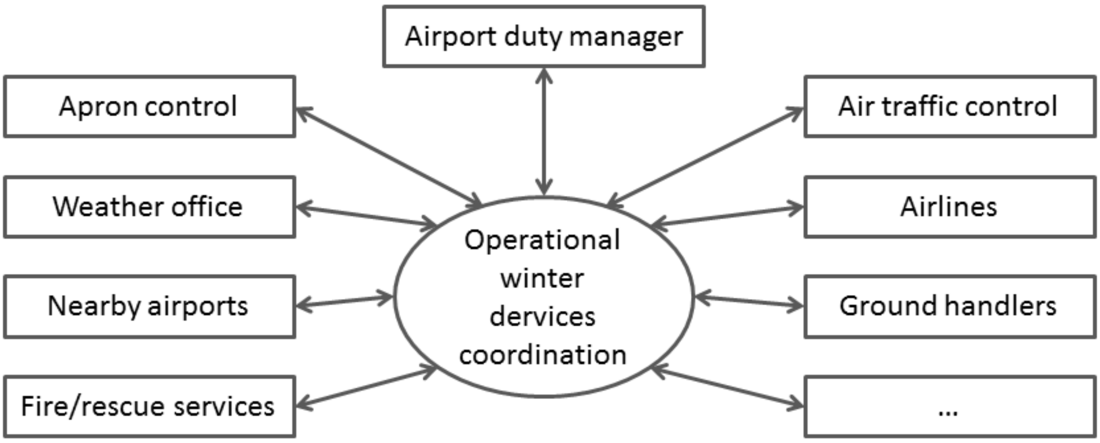


Fig. 1: Complex communication relations of winter services coordination at airports (following [1], fig. 16.5, p. 513)

The winter services coordination maybe a dedicated control room or integrated in a control room like an Airport Operational Control Center (AOCC) that covers a wide range of coordination tasks at the airport (see [1], p. 512).

2.2 Related Work

The given solution is related to well-established concepts from aviation domain (Airport Collaborative Decision Making) and military domain (situational awareness systems).

2.2.1 Airport Collaborative Decision Making

Activities for establishing a common view on operational information in airport environments are discussed for decades. The Airport Collaborative Decision Making

(A-CDM) does this. The aim of A-CDM is "…improving Air Traffic Flow and Capacity Management (ATFCM) at airports by reducing delays, improving the predictability of events and optimising the utilisation of resources." ([3], p. XVII, Airport CDM Definition). A-CDM is about information sharing between different stakeholders to enable them adjusting their processes in operation. A-CDM does not go deep into airport processes. The focus is a capacity optimisation of the air traffic management. Therefore only the relevant connection points to processes at the airport are considered, so A-CDM is no concept for optimisation of internal airport operation processes.

2.2.2 Situational awareness systems

Systems for situational awareness like Command and Control Systems (C2 systems) in military use are widely used in different variants. One important concept of those systems is creating a Common Relevant Operational Picture (CROP, [2], pp. 252). A CROP enabled easy access to the relevant information, where the 'R' for 'relevant' stands for the link between the roles and processes of the operators and the required information. Today more and more information is available, so context sensitive information display and targeted information distribution are important concepts that were also used in the presented solution.

3 CONCEPT AND IMPLEMENTATION

The given solution was supposed to create a common situational awareness by establishing a central system that contains all information that is relevant for winter services. Additionally a monitoring of airport processes, based on this central situation picture, was foreseen for enabling decision support. Monitoring the airport processes allows evaluating changes to the current situation and giving decision support in the meaning of alerts and recommendation for action at an early point in time.

3.1 Concept

Severe weather conditions at airports typically lead to the following operational effects:

a) local infrastructure capacity is reduced (caused by visibility conditions, surface conditions, etc.)

b) local resources are highly utilised and staff has heavy workload (as a result of non-routine situations and non-routine tasks)

c) additional challenges, like diverted flights, exceptional situations (emergency landings, etc.)

This means scarce infrastructure resources (a) while available resource utilisation as well as staff workload is high (b) and unexpected, additional workload occurs (c). For increasing the robustness for severe weather situations, counter measures for these three effects are supported: Coordination of local infrastructure usage is improved, so reduced capacity (a) is addressed. Many routine-tasks allow some degree of automation, for example a main part of the documentation in winter services can be done by a system if it receives the relevant data. Even most non-routine tasks allow system support for taking some load from the airport employees (b).

This support for effects (a) and (b) enables winter services coordination to focus on additional challenges (c) that require special processes and flexible acting, which is also supported as far as possible.

The following sections describe the particular parts of the concept.

3.1.1 Process analysis

Common situational awareness and decision support, based on monitoring of the airport process status, ensure that the actors are informed about possible precarious developments and thus could initiate mitigating measures at an early point in time. To realise this, in a first step, the winter services operation processes were analysed. For supporting these processes, the following information was documented:

- standard process flow
- actors of the different process steps
- decisions to be taken and information needs
- communication relationship to other actors

This was the basis for monitoring process status.

3.1.2 Common situation picture

To get the required information from the systems running at the airport, data interfaces were established. The proven procedures for creating a Common Relevant Operational Picture (CROP) ([2], pp. 247) were applied to this data. It was mapped to a common data format (syntactic fusion) and based on this aggregated (semantic fusion) to allow reasoning over the overall situation.

3.1.3 Early warning and decision support

Based on the CROP, a rule engine was used to enable the above mentioned reasoning functionalities. Based on the process analysis, dependencies like process interdependencies and required resources were formalised in rules. These rules consist of a conditional part that describes when a potential critical situation occurs and an action part that contains the reaction of the system. The rules are not hard-coded in the system, so the basis for the decision support functionality could be extended during runtime.

3.1.4 Information distribution and action support

Getting the relevant information into the system and building a CROP for situation assessment are the prerequisites for detecting of precarious developments. As soon as they are detected, the system has to alert the responsible person as well as support the introduction of counter measures. Therefor again the process analysis was used as basis. The relevant actors could be identified and, based on the process interdependencies and resource usage, effects of measures can be derived.

3.1.5 Combining all parts for system support

With the knowledge of the airport processes, a common situation picture can be established and precarious developments can be detected as well as counter measures can be introduced, based on decision support functionalities. In combination this enables the optimization of airport operation processes in various areas, such as

- Resources and staff assignment optimization: Detecting potential bottlenecks and time critical conflicts allows better planning and an improvement of safety.
- Shift handover: The overview about processes that go beyond changes of shifts ensures that the shift handover influences process flow as less as possible.
- Targeted information propagation: A common source of information (data hub) not only lets users access the relevant data for their tasks in a seamless way. They also get notified if operational status changes affect their current area of work, according to their responsibilities in different roles.

- Documentation: Manual data integration and documentation of distributed information is a time-consuming and unsatisfactory task. Reducing workload at this point leads to the improvement of working conditions.

All relevant information and processes are collected in a central place and are made accessible via a single interface.

3.2 Implementation

A proof of concept implementation at Cologne Bonn Airport (CGN) was installed in November 2013 and continuously extended since then. Beginning with November 2014 the solution is able to run stable in 24/7-operation and thus provide continuous support for winter services coordination.

To meet the user requirements and consider airport processes as far as possible, a human-centered design approach according to ISO 9241-210 ([4]) was used for implementation. Numerous iterations and close cooperation with the users led to continuous improvements. Extension to additional working positions like support for the dispatching of winter services tasks also brought collaboration functionalities that led to reduction of communication overhead (email as well as phone or radio communication).

As stated in section 2, existing IT systems and processes at the airport that were out of scope for this project must not be influenced by the solution. This is why a domain-driven design approach was used, with winter services operation as application domain and defined interfaces to connected processes as well as data interfaces for relevant airport systems.

4 RESULTS DISCUSSION

For prove of concept and for improved support of operational processes in winter services at CGN, the system “Intelsys” (German abbreviation for integrated decision support and situational awareness system) was developed and tested in airport operation. This was regarded as successful. In particular the user feedback confirmed that the following effects showed up:

- Integration of information reduced workload, the users did no longer have to switch between multiple systems to get an overview of the current airport situation
- The time for overhead-work was reduced as main parts of the documentation happen in the background
- The collaboration of different actors was supported, reducing communication via phone or email

These effects have benefits in every day operation, but they are especially valuable if the airport is not in “normal operation”. If the users have to deal with scarce infrastructure resources, heavy workload and unplanned, additional challenges (as discussed in section 3.1), targeted system support according to the airport processes brings improvements to the robustness of airport operation.

4.1 Implications for airport operation

With the given solution CGN improved robustness for severe weather situation as multiple improvements support airport operation under these conditions.

As the solution is an integrated system that interacts with the relevant airport systems, the users have less effort for getting a picture of the overall situation. This itself already reduces work overhead and enables early detection of potential resource bottlenecks.

These effects are increased by warnings and decision support functionality that is exactly tailored to the airport processes. The manual information evaluation by the users gets supported by the system and its mighty rule engine that checks every change of the common situation picture against known process interdependencies and resource dependencies. The early detection of potential bottlenecks enables an early reaction that is also supported by the solution.

The collaboration between different stakeholders at the airport benefits from the common situation picture, as all involved stakeholders have the same information available. The targeted information distribution to stakeholders that do not work with the system but are also involved in the processes reduces phone, radio and email communication, which also reduces workload and noise level.

Last but not least documenting all changes of the situation picture in the background ensures a complete documentation even under stressful conditions.

4.2 Chances for Safety and Security

Safety aspects always part of discussions about airport processes. One example that illustrates this is the Concorde accident in 2000 ([1], p. 137) that led to a tragically explosion which often comes up in discussions about runway safety. The focus of the described work was to support operational processes and thereby also reduce possible safety issues. With a common operation picture of the overall airport situation, detection of safety critical situations is improved.

Improving security was not in the primary part of the project. Nevertheless it became clear, that bringing together operational information with information from security would increase planning capabilities, for example for passenger security control in terminals. For example federal police could be integrated into the solution and thereby would be directly integrated in information flow and aware of relevant information from airport operations.

5 CONCLUSION AND FUTURE WORK

The integrated solution improved the robustness for severe weather situations, but it is also capable to increase robustness for other disturbances in operation. As the solution is implemented as modular software, it could be extended at any time.

The evaluation of the described solution was successful in winter services environment, so the extension to other parts of airport operations has already started. Many other areas of airport operations suffer from similar problems and would benefit from this solution. Additionally the value of the whole solution grows with the number of covered processes. If more processes and their interdependencies are integrated into the solution, more factors are taken into account in evaluation of the current situation.

REFERENCES

[1] Ashford, N. (2013). *Airport Operations, Third Edition*. McGraw-Hill.

[2] Wunder, M. et. al. (2009). *Verteilte Führungsinformationssysteme.* Springer-Verlag.

[3] Eurocontrol. (2012). *The Manual – Airport CDM Implementation, Version 4.* European Organisation for the Safety of Air Navigation (EUROCONTROL)

[4] International Organization for Standardization. (2010). *Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems*. ISO.

INTEGRATION OF CT METHODS INTO HAND LUGGAGE SCANNING PROCESSES AT AIRPORT CHECKPOINTS BASED ON EXISTING MULTI-VIEW SCANNING SYSTEMS

Victoria Heusinger[1], Stefan Moser[1], Markus Büttner[1], Benjamin Lang[1] and Siegfried Nau[1]

[1] *firstname.surname@emi.fraunhofer.de*
Fraunhofer Institut für Kurzzeitdynamik, Ernst-Mach-Institut, Am Klingelberg 1, 79588 Efringen-Kirchen (Germany)

Abstract

In this presentation, an efficient way to integrate Computed Tomography (CT) methods into the scanning process of carry-on baggage at airport checkpoints is proposed. The implementation suggested is designed to employ existing multi-view scanner geometries.

The first key element of this approach addresses the problem of the optimal scanning geometry and focuses on the apt choice of positioning as few as possible additional projection views along the conveyor belt.

The second key element is the choice of a suitable and efficient algebraic reconstruction algorithm and its optimization for the purpose of luggage scanning. The main challenge addressed in this investigation is to enhance the quality of the reconstruction of strongly underdetermined data sets with scanned objects whose composition is mostly unknown. This is clearly the case for hand luggage and its very wide ranged possibilities of content. Further technical challenges like the minimization of the reconstruction runtime to in-line capability and several methods to reduce typical artifacts are discussed.

Artifact reduction methods shown in the presentation are a, for the used algorithm specialized, metal artifacts reduction (MAR). Also the reduction of noise influence or other image impairments is faced with a splatting type regularization method. An approach to streak artifacts reduction via an individual correction term weighting method is presented.

Finally a practical application of the reconstruction results is given where the reconstructed volume is employed to enhance the typical 2D images operators are used to interpret. This is accomplished by removing certain parts of the volume, providing a step towards the ambition that objects like laptops, electronics or other heavy absorbers can be left in the baggage.

Keywords: ART, artifact reduction methods, aviation, CT, checkpoint, metal artifacts, noise, scanning geometry optimization, streak artifacts,

1 INTRODUCTION

The introduction of CT methods in the processes of hand luggage scanning at the checkpoint has been contemplated for years [1]. One of the reasons for this is that automated threat recognition (ATR) can greatly benefit from using 3D-data as overlapping and shading hinders a clear recognition of objects in 2D [2]. The possibilities of improving material analysis such as Dual-Energy methods also gives a great incentive for the application of CT methods. CT reconstructed volumes at different energy levels allow for a localized analysis of materials based on each individual voxel instead of the Z effective along a whole ray of the 2D multi-energy imaging [3]. In any case the reduction of the necessity of disassembling or unpacking the examined object (e.g. hand luggage) is one of the expected benefits. Due to the larger amount of detail provided by a CT analysis, the false alarm rate should also be reduced significantly.

However, there are many obstacles to the application of CT in airport security checkpoints. Conventional CT devices require many projections in order to an object whose composition is generally unknown. To gain those high projection numbers typically gantry systems are used. Those systems are also applied at the airport for checked in baggage screening. The drawback of those is that they are either too slow or too expensive (or both) for the massive high throughput application as it is needed for carry on hand luggage scanning at passenger checkpoints.

Following another approach, Fraunhofer EMI has worked on the incorporation of CT and its methods in the setting of standard x-ray security inspection equipment, that is state of the art at most airport security checkpoints by expanding the number of existing views (2-4 views depending on the manufacturer) with only a very few additional, spatially static source-detector-pairs.

Some of the results will be presented in the following. The two main factors, which have been considered in order to customize and optimize CT for this field of application are the scanning geometry and the reconstruction algorithm optimization.

2 OPTIMIZING THE SCANNING GEOMETRY

Since only very few projection views are available to begin with and as few as possible are planned to be added to modify the existing scanning geometry for CT application, the extent of additional information should be maximized by each new view. Therefore, the geometrical alignment of the new views is important.

The conventional planar arrangement, in which the views are placed around the object in a circular stripe, works well if many views are used but is suboptimal if just a few projection directions are employed. The new information gathered is less than with a geometry that exploits all three dimensions of space, with the angles between the views as large as possible [4]. The positioning of views along edges is also a very important aspect, which has to be considered [5], [6]. However, in contrast to medical CT or industrial inline CT, where the test object is known, the internal composition of a piece of luggage consists of a very wide variety of objects and possible orientations so that relevant edges cannot be determined that easily. Here, positioning of the views in all three dimensions of space, in particular outside of the planar setup, should also be of advantage because the sampling direction for edges is more varied and the chance to look along relevant edges is more widely spread than in the conventional planar setting.

Keeping the application background in mind, objects in the luggage are often oriented along the outer form of the luggage case. Hence, if positioning the luggage piece parallel to the conveyor belt for an optimal 2D-view for the conventional Dual-Energy imaging, additional views should be perpendicular to this view. This also corresponds to the angle maximization requirement mentioned above.

From a more practical point of view there are limits to the realization of these recommendations. The standard conveyor belt setting, which is very convenient for the handling of luggage, restricts the options of modifying the scanning geometry. For example, placing an additional projection view in the direction of motion of the conveyor belt is impractical without massive modification of the existing scanner layouts. Furthermore, lowering and raising such a view onto the conveyor belt for each luggage piece would increase the time of processing hand luggage immensely. Also, physical space (footprint) for scanning equipment is limited at airport security checkpoints. A possible practical approach to this aspect is based on the fact that for the reconstruction there is no difference between changing the projection direction and changing the orientation of the scanned object relative to the views. Hence, repositioning the luggage piece is a possibility to face those problems and seems realizable with several methods.

The simulation studies carried out ignore such restrictions in these first investigation. Results confirm that new views placed inclined (up to an angle of 90°) with respect to the plane defined by the traditional views perpendicular to the conveyor belt movement direction enhance the quality of reconstructed volumes to a greater extent than adding the same number of views in the same plane (Fig. 1). This is especially evident in the slice images that lie along that plane (xy-slice images in Fig 1).

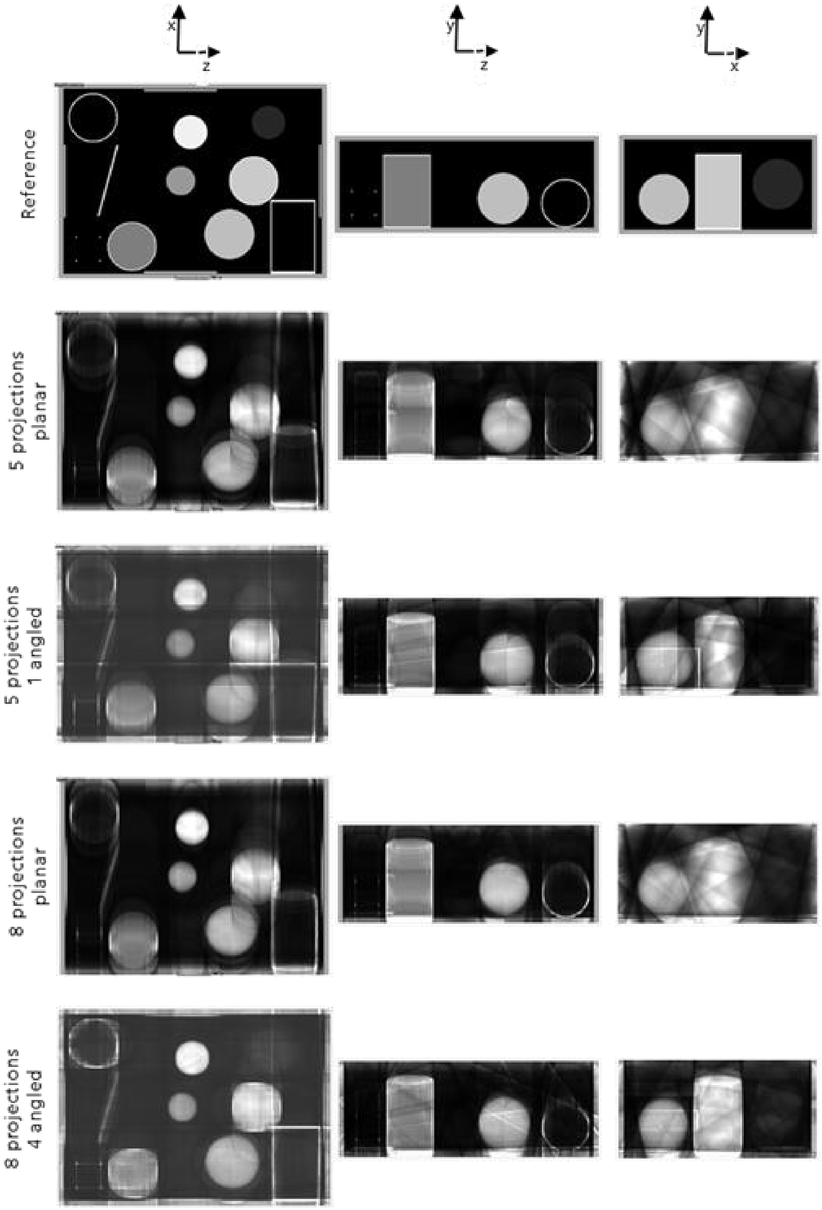


Figure 1. Comparison between a reference volume and its reconstruction, showing the effect of different modifications of the standard setup of x-ray scanners at airport security checkpoints, utilizing four projections which are all perpendicular to the conveyor belt: (a) reference volume, (b) 5 projections, one view added in the same plane (c) 5 projections, one additional view tilted by 90°, (d) 8 projections, four views added in the same plane, (e) 8 projections, four additional views, which are all tilted by 90°. All reconstructions were carried out with a basic ART algorithm without further artifact correction mechanisms.

Ultimately, the specific intended usage of the results by the operators plays the decisive role in finding the optimal solution for the scanning geometry:

For a sole support of 2D imaging enhancement, it seems to be sufficient to gather additional information perpendicular to the 2D line of sight in order to correctly determine the size of objects in the direction of the radiographic rays (Fig. 1, 5 views xy-perspective).

For true 3D imaging more views will be required (Fig. 1, 8 views). For ATR the required reconstruction quality is most likely somewhere in between those cases. But altogether, analyses of synthetical data suggest that it is possible to apply CT techniques with very few views and moderate additional engineering effort beneficially to the scanning of hand luggage.

3 RECONSTRUCTION ALGORITHM

The use of only very few projections (undersampled dataset) in CT is always combined with the use of iterative, algebraic reconstruction methods since the completeness of the data is not as rigid a requirement as with their analytical counterparts (e.g. Feldkamp). Another advantage is that they allow for an implementation of any arbitrary scanning geometry in an inherent way [7].

The general concept behind iterative, algebraic algorithms is that each radiographic vector from the source to a pixel p_j is viewed as a row of an inhomogeneous linear system of equations, where the optical density values d_n of the voxels that intersect with the ray with a transmission length v_{nj} are the unknowns [8][9].

$$p_j^i = \sum_{n=1}^{N} d_n^i v_{nj}$$

Initially, a guess for the solution is made, which is substituted into the system of equations. This results in a virtual forward projection, which is then compared with the actual pixel values of the image. Comparing the forward projected, virtual pixel value p_j^i and the corresponding actual image value r_j, a correction term c_j is gained for each pixel. In the back-projection-step the average a_n^i over all respective correction terms is formed for each voxel and then taken to adjust the value of it. These steps are repeated (i in the equations above is the index for the current iteration step) until a specific criterion is reached, which terminates the algorithm.

Our basic ART implementation [9][10] is a derivative of an averaged multiplicative algebraic reconstruction technique (AVMART) algorithm [10] where the correction term is gained via the quotient of p_j^i and r_j.

Iterative algorithms have the drawback that they are substantially more time-consuming than direct analytic approaches. Indeed, only elementary operations such as addition and multiplication are performed but in many repetitive steps of the calculation. However, especially those elementary operations can be very well executed in parallel by a graphics processing unit [11]. Due to this parallelization, the EMI-ART algorithm achieves the reconstruction of a piece of hand luggage from 4 views in about 4-6 seconds on standard consumer nVidia graphic cards. Hence, this algorithm is inline capable and as such useable for an application in airport security checkpoints.

Another important point in the application of CT to airport passenger checkpoints is that especially for ATR purposes the reconstruction needs to be as free of artifacts as possible. In this the proposed very small number of projections is a considerable problem as the system of equations becomes strongly underdetermined, i.e. the solution space becomes quite large, which gives way for even more possibilities for the typical CT artifacts such as streak or metal artifacts, or noise. For this reason, several mechanisms to reduce these artifacts are being developed especially for the EMI-algorithm, which restrict the solution space e.g. by using a priori knowledge.

3.1 Metal artifact reduction

In order to reduce artifacts that are stemming from highly absorbing areas within the test object, inherent properties of ART-algorithms are exploited [12]. Rays that are passing through highly absorbing materials are simply not regarded for the computation of a voxel on their path if they yield little or no additional information at all, or even influence its calculation negatively. Thus, only such rays j are considered for the calculation of the voxel's correction factor a_n^i that have a "clear field of sight" on the voxel, without heavy absorbers lying in between.

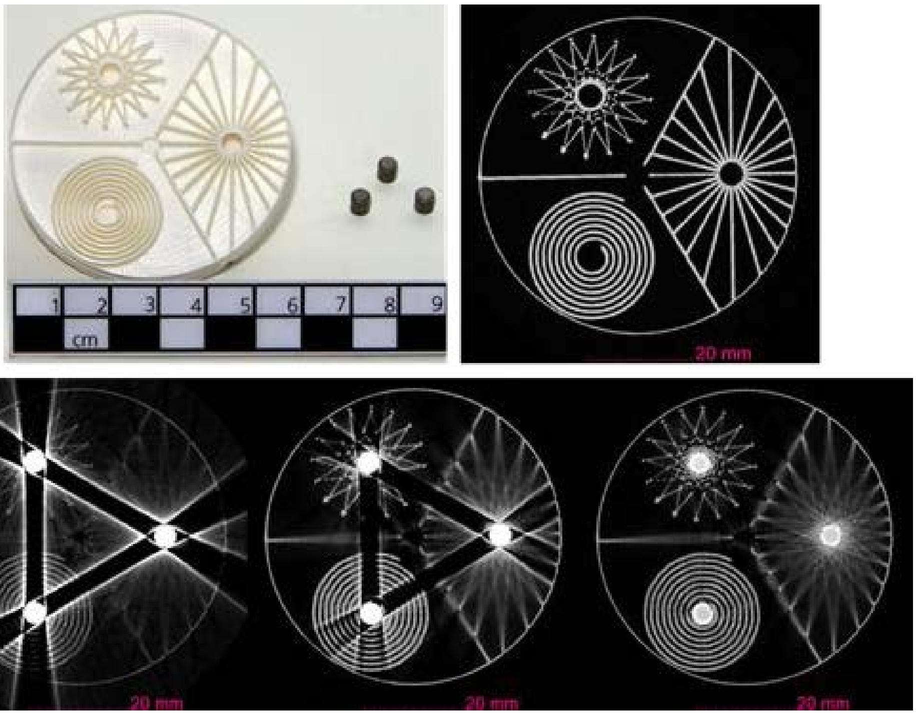


Figure 2. Comparison of an x-ray phantom of ABS plastic (a) equipped with three tungsten studs, (b) reconstructed without the studs, (c) with FBP, (d) with ART and without the execution of the MAR method, and (e) with ART and with MAR.

Thus, many common effects of metal artifacts such as shading, blooming and streak artifacts can be significantly reduced or even completely suppressed (see Fig. 2). Structures (e.g. edges) that lie along the direction of the rays that are ignored, however, cannot be recovered by this practice (see Fig. 2, right side of the object).

3.2 Noise reduction

For a reduction of the influence of noise on the reconstruction, a regularization method called splatting is deployed [9]. In this method, not only the affected pixels r_j are used for the calculation of the correction factors c_j but also neighbouring pixels within a certain radius are used. The effect of pixel defects and inhomogeneities in the projections can thus be reduced (Fig. 3). During the calculation a weighting form factor (splatting factor) is used to fine-tune the application.

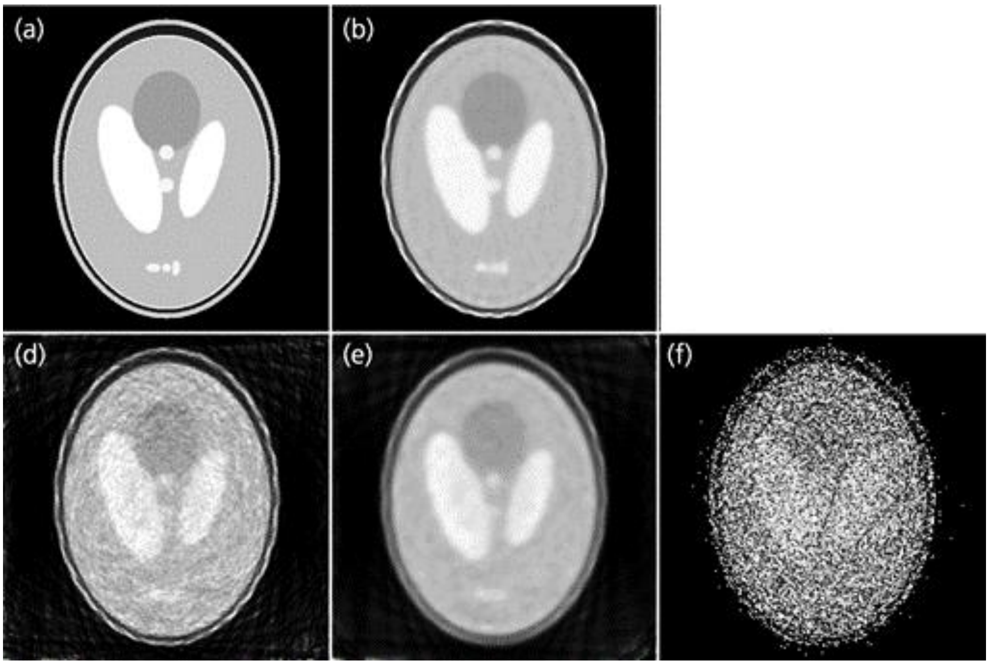


Figure 3. Different SNR and varying splatting factor values, 30 projections: (a) reference, (b) reconstruction without noise, (c) SNR 10 and sf 1.0, (d) SNR 10 and sf 5.0, (e) SNR 10 and no splatting.

3.3 Streak artifact reduction

Streak artifacts arise from rays which pass from strongly absorbing areas to weakly absorbing areas or vice versa. In particular, they occur along the edges of strong absorbing parts of the test object [13].

They can be reduced by a suitable weighting of the correction factors. Due to various approximations (rounding, conversion from grey values to pixel values for the calculation, etc.) during the different steps of the computation, each calculated parameter (and therefore the correction terms) exhibit a certain range of inaccuracy. This results in a deviation for each parameter which is, taken into account in the calculation of the averaged correction a_n^i. As can be seen in Fig. 4, the negative effect of streak artifacts can be reduced significantly.

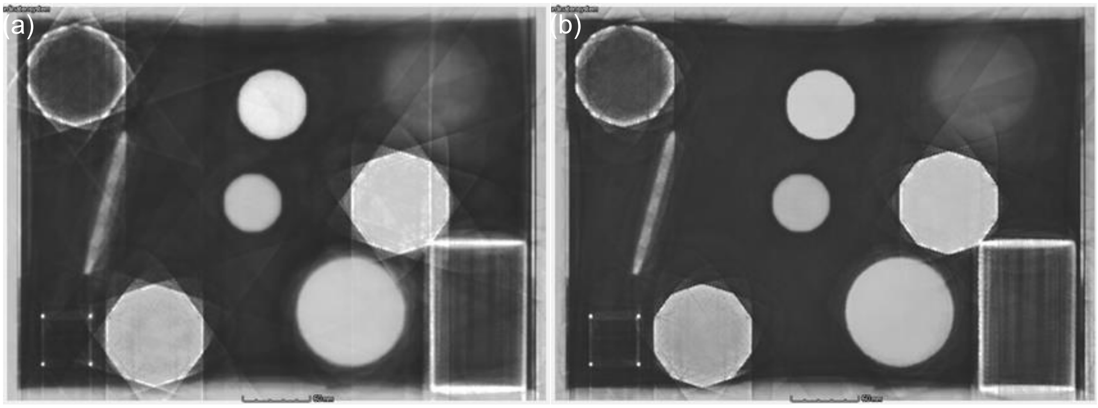


Figure 4. Comparison of a reconstruction without (a) and with (b) employment of the streak artefact correction (dataset size: 20 projections).

4 DISCUSSION AND CONCLUSION

Based on the presented work on the optimization of scanning geometries and reconstruction algorithms, it seems to be promising as well as technically feasible to integrate CT and its methods into the scanning process of hand luggage at airport security checkpoints. By a smart choice of the scanning geometry and the use of a reconstruction algorithm which is adapted for CT with only a very few projection views, it should be possible to significantly improve on the imaging and other automated processes such as ATR of current scanning devices for hand luggage, and thus on the overall workflow.

REFERENCES

[1] L. Parker, „Explosives Detection in Aviation Applications Using CT“, Int. Conf Image Formation in X-Ray CT, Salt Lake City 2014.

[2] ALERT Center, “Advances in Automatic Target Recognition (ATR) for CT-Based Object Detection Systems” , Final Report Automated Threat Recognition Initiative of DHS COE ALERT Center, Boston 2015

[3] R. Alvarez „Energy-selective Reconstructions in X-Ray Computerized Tomography” in Phys. Med. Biol. Vol 21 (5), 1976, pp. 733-744.

[4] V. Heusinger et al. „X-Ray CT Geometry Optimization“, to be published

[5] Z. Zheng „Identifying Sets of Favorable Projections for Few-View Low-Dose Cone-Beam CT Scanning“, Fully 3D, Potsdam 2011.

[6] M. Schrapp et al. “CT Reconstruction with Object Specific Non-Standard Trajectories”, DIR2015 , Ghent 2015

[7] X. Pan et al. “Why do commercial CT scanners still employ traditional, filtered back-projection for image reconstruction?”, Inverse Probl., Vol. 25 (12), 2009

[8] R. Gordon et al. “Algebraic Reconstruction Techniques (ART) for Three-dimensional Electron Microscopy and X-Ray Photography”, J. theor. Biol., Vol. 29, 1970, pp. 471 - 481

[9] S. Moser et al. “In situ flash x-ray high-speed computed tomography for the quantitative analysis of highly dynamic processes”, Meas. Sc. Tech., Vol 25, 2014

[10] D. Mishra et al. “A robust MART Algorithm for tomographic applications”, Numerical Heat Transfer, Part B: Fundamentals, Vol 35 (4), 1999.

[11] K. Mueller, “On the use of Graphics Hardware to accelerate Algebraic Reconstruction Methods” in *SPIE Medical Imaging Conference,* San Diego, 1999.

[12] B.E: Oppenheim “Reconstruction tomography from incomplete projections” in *Reconstruction Tomography in Diagnostic Radiology and Nuclear Medicine.* Eds. Baltimore, MD: University Park, 1977, pp. 155-183.

[13] J. Hsieh, “Image Artifacts: Appearances, Causes, and Corrections”, in *Computed Tomography - Principles, Design, Artifacts, and Recent Advances,* Second Edition, SPIE, Bellingham, 2009, pp. 207 - 300

.

STAND-OFF MM-WAVE IMAGING USING ARRAYS BASED ON GLOW DISCHARGE LAMPS

H. Altan,[1] A. B. Sahin,[2] A. Abramovich,[3] Y. Ytzhaky,[4] N. Kopeika[5]

[1] haltan@metu.edu.tr
Department of Physics, Middle East Technical University, Cankaya, Ankara, 06800 (Turkey)

[2] absahin@ybu.edu.tr
Department of Electrical and Electronics Engineering, Yildirim Beyazit University, Ulus, Ankara, 06030 (Turkey)

[3] amir007@ariel.ac.il
Ariel University, POB 3 Ariel, 40700 (Israel)

[4] ytshak@bgu.ac.il
Dept. Electro-Optics Engineering, Ben-Gurion University of the Negev, POB 653, Beer-Sheva (Israel)

[5] kopeika@ee.bgu.ac.il
Dept. Electrical & Computer Eng., Ben-Gurion University of the Negev, POB 653, Beer-Sheva (Israel)

Abstract

The development of mm/sub-mm imaging systems has progressed rapidly in the last twenty years. Stand-off detection systems have been developed to image scenes at a distance using these long wavelengths. While active systems benefit from the ability to work in closed environments they lack the simplicity in imaging due to the reduced complexity of optics offered by passive imaging systems. Furthermore, passive imaging systems typically require expensive cooled detectors which so far has hindered this technology from widespread use. The development of affordable, sensitive room temperature detectors will allow the necessary breakthrough to carry this technology into a variety of industrial and defense related fields. Plasma oscillations in various media provide an effective means to detect such long wavelengths event at room temperature operation of the device. Surprisingly the plasma created inside a miniature glow-discharge lamp is also sufficient medium for detection of these long wavelengths. By using a relatively inexpensive array based on commercially available neon indicator lamps and heterodyne detection techniques our team members have already demonstrated active imaging systems that can rapidly image a scene in 3D at stand-off distances [1]. In order to improve the detection sensitivity and better understand the underlying physical principles behind the mm-wave plasma interaction an RF/DC glow discharge plasma chamber was constructed to test operation under different Penning mixtures. Further studies were done to understand the effect of the mm/sub-mm wave radiation on the overall device performance using commercially available lamps. With the knowledge gained from these studies future work will focus on developing a 16 x 16 discharge lamp array, incorporate it into a stand-off active imaging system, and test its performance with respect to a similar array built with commercial neon indicator lamps.

Keywords: Glow Discharge Lamps, Plasma, Terahertz, MM-wave, Stand-off Imaging.

1 INTRODUCTION

Millimeter wave and terahertz (THz) regions of the electromagnetic spectrum are gaining importance for a multitude of applications in security fields owing to their unique properties. THz and mm-waves are capable of penetrating most non-metallic and non-polar materials. Imaging systems based in this frequency range can be utilized to safely identify concealed substances and weapons through clothing and other barriers. In addition, hazardous substances such as illegal drugs and explosives have unique signatures in the THz region, making these technologies essential for screening people and packages [2-4]. Despite the promise of novel applications, detection of mm and THz waves at room temperature is still a challenging task. There are various uncooled detectors for direct detection of mm-wave/THz radiation. Golay cells, photoconductive antennae, pyroelectric sensors, piezoelectric resonant structures, Si Field Effect Transistor (FET) type devices, direct Schottky diode detectors, and bolometers are some of the most common types employed today. These detectors have noise equivalent power (NEP) values that range from 10^{-8} to 10^{-12} W/Hz$^{1/2}$. Golay cells, and pyroelectric sensors typically have a broad spectral response covering 0.1-10 THz. Disadvantage of using a Golay Cell is that it operates at low modulation frequencies and has long response times. Pyroelectric sensors on the other hand can operate at high modulation frequencies above a few kHz but typically have a lower sensitivity. Furthermore, these detectors share a common drawback of being difficult to implement into an array in order to perform video rate imaging [5]. Recent studies show that a miniature neon indicator lamp, also known as the Glow Discharge Detector (GDD) is a low-cost alternative having a fast response time, broad spectral response, low NEP and room temperature applicability for imaging purposes [6].

2 GLOW DISCHARGE DETECTOR

Previously, we have investigated various GDDs in terms of their speed, frequency response and polarization dependence based on their orientation with respect to the incident light [7]. In order to investigate the effects of discharge breakdown and glow scenarios for various inert gasses as well as various Penning mixtures on the mm-wave/THz detection mechanism between the anode and cathode, a small plasma vacuum chamber is designed and built as shown in Fig. 1.

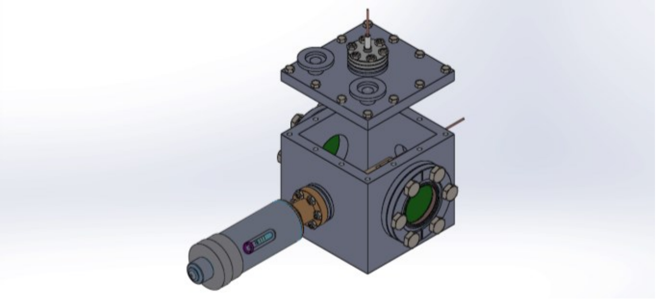


Fig. 1. Plasma Discharge Chamber. The electrode separation is controlled using a micrometer.

A breakdown is typically achieved in a gas mixture under vacuum by applying a bias DC voltage to the electrodes. Under optimum conditions the electric field of the modulated incident radiation increases the total electric field and can generate variations in the plasma current. The effect of incident radiation on the plasma current depends on several parameters such as the extent of the plasma region, types of gases in the mixture, electrode geometry including separation between leads and polarization orientation of the radiation with respect to the plasma electric field. Based on the measured discharge current values, to the device is seen best to operate within the abnormal regime of the glow, before the arc region. In this region the electric field of the incoming THz radiation, when aligned with the applied DC field is expected to increase the rate of collisions [8]. The vacuum chamber having a dimension of roughly 10x10x10 cm^3, has two quartz windows that allow the transmission of incident THz radiation through the DC glow discharge between the electrodes. Electrodes with different geometries can also be used in the constructed chamber. The electrode separation can be controlled with 10 μm resolution and can be extended up to 2 cm. Also the chamber admits a floating probe allowing the measurement of changes in plasma current and plasma voltage.

2.1 Glow discharge-mm wave interaction

In order to study response of the built GDD at various modulation frequencies of incident mm-wave, an experimental set-up shown in Fig.2 is constructed. The far infrared radiation is generated using a Virginia Diodes Inc. (VDI) multiplied source (WR2.8AMC), driven by a frequency tunable Yttrium Iron Garnett (YIG) oscillator. The source was modulated electronically providing a frequency tunable output in the 82-125 GHz and 246-375 GHz frequency range by use of a passive tripler. The setup allows both the measurement of the plasma current and the intensity of the transmitted EM radiation. For the measurement of plasma current a custom built lock-in amplification electronic circuit is used. Furthermore the second quartz window at the other end of the chamber allows for measurement of the transmitted field by a Golay cell (TYDEX GC-1P) which allows one to study resonant interactions between the mm-wave field and detector geometry. Modulated beam is focused on the electrode gap by using a set of Teflon lenses (50 mm diameter, F#2). The beam diameter at the focus is measured approximately to be 8 mm.

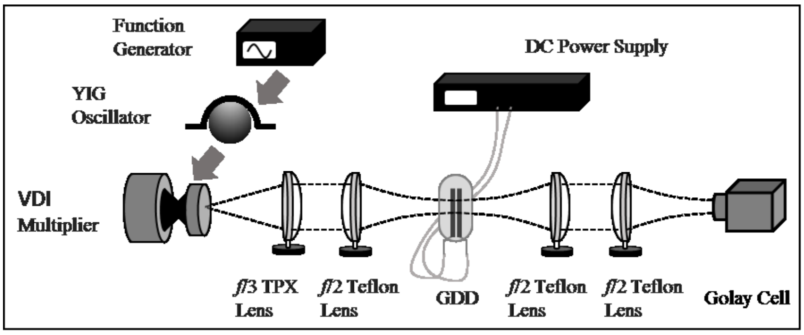


Fig. 2. Schematic representation of the mm-wave/THz measurement system, working in 260-380 GHz region.

Recent work done with commercially available discharge lamps have shown that these detectors can be incorporated into arrays to perform stand-off imaging using optical designs based on confocal Gregorian optical geometries [1]. Using the set-up depicted in Fig. 2 the goal is to optimize the detection geometry specifically for W-band radiation by investigating the role of penning mixtures as well as electrode separation. Once completed efforts will concentrate on developing a 16x16 array to integrate into a stand-off imaging system.

3 CONCLUSION

This work aims to further develop the previous studies started on various Penning mixtures [9] by extending the measurement at various far infrared radiation frequencies as well as different modulation frequencies. The constructed system will also aid in observing the effect of the different glow characteristics due to the electrode geometry. The results of this work will be crucial for developing security measures since GDDs are relatively cheap and can be integrated into FPA geometries allowing rapid imaging. Optimizing the structure for rapid imaging at in 3D at stand-off distances and integrating it in a prototype imager will result in a product or tool that will be the first of its kind. Working at room-temperature, its relative insensitivity to environmental conditions, coupled with its expected low-cost will make this system desirable to many who work in security whether it is civilian or military. These efforts are described within the framework of our project funded under the NATO-Science for Peace and Security program - sponsored in part by the NATO Science for Peace and Security Programme grant MD.SFPP 984775.

REFERENCES

[1] D. Rozban, A. Levanon, H. Joseph, A. Akram, A. Abramovich, N.S. Kopeika, Y. Yitzhaky, A. Belenky, and O. Yadid-Pecht, "Inexpensive THz focal plane array imaging using miniature neon indicator lamps as detectors", *IEEE Sensors J.*, VOL. 11, NO. 9, p 1962, 2011

[2] M. Tonouchi, Cutting-edge terahertz technology, Nature Photonics, 1, 97-105 (2007). doi:10.1038/nphoton.2007.3

[3] J. F. Federici, B. Schulkin, F. Huang, D. Gary, R. Barat, F. Oliveira, D. Zimdars, THz imaging and sensing for security applications—explosives, weapons and drugs, Semicond. Sci. Technol. 20, S266-S280 (2005). doi:10.1088/0268-1242/20/7/018

[4] A. Y. Pawar, D. D. Sonawane, K. B. Erande, D. V. Derle, Terahertz technology and its applications, Drug Invention Today, 5, 157-163 (2013). doi: 10.1016/j.dit.2013.03.009

[5] A. Rogalski, F. Sizov, Terahertz detectors and focal plane arrays, Opto-electronics review, 19, 346-404 (2011). doi: 10.2478/s11772-011-0033-3

[6] A. Abramovich, N. S. Kopeika, D. Rozban, E. Farber, Inexpensive detector for terahertz imaging, Appl. Opt., 46, 7207-7211 (2007). doi: 10.1364/AO.46.007207

[7] N. Alasgarzade, T. Takan, I. U. Uzun-Kaymak, A. B. Sahin, and H. Altan,"Modualtion and frequency response of GDDs in the millimeter wav/THz region", Proc. SPIE, 9510C, October, 2015.

[8] D. Rozban, N. S. Kopeika, A. Abramovich, and E. Farber, "Terahertz detection mechanism of inexpensive sensitive glow discharge detectors", *Journal of Applied Physics*, 103, no. 093306, 2008.

[9] L. Hou, W. Shi, S. Chen, and Z. Yan "Terahertz continuous wave detection using weakly ionized plasma in inert gases", *IEEE Elec. Dev. Lett.,* 34(5), pp. 689-691, May, 2013.

RISK BASED APPROACH FOR THE PROTECTION OF LAND TRANSPORT INFRASTRUCTURE AGAINST EXTREME RAINFALL (RAINEX)

Kalliopi Anastassiadou[1], Ingo Kaundinya[2], Iraklis Stamos[3], Evangelos Mitsakis[4], Harald Kammerer[5] and Robert Mikovec[6]

[1] *anastassiadou@bast.de*, [2] *kaundinya@bast.de,*
Federal Highway Research Institute (BASt), Brüderstrasse 53, 51427 Bergisch Gladbach (Germany)

[3] *stamos@certh.gr*, [4] *emit@certh.gr,*
Hellenic Institute of Transport - Centre for Research and Technology Hellas, 6th Km Charilaou-Themis, 57001Thermi, Thessaloniki (Greece)

[5]*Harald.Kammerer@ilf.com*
ILF Consulting Engineers, Harrachstrasse 26, 4020 Linz (Austria)

[6]*Robert.Mikovec@ilf.com*
ILF Consulting Engineers, Feldkreuzstrasse 3, 6063 Rum bei Innsbruck (Austria)

Abstract

The aim of the research project “Risk based approach for the protection of transport infrastructure against extreme rainfall RAIN**EX**” is the development of a practical methodology for the identification and assessment of both vulnerable as well as critical transport infrastructures towards extreme rainfall events end their consequences. The developed methodology is based on expert knowledge and includes qualitative and semi-quantitative analyses regarding the assessment of the vulnerability and criticality of relevant transport infrastructures. The process chain from the spatial rainfall to the concentrated runoff in the river channel was shown to assess the local hazard resulting in the local risk. The main result of the project is a practice-oriented and applicable methodology and a comprehensive and well-developed security handbook.

Keywords: extreme rainfall, risk-based approach, flood, climate change, land transport infrastructure, rainfall induced hazards, handbook, CIPS project.

1 INTRODUCTION

Floods have affected more people and caused more damage globally than any other natural hazard [1]. The June 2013 floods in central Europe caused 25 fatalities [2]. They were the costliest global loss event of that year and exceeded in ferocity and in total affected area both the July 1954 flood (previous record) and summer flood of August 2002 [3]. As a consequence, large areas were affected by flood with strong impacts on society in terms of direct damage and interruption of transportation systems [4].

Climate change related disasters and extreme weather events are expected to significantly increase the risk of damages on networks, systems and transportation assets. In view of these anticipated adverse effects, the necessity to adjust the required security level to the actual risk is of central importance. This does not merely imply the exposure, but also the vulnerability and criticality of infrastructures. Designing future transport systems without taking into account security concerns for a specific return period (e.g. for a 100 years flood event) may be appropriate for single infrastructure elements but cannot ensure the long-term viability, functionality and operation of the overall transportation system (infrastructure and networks). Major challenge is to establish a comprehensive design approach addressing security that will have an increasing impact on the availability and quality of transport networks, especially in light of the ever changing climatic conditions and parameters of extreme weather events especially rainfall and resulting natural hazards (frequency, intensity, spatial and temporal distribution).

2 THE RAINEX APPROACH

2.1 Sequence chain

In order to establish a general framework for linking hazards to infrastructure elements, a sequence chain was identified by utilizing previous research results and building on them [5]. Fig. 1 illustrates the sequence chain used in RAIN**EX**.

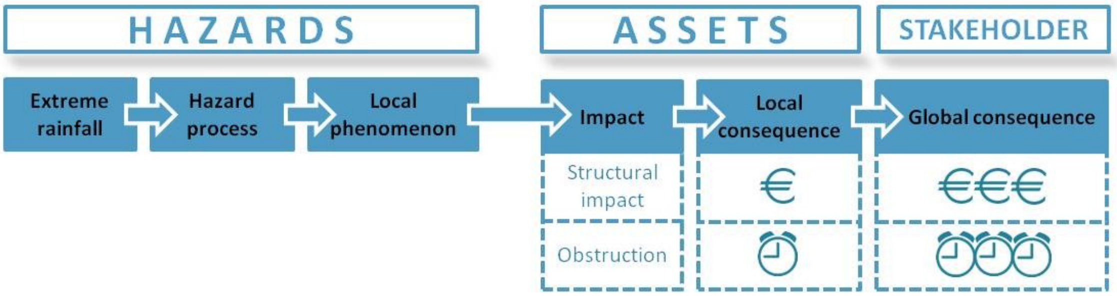


Figure 1. The sequence chain of RAIN**EX**

In order to evaluate the impact of heavy or extreme rainfall resulting in floods on the transport infrastructure several parameters had to be taken into account. The heavy rainfall is a trigger for the floods combined with the state of the river basin in terms of the soil saturation. The process chain from the spatial rainfall to the concentrated runoff in the river channel was shown to assess the local hazard resulting in the local risk.

Different hazard processes were introduced and the preconditions of the formation of these types, as well as, the impact of them on the transport infrastructure were analyzed. Firstly, the natural processes of meteorology and hydrology had to be explained. The understanding of the natural processes enables the users of the methodology to assess and to reduce the risk, as well as, to plan protection measures. In this way, the possible severity of an extreme event can be explained and clearly understood. An severe flood as a consequence of extreme rainfall event can cause a local phenomenon (e.g. bank erosion, overtopping etc.) through a hazard process (e.g. riverine flooding). The causal link can be direct (e.g. rain causes debris flow) or indirect (e.g. rain causes a dam failure, which in turn results in flooding somewhere else). In principle, there can be multiple intermediate steps. The next step links the local phenomenon (the way in which the hazard materializes next to the asset) to the impact (the way in which the hazard acts on the asset). If the local phenomenon is bank erosion, the impact would be obstruction or structural impact. While the impact refers to the phenomena that act on the structure, it says nothing about the consequences. Any potential consequences and their degree of severity depend on the vulnerability and the exposure of the asset.

2.2 The risk-based approach

A practice-oriented and easy applicable methodology was developed which includes qualitative and semi-quantitative analyses regarding the assessment of the vulnerability and criticality of relevant transport infrastructures.

The task of the assessment methodology is to link hazards with assets in a meaningful way, i.e. so that reality is represented in a reasonable way and adds value for infrastructure operators. In order to meet this objective, the following steps are required for the methodological approach (Fig. 2).

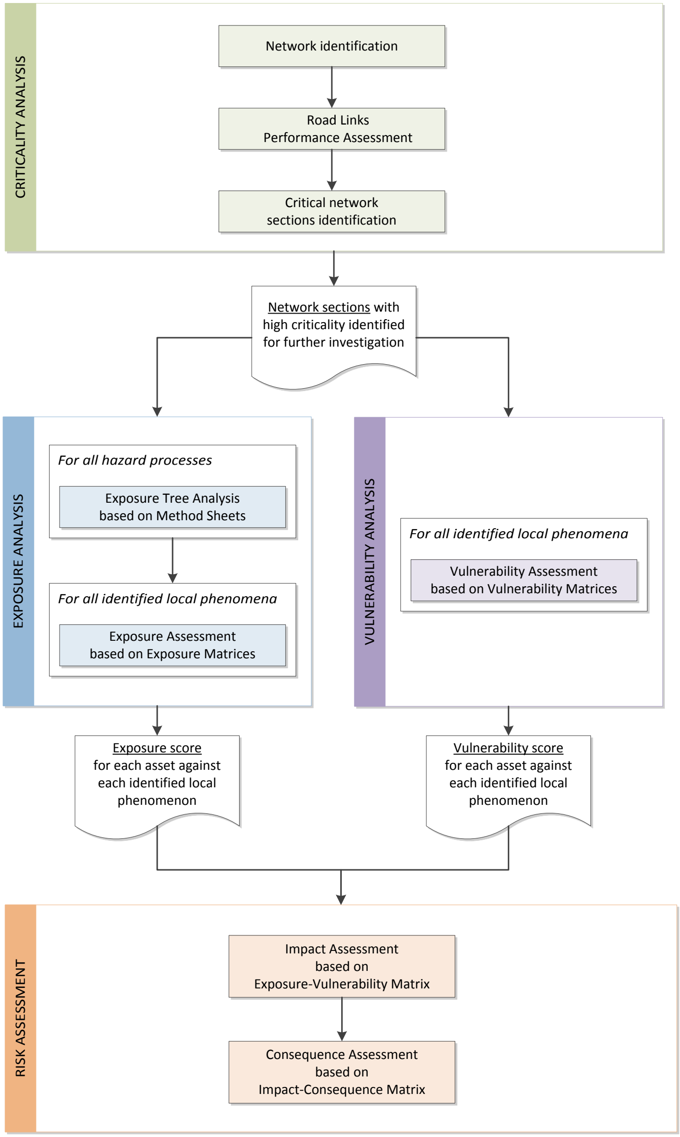

CRITICALITY ANALYSIS
Network identification
Road Links Performance Assessment
Critical network sections identification
Network sections with high criticality identified for further investigation
EXPOSURE ANALYSIS
For all hazard processes
Exposure Tree Analysis based on Method Sheets
For all identified local phenomena
Exposure Assessment based on Exposure Matrices
VULNERABILITY ANALYSIS
For all identified local phenomena
Vulnerability Assessment based on Vulnerability Matrices
Exposure score for each asset against each identified local phenomenon
Vulnerability score for each asset against each identified local phenomenon
RISK ASSESSMENT
Impact Assessment based on Exposure-Vulnerability Matrix
Consequence Assessment based on Impact-Consequence Matrix

Figure 2. Methodological approach of RAIN**EX**

In the first step, the criticality analysis, the road and/or rail network to be investigated has to be defined and assessed based on a road link performance measure method. The size of the investigated network depends on the scope of the study. This step is on “network level” and its output is a set of critical network sections which shall be assessed in the subsequent steps.

The following steps are on “object level” meaning that they have to be carried out for each asset on the identified critical network sections. For this purpose, “exposure trees” for each hazard process were developed in order to understand and structure the complex concept of hazard processes, local phenomena and object types.

Fig. 3 shows a schematic illustration of an exposure tree with its components. The exposure trees are tools which contain different steps for analyzing the potential risk for special sections of the infrastructure.

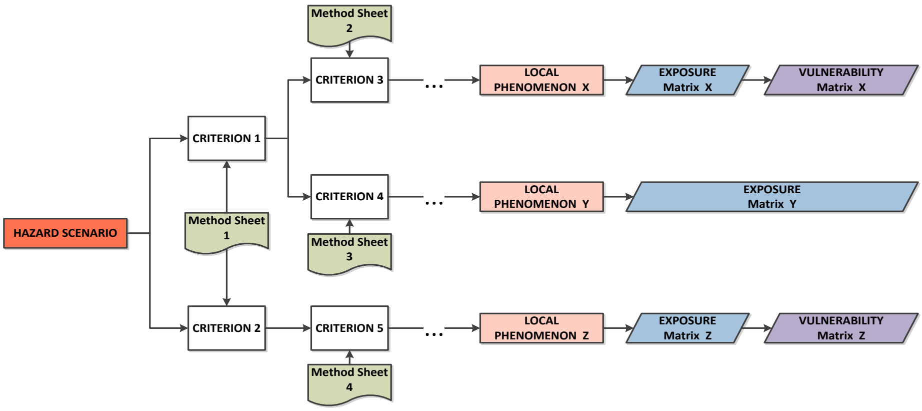


Figure 3. Schematic illustration of an exposure tree

The result of this analysis is a set of local phenomena relevant for the asset under investigation. For each identified local phenomenon an exposure respectively a vulnerability analysis based on predefined assessment matrices is carried out. The result of each of these two steps is a score on which each asset can be categorized. These two values are input for the final step, the risk assessment. First, in the impact assessment both the exposure and the vulnerability score are combined in the Exposure-Vulnerability matrix. The impact of the local phenomena on the asset is again input for the consequence assessment in the impact-consequence matrix. The output of this method is a risk category for each asset with respect to all local phenomena. The developed methodology is based on expert knowledge.

ACKNOWLEDGEMETS

The RAIN**EX** project is funded by the European Commission DG General Home Affairs under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Program (CIPS). The project is implemented by the Federal Highway Research Institute of Germany (BASt) together with project partners from Austria (ILF Consulting Engineers) and Greece (Hellenic Institute of Transport - Centre for Research and Technology Hellas, HIT-CERTH).

REFERENCES

[1] Zurich Insurance Company Ltd – ZIC (2014). Central European floods 2013: a retrospective.

[2] Deutsche Komitee Katastrophenvorsorge e.V. – DKKV (2015). DAS HOCHWASSER 2013 – Bewährungsprobe für das Hochwasserrisiko-management in Deutschland, 2015.

[3] Center for Disaster Management and Risk Reduction Technology – CEDIM (2013). CEDIM Report June 2013 Flood Central Europe, Report 1 – Update 2: Preconditions, Meteorology, Hydrology.

[4] Bundesanstalt für Gewässerkunde – BfG (2013). Bericht BfG-1797 Länderübergreifende Analyse des Juni-Hochwassers 2013.

[5] Bundesanstalt für Gewässerkunde – BfG (2013). Bericht BfG-1797 Länderübergreifende Analyse des Juni-Hochwassers 2013.

[6] AllTraIn Consortium (2015). All-Hazard Guide for Transport Infrastructure – AllTraIn.

REAL-TIME SCREENING OF COUNTERFEIT MEDICINES

Sebastian Engelbrecht[1], Kai Tybussek[1], Lionel Merlat[1] and Bernd Fischer[1]

[1] *sebastian.engelbrecht@isl.eu*
French-German Research Institute of Saint-Louis, 5 rue du Général Cassagnou, F-68301 Saint-Louis Cedex, France

Abstract

In this work we use THz time domain spectroscopy (THz-TDS) for the identification and detection of counterfeit, falsified or poor quality pharmaceutical products. The technology allows access to several aspects necessary for a successful identification. Using THz-TDS it is possible to detect changes in the concentration of a substance, distinguish products of different suppliers, as well as, detect changes in the morphology, like crystal structure or isomeric form.

Keywords: Terahertz, spectroscopy, counterfeit medicines.

1 INTRODUCTION

Counterfeit, falsified or poor quality pharmaceuticals are a growing problem today. Treatments with such medicines results in serious risks of public health as the quality of the medicine impacts the safety and efficiency of the treatment. In addition, the use of counterfeit medicines with insufficient content of the active substance could lead to an increased resistance (especially for antimalarials and antituberculars). These products enter the European market more and more via Internet sales and therefore pose a serious thread. In order to detect such products currently various different approaches are used. Ranging from spectroscopic techniques like ultraviolet (UV-vis.) or Fourier Transform Infrared (FT-IR) spectroscopy to separative techniques which are coupled with an appropriate detection method, like Thin Layer/Gas Chromatography or HPLC/UV-vis.-Diode Array (DAD) [1-3]. Each method currently used has its advantages and also its limitations in terms of skill needs, time-consumption, sample preparation and equipment size and cost. While easy to use and quick methods like simple refractive index testing often suffer from a lack of selectivity/specificity, the more sophisticated methods require a high skill level and/or are very time consuming. Therefore, their use in real life applications, like custom controls, is very limited.

However, a possible solution could be the advent of the terahertz (THz) technology in recent years. The THz frequency range lies in between the microwave and infrared region of light (ranging from ~100 GHz to 10 THz) and therefore in an energy range, where many molecules show characteristic vibrational states, which can be used to identify them [4]. Furthermore, THz radiation has some interesting properties, which could lead to very innovative and novel applications. These properties include the ability to penetrate many non-conducting materials, high spectral sensitivity and to be neither of hazardous nor of ionizing nature. In recent years the THz-technology has undergone a rapid development due to the availability of reliable femtosecond laser systems and THz sources [5]. Using fiber-coupled laser systems the production of small reliable THz systems is easily possible.

This presentation shows the potential of THz spectroscopy to be used to detect and identify counterfeit, falsified, or poor quality medicines. The focus of investigation slightly differs for the different purposes in this project. For the detection of poor quality pharmaceuticals it is crucial to determine the concentration of the active substance. In contrast, for falsified or counterfeit medicines it is more important to identify the active substance and if possible to determine the supplier by means of other characteristic features in the spectra. Crucial for both falsified, as well as poor quality products is the determination of the morphological state of the active ingredient, since the medical effect can depend strongly on it. In this article all of these issues will be discussed by means of chosen examples.

2 EXPERIMENTAL

The experiments in this article were conducted using the commercially available fiber-coupled THz time-domain spectroscopy setup (THz-TDS) Toptica TeraFlash. Details of the system can be found in [6]. A very fast optical delay line allows the almost real-time screening of substances under study. Experiments were done in transmittance geometry. A set of four off-axis parabolic mirrors is used to focus the THz beam on the sample. The dielectric function of a material is determined by first measuring a reference pulse $E_{ref}(t)$ through an empty spectrometer and a sample pulse $E_{sam}(t)$ with the sample of thickness d in the THz path. These time dependent pulses are then transformed into the frequency domain. From the amplitude A(v) and phase Φ(v) of the ratio of the two frequency dependent spectra $E_{sam}(v)/E_{ref}(v)$ the absorption coefficient α(v) and index of refraction n(v) can be calculated using :

$$n(\nu) = 1 + \frac{c}{2\pi \nu d}\Phi(\nu) \qquad (1)$$

$$\alpha(\nu) = -\frac{2}{d}\ln\{A(\nu)\frac{[n(\nu)+1]^2}{4n(\nu)}\} \qquad (2),$$

where c is the speed of light in vacuum and v the frequency of the radiation.

In order to carry out the measurements, pellets of each pharmaceutical mixed with polyethylene (PE) have been fabricated. The respective mixture of substance to PE will be given in the according figures. After both quantities are perfectly mixed, the pellets are created by means of a hydraulic press using about 6 tons of pressure. The diameter of the pellets was fixed to 13 mm. The final thickness of the samples was dependent on the respective substance and was between 0.6 and 0.8 mm.

3 DISCUSSION

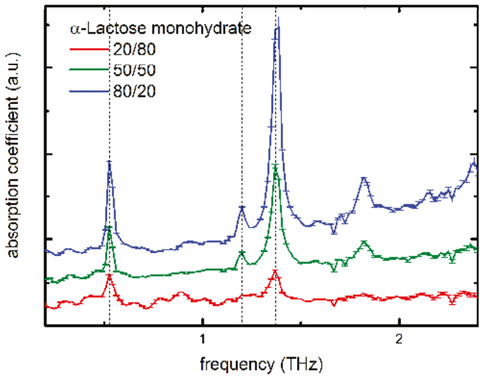


Figure 1: Absorption coefficient of α-Lactose Monohydrate. Legend gives mixture ratio of Lactose to PE in wt.%.

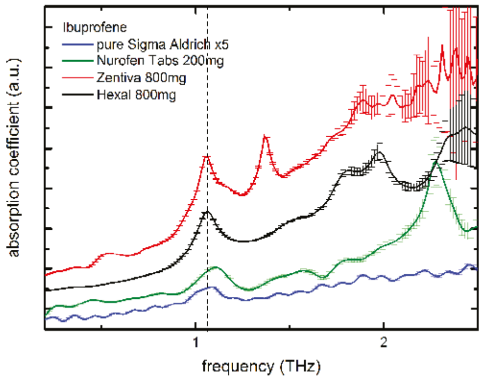


Figure 2: Absorption coefficient of different commercial samples of Ibuprofen.

Figure 1 shows the measured absorption

coefficient for three different samples with varying concentrations of α-lactose monohydrate, a substance commonly used as excipient in commercial pharmaceuticals. As can be clearly seen there are two very strong absorption modes at 0.53 THz and 1.37 THz. Moreover, the higher concentration samples reveal two additional modes at 1.20 THz and 1.82 THz. The most interesting point here is the development of the strength of the modes with the concentration of the substance. As can be clearly seen, the strength of the modes strongly increases with the concentration of the substance. This, however, is just a first qualitative statement. But making a detailed quantitative analysis should therefore allow drawing conclusions about the concentration of the substance under investigation, which is one of the key features regarding the detection of poor quality medicines.

Figure 2 shows the absorption coefficient of different samples of commercially available Ibuprofen. The mixture between substance and PE of the Hexal and Zentiva samples is 50/50, for the Nurofen Tabs it is 75 wt.% substance to 25 wt.% PE and for the pure substance it is 10 wt.% to 90% PE. The low concentration of the pure sample was intentionally chosen, as a very large response was expected. However, it turned out, that the overall concentration in this sample was too low and therefore the obtained signal very small. Nevertheless, also in the pure sample a distinct absorption peak could be identified at 1.06 THz. This peak is also present in all the commercially available Ibuprofen samples and therefore could be attributed as the intrinsic active substance peak. However, in the commercially available products additional peaks are clearly observable. The Zentiva sample (red) shows two additional peaks at 0.53 THz and 1.37 THz, while the Hexal sample (black) shows an additional double peak structure slightly below 2 THz. The Nurofen Tabs (green) show an additional peak at 2.27 THz. The origin of these additional peaks can be easily identified. In commercially available pharmaceuticals the active substance is just one component. As indicated by the weight information given in the legend, the content of the active substance in fact is very small, i.e. 200 mg/800 mg. However, to obtain enough material to produce manageable pills additional excipients are added, which also can have a distinct THz signature. Therefore, those additional peaks arise due to the presence of excipients in the substances. Comparing these results to Fig. 1 in addition directly identifies the excipient in the Zentiva sample to be α-lactose monohydrate. Since these excipients do not have any medical effects, different suppliers can use different excipients, which will lead to different results in the THz spectra. This now shows two advantages of the THz technology. The first is that using our method we indeed can measure both the active substance as well as the excipient in a single measurement, which saves a lot of time compared to advanced chemical analysis. The second is that we can use this property to identify the supplier of a certain pharmaceutical, since its composition of active substance and excipients is in most cases characteristic for a certain product.

Another important point in falsified or poor quality pharmaceuticals is the use of chemically similar but morphologically different substances. In such cases the chemical composition of a substance is the same but the crystal structure, chirality or isomeric form differs. However, the morphology can have a large impact on the medical effect [7]. Therefore, an easy method of determining the morphology is an important factor for detecting falsified or poor quality pharmaceuticals. It has already been shown, that THz-TDS is very well suited to distinguish between different chiral forms of a substance [8]. In this work it will be presented, that THz-TDS is also capable of distinguishing two isomeric forms of a substance. The analysis of the molecular morphology is reported on synephrine which is a common ingredient of slimming products sold on the Internet. The difference between the para- and meta-forms of synephrine is the position of the OH-group on the benzene ring. The para-form has a distinct double peak structure between 1 and 1.5 THz in the absorption coefficient. However, this structure disappears in the meta-form. This clearly proofs, that THz-TDS is indeed able to distinguish different isomeric forms of the same substance. We have also demonstrated the capability to discriminate between two crystal forms of a substance. We report on THz signatures of Paracetamol with a metastable state obtained through a controlled temperature crystallization process. The THz spectrum allows in addition to identify the glass transition temperature.

4 CONCLUSION

THz-TDS is presented as a potential tool for the detection and identification of falsified, counterfeit and poor quality pharmaceutical. Due to an easy availability in Internet market places, such products are a growing problem and pose a serious threat to public health safety. For poor quality medicines an important indicator is the content of active substance in a product. Using the example of α-Lactose Monohydrate it has been shown, that THz-TDS is indeed able to qualitatively determine the content of a substance. Moreover, suitable data analysis algorithms should be able to make a quantitative evaluation possible in the future. Furthermore, it has been shown that THz-TDS is able to detect the active substance and the excipient in an actual medicine simultaneously. In combination with the characteristic suppliers choice of the excipient it is therefore possible to make a distinction between products of different suppliers, which is especially important for falsified medical products. With the example of Synephrine it has been shown that THz-TDS is also a suitable method for the distinction of different isomers, which is peculiarly crucial in pharmaceutical products, since their medical effects strongly depend on their morphology. In addition, it has been shown, that changes in the crystal structure as well as glass transitions can also be measured using THz-TDS. In summary, THz-TDS is a very powerful tool, for the detection of chemical and morphological changes which are crucial in the determination of falsified, counterfeit or low quality pharmaceuticals.

REFERENCES

[1] A. Lanzarotta *et.al.*, *Analysis of counterfeit pharmaceutical tablet cores utilizing macroscopic infrared spectroscopy and infrared spectroscopic imaging,* Anal. Chem. 83(15), 5972-5978, 2011.

[2] T.E. Elizarova *et.al.*, *Using near-infrared spectrophotometry for the identification of pharmaceuticals and drugs,* Pharm. Chem. J. 42(7) 432-34, 2008.

[3] E. Deconinck *et.al.*, *A validated Ultra High Pressure Liquid Chromatographic method for the characterisation of confiscated illegal slimming products containing anorexics*, J. Pharm. Biomed. Anal. 59, 38-43, 2012.

[4] B.M. Fischer *et.al.*, *Chemical recognition with broadband THz Spectroscopy*, Proceedings in the IEEE, 95(8) 1592-1604, 2007.

[5] P.U. Jepsen *et.al.*, *Terahertz spectroscopy and imaging*, Laser Photonics Rev. 166(1) 124-166, 2011.

[6] N. Vieweg *et. al.*, *Terahertz-time domain spectrometer with 90 dB peak dynamic range*, J. Inrared Milli Terahz Waves, 2014

[7] J. Bernstein, *Polymorphism in Molecular Crystals*, Clarendon Press, 2002.

[8] E.M. Witko *et.al.*, *Investigation of the low-frequency vibrations of crystalline tartaric acid using terahertz spectroscopy and solid-state density functional theory*, J. Phys. Chem. A 11(35), 10052-8, 2011.

RADIATION HARDENING OF AUTONOMOUS SYSTEMS

Bodo Gudehus[1] and Jürgen Zabel[2]

[1] *BodoGudehus@bundeswehr.org*
Bundeswehr Research Institute for Protective Technologies and NBC Protection,
Humboldtstrasse 100, 29633 Munster (Germany)

[2]*juergenzabel@t-online.de*
Helmut-Schmidt-University / University of the Federal Armed Forces (HSU), Institute of Automation Technology, Holstenhofweg 85, 22043 Hamburg (Germany)

Keywords: microelectronics - X-Rays, gamma radiation - neutrons, radiation hardening - COTS products - CCD-camera - CMOS-camera

Abstract

The aim of this work was to find radiation hard COTS (Commercial off the Shelf) electronic to construct a functional model of a radiation hardened vehicle with electronic parts which will be able to withstand a high dose of ionizing radiation and neutron fluence. To reach this aim many several COTS electronic devices were tested to get information about their radiation hardness. Most of these tests were already done in former projects and some tests are still to do. Here are the results of tests with neutron and gamma radiation on the vehicle itself, electronic memory devices and camera sensors presented.

1 INTRODUCTION

The wish to use unmanned autonomous vehicles especially in harsh environments is quite old. The employment of such systems offers the possibility to enter hazardous environments without endangering human life during the mission. Autonomous systems shall able to operate self-dependent, without any human controlling. Nowadays, modern microelectronics offers many technical solutions to realize such systems within reasonable costs. The use of electronic systems in heavily radiological contaminated environments is a conceivable scenario of the employment of such systems. Unfortunately, modern electronic includes several risks which endanger its correct function. The nuclear radiation is one of these risks. This ionizing radiation does not only harm men, it also leads malfunctions and finally failures on microelectronics, but it is possible to stave off the failure threshold by selection of components.

The world had to see the results of missing radiation hardened technology at the severe nuclear reactor catastrophe in Chernobyl where several men received a dose which led at least to severe damage to the health of the working people.

2 TESTED DEVICES

At previous tests a lot of devices of microelectronic devices produced by several different manufactures were already tested. None of the tested devices were explicitly declared as radiation hard, all of them were COTS products.

At this project a function model of an autonomous system was tested. It was constructed with selected electronic parts which had mostly shown already in former tests to be radiation hard. Additionally, 4 different small semiconductor camera modules (Table 2.1.) were tested. The major aim here was to find out how the devices behave during and after high accumulated neutron fluence and gamma dose. Four SRAMs (Static Random Access Memory) out of the already tested devices with neutrons were selected for a gamma dose test.

The irradiation tests with gamma rays on the camera modules and more SRAMs will take place in the near future.

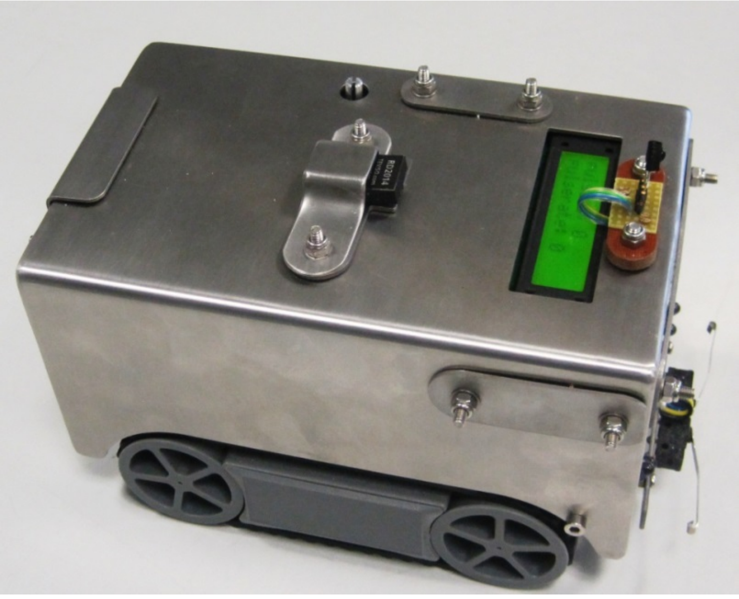


Figure 2 The tested function model of the autonomous vehicle.

Table 2.1 Table of the tested cameras.

	Camera Type	Amount
1	CCD color camera	2
2	CMOS camera	2
3	CCD camera	2
4	CMOS camera	2

(CCD - Charge Coupled Device; CMOS – Complementary Metal Oxide Semiconductor)

3 TEST SET-UP

3.1 NEUTRON TEST

The neutron tests took place at the converter facility (SR10) operated by FRM II at the Heinz Maier-Leibnitz Zentrum (MLZ), Garching, Germany. The neutron tests on the cameras were conducted with neutrons of different kinetic energies. The set-up for the irradiation for fast neutrons, this means neutrons with main neutron energy of about 1.9 MeV, is shown in in figure 3.1.1. Here no moderator was used. To moderate the neutron energy the UUT (Unit under Test) was put into a Polyethylene cover. This resulted in an increase of about 30 – 40 % of the thermal neutrons with an energy of <100 meV at the UUT. Figure 3.1.2 shows the test set-up with a Polyethylene cover which enclosed the UUT mostly. The overall flux was $8.3 \cdot 10^{11}$ n/cm² h on both settings.

Only the camera modules were irradiated with fast neutrons as well as with thermal neutrons. The figures below show the test set-up for the different neutron tests.

Before, during and after the irradiation the rainbow image (Fig. 3.1.1 and 3.1.2) was recorded. The value and amount of corrupted pixels were determined with a computer. This procedure made it possible to judge the hardness of the different cameras.

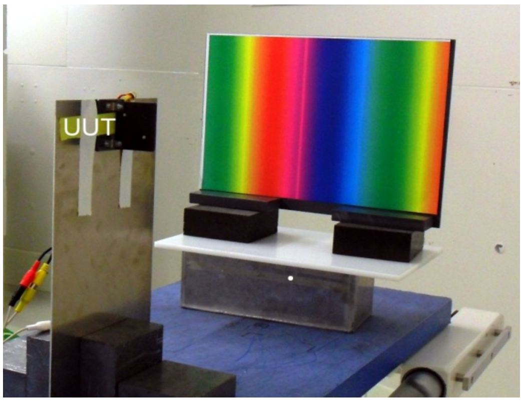


Fig. 3.1.1 Set-up for the neutron test with unmoderated neutrons.

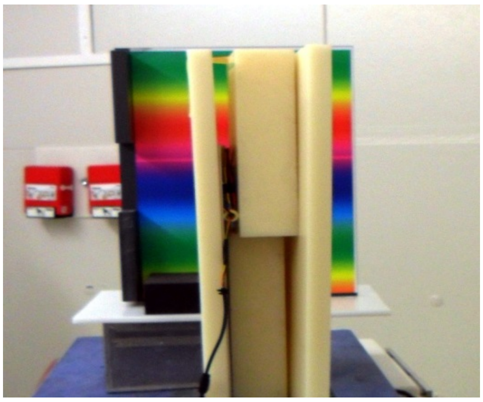


Fig. 3.1.2 Set-up for the neutron test with moderated neutrons.

3.2 GAMMA DOSE TESTS

The test objects were put close to a Co-60 source. The distance between the radiation source and the UUT defined the dose rate and irradiation time respectively. To accumulate the requested gamma dose of 10,000 Gy the irradiation time took at least about two days in the closest distance. During this time the UUT was permanently monitored and checked from time to time respectively.

All these gamma dose tests took place at the Cobalt-60 irradiation facility BSA 2000 at the Bundeswehr Research Institute for Protective Technologies and NBC Protection.

4 TEST RESULTS

4.1 Neutron Test

At first the autonomous vehicle was tested in a circuit with some obstacles, were it self-controlled operated. After six hours this test was finished without any failure. At the second test the vehicle was irradiated in a fix position. The vehicle failed finally at this test. The final accumulated neutron fluence was about $1 \cdot 10^{12}$ n/cm². An optical revolution sensor failed. It was part of the propulsion system.

The results of the tested semiconductor cameras are shown in Figure 4.1.1. It is easily to see that camera 2 showed least pixel errors under all test conditions. The differences between the camera modules were quite big.

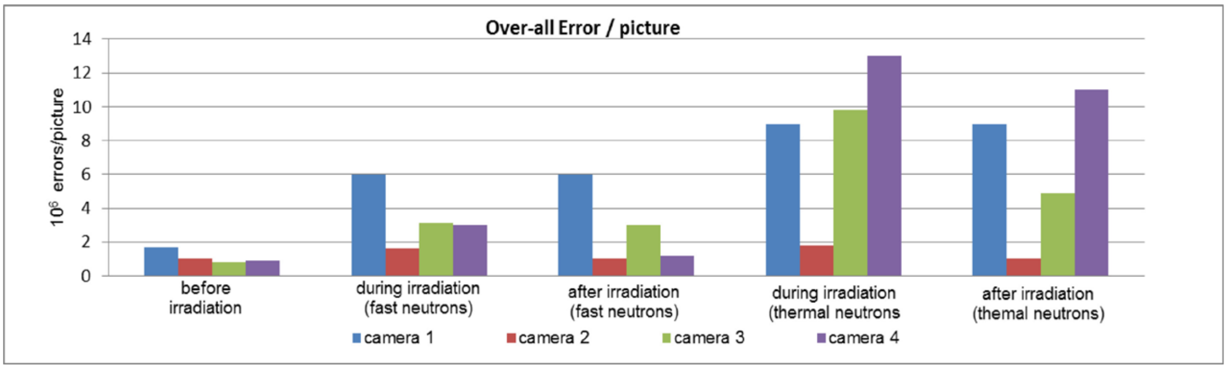


Fig. 4.1.1 Diagram of the pixel errors/picture on the tested camera

4.2 Gamma Dose Test

4.2.1 Gamma Dose on selected SRAM

At this test three SRAMs of different manufacturer were tested until they failed or the requested gamma dose of 10,000 Gy was accumulated. Because of the limited dose rate of 216 Gy/h each test took at least more or even much more than one day. The results are shown in the table below.

Tabl. 4.2.1.1 Test results of the gamma dose test on SRAMs

SRAM	accumulated dose	SEU	failure	gate length	chip thickness	transistor width
SRAM 1	approx. 1300 Gy	no	yes	90 nm	175 µm	890 nm
SRAM 2	approx. 2400 Gy	no	yes	180 nm	165 µm	650 nm
SRAM 3	approx. 10000 Gy	no	no	180 nm	770 µm	1500 nm

The SRAM 3 was the only one which reached the requested dose. The table above shows that there are two significant differences, the chip thickness and transistor width. These differences could be the reason for the very good hardness against gamma dose effects. We have to point out that these results and those of the cameras referred only to the tested devices and are not conferrable to other devices of the manufacturers.

4.2.2 Gamma Dose on the Autonomous System

The autonomous system was irradiated until something failed. It did not reach the level of the requested 10,000 Gy. The applied dose rate was 54 Gy/h in a distance of 20 cm to the radiation source.

During the irradiation the following failures occurred at a level of:

1. approx. 800 Gy	an optical revolution sensor failed.
2. approx. 1600 Gy	the LC-Display of one microcontroller failed.
3. approx. 2650 Gy	an analog voltage controller failed.

After the exchange of the failed parts the two microcontrollers still work. The revolution sensor was part of the propulsion system and failed already at the irradiation with neutrons. For example it is easily to replace with a mechanical sensor and it will surely not fail because of irradiation. To find a replacement for the voltage controller additional tests on such devices are necessary. The LC-Display is not a vital device for the autonomous function itself.

REFERENZES

[1] Zabel, J., Krüger, K.: Untersuchung der Strahlenresistenz aktueller SRAM-Bausteine. Abschlussbericht. E/E590/7Z006/5F0158-3, Hrsg.: Helmut Schmidt Universität, Universität der Bundeswehr, Hamburg 2009.

[2] Zabel, J., Krüger, K.: Untersuchung der Strahlenresistenz aktueller AD/DA Wandlerbausteine. Abschlussbericht E/E590/9Z022/5F0158-2, Hrsg.: Helmut Schmidt Universität, Universität der Bundeswehr, Hamburg 2012.

[3] Messenger, G. C., Ash M. S.: The Effects of Radiation on Electronic Systems. Van Nostrand Reinhold Company, New York 1986

[4] Homes-Siedle A., Adams, L., Handbook of Radiation Effects. Oxford Science Publications, Oxford, New York, Tokyo 1994

UNCOOLED MCT ARRAYS FOR TERAHERTZ IMAGING

J. Gumenjuk-Sichevska[1], Z. Tsybrii[1], V. Zabudsky[1], O. Golenkov[1], M. Sakhno[1],
I. Lysjuk[1], A. Shevchik-Shekera[1], E. Dieguez[2], and F. Sizov[1]
[1] *e-mail: gumenjuk@isp.kiev.ua*
V. E. Lashkaryov Institute of Semiconductor Physics National Academy of Science of
Ukraine (ISP), Nauki av. 41, 03680, Kyiv (Ukraine)
[2] *ernesto.dieguez@uam.es*
Universidad Autonoma de Madrid (UAM), (Spain)

Abstract

Here is considered the conception of two-color broadband detectors based on narrow-gap mercury-cadmium-telluride (MCT) thin layers. Two-colour un-cooled and cooled to 78 K MCT thin layers with antennas were considered both as sub-terahertz (sub-THz) direct detection bolometers, and 3 to 10 μm infrared (IR) photoconductors. The design and dimensions of THz detector antennas were calculated for reasonable detector sensitivity within the 150–300-GHz frequency range. Implications of printed antennas usage in FPA on thick substrate are investigated. Patterns of detector element with planar antenna in the focal plane of the focusing system are studied. Diffraction limited optical system was designed and manufactured with four identical plano-convex aspherical lenses. THz images of objects hidden behind the gypsum plasterboard or foam plastic packing are presented for the radiation frequencies 70, 140, and 275 GHz.

Keywords: THz imaging, focal plane array, mercury-cadmium-telluride bolometers, planar antenna, substrate lens, aspherical lens, hidden objects.

1 INTRODUCTION

The key role in obtaining the information about an environment is played by detectors which should operate in different spectral ranges. It is desirable to have detectors based on the same technological base, or even one material to downrange the manufacturing operations. However, the realization of wide range detectors based on one material is a challenge because the physics of detector sensitivity in different spectral ranges are based on different physical phenomena. For this point of view, the solid solution of mercury-cadmium-telluride (MCT) attracts a particular attention in nowadays due its unique properties in the different spectral ranges originated from the wide variability of its energy band structure. The band-gap of this material is varied by altering the composition from x =1 (CdTe band gap $E_g \approx 1.6$ eV) to $x \approx 0.165$ (band gap $E_g \approx 0$ eV). MCT is the material of choice for many IR focal plane array (FPA) applications. Characteristics of this semiconductor especially for composition $x \approx$ 0.2–0.3 were widely discussed as they as detectors are suitable for λ~0.8-2.5, 3-5 and 8-12 μm regions though they should be cooled, as a rule, to $T \approx 80 - 150$ K (see e.g. [1]). Low leakage currents and high carrier mobility in MCT detectors result in the possible upper limit performance. On the basis of earlier proposed theoretical conception of other detection mechanism compared to IR region, the semiconductor hot electrons bolometers (SHEB) as THz detectors [2] was offered, the sensitive structures based on epitaxial layers of $Cd_xHg1-xTe$ / CdZnTe (x = 0.22 ÷ 0.23) with p-type conductivity were designed and manufactured [3]. These SHEB detectors have noise equivalent power NEP ≈ 10^{-10} W*Hz$^{-1/2}$ at the ambient temperature in the frequency range of 0.0037-1.54 THz.

For THz imaging it is still a challenge yet to create multi-element detector focal plane array (FPA), which are operating at the ambient temperatures. Such type new generation of multi element focal plane arrays is expected to enable real-time imaging, reduce the scanning time and increase the information capacity and reliability of the video system by eliminating mechanical scanning components. Currently, there are no large-format THz-range FPAs with good spatial resolution capable to real-time operation. In this work we consider the conception of two-color broadband detectors based on narrow-gap mercury-cadmium-telluride (MCT) thin layers. Two-color un-cooled and cooled to 78 K MCT thin layers with antennas were considered both as sub-terahertz (sub-THz) direct detection bolometers, and 3 to 10 μm infrared (IR) photoconductors.

2 MCT DETECTOR ARCHITECTURE, IMPLIMENTATION, AND TESTING

To fabricate the detectors, we prepared $Hg_{1-x}Cd_xTe$ (x ~ 0.2...0.32) layers grown using liquid-phase epitaxy (LPE) with the initial thickness of the layers up to 20 μm. MCT layers were grown on $Cd_{1-y}Zn_yTe$ (y ≈ 0.03 - 0.05) substrates. The technological route of these structures manufacturing consisted of the following stages: preliminary chemical preparation of MCT surface; formation of CdTe passivation layers; multilayered photolithography processes; metallization by the lift-off photolithography or etching the mesa-structures methods to create planar contacts, samples cutting, bonding of samples for subsequent investigations. The design and dimensions of THz detector antennas were calculated for reasonable detector sensitivity within the 150–300-GHz frequency range. Implications of printed antennas usage in FPA on thick substrate are investigated. Here was chosen the simple bow-tie antenna with 90^0-divergence angle of side of antenna from the center of sensitive element. At the same time, such construction of detector allows using symmetric and identical area current contacts (antenna blades) for photocurrent registration in IR spectral region. Sensitive layers thicknesses (~5 μm) were optimized for IR and sub-THz response.

In this work, an active terahertz (THz) imaging model with 8 detectors in each linear un-cooled detector array detectors have been developed and exploited. Photo of assembled detector chips on the testing board is shown in Fig. 1.

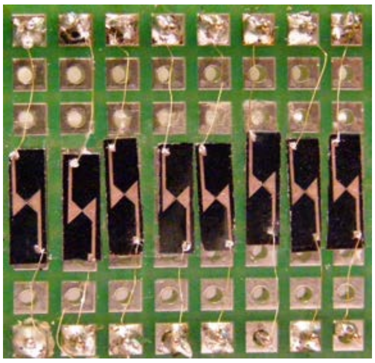


Fig.2. Photo of MCT chips assembled on the testing board.

The active THz-imaging system consisting of the source combined with the horn emitter, lens system, scanning mirror, linear detecting array, and electronic board with circuits for detectors biasing, multiplexing and amplification of the output signals have been designed and manufactured. The first pair of lens focuses the radiation on the object; the second focuses it to THz detector. Ultra high molecular weight polytetrafluoroethylene (PTFE) with a refractive index of 1.43 within wide wavelength region was selected as lens material. Aspherical lenses were chosen because a single aspheric lens can replace much more complex multi-lens system. Diffraction limited optical system with four identical plano-convex aspherical lenses (hyperboloid) was designed and manufactured.

The IR photo-response of the detector system was obtained using globar as the source of IR radiation with the temperature $T \approx 1600^0$ C and IR monochromator as a spectral instrument with spectral resolution $\Delta\lambda \approx 0.1$ μm. Detectors were biased with I_{bias} = 50 – 100 μA. The IR response (as well as sub-THz one and the noise level) was measured by lock-in amplifier. The detectors used as an IR photoconductor showed the responsivity at the temperatures T = 78 K and 300 K with signal-to-noise ratio S/N ≈ 750 and 50 respectively [4].

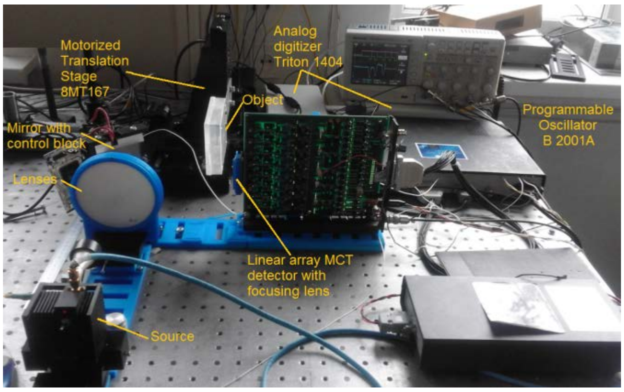

Motorized Translation Stage 8MT167
Analog digitizer Triton 1404
Object
Programmable Oscillator B 2001A
Mirror with control block
Lenses
Linear array MCT detector with focusing lens
Source

Fig.2. Photo of THz/sub-THz vision system's experimental set-up.

For this detector used for sensing of a sub-THz radiation at ν = 140 GHz [4], the best measured noise equivalent power values were $NEP_{300K} \approx 4.5 \cdot 10^{-10}$ W/Hz$^{1/2}$ and $NEP_{78K} \approx 5 \cdot 10^{-9}$ W/Hz$^{1/2}$. The noise level was measured using the lock-in amplifier Stanford SR 830, for which the intrinsic input noise is 6nV/Hz$^{1/2}$. The important characteristic of THz detectors is their response time that is rather large in THz thermal detectors (uncooled bolometers or piezoelectric detectors, τ ~ 1...10 ms). We measured the MCT HEB photoresponse with the 70-GHz pulse generator with 100-ns pulse duration. Relaxation time was defined by time decay of the photoresponse by *e* times and gave the value $\tau \approx$ 90 ns.

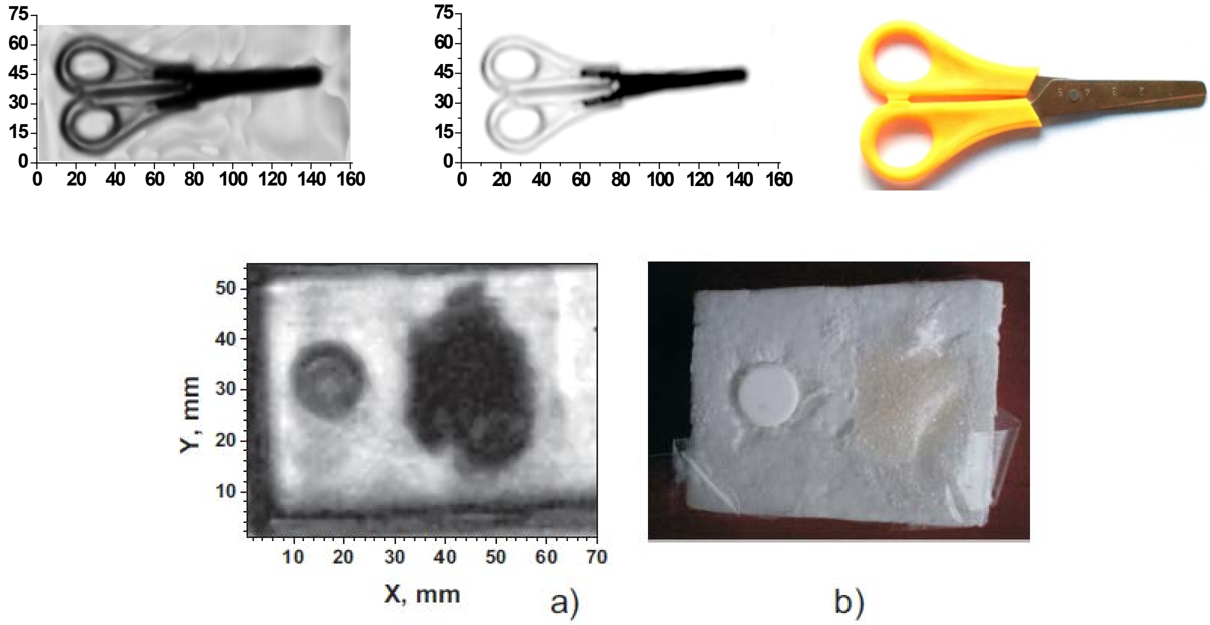


Fig.3. a) Sub-THz image (ν = 140 GHz, P ≈ 15 mW) of scissors in non-transparent envelope in transmission mode: linear brightness scale; logarithmic brightness scale, and visible image. b) The tablet and powder sugar, hidden in a hollows in a foam plastic: THz image (ν = 275 GHz, backside illuminated) and front side visible image.

It was proved that for known un-cooled detectors there is no feasibility of passive imaging by direct detection, as NEP does not satisfy the requirements for THz system passive imaging. For un-cooled MCT detectors from the arrays used for sensing of sub-THz radiation at v=140 GHz the noise measured was about 30 nV·Hz$^{-1/2}$ at 3 mA bias and corresponding values of NEP were within $NEP_{300K} \approx (2.6 \div 9) \cdot 10^{-10}$ W/Hz$^{1/2}$. The system can locate and image hidden objects that are either absorbing or reflecting in the THz/sub-THz region, and is capable of active imaging, e.g., of postal mailings. Examples of sub-THz images obtained using the system developed are shown below.

Traditionally, THz images are obtained using reflected radiation or radiation passed through an object, inhomogeneity of which leads to formation of the contrast picture. To increase information ability of working THz prototype an active THz system has been developed, the design of which allowed to receive images of objects in a configuration of the objects "transmission and reflection" at the same time. Proposed technique of obtaining images in THz/sub-THz spectral region with use of a method of a transmission and reflection in the same time allows separate metallic parts of the objects from others. In Fig.3 THz images of objects hidden behind the gypsum plasterboard or foam plastic packing are presented for the radiation frequencies 14 and 275 GHz.

3 CONCLUSIONS

In this project, an active terahertz (THz) imaging model with a small number of detector in linear arrays based on narrow-gap HgCdTe semiconductor has been developed and exploited. Mercury-cadmium-telluride (MCT) semiconductor thin layers grown by liquid phase epitaxy or molecular beam epitaxy methods on high-resistive CdZnTe or GaAs substrates, with bow-type antennas both located on these high permittivity substrates, have been considered as sub-terahertz direct detection bolometers. Their room temperature noise equivalent power (NEP) at the frequency v ≈ 140 GHz reached the value ~ 2.6 10^{-10} W/$Hz^{1/2}$ satisfying the requirements for active imaging THz systems. Aspheric lenses used for obtaining the images in sub-THz spectral region were designed and manufactured. Imaging data taken at 140 and 270 GHz with these detectors have been presented. Developed model of MCT/CZT THz/sub-THz detectors showed the possibility to operate in 150- 300 GHz spectral range. THz images of some hidden objects (e.g., a bullet, a lighter, scissors, medical pills, sugar and different small area plastics (several mm) considered as imitating substances of explosives placed in non-transparent envelopes, foam plastic packing and behind gypsum plasterboard with d=12 mm) have been obtained. THz active optical system with using of linear array of uncooled HgCdTe detectors can be implemented for recognition the matter or their shape, any hidden and explosives concealed behind non-metal packaging with dimensions up to several mm or larger.

NATO Project NUKR.SfP 984544 supported this research.

REFERENCES

[1] A. Rogalski, *Infrared Detectors,* 2nd. Ed., New York, Taylor & Francis, Boca Raton (2011).

[2] V. Dobrovolski, F. Sizov, “THz/sub-THzbolometer based on electron heating in a semiconduc-tor waveguide”, *Optoelectr. Rev.*, **18**, # 3, p. 250-258 (2010).

[3] V. Zabudsky, F. Sizov, N. Momot, Z. Tsybrii, N. Sakhno, S. Bunchuk, N. Michailov, and V. Varavin, “THz/sub-THz direct detection detector on the base of electrons/holes heating in MCT layers,” *Semicond. Sci. Technol.* **27**, 045002 (2012).

[4] F. Sizov, V. Zabudsky, S. Dvoretskii, V. Petryakov, O. Golenkov, K. Andreyeva, Z. Tsybrii. Two-color detector: Mercury-Cadmium-Telluride as a terahertz and infrared detector, *Applied Physics Letters*, **106**, p. 082104-1 – 182104-4 (2015); doi: 10.1063/1.4913590.

SENSE4METRO: A BI-NATIONAL MULTI-DISCIPLINARY PROJECT FOR MONITORING UNDERGROUND METRO ENVIRONMENTS IN DISASTER EVENTS

Scott Kempf[1], Frank Schäfer[1], T.G. Sitharam[2], Per Kleist[3], Wilfried Gräfling[3], Neil Ferguson[4], Tim Stuchtey[4], Tanushree Chakraborty[5], Vasant Matsagar[5] and Norbert Gebbeken[6]

[1] *scott.kempf@emi.fraunhofer.de*
Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Eckerstr. 4, 79104 Freiburg (Germany)

[2] *sitharam@civil.iisc.ernet.in*
Indian Institute of Science, Dept. Of Civil Engineering, Centre for infrastructure, Sustainable Transportation & Urban Planning (CiSTUP), CV Raman Avenue, Bangalore – 560 027 (India)

[3] Berlin Fire Brigade, Rathausstr. 70-72, 12105 Berlin (Germany)

[4] Brandenburg Institute for Society and Security (BIGS), Rudolf-Breitscheid-Str. 178, 14482 Potsdam (Germany)

[5] Indian Institute of Technology Delhi, Dept. Of Civil Engineering, Hauz Kaus, 110016 New Delhi (India)

[6] University of the Armed Forces, Institute of Engineering and Structural Mechanics, W-Heisenberg-Weg 39, 85577 Neubiberg (Germany)

Abstract

The current trend towards global urbanization and the resulting migration to underground mass transportation has resulted in an increase in security related challenges, whether due to terror attacks or natural disasters. Such mass transportation systems are highly vulnerable and require new approaches to minimize vulnerabilities and limit damage in the event of disasters.

Since 2015, several German and Indian institutions have been engaged in the bi-national and multi-disciplinary project SenSE4Metro as part of the “Indo-German Initiative for Civil Security Research (IGI-CSR)”. The overall objective of the project is to improve the security of persons in urban underground trains and stations in emergency situations, specifically terrorist attacks and natural disasters.

This paper presents the multi-disciplinary approach applied, a discussion of the state-of-the-art and the initial results of the project, including the threat and requirements analysis.

Keywords: structural monitoring, energy harvesting, critical infrastructure.

1 INTRODUCTION

Global urbanization contributes significantly to the economic, social and cultural development of nations. At the same time, the requirements for urban transportation systems are increasing. The result is a migration to underground mass transportation systems, whereby new security-related challenges arise. The most recent examples of terror attacks [Madrid, 2004 and London, 2005, Moscow 2010, Minsk 2011, Brussels 2016] and natural disasters [Prague 2002, New York 2012] or other fatal accidents

[Valencia 2006, Moscow 2014] demonstrate the high vulnerability of mass transportation systems. In order to minimize such vulnerabilities, intelligent situational awareness systems and a better understanding of the behavior of passengers and rescue forces during such events are necessary.

2 PROJECT OBJECTIVES

The overall objective of the project is to improve the security of persons in urban underground trains and stations in emergency situations and catastrophes. The emergencies and catastrophes in the context of the proposed project are the result of:

- Terrorist attacks on underground trains and train stations leading to casualties and fatalities as well as massive mechanical damages in the building structure of the underground construction,
- Natural disasters such as earthquakes and flooding, as well as other large-scale disasters leading to structural damages, water ingress, outbreak of fire and/or smoke generation.

3 MULTI-DISCIPLINARY APPROACH

The multi-disciplinary approach to attaining this objective involves the engagement of consortium institutions in research ranging from basic material physics to technological development to individual and group sociology. The project is organized in four research areas defined as specific research objectives:

Analyses of metro environments in terms of vulnerability to explosions, carried out by combining physical material experiments with numerical models of blast effects and propagation, the objective of which being the development of solutions for minimizing the effects of explosions both in terms of prevention of casualties and mitigation of damage to the load-bearing structure.

The development of a security management and emergency response system composed of a wireless sensor network and an information distribution system, undertaken in order to acquire relevant situational monitoring data in tunnels, assess emergency situations and levels, calculate safe access and escape routes and effectively communicate the necessary information to the participating stakeholders (metro operators, rescue forces and passengers).

Sociological and psychological studies of first responder and general population groups through the use of behavioral games, providing insight into and ultimately recommendations for the improvement of rescue protocols and first responder training and the development of man-machine interfaces of emergency management systems.

An historical assessment of social behavior in underground installations in extreme situations, focused on the influence of demographics, as well as national and sub-cultures, on mass behavior, incident management and disaster preparedness in order to design improved communication procedures going forward.

The research in all four areas is regarded in an international context and the consideration of differences in culture, construction and environment are considered central to the advancement of the state-of-the-art offered by the project.

4 STATE-OF-THE-ART

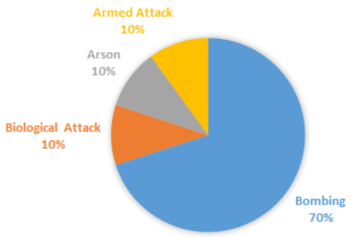
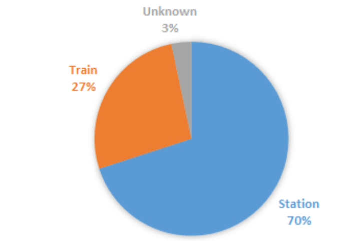
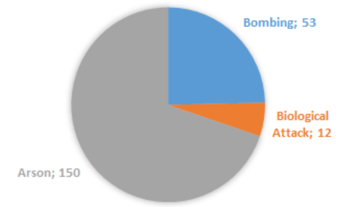
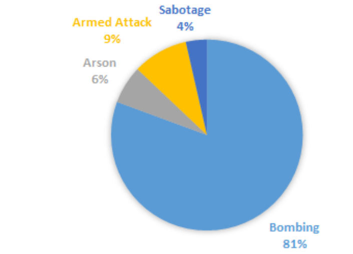
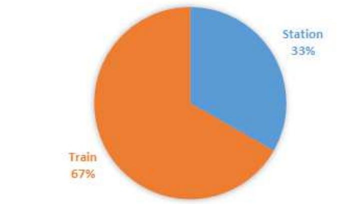
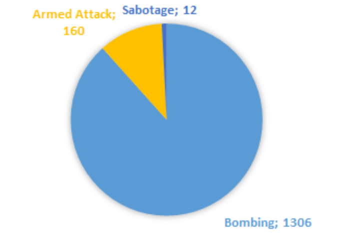
The development of real-time information for passengers and emergency response forces requires precise knowledge of the situation and environment, train location structural health and conditions and movement of threat situations. With the exception of the release and spread of biological agents [1], such comprehensive situational awareness information for underground trains and stations does not currently exist. The development of system to provide such information represents a significant advancement on the state-of-the-art, as far as mitigating damage during emergency events.

5 THREAT ANALYSIS AND INITIAL SYSTEM DESIGN

A past assessment of terrorist attacks against underground, tunnel and rail infrastructure was performed with the intention of gaining an understanding of the trends in strategy, targeting and effectiveness of such attacks. The assessment was performed using the EMI developed Terror Event Database (TED) and TED Analysis Software (TEDAS). The goal of the assessment was the establishment of event scenarios for the configuration of the security and emergency management system.

The database contains reports of 339 attacks on underground, tunnel and rail infrastructure since the early seventies. The attacks were assessed based on tactic, target, number of casualties and, depending on the tactic, success rate of detonation. The tactics involved: explosives, chemical or biological agents, arson (fire or firebombing), armed attacks and sabotage. The distribution of the data regarding the terror event assessment can be seen in Table 1.

Table 1: Distribution of past terrorist events and fatalities by tactic and target.

	Events by Tactic	Events by Target	Fatalities by Tactic
Underground			
Rail Infrastructure			

It can be observed from the data that both biological and arson attacks in underground environments demonstrate significantly higher casualty rates than other tactics, or the same tactics in the above ground environment. Whereas the deadliest attack tactic in the above ground environment is bombing, averaging approximately 6.5 deaths per successful detonation, in the underground area, a single biological attack and a single arson attack resulted in 12 and 150 deaths respectively.

From the results of the threat analysis, a series of scenarios were defined and rated in terms of relative probability and criticality, from which bombing and arson attacks were considered foremost, due to the combination of frequency and criticality (attacks with biological agents have been assessed in previous studies and lie outside the scope of this project). Although not indicated in the results above, an assessment of the individual events indicated that criticality (in terms of deaths per event) was higher in the event that underground trains, as opposed to underground stations, were targeted, can likely be attributed to the enclosed nature of the environment. As the project is not limited to terrorist events, earth quakes, flooding and general malfunctions have also been added as scenarios.

The security and emergency management system has been tentatively designed as a series of tunnel-based energy-autarkic wireless sensor networks (WSNs), which report to a central security management and emergency response system (SMERS) server, which handles the distribution of the appropriate information to the relevant invested parties (metro operators, first responders and, tentatively, passengers). The WSN concerns itself primarily with the gathering of raw environment-related situational data. From the raw data, the developed data processor establishes the situational data regarding alarm levels, tunnel segment traversability, and safest access / escape routes based on stranded train location. A superficial system data flow can be visualized in Fig. 1.

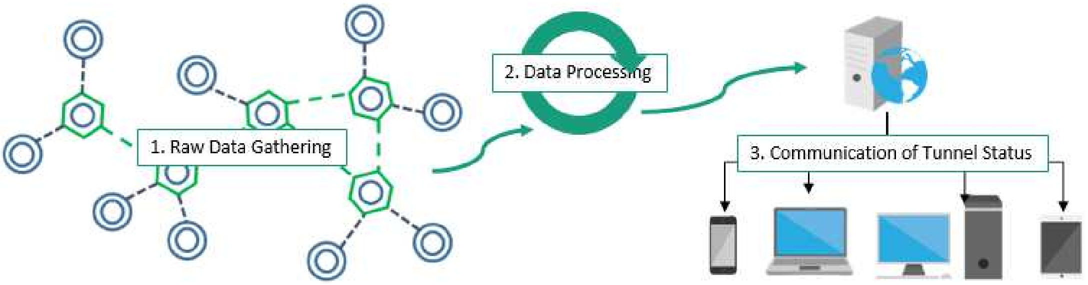


Figure 1: Simplified SMERS data chain.

6 CONCLUSIONS / OUTLOOK

The increased vulnerability of underground transportation infrastructure can be demonstrated anecdotally (see “Introduction”) and statistically (“Threat Analysis”). In general, due to its enclosed nature, the tunnel environment provides significant obstacles to the safe and efficient evacuation of passengers following an event.

The improved understanding gained from the novel multi-disciplinary approach shall in the future lead to a more efficient response to potentially fatal emergency events in underground metro environments. This improved understanding is attainable through the integration of results of the individual tasks, specifically an improved understanding of: potential threats and event scenarios; the physical effect of explosions in underground environments; the effect of rescue and training protocol on first responders; and the behavior of passengers in extreme situations.

The results of these individual studies, informed additionally by cultural differences between Germany and India, will inform the design of the security management and emergency response system and be combined with the developed demonstrator for the evaluation of new rescue protocols and the performance of large-scale field tests in an underground metro environment.

REFERENCES

[1] Koch, R. and Plaß, M. (2009). *Optimising Rescue Operations in Subways: the OrGaMIR Project*. Future Security 4th Security Research Conference Karlsruhe, pp. 11-16.

AMBIENT MASS SPECTROMETRY: DIRECT ANALYSIS IN REAL TIME (DART) VERSUS DESORPTION ELECTROSPRAY IONIZATION (DESI)

Dr. Vanessa Kunde

drvanessakunde@bundeswehr.org
Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS),
Humboldtstraße 100, 29633 Munster (Germany)

Abstract

A first approach to unknown samples, potentially contaminated with toxic substances or explosives, usually employs screening techniques for the estimation of further analytical steps. Within the following laboratory procedures, depending on the matrix, possibly time consuming preparation of the complex mixtures is essential to gather the required information e.g. on the detailed composition or forensic aspects. A recent innovation in mass spectrometry is the ability to record mass spectra on ordinary samples with reduced sample pretreatment or even without sample preparation. Two suitable ionization methods, DESI (desorption electrospray ionization) and DART (direct analysis in real time) were introduced in 2004 and 2005. The so-called ambient mass spectrometry provides numerous (forensic) applications in analysis of toxic industrial compounds (TIC), chemical warfare agents (CWA), explosives, drugs, fingerprints, etc.

Keywords: ambient mass spectrometry, electrospray ionization, desorption ionization, chemical warfare agents, explosives

1 INTRODUCTION

Explosive or chemical warfare agent detection requires techniques that are fast, sensitive, selective and capable of analyzing a large number of samples. The main advantage in comparison to other methods using DART or DESI for ionization in combination with mass spectrometry is its very high specificity. It does not require any surface pretreatment and can be formed under ambient conditions.

2 INSTRUMENTATION

2.1 DART

DART is an atmospheric pressure ionisation technique allowing direct measurements of solids or liquids without prior sample treatment. The ionisation process takes place directly from a sample surface (e.g. from the tip of a cotton swap) in a heated stream of ionised helium, which is directed towards the inlet of the mass spectrometer. DART ionisation generally yields reproducible compound spectra devoid of adduct formation. Consequently, full-scan mass spectra reveal protonated molecule ions that are individually isolated and fragmented for a comprehensive database comparison.

2.2 DESI

DESI is closely related to the commonly used electrospray ionisation (ESI) process, though sample ionisation occurs on a designated surface area. Analytical imaging methods provide the ability to examine untreated sample surfaces, or to visualise preliminary thin layer chromatography (TLC) studies.

2.3 High Resolution Mass Spectrometry (HRMS)

HRMS is the method of choice for non-targeted screenings as it contains the maximum amount of information in its datasets. Combining DART or DESI with Orbitrap HRMS offers:

- Highly sensitive targeted evaluation of full-scan high resolution data, also retrospectively, without additional need for specifically designed targeted experiments.
- High resolving power (up to 240,000 at m/z 400), high mass accuracy (no internal celebrant needed), high dynamic range (full-scan experiments) and high sensitivity.
- Full-scan HR-analysis combined with data dependent MS/MS capabilities (specifically MS/HRMS) facilitates mass spectral identification of unknown compounds (e.g. reaction products of CWC scheduled chemicals).

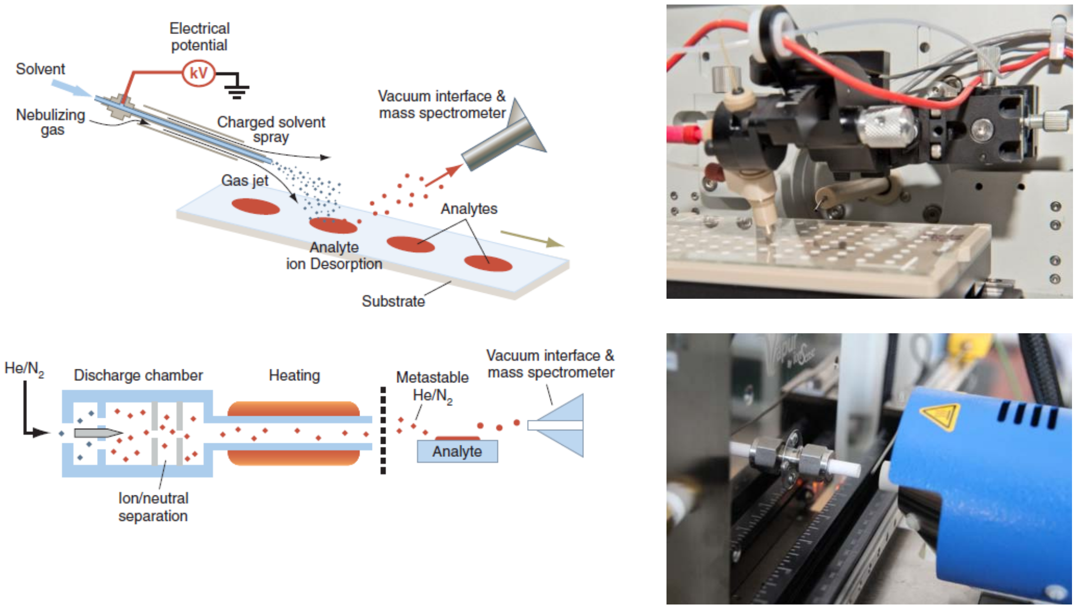


Fig. 1: Schematic diagrams and image-sections of the DESI (top) and DART (bottom) ion sources. [1]

3 ANALYTICAL APPLICATIONS

One imaginable field of an application is the analysis of improvised explosive devices (IED) with or without extra load. That means the “classical” IED and the Chemical IED (IED filled with CWA or TIC). So one focus of the investigations was the proof of contamination by explosives in different scenarios. It was possible to detect TNT in lower nanogram amounts in surface swabs out a car, whose driver had access to an explosive processing area before. In a next step the investigations were extended to simulating substances representing chemical warfare agents to estimate the further potential of DART and DESI.

REFERENCES

[1] Cooks, R.G., Ouyang, Z., Takats, Z., Wiseman, J.M. *Science* 311 (2006)

A NOVEL SIMULATION APPROACH FOR CRITICAL INFRASTRUCTURES BASED ON TIME DOMAIN METHODS

Sebastian Lange and Martin Schaarschmidt and Frank Sabath

[1] *sebastian1lange@bundeswehr.org*
Bundeswehr Research Institute for Protective Technologies and NBC Protection,
Humboldtstrasse 1 29633 Munster (Germany)

Abstract

The wideband excitation of critical infrastructures with electromagnetic high frequency fields is examined due to security questions like protection from interference, lightning protection, radiation, etc.. Here, computational electromagnetics (CEM) gains importance by the constantly rising efficiency of economically available computer hardware like massively vectorial and parallel working graphic processing units.

The numerical simulation of wideband electromagnetic interference puts a strong emphasis on methods in time domain. The stable subgrid finite difference time domain method gives the opportunity for an efficient adaptive discretization in time and space. The MPI parallelization and in particular the GPU as well as multi-GPU implementation of this method provides a simulation tool of high benefit.

In contrast to standard FDTD the subgrid FDTD allows an arbitrary local grid refinement. The number of cells therefore may be reduced while the representation of small structures is given at the same level of detail. This allows the consideration of metallic reinforcements in concrete wall structures.

Keywords: FDTD, CEM, Critical Infrastructure, Subgrid, Reinforcement, Concrete Wall Structure.

1 INTRODUCTION

The numerical description of wideband electromagnetic interaction for real world applications increases the need for stable, robust, and flexible time domain based methods. The modelling of strongly inhomogeneous domains like anatomical human models or real infrastructures yields in sophisticated computational applications. For that reason high flexible volume dicretizing methods like finite elements (FEM), finite differences (FDTD) and finite volumes (FVM) are the most important in time domain regime.

Since computing power became more widely available numerical methods where used to solve practical engineering and scientific problems. Both the numerical methods and high performance computers are still under further development. The finite difference time domain method is one of the most evaluated methods in CEM.

An optimized parallelization is needed in order to enable the application of an approved subgrid FDTD code to large and complex problems. The goal of paralleization is a compromise between the minimization of interprocess communication and load balancing between the processor cores. This compromise is highly application dependent, so that the parallelism essentially depends on the spatial partitioning. This is fulfilled by a common message path interface (MPI) parallelisation.

A multi-GPU parallelization is the next step in the improvement of the performance using a combination of the GPU implementation with the distributed memory parallelization. A corresponding hardware concept was found.

2 FINITE DIFFERENCE TIME DOMAIN ON SUBGRIDS

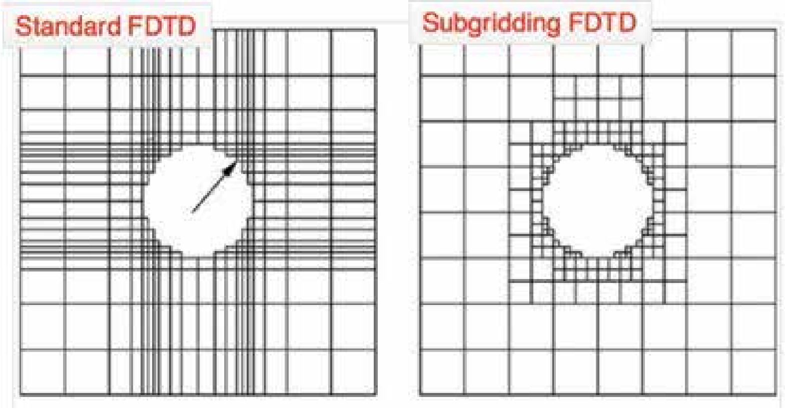


Figure 1 Comparison between standard and subgrid FDTD

The method presented here was published for the first time in 1997 [2]. In contrast to a standard formulation the subgrid FDTD allows an arbitrary local refinement of the grid see fig. (1). This allows a reduction of the number of cells and a representation of small structures at the same level of detail like a high resolution standard FDTD grid. Furthermore a local time stepping is possible in this refinement strategy. Within standard FDTD the timestep is determined by the smallest cell. The timestep is determined by the smallest cell in a standard FDTD. The subgrid FDTD approach allows a local timestepping which is adapted to the smallest cell size of the particular subgrid level. Figure 2 displays the subgrid FDTD of the concrete reinforcement wall of the EMOM.

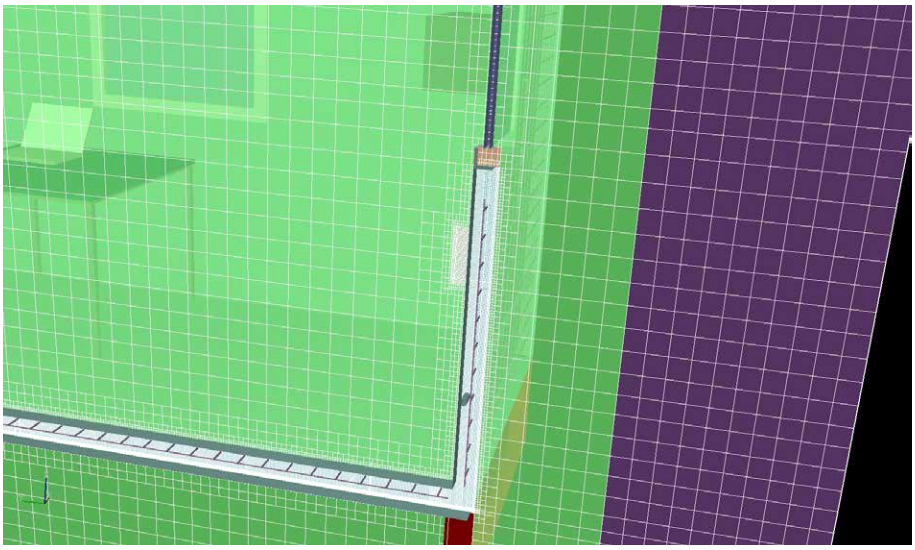


Figure 2 Subgrid representation of concrete and reinforcement

3 HPEM EXPOSURE OF CRITICAL INFRASTRUCTURE

The Bundeswehr Research Institute for Protective Technologies and NBC-Protection (WIS) developed an office module.

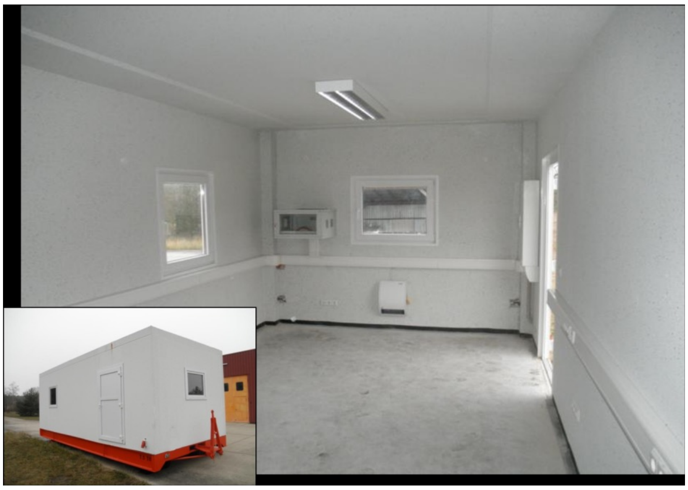


Figure 3 The Electromagnetic Office Module

This so called electromagnetic office module (EMOM) is made up of reinforced concrete and is equipped with electrical power and data network installation, see fig. 3. One standardized testing setup is the high-altitude electromagnetic pulse (HEMP) which is based on the waveguide simulator (DIESES). DIESES produces a well-defined pulse according to VG 95371-10 with a 50 kV/m peak amplitude and a rise time of 25 ns. A plane wave excitation with the standardized pulse form is the corresponding regime in FDTD simulations.

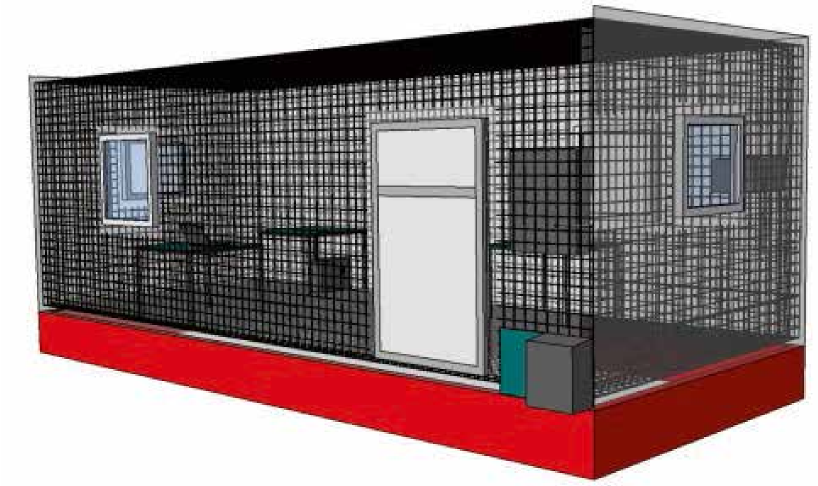


Figure 4 CAD Model of the EMOM

Since the reinforcement is not specified the EMOM was re-engineeried using technical drawings. For that reason some assumptions are made in the CAD model, see fig 4.

The electric field inside of the EMOM is computed. As an example for the results the electric field at 90MHz is given in figure 5.

The calculation of the exposure of a HEMP-event is presented here as a first numerical result. It is proofed, that a direct consideration of reinforcements is possible. This allows further survey of critical infrastructures and more complex scenarios using bigger building models. This will allow a preparation of virtual tests in order to prepare experiments of critical infrastructures.

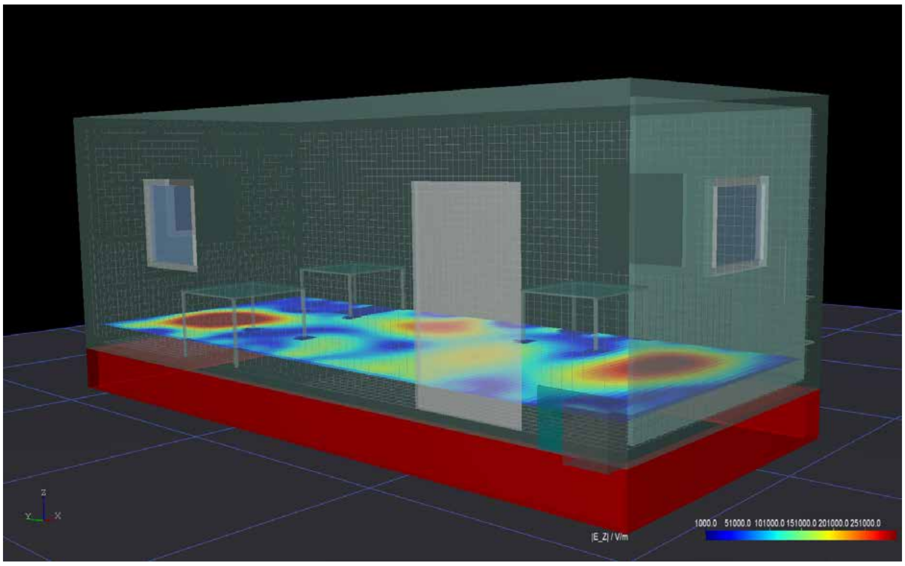


Figure 5 Electrical Field inside of the EMOM

4 CONCLUSION AND FUTURE WORK

A stable subgrid FDTD method has been presented here. A general idea behind the parallelization and acceleration by GPUs was presented. Numerical examples present the high flexibility of the subgrid approach.

A high sensitivity to the design of the reinforcement was found using different assumptions about the EMOM. For that reason some assumptions will be proofed and the CAD model corrected. Furthermore the EMOM will be equipped with a 19” Rack server. This should allow more realistic surveys of data center scenarios. A cable solver is under development in order to compute the irradiation of EM fields into the cabling of the EMOM.

REFERENCES

[1] A. Taflove and S.C. Hagness “Computational Electromagnetics”, Artech House, 3rd edition, 2005

[2] J. Ritter and F. Arndt, ”A generalized 3D subgrid technique for the finite-difference time domain method”, IEEE MTT-S, International Microwave Symposium Digest, vol. 3, pp. 1563–1566, 1997.

[3] J. Ritter and F. Arndt, ”Fast subgrid FD-TD matrix pencil technique for the rigorous analysis of resonant 3D microwave structures”, IEEE MTT- S, International Microwave Symposium Digest, vol. 3, pp. 1271–1274, 1998.

[4] S. Sevskiy, Multidirektionale logarithmisch-periodische Indoor-Basisstationsantennen, Dissertation, University of Karlsruhe, 2006.

[5] ”IEC 61000-4-20, Electromagnetic compatibility (EMC) - Part 4-20: Testing and measurement techniques - Emission and immunity testing in transverse electromagnetic (TEM) waveguides”, International Electrotechnical Commission, Edition 2.0, 2010-08, ISBN 978-2-88912-149- 6.

[6] Ritter, J., Benjes, M., Murso, M., Wulf, D., and Lange, S. “A Stable Subgridding Finite Difference Time Domain Method on Multi-GPU Cluster”, EMC Europe 2015, Dresden, GermanyMETIS partition

[7] Christ A, et al: The Virtual Family – Development of surface-based anatomical models of two adults and two children for dosimetric simulations, Physics in Medicine and Biology, 55(2): N23-N38, 2010.

A LEGALLY COMPLIANT MULTI-SENSOR SYSTEM FOR SECURITY ENHANCEMENT AND REAL-TIME SITUATION AWARENESS IN COMPLEX SCENARIOS

Frank Pagel[1], Jürgen Moßgraber[1], Igor Tchouchenkov[1], Jürgen Metzler[1], Manfred Schenk[1], Matthias Kollmann[1], Eduardo Monari[1], Carsten Decker[2], Roger Jäger[2], Robert Weinhold[3], Frank Meyering[4], Martin Gehrt[4], Michael Mell[5], Rüdiger Czech[6], Marco Krüger[7] and Katrin Geske[7]

[1] *{frank.pagel, juergen.mossgraber, igor.tchouchenkov, juergen.metzler, manfred.schenk, matthias.kollmann, eduardo.monari}@iosb.fraunhofer.de*
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB)
Fraunhoferstr. 1, 76131 Karlsruhe (Germany)

[2] *{carsten.decker, roger.jaeger}@polizei.bund.de*
German Federal Police, Direktion Bundesbereitschaftspolizei,
Niedervellmarsche Straße 50, 34233 Fuldatal (Germany)

[3] *r.weinhold@uni-kassel.de*
University of Kassel, Research Group *provet*,
Pfannkuchstr. 1, 34109 Kassel (Germany)

[4]*{meyering, martin.gehrt}@imst.de*
IMST GmbH,
Carl-Friedrich-Gauss Straße 2-4, 47475 Kamp Lintfort (Germany)

[5] *michael.mell@polizei.nrw.de*
State Agency for Central Police Services (LZPD)
Schifferstraße 10, 47059 Duisburg (Germany)

[6] *ruediger.czech@deutschebahn.com*
Deutsche Bahn AG, DB Security,
Köthener Straße 4, 10963 Berlin (Germany)

[7] *marco.krueger@izew.uni-tuebingen.de, katrin.geske@posteo.de*
University of Tübingen, International Centre for Ethics in the Sciences and Humanities,
Wilhelmstraße 19, 72074 Tübingen (Germany)

Abstract

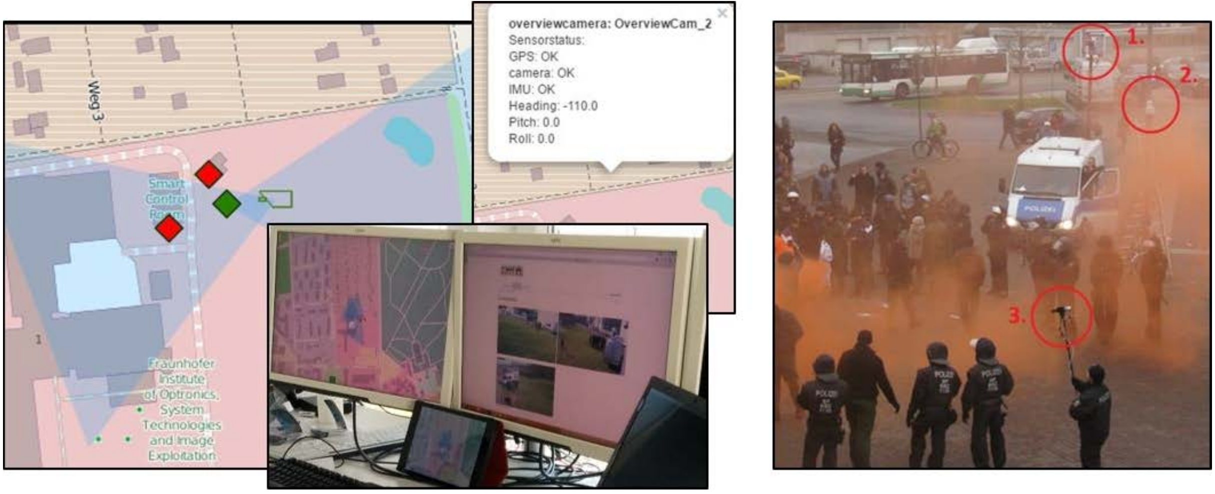
Today, in crowded and potentially violent scenarios, it becomes increasingly difficult for police forces to identify and prosecute offenders due to the complexity of such scenarios as well as the technical and legal requirements. Additionally, due to the sensitive nature of operations in public places, the police needs to strictly differentiate between offenders and uninvolved people in the crowd, in order to avoid that people will be falsely accused of being delinquent. The *Muskat* research project investigates and develops sensor and communication technologies in order to support the police in tracking and detaining offenders in complex scenarios. Using the example of *Muskat*, we show how legal and ethical guidelines can be considered and implemented during all development phases of such a networked and complex security technology.

Keywords: Multi-Sensor Cluster, Privacy-by-Design, Law Enforcement, Information Gathering, Evidence Preservation

1 INTRODUCTION – THE MUSKAT PROJECT

The ongoing research project *Muskat* (“Multisensorielle Erfassung von Straftätern bei komplexen Einsatzlagen”) funded by the German Ministry of Education and Research aims at improving the security while respecting the citizens privacy and fundamental rights [1]. For that purpose, a flexible multi-sensor demonstration platform has been designed in order to support security forces in the field by tracking single offenders and generating court-proof evidence. A sensor cluster will consist of several static and mobile video cameras, extended by inertial and GPS sensors. After a suspect was manually detected, he or she will be tracked automatically and mapped in a calibrated network of stationary cameras. Therefore, video exploitation algorithms for robust person tracking in crowds have been implemented, explored and adapted to the specific challenges (e.g. [3]).

The central part of the sensor cluster is the Information Control Center (ICC) [2], which is responsible for the communication between the sensor nodes and the visualization of the information in a dynamic situation map. In this map, information such as sensor positions, footprints, video streams, tracks of captured offenders and status information can be visualized in real-time. The operator in charge can control communications between sensor nodes (e.g. officers in the field) and manually interact with the tracking process in a feedback loop. An ontology has been developed that models all objects and relations relevant for a faster and more accurate decision support.



overviewcamera: OverviewCam_2
Sensorstatus:
GPS: OK
camera: OK
IMU: OK
Heading: -110.0
Pitch: 0.0
Roll: 0.0

Weg 3
Smart Control Room
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation
1.
2.
3.

Figure 1: Left: Information Control Center with online situation and status visualization as well as live streaming of video nodes. Right: Scene from an exercise in Dec. 2014 with two overview cameras (1+2) and one handheld sensor device (3).

2 ACHIEVING LEGAL COMPLIANCE

The technical development in this project is closely flanked by legal research in order to guarantee a lawful system. Therefore, several workshops based on the four-step approach called KORA (“Konkretisierung rechtlicher Anforderungen”) were held in order to develop legal guidelines. KORA was designed to bring legal suggestions into a technical development process. The approach has already been successfully tested and employed in numerous projects [4].

Prior to the first step of the KORA process, preliminary research needs to be conducted. This includes the examination of the sub-constitutional national, constitutional national and European legal framework. Furthermore, the opportunities and risks associated with the planned technology for this legal framework have to be set out. The constitutional legal framework is determined by the human dignity, the right to freedom of action, the general principle of equality and the rule of law.

In the first step of the process, abstract legal requirements are deduced built upon the results of the preliminary research and especially the constitutional legal framework. As an example, the right to informational self-determination is a legal requirement in the *Muskat* case. These requirements are further specified in order to formulate concrete legal criteria. In contrast to the legal requirements, legal criteria refer to the system to be developed. In the next step, a switch from a legal language to a technical vocabulary takes place and technical aims will be derived from legal criteria. In the last step, specific technical design proposals referring to the system to be developed will be derived from these technical aims.

Numerous technical design suggestions have been made as a result of this process. Many of them could already be respected during the design phase and therefore are integrated into the final system. These include, among others, end-to-end encryption of communication within the video sensor network and its components, anonymization of video-streams, timestamps and the usage of ring buffers. One notable suggestion is the three-stage model, which was primarily developed in the project *CamInSens* [5]. One task during the preliminary research was to clarify the basic issue, whether the three-stage model can be applied in the current system. Briefly, the model provides the user of the system only with those functionalities which are both necessary and appropriate for a particular situation with respect to the specific risks for the rights and freedoms of the affected people.

The legal research should result in a catalogue of legal requirements and criteria for video-sensor-networks in general, which can be fulfilled by the cohering technical criteria and proposals. The approach will be limited, where parts or components of the used technology are comprehensively designed, for example a chipset, sensor, or hardware-component.

3 ETHICAL ASSESSMENT

Beside legal requirements, security technologies – especially when applied in public space – have also to face ethical considerations. The ethical assessment investigates among other issues ***a)*** privacy concerns, ***b)*** discriminatory potentials, ***c)*** normalization and displacement potentials as well as ***d)*** justification of the means considering the scenario. Based on these assessments, potential alternatives to *Muskat* and fields of application other than the research scenario are examined and evaluated.

a) The conscious and earmarked treatment of data is one central demand for state-driven security routines. *Muskat* should not gather more data of bystanders than current video systems, but should reduce visibility of those not involved.
b) *Muskat* is being investigated with respect to its discriminatory potentials. Algorithms might be a great tool when it comes to privacy requirements and are often seen as a means to overcome human subjectivity, in particular personal biases [6]. However, they are written by people, and often based upon implicit prejudice [7]. Additionally, *Muskat* raises accountability questions as police decisions are made on algorithmically processed – and thus to a certain degree filtered – information [8]. The ethical assessment should disclose those shortcomings and potential presuppositions, if applicable.
c) Resulting from the impression of being under automated surveillance, people might feel the need to adapt to a certain image of "normality" and thereby change their behavior. Others might be scared and avoid football matches entirely or use the surveillance system as stage for performance. Therefore, the algorithms should be reliable.
d) And finally, the ethical researchers ask whether the football scenario really justifies a system as *Muskat*. Is it maybe too intrusive or does the potential danger justify semi-automatic tracking and multiple video recording? *Muskat*, as a security routine, is suited to increase the securitization of sport events [9]. The project is in line with an ongoing research on security in sports mega events which suggests to critically reflect the securitization of sports with regard its societal consequences [10]. Therefore, it is necessary to check the

surveillance system against other, (non-)technical alternatives in order to identify the least intrusive and ethically most unproblematic way to tackle the underlying societal and technical problems of the research scenario.

In order to make a reliable assessment of the system, multiple sources are being used. All research results are being reviewed and discussed in regular meetings. Besides literature reviews and technology analysis, we also conducted interviews with a number of different stakeholders. Experts for the football fan community were consulted as well as police officers responsible for operating cameras and arresting offenders. Two ethical assessments are being prepared concerning the social impacts and the technical challenges respectively.

4 OUTLOOK

The *Muskat* project will end in September 2017. The second half of the on-going project focuses at optimizing the technical components with respect to their interaction and usability, fulfilment of legal requirements and the implementation of a data exchange between two clusters. Further workshops with legal and ethical experts will take place to guarantee a lawful and ethically compliant realization of the demonstrator. A second exercise in order to evaluate the so far developed system is planned for early 2017. At the end of the project, a final version of the demonstrator will be presented including all implementations of legal requirements developed in the project.

ACKNOWLEDGEMENT

The research project *Muskat* is funded by the German Ministry of Education and Research (BMBF).

REFERENCES

[1] F. Pagel, J. Moßgraber, C. Decker, J.-P. Germann, *A multi-sensor technology for improving security at complex scenarios with increased risk of violence*, 10th Future Security 2015, Stuttgart: Fraunhofer Verlag, 2015.

[2] J. Moßgraber, M. Rospocher, *Ontology Management in a Service-oriented Architecture*, Int. Workshop on Web Semantics and Information Processing (WebS), 2012.

[3] J. F. Henriques, R. Caseiro, P. Martins, J. Batista, *Exploiting the circulant structure of tracking-by-detection with kernels*, In proceedings of the European Conference on Computer Vision, 2012.

[4] V. Hammer, U. Pordesch, A.Roßnagel, *Betriebliche Telefon- und ISDN-Analagen rechtsgemäß gestalten*, Darmstadt, 1993.

[5] A. Roßnagel, G. Hornung, M. Desoi, *Gestufte Kontrolle bei Videoüberwachungsanlagen. Ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung*, DuD,2011.

[6] M. Leese, *The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union*, Security Dialogue, 45(5), 2014.

[7] Propublica, *Machine Bias* (URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing), 2016.

[8] R. Giulianotti, *Sport Mega Events, Urban Football Carnivals and Securitised Commodification: The Case of the English Premier League,* Urban Studies, 48(15), 2011.

[9] T. Matzner, *The Model Gap: cognitive systems in security applications and their ethical implications*. AI & Society, 31(1), 2016.

[10] D. Bigo, *Security and Immigration: Toward a Critique of the Governmentality of Unease*. Alternatives, 27, 2002.

INVESTIGATION OF METAL ORGANIC FRAMEWORKS AS SELECTIVE PRECONCENTRATOR MATERIAL VIA INVERSE GAS-CHROMATOGRAPHY

Max Rieger[1], Michael Wittek[2], Philip Scherer[2], Frank Schnürer[2] and Stefan Löbbecke[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

Trace-amount detection of low volatile organic compounds (LVOCs), in ambient air (e.g. explosives and its precursors) contains two central challenges. Low concentrations of the target compounds in the sub-ppm region require a high sensitivity while an increasing number of interfering substances in these low-concentration regions demands for enhanced selectivity. Both factors reduce the effectiveness and reliability of common analytical methods. This may be overcome using a pre-filter or selective preconcentrator with a substance dependent adsorption-, diffusion- or desorption-behavior e.g. a varying retention volume or Henry-constant as compared to interfering substances.[1-3]

Metal Organic Frameworks (MOFs) are a promising new substance class of crystalline highly porous materials. They are comprised of metal- or metal-cluster-cations (“nodes”) and multidentate anionic or neutral organic molecules (“linkers”).[4] This 1, 2 or 3-dimensional network contains pores and/or channels with spatial and chemical uniformity. Pore sizes reaching from 4 Å to 98 Å have been reported.[5] By varying the linkers and nodes, it is possible synthesize distinct structures and tailor them for specific applications. Their applicability as preconcentrator material for phosphonates [6] and formaldehyde [7] as well as sensing material for nitro-compounds[8,9] was shown recently.

Materials and Methods

We modified a gas-chromatographic system in order to investigate MOFs for their physicochemical characteristics with respect to different guest molecules (analytes) (see Figure 1). The principle of inverse gas-chromatography was used.[10] For this purpose, vapor samples of different analytes are injected into a stream of carrier-gas.[10] The sample containing gas stream is then conducted through a packed bed of pure MOF material. Analyte concentrations in the gas stream are permanently monitored using a thermionic-ionization (TID) and photoionization detector (PID) between the packed bed and the exhaust. Gas flow are measured using a mass-flow meter.
Via analyzing retention-times of different analytes-adsorbent combinations it is possible to state Henry constants (analyte-sorbent sorption constants at infinite dilution) and analyte-MOF selectivities.[10,11]
For preliminary testing runs, widely known MOFs such as HKUST-1 (Cu_3BTC_2), MIL-53(Al) or ZIF-8 are examined. They may be compared to state-of-the-art adsorbents like Tenax TA ®.

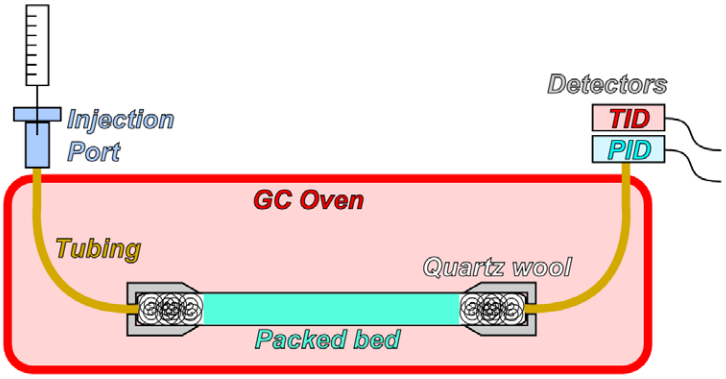


Figure 1: Schematic showing experimental Set-up. Vapor samples of analytes are injected via a syringe, conducted through a packed bed of sorbent via a carrier gas flow. Its concentration is continuously monitored after passing the bed.

Using equations *1*,*2* and *3*, retention volumes can be converted into normalized retention volumes (eq1), and more familiar units of henry constants $(mole/(kg \cdot Pa)$ (eq3).

$$V_G^0 = \frac{j}{m} \cdot \dot{V} \cdot (t_A - t_0) \cdot \left(\frac{T_C}{T_{MFM}}\right) \qquad \textit{[eq1]}$$

$$j = \frac{3}{2} \cdot \left(\frac{\left(\frac{p_i}{p_0}\right)^2 - 1}{\left(\frac{p_i}{p_0}\right)^3 - 1}\right) \qquad \textit{[eq2]}$$

$$K_C = \frac{V_G^0}{R \cdot T_C} \qquad \textit{[eq3]}$$

Where j depicts the “James Martin” pressure drop correction, m the sorbent mass (in g), $\mathrm{t_A}$ and $\mathrm{t_0}$ the retention times of the analyte and methane after injection time (in min), $\mathrm{T_C}$ and $\mathrm{T_{MFM}}$ the temperatures of the GC-column and mass flow meter (K) and $\dot{\mathrm{V}}$ the carrier gas flow (in ml/min).
Plotting $\ln{(V_G^0)}$ versus $\frac{1}{T_C}$ the slope of a linear regression yields the enthalpy of adsorption for the respective guest molecule on the MOF in the packed bed (*eq4*).

$$\Delta H_{ads} = -R \frac{\partial(\ln{(V_G^0)})}{\partial\left(\frac{1}{T_C}\right)} \qquad \textit{[eq4]}$$

Results

A strong decrease in retention volumes for all nitro compounds by 2 to 3 orders of magnitude when going from 50 to 200°C can be observed for HKUST-1 (Figure 2). This may render it a candidate for a high enrichment factor. Being also able to have a molecular weight-dependent retention time, a pre-separation on a molar sieving basis may also be possible.

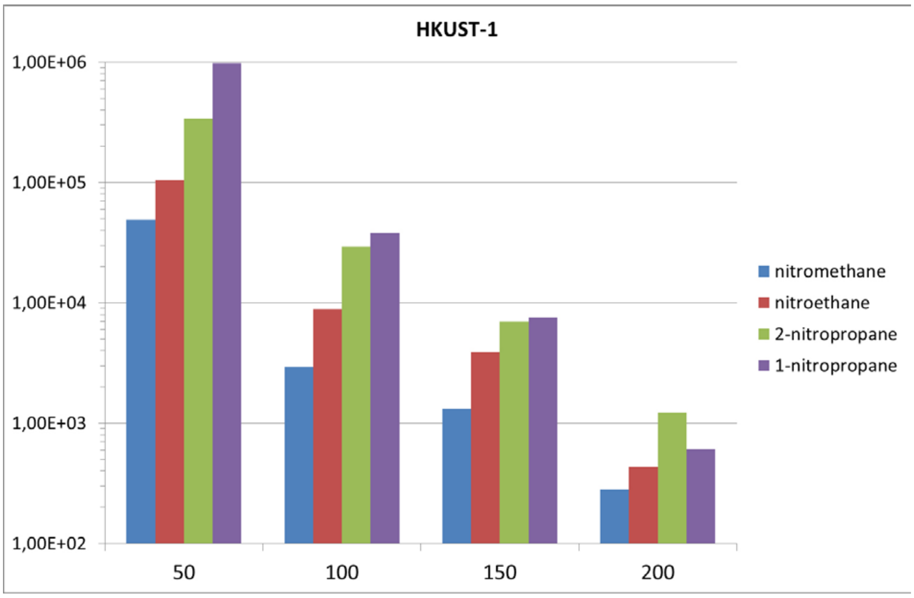


Figure 2: Example of retention volumes for varying nitro compounds at different temperatures on HKUST-1 (Cu). Y-axis shows retention volumes in ml/g of sorbent. Temperatures in °C.

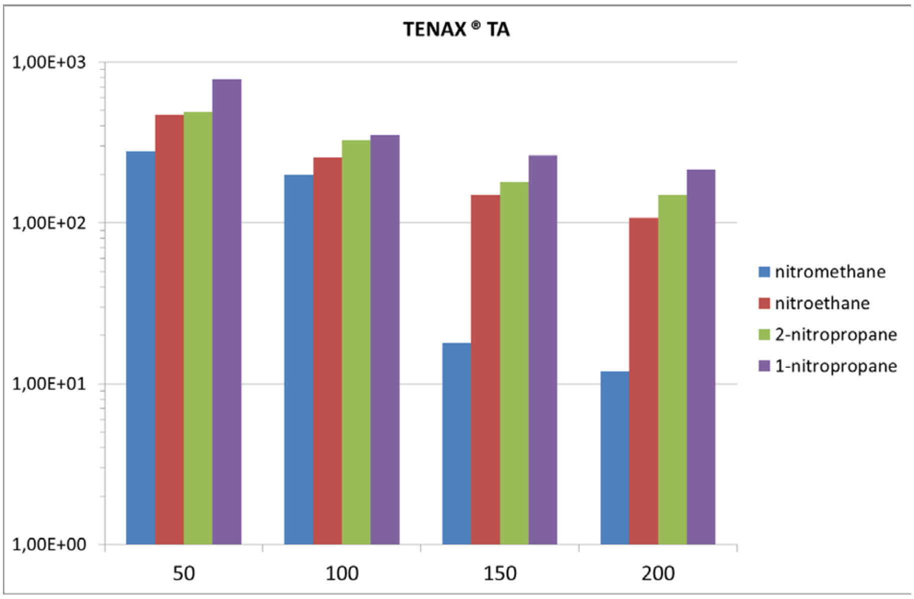


Figure 3: Example of retention volumes for varying nitro compounds at different temperatures on TENAX ® TA. Y-axis shows retention volumes in ml/g of sorbent. Temperatures in °C.

In case of Tenax ® TA, a maximal shift of 12 is observed (nitromethane) (Figure 3). Other analytes are only shifted by a factor of 3-7 when going from 50 to 200°C. In general Tenax shows smaller retention volumes as compared to HKUST-1 or MIL-53.

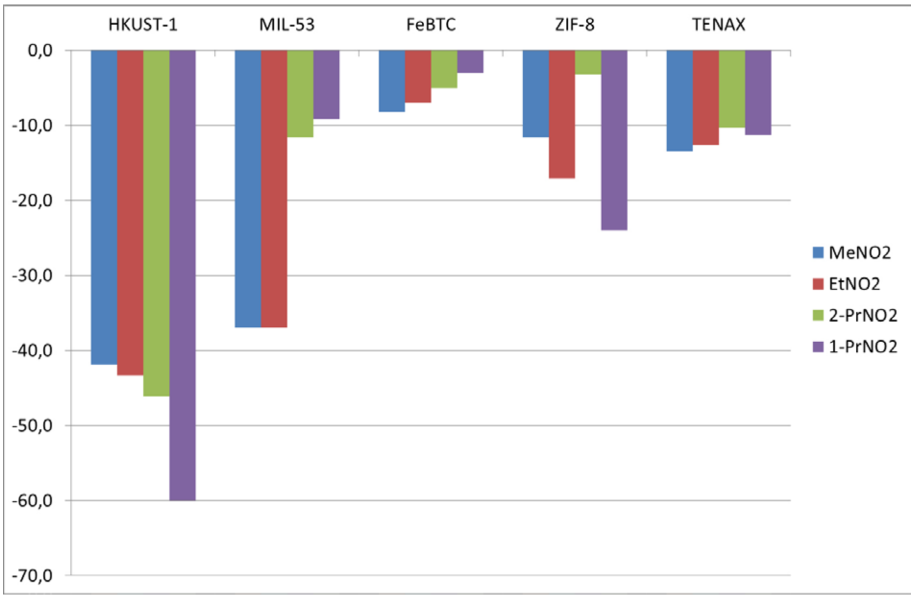


Figure 4: Barcharts of heats of adsorption (in kJ/mol) for various MOF-analyte combinations.

The above mentioned effect is also resembled in the heats of adsorption. In general, HKUST-1 shows the highest heats of adsorption for any nitro compound. This may be attributed to its open-metal-sites (copper) within the framework. This would also explain, why FeBTC, having the same organic linker (trimesic acid) has lower heats of adsorption than Tenax. ZIF-8 shows interesting steric favors for linear nitro compounds, but not for "branched" ones like 2-nitropropane.
Tenax does show decreasing heats of adsorption for the heavier homologues, as does FeBTC. As this effect may be attributed to both, the poor crystallinity of FeBTC and the sheet-like morphology of Tenax.

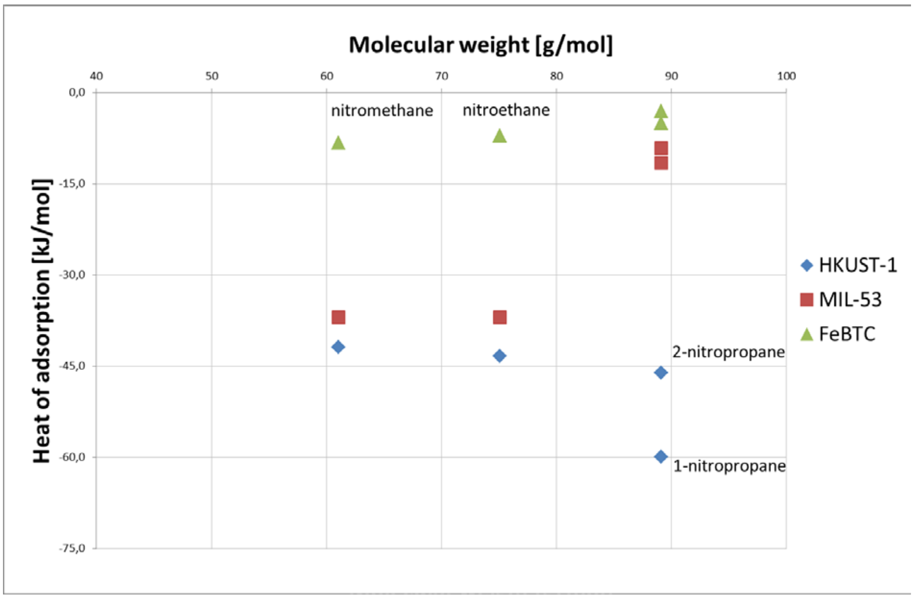


Figure 5: Plot of analytes molecular weight vs. their heats of adsorption on 3 different MOFs.

HKUST-1 is able to discriminate between both nitropropane isomers by an adsorption enthalpy of almost 15 kJ/mol. No other sorbent showed a comparable effect. This shows that also steric factors play a role in the adsorption mechanism of nitro alkanes on HKUST-1.

Conclusions

Metal-organic frameworks pose interesting and efficient preconcentration materials for gas sampling or sample enrichment within a sensor system. They are also in the price range of commercially available state-of-the-art sorbents like Tenax ® TA.

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] 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(4), 1290–3. http://doi.org/10.1021/ac0613075

[7] Gu, Z.-Y., Wang, G., & Yan, X.-P. (2010). MOF-5 metal-organic framework as sorbent for in-field sampling and preconcentration in combination with thermal desorption GC/MS for determination of atmospheric formaldehyde. Analytical Chemistry, 82(4), 1365–70. http://doi.org/10.1021/ac902450f

[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] Pramanik, S., Hu, Z., Zhang, X., Zheng, C., Kelly, S., & Li, J. (2013). A Systematic Study of Fluorescence-Based Detection of Nitroexplosives and Other Aromatics in the Vapor Phase by Microporous Metal-Organic Frameworks. Chemistry (Weinheim an Der Bergstrasse, Germany), 1–9. http://doi.org/10.1002/chem.201301194

[10] Thielmann, F. (2004). Introduction into the characterisation of porous materials by inverse gas chromatography. Journal of Chromatography A, 1037(1-2), 115–123. http://doi.org/10.1016/j.chroma.2004.03.060

[11] 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

A NEW X-RAY SECURITY INSTRUMENT BASED ON THE METHOD OF THREE-ENERGY DIGITAL RADIOGRAPHY

V. Ryzhikov[1], A. Opolonin[1], S. Naydenov[2], and A. Krylov[3]

[1] ryzhikov@isma.kharkov.ua
Institute for Scintillation Materials, 60 Lenin Ave., 60001 Kharkov (Ukraine)

[2] sergei.naydenov@gmail.com
Institute for Single Crystals, 60 Lenin Ave., 60001 Kharkov (Ukraine)

[3] alexander.krylov@folgat.com
FOLGAT AG, Melsunger Str. 9, D-60389, Frankfurt am Main (Germany)

Abstract

The method of multi-energy radiography and the corresponding X-ray three-energy detection system was developed. Experiments were carried out with different objects that simulate some explosives due to their similar chemical composition. Results are presented on experiments aimed at obtaining radiographic images in three energy ranges (of effective energies about 30, 60 and 100 кeV) for testing objects with effective atomic number Z_{eff} from 6 to 29. With special software we develop special 2- and 3-coordinates identification colour palettes. Using the developed reconstruction method it is possible to detect imitators of explosives even with small difference of their Z_{eff} (for example, from 7.08 to 8.07) with accuracy about 5%, therefore to distinguish explosives from safety organic materials.

Keywords: multi-energy radiography, effective atomic number, organic materials detection, X-ray mass attenuation coefficient.

1 INTRODUCTION

Many X-ray inspection systems widely use ordinary (not multi-energy) digital radiography that allow to image but only qualitatively recognize objects from different materials. Modern inspection systems produced by Smith-Heimann firm apply dual energy radiography method with a possibility to quantitatively recognize of materials with high effective atomic number Zeff (metals, stones, etc.) from more easy materials (salt, water, organics). The number of achievements of the dual-energy method is connected with the using of exclusive ZnSe(Te) scintillator (produced by Institute of Scintillation Materials, Kharkov, Ukraine) for low energy X-ray detectors [1].

Other years we proposed multi-energy method [2], in part, adapting of three lines of detectors for X-ray detection at low (20-30 keV), medium (50-60 keV) and high (about 80 keV and up to 120-140 keV) photon energies. For perfect three-energy inspection system it is worth to use three monochromatic X-ray sources ore one X-ray source with quasi-monochromatic multi-energy X-ray filters. But practically it is very difficult for realization and too expensive. Instead this we have chosen to take a set of usual metal filters from different materials (aluminium, copper, steal, lead) and different thicknesses that have been used in three lines of detectors for X-ray detection in low (L signal), medium (M signal) and high (H signal) energy ranges. This get possibility cut off wide energy spectrum of X-ray tube to more narrow bands of spectrum.

Separate recording of the low- and high-energy regions of broad X-ray radiation spectra allows obtaining additional (as compared with film radiography) information on the object of radiographic monitoring. The method of two-energy radiography is based on substantial difference in the energy dependence of mass attenuation coefficient μ_m *(E)* for substances with different atomic number. From the signal ratio of low- and high-energy detectors, one can obtain an estimate of the effective atomic number Z_{eff} of the inspected object [3-7]. In this work, we describe the results of our experiments on obtaining radiographic images in three energy ranges, as well different methods of signal processing for discrimination of substances by their Z_{eff} .

2 EXPERIMENTAL SETUP

Our experiments were carried out on the basis of three-energy scanner developed under the project NATO SfP-982823 "New Generation of Multi-Energy X-ray Scanners for Anti-terrorist Inspection" (Fig. 1). As testing objects, we used both simple substances and chemical compounds. The objects were prepared in the form of step wedge: copper (Z=29) and iron (Z=26) of thickness from 1 to 15мм, aluminium (Z=26) of thickness from 2 to 30mm, organic glass of thickness from 20 to 100 mm. We also used friable substances placed in paper containers. The thickness was chosen in such a way as to ensure close values of attenuation of intensity when blocking the X-ray radiation flux: salt (Z_{eff} = 15.9), soda (Z_{eff} = 8.76), sugar (Z_{eff} = 6.93), urea (Z_{eff} = 6.83), smokeless gunpowder.

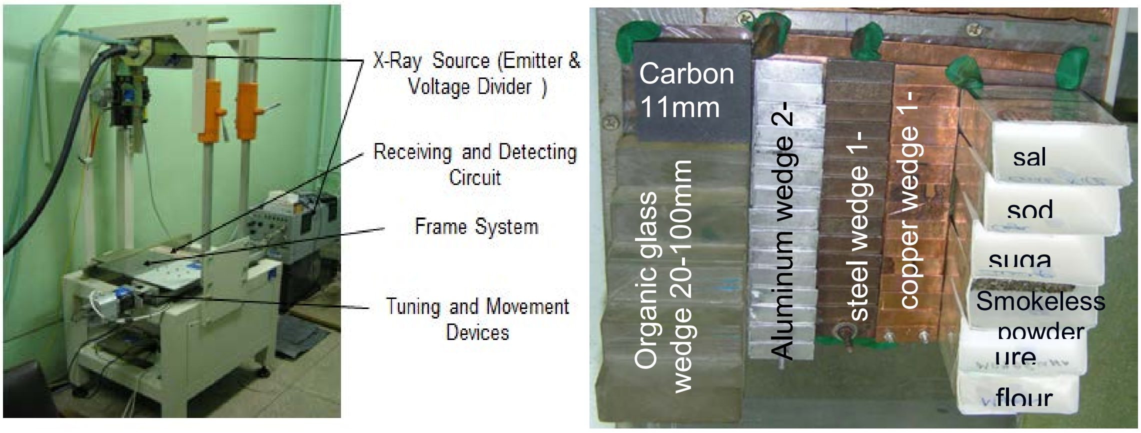

X-Ray Source (Emitter & Voltage Divider)
Receiving and Detecting Circuit
Frame System
Tuning and Movement Devices
Carbon 11mm
Organic glass wedge 20-100mm
Aluminum wedge 2-
steel wedge 1-
copper wedge 1-
sal
sod
suga
Smokeless powder
ure
flour

Fig. 1. Experimental setup (scanner) for three-energy X-ray radiography (on the left) and the testing objects used (on the rigth).

Using three operation modes of the X-ray emitter as a part of three-energy scanner (Fig. 1), we obtained three radiographic images of a set of testing objects (Fig. 2).

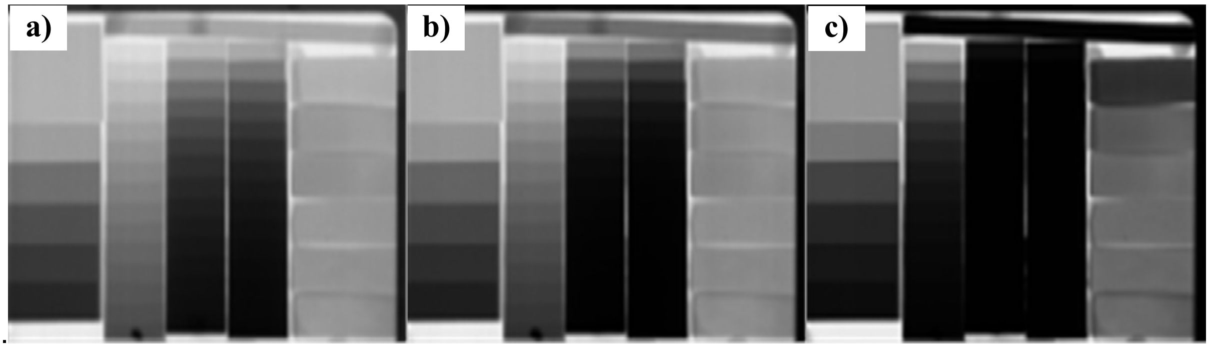


Fig. 2. Radiographic (black and white) images of the set of testing objects obtained in three different energy ranges: (a) anode voltage U_a = 150 kV, copper filter of thickness 5 mm; (b) U_a = 100 kV, copper filter of thickness 2mm; (c) U_a = 50 kV, aluminium filter of thickness 4 mm.

3 RESULTS

For identification of materials with different atomic numbers it is possible to apply special colour palettes and every material will correspond to definite own colour. The principle of input of 2D colour palette is the following. If we display all points as corresponding to their radiographic images at coordinates *(x, y)*, where *x* – value characterizing the total X-ray attenuation property of the object (e.g., value *H*, *(H+M+L)/3*, others), *y* – value characterizing the material (e.g., *L/M*, *M/H*, *H/L*, others), then combining a set of points with a 2D colour palette, we can assign to each point of radiographic image the corresponding colour and brightness. Using the procedure involving taking the logarithms of detector signals, some data from [8] and piecewise-linear approximation for calculation of the parameter that characterizes the energy dependence $\mu_m(E)$, which was described in detail in [7], we constructed point charts of radiographic images (Fig. 3).

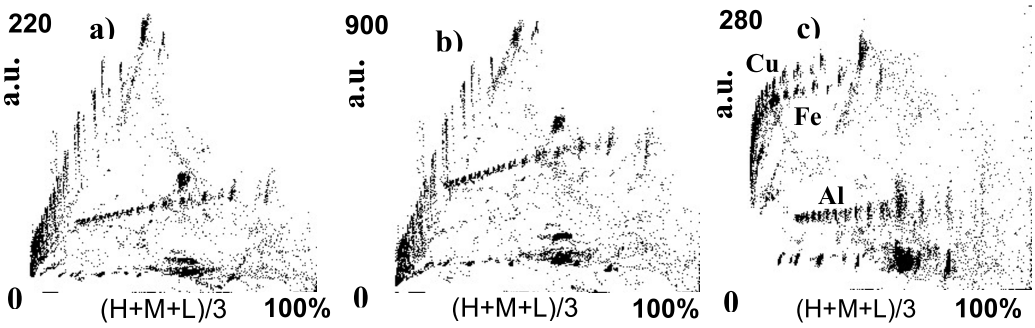


Fig. 3. 2D maps of points corresponding to two-energy images of test objects. Abscissa axis – total detector signal. Ordinate axis – special parameter characterizing the energy dependence of $\mu_m(E)$ for ratio of signals *H/L* (a), *M/L* (b), *H/M* (c).

Overlaying of point charts on 2D colour palette (Fig. 3), one can ascribe a certain colour to each pixel of the two-energy radiographic image, thus obtaining colour discernment of two substances by their Z_{eff} (Fig. 4). Varying the scale of the point chart for the image fragment framed by the rectangle on Fig. 4b and using the corresponding palette (see Fig. 4c), one can obtain colour separation of "light" substances with close values of their Z_{eff} (see Fig. 4d).

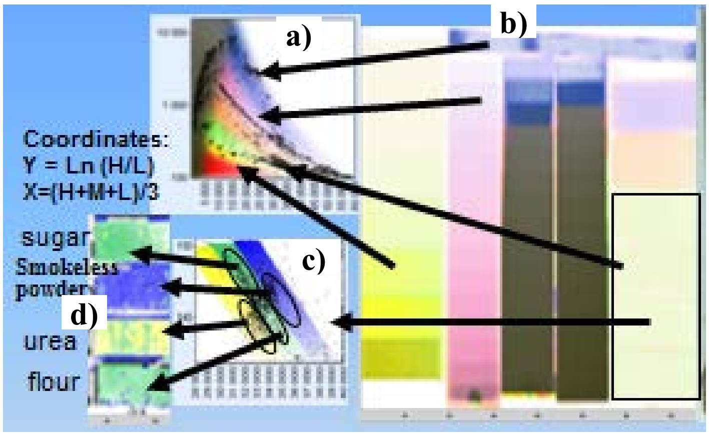


Fig. 4. Using 2D palette for obtaining colour two-energy radiographic image: (a) colour palette upon the point chart of all the data set; (b) two-energy radiographic image; (c) a fragment of 2D colour palette; (d) a fragment of the image with "light" substances.

Using 3D colour (analogue of RGB) palette, we also obtained three-energy images of testing objects in coordinates x^{red} =*(H+M+L)/3*, y^{green} = $\mu_m(E)_{M/L}$, z^{Blue} = $\mu_m(E)_{H/M}$ (Fig. 5), where $\mu_m(E)_{M/L}$ and $\mu_m(E)_{H/M}$ are parameters characterizing the energy dependence of $\mu_m(E)$ and calculated for ratio of signals *H/M* and M/L respectively, using the procedure described in [7].

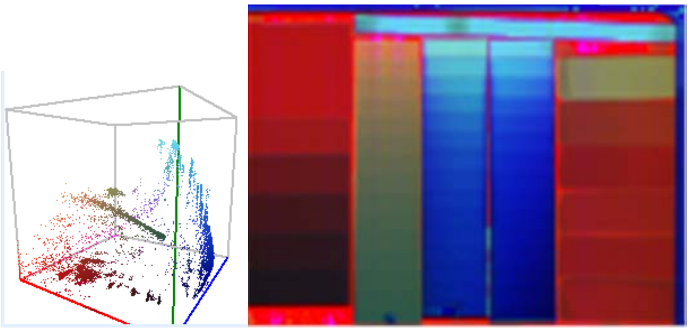


Fig. 5. Three-energy radiography: 3-color palette (on the left) and three-energy image of testing objects (on the right).

One can see from Fig. 5 that the use of three energies and application of 3D color palette allowed substantial improvement of substance discrimination by Z_{eff} , even when the influence of scattered radiation is substantial. Also, one can expect substantially improved separation of “light” substances with close values of $Z_{eff} < 10$.

4 CONCLUSIONS

The proposed methods for obtaining two- and three-energy images, as claimed by the authors, can substantially broaden the possibilities of the existing radiographic and tomographic systems, as well as lead to creation of essentially new systems. When X-ray radiation is attenuated by more than 80%, scattered radiation can substantially affect the results on substance separation by their Z_{eff} . The use of 3D colour (RGB) palette instead of 2D colour palette allows to improve the visual presentation of three-energy radiographic images.

AKNOWLEGMENTS

This work was supported in part by NATO's Emerging Security Challenges Division in the framework of the Science for Peace and Security Program by Project SfP-982823 (completed in 2012) and current Project SfP-984605 (2014-2017).

REFERENCES

[1] Frank, A., Schall, P., Geus, G. (2002). U.S. Patent No. US6445765, B1.

[2] Naydenov, S., Grynyov, B., Ryzhikov, V. (2011). U.S. Patent No. US7912177, B2.

[3] Naydenov S., Ryzhikov, V. (2002). On determination of chemical composition by means of multi-energy radiography. Pis’ma v ZhTF, Vol. 28, No. 9, 71-77.

[4] Ryzhikov, V.D., Naydenov, S.V., Grinyov, B.V., Lisetskaya, E.K., Kozin, D.N., Opolonin, A.D., Starzhinskiy, N.G. (2003). *Multi-energy radiography on the basis of scintillator-photodiode detectors*. Nucl. Instrum. and Meth. A505, 549-551.

[5] Naydenov, S.V., Ryzhikov, V.D., Smith, C.F. (2004). *Direct reconstruction of the effective atomic number of materials by the method of multi-energy radiography*. Nucl. Instrum. and Meth. B215, 552-560.

[6] Ryzhikov, V., Opolonin, O., Galkin, S., Lysetska, O., Voronkin , E. (2011). *X-ray Radiation detectors of "scintillator-photodiode" type for security and nondestructive testing*. 2011 IEEE NSS-MIC Conference, doi: 10.1109/NSSMIC.2011.6154450

[7] Opolonin, O.D., Ryzhikov, V.D (2013). Increasing informativity of digital radiographic systems. Functional Materials, Vol. 20, No. 4, 528-533.

[8] NIST database, http://physics.nist.gov/PhysRefData/XrayMassCoef/tab4.html

HARMONIZED EVALUATION, CERTIFICATION AND TESTING OF SECURITY PRODUCTS (HECTOS) – CASE STUDY: EXPLOSIVE TRACE DETECTION

Frank Schnürer[1], Christian Ulrich[2] Anneli Ehlerding[3] and Anders Elfving[4]

[1] *frank.schnuerer@ict.fraunhofer.de*
Fraunhofer Institute for Chemical Technology ICT, Joseph-von-Fraunhofer-Str. 776327
Pfinztal (Germany)

[2] *christian.ulrich@ict.fraunhofer.de*
Fraunhofer Institute for Chemical Technology ICT, Joseph-von-Fraunhofer-Str. 776327
Pfinztal (Germany)

[3] *anneli.ehlerding@foi.se*
FOI - Swedish Defence Research AgencySE-164 90 Stockholm (Sweden)

[4] *anders.elfving@foi.se*
FOI - Swedish Defence Research AgencySE-164 90 Stockholm (Sweden)

1 OVERALL CONCEPT OF HECTOS

HECTOS is a European project focusing on harmonisation of evaluation, certification and testing of physical security products. Physical security equipment and systems are very diverse in technology, concept of operation, application area and performance. Similar security products are difficult to compare in terms of performance, accuracy, usage, trust and validation of functionality.

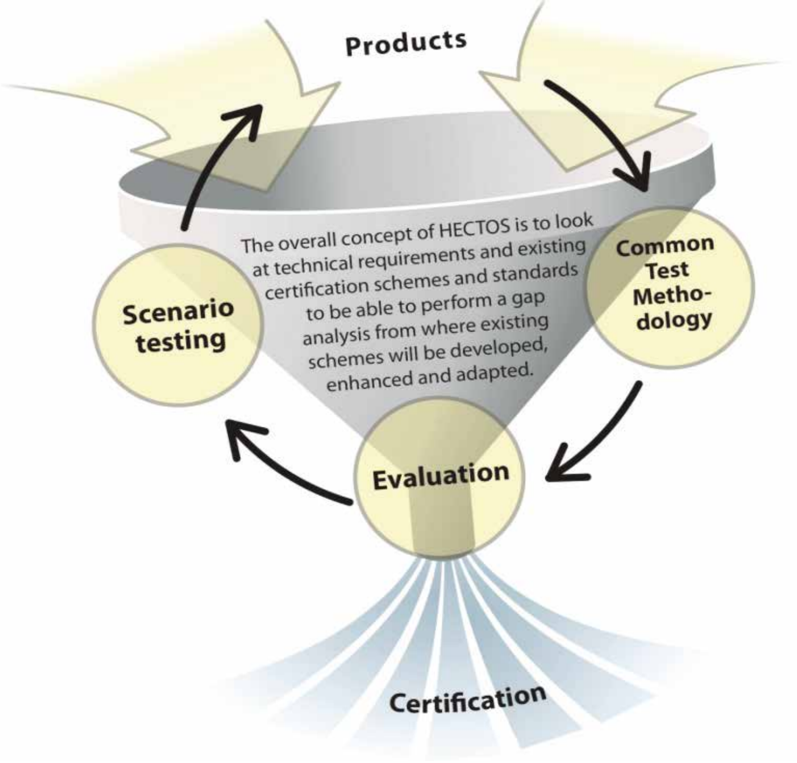

Products
The overall concept of HECTOS is to look at technical requirements and existing certification schemes and standards to be able to perform a gap analysis from where existing schemes will be developed, enhanced and adapted.
Common Test Metho-dology
Scenario testing
Evaluation
Certification

Fig.1: Overall concept of HECTOS

Currently, there are very few test, evaluation and certification procedures in Europe that are mutually recognized by different Member States. This leads to fragmentation of the market, as identified in the recent EC Communication on Security Industrial Policy, with negative impacts on both suppliers and users. The HECTOS project focuses on evaluation and certification schemes for physical security products, and studies how existing schemes used in other areas could be applied, adapted or developed for products used for physical security of people, property and infrastructure.

The HECTOS project started in September 2014 and is a collaboration between nine partners, coordinated by FOI, the Swedish Defence Research Agency.

- Totalförsvarets Forskningsinstitut – FOI (Sweden)
- Fraunhofer Institute for Chemical Technology ICT (Germany)
- Fraunhofer Institute for Computer Graphics Research IGD (Germany)
- Morpho, SAFRAN Group (France)
- Iconal Technology Ltd (Great Britain)
- Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek – TNO (Netherlands)
- The University of Warwick (Great Britain)
- NPL Management Limited (Great Britain)
- DIN e.V. (Germany)

2 CASE STUDIES

Developed evaluation and certification schemes will be validated by applying them to two different product groups as case studies; explosives detection systems (outside of aviation security) and biometric recognition. The HECTOS project will also learn from and work with other initiatives working in broader areas such as security systems and cybersecurity, as well as with other standardisation and certification initiatives, including the EU research project CRISP. HECTOS will result in a roadmap for the development of harmonised European certification schemes for physical security products, and initiate standardisation activities.

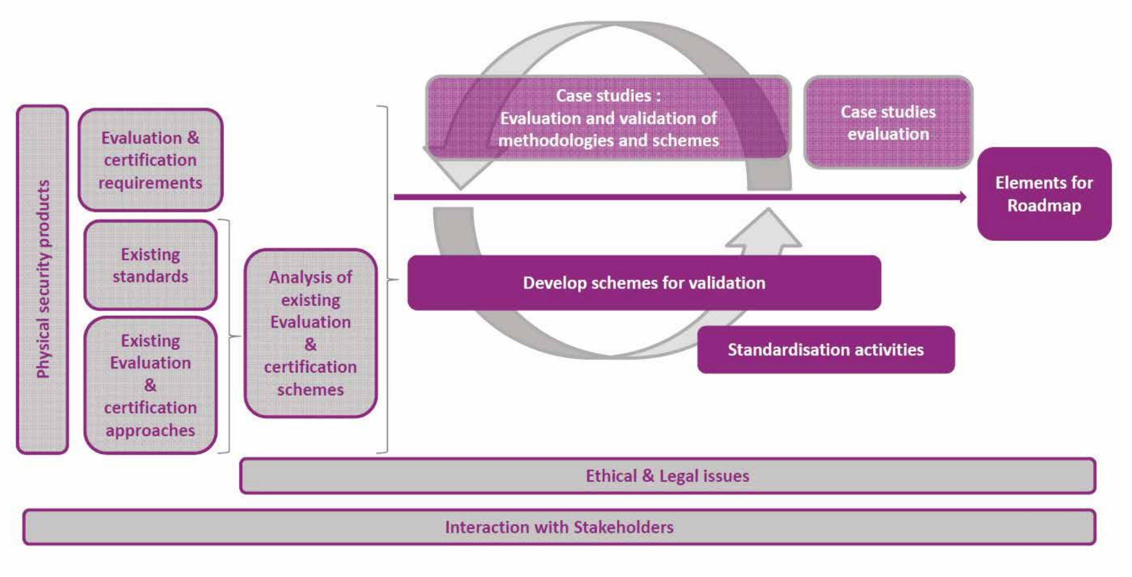

Physical security products
Evaluation & certification requirements
Existing standards
Existing Evaluation & certification approaches
Analysis of existing Evaluation & certification schemes
Case studies : Evaluation and validation of methodologies and schemes
Case studies evaluation
Elements for Roadmap
Develop schemes for validation
Standardisation activities
Ethical & Legal issues
Interaction with Stakeholders

Fig. 2: Path towards Harmonisation Roadmap

3 EXPLOSIVE TRACE DETECTION

This poster provides details concerning the tools by which this validation is performed for the area explosive trace detection (ETD). Starting with the analysis and comparison of existing standards and technical documents the requirements for harmonised testing have been derived taking into account also the stakeholder’s needs, scenario related requirements and various requirements for harmonised evaluation. This led to the conclusion, that in case of ETD the most important requirements are concerning security performance by measuring of detection rate and false alarm rate. These two are not fixed parameters but are extremely dependant on the amount and the selection of threat and background substances. Therefore scenario related requirements have been derived in order to allow scenario adjusted evaluation.

Test methods and finally test results are the basis on which a harmonised evaluation is settled. Therefore it was important to extract the main structures of test methods for high TRL ETD-systems identifying critical elements for repeatability and precision. The examination of the influence of those elements on testing results will be one major part of the testing which will be performed in the further progress of the project. Especially difficulties in the preparation of reliable test samples will be further examined. Only when testing fulfils all requirements of repeatability and precision its result can be used for type certification, while the certification process itself is not specific to explosives trace detectors and can be done according to the certification frameworks that are in place for various other application areas.

The focus on testing trace detectors at an earlier state (low-TRL) is somehow different. While type certification is not important at an early stage of development, repeatability and applicability to the planned use for example for optical non-contact detectors are crucial also for low TRL testing. Basic test methods for low-TRL explosive trace detectors will be developed in further process of HECTOS.

PROMOTION

The research project HECTOS is financed from the European Community's Seventh Framework Programme (Call: FP7-SEC-2013-1: SEC-2013.5.4-1: Evaluation and certification schemes for security products – Capability Project). Project Number: 606861

AGENT BASED MODELING FOR CRITICAL INFRASTRUCTURE PROTECTION – MODELING ATTACK SCENARIOS IN THE PUBLIC TRANSPORT

Martin Zsifkovits[1] and Stefan W. Pickl[2]

[1] *martin.zsifkovits@unibw.de*
Universität der Bundeswehr München, Faculty of Informatics, COMTESSA
Werner-Heisenberg-Weg 39, 85577 Neubiberg (Germany)

[2] *stefan.pickl@unibw.de*
Universität der Bundeswehr München, Faculty of Informatics, COMTESSA
Werner-Heisenberg-Weg 39, 85577 Neubiberg (Germany)

Abstract

In the past decades, the importance of Agent Based Modeling has significantly increased. One of the major reasons therefore is that improvements in computational power led to huge opportunities for modelers. Especially in the field of safety and security, the coupling with artificial intelligence allows for in-depth analyses and testing of various security strategies and technologies. Another important issue is the adequate placement of such technologies in order to optimize their effort. The analysis and testing from a microscopic perspective on an individual level is especially favorable when corresponding data is available, which is nowadays more and more often the case. In our research we are aiming for analyzing the vulnerability and resilience of systems, with a special focus on the rail bound public traffic and the corresponding stations in the system. We therefore created an agent-based model for testing individual passenger behavior and the resulting crowd behavior within a train station or within a train on the one hand, and for evaluating attack scenarios within this environment on the other hand. The model is parameterized based on a real-life experiment, expert opinions, table-top exercises, and historic events and validated with experts on the field. For an adequate representation of the results, heat maps for the crowd behavior and 3D representations for the evaluation of attacks were produced. This is also valuable for a better decision support.

Keywords: Agent Based Modeling, Critical Infrastructure Protection, Attack Scenarios, Counter Terrorism,

1 BACKGROUND

In the BMBF-funded project RiKoV it was the main aim to identify the risks and costs of terroristic threats in the rail bound public transport in Germany. In order to tackle these highly complex questions, multiple methods were applied and combined. Firstly, an extensive review of historic attacks was done in order to get a picture of former behavior of attackers. For identifying vulnerable spots from a macroscopic perspective, graph theory was applied in order to identify the most critical stations in the German rail network [1,2]. In a further step, observations were made in Munich main station in order to see how passengers behave in several situations over the week. These observations were analyzed in further quantitative analyses [3] in order to gain data on an individual's level. The behavior and efficiency of security installations were tested in a real-life experiment in Cologne, where several experimental runs were conducted using several weapons [4]. While these experiments the behavior of the actors were collected and saved in a database.

All the mentioned steps therewith gave deeper insights into individual levels of behavior in the system. In order to accumulate this knowledge and test for interactions, an agent-based simulation model was set up. As a primary setting, agents were parameterized using the information from the real-life experiments. For alternative scenarios, artificial intelligence was set up based on findings from historic attacks and experts' opinions. The environment of the simulation is the train station from the real-life experiment.

2 RESULTS

The model is able to identify critical spots within an environment due to crowded areas, as well as test for the effectivity of security installations for protecting those areas. However, applying artificial intelligence and a game theoretic basis to the attacker's decision making shows that various previous models are not adequate for the complex analysis at hand. We implemented a basic setting, where a real-life experiment was copied to the model and simulated in a 3D environment. In further steps, changes to the settings compared to the experiment were set. For example, detectors for explosives were removed or their detection rates increased (due to an expected progress in the technology.

Figure 1 shows a screenshot of the standard setting simulation, where security checks are conducted at the entrance to the station.

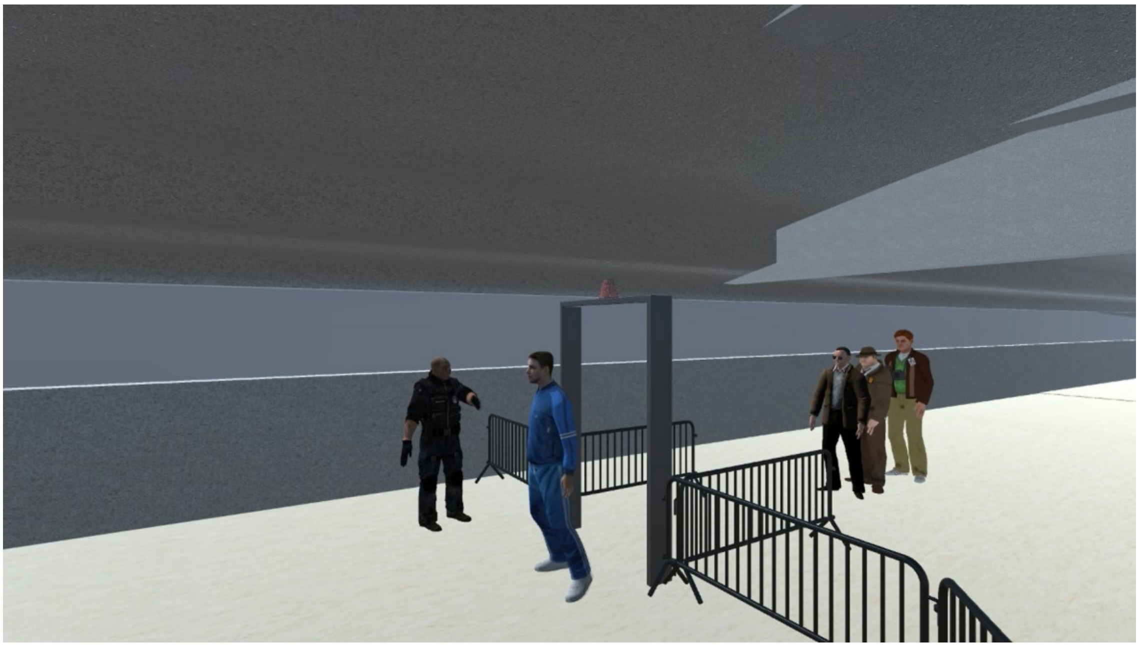


Figure 1. Screenshot from 3D Simulation with standard settings

In the analysis of an alternative case one can see the logic behind the artificial intelligence. An attacker with an explosive device manages to enter the train station. He walks to the spot with the highest density of passengers and drops the bomb. After seconds, the bomb detonates as shown in Figure 2.

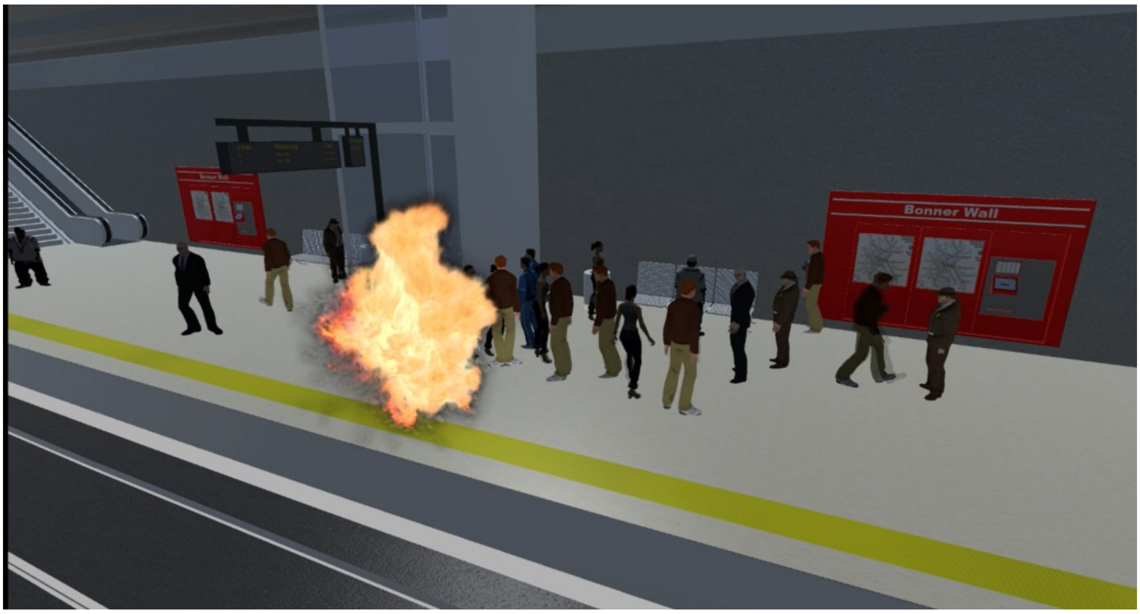


Figure 2. Screenshot from 3D Simulation in attack scenario

The simulation allows for testing various attack scenarios compared to defender strategies. Security installations can be set or removed, as well as novel weapons tested regarding their damage and probability of detection at security checks. However, the model also allows for testing the practicability of security strategies in terms of waiting times and passenger flow, as well as analyzing evacuations scenarios. One has to note that the evacuation behavior is by now kept rather simple and needs adjustment for in-depth analysis.

REFERENCES

[1] Nistor S.M., Pickl S.W., Raap M., Zsifkovits M. (2016) Network Efficiency and Vulnerability Analysis using the Flow-Weighted Efficiency Measure, Management and Governance of Networks, *forthcoming.*

[2] Nistor S.M., Pickl S.W., Raap M., Zsifkovits M. (2015) Quantitative Network Analysis of Metro Transportation Systems: Introducing the Flow-Weighted Efficiency Measure, In: Proceedings of the seventh international conference on ECONOMICS AND MANAGEMENT OF NETWORKS, Cape Town, South Africa.

[3] Nistor M.S., Zsifkovits M., Meyer-Nieberg S., Pickl S.W. (2016) Passenger Pattern Recognition in Railway Stations using Quantitative Network Analysis, International Journal of Information Assurance and Security (JIAS), Vol. 11 Issue 1, p11-20.

[4] Meyer-Nieberg S., Zsifkovits M., Brauner F. (2015) Assessing Passenger Flows and Security Measure Implementations in Public Transportation Systems, In: Proceedings of the Future Security Conference 2015, Berlin, Germany

INDEX OF AUTHORS

INDEX OF AUTHORS

INDEX OF AUTHORS

INDEX OF AUTHORS

EDITORIAL NOTES

Editors

Oliver Ambacher, Rüdiger Quay, Joachim Wagner

Contact

Fraunhofer Institute for Applied Solid State Physics IAF
Tullastrasse 72
79108 Freiburg, Germany
www.iaf.fraunhofer.de

Julia Roeder
Press and Public Relations

Phone	+49 761 5159-418
E-Mail	medien@iaf.fraunhofer.de

Layout	Sandra Iselin, Fraunhofer IAF

Conference Host

Fraunhofer Group for Defense and Security
www.vvs.fraunhofer.de

Bibliographic information published by Die Deutsche Bibliothek

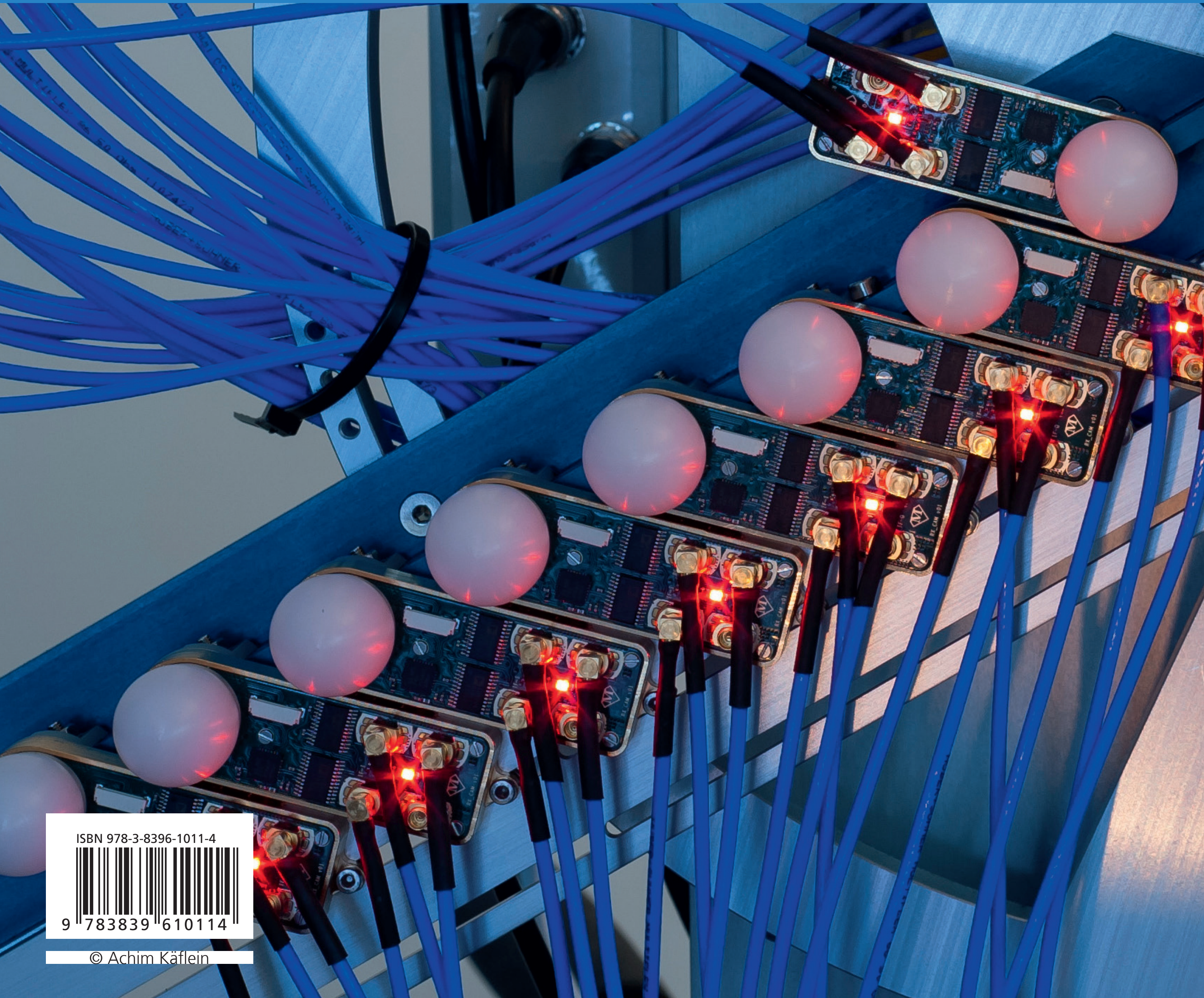
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliografic data is available in the Internet at http://dnb.d-nb.de.

ISSN 2364-3986
ISBN 978-3-8396-1011-4

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

Printing and Finishing
IRB Mediendienstleistungen
Fraunhofer-Informationszentrum Raum und Bau IRB, Stuttgart



ISBN 978-3-8396-1011-4

9 783839 610114

© Achim Käflein