SECURITY RESEARCH PROJECTS
under the 7th Framework Programme for Research

Investing into security research for the benefits of European citizens

September 2010

European Commission
Enterprise and Industry

REA

SEVENTH FRAMEWORK PROGRAMME

—

Further information available at: http://ec.europa.eu/enterprise/security/index_en.htm

Cataloguing data can be found at the end of this publication.

ISBN-13 : 978-92-79-16426-2
doi : 10.2769/74411

European Commission
Enterprise and Industry

INTRODUCTION

Investing into security research for the benefits of European citizens, critical infrastructures, SMEs and industry.

© Fotolia

Under its wider R&D budget for 2007-2013 – known as the Seventh Framework Programme for Research (FP7) – the EU is investing EUR 1.4 billion for security research. This catalogue presents an exhaustive overview of all projects currently supported by FP7's Security Research budget as of July 2010.

Europe has never been so peacefully consolidated or prosperous, yet it is also vulnerable to threats such as terrorism, organised crime and natural disasters. Making Europe more secure and resilient for its citizens and critical infrastructures, while strengthening its SMEs and industrial competitiveness is the goal of Security Research. To date a significant proportion of the committed budget (> 20%) is going to SMEs. By stimulating research and innovation – and promoting direct cooperation between providers and end-users of security equipments, systems and knowledge – the EU can better understand and prepare itself to face risks and disruptive events in a constantly changing world.

The evolving nature of security implies many new challenges. To strengthen the respect of fundamental human rights, including privacy, research into the preparedness and response of society to potential or actual threats and crises is essential. Thus, it is promising to see that European Security Research efforts in this area have increased substantially in the last few years, as readily seen in the below catalogue of FP7 projects.

These projects cover the entire range of FP7's Security theme, including advanced research into the societal dimension of security, protection of citizens against chemical, biological, radiological, nuclear and explosive (CBRNE) materials or man-made and natural events, critical infrastructure protection, crisis management capabilities, intelligent maritime and land border surveillance, pre-standardisation and the interoperability of systems.

European Commission
Enterprise and Industry

TABLE OF CONTENTS

Further information is available at:

http://ec.europa.eu/enterprise/security/index_en

Prepared by the European Commission, Directorate-general Enterp
E-mail: entr-security-research@ec.europa.eu

ADABTS / Automatic detection of abnormal behaviour and threats in crowded spaces

© Lv Design - Fotolia.com

Project objectives

ADABTS aims to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime and riots by the automatic detection of unusual human behaviour.

ADABTS aims to develop models for abnormal and threat behaviours and algorithms for automatic detection of such behaviours as well as deviations from normal behaviour in surveillance data.

ADABTS aims to develop a real-time evaluation platform based on commercially available hardware, in order to enable high-performance low-cost surveillance systems.

Description of the work

ADABTS will gather experts in human factors, signal processing, computer vision, and surveillance technology. In a first stage, focus will be on human factors in order to define and model behaviours. Then, the focus will be shifted towards automatic analysis of surveillance data (video and audio). Finally, a demonstration system will be implemented.

ADABTS will create models of behaviour that can be used to describe behaviours to be detected and how they can be observed. Such models will enable the prediction of the evolution of behaviour, so that potentially threatening behaviour can be detected as it unfolds, thus enabling pro-active surveillance. In order to detect behaviour defined by these models, advanced methods for sensor data analysis are needed. These methods should extract sensor data features that can be coupled to the defined behaviour primitives, and thus detect the presence of the (potentially) threatening behaviour and to detect behaviour that is not considered normal.

ADABTS will develop new and adapt existing sensor processing methods and algorithms for detecting and tracking people in complex environments, involving groups of people or crowds. Extracted sensor data features (e.g. tracks, voice pitches, body articulations) need to be related to the behaviour primitives, and, moreover, to be dynamic and adapt to the context.

ADABTS will adapt the above algorithms to run on commercially available low-cost hardware architectures consisting of multi-core CPU's combined with several multi-stream GPU's (Graphical Processing Units). Such hardware, in rapid development driven by the game industry, represents a huge potential for high-performance surveillance systems.

ADABTS will communicate results to the various kinds of identified actors: Security stakeholders like European and national authorities, police organisations or event organizers; Security system operators and security service companies; Security system integrators; Technology developers; the Research communities for psychology, human factors, and signal processing communities.

ADABTS will involve all these actors, either as principal contractors, as subcontractors, or in an associated stakeholder group.

Expected results

The main impact of the ADABTS project is expected to be on the technological level, with advancements in three directions:

Understanding of the user needs for automatic detection of unusual behaviour in crowds and new definitions of and methods for describing such behaviour.

Methods and algorithms for unusual behaviour detection based on video and acoustic sensors.

Real time optimization for commercially available low-cost hardware, including an on-line demonstration of capabilities at a football stadium.

Information

Acronym:
ADABTS

Grant Agreement N°:
218197

Total Cost:
€ 4,478,990

EU Contribution:
€ 3,229,034

Starting Date:
01/06/2009

Duration:
48 months

Coordinator:

TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)
Division of Information Systems
Postal Box: 1165
Sweden - SE-58111 Linköping

—

Contact:
Jörgen Ahlberg
Tel : +4613378068
Mobile: +46706757384
Fax : +4613378287
E-mail : adabts_coordinator@foi.se

Partners

NAME	COUNTRY
FOI	Sweden
BAE Systems	United Kingdom
Detec A/S	Norway
Home Office Scientific Development Branch	United Kingdom
Institute of Psychology – Ministry of the Interior	Bulgaria
SINTEF	Norway
TNO	The Netherlands
University of Amsterdam	The Netherlands

AMASS / Autonomous maritime surveillance system

© Volodymyr Kyrylyuk - Fotolia.com

Maritime surveillance

At present, Blue Border Surveillance is carried out predominantly by coast guard ships, aeroplanes and helicopters. These expensive measures are only fragmentary.

They are not suitable to locate small boats within a wider maritime area and they do not allow a continuous 24 h/7 surveillance as a countermeasure to illegal immigration.

Concept

The surveillance system developed under the AMASS project will form an array of autonomous, automated surveillance platforms with active and passive sensors.

The key sensors being used are high-end technology-un-cooled thermal imagers and highly sophisticated Hydrophones linked together via a wideband radio network.

Alarms from the sensors will be analysed and integrated with back ground details (location, speed, class,…) into a "Geographical Information System" situated within a blue border command centre.

The operator will also be able to request live video data from the platform, should further verification be required.

The target for AMASS is the improvement of European maritime security through continuous control and surveillance, whilst reducing running costs.

Project objectives

Based on in depth research into the situational data a good understanding of the operational as well as technical requirements of such a highly sophisticated surveillance system is forming the basis of this project.

With AFM and ICCM acting as end users, tests at the end of the project will be under realistic conditions in territorial waters of countries (Malta / Canary Islands) highly affected by illegal immigration.

System configuration

The platforms forming the maritime network will be equipped with various modules:

- Optic and acoustic sensors.
- PC with related software for image stabilisation, image processing and signal generation.
- Radio equipment for bi-directional data exchange with headquarters.
- Fully autonomous power supply on the platform (renewable energy).
- Sophisticated Management-Software for the operator.

Aim

The aim of the AMASS project is to provide a system with the following features:

- Identification of small targets within the maritime environment.
- Decrease of procurement and system life costs in comparison with systems already available on the market.
- Upgrade potential (integration of additional sensors).
- Architecture allowing interface to existing surveillance systems (e.g. Vessel Traffic Control Systems VTCS).

Information

Acronym:
AMASS

Grant Agreement N°:
218290

Total Cost:
€ 4,970,709

EU Contribution:
€ 3,580,550

Starting Date:
01/03/2008

Duration:
42 months

Coordinator:

Carl Zeiss Optronics GmbH
Carl-Zeiss-Straße 22
DE – 73447 Oberkochen
Germany

—

Contact:
Thomas Anderson
Tel: +49 73 64 20 - 2833
Fax: +49 73 64 20 - 3277
E-mail: t.anderson@optronics.zeiss.com

Website:
www.amass-project.eu

Partners

NAME	COUNTRY
Carl Zeiss Optronics GmbH	Germany
Crabbe Consulting Ltd	United Kingdom
Armed Forces Malta	Malta
Instituto Canario de Ciencias Marinas	Spain
Fugro Oceanor	Norway
OBR Centrum Techniki Morskiej	Poland
Fraunhofer Institut Informations- und Datenverarbeitung	Germany
IQ-Wireless	Germany
HSF	Czech Republic
University of Las Palmas de Gran Canaria	Spain

BeSeCu / Human behaviour in crisis situations: a cross cultural investigation in order to tailor security-related communication

© Jargen Priewe - Fotolia.com

Project objectives

The aim of the BeSeCu project is to investigate cross-cultural and ethnic differences of human behaviour in crisis situations in order to better tailor security related communication, instructions and procedures with a view to improving evacuation and protection. The project will provide evidence that will be useful to first responders, building designers and those involved in the development of emergency operating procedures for buildings.

Description of the work

The BeSeCu project will carry out the following research studies:

» A cross-cultural survey of individual experiences will be conducted to identify determinants of inter-individual differences in people who have experienced evacuation situations, fire disaster survivors and survivors of similar crisis situations, but also workers and first responders as well as those affected in the community.

This retrospective study will be carried out across 7 European countries with diverse cultural background.

» Experimental trials will be carried out simulating real time evacuation scenarios in standardized settings including objective measures (e.g. response time) as outcomes as well as video-tape analysis.

Results will be analysed to identify similarities and differences between cultures and ethnic groups as well as a range of socioeconomic factors. The analysis will triangulate findings obtained with objective measures, subjective experiences and behavioural observations. The research will be carried out by a consortium of 8 European partners including end-users (e.g. fire service colleges).

Expected results

Two types of research findings and products will be provided by the BeSeCu project:

» An evidence base that will enable designers of buildings to develop culturally appropriate emergency operating procedures.

» An evidence base of inter-individual differences that will be employed to improve communication in emergency interventions.

© BeSeCu

Information

Acronym:
BeSeCu

Grant Agreement N°:
218324

Total Cost:
€ 2,446,144

EU Contribution:
€ 2,093,808

Starting Date:
01/05/2008

Duration:
36 months

Coordinator:

Ernst-Moritz-Arndt-Universitat Greifswald
Lehrstuhl Gesundheit und Pravention
Institut fur Psychologie
Robert-Blum-Str. 13
17487 Greifswald
Germany

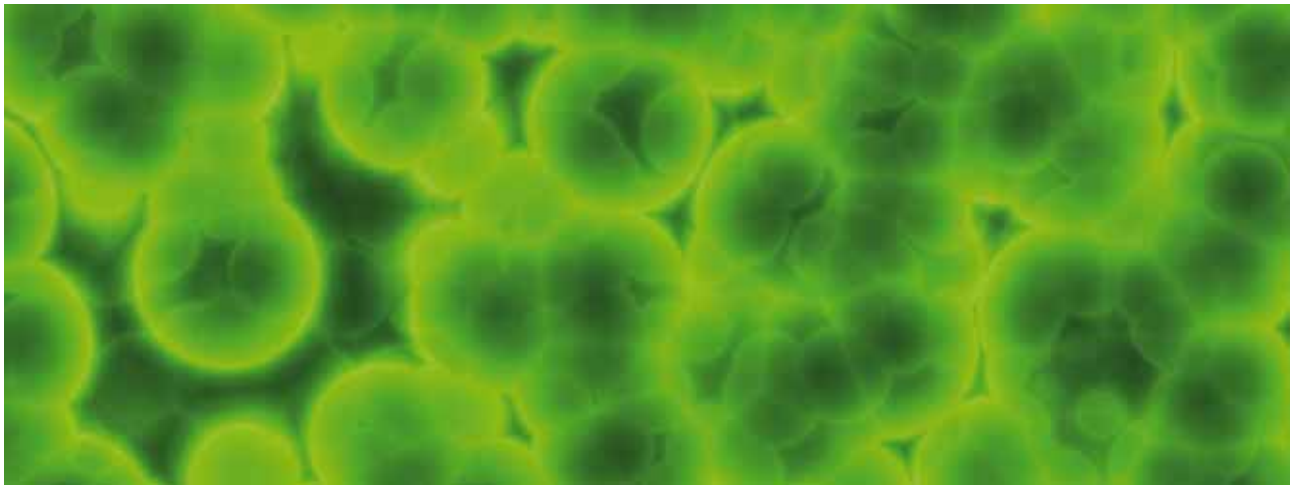
Contact:
Prof. Silke Schmidt
Tel: (+49) (0) 3834 863810
Fax: (+49) (0) 3834 863801
E-mail: silke.schmidt@uni-greifswald.de

Website:
www.besecu.de

Partners

NAME	COUNTRY
Ernst-Moritz-Arndt-Universitat Greifswald	Germany
University Medical Centre Hamburg	Germany
University of Greenwich, School of Computing and Mathematical Sciences	United Kingdom
Institute of Public Security of Catalunya	Spain
Hamburg Fire and Emergency Service Academy	Germany
Man-Technology-Organisation (MTO)-Psychology	Sweden
Faculty of Fire Safety Engineering (SGSP)	Poland
Prague Psychiatric Centre University of Prague	Czech Republic
Association of Emergency Ambulance Physicians	Turkey

BIO-PROTECT / Ionisation-based detector of airborne bio-agents, viruses and toxins for fast-alert and identification



© kentoh - Fotolia.com

Project objectives

The malevolent use of Anthrax spores on civilians in 2001 has shown the necessity to protect citizens from criminal use of biological agents. The success of such attack depends on sufficient concentration of pathogens in a defined area.

Detecting pathogenous bacteria, spores and viruses must be accomplished by triggering short-term alarm and identification of the type of threat.

Since most the bio sensors available today are laboratory bound or require special equipment which needs training as well as experience, new systems are needed.

The concept of BIO-PROTECT is the development of a fast-alert, easy-to-use device for detection and identification of airborne bacteria, spores, viruses and toxins. It is based on bioaerosol detection by fluorescence, scattering and background aerosol measurement followed by ionisation of air flow and analysis of the spectrum of relative speed of passage, enabling identification of biological agents.

Description of the work

The work in BIO-PROTECT will be structured in several technical Work Packages, addressing the following activities:

1. Development of a bio-agent detection system based on a miniaturised GC-IMS (Gas Chromatograph - Ion Mobility Spectrometry) instrument able to identify and separate extremely small amounts of a wide range of organic molecules resulting of heat-decomposed organic matter.

2. Integration of a particle size analyser which constantly monitors the ambient air, thus triggering a measurement if a sudden change in particle size and/or density occurs.

3. Improvement and integration of a continuously operating bioaerosol detector measuring fluorescence, scattering and background aerosol properties to detect presence of potentially harmful biological agents in ambient air and to trigger further identification.

4. Research and development of a combined pre-concentration and pyrolysis unit for use with a GC-IMS, that can separate all types of bio-agents from aerosols. The target is to detect bio-agent concentrations likely to infect or intoxicate.

5. Development of pattern analysis software for the interpretation of the acquired spectra, thereby identifying bio-agents and distinguishing them from background bacteria.

Expected results

The development of the proposed device will provide security personnel with a viable tool to take fast effective countermeasures on biological threats. This will drastically reduce the potential impact of terrorist aggressions or accidental release of bio-agents from laboratories, as well as detect spreading of pathogenic microorganisms in the food producing industry or in hospitals.

This breakthrough would lead to technological advantage and favour leadership of European industry in this field.

Information

Acronym:
BIO-PROTECT

Grant Agreement N°:
242306

Total Cost:
€ 3,954,812

EU Contribution:
€ 3,125,577

Starting Date:
01/06/2010

Duration:
36 months

Coordinator:

LGI CONSULTING
37, Rue de la Grange aux Belles
75010 Paris
France

—

Contact:
Vincent Chauvet
Tel: (+33) (0) 67539 8727
Fax: (+33) (0) 80074 1853
E-mail: vincent.chauvet@lgi-consulting.com

Partners

NAME	COUNTRY
LGI Consulting	France
AVSISTA	Lithuania
C-Tech Innovation Ltd	United Kingdom
Environics Oy	Finland
CEA	France
Institut für Umwelt Technologien GmbH	Germany
Robert-Koch Institut	Germany
University of Aalborg	Denmark

BOOSTER / Bio-dosimetric tools for triage to responders

© Tommy Windecker- Fotolia.com

Project objectives

The effective management of an incident involving exposure of a large number of people to radioactive material, whether accidental or following malevolent use of radioactivity requires a mechanism for rapid triage of exposed persons.

BOOSTER is a capability project to develop new bio-dosimetric tools and to integrate them into a toolbox in order to quickly evaluate the level of potential casualties and allowing an efficient triage of exposed people. A real exercise will be carried out to validate the toolbox and to train civil protection operators and define commercial exploitation potentialities.

Finally, the objectives of BOOSTER can be summarized as below:

» *Objective 1:* Rapid evaluation of radiological incidents by sensors and retrospective dosimetry.

» *Objective 2:* Development of novel, rapid bio-dosimetric capacities.

» *Objective 3:* To integrate all these sensors and methods in a portable toolbox usable by First Responders.

» *Objective 4:* To validate the tools and train the First Responders.

Description of the work

The project is divided into six workpackages:

» *Management*

» *Systems Requirements & Design Concept* A general methodology will be developed to identify the needs of the different BOOSTER end user categories and to build the global design of the system.

» *Fast evaluation* This WP aims at using and adapting existing sensors together with newly developed ones (e.g. retrospective dosimetric systems) in order to estimate the level of radiation.

» *New bio-dosimetric tools* The work is to develop new biodosimetry systems and to integrate them with other procedures to determine radiation exposure. Two techniques will be investigated:

- γ-H2AX quantification; and
- Centrosome quantification.

The two approaches we propose here can detect radiation-induced cellular responses within short-term (hours) and medium-term (1-2 days) periods after exposure and lend themselves to automation and rapid turnaround.

» *Software development and integration of components* This WP has two major objectives. First the new bio-dosimetric sensors will be integrated into a hardware package which comprises the gamma camera, the biodosimetric tools and the front-end to the first responder. The software components to be developed support not only the first responder in applying the equipment but also the commander in chief responsible locally in optimising the strategy for the use of the devices. In this respect a decision aiding component will be developed which help to optimise the application of the biodosimetric sensors.

» *System Validation and Training* The operational efficiency of the toolbox will be assessed by performing a real field exercise and train the responders in several languages.

Expected results

The development of the proposed device will provide security personnel with a viable tool to take fast effective countermeasures on biological threats. This will drastically reduce the potential impact of terrorist attacks or accidental release of bio-agents from laboratories, as well as detect spreading of pathogenic microorganisms in the food producing industry or in hospitals.

This breakthrough would lead to technological advantage and favour leadership of European industry in this field.

Information

Acronym :
BOOSTER

Grant Agreement N° :
242361

Total Cost :
€ 4,536,559.24

EU Contribution :
€ 3,284,291

Starting Date :
01/07/2010

Duration :
36 months

Coordinator :

CEA
Mehdi GMAR
CEA LIST
Bât 516, PC 72
91 191 Gif-sur-Yvette
FRANCE

Contact :
Medhi GMAR
Tel : (+33) (0) 1 69 08 39 45
Fax : (+33) (0) 1 69 08 60 30
E-mail : mehdi.gmar@cea.fr

Website :
http://www.booster-project.org/

Partners

NAME	COUNTRY
CEA	France
National University of Ireland, Galway (NUIG)	Ireland
Karlsruher Institut fuer technologie (KIT)	Germany
Izotopkutato Intezet - Magyar Tudomanyos Akademia (IKI)	Hungary
Canberra France (CANBERRA)	France
Universidad politecnica de Valencia (UPVLC)	Spain
Orszagos Atomenergia Hivatal (HAEA)	Hungary

CAST / Comparative assessment of security-centered training curricula for first responders on disaster management in the EU

© Gail Johnson - Fotolia.com

Project objectives

1. To provide all parties involved in First Responder (FR) training with fully comprehensive and trustworthy information on state-of-the-art methodologies and equipment concerning security threats to the FR community, protection of members of the FR community and disaster management by the FR community;

2. To assist in exploiting Europe's scientific and industrial strength by developing a standardised training curriculum on disaster management for FR, meeting highest quality standards and enabling the FR community in the EU to perform their challenging tasks also in the new security environment of catastrophic terrorism, in addition to threats resulting from major technical and natural disasters;

3. To overcome the current differences in training of first responders on disaster management in different EU member states by strengthening the first line of defence in a cost-efficient manner due to avoiding duplication and optimising interoperability between FR groups.

Description of the work

Security-centered training course curricula on disaster management for first responders (FR)* in EU member states will be comparatively assessed with a specially developed matrix-based software: (1) for all EU member states (2) as derived from international best practices in the US, Russia and Israel as countries with extensive experience in this field.

The comparative assessment will cover:

- Didactic areas (electronic and hardcopy teaching materials used, computer modelling, field exercises);
- Subject areas (terror threats to FR; risk assessment and management; catastrophic terrorism; weapons of mass destruction, mass killing, mass disturbance; synchronization of response staff;
- Comparative evaluation of training course curricula by virtual reality safety training with biofeedback.

Representatives of FR organisations and SME's in security technology will be involved throughout the assessment. This new integrative approach reflects the necessity of the integrative operation of end-users and representatives of the research and development community to enhance European joint- security capabilities.

The results of the assessment will be used to:

1. Establish an EU-security curricula database;

2. Identify potentially existing gaps in the EU training curricula;

3. Recommend an Action Plan for eliminating training deficiencies;

4. Develop a standardized security-centered training curriculum for first responders on disaster management;

5. Enhance the implementation of technology-based security programs into FR organisations

Expected results

Creation of a standardised training curriculum on disaster management for First Responders, covering:

- Identification of new threats leading to enhanced awareness and preparedness
- A standardised European curriculum providing enhanced interoperability
- Advanced software-technologies for interactive education, including biofeedback
- Integration of tools for enhanced interoperability
- Standardised network of information on demands and on security-related technologies

Information

Acronym:
CAST

Grant Agreement N°:
218070

Total Cost:
€ 2,858,318

EU Contribution:
€ 1,974,620

Starting Date:
01/07/2009

Duration:
24 months

Coordinator:

UNIVERSITAT SALZBURG
Office of the Rectorate
Research Support Unit
Kapitelgasse 6
A-5020 Salzburg
Austria

—

Contact:
Prof. Friedrich Steinhäusler
Tel : +43-1-890 52 57
Mobile : +43-680-123 7158
Fax : +43-662-8040 150
E-mail : steinhaeusler@isccentre.at

Website:
www.research.sbg.ac.at/cast

Partners

NAME	COUNTRY
Universität Salzburg	Austria
Austr.Tech.(AT&SFU)	Austria
DSTS-Advisers to Executives	Austria
Hamburg Fire Brigade - Academy	Germany
Research Institute of Red Cross (FRK&ABZ)	Austria
Fraunhofer Institut (Chem. Technologie)	Germany
BMLV (MoD Austria/ HVS)	Austria
University of Defense Brno	Czech Republic
Corvinus University Budapest (VGT)	Hungary
SAAB Training Systems	Sweden
Swedish Counter Terrorist Police	Sweden
Diamond Aircraft Industries	Austria
Tecnatom	Spain

CBRNEmap / Road-mapping study of CBRNE demonstrator

© Morane- Fotolia.com

Project objectives

The objectives of CBRNEmap are to:

- Develop a technological road-map for investments in research and technology developments that result in 1 to 3 demonstrator topics to be realised in phase 2 Demonstration Programme.
- Develop and achieve a broad stakeholder consensus on the CBRNEmap Road-map.
- Identify a stakeholder supported suggestion for future research investments.

Description of the work

CBRNEmap will address the cross-cutting activity required to develop a CBRNE Demonstrator using a holistic approach that puts end-users, industrialists and other stakeholders together with members of the S&T community in the forefront of development.

CBRNEmap will evaluate the complex matrix of temporal events (before, during and after), against sectors (such as law enforcement, civil protection,rescue and health together with such processes as border control, and mass transport), and will take into consideration that each of the letters 'CBRNE', may have its own aspects of vulnerabilities, priorities and possible solutions.

These generic needs will be matched by advanced technological solutions that will be integrated at the system of systems level to become the CBRNE Demonstrator.

Expected results

CBRNEmap will prioritise demonstration tasks based on systematic analysis of end-user requirement and comprehensive reviews of available CBRNE S&T investments. The final road-map will be developed for an optimised demonstration programme based on a Concept Development & Experimentation (CD&E) approach. Interlinked with developing the road-map for the CBRNE demonstrator is the analysis of gaps and needs in CBRNE research.

Information

Acronym :
CBRNEmap

Grant Agreement N° :
242338

Total Cost :
€ 1,662,022

EU Contribution :
€ 1,376,185

Starting Date :
01/06/2010

Duration :
16 months

Coordinator :

European CBRNE center at Umeå University
KBC Building
90187 UMEA
Sweden

—

Contact :
Agneta H. Plamboeck
E-mail : Agneta.Plamboeck@cbrnecenter.eu

Website :
http://http://www.cbrnemap.org/

Partners

NAME	COUNTRY
European CBRNE Center	Sweden
Police National CBRN Centre	Great Britain
National Institute for NBC Protection	Czech Republic
Robert Koch Institute	Germany
DGA Maîtrise NRBC	France
Lindholmen Science Park	Sweden
French High Committee for Civilian Defence	France
Compagnie Industrielle des Lasers	France
European Aeronautic and Space Company	Germany
FOI	Sweden
Foundation for Strategic Research	France
Istituto Affari Internazionali	Italy
Selex Galileo	Italy
Catholic University of Louvain	Belgium

COCAE / Cooperation across Europe for Cd(Zn)Te based security

© COCAE

Project objectives

Fixed and portable detectors are usually used to detect, locate and identify radioactive and nuclear material at the checkpoints such as those at road and rail boarder crossings, airports or seaports. After a first alarm signal, a secondary inspection must be performed. Handheld detectors are then used to distinguish the innocent and false alarm from the real alarms. Hundreds of innocent alarms may take place per day at the boarder control from the portal detectors.

» To make spectroscopic measurements with efficiency equivalent to that of NaI detectors and energy resolution close to that of HPGe devices but without using cryogenic systems.

» To find the direction and the distance of the radioactive source.

» To localize the source into a cargo

» To work at a wide range of absorbed dose rates by adjusting the effective volume of the detector.

The above capabilities will improve the quality of the data gathered by the customs officers during the routine inspections at the boarders and will assist the first responders in case of a radiological or nuclear emergency to estimate the exact situation.

Technology challenges

» The growth of high purity, detector grade Cd(Zn)Te crystals. Their performance will be optimized by material purification, selection of right dopants and post-growth processing to obtain high resistivity, high transport properties and homogeneous distribution of these material properties in the grown crystals. The growth of crystals with a diameter up to 75 mm will be performed.

» The fabrication of pixel detectors having structure of p-n and Schottky diodes. This will permit the application of bias voltage high enough to collect all the induced charge by both electrons and holes.

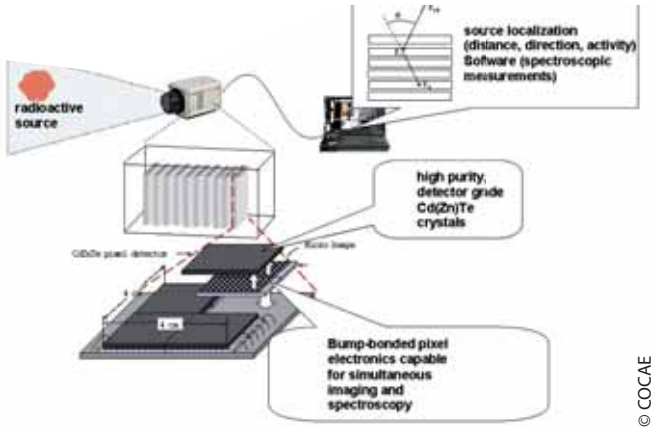
» The design of pixel electronics capable for simultaneous imaging and spectroscopy. The electronics will be bump bonded to the pixel detectors. This is essential for the localization and the identification of the radioactive source.

» The construction of a portable instrument having a stack of detecting elements.

This will allow to exploit the Compton Effect for the localization of the radioactive source and also to have variable detection efficiency.

Expected results

Measurements performed by the now available detectors cannot distinguish between a small activity radioactive source placed close to the cargo external surfaces and a high activity shield source placed in the middle of the cargo. The proposed detector has the unique ability to give information about the spatial distribution of the radioactive contamination and to detect the existence of a shielding material around the source. At the same time it will gather a high-resolution gamma ray spectrum to identify the radioisotopes case the alarm. Using this information it will be able to estimate the source activity.



© COCAE

Information

Acronym:
COCAE

Grant Agreement N°:
218000

Total Cost:
€ 2,653,077

EU Contribution:
€ 2,037,610

Starting Date:
01/09/2008

Duration:
36 months

Coordinator:

TECHNOLOGICAL EDUCATIONAL INSTITUTE OF HALKIDA (TEI)
Thesi Skliro
34400 Psahna-Evia
Greece

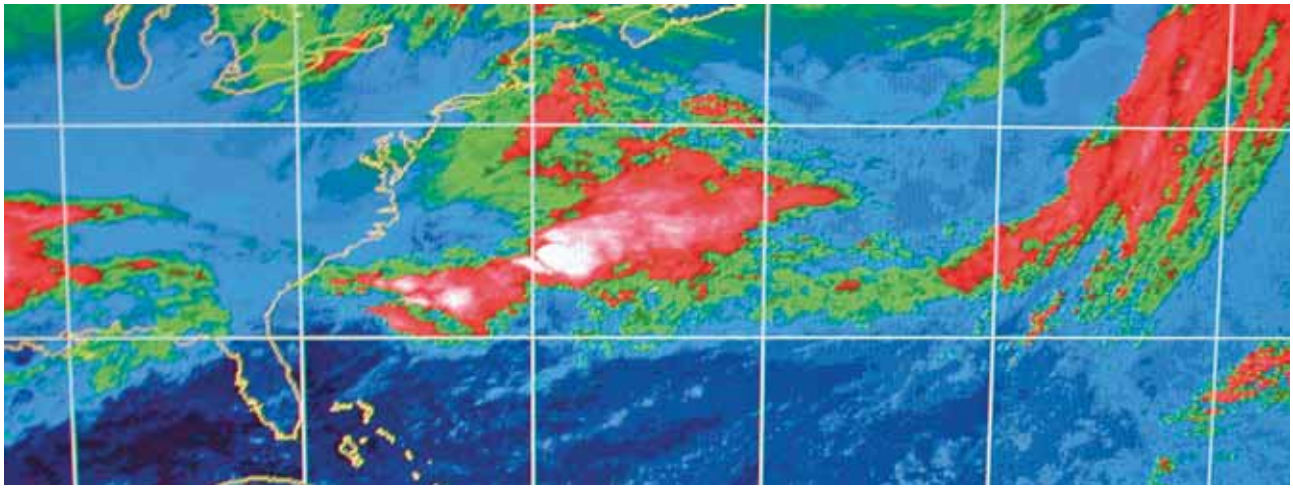
—

Contact:
Dr. Charalambos Lambropoulos
Tel: +30-22280-99631
Fax: +30-22280-23766
E-mail: lambrop@teihal.gr

Partners

NAME	COUNTRY
Technological Educational Institute of Halkida (TEI)	Greece
Greek Atomic Energy Commission	Greece
Institute of Nuclear Physics, National Center for Scientific Research Demokritos	Greece
Oy Ajat Ltd	Finland
Freiburger Materialforschungszentrum, Albert Ludwigs Universität	Germany
Universidad Autonoma de Madrid, Departemento de Fisica de Materiales	Spain
Riga Technical University	Latvia
V.E. Lashkaryov Institute of Semiconductor Physics, National Academy of Sciences of Ukraine	Ukraine
Chernivtsi Yuri Fedkovych National University	Ukraine

COPE / Common operational picture exploitation



© Janice Barchat- Fotolia.com

Project objectives

The objective of the Common Operation Picture Exploitation (COPE) project is to achieve a significant improvement in **civil crisis management** command and control performance, reliability, and cost. New solutions will be created by combing a user oriented human factors approach with the technology development.

The aim is a step improvement in information flow both from and to the first responder in order to increase situational awareness across agencies and at all levels of the **command chain** in emergency management situations.

A user-driven approach is taken to develop new technologies for supporting user information requirements at the scene of the event. First responders belong to a heterogeneous group in terms of **crisis environments** as well as roles, **command structure,** organisational and national differences.

The project applies a wide range of human factors methods from functional task modelling to end user simulations to better understand the processes of individual agencies and to ensure that new systems both match requirements and can be integrated with legacy processes and technologies.

Description of the work

The project team has much experience from crisis management projects and it uses the skills and competences of research scientists both from industry and academia, of technology providers and systems integrators supported by end users. The COPE project will develop use cases and scenarios with end users to build a rich picture of the requirements and the differences in requirements across agencies, organisations and nations. The requirements will be mapped against the technologies developed to offer tailored solutions. Commercial of-the-shelf products and novel technologies will be integrated to a prototype system allowing operational evaluation with the selected realistic scenarios.

The key objective is to develop novel technical support tools and mechanisms for collecting, gathering and disseminating information for the development of a Common Operational Picture (COP) in crisis circumstances.

The research and development work focuses on the following objectives:

- To understand and specify the information requirements of the first responder.
- To enable effective and appropriate communication links between teams at the first responder level and to enable them to feed information back to support the COP.
- To develop a user-driven methodology to understand working processes in order to map technologies on the user requirements and to take into account the similarities and differences between agencies, their differing levels of technological sophistication and to enhance capability in conjunction with legacy systems.
- To define how the first responder can feed the COP to give ground truth and to reduce the cultural power distance between the command centre and the ground.
- To trial and evaluate the technological feasibility of the solution.
- To develop and evaluate tailored computer-based decision support systems.
- To enhance the cognitive situational awareness of the first responder.

Expected results

The COPE project will develop use cases with end users to build a rich picture of the requirements and the differences in requirements across agencies, organisations and nations.

The project will realise and trial mobile technologies for:

- The ability to share ground truth with the COP.
- Increased situational awareness to enhance decision making.
- Support for multi-agency co-operation and communication.
- The ability to localise personnel, to navigate and to generate maps.
- The capability to monitor safety issues, tasking as well as post crisis audit.

Information

Acronym :
COPE

Grant Agreement N° :
217854

Total Cost :
€ 3,886,574

EU Contribution :
€ 2,535,049

Starting Date :
01/02/2008

Duration :
36 months

Coordinator :

VTT TECHNICAL RESEARCH CENTRE OF FINLAND
P.O. Box 1000
FI-02044 VTT
Finland

—

Contact :
Jari Hämäläinen
Tel : +358 20 722 6467
Fax : + 358 20 722 6027
E-mail : jari.hamalainen@vtt.fi

Website :
http://cope.vtt.fi/

Partners

NAME	COUNTRY
VTT Technical Research Centre of Finland	Finland
BAE SYSTEMS (Operations) Limited	United Kingdom
BAE Systems C-ITS AB	Sweden
University of Dublin, Trinity College	Ireland
UTI SYSTEMS Inc.	Romania
Skysoft Portugal	Portugal
Centre for European Security Strategies	Germany
General Inspectorate for Emergency Situations	Romania
Emergency Services College	Finland

CPSI / Changing perceptions of security and interventions

© Zoe - Fotolia.com

Project objectives

CPSI – Changing Perceptions on Security and Interventions –aims to create a methodology to collect, quantify, organize, query, analyse, interpret and monitor data on actual and perceived security, determinants and mediators.

The four main objectives of the project are to:

» Develop a conceptual model of actual and perceived security and their determinants,

» Design a methodology to register and process security-related data,

» Develop a data warehouse to store amassed data and

» Carry out an empirical proof-of-principle study to test the model, methodology and data warehouse.

In CPSI we focus on security related to "everyday" crime, such as theft, assault and vandalism. The CPSI methodology, however, can be applied to other areas of security as well, such as terrorism or financial security.

The main deliverables include a detailed description of the methodology, data warehouse, and empirical study. In addition, we will develop an "instruction manual" describing how an end-user can implement the CPSI methodology.

Description of the work

The core of CPSI is psychological in nature. The conceptual model is based on factors related to each individual which determine perceived security, such as demographic characteristics, personality traits and lifestyle, and history of victimization. The model was developed using literature review and morphological analysis, a structured group-discussion technique used to give concrete form to multidimensional non-quantifiable problem spaces.

Overall, however, CPSI takes an explicitly multidisciplinary approach. Aside from psychological aspects, we believe that security also has strong links with sociological factors and national culture. Specifically we will examine the relationship between public opinion and the media, in addition to an analysis of national security cultures across Europe.

In this project we will test if it is possible to answer relevant security-related questions from the field using the CPSI methodology. Example questions include:

» How does actual security relate to the subjective perception of security?
» What are the levels of perceived and actual security in specific locations?
» Which interventions work where?
» How does security change over time?

In an empirical study taking place in Amsterdam, The Netherlands, we are filling a data warehouse with data on registered crimes, results from a survey on perceived security, and analyses of media expressions concerning crimes and security in general. From this information, we can test the validity of the conceptual model and the applicability of the methodology.

The widespread implementation of monitoring tools such as the CPSI methodology brings with it ethical and legal risks related to – among other things – citizens' privacy and the use of data. In CPSI we take these issues seriously and are employing a technique known as ethical parallel research in which ethical and legal issues are addressed as they arise during the execution of the project.

Expected results

Envisaged end-users include governmental bodies at the local, provincial, national and international levels, law enforcement organisations, emergency services, other organisations engaged in policy making and strategy development.

With information from the implementation of the CPSI methodology, it will be possible for end-users to:

» Monitor security down to the neighbourhood level,

» Implement interventions in a more focused (and cheaper) manner,

» Formulate better policy,

» Learn from the experiences of others.

Information

Acronym :
CPSI

Grant Agreement N° :
217881

Total Cost :
€ 2,712,487

EU Contribution :
€ 2,165,637

Starting Date :
01/04/2008

Duration :
24 months

Coordinator :

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK – TNO
Defence, Security and Safety
Kampweg 5
P.O. Box 23
3769 ZG Soesterberg, The Netherlands

—

Contact :
Dr. Heather J. Griffioen-Young
Tel : +31-346-356-378
Mobile: +31-6-2246-1065
Fax : +31-346-353-977
E-mail : heather.griffioen@tno.nl

Website :
www.cpsi-fp7.eu

Partners

NAME	COUNTRY
TNO	The Netherlands
FOI	Sweden
University of Kent	United Kingdom
Sogeti	France
Temis	France
JRC	Italy
Centre for European Security Studies	Austria
Social Cultural Planning Office	The Netherlands
VLC	The Netherlands

CREATIF / Related testing and certification facilities / a networking strategy to strengthen cooperation and knowledge exchange within Europe

© Kentoh - Fotolia.com

Project objectives

In the 30-month project CREATIF, a network of testing facilities for security-related products and services focused to CBRNE detection will be established.

Main objectives of CREATIF are to :

» provide information on test facilities & their portfolio of expertise (database)

» support user decisions and industry product / service development

» define a roadmap for the future development of testing (incl. standardization & certification)

» harmonize testing

- initiative to produce harmonized EU-wide standards (geographic harmonization)
- exchange formal & informal information on best practice to encourage a Europe-wide uniform technical level of testing (technical harmonization, quality assurance)

» define minimum requirements of testing facilities and service providers

» generate certification strategies for facilities, service providers and devices

» offer a forum to involve decision makers, end-users and other stakeholders (industry, EU-bodies, CEN) into the discussion about security related testing

» suggest amendments to testing procedures to cover human factors and operational issues like scenario-based testing

Description of the work

The CREATIF network is dedicated to provide a communication platform for technology users and decision makers, providers and testers to discuss the future development of testing and to support user decisions and industry product / service development.

All these stakeholders are invited to become members of the network and exchange their views and knowledge: testing facilities can publish information about their expertise and testing capabilities / amenities in a database on testing facilities within EU-27, an advisory board of end-users and industrial experts will be established to integrate their point of view into project deliverables and topical workshops.

In these workshops specific themes in the field of certification and testing of CBRNE detection equipment will be discussed. Proceedings will be compiled to distribute the outcome of discussions and present information to a wide audience. CREATIF will ensure a careful examination of existing testing protocols and relevant standards to suggest harmonization of testing in the field of CBRNE detection both on a geographic scale within EU-27 and on a technical level. This will allow quality assurance and comparability of testing results. Possibilities to amend testing protocols by covering human factors and operational / scenario-based testing will be suggested. Additional deliverables of the network will be a roadmap for a European certification system for CBRNE detection products & services and a concept on the continuation of the CREATIF network as an autonomous body after the end of the funded project. Based upon the experience of network building within well-focused groups of testing experts related to CBRNE detection, CREATIF will suggest a generic strategy for expanding the network further to security related products & services.

Expected results

» Data base on testing facilities for CBRNE detection equipment & Outline for joint-testing exercises.

» Report on standards, specification for CBRNE detection methods and relevant labelling systems.

» Workshops & proceedings on specific topics related to testing of CBRNE-detection equipment.

» Road map for developing a European certification system for CBRNE sensor systems and devices.

» Report "The future of testing security related products".

» Periodic newsletter and CREATIF web-site.

» Business plan for the independent future of CREATIF network of testing facilities.

Information

Acronym :
CREATIF

Grant Agreement N° :
217922

Total Cost :
€ 831,300

EU Contribution :
€ 831,300

Starting Date :
01/02/2009

Duration :
30 months

Coordinator :

Div. Radiation Safety and Applications :
Austrian Research Centers GmbH - ARC
A-2444 Seibersdorf
Austria

—

Contact:
Friederike Strebl
Tel : +43 (0) 50550 3265
Mobile: +43 (0) 664 8251055
Fax : +43 (0) 50550 2502
E-mail : friederike.strebl@arcs.ac.at

Website :
www.creatif-network.eu

Partners

NAME	COUNTRY
Austrian Research Centers GmbH (Coordinator)	Austria
Ministère de la défense - Centre d'Etudes du Bouchet	France
Ministère de la défense - Technical Centre of Bourges	France
Cotecna Inspection S.A.	Switzerland
Federal Institute for Materials Research and Testing	Germany
FOI	Sweden
Netherlands Organization for Applied Scientific Research	The Netherlands

CRESCENDO / Coordination action on risks, evolution of threats and context assessment by an enlarged network for an r&d roadmap

©Fotolia

Project objectives

» To strengthen, enlarge and render sustainable the networks created by SeNTRE and STACCATO with Associated Countries;
» To analyse the evolution of threats (aggressions) and risks (accidents) assessment taking into account the balance between security and civil liberties;
» To analyse the policies, the regulations and standardization and encourage the harmonisation of European-wide security related regulations and standards by benefiting from the on-going national and European relevant activities with the support of CEN in connection with existing networks and associations;
» To analyse the innovation process (the demand the supply chain and the links between actors Academia, RTOs, Industries, SMEs, Service sector and End-users);
» To elaborate recommendations for some key themes for the Security Research Programme such as emerging technologies, maturity of current systems and areas of improvement, evolution of standards to enhance systems connectivity, regulatory issues if any across EU27 and associated countries in an integrated roadmap;
» To advise on the implications for future programmes as well as on the best way to continue the network and optimize the dialogue between all stakeholders.

Description of work

On the basis of SeNTRE and STACCATO PASR supporting activities, CRESCENDO will focus on keeping this unique, results-driven, multi-sector public private network alive but also on expanding it, so as to include as many as possible private sector security research requirement owners, operative end-users and technology supply chain experts, including from the new MS in the enlarged EU-27 and the Associated Countries. To achieve the objectives of the project, CRESCENDO work plan is divided into 6 technical work packages:

Organisation and operation of the network
» Experts & stakeholders Identification.
» Expert & stakeholders assessment methodology.
» Network organisation and methodology / workshops.
» Network support tools.

Society security evolutions (threats and risks)
» Assessments of threats and risks.
» Translation into security policies.
» Changing providers of security. The balance between civil liberties and security.
» Supporting the evolution of the security market.

Policies, regulation and standardization
» Regulations Mapping and Analysis.
» Standards Mapping and Analysis.
» Development of a network/expert body for policy suggestions.
» Development of a network/expert body for standardisation and regulations harmonisation proposals.
» Development of working methods and processes for the networks.

Innovation process
» Demand structuring and development.
» Regulation and supply chain.
» Ways to improve the links between the academic sector and industries, SMEs and the service sector.
» ESTIB structuring and supply chain development.

R&D Roadmaps
» Coordination with ongoing research programmes.
» Proposed R&D implementation.
» Launch of other initiatives and programmes (beyond R&D).

Consolidation and continuous dialogue and recommendations for future programmes/ projects
» Proposals and recommendations.

Expected results

» Analysis of the future capability needs and possible new threats scenario.
» Identification of technological solutions/priorities to address the capability needs leading to a technology oriented research strategy.
» Continuous mapping of European competencies initiated in STACCATO.
» Continuous update list of national, regional, European and international research programmes initiated in STACCATO, identification of possible synergies and further cooperation opportunities leading to a comprehensive strategic R&T roadmap to guide, orientate and underpin all these different research programmes.
» Supporting the definition of new standards in strong cooperation with CEN and in line with its activities and processes.

Information

Acronym :
CRESCENDO

Grant Agreement N° :
218026

Total Cost :
€ 499,523

EU Contribution :
€ 499,523

Starting Date :
07/07/2009

Duration :
24 months

Coordinator :

CEA LIST
Commissariat à l'énergie atomique
Centre de Saclay- Bât 476
F91191 Gif-Sur-Yvette Cedex
France

—

Contact :
Mr. Jean-Louis SZABO
Tel : +33 1 69 08 33 71
Mobile : +33 6 07 44 07 13
Fax : +33 1 69 08 18 19

Partners

NAME	COUNTRY
CEA	France
European Aeronautics Defence and Space Company EADS France SAS	France
Astrium SAS	France
Finmeccanica- Societa Per Azioni	Italy
Sagem sécurité SA	France
Thales avionics SA	France
Österreischiches Forschung- und Prüzentrum Arsenal GesmbH	Austria
FOI	Sweden
TNO	The Netherlands
Valtion Teknillinen Tutkimuskeskus	Finland
European Materials research society	France
Tübitak Marmara research centre information technology institute	Turkey
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.	Germany
Stiftelsen SINTEF	Norway
Fundación Robotiker	Spain
Fondation pour la Recherche Stratégique	France
Instituto Affari Internatiozionali	Italy
JRC	Belgium
European Biometrics forum limited	Ireland
Association française de normalisation	France
Ministère de l'intérieur	France
Center for Security Studies	Greece

CrisComScore / Developing a crisis communication scorecard

© Fotolia.com

Project objectives

The goal of this project is to develop an audit instrument and relevant guides for crisis communication strategies, with which public authorities are better prepared to communicate in crisis situations.

To meet this goal the project has four key objectives:

» First objective is to identify critical factors for communication strategies in *media relations* before, during and after crisis situations.

» Second objective is to identify critical factors for communication strategies in relations with *civilians and miscellaneous public groups* (survivors, casualties, deceased victims, family to workers, first responders and affected communities) before, during and after crisis situations.

» Third objective is to construct a *Balanced Scorecard* for public authorities to measure and improve their readiness to communicate in crisis situations.

» Fourth objective is to stimulate implementation by *facilitating* the use of the Balanced Scorecard and the Strategy Guides for spokespeople and crisis communication with other public groups.

Description of the work

By this project we pursue to improve crisis communication, by identifying *critical factors* in media relations and relations with civilians of miscellaneous public groups (survivors, casualties, deceased victims, family to workers, first responders and affected communities) before, during and after crisis situations. These crises may be the result of acts of nature, or acts of man (both intended, such as terrorism, or unintended, such as major accidents and infrastructure failure).

We will study communication strategies in various recent cases and analyse the reception of information in stressful situations.

By identifying critical factors the challenges of crisis communication are addressed. The findings will be reported in Strategy Guides and used as a basis for the Balanced Scorecard. The results will be available for public authorities. Many organisations use the balanced scorecard to organise a system of quality control (Kaplan and Norton, 2001).

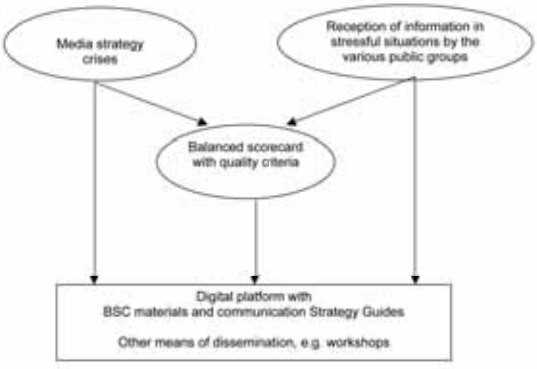
Scorecards are action-oriented and the assessment must be more than a picture of a given moment in time. It should present opportunities for a continuous process of assessment and improvement. In this sense, it can be seen as a strategic feedback system. The indicators that assess performance must aim at core processes and critical variables so that opportunities for improvement can be identified.

What is needed is an *integrated approach,* stimulating cooperation between the various organisations involved in crisis management and government levels. The consortium consists of four universities in various countries and an end user organisation that has extensive experience in the field and a good network with related public and other organisations involved in crisis management.

Expected results

The outcome of this project will be an audit instrument - a Scorecard and relevant Guides - as a tool for ensuring effective crisis communication strategies and implementation.

The Scorecard will enable public authorities to measure and improve their readiness for crisis communication. The Guides facilitate effective media relations and crisis communication strategies for various public groups. The outcome will be made available for public authorities on a digital platform together with support materials.



Information

Acronym :
CrisComScore

Grant Agreement N° :
217889

Total Cost :
€ 1,013,207

EU Contribution :
€ 799,174

Starting Date :
01/02/2008

Duration :
39 months

Coordinator :

UNIVERSITY OF JYVÄSKYLÄN YLIOPISTO
Department of Communication (Matarankatu 6)
P.O. Box 35 (TOB)
FI - 40014 University of Jyväskylä, Finland

—

Contact :
Marita Vos, prof.
Tel : +358 14 260 1554
Mobile : +358 50 4410 358
Fax : +358 14 260 1511
E-mail : marita.vos@jyu.fi

Partners

NAME	COUNTRY
University of Jyväskylä Yliopisto	Finland
Ben Gurion University of the Negev	Israel
University of Tartu	Estonia
Norwegian University of Science and Technology	Norway
Emergency Services College Finland	Finland

CRISIS / Critical incident management training system using an interactive simulation environment

© Francois Doisnel - Fotolia.com

Project objectives

The goal of the CRISIS Collaborative Project is to research and develop in Europe:

» A training and simulation environment focusing on real-time decision making and responses to simulated but realistic critical incidents, focusing on problem diagnosis, planning, re-planning, and acting, rather than just procedural training.

» A distributed, secure, scalable, based on state of the art computer games technology, enabling collaborative and interactive simulation and on-demand- training environment for crisis management training in airports, of individuals and team-based activities at command post levels.

» A readily configurable software architecture that can be used at other critical sites such as nuclear power plants.

» A flexible platform that functions as a test bed and evaluation tool for new and current operational procedures.

Description of the work

The project will be executed over a 36-month period in three stages:

» *First stage* – spiral concept development cycle where mock-ups and existing prototypes will be used to illustrate the full CRISIS approach.

» *Second stage* – the design and development of the CRISIS components will take place. The prototype will be informed by insights derived from the research team into crisis management decision support and advanced interaction technology. Early evaluation will be combined with training to give early feedback to the users. The components will then be adjusted during development and before final integration starts.

» *Third stage* – The components will be integrated into a secure architecture together with supporting tools.

Expected results

The expected impacts are :

To develop for airport crisis managers, a prototype simulation training system that will allow users across different organisations and nations to interactively experience and manage crisis and security threats in a simulated airport environment. This will enhance their operational readiness and preparedness to respond to hostile actions at airports. It will also allow users to train on demand, more frequently, and at different levels of the organisation.

Information

Acronym :
CRISIS

Grant Agreement N° :
FP7-242474

Total Cost :
€ 4,591,760.99

EU Contribution :
€ 3,495,611.99

Starting Date :
01/05/2010

Duration :
39 months

Coordinator :

SCHOOL OF ENGINEERING & INFORMATION SCIENCES,
Middlesex University
London NW4 4BT

—

Contact :
Prof. William Wong, BCom (Hons.) PhD FNZCS – Head, Interaction Design Centre.
Tel : +44 20 8411 2684
E-mail : w.wong@mdx.ac.uk

website
http://idc.mdx.ac.uk/projects/crisis/
http://www.eis.mdx.ac.uk/research/idc/

Partners

NAME	COUNTRY
Middlesex University	United Kingdom
3D Connections	Denmark
National Aerospace Laboratory	Netherlands
ObjectSecurity Ltd	United Kingdom
Space Applications Services	Belgium
VSL Systems AB	Sweden
Linkoping University	Sweden
Haskoli Island (University of Iceland)	Iceland
AE Solutions	United Kingdom
ANA	Portugal
British Transport Police	United Kingdom
Flugstodir (ISAVIA)	Iceland

CUSTOM / Drugs and precursor sensing by complementing low cost multiple techniques

© morrbyte - Fotolia.com

Project objectives

The project aims to develop a chemical sensor able to perform chemical identifications in contexts such as custom offices, where inspection of trucks, cars, containers, as well as people and baggage is required, in order to control the distribution of illegal narcotics and synthetic substances as pseudoephedrine and ephedrine.

The detection approach should use established techniques so that it can provide unambiguous response.

The project will focus on employing multiple techniques, integrating them in a complex system in a complimentary approach, in order to identify an optimum trade-off between opposite requirements: compactness, simplicity, low cost vs. sensitivity, low false alarm rate, selectivity.

Description of the work

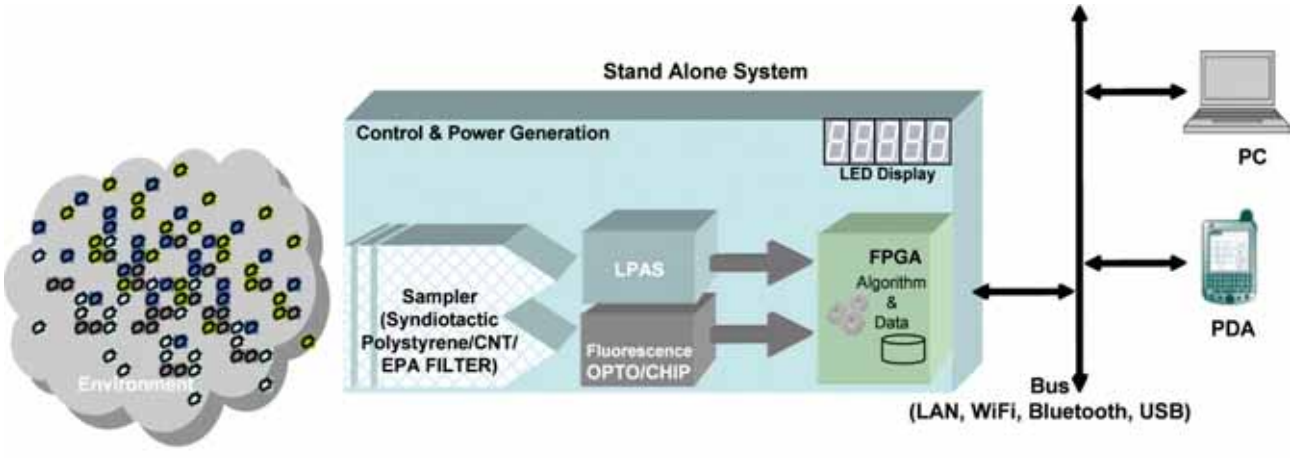
A drug precursor sensor demonstrator, implementing two main techniques will be developed:

- a low cost, high data throughput sensing technique, based on UV-Vis-NIR fluorescence which incorporates an array of different properly engineered chemical proteins able to bind the target analytes as happen in an 'immuno-type' reaction; and
- a highly sensitive and selective, compact and low weight, spectroscopic sensing technique in Mid-IR optical range, based on Laser Photo-Acoustic Spectroscopy (LPAS).

Parallel efforts will be spent on: identifying proper sampling techniques both for vapour and powder phase compounds; collecting or, where not existing, building-up a database of characteristic spectra for both measurement techniques.

Expected results

The sensor will be able to detect Drug Precursor such as ephedrine, P2P, BMK, Acetic anhydride and Phenylacetic acid and others compound with a screening time of 10 seconds and a sensitivity of 50ppm.



Information

Acronym :
CUSTOM

Grant Agreement N° :
242387

Total Cost :
€ 5,295,523

EU Contribution :
€ 3,486,406

Starting Date :
01/06/2010

Duration :
36 months

Coordinator :

SELEX SISTEMI INTEGRATI

—

Contact :
Anna Maria Fiorello
Tel : + 39 (0)6 4150 3104
Mobile: + 39 3351379733
E-mail : afiorello@selex-si.com

website
www.selex-si.com

Partners

NAME	COUNTRY
SELEX Sistemi Integrati	Italy
GASERA	Finland
University of TURKU	Finland
INAS-Tecnalia	Spain
Alcatel-Thales III-V Lab	France
CNR IBP	Italy
ENEA	Italy
INSTM	Italy
Aalto University Foundation	Finland
Direction Nationale du Renseignement et des Enquêtes Douanières	France

DECOTESSC1 / Demonstration of counterterrorism system-of-systems against CBRNE phase 1

© Martijn Smeets - Fotolia.com

Project objectives

DECOTESSC1 proposes a demonstration of a counterterrorism system-of-systems against CBRNE.

The basic idea of DECOTESSC1 is an analysis and subsequent prioritization of the gaps between the current situation and the ideal situation of CBRNE system-of-systems counterterrorism.

Furthermore, a strategic roadmap will be proposed that should aim at filling the identified gaps. This includes linkages with related subject areas and with stakeholder communities and a study regarding proposals for real demonstrations in phase 2. The strategic roadmap to be developed in DECOTESSC1 will address the full concept of an EU counterterrorism system-of-systems against CBRNE and outlines all the necessary missions, tasks, capabilities, systems, technologies, etc. to be considered.

Description of the work

DECOTESSC1 starts with developing a thorough understanding of the system-of-systems structure. Based of this the requirements for an ideal system will be proposed as well as a description of the current state-of-the art. A gap analysis will reveal the differences between the current situation and the ideal situation. The gaps thus obtained will be ranked. Also, in order to fill the gaps a strategic roadmap will be developed to guide the improvement cycle by proposing, technological and organizational topics to be addressed and implemented in a future phase 2 of the demonstration project CBRNE counterterrorism and beyond.

This will be primarily done by a Core Group of partners. In addition, to achieve this, the DECOTESSC1 project will, on top of the efforts of the Core Group, consider the needs of the various stakeholders (government representatives, local authorities, users with different think-tanks, universities, RTOs and industry (including SMEs)) by direct interaction. This will be achieved by involving the stakeholders, brought together in an Expert Group, by continuously organizing workshops at relevant moments during the work of DECOTESSC1, by organizing a mid-term stakeholders meeting and well as a final symposium. Interviews with individual stakeholders will also be a mechanism for interaction.

All interactions above will not only provide input for DECOTESSC1s work but also provide dissemination of its findings throughout the EU community and raise awareness for this very important subject area.

Expected results

A well defined picture of ideal solutions in all phases of the security cycle before and after a possible attack yielding a layered and threat- and scenario-related set of requirements for the system-of-systems of CBRNE counterterrorism.

A strategic roadmap will be defined as a strategy to fill the gaps that are identified and ranked, both at an integrated system-of-systems level as well as sub-system level.

Recommendations will be made in order to define the Phase 2 CBRNE demonstration project. Also proposals for suitable demonstrations will be made.

Information

Acronym :
DECOTESSC1

Grant Agreement N° :
242294

Total Cost :
€ 1,587,642

EU Contribution :
€ 1,001,627

Starting Date :
01/04/2010

Duration :
15 months

Coordinator :

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk Onderzoek - TNO
Schoemakerstraat 97
PO Box 6060
NL-2600 JA Delft
The Netherlands

—

Contact :
Mr Mark van den Brink
Tel: +31 703740160
Fax: +31 152843963
E-mail: mark.vandenbrink@tno.nl

Website :
www.decotessc1.eu

Partners

NAME	COUNTRY
TNO	The Netherlands
Seibersdorf Labor GmbH	Austria
JRC	Belgium
AIT Austrian Institute of Technology GmbH	Austria
CEA	France
Fundación Inasmet	Spain
FOI	Sweden
Valtion Teknillinen Tutkimuskeskus	Finland
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V	Germany

DEMASST / Demo for mass transportation security: roadmapping study

© NZ photo - Fotolia.com

Project objectives

DEMASST is the first phase of the FP7 demonstration programme for security in mass transportation with the task to provide a roadmap for the development and integration of system-of-system solutions. By virtue of the similarity of problems across big cities in Europe, such security solutions have a potentially very important EU-wide market.

Mass transportation systems with their very high densities of people are attractive targets for intentional malevolent acts, as already evidenced by devastating attacks in EU Member States. They are public and easily accessible, the passengers often carry hand luggage where explosives or weapons can be hidden and there are many persons concentrated in an enclosed area. But in addition to their potential for very large human casualties, due to crime or accident, mass transportation systems are also a critical infrastructure for employees to get to their workplaces, meetings, etc. Disturbances to this function may have very large economic consequences.

Description of the work

DEMASST will take on the dual challenges of analysis and networking necessary to define and achieve commitment for the strategic roadmap for the Phase 2 Demonstration project. "Mass transportation" in the context of the security terminology used in the European Union is mostly oriented towards urban public transportation, such as metro, tram, commuter train, city busses and inter-modal, critical nodes including those connecting long-distance transports with urban transport systems. The approach of DEMASST is thus a broad range of public transport but focusing on rail in megacities.

DEMASST will develop a highly structured approach to the demonstration programme built on identifying the main security gaps and the most promising integrated solutions, utilising sufficiently mature technologies for filling them. In this process, DEMASST also expects to identify both "low-hanging fruit" (useful integrated solutions with very near realisation) and more futuristic research priorities.

In the type of system-of-system development approach proposed, the experiments must be designed and analysed so as to be maximally informative. Given the vast variation in mass transportation systems, an effective demonstration programme must also identify synergies between demo tasks and use less costly methods than full-scale demonstration whenever helpful – or necessary due to security constraints for example.

DEMASST proposes to build the methodological infrastructure for this. But an optimal demo project design does not stop with finding scientific answers: the issue of turning demonstration into innovation is top on DEMASST's agenda. And this approach will have utility also beyond transportation. The project is planned to be carried out between January 2009 and April 2010.

Expected results

- Roadmap for phase II.
- Comprehensive and structured mass transport threat database.
- State-of-the-art on mass transport security legacy.
- "Low hanging fruit" for quick implementation.
- Identification of future research needs.
- Generic development of the system-of-system development programme instrument.
- Awareness-raising and network-building.

Information

Acronym:
DEMASST

Grant Agreement N°:
218264

Total Cost:
€ 1,840,555

EU Contribution:
€ 956,650

Starting Date:
12/01/2009

Duration:
16 months

Coordinator:

FOI (SWEDISH DEFENCE RESEARCH AGENCY)
Division of Defence Analysis
SE-16490 Stockholm
Sweden

—

Contact:
E. Anders Eriksson
Tel : +46-8 5550 3747
Mobile: +46 709 277 281
Fax : +46-8 5550 3866
E-mail : e.anders.eriksson@foi.se

Website:
http://www.demasst.eu

Partners

NAME	COUNTRY
FOI	Sweden
Ansaldo STS	Italy
CEA	France
Diehl	Germany
EADS Astrium	France
FFI	Norway
Fraunhofer-INT	Germany
INECO	Spain
SINTEF	Norway
TECNALIA-INASMET	Spain
THALES Security Systems	France
TIFSA	Spain
TNO	The Netherlands
VTT	Finland

DETECTER / Detection technologies, terrorism, ethics and human rights

© V. Yakobchuk - Fotolia.com

Project objectives

To identify human rights and other legal and moral standards that detection technologies in counter-terrorism must meet, while taking into account the effectiveness of these technologies as judged by law-enforcement bodies responsible for counter-terrorism, and other relevant authorities.

Description of the work

After 9/11 and the terrorist bombings in Madrid (11 March 2004) and London (07 July 2005), policing and intelligence activity have increasingly focused on methods of preventing future attacks, and not just on identifying the perpetrators of offences already committed. Preventive police work includes the use of detection technologies. These range from CCTV camera-surveillance of suspicious behaviour in public places to secret internet monitoring and data-mining. Such technologies raise ethical and legal issues (notably issues of privacy) that must be confronted against the background of the legal and ethical issues raised by counter-terrorism in general.

This project will review detection technologies, and identify ethical issues of preventive counter-terrorism measures. It will survey developments in international law in support of counter terrorism, particularly in human rights. It will look at data mining, electronic surveillance of internet traffic and the use of pre-entry screening measures for migrants, including asylum-seekers.

Meetings are planned with policy makers, manufacturers and law-enforcement officials to present assessments of both desirable and undesirable features of detection technology products, as well as general standards for products to meet.

Expected results

The project will produce a substantial review of the human rights' consequences of countering terrorism. The project will meet with technology developers, commissioners, users and provide reports and papers setting out the moral, ethical and legal framework for these products. A survey of data mining technologies and electronic surveillance of the internet and other counter- terrorism techniques will be undertaken and assessed and safeguards proposed. A major conference will be held in the UK to disseminate the project's results to all those working in this field.

Information

Acronym :
DETECTER

Grant Agreement N° :
217862

Total Cost :
€ 2,424,416

EU Contribution :
€ 1,869,684

Starting Date :
01/12/2008

Duration :
36 months

Coordinator :

UNIVERSITY OF BIRMINGHAM
Dept. of Philosophy, School of Social Sciences
Edgbaston
United Kingdom
B15 2TT BIRMINGHAM

—

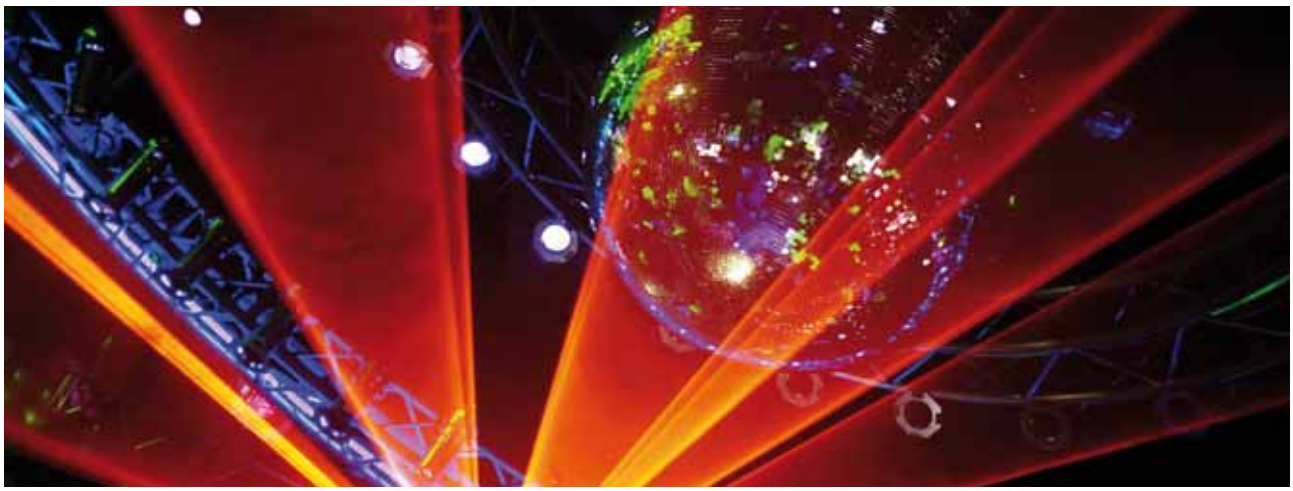
Contact :
Tom Sorell
Tel : +44-121-414-8443
Fax : +44-121-414-8453
E-mail : t.sorell@bham.ac.uk

Website :
www.detecter.bham.ac.uk

Partners

NAME	COUNTRY
University of Birmingham	United Kingdom
Åbo Akademi University	Finland
University of Nottingham	United Kingdom, until 31.01.09
University of Zurich	Switzerland, from 01.02.09
University of Oslo, Centre for Human Rights	Norway
Raoul Wallenberg Institute of Human Rights and Humanitarian Law	Sweden
Danish Institute for Human Rights	Denmark
European University Institute	Italy

DIRAC / Rapid screening and identification of illegal drugs by IR absorption spectroscopy and gas chromatography



© G.K. - Fotolia.com

Project objectives

The goal of this project is to develop an advanced sensor system that combines miniaturized Gas Chromatography (GC) as its key chemical separation tool, and Hollow-Fiber-based Infra Red Absorption Spectroscopy (HF-IRAS) as its key analytical tool to recognize and detect illicit drugs and precursors. Currently, GC-IRAS (through FTIR implementation) is, together with GC-Mass Spectrometry, the most powerful technique for the identification and quantification of amphetamines. However, so far it has been implemented only as bench-top instrumentation for forensic applications and bulk analysis. In DIRAC, the use of micromachined GC columns, solid state lasers, and hollow fibres IR, will allow to develop a sensor that features hand-portability and prompt response –for field operation– and is capable to perform both bulk and trace analysis. The DIRAC sensor will further feature a) an advanced sampling device, that separates the analyte from larger amounts of materials by electrostatic charging; and, b), an advanced micro-machined pre-concentrator that treats sequentially both volatile ATS substances and non volatile ammonium salts.

Description of the work

The project has a duration of 42 months, and is divided into three phases as follows:

» Phase 1 (6 months), where requirements are reviewed;

» Phase 2 (24 months), where the sensor is developed together with its sensing modules, techniques and procedures;

» Phase 3 (12 months), where the sensor is tested, optimized and validated.

The main Work Package (WP) active in phase 1 is **WP1**, where a review is made of the target chemicals (amphetamines, precursors, and street compounds) and of the operational requirements for the sensor.

WPs active in phase 2 are:

» **WP2,** where the sensing prototype is developed, with its strategies, procedures, and process controls

» **WP3,** that develops the sampling module, with its methods and procedures

» **WP4,** that develops the pre-concentration module, with its methods and procedures

» **WP5,** that develops the HF-IRAS module, with its methods and procedures

» **WP6,** that develops the GC separation and detection module, with its methods and procedures

» **WP7,** that develops the Expert System as a pattern recognition and learning machine.

The main WP active in phase 3 is **WP8**, where the sensor is tested and validated in the lab and through a small-scale field-campaign, and performance is assessed quantitatively, that is in terms of False Positive and False Negative Probabilities.

The Work-Plan further includes a **WP0** (Management) and a **WP9** (dissemination and exploitation of results), both active along the full duration of the project.

Expected results

The main output of the project will be the initial prototype of a sensor capable to provide real support to customs officers in their daily fight against the trafficking and distribution of illicit drugs. The prototype is therefore expected to show:

» Reliability (ability to reject interferents);

» Hand portability;

» Fast response (few minutes);

» Good sensitivity (tens of nano-grams or better);

» Broad chemical spread (sensitivity towards different drugs and precursors);

» Identification capacity, (ability to distinguish one target compound from another at least on a family base).

Information

Acronym:
DIRAC

Grant Agreement N°:
242309

Total Cost:
€ 4,256,753.33

EU Contribution:
€ 2,987,717

Starting Date:
01/06/2010

Duration:
42 months

Coordinator:

CONSORZIO CREO
Centro Ricerche Elettro-Ottiche
SS 17 Localita Boschetto
L'Aquila 67100, Italy
—

Contact:
Sandro Mengali
Tel: +39-0862346210
Fax: +39-0862346201

Website:
www.consorziocreo.it

Partners

NAME	COUNTRY
Consorzio CREO- Centro Ricerche Elettro-Ottiche	Italy
Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V	Germany
Consiglio Nazionale delle Ricerche	Italy
EADS Deutschland GMBH	Germany
ELSAG DATAMAT S.p.A.	Italy
Universite de Lausanne	Switzerland
Universitatea Dunarea de Jos Din Galati	Romania
Institut National de Criminalistiek en Criminologie	Belgium
National Bureau of Investigation	Finland
Consorzio Interuniversitario Nazionale per la Scienza e la Tecnologia dei Materiali	Italy

DITSEF / Digital & innovative technologie for security & efficiency of first responder operations

© sonya etchison - Fotolia.com

Project objectives

One of the main problems of the First Responders (FR) (fire fighters, police, etc.) in case of crisis occurring at critical infrastructures is the availability of relevant information for the First Responder level and for the local manager. The loss of communications and location, the lack of information concerning the environment (temperature, hazardous gases, etc.) and the poor efficiency of the Human Machine Interface (HMI) on the first responder side are the main current drawbacks. Therefore, during the intervention there is a gap between the First Responders' situation (positioning, health, etc.) and the overall overview at their mobile headquarter.

DITSEF aims at increasing the effectiveness and safety of First Responders by optimal information gathering and sharing with their higher command levels.

Description of the work

The Ditsef project is organised in a number of sub projects and 5 worshops:

» *First Workshop :* The first workshop is dedicated to the common and usual scenarios which drive for a FR interventions (analysis of potential threats, typical emergency operations with definition of role of FR according their defined missions).
End-user inputs: Presentation of some typical infrastructures (arrangement of the buildings, legal constraints, emergency measures) and of typical intervention of FR

» *Second Workshop :* Discussion and analysis of the technical and functional requirement issues.
End-user inputs: classification of expected functional requirements in line with defined scenarios.

» *Third Workshop :* Presentation by the consortium of the selected technologies (innovated and/or improved) and analysis by end-users.
End-user inputs: Analysis and Classification of the most valuable future technical solutions proposed by R&D.

» *Fourth Workshop:* Presentation of innovative results proposed by R&D in line with the End-users support.
End-user inputs: Analyse and comments with the R&D team of the proposed solutions and first view on the integration in a systemic approach.

» *Fifth Workshop :* Demonstration on site with concrete FR evolving in concrete site and scenario.
End-users inputs: Discussion on future needs and research plan experimentation and demonstration program.

Expected results

The Ditsef project will provide solutions in four areas :

» Communication
» Indoor localisation
» Sensors
» Human Machine Interface

The aim of the project is to propose to integrate these technologies into a system through scenarios validated by the end users.

These new technologies must respond to the end user's needs.

Information

Acronym :
DITSEF

Grant Agreement N° :
225404

Total Cost :
€ 4,245,436

EU Contribution :
€ 2,800,000

Starting Date :
01/01/2010

Duration :
36 months

Coordinator :

Sagem Defense Securite (SDS)
Le Ponant de Paris
27 Rue Leblanc
F-75512 Paris Cedex 15
France

—

Contact :
Philippe Clément
Tel: +33.1 69 19 94 85
E-mail : Philippe.clement@sagem.com

Website :
http://www.ditsef.eu/

Partners

NAME	COUNTRY
Sagem Defense Securite (SDS)	France
TNO	Netherland
EADS	France
Center for Security Studies (KEMEA)	Grece
CEA	France
Elsag Datamat spa (ED)	Italie
National Centre for Scientific Research "Demokritos"	Grece
INFITHEON Technologies Ltd (INFI)	Grece
T - SOFT spol. s r.o. Praha	Czech Republic
Ministry of Emergency Situations Territory Depertment"Civil Protection"- Montana Region	Bulgaria

E-SPONDER / A holistic approach towards the first responder of the future

© Fotolia.com

Description of the work

The proposed system addresses the need for an integrated personal digital support system to support first responders in crises occurring in various types of critical infrastructures under all circumstances. E-SPONDER proposes modular terminal and overall open system architecture in order to facilitate the need for enhanced support provision in all cases. It deals with the study, design and implementation of a robust platform for the provision of specialized ad-hoc services, facilities and support for first responders that operate at crises scenes located mainly within critical infrastructures. In order to address the diverse needs stemming from the complexity of operations, a three-layer approach is proposed. Modularity is a key issue to the overall system design whether it refers to the mobile/dispersed units of the first responders or the back-office applications, systems and services.

» *First Responder Units (FRU).* As far as the first responders' units are concerned, different operational needs have to be addressed according to the origin of the first responder. In other words, there are different functional, performance and specific requirements for different users including police officers, paramedics, rescuers and fire brigades crewmen.

» *Mobile Emergency Operations Centre (MEOC)* The Mobile Emergency Operations Centre is a vital part of the entire system. It provides a common operational picture of the situation as well as a communication bridge between the first responders that operate in the field and the main, remotely located Emergency Operations Centre (usually located at Civil Protection Headquarters).

» *Emergency Operations Centre (EOC)* The Emergency Operations Centre is the heart of the E-SPONDER platform. It contains the entire necessary infrastructure (communications, GIS, data processing modules, database) suitable and selected for crisis management purposes.

» *Training of First Responders* The goal of the E-SPONDER platform is to provide, at both a state and local level, an up-to-date list of available trained personnel that can be identified and deployed quickly in the event of a crisis situation. In that sense, E-SPONDER will help the authorities to better define first responder job profiles and technical competencies. These profiles and competencies will then be managed by the e.Learn platform that will link individual competency gaps to learning and development, and create a central repository of resources and associated skill sets for proactive selection and succession planning.

» *Logistics of First Responders* A full and comprehensive analysis and study of the current situation as well as the one derived from E-SPONDER outcomes will be performed in order to set up the conceptual design parameters of an Emergency Management Process based on ERS&LS (Emergency Resource Support & Logistics System) capable of providing comprehensive situational awareness to decision makers to ensure a timely, co-ordinated and effective response to large scale disasters.

Expected results

Measures	Metrics
Preparedness	
Percent of responders trained to respond to anticipated emergencies (e.g. 15 planning swcenarios)	100%
Safety Officer(s) have the training and experience necessary to manage hazards associated with all potential planning scenarios	YES
Percent of responders capable of using E-SPONDER (e.g., responders are fitted and medically cleared to use necessary E-SPONDER components) so that they have the necessary health and safety training to perform their anticipated tasks (e.g. awareness level, technician level, etc.) in response to an incident	100%
Activate Response Safety and Health	
Percent of responders injured or falling ill in response to the incident	0%
Time in which Safety Officer is designated within the First Response structure (separate from MEOC, who may hold this role for a period of time)	Within 30 minutes from arrival of responders
Time in which deployment actions are initiated for Assistant Safety Officers or Safety Officers to provide technical assistance to incident safety official	Within 1 hour from arrival of responders
Identify safety needs	
Percent of hazards detected/identified and characterized	100%
Time in which an initial incident safety analysis is completed	Within 1 hour from responder arrival
Site/Incident Specific Safety and Health Training	
Percent of emergency workers responding to an incident who are provided on-site training prior to assignment to work at incident	100%
Ongoing Monitoring of Responder Safety and Health	
Time in which the medical unit is opened and operating within a MEOC structure	Within 30 minutes from arrival of responders arrival on-site
Percent of personnel wearing the required E-SPONDER equipment for site entry and work	100%
Percent of workers who have their representative exposure to hazardous substances quantified and recorded	100%

Information

Acronym:
E-SPONDER

Grant Agreement N°:
FP7-242411

Total Cost:
€ 12,922,363.40

EU Contribution:
€ 8,790,044

Starting Date:
01/07/2010

Duration:
48 months

Coordinator:

EXODUS S.A.
6-10 Farandaton Street
11527, Athens
Greece

—

Contact:
Dr. Dimitris Vassiliadis
Tel: +30.210.7450321
Fax: +30.210.7450399
E-mail: dvas@exodussa.com

Website:
www.e-sponder.eu

Partners

NAME	COUNTRY
Exodus S.A.	Greece
University of Modena and Reggio Emilia	Italy
CrisisPlan B.V.	The Netherlands
Prosyst Software GmbH	Germany
Immersion S.A.	France
Rose Vision	Spain
Telcordia Poland Sp. z.o.o.	Poland
Centre Suisse d'Electronique et de Microtechnique S.A.	Switzerland
Smartex Srl	Italy
Technische Universität Dresden	Germany
YellowMAP AG	Germany
PANOU S.A.	Greece
Telcordia Taiwan	Taiwan
Institute for Information Industry	Taiwan
Entente pour la forêt Méditerranée	France

EFFISEC / Efficient integrated security checkpoints

© Natalia Bratslavsky - Fotolia.com

Project objectives

Illegal immigration and illicit material detection is a growing concern at the European borders; in that respect border security checkpoints must be particularly efficient against any kind of threat.

Seaport checkpoints differ strongly from airports ones and are more complex to process. The global objective of EFFISEC, a mission oriented project, is to deliver to border authorities more efficient technological equipment: that provides higher security level of identity and luggage control of pedestrians and passengers inside vehicles, at land and maritime check points.

In the same time, EFFISEC will maintain or improve the flow of people crossing borders and will improve the work conditions of border inspectors, with more powerful capabilities, less repetitive tasks, and more ergonomic equipment.

Description of the work

EFFISEC is based on the integration of a set of existing and complementary technologies (biometrics, e-documents, signal recognition and image analysis, trace and bulk detection of substances, etc.). It will take into account legal and privacy issues and will also include a standardisation step.

EFFISEC will allow performing systematic security check of pedestrians, cars and buses with a high level of confidence while keeping high the flow crossing a border. It will allow lowering the number of travellers, luggage and vehicles that have to go through in depth supplementary checks, out of line.

EFFISEC will benefit of recent progress in e-Gates for Airport, and it is expected that some results (like automatic luggage scanning with the e-Gate) will be transferred back to airport security solutions.

The project concentrates on land and seaport checkpoints. It is clear that transposition of the project results to other types of checkpoints, as for example trains and in particular high speed train (HST/TGV) stations, will be quite easy and it is expected that it will be carried by some EFFISEC partners interested in providing security solutions.

By the end of the project, EFFISEC prototypes results will need industrial development for massive deployment in mid-term (2014-2020) at land/maritime border check points.

Expected results

EFFISEC will provide border officers with up-to-dated technologies:

- allowing systematic in depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles, through the use of automatic gates and portable identity check and scanning equipment,
- providing objective criteria for submitting some travellers/vehicles/luggage to an extensive check in specific lanes.

Based on a detailed analysis of the operational requirements (including ergonomics, security and legal issues) for all types of borders, EFFISEC will focus on four technical key issues: documents and identity check, detection of illicit substances, video surveillance and secured communications.

The technology proposed will be demonstrated for pedestrians, and travellers using cars and buses; standardisation aspects will be considered and results disseminated.

Information

Acronym:
EFFISEC

Grant Agreement N°:
217991

Total Cost:
€ 16,310,974

EU Contribution:
€ 10,034,837

Starting Date:
01/05/2009

Duration:
48 months

Coordinator:

SAGEM SÉCURITÉ
Le Ponant de Paris
27 Rue Leblanc
F-75015 Paris Cedex 15
France

—

Contact:
Krassimir Krastev
Tel: +33 (0) 1 58 11 25 43
Fax: +33 (0) 1 58 11 87 01
E-mail: krassimir.krastev@sagem.com

Website:
www.effisec.rdc.ac.uk

Partners

NAME	COUNTRY
Sagem Sécurité	France
Thales Security Systems	France
Thales Electron Devices	France
Galileo Avionica	Italy
Elsag Datamat Spa	Italy
Smiths Heimann	Germany
Sociedad Europea de Analisis Diferencial de Movilidad	Spain
VTT	Finland
FOI	Sweden
University of Reading	United Kingdom
Ministry of Interior – Romanian Border Police	Romania
Secalliance	France
MC2	France
Port of Lisbon	Portugal
JRC	European Union
Thales Security Systems Portugal	Portugal

EMILI / Emergency management in large infrastructures

© TebNad - Fotolia.com

Project objectives

The project EMILI ("Emergency Management in Large Infrastructures") is a capability project which aims at a new generation of data management and control systems for large infrastructures (CIs) including appropriate simulation and training capabilities. New Internet-based technologies like active and reactive behaviour through complex event processing and event action rules will be developed and adapted. Semantic technologies will allow computer systems to capture the meaning of a large variety of information relevant in emergency management.

Description of the work

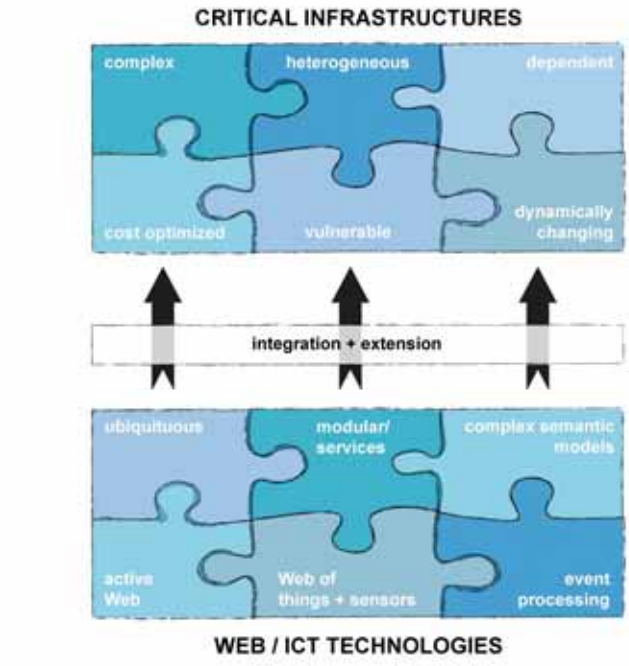
This is especially important in the case of emergencies and crises. Large Infrastructures are cost intensive, large, complex technical systems. They are frequently operated at their limits. Today, they are changing their characteristics rapidly in various respects. These CIs depend on each other and interact with each other in many ways. Even small disturbances may trigger avalanches of failures in the same system and in depending ones. Quick and adequate reactions are key factors in safe and efficient operations of Critical Infrastructures today. Currently used data management and control systems of large Infrastructures mainly collect data from their own system and process them in a more or less pre-defined way. In order to adapt today's control systems to the new challenges - especially to an efficient management of emergencies - we need a new generation of these control systems, their methodology and technology

Expected results

This new generation of control systems is needed in order to improve the security of CIs like power grids and telecommunication systems, airports and railway systems, oil and gas pipelines under future technical, economic, organisational, political, and legal conditions. Especially with a view to an efficient management of emergencies - a new generation of these control systems, their methodology and technology is needed.

EMILI's results will support the need for more complex and sophisticated control systems for CIs. This includes the necessary sophisticated human operator decision support. Training systems built on EMILI's technology will enable effective and efficient preparation of people to all relevant kinds of decision making in critical situations.

Airport, public transport (Metro) and power grid systems will serve as demonstration and validation base.



Information

Acronym:
EMILI

Grant Agreement N°:
242438

Total Cost:
€ 3,997,230.40

EU Contribution:
€ 3,139,228

Starting Date:
01/01/2010

Duration:
36 months

Coordinator:

FRAUNHOFER IAIS
Schloss Birlinghoven
D-53754 Sankt Augustin
Germany

—

Contact:
Dr. Rüdiger Klein
Tel: +49 2241 14 2608
Fax: +49 2241 14 2342
E-mail: Ruediger.Klein@IAIS.Fraunhofer.de

Website:
www.emili-project.eu

Partners

NAME	COUNTRY
Fraunhofer IAIS	Germany
Asit AG	Switzerland
Aplicaciones en Informática Avanzada SA	Spain
Skytec AG Consulting in Information Technologies	Germany
Stichting Centrum voor Wiskunde en Informatica (CWI)	The Netherlands
Institut Mihajlo Pupin	Serbia
Ludwig-Maximilians-Universität München	Germany

ESCoRTS / European network for the security of control and real-time systems

© TebNad - Fotolia.com

Project objectives

ESCoRTS is a joint endeavour among EU process industries, utilities, leading manufacturers of control equipment and research institutes, to foster progress towards cyber security of control and communication equipment in Europe. This coordination action will address the need for standardisation in this area (where Europe lags behind other world actors), indicating R&D directions by means of a dedicated roadmap.

ESCoRTS will be a leading force for disseminating best practice on Supervisory Control And Data Acquisition (SCADA) security implementation, ensuring convergence and hastening the standardisation process worldwide, and paving the way to establishing cyber security testing facilities in Europe.

Networked computers reside at the heart of critical infrastructures and systems on which people rely, such as the power grid, the oil & gas infrastructure, water supply networks etc. Today these systems are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, or expose private information.

Attacks compromising security of monitoring and control systems may also have negative impact on the safety of personnel, the public and the environment, by causing severe accidents like blackouts, oil spills, release of pollutants in the air, water and soil.

Pressure to ensure cyber security of control and communication systems is strong in the US, where industry sectors - electricity, oil, gas etc. are issuing guidelines and have set up a common platform, the Process Control Systems Forum. There national facilities where to test the security of control and communication components are available. . In the EU, the importance of the issue starts to be recognized as well: vendors and many users are trying to accommodate what emerges as best practice security.

Nevertheless, a common strategy towards standardisation is lacking; the efforts are scattered across industrial sectors and companies. In addition, due to the lack of testing facilities in the EU, manufacturers and operators currently need to resort to US cyber security facilities to verify their products and services.

Description of the work

The key objectives of ESCoRTS include:

- Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation, accompanied by a raising awareness programme reaching all stakeholders.
- Identifying and disseminating best practice, possibly in a joint endeavour between manufacturers and end users, resulting in a joint capability and technology taxonomy of security solutions.
- Stimulating convergence of current standardisation efforts. Liaising with international efforts and especially with the US Process Control Forum.
- Developing a strategic R&T and standardisation roadmap.
- Developing and deploying a secure ICT platform for the exchange of relevant data among the stakeholders.
- Identifying requirements for appropriate test platforms for the security of process control equipment and applications.

Expected results

ESCoRTS will result in coordinating standardisation efforts in the sector and in paving the way for the development of testing facilities for industrial cyber equipment across Europe.

The consortium is inter-sector, and involves the main EU manufacturers of SCADA equipment under CEN lead, and important SCADA end-users in different processes: power generation, electricity transmission and water management. A stakeholder board including partners from several process areas (power, gas, oil, water, chemicals and petrochemicals, pharmaceuticals) will ensure coherence between, and across, the different stakeholders and activities.

Information

Acronym :
ESCoRTS

Grant Agreement N° :
218245

Total Cost :
€ 1,076,091

EU Contribution :
€ 673,603

Starting Date :
16/06/2008

Duration :
30 months

Coordinator :

COMITÉ EUROPÉEN DE NORMALISATION (CEN)
Rue de Stassart 36
BE – 1050 Bruxelles
Belgium

—

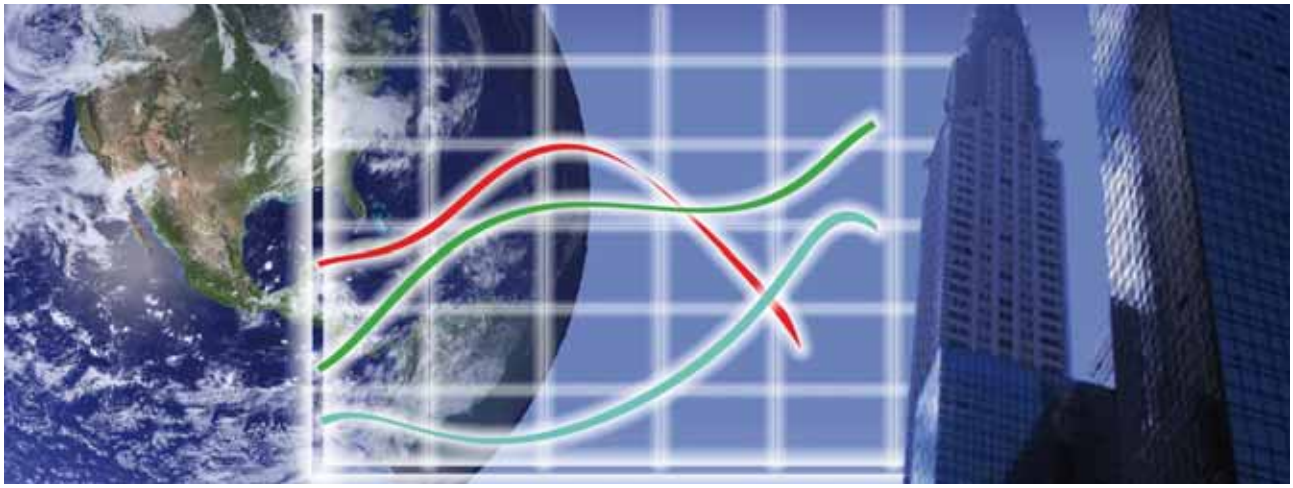
Contact :
Luc Van den Berghe
E-mail : luc.vandenberghe@cen.eu

Website :
www.escortsproject.eu/

Partners

NAME	COUNTRY
CEN	Belgium
JRC	European Union
ABB	Switzerland
Areva	France
Siemens	Germany
Opus	United States of America
EngiNet	Italy
ENEL	Italy
Transelectrica	Romania
Mediterranea delle Acque	Italy
UNINFO	Italy

ESS / Emergency support system



© Phil_Good- Fotolia.com

Project objectives

The purpose of ESS is to enable improved control and management of major crisis events such as natural disasters, industrial accidents, terror attacks etc. The idea guiding the development of ESS is a portable, modular and autonomous system which fuse in real-time various forms of field-derived data including video, audio, weather measurements, location tracking, radioactivity, biochemical, telecom derived data, affected population reports and other information. The data is collected and communicated via both portable and fixed platforms including wireless communication devices, Unmanned Aerial Vehicle (UAV), Unmanned Ground System (UGS), air-balloon and field-vehicles. The fusion of the data is handled within a central system which performs information analysis and provides decision support applications for web based command and control systems. This provides flexible, yet comprehensive coverage of the affected area.

Once available to the market, the ESS concept will offer real time synchronization and information sharing between first responders and support forces at the site of the incident. ESS will also enable the commanders to communicate with the affected on-site personnel by sending text (SMS) or recorded voice messages.

Description of the work

The ESS consortium intends to develop a revolutionary crisis communication system that will reliably transmit filtered and pre-organized information streams to the crisis command system, which will provide the relevant information that is actually needed to make critical decisions.

The information streams in ESS will be organized in such a way that they can be easily enhanced by and combined with other available applications and databases (thus enabling the coupling of the ESS system with crisis decision support systems currently under development). The ESS will provide an open API in order to allow any public authority, if needed, to add more applications customized to its particular needs. ESS interfaces are open as they are based on OGC standards. Each commercial application which will adopt OGC standards will be able to connect to ESS in a plug and play manner.

Any abnormal event may register as a sudden change or cumulative changes in one or several mediums which it interacts with (Telecom, Air, Spatial, Visual, Acoustic and more). Therefore, effective control of such an abnormal event means: monitoring each medium independently in real-time, activating an alarm when sudden or cumulative changes in one or more mediums are detected, and when necessary contacting the affected population and providing mass evacuation capabilities. ESS will integrate all these means to one central system which will enable crisis managers to respond to these challenges.

In order to validate the system it will be tested in three different test fields: a fire in a forested area, an event in a crowded stadium and a toxic waste dump accident. Operating ESS under different scenarios is needed in order to test the system's capabilities in different kinds of crises using a variety of collection tools.

The partners in the ESS project are on the forefront of technological development. Each of the partners brings important and complementary expertise to the project. Three partners represent the end users for ESS technologies, solutions and perspective.

Expected results

First and foremost, ESS will aid in the development of novel tactical intelligence system for crisis events. In addition, ESS will change the way data is gathered and handled during times of crisis. Other important advances that will be brought about by ESS will be the development of novel methods for decision support, and the use of web-portals as hubs for real-time, actionable information. Lastly, additional technological impacts that are expected from the development of the ESS system include, for example, the integration of road traffic information systems.

Information

Acronym:
ESS

Grant Agreement N°:
217951

Total Cost:
€ 14 M

EU Contribution:
€ 9,1 M

Starting Date:
01/06/2009

Duration:
48 months

Coordinator:

VERINT SYSTEMS LTD
Mr. Gideon Hazzani
33 Maskit St Herzliya, 46733 Israel

—

Contact:
Mr. Gideon Hazzani
Email: Gideon.Hazzani@verint.com,

Website:
www.ess-project.eu

Partners

NAME	COUNTRY
VERINT SYSTEMS LTD	Israel
Wind Telecomunicazioni SpA	Italy
International Geospatial Services Institute	Germany
Intergraph CS	Czech Republic
GMV Sistemas S.A.	Spain
CS Systèmes d'Information	France
Fraunhofer Institute IAIS	Germany
ITIS Holdings plc.	UK
Algosystems SA	Greece
Alcatel-Lucent Italia	Italy
APD Communications Ltd.	UK
Centre d'Essais et de Recherche de l'Entente	France
ANCO S.A.	Greece
FAENZI srl.	Italy
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
The Imego Institute	Sweden
Magen David Adom	Israel
Ernst & Young	Israel
Aeronautics Defense Systems	Israel

EULER / European software defined radio for wireless joint security operations

© RCP Photo - Fotolia.com

EULER collaborative research project gathers main European actors to demonstrate how the benefits of Software Defined Radio can be leveraged in order to enhance interoperability and fast deployment in case of crisis needed to be jointly resolved.

Project objectives

Communication systems used on field by security organisations constitute major elements enabling restoring security and safety after crisis in an efficient manner. Large scale events necessitate the cooperation between security organisations of different nature and different nations. In connection with a strong group of end-users in Europe, EULER will contribute in proposing a more agile, interoperable, robust communication system supporting a new range of services to its users. In order to achieve these goals, three main components will be combined: a reference high-data-rate radio technique, a communication system architecture allowing integration of heterogeneous radio standards and Software Defined Radio (SDR) as a key enabler for this.

Description of the work

Enable enhanced deployment of protection organisations on a crisis location: groups gathered to operate need their radio systems to coexist and to be inter-connected, with short configuration time. EULER will provide a reference system architecture enabling on-the-field integration of such radio techniques.

Enhance the capabilities of wireless communication systems to enable high-speed communication backbone and also allow emerging types of services (such as on-field video, telemedicine, on-field sensors' values transmission) but also usual PMR ones. To this end, a new reference high-speed radio waveform will be proposed in line with functional, security and operational conditions (e.g urban, rural areas, …).

Provide fully programmable radios via a standardised software interface (Software Defined Radio), allowing to realise the system architecture and reference wireless communication waveform in a software-portable fashion, hence guaranteeing re-usability of these elements across platforms from different organisations and suppliers.

EULER approach towards the objectives

The consortium will be dealing with activities of several types. The overarching one will consist of interacting with public-safety organisations to shape and refine operational scenarios and requirements. Analysis, specification and interaction with standardisation bodies will be the basis for implementation in the several areas the project targets. These outcomes will constitute one of the first European demonstrators of interoperability in a civil- crisis situation based on SDR.

© wayne ruston - Fotolia.com

Information

Acronym :
EULER

Grant Agreement N° :
218133

Total Cost :
€ 15,468,483

EU Contribution :
€ 8,720,692

Starting Date :
01/03/2009

Duration :
36 months

Coordinator :

THALES COMMUNICATIONS S.A.
Boulevard de Valmy 160
FR-92700 Colombes
France

—

Contact :
Bruno Calvet
Tel : +33 (0) 1 41 302 084
Fax : +33 (0) 1 46 132 555
E-mail : bruno.calvet@fr.thalesgroup.com

Partners

NAME	COUNTRY
Thales Communications S.A	France
Eads Secure Networks	France
Astrium Limited	United Kingdom
Budapest University of Technology and Economics	Hungary
Elsag Datamat s.p.a.	Italy
Selex Communications S.P.A.	Italy
Telespazio S.P.A.	Italy
Universita di Pisa.	Italy
Saab Communications	Sweden
TNO	The Netherlands
Indra Sistemas S.A.	Spain
Rohde & Schwarz gmbh.	Germany
Center for Wireless Communications, University of Oulu	Finland
Prismtech Limited	United Kingdom
IMEC	Belgium
JRC	Belgium
Ecole Superieure d'Electricite	France
Elektrobit Wireless Communications	Finland

EURACOM / European risk assessment and contingency planning methodologies for interconnected networks

© Fotolia.com

Project objectives

EURACOM addresses the issue of the protection and resilience of energy supply for European interconnected energy networks.

Its objective is to identify, together with European critical energy infrastructures operators, a common and holistic approach (end-to-end energy supply chain) for risk assessment and risk management solutions.

By establishing links and coherent risk management procedures across energy sectors and EU countries, the resilience of critical energy services across the whole ('end-to-end') energy infrastructure chain is sought to be increased.

Description of the work

EURACOM will pursue 4 main objectives:

» *Promoting a dialogue between energy and security stakeholders.*

EURACOM will initiate a common platform for discussion and future decision-making at European level between all stakeholders of the energy chain from the different European countries, thus strengthening a common understanding of threats and risks, the establishment of common procedures, and developing effective and coherent tools for the planning of contingency measures.

The EURACOM Consortium planned several activities: 6 workshops and a final conference will take place in 2010. Some of these workshops will be sector-specific, and all of them will address risk assessment and contingency planning methodologies.

» *European Forum for Energy Infrastructures – Security and Resilience*

The EURACOM Project seeks to set up a lasting Forum to establish trust and co-operation among the energy supply and demand sides. To this end, a restricted website, will link national users and operators and enable them to share information in an environment of mutual trust.

A common European methodology for risk management and contingency planning

By linking the different approaches at national and local level, EURACOM aims at creating the basis for a common and coherent methodological approach across different sectors of the energy infrastructure supply chain, enabling cost-effective cooperation and coordination across the extended borders of the European Union.

This Pan-European methodology will be derived from:

- the definition of generic energy infrastructure/network model,
- the study of available methodologies,
- the identification of commonalities, and
- practical discussions and exercises with energy infrastructures operators.

» *Supporting European policies for the protection of critical energy infrastructures*

The EURACOM Partners will eventually make suggestions to support European policies for the protection of critical energy infrastructures, as well as to start the creation of a comprehensive and common understanding on part of the Member States and sectoral stakeholders for the development of more secure, integrated frameworks, and for the implementation of emergency plans.

Expected results

The EURACOM methodology will not only offer the basis for common and compatible assessment and management tools that can be adapted to different situations, energy operators, and countries, but it will also reinforce the European industry's potential to create important market opportunities.

The common methodology will also contribute to enhanced co-operation and co-ordination across Europe, the development and promotion of metrics, standards, evaluation and certification methods and best practices, which will improve the overall protection of energy infrastructures.

Information

Acronym :
EURACOM

Grant Agreement N° :
225579

Total Cost :
€ 1,038,290

EU Contribution :
€ 833,860

Starting Date :
01/07/2009

Duration :
18 months

Coordinator :

EOS – THE EUROPEAN ORGANISATION FOR SECURITY

—

Contact :
Sophie Batas
E-mail : Sophie.batas@eos-eu.com

Website:
www.euracom-project.eu

Partners

NAME	COUNTRY
EOS -The European Organisation for Security	EU
ALTRAN	France
CEA	France
JRC	The Netherlands
TNO	The Netherlands
THALES	United Kingdom
EDISOFT	Portugal

EU-SEC II / Coordinating national research programmes and policies on security at major events in Europe

© Fotolia.com

Project objectives

The main objective of EU-SEC II is to facilitate the interaction between different stakeholders in the European technology research, thereby synchronizing efforts, as well as an adequate level of coordination between national and European efforts to achieve cost effective security solutions. The project aims at contributing to the harmonization of national research policies and to the common understanding and identification of needs and priorities among its Partners, all EU national authorities, through the creation of a durable structuring effect of the demand side of the European technology market. Thus, the involved Partners will be able to address the technology suppliers, push the market to effectively react to meet their exigencies. Furthermore, EU-SEC II will be able to elaborate strategic research and technology roadmaps to guide, orientate and underpin European, national and private research programmes and the consequent allocation of funds. The final goal and ambition of EU-SEC II is to assist the creation of a European House of Major Events Security (EHMES), a long-lasting tool at the disposal of EU countries hosting a major event. The EHMES will provide both coordination methodologies and technical assistance, delivering results that will be sustainable over a long period of time and remain useful for EU Member States in future decades.

Description of the work

In order to achieve its objectives, a step by step approach has been devised to implement the various phases of the coordination plan:

Information exchange
Providing with a mapping exercise that will ensure the systematic exchange of information on existing national research programmes and policies among Partners.

Strategic activities
Exploring complementarities, gaps and barriers to the coordination and management of available human and financial resources of different national research programmes and policies, laying the bases to support the innovation needed thought the development of the project.

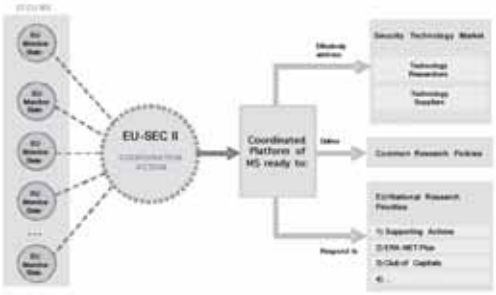
Joint activities
Producing a common methodology for the joint elaboration of a common research policy, paving the way for the elaboration of a pilot security research and technology strategic roadmap for European, national and private research programmes.

Transnational activities
Setting the modalities of concrete response of the EU-SEC II Partners to European and national research priorities and exigencies in the field of security at Major Events, while simultaneously becoming the main interlocutor for the private sector and all other stakeholders involved in the provision of security in Europe.

EU-SEC II Manual
Collecting all materials and documents resulting from the implementation of the project in order to provide the International community with a manual of best practices in coordination of research programmes and policies in the field of security at Major Events.

Expected results

- Harmonization of national research policies.
- Synchronization of national end-users into a coordinated platform to effectively address other stakeholders' requirements involved in the provision of security at Major Events.
- Elaboration of a common understanding, identification and ways to respond to research needs and priorities among EU-SEC II Partners and EU national authorities thorough the creation of a durable structuring effect of the demand side of the European technology market.
- Elaboration of a strategic research roadmap for relevant EU and national institutions.



Information

Acronym:
EU-SEC II

Grant Agreement N°:
218037

Total Cost:
€ 2,527,000

EU Contribution:
€ 2,527,000

Starting Date:
01/07/2008

Duration:
36 months

Coordinator:

UNITED NATIONS INTERREGIONAL
Crime and Justice Research Institute
Security Governance and Counter-Terrorism Laboratory
Italy- 10127- Turin

—

Contact:
Alberto Pietro Contaretti
Tel: +39 011 6537 111
Fax: +39 011 6313 368
E-mail: contaretti@unicri.it

Website:
www.eu-secii.org

Partners

NAME	COUNTRY
United Nations Interregional Crime and Justice Research Institute	Italy
EUROPOL	The Netherlands
Bundesministerum für Inneres / Ministry of the Interior	Austria
German Police University	Germany
Cuerpo Nacional de Policía	Spain
Ministry of the Interior / Police Department	Finland
Direction Générale de la Police Nationale	France
Metropolitan Police Service	United Kingdom
An Garda Siochana	Ireland
Ministero degli Interni	Italy
Ministry of Justice	The Netherlands
Ministry of the Interior / Higher Institute on Police Sciences and Internal Security	Portugal
Centre for Security Studies	Greece
Police Academy of Latvia	Latvia
Ministry of Interior and Administration Reform General Inspectorate of the Romanian Police	Romania
Ministry of Interior of the Slovak Republic	Slovakia
Academy of the Ministry of the Interior	Bulgaria
Policijska uprava Maribor	Slovenia
Personal Protection and Law Enforcement Police	Estonia
Cyprus Police	Cyprus
Hungarian National Police Headquarters	Hungary
Malta Police Force	Malta
Swedish National Police Board	Sweden
National Police Department / National Police College	Denmark

EUSECON / A new agenda for european security economics

Project objectives

EUSECON strives to create an analytical framework for complementary research within the discipline of security economics. This framework relates human-induced insecurity (terrorism and organised crime) to other forms of insecurity (industrial accidents, natural disasters, geo-political insecurity) and security measures.

Beyond creating this framework and defining the field of security economics, EUSECON provides policy advice for security policy makers, security research programme makers, and security research analysts. This is achieved by focusing scholarship on the relationships between human-induced insecurity (terrorism and organised crime), security provision, and the prevailing socio-economic policy framework.

EUSECON will investigate the relationship between security, insecurity, and the economy by drawing on the research activities of the project participants, the most relevant European players in this field.

This research capacity has allowed research to focus on the underlying micro-economic processes and resulting macro-economic impacts both conceptually and in the European context.

Description of the work

EUSECON's strategy focuses on utilizing an overarching theoretical framework to relate human-induced security threats, such as terrorism or organised crime, to other forms of insecurity such as natural disasters, industrial accidents, and conflict.

It will employ the following methods:

» Acknowledging Historical Context: The work strategy will revisit occurrences of insecurity in their historical contexts, going beyond identifying the conceptual and practical similarities and differences between forms of insecurity.

» Analyzing Perceptions of Insecurity: Efforts will be focused on understanding the responses of stakeholders of various levels, on differentiating between inter- and intra-national conflict, and on understanding the historical notions of insecurity among the different member states of the EU.

» Filling Knowledge Gaps: A research strategy will be implemented that strives to fill data gaps and overcome the current methodological problems in order to account for the economic repercussions of security and insecurity.

Expected results

A clear research strategy that defines the field of security economics and copes with insecurity and its economic consequences will be developed:

» Knowledge gaps, including those that deal with responses to insecurity at the micro level, will be filled.

» Increased understanding of the costs and benefits of security policies will produce results which can be used to improve policy making in the EU.

» Academic and policy relevant knowledge will be disseminated quickly and efficiently within the European security economics research community, promoting continued study in the area.

» EUSECON developed a conceptual framework for the project as a whole in the first year. Outputs include papers on the definition of security economics, data requirements and availability, a historical mapping of security policies in the EU, and a look at insecurity threats from the policy-maker's perspective. These outputs are disseminated through the Economics of Security Working Paper Series, which can be accessed from the project's website (www.economics-of-security.eu/eusecon).

Information

Acronym:
EUSECON

Grant Agreement N°:
218105

Total Cost:
€ 3,000,736

EU Contribution:
€ 2,357,188

Starting Date:
01/03/2008

Duration:
48 months

Coordinator:

GERMAN INSTITUTE FOR ECONOMIC RESEARCH
Department of International Economics
Mohrenstr. 58, 10117 Berlin, Germany

—

Contact:
Prof. Dr. Tilman Brück
Tel: +49-30-89789-591
Fax: +49-30-89789-108
E-mail: tbrueck@diw.de

Website:
www.economics-of-security.eu/eusecon

Partners

NAME	COUNTRY
German Institute for Economic Research	Germany
Institute for Peace Research and Security Policy at the University of Hamburg	Germany
Economics Institute of the Academy of Sciences of the Czech Republic	Czech Republic
Charles University Prague	Czech Republic
University of Patras	Greece
The Chancellor, Masters and Scholars of the University of Oxford	United Kingdom
Queen Elisabeth House, University of Oxford	United Kingdom
Centre for Criminology, University of Oxford	United Kingdom
Ingeniería de Sistemas para la Defensa de España, S.A.	Spain
Basque University	Spain
RAND Europe	United Kingdom
Hebrew University Jerusalem	Israel
University of Thessaly	Greece
University of Linz	Austria
International Peace Research Institute, Oslo	Norway
Institute of Social Studies	The Netherlands

FASTID / Fast and efficient international disaster victim identification

© FASTID

Project objectives

1. Development of an information management and decision support system for disaster victim and missing person identification satisfying end user requirements enabling the storing and comparison of different characteristics which may lead to the identification of any one individual.

2. To develop an internationally acceptable format and training for accurate and repeatable data recording in the system.

3. To test and evaluate the system.

4. To develop exploitation strategies.

Description of the work

The project will start by collecting detailed end-user requirements.

It will be necessary to consider not only the performance of the system itself for international and national police work but also its interface to INTERPOL's present network and channels for uploading and distributing data and other identification software.

These requirements will feed into the design of the overall system and the specific specifications for system modules and interfaces.

A core system will be developed taking INTERPOL's paper Ante-Mortem (AM) Disaster Victim Identification (DVI) form and Post-Mortem (PM) DVI together with its Yellow Notice and Black Notice forms, which use the minimum international standards agreed to date for the collection of data for identification of victims and present software as a basis and these will be extended with Rich Internet Application methods and further identification techniques.

An 'aide aside' will be designed that will facilitate a commonality of reporting and understanding of the terms in the INTERPOL forms leading to a better understanding of the nature of the data being recorded and its true international translation. This will form the starting point for a full online training programme which will be developed utilising the most effective and efficient means of ensuring operational commonality between countries and organisations.

Research will be carried out into image retrieval methods for assisting forensic identification with respect to faces, body modifications (e.g. tattoos), decorations, property and clothing. 3D morphing and craniofacial reconstruction and superimposition approaches will be investigated for this application. The best results are planned to be implemented into the core system.

There will be extended testing and evaluation of the results in and these will allow for some development reiteration. Exploitation strategies will be developed.

Expected results

A centralised worldwide system at INTERPOL's General Secretariat in Lyon with decentralised access, applicable to disasters and everyday policing. The system will include its own search capabilities for some identifiers and will be interfaced to other software for further identifiers such as fingerprints. It should be possible for INTERPOL's General Secretariat and its member countries to use a fully operational system within a short time-to-market period.

Information

Acronym:
FASTID

Grant Agreement N°:
242339

Total Cost:
€ 2,990,190

EU Contribution:
€ 2,270,476

Starting Date:
01/04/2010

Duration:
36 months

Coordinator:

THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION — I.C.P.O.
INTERPOL, General Secretariat
200, Quai Charles de Gaulle
69006 Lyon, France

—

Contact:
Peter Ambs, Operational Police Support Directorate
Tel: +33 (0)4.72.44.72.92
Fax: +33 (0)4.72.44.73.80
E-mail: p.ambs@interpol.int

Website:
http://www.interpol.int/FASTID.asp

Partners

NAME	COUNTRY
INTERPOL	France
Bundeskriminalamt	Germany
Plass Data Software A/S	Denmark
UNIVERSITY OF DUNDEE	United Kingdom
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V	Germany
Crabbe Consulting Ltd	United Kingdom

FESTOS / Foresight of evolving security threats posed by emerging technologies

© Nmedia - Fotolia.com

Project objectives

New technologies can greatly improve our quality of life, but they may also have a "dark side". What if technologies that we have not yet imagined end up being inadequately used or even intentionally abused?

The objectives of FESTOS are to identify and assess evolving security threats posed by the abuse or inadequate use of emerging technologies and new scientific knowledge and to propose means to reduce their likelihood.

Looking ahead to the year 2030, this foresight study will scan the horizon of fields such as nanotechnologies, biotechnologies and information technologies, as well as capabilities that may emerge from converging technologies.

Possible prevention means and policy measures will be studied in the context of trade-offs between security needs and the freedom of research and knowledge, taking into account shifts in public perceptions of threats and related security issues.

Description of the work

FESTOS is based on three pillars: a) identifying new potentially threatening technologies and fields of techno-science research; b) assessing emerging threats and constructing related scenarios, with appropriate early-warning indicators and c) deriving preparedness measures and policy guidelines.

FESTOS will first identify relevant emerging technologies and new techno-science research areas which may be the source of potential threats. The focus is on five main areas: material science, robotics, nanotechnologies, biotechnologies and information technologies. In addition, relevant technologies may emerge from the convergence of different fields. Emerging and evolving threats will then be evaluated by using various methods:

- Expert surveys to forecast likely onset of threat realization, assign prioritization and project the nature and extent of potential damage and social issues.
- Brainstorming to identify, discuss, classify and assess the potential threats.
- Listing and classifying interesting "weak signals" in order to identify "wild cards": unlikely but highly affecting events.

Specific threat scenarios will be developed that will take societal contexts (e.g. changing perceptions of security) into account, and will pay special attention to potentially high- impact events, even if perceived as very unlikely.

Critical early-warning indicators that hint at the growing likelihood of specific scenarios will be identified. Also, FESTOS will analyse the needs for monitoring and control on the proliferation of knowledge-form R&D activities, taking into account societal and ethical issues in the context of trade-offs between security, human rights and the freedom of research and knowledge creation. A policy workshop will be organised based on FESTOS' results, to be attended by representatives of relevant stakeholder groups. Policy guidelines and recommendations will be derived for the EU as a whole as well as for its individual member countries.

Expected results

- Awareness of potential threats of specific new technologies.
- Initiation of a foresight process in Europe that continuously scans the unfolding technology landscape in anticipation of evolving threats.
- Alternative scenarios that outline future impacts of security threats with special attention to low likelihood but high- impact events.
- Identification of "early warning signals" that might hint at the growing likelihood of unforeseen scenarios.
- Policy guidelines aiming at novel means of preparedness for future threats.

Information

Acronym :
FESTOS

Grant Agreement N° :
217993

Total Cost :
€ 1,232,976

EU Contribution :
€ 824,552

Starting Date :
01/03/2009

Duration :
30 months

Coordinator :

INTERDISCIPLINARY CENTER FOR TECHNOLOGY ANALYSIS AND FORECASTING (ICTAF)
Tel-Aviv University
Israel
69978 RAMAT AVIV, TEL AVIV

—

Contact :
Yair Sharan
Tel : +97236407574
Mobile: +972544381600
Fax : +97236410193
E-mail : sharan@post.tau.ac.il

Website :
www.festos.org

Partners

NAME	COUNTRY
Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF)	Israel
Turku School of Economics, Finland Futures Research Centre	Finland
Foundation for European Scientific Cooperation	Poland
EFP Consulting	United Kingdom
Technical University of Berlin	Germany

FORESEC / Europe's evolving security: drivers, trends and scenarios

© Cornelius - Fotolia.com

Project objectives

The objective of FORESEC is to tie together the multiple threads of existing work on the future of European security so as to provide more cogent guidance, orientation and structure for all future security-related research activities. It aims to enhance the shared understanding of the complex global and societal nature of European security, in order to pre-empt novel threats and capture technological opportunities. In particular, FORESEC seeks to identify security responses in which there is particular added-value and shared interest to work at the European level. FORESEC is targeted to provide critical policy support and advice for security researchers and decision-makers, including the European Security Research and Innovation Forum (ESRIF), with a view to providing recommendations in the medium-to-long-term timeframe. Due to the nature of support actions, FORESEC also produces results relevant to policy matters and the broader security policy community. FORESEC forms a pan-European network for European security foresight and helps foster societal debate on European security and security research.

Description of the work

FORESEC achieves its results through a participatory process aimed at deepening the dialogue within European societies on security issues and by nurturing broad, pan-European participation by including stakeholders from governments, universities, the private sector and civil society in EU Member States

FORESEC employs the following methods:

- *Desk study:* A state-of-the-art scan of security and security research in 12 selected EU Member States and an analysis of the global context of European security are conducted to provide a common basis for the participatory foresight process.
- *Participatory foresight methods:* A kick-off workshop initiated public debate on European security and provided commentary and validation of state-of-the-art findings regarding threats and drivers. The workshop also produced statements on security and the security technologies that were used in the Delphi survey.

Delphi: FORESEC engaged a broad range of experts and stakeholders through the Delphi survey which was carried out in two rounds online. The objective of survey was to identify future trends relevant to European security that go beyond what is generally known. The survey focused on societal trends in Europe and their relevance to security; global trends with a major impact on EU security; technologies and innovations related to European security; and the creation of a European conception of security. The results of the Delphi survey were further systematically analysed and evaluated. An analytical framework for the assessment of security challenges and their drivers was developed and used as input for the scenario analysis.

Scenario analysis: Scenario analysis involves a small multidisciplinary group of experts in six selected countries. The scenario analysis aims to help to understand the specific threats that might manifest themselves in the lives of European citizens and to identify national and European level policy options that can prevent, counter and mitigate the threats and identify security gaps. The analysis is based on five to six threats that emerged as most prominent in the Delphi survey and which clearly represent a European consensus with European dimensions. The scenario analysis will reveal societal and ethical challenges as well as possible technological opportunities.

Expected results

The concrete results of the project are:

- A series of reports: global and country reports, Delphi report, trend-assessment reports, drivers and threats, scenario descriptions and analysis, technological opportunities and a final summary report,
- An interactive website,
- Vision-building and dissemination events,
- Increased public interaction and involvement as a stakeholder in the process.

The more intangible outcomes of the project include:

- Enhanced networks, i.e. creating, expanding and maintaining networks of people and organisations from different sectors working with security issues across Europe,
- The development of a consensus and a shared vision regarding European security,
- Creation of a foresight culture on European security,
- Integration of Foresight results into the European Security Research, policy programmes and national programmes.

Information

Acronym :
FORESEC

Grant Agreement N° :
218199

Total Cost :
€ 942,202

EU Contribution :
€ 942,202

Starting Date :
01/02/2008

Duration :
22 months

Coordinator :

CRISIS MANAGEMENT INITIATIVE
Pieni Roobertinkatu 13 B 24-26
00130 Helsinki, Finland

—

Contact :
Kristiina Rintakoski
Tel : +358 9 4242 810
Fax : +358 9 4242 8110
E-mail :kristiina.rintakoski@cmi.fi

Website :
http://www.foresec.eu

Partners

NAME	COUNTRY
Crisis Management Initiative	Finland
Austrian Research Centres System Research	Austria
International Institute for Strategic Studies	United Kingdom
FOI	Sweden
Centre for Liberal Studies	Bulgaria
JRC	Italy

FRESP / Advanced first response respiratory protection

© Loren Rodgers - Fotolia.com

Project objectives

Protection against terrorism is one of the major issues of this programme. If an incident occurs, despite precautions taken to prevent incidents at all, it is important to reduce the consequences, i.e. to minimise the effects of chemical, biological, radiological and nuclear (CBRN) attacks.

The objective of the project is to create the network of scientists and research institutions, who will develop a broad-spectrum, low-burden, tailor-made nanoporous adsorbent, with the aim to integrate the two main areas of protection (versus chemical warfare agents and versus toxic industrial chemicals) without a significant loss of capacity in either of them. It will also integrate features that are not at all (certainly not explicitly) available in the current state-of-the-art adsorbents: protection against radioactive gases and against biological threats.

This integration requires an in-depth study of mutual effects of impregnates and impregnation methods, as well as ways to diminish the deleterious effect of water vapour on the adsorption capacity. Moreover, the possibility of commercialisation procedure of the new adsorbents will be investigated.

Description of the work

The primary goal of this project is the development of broad-spectrum low-burden respiratory protection systems for first responders. The first step in this process is developing novel nanoporous sorbents, combined with new or existing types of additives for chemisorption, possibly in combination with catalytic conversion, to neutralise weakly adsorbed components. The new nanoporous adsorbents and additives can be integrated or can be combined in mixtures or separate layers. Specific tasks have been selected in order to meet project objectives:

1. Nanoporous adsorbent development

- Development of nanoporous adsorbent materials with increased protection against toxic industrial chemicals (TIC) such as ammonia and highly volatile organics, chemical warfare agents, radiological and biological threats.
- Development of materials with low burden in weight and breathing resistance.
- Health and safety examination of the sorbents (flammability, ecotoxicity, mechanical resistance, etc.).

2. Evaluation and optimisation of adsorbent performance

Establishment of the relation between the structural characteristics and interfacial properties of the adsorbent's performance. Application of Model predictive control (MPC) to optimise the preparation conditions in order to achieve the required optimum structure and performance.

3. System development

Development of a new gas mask canister and protective hood, both based on the new nanoporous adsorbent.

4. System evaluation and optimisation of the performance

- Determination of the optimum characteristics for the advanced respiratory protection systems.
- Optimisation of the filter and hood systems.

5. Economic feasibility and manufacturability, exploitation and dissemination, IPR policy

Examination of viability of a full scale production of the nanoporous adsorbent, the filter canister and the hood.

Expected results

The final product will have to respond to the following requirements:

- Effective protection against chemical warfare agents.
- Effective protection against a wide range of toxic chemicals, with special attention to ammonia and highly volatile organic compounds.
- Supplementary protection against radioactive gases.
- Supplementary protection against biological hazards (essentially bacteria, viruses and their toxins).
- Low specific weight.
- Low pressure drop over a bed of the adsorbent.
- Limited negative influence of ambient air on immediate performance and ageing effects of the impregnations.

Information

Acronym:
FRESP

Grant Agreement N°:
218138

Total Cost:
€ 4,032,757

EU Contribution:
€ 3,029,967

Starting Date:
01/06/2008

Duration:
42 months

Coordinator:

ROYAL MILITARY ACADEMY
Avenue de la Renaissance 30
BE-1000 Brussels
Belgium

—

Contact:
Dr. Peter Lodewyckx
Royal Military Academy – DEAO
E-mail: Peter.Lodewyckx@rma.ac.be

Website:
www.rma.ac.be/fp7-fresp

Partners

NAME	COUNTRY
Royal Military Academy	Belgium
Budapest University of Technology and Economics	Hungary
University of Brighton	United Kingdom
University of Alicante	Spain
TNO	The Netherlands
High Technology Filters s.a.	Greece
MAST Carbon	United Kingdom
NORIT Nederland B.V	The Netherlands
Laser Optical Engineering Ltd.	United Kingdom

GLOBE / Global border environment

© Fotolia.com

Project objectives

The GLOBE project will provide a comprehensive framework in which an integrated border management system must be developed. The project will take into account the current and future technological environment.

Additionally, GLOBE's scope reaches even further by looking into other key aspects of border management beyond isolated technology, such as the legal and political environment, the social and economic impact of border issues and, more specifically, the impact on information management and integration.

The GLOBE is meant to cover the full scope of an integrated border management system, moving throughout the four main layers of border control, namely, country of origin, transit areas, regulated and unregulated border lines and internal territory.

As a result, GLOBE will identify what already exists, what is being done, what needs to be improved, how to integrate all the information together and how to present it so it proves useful for all relevant EU and national institutions to make better decisions for dealing with issues of such importance as illegal immigration and movements of illegal goods and materials.

Description of the work

The main objective of GLOBE is to provide the best route to achieve a global border environment by identifying the synergies between current and future systems while analysing the potential pitfalls that may hinder this coordination, thereby providing authorities with the best information possible for decision making.

The GLOBE will provide a comprehensive Roadmap that will include the political and legal situation on border security, and the steps to achieve a situation of full coordination between institutions, where political and strategic EU border management decisions have a supranational nature, but can also be translated into operational and tactical actions depending on each border's specific situation and problems.

In order to achieve this goal, the GLOBE concept has been developed from the following foundations:

- Knowledge of the problems from the user's perspective. Addressing border problems from their point of view is key in obtaining useful information for the roadmap.
- Consortium's extensive hands-on experience in border management projects. All the companies in the consortium have vast experience in working with the end users on the day to day challenge of border management.
- Integration as the driving force. The challenge in this project is not how to improve individual technologies, but rather to understand what they provide and create a framework for their interaction.
- Move beyond technology. Threats such as illegal immigration and smuggling of illegal goods and materials must be considered.
- The Broad border framework. Country of origin, transit areas, regulated and unregulated border lines and internal territory.

Expected results

By following this approach, GLOBE will identify the best route to achieve a global border environment by taking advantage of the synergy between current and future systems thereby providing authorities with the best information possible for decision making.

© Fotolia.com

Information

Acronym :
GLOBE

Grant Agreement N° :
218207

Total Cost :
€ 999,891

EU Contribution:
€ 999,891

Starting Date :
01/07/2008

Duration:
12 months

Coordinator :

TELVENT INTERACTIVA S.A.
Mr. Manuel Parra
Av. Valgrande, 6
ES-28108 Alcobendas
Spain

—

Contact :
Víctor Alejandro Luaces Bustabad
E-mail : victor.luaces@telvent.com

Website :
http://globe.ti-projects.com

Partners

NAME	COUNTRY
Telvent Interactiva S.A.	Spain
Amper Sistemas S.A.	Spain
GMV Aerospace and Defence, S.A	Spain
Fundación Robotiker	Spain
Instituto Nacional de Técnica Aeroespacial	Spain
Altran Technologies	France
SETTCE	Slovenia
Econet Polska sp. z.o.o.	Poland
Eurosense Belfotop N.V.	Belgium
Skysoft Portugal, Software e Tecnologias de informaçao, S.A.	Portugal
CES vision Ltd.	Hungary
PRIO	Norway
Empresa de Serviços e Desenvolvimento de Software, S.A.	Portugal
Cogent Systems GMBH	Austria

iDetecT 4ALL / Novel intruder detection and authentication optical sensing technology

© Antonis Papantoniou - Fotolia.com

Project objectives

The limited sensing capabilities as well as the very high costs of existing security equipment imposes a barrier to implement necessary security means for all critical infrastructures, especially those having budget constraints. The iDetecT goal is to develop innovative optical intruder sensing and authentication technologies that will significantly improve security systems performance, available at an affordable cost, leading to the widespread availability of affordable security, allowing more protection for infrastructures. The iDetecT project will develop a novel photonic sensing technology based on an innovative approach using ultra low cost electro-optical components. This technology allows both detection and authentication of objects by a single sensor, which dramatically improves the performance and reliability of the security system.

This innovative approach is enabled by recently invented very advanced digital signal processing (DSP) techniques that enable distance measurement using continuous modulated light signals (invisible to humans) and requires far less optical power than existing laser scanning technologies. The result will be increased performance with reduced cost for reliable intruder detection.

Description of the work

This technology will detect the presence of objects (human beings, vehicles, goods), inside or in the surrounding area of restricted critical infrastructures. It will identify authorized objects and will alert if an unauthorized object is found within the protected zone. For this purpose, the following Research and Technological Development (RTD) activities will be undertaken:

- The development of ultra sensitive optical sensing and detection technology, using the same photonic methodology. This sensing technology will enable a highly robust indoor and outdoor remote intruder detection technique and remote scanning of optical tags. The sensor and tag will also use the common technology basis for optical communication between the tag and the sensor for authentication data exchange.
- The research and development of optical tagging technology, that will be based on the above mentioned photonic methodology. These tags will be attached to objects for their remote identification and authentication.
- The development of other technological components necessary to complement the sensing and tagging technologies including: alert tracking, networking and communication.

The work plan includes field trials using a prototype system combining the technology components that will be developed. The field trial will be carried out to verify and validate the usefulness and effectiveness of the technologies under real world conditions.

The Field trial prototype system will present an "end to end" security application, integrating the following components:

- An array of multiple ID2 sensors, capable of detecting intruder objects and reading the optical ID (OPID) tags within the field of view,
- Multiple ID tags for identification, that will be attached to authorized objects;
- Server hosting situational awareness algorithms and software capable of alerting predefined threats and tracking them;
- An electro-optical alert tracking observation module that will be directed to any unauthorised object detected, and will be used to track and observe the object being identified as a potential threat;
- Threat alerts display at a command and control room for the security operator;
- Low cost communication and networking units, for the interconnections of the prototype components.

Expected results

- The solution will have the following capabilities:
- Remote detection of static and moving objects within a predetermined field of view.
- Remote scanning and authentication of optical ID tags (OPID).
- Threat identification, tracking and observation.
- 24 hour operational capability in all lighting and weather conditions.
- Inherent immunity to natural phenomena causing false alarms.
- Minimal power consumption and therefore compatible and easily installable in existing security installations using existing infrastructure.
- Maintenance free design.

Information

Acronym :
iDetecT 4ALL

Grant Agreement N° :
217872

Total Cost :
€ 3,236,675

EU Contribution :
€ 2,298,014

Starting Date :
01/07/2008

Duration :
30 months

Coordinator :

INSTRO PRECISION LTD.
15 Hornet Close
Pysons Rd Industrial Estate
Broadstairs, Kent, CT10 2YD
United Kingdom

—

Contact :
William Caplan, MSE
Electro-optic Project Manager
Instro Precision Limited.
Tel : +44 (0) 1843 60 44 55 ext. 110
E-mail: williamcaplan@instro.com

Website :
www.idetect4all.com

Partners

NAME	COUNTRY
Instro Precision Ltd.	United Kingdom
ARTTIC	Belgium
Motorola Israel Ltd.	Israel
EVERIS Consulting	Spain
Cargo Airlines	Israel
3D s.a.	Greece
ANA Aeroportos de Portugal	Portugal
LACHS	Belgium
Azimuth Tecnologies Ltd.	Israel
S.C. PRO OPTICA S.A.	Romania

IMCOSEC / Integrated approach to improve the supply chain for container transport and integrated security simultaneously

© Soleg - Fotolia.com

Project objectives

There are two contradicting trends in global transport (which are valid also for the segment of containers and other ILUs) that have to be aligned in the most efficient way – assuring free trade and assuring transport security. On the one hand huge efforts have been made to eliminate trade barriers in order to ensure free trade and cargo flow within regions (such as the European Single Market or free trade area agreements) and globally. On the other hand additional security requirements such as checking the integrity of containers, their contents or third parties as well as advance data reports have the opposite effect.

The main objective of the project IMCOSEC is to create a win-win solution between industry and supervision whereby the level of security is at an optimum level balancing effectiveness with practicality within the regulatory framework. Thus IMCOSEC will not aim at introducing as much security as possible, rather than as much as needed, suitable and acceptable.

Description of the work

IMCOSEC will be guided by the following approach:

- Identification of security gaps based on the current processes, e.g. using the resilience matrix approach.
- Elaboration of target processes for closing these gaps and ensuring product integrity is supported by technologies either already deployable or under development.
- Identification of existing technologies to support and improve the container transport chain and integrate security.
- Consideration of ongoing projects and their intended results as well as parallel actions.
- Identification of additional requirements for R&D actions where these gaps cannot be closed by existing measures or research.
- Provision of a roadmap for demonstration activities where target processes and supporting technologies can establish efficiency, effectiveness and acceptance.
- Development of a guideline to improve existing or develop new technologies in order to meet the requirement given by the developed research roadmap.

Acceptance by the industry is one of the most important issues regarding the sustainability of the roadmap to be developed. Therefore, all the above issues will be discussed and validated by workshops with stakeholders and the projects Advisory Board involving additional stakeholders from private end-users and public end-users. Together with the international workshops these groups will ensure European wide awareness and that the target processes and technologies will be acceptable to the global business. The three public workshops will be held in Ostende, Berlin and Brussels.

Expected results

The major result of IMCOSEC is to determine a basic concept and roadmap for a large scale demonstration where intermodal chains will be demonstrated as "secure" corridors with effective processes and state of the art information, security and component technologies.

Information

Acronym :
IMCOSEC

Grant Agreement N° :
242295

Total Cost :
€ 1,142,591

EU Contribution :
€ 930,718

Starting Date :
01/04/2010

Duration :
12 months

Coordinator :

TSB INNOVATIONSAGENTUR BERLIN GMBH / BEREICH FAV
Fasanenstr. 85, 10623 Berlin
Germany

—

Contact :
Markus Podbregar
Tel : +30 46302 579
Office: +30 46302 563
Fax: +30 46302-588
E-mail: mpodbregar@fav.de

Website :
www.imcosec.eu

Partners

NAME	COUNTRY
TSB Innovationsagentur Berlin GmbH (FAV)	Germany
International Container Security Organisation (ICSO)	Belgium
Union Internationale des sociétés de transport combine Rail-Route (UIRR)	Belgium
Bureau International des Containers (BIC)	France
CBRNE Ltd.	United Kingdom
Studiengesellschaft für den Kombinierten Verkehr e. V. (SGKV)	Germany
Politecnico di Milano (POLIMI)	Italy
Technische Universität Hamburg-Harburg (TUHH)	Germany
Institut für Seeverkehrswirtschaft und Logistik (ISL)	Germany

IMSK / Integrated mobile security kit

© Fotolia.com

Project objectives

The Integrated Mobile Security Kit (IMSK) project aims at increasing the security of citizens in the scope of events gathering a large number of people, such as medium to large scale sports events (from football games to the Olympic Games), political summits (G8 summit) etc. The security related to these types of events with intense mass media coverage has indeed become an increasing concern due to new threats of terrorism and criminal activities (such as suicide bombers, improvised explosive devices, increasingly credible CBRN threats).

To counter this situation, new systems are needed that can cover various security aspects and allow for cooperation between different stakeholders. The systems need to be mobile and adaptable in order to address situations of different kinds and different locations. The main objective of the proposed project is the study, development, assessment and promotion of such a system, the IMSK, providing emerging solutions for increased probability of rapid detection and response to threats.

Description of the work

The Integrated Mobile Security Kit (IMSK) project will combine technologies for area surveillance, checkpoint control, also CBRNE detection and support for VIP protection into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc) which temporarily need enhanced security. The IMSK accepts input from a wide range of sensor modules, either legacy systems or new devices brought in for a specific occasion. Sensor data will be integrated through a (secure) communication module and a data management module and output to a command & control centre.

IMSK will have an advanced man-machine interface using intuitive symbols and a simulation platform for training. End-users will define the overall system requirements, ensuring compatibility with pre-existing security systems and procedures. IMSK will be compatible with new sensors for threat detection and validation, including cameras (visual & infra-red), radar, acoustic and vibration, x-ray and gamma radiation and CBRNE.

Tracking of goods, vehicles and individuals will enhance situational awareness and personal integrity will be maintained by the use of, for example non-intrusive terahertz sensors. To ensure the use of appropriate technologies, police and counter-terrorist operatives from several EU nations have been involved in defining the project in relevant areas.

Close cooperation with end-users will ensure compatibility with national requirements and appropriate interfaces with existing procedures. The effectiveness of IMSK will be verified through field trials. Through IMSK, security of the citizen will be enhanced even in asymmetric situations.

Expected results

The project will employ legacy and novel sensor technologies, design a demonstrable system (IMSK) that will integrate sensor information to provide a common operational picture where information is fused into intelligence. A Privacy Impact Assessment will be performed to ensure that both system design and utilisation guidelines take fully account of privacy and related civil liberty issues. A field trial will be performed to validate the concept and demonstrate the functions of the system and the result of the research performed.

© hasan bensliman - Fotolia.com

Information

Acronym :
IMSK

Grant Agreement N° :
218038

Total Cost :
€ 23,468,530

EU Contribution:
€ 14,864,308

Starting Date :
01/03/2009

Duration:
48 months

Coordinator :

SAAB AB
Saab Microwave Systems
SE-412 89 Göteborg, Sweden

—

Contact :
Daniel Forsberg
Tel : +46 31 794 9123
Fax : +46 31 794 9475
E-mail : daniel.forsberg@saabgroup.com

Partners

NAME	COUNTRY
Saab AB	Sweden
Selex Sensors and Airborne Systems Limited	United Kingdom
Selex Communications S.p.A.	Italy
Telespazio S.p.A.	Italy
Cilas	France
Diehl BGT Defence GmbH & CO KG	Germany
Thales Security Systems SA	France
Bruker Daltonik GmbH	Germany
Totalförsvarets Forskningsinstitut, (FOI)	Sweden
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Commissariat à l'Energie Atomique (CEA)	France
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
Fraunhofer	Germany
Ministère de l'intérieur- STSI	France
Universita Degli Studi Di Catania	Italy
Thyia Tehnologije d.o.o.	Slovenia
AS Regio	Estonia
EPPRA S.A.S	France
Qascom S.r.l	Italy
Rikskriminalpolisen - Swedish National Police Board	Sweden
Regione Lombardia	Italy
Thales Research and Technology Ltd	United Kingdom
TriVision ApS	Denmark
JRC	Italy
Deutscher Fußball-Bund e.V.	Germany
AirshipVision International S.A	France
University of Reading	United Kingdom

INDECT/ Intelligent information system supporting observation, searching and detection for security of citizens in urban environment

© Andy Dean- Fotolia.com

Project objectives

The main objectives of the INDECT project are:

» to develop a platform for the registration and exchange of operational data, acquisition of multimedia content, intelligent processing of all information and automatic detection of threats and recognition of unusual behaviour or violence,

» to develop the prototype of an integrated, network-centric system supporting the operational activities of police officers, providing techniques and tools for observation of various mobile objects,

» to develop a new type of search engine combining direct search of images and video based on watermarked contents and the storage of metadata in the form of digital watermarks, and

» to develop a set of techniques supporting surveillance of internet resources, analysis of the acquired information and detection of criminal activities and threats.

Description of the work

While **taking fully into account privacy issues,** the INDECT project's main aim is the elaboration of a concept, method and technology for intelligent monitoring of objects and urban areas for the purpose of automatic detection of threats related to crime, terrorism and violence acts. The INDECT system will contain many novel solutions based on multimedia technologies and intelligent monitoring of objects and areas. The INDECT concept of the multimedia platform assumes the elaboration of a distributed system whose principal element is an autonomous node station designed for the purposes defined in the project. The automatic data acquisition station will be used to acquire data, signals and images from the surveyed area, then to pre-process the data intelligently and transmit the gathered information to the remote servers. The distributed data processing system, provided with huge computational power and a vast repository of knowledge connected also to a spatial information system, will be programmed in a way that will allow the automatic detection of behaviours that could pose a potential threat to security and safety.

The integral part of the INDECT proposed research consists of the integration of security systems with emergent wireless communication systems and self-organizing computer networks in order to achieve their interoperability for extraction, processing, distribution and supporting of security information on citizens of urban environments. INDECT plans to carry out the research in several parallel directions:

» monitoring of various people clusters and detection of unusual behaviour and situations of danger,

» development and evaluation of complex multimodal biometric procedures and systems for people authentication/verification (e.g. in schools, hospitals, offices, etc.) and for people recognition/identification (e.g. in order to determine guilty persons in chosen situations of danger),

» intelligence gathering from the web and monitoring of suspicious activities in the Internet,

» development of automatic people-notification services using emergent wireless communication systems and self-organizing computer networks, and

» development of watermarking technology and new type of search engine.

Expected results

The main expected results of the INDECT project are:

» to realise a trial installation of the monitoring and surveillance system in various points of city agglomeration,

» implementation of a distributed computer system that is capable of acquisition, storage and effective sharing,

» construction of a semantic search engine for fast detection of persons and documents based on watermarking,

» construction of a network of agents assigned to continuous and automatic monitoring of public resources, and

» elaboration of internet based intelligence gathering system, both active and passive.

Information

Acronym :
INDECT

Grant Agreement N° :
218086

Total Cost :
€ 14,863,988

EU Contribution :
€ 10,906,984

Starting Date :
01/01/2009

Duration :
60 months

Coordinator :

AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICAW KRAKOWIE
Department of Telecommunications/Faculty of Electrical Engineering, Automatics, Computer Science and Electronics
al. Mickiewicza 30
Poland – PL-30059 – Krakow

—

Contact :
Prof. Andrzej Dziech
Tel : +48-12-6172616
Mobile: +48-607720845
Fax : +48-12-6342372
E-mail : dziech@kt.agh.edu.pl

Website :
www.indect-project.eu/

Partners

NAME	COUNTRY
AGH – University of Science and Technology	Poland
Apertus	Hungary
Gdansk University of Technology	Poland
InnoTec DATA GmbH & Co. KG	Germany
IP Grenoble (Ensimag)	France
MSWiA – General Headquarters of Police (Polish Police)	Poland
Moviquity	Spain
Products and Systems of Information Technology	Germany
Police Service of Northern Ireland	United Kingdom
Poznan University of Technology	Poland
Universidad Carlos III de Madrid	Spain
Technical University of Sofia	Bulgaria
University of Wuppertal	Germany
University of York	United Kingdom
Technical University of Ostrava	Czech Republic
Technical University of Kosice	Slovakia
X-Art Pro Division G.m.b.H.	Austria
Fachhochschule Technikum Wien	Austria

INDIGO/ Crisis management solutions

© Galina Pankratova- Fotolia.com

Project objectives

The INDIGO project aims to research, develop and validate an innovative system integrating the latest advances in Virtual Reality and Simulation in order to enhance both the effectiveness of operational preparedness and the management of an actual crisis or disaster.

The proposed system will prove an essential and integrated tool for training personnel, planning operations, and facilitating crisis management and co-operation across organisations and nations. It will enable users to:

- display and manipulate an operational visual representation of the situation that is as complete and as easy to understand as possible, for indoor and outdoor situations;
- simulate different evolving scenarios for planning, training, and anticipating future states and impending developments during operations, and analyse events after the crisis;
- involve first responders and emergency field units in simulated exercises;
- enhance the work across organisational boundaries and decision levels.

Description of the work

The INDIGO consortium provides the world-class and complementary competencies required to tackle the following scientific and technological challenges:

- The 3D interactive and realistic visualisation of the complete crisis environment, including data coming from the field, simulation results, and building interiors.
- The intuitive authoring and simulation of different evolving scenarios for planning, training, and anticipating future states and impending developments during operations, and analyse events after the crisis.
- The involvement of multiple participants (field units as well decision makers and commanders), thanks to its distributed architecture, while offering a unique pictorial way of sharing and communicating complex knowledge across organisation boundaries.
- The preparation of a standard proposition for a European 2D/3D emergency symbology (symbols, indicators, colours) on 2D and 3D maps.

Expected results

The main results of the project will be tightly integrated into the INDIGO system and include:

1. The INDIGO distributed framework enabling:
   - The involvement of multiple users in crisis exercises;
   - The intuitive authoring and control of crisis scenarios;
   - The visualization of a 2D/3D interactive Common Operational Picture;
   - The visual command and control of field units;
   - The development of additional modules with the INDIGO SDK.
2. The mobile INDIGO system that enables first responders and other field units to participate in INDIGO crisis exercises.
3. The Environment Service that hosts and delivers, in interactive time, all the information related to the situation, including massive geographic, cartographic and architectural data about the environment.
4. The Real-time Simulation Services that can stimulate the scenario or be used to support decision during real crisis.
5. The portable map table that will offer an extremely innovative and intuitive mean to interact with the Common Operational Picture in mobile crisis centers.
6. The standard proposition for a European 2D/3D emergency symbology.

Information

Acronym:
INDIGO

Grant Agreement N°:
242341

Total Cost:
€ 3,830,000

EU Contribution:
€ 2,790,000

Starting date:
01/05/2010

Duration:
36 months

Coordinator:

DIGINEXT SARL
Impasse de la Draille
Parc d'Activités La Duranne
13100 Aix en Provence, France

—

Contact:
Jerome Duchon
Tel : +33 (0)5 61 17 66 66
Fax : +33 (0)5 61 17 65 78
E-mail : Duchon@diginext.no-spam.fr

Website:
http://indigo.c-s.fr

Partners

NAME	COUNTRY
Diginext	France
Consiglio Nazionale delle Ricerche	Italy
Centre for Advanced Studies, Research and Development in Sardinia	Italy
Immersion SAS	France
European Committee for Standardization	Belgium
Crisisplan	The Netherlands
Swedish National Defence College	Sweden
Entente pour la forêt méditerranéenne	France

INEX / Converging and conflicting ethical values in the internal/external security continuum in Europe

© quayside- Fotolia.com

Project objectives

The interdisciplinary project INEX is designed to contribute to existing understandings of European security through an innovative analysis of the value based premises and ethical consequences of the internal/external security continuum.

This security continuum results from the blurring of the demarcation between external and internal security questions, as external security authorities seek to locate threats in the internal security sphere and traditional internal authorities pursue security threats externally.

While this continuum is studied in ongoing research, it contains essential value assumptions and ethical consequences that remain largely under-theorised, with significant consequences for both European policy and law-making.

The aim of the project is to fill this lacuna by supplementing current research with an ethical and value-oriented analysis.

INEX advances and tests the hypothesis that:

- Practices that make up the internal/external security continuum are driven by an implicit logic of ethical values,
- these values contribute significantly to structuring the continuum of security practices, and
- they consequently have significant implications for how present and future security policy should be formulated and implemented.

Description of the work

The scientific research proposed by INEX is structured in two main phases.

Phase I will seek to document, clarify and analyze the ethical value assumptions implicit in four main dimensions of internal/external security practice:

- the proliferation of security technologies for surveillance and border control,
- the transnational legal dilemmas of European security practice,
- the proliferation and shifting roles of security professionals, and
- the ethical implications of CFSP/EDSP implementation and its linkages to internal security challenges.

This phase of the research provides the initial conceptualisation of these themes, developed from the empirical examination of security practices in Europe.

Phase II will articulate and evaluate the above ethical themes relative to the provisional results and future ambitions of the European Neighbourhood Policy (ENP) by examining in detail six representative countries covered by the ENP (Belarus, Ukraine, Moldova, Morocco, Algeria and Egypt). The ENP is today the most comprehensive institutional response to the deepening internal/external security continuum described above. It politically links the non-military dimensions of the new security concept – immigration, narcotics and human trafficking, pandemic, energy, resources, terrorism, etc. – to the geopolitical challenges of the CFSP.

The ENP will serve as the lens through which the geopolitical adaptability of the internal/external security continuum, and the security practices described by the four themes above, is tested on a comparative geographical basis.

This work will serve both as a set of transversal test cases evaluating the validity of the principles produced by PHASE I and will contribute to correcting and expanding the relationship between ethical values and security.

Expected results

The state-of-the-art research carried out by the project will result in a variety of different outputs aimed primarily at relevant policymakers, researchers and educators. It will present analyses of current security challenges with particular attention given to the human side of the issues. On this basis it will make informed policy recommendations for improving security practices and meeting the new challenges of the internal/external security continuum.

Information

Acronym :
INEX

Grant Agreement N° :
218265

Total Cost :
€ 2,422,082

EU Contribution :
€ 1,890,248

Starting Date :
01/08/2008

Duration :
36 months

Coordinator :

INSTITUTT FOR FREDSFORSKNING /
International Peace Research Institute
Hausmannsgate 7
NO-0186 Oslo
Norway

—

Contact :
J. Peter Burgess
Tel : +47 22 54 77 00
Fax : +47 22 54 77 01
E-mail : peter@prio.no

Website :
http://www.inexproject.eu

Partners

NAME	COUNTRY
International Peace Research Institute, Oslo	Norway
Ericsson Security Systems	Norway
Centre d'études sur les conflits	France
Vrije Universiteit Brussel	Belgium
Vrije Universiteit Amsterdam	The Netherlands
Centre for Security Studies, Collegium Civitas	Poland
Centro de Investigación de Relaciones Internacionales y Desarrollo	Spain
Bilkent University	Turkey
Centre for European Policy Studies	Belgium

INFRA / Innovative & novel first responders applications

© Duncan Noakes- Fotolia.com

Project objectives

The fundamental objective of the INFRA project is to research and develop novel technologies for personal digital support systems, as part of an integral and secure emergency management system to support First Responders in crises occurring in Critical Infrastructures under all circumstances.

The specific objectives of the project fall under the following categories:

- Communications objectives, which involve the research and development of an integral and interoperable wireless communications system that will allow First Responders to have reliable means of communications as they enter subway tunnels and buildings with thick concrete walls.
- First Responders objectives, which entail the R&D of a robust indoor-site navigation system based on three location sensors (an inertial sensor, a wireless sensor and a video sensor), a video annotation system for First Responder PDAs, sensors for real time identification of radiation exposure and hazardous materials and applications for gas leakage and hidden fire detection.
- Standardization objectives, which includes R&D of a European level proposal for the standardization of the framework of communications and applications as proposed by INFRA.
- Demonstration objectives, which consist on the demonstration of the validity of INFRA's standards, communications and First Responder applications being developed.

Description of the work

The work to be developed is comprised of the following areas:

The Critical Infrastructure Broadband Communications Base area will cover advanced wireless broadband network technology that is specially adapted to the needs of First Responder teams in Critical Infrastructure sites. The network shall support video, data and voice communications and it will consist of multi-radio mesh topology with self- adaptive and self-healing functionality.
The Critical Infrastructure Open Interoperability Standard area will cover the development of a highly dynamic system of systems made up of elements that interact with each other in unplanned and spontaneous ways. It will also cover the development of a First Responder oriented network-programming platform that will implement the systems-of-systems nature of First Responder applications and communications.
In addition, the abstraction level provided by this communication layer will be able to support future applications that will conform to the INFRA specifications, aiming to lay the foundation for a European First Responder interoperability standard.
The Communications Space will provide an unprecedented level of interoperability for voice and data communications. All First Responder teams, First Responder command posts and the Critical Infrastructure control centre, regardless of their radio technology, will be able to communicate with each other. Furthermore, First Responders will be able to use their legacy equipment inside buildings with thick concrete walls and in underground tunnels, where typically radio RF propagation is impaired. The Application Space will provide novel technologies and applications for the use of First Responders in Critical Infrastructure sites. These shall be Site Indoor Navigation (based on inputs from three independent tracking sources for increased reliability and accuracy), Thermal imaging (including gas-leaks detection and hidden-fire detection), Advanced Sensors (robust and lightweight fibre optic based sensors for the detection of hazardous materials) and Video Annotation (annotated with symbols and graphical components through dedicated authoring tools and short textual descriptions that aim at focusing the attention of the First Responder on a specific part of the picture).

Expected results

To create an open, standards based interoperability layer that will allow:
- Broadband access for high bandwidth applications.
- Autonomous wireless broadband in underground tunnels and concrete buildings.
- Full voice and data communication interoperability between all First Responder teams.
- Full interoperability of First Responder applications.

To provide practical and useful novel applications for First Responder teams, including:
- Thermal imaging applications.
- Video annotation.
- Advanced fibre-optic sensors.
- Indoor navigation system.

Information

Acronym:
INFRA

Grant Agreement N°:
225272

Total Cost:
€ 3,820,811

EU Contribution:
€ 2,642,895

Starting Date:
01/04/2009

Duration:
24 months

Coordinator:

Athena GS3 Security Implementations Ltd.
5 Hatzoref St.
Holon 58856
Israel
www.athenaiss.com

—

Contact:
Omer Laviv
Tel: +972-3 5572462
Fax: +972-3 5572472
Mobile: +972-52-8665807
olaviv@athenaiss.com

Website:
www.infra-fp7.eu

Partners

NAME	COUNTRY
Athena GS3 Security Implementations Ltd.	Israel
Halevi Dweck & Co. ARTTIC Israel Company Ltd.	Israel
University of Limerick	Ireland
ISDEFE Ingeniería de Sistemas S.A.	Spain
Democritus University of Thrace	Greece
Rinicom	United Kingdom
Everis Spain S.L.	Spain
Hopling Networks B.V.	The Netherlands
Opgal Optronic Industries Ltd.	Israel
Research and Education Laboratory in Information Technologies	Greece

ISTIMES / Integrated system for transport infrastructure surveillance and monitoring by electromagnetic sensing

© TOM ANG - Fotolia.com

Project objectives

The transportation sector's components are susceptible to the consequences of natural disasters and are attractive as terrorist targets. This is also due to the very high social and economic importance of this sector for the European countries. On the other hand, the terrorist events of the last years have pointed out that achieving clear and concise situational awareness is a key factor in the crisis management. This entails an accurate monitoring as well as the possibility to achieve and quasi real-time information on the scenario of crisis.

In this framework, the ISTIMES project aims at designing, assessing and promoting an ICT-based system, exploiting distributed and local sensors, for non-destructive electromagnetic monitoring of the critical transport infrastructures. The outcomes of the monitoring system is in terms of detailed real time information and images of the infrastructure status so as to provide support to the decision for emergency and disasters stakeholders.

Description of the work

The ISTIMES project aims at designing a prototype electromagnetic sensing monitoring and surveillance system to improve safety and security of the transportation infrastructures. The system will use and integrate heterogeneous, state-of-the-art electromagnetic sensors, enabling a self-organizing, self-healing, ad-hoc networking of terrestrial in situ sensors, supported by specific airborne and satellite measurements. The effectiveness of the system will be tested at two challenging test beds in Switzerland and Italy.

The project activities of ISTIMES have been broken down in seven work packages:

» *ACTIVITY 1* will regard the definition of user requirements of the system for the electromagnetic diagnosis and monitoring of strategic infrastructures. This is a key activity for the acceptance of the usefulness of the system from the end user's point of view.

» *ACTIVITY 2* will deal with the development of the ISTIMES e-infrastructure organized in three sub-infrastructures: infrastructure for real time and interactive access to the information by end-user; infrastructure for enabling remote use of and control of instrumentation and processing of measurements; wireless network services for sensors communication.

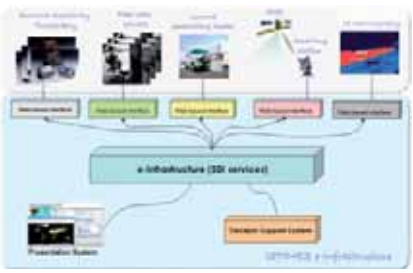
» *ACTIVITY 3* will deal with the exploitation, improvement, and integration of processing approaches and measurement strategies for non invasive monitoring of the structure at different temporal and spatial scales. Several electromagnetic sensing techniques will be exploited and their performance analysis will be performed in controlled conditions at state-of art and innovative test sites.

» *ACTIVITY 4* will deal with the implementation of the system and demonstration activities at two test beds such as a highway-bridge in Switzerland and railway and highway infrastructures in Italy.

» *ACTIVITY 5* will deal with the dissemination, technological transfer and use-exploitation of the project results.

Expected results

» A prototype of electromagnetic sensing (ES) monitoring and surveillance system based on an ad-hoc networking of in situ sensors and airborne/satellite data.
» 4D tomographic infrastructure monitoring thanks to the exploitation and integration of the ES techniques.
» Validation of ES techniques through experiments at two test sites.
» Demonstration of the effectiveness of the system at two challenging test beds.
» Dissemination of ISTIMES approach and outcomes to public institutions and private companies.



Information

Acronym:
ISTIMES

Grant Agreement N°:
225663

Total Cost:
€ 4,342,283

EU Contribution:
€ 3,113,460

Starting Date:
01/06/2009

Duration:
36 months

Coordinator:

TECHNOLOGIES FOR EARTH OBSERVATIONS AND NATURAL HAZARDS CONSORTIUM (TERN)
c/o CNR-IMAA
C.da S. Loja, Zona Industriale
85050 Tito (PZ)
Italy

—

Contact:
Prof. Vincenzo Cuomo
Phone: +39 0971 427229/208
Fax: +39 0971 427271
E-mail: tern@imaa.cnr.it

Website:
www.istimes.eu

Partners

NAME	COUNTRY
Technologies for Earth Observations and Natural Hazards (TeRN)	Italy
Elsag Datamat (ED)	Italy
Dipartimento di Protezione Civile (DPC)	Italy
Eidgenoessische Materialpruefungs- und Forschungsanstalt (EMPA)	Switzerland
Laboratoire Central des Ponts et Chaussées (LCPC)	France
Lund University (ULUND)	Sweden
Tel Aviv University (TAU)	Israel
Territorial Data Elaboration SRL (TDE)	Romania
Norsk Elektro Optikk (NEO)	Norway

L4S / Learning for security project

© fotografiche.eu - Fotolia.com

Project objectives

The aim of the L4S project is to provide a clear understanding, in both interdisciplinary scientific/academic models and best/worst practices and experiences in the field of transportation, of the factors inhibiting effective collaboration dynamics in crises and leading to the failure of effective crisis management and of the interventions required to reduce these risks.

This know-how is integrated into an innovative framework for addressing the development of collaboration competencies of crisis managers in the transportation sector. The L4S Framework is validated through the implementation of state-of-the-art highly interactive and experiential learning solutions that enable the effective understanding and management of the challenges in crisis situations, as validated with the participation of practitioners in the field.

These challenges include :

- acting under extreme time pressure,
- facing the lack, ambiguity, and/or asymmetries of information,
- dealing with human factors like cognitions, attitudes and emotions, and
- addressing the interpersonal relationship dimension like fast relationship building and activation for the mobilization of social resources, trust building, cohesion and role definitions and also handling diversity and conflicts.

Description of the work

The implementation scheme of the L4S is developed across three main pathways:

- collaboration challenges and related competencies & dynamics for crisis managers,
- knowledge processes and community building, and
- advanced technological tools for simulation games.

The pathways document the full network of options and the choices actually explored within the project as well as separate trends of development that may occur as a result of the different trial environments. All three pathways include at regular intervals analytical reports from the meetings and the workshops, observations and reports from the field trips, technical, pedagogical and evaluation reports following the development of the artefacts and their components. These reports also compare with the state of the art in their respective areas. The interconnection amongst the three pathways will be facilitated through the extended pilots that further strengthen the involvement of domain expertise.

All pathways evolve in the framework of an embedded and continuous evaluation study. The main aims of this study are continuous assessment of the knowledge output and technologies developed and documentation of the evaluation methodology and results in order to:

- develop the guidelines required for the development of the L4S simulation learning tools,
- provide guidelines and useful input from the users for improving the usability of the final prototypes and
- investigate the impact that simulation learning technology has on how end users experience L4S e-learning applications.

The pathways are connected with cross-links of interactions between technological (hardware and software developers) simulation learning experts, tutors, cognitive science experts and end-users. Final packaging and the exploitation prospects of the project are also taken into consideration..

Expected results

In terms of outputs, the project deliver's significant contributions:

1. A comprehensive online knowledge community integrating a knowledge base and an active virtual learning community on advanced collaboration dynamics and technologies of L4S
2. An experience-based learning framework to address the effective development of collaboration competencies for crisis managers.
3. Four simulation games: validated experienced based learning solutions deployable in educational and organizational contexts,
4. L4S deployment package: effective instruments and tools for the generation of simulation based learning experiences.

Information

Acronym:
L4S

Grant Agreement N°:
225634

Total Cost:
€ 3,503,621

EU Contribution:
€ 2,415,768

Starting Date:
01/07/2009

Duration:
24 months

Coordinator:

DELOITTE BUSINESS SOLUTIONS
c/o CNR-IMAA
C.da S. Loja, Zona Industriale
85050 Tito (PZ)
Italy

—

Contact:
Christos Konstantinou
E-mail: ckonstantinou@deloitte.gr

Website:
www.L4S-project.info

Partners

NAME	COUNTRY
Deloitte Business Solutions Anonymi Etairia Symvoulon Epicheiriseon	Greece
Oesterreichische Studiengesellschaft Fuer Kybernetik	Austria
Alphalabs SARL	France
Universitaet Der Bundeswehr Muenchen	Germany
Athens Laboratory of Business Administration	Greece
Universita Cattolica Del Sacro Cuore	Italy
FVA SAS	Italy
Athens International airport S.A.	Greece
Creurers del port de Barcelona SA	Spain
Frequentis AG	Austria
Akad Wissenschaftliche Hochschule Lahr GMBH	Germany

LOGSEC / Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security

© Fotolia.com

Project objectives

The LOGSEC project has the following three main objectives:

1. To deliver a strategic roadmap for supply chain security in Europe; roadmap depicting possible security gaps and responsibility backlogs between different operators, both business and governmental.

2. To address relevant political, policy, regulatory, technology and service aspects, together with their combinations and to define the ones most critical in security research.

3. To combine global supply chain management expertise and technological expertise with crime prevention expertise to improve real security in end-to-end supply chains, in a cost-efficient manner.

Description of the work

The LOGSEC project team consists of organisations with in-depth experience in European and global supply chain security research and technology analysis and partners representing a broad set of European shippers and logistics operators and customs administrations.

Key technologies and procedural aspects covered by the project include: container and goods/inventory, authentication, traceability, inspection and monitoring technologies; risk assessment systems and models; Information transfer systems; Intermodal transport security; modernisation of customs procedures; protection of supply chain infrastructure.

User requirements and data collection steps include:

» literature and project reviews,

» end-user expert interviews,

» user surveys, and

» user workshops.

Expected results

The LOGSEC project will deliver a strategic roadmap for a large scale demonstration project in European logistics and supply chain security, characterised by adequate security for the benefit of business and governments, on low time-delay and other cost implications.

LOGSEC will identify the most relevant/promising research areas and research gaps, which should be addressed in the follow-up demonstration project.

An instrumental part of the roadmap project is to build a solid basis for future metrics necessary to evaluate supply chain and security performance and to monitor supply chain vulnerabilities.

Information

Acronym :
LOGSEC

Grant Agreement N° :
241676

Total Cost :
€ 800,047

EU Contribution :
€ 753,373

Starting Date :
01/04/2010

Duration :
12 months

Coordinator :

EFP CONSULTING (UK) LTD.

—

Contact :
Dana Remes
Phone: +44 141 649 3244
E-mail: dana@efpconsulting.com

Website :
www.logsec.org

Partners

NAME	COUNTRY
EFP Consulting (UK) Ltd	United Kingdom
Cross-border Research Association	Switzerland
Innovative Compliance Europe Ltd	United Kingdom
European Shippers Council	Belgium
European Association for Forwarding, Transport, Logistics and Customs Services	Belgium
ATOS Origin	Spain
Warsaw School of Economics	Poland
Swiss Federal Customs Administration	Switzerland

LOTUS / Localization of threat substances in urban society

© paolo toscani - Fotolia.com

Project objectives

The overall objective of the LOTUS project is to develop a new anti-terrorism tool for law enforcement agencies in the form of an integrated surveillance system for continuous chemical background monitoring with fixed site and/or mobile detectors in order to identify "chemical hotspots", such as bomb or drug factories.

The LOTUS project aims to create a system by which illicit production of explosives and drugs can be detected during the production stage rather than preventing terrorist attacks while they are already in motion, which is extremely difficult.

The LOTUS concept is aimed at detecting chemical signatures over a wide urban area. The detectors may be placed at fixed positions although most detectors should be mobile. These distributed detectors continuously sample air while its carrier performs its daily work. When a suspicious substance is detected in elevated amounts, information about the type, location, amount and time is registered and sent to a data collection and evaluation centre for analysis. Several indications in the same area will trigger an alert, enabling law enforcement agencies to further investigate and respond.

Description of the work

The goal of LOTUS is to use an innovative approach to monitor illicit production of explosives and drugs, thus stopping terrorist attacks at an early stage and preventing produced drugs to get as far as the street.

A number of key components necessary to achieve the goal have been identified: knowledge of the threat and dispersion of threat substances, sensors for their detection, system communication, information management, testing & verification and a field demonstration.

Continuous communication with end users is planned as well as a field demonstration at the end of the project.

The project aims at demonstrating system capability by the modification of existing sensors and sensors in development in order to detect selected precursors and integrating the sensors in a network system using existing technology. By using existing global infrastructures for positioning (GPS) and networking (GSM, GPRS or 3G) the LOTUS system can be used more or less anywhere in the world at relatively small cost for supporting installations and extra personnel. Special attention will be given to secure communication.

In order to interpret and present the results it is also necessary to learn how chemicals around an illicit production site are dispersed by full-scale measurements and modeling.

Expected results

The threat of terrorist attacks is a very real concern for citizens in many parts of Europe. Today there is no detection system that focuses on the production phase of explosives. A system like LOTUS would allow law enforcement agencies to become proactive, to act during a phase where there is low threat to citizens and thus prevent production during a time where alternative response actions can be exploited. The same system could also be used for combating organized crime by detecting if drug production.

Information

Acronym :
LOTUS

Grant Agreement N° :
217925

Total Cost :
€ 4,298,593

EU Contribution :
€ 3,189,146

Starting Date :
01/01/2009

Duration :
36 months

Coordinator :

SWEDISH DEFENCE RESEARCH AGENCY (FOI)
Department of Energetic Materials
Grindsjön Research Centre
SE-147 25 Tumba
SWEDEN

—

Contact :
Dr. Sara Wallin
Tel : +46 8 5550 4097
Mobile: +46 709 277008
Fax : +46 8 5550 3949
E-mail : sara.wallin@foi.se

Website :
www.lotusfp7.eu

Partners

NAME	COUNTRY
FOI	Sweden
Portendo AB	Sweden
Saab AB	Sweden
Bruker Daltonik GMBH	Germany
Ramem S.A.	Spain
Bruhn NewTech A/S	Denmark
Research and Education Laboratory in Information Technologies	Greece
TNO	The Netherlands
Universidad de Barcelona	Spain
Secrab Security Research	Sweden

MULTIBIODOSE / Multi-disciplinary biodosimetric tools to manage high scale radiological casualties

© rolffimages - Fotolia.com

Project objectives

In the event of a large scale radiological emergency biological dosimetry is an essential tool that can provide timely assessment of radiation exposure to the general population and enable the identification of those exposed people, who should receive immediate medical treatment. A number of biodosimetric tools are potentially available, but they must be adapted and tested for a large-scale emergency scenario. These methods differ in their specificity and sensitivity to radiation, the stability of signal and speed of performance. A large scale radiological emergency can take different forms. Based on the emergency scenario different biodosimetric tools should be applied so that the dosimetric information can be made available with optimal speed and precision.

Description of the work

One work package (WP) will be devoted to each tool. Starting with the state of the art, each tool will be validated and adapted to the conditions of a mass casualty situation. A training programme will be carried out where appropriate and automatisation as well as commercial exploitation of the tools will be investigated and pursued. Towards the end of the project, a comparative analysis of the tools will be carried out with respect to their sensitivity, specificity and speed of performance. Future training programmes will be developed. Two additional WPs will deal with: (1) the development of an integrated statistical software tool that will allow fast interpretation of results, and (2) the development of a guidance document, based on the TMT handbook, regarding the logistics of biodosimetric triage in a large scale accident and decision making regarding the methods best suitable for a given accident scenario. Moreover, a programme of disseminating the results among European emergency preparedness and radiation protection authorities will be carried out, so that the functional laboratories and networks can be easily contacted in the case of an emergency.

The project beneficiaries will be supported by an advisory committee that will include experts in bio-dosimetric tools and management of radiation accidents.

Expected results

The project will lead to the development and validation of biodosimetric tools used in mass casualty radiation accidents. The final result will be establishment of a biodosimetric network that is fully functional and ready to respond in case of a mass casualty situation. Thus, the project will strengthen the European security capabilities by achieving tangible technical and operational results.

Information

Acronym :
MULTIBIODOSE

Grant Agreement N° :
241536

Total Cost :
€ 4,661,432

EU Contribution :
€ 3,493,199

Starting Date :
01/05/2010

Duration :
36 months

Coordinator :

CENTRE FOR RADIATION PROTECTION RESEARCH
Department of Genetics, Microbiology and Toxicology
Stockholm University
Svante Arrhenius väg 20C
106 91 Stockholm, Sweden

—

Contact :
Andrzej Wojcik
Tel : +46 8 16 1217
Mobile: +46 762 122 744
Fax : +46 8 16 4315
E-mail : andrzej.wojcik@gmt.su.se

Website :
www.multibiodose.eu

Partners

NAME	COUNTRY
Stockholm University (SU)	Sweden
Bundesamt für Strahlenschutz (BfS)	Germany
Universiteit Gent (UGent)	Belgium
Health Protection Agency (HPA)	United Kingdom
Institut de Radioprotection et de Sûreté Nucléaire (IRSN)	France
Istituto Superiore di Sanità (ISS)	Italy
Norwegian Radiation Protection Authority (NRPA)	Norway
Radiation and Nuclear Safety Authority (STUK	Finland
Westlakes Scientific Consulting (WSC)	UK
Universitat Autonoma de Barcelona (UAB)	Spain
Institute of Nuclear Chemistry and Technology (INCT)	Poland
Helmholtz Zentrum München (HMGU)	Germany
Bundeswehr Institut für Radiobiologie in Verbindung mit der Universität Ulm (UULM)	Germany
Gray Institute for Radiation Oncology and Biology	United Kingdom
University of Oxford (UOXF)	United Kingdom
EURADOS (EURADOS)	Germany

NI2S3 / Net-centric information & integration services for security systems

© Aaron Kohr - Fotolia.com

Project objectives

Complex interactions between the elements of a critical infrastructure indicate, that there is also a need to deploy a corresponding infrastructure protection system, which is capable of extending security control to all elements of the protected system, and, at the same time, of maintaining a global view of the infrastructure.

The key objective of the NI2S3 project is to research and implement a reference methodology for developing security systems based on NEC Information and Integration Services for Critical Infrastructures. The security systems must be capable to of collecting and processing information from many heterogeneous sources in order to build up or improve situation awareness of critical infrastructures.

More specifically, the NI2S3 Project aims:

- to provide a definition and a design of an NI2S3 critical infrastructure protection system regarding the security, resiliency and availability of the subject infrastructure,
- to define performance indicators and tools for system validation,
- to develop a technology for the evaluation of the performance, robustness and reliability of such a protection system, and
- to develop a NI2S3 application demo.

Description of the work

The NI2S3 project is focused on the research and development of a reference methodology to guide the design and implementation of security systems for critical infrastructure protection, basing on the philosophy and the concepts of the NEC-based systems approached with SOA techniques.

The refining and validation of this methodology is performed by an application demonstrator, realized in accordance with NEC and SOA concepts.

R&D activities will be articulated into seven work packages:

1. Management;
2. Analysis of the state of the art;
3. Definition of scenarios, analysis and extraction of the system specifications;
4. Development of a reference methodology for design, and realization of a NI2S3;
5. Definition of a set of metrics and validation capabilities for the components and the protocols involved in NI2S3;
6. Project and design of prototype, and
7. Dissemination and exploitation.

The resulting protection system should involve all the necessary components and tools to acquire, exchange and process the state monitoring information. It should rely on the continuous feeding of the information, in order to ensure that it arrives at the right place, right on time, preferably in the form, which makes it quickly usable for the intended use purpose, and which can result in appropriate and timely actions.

NI2S3 Project will ensure that the prospective protection system is error-proof, in what concerns vulnerabilities. As an example, the protection system must not react in ways that may lead to erroneous, inadequate or disproportional system reactions. Instead, the NI2S3 system has to provide information at different granularity levels in a timely manner to plan, direct and control all operational activities pertaining to critical infrastructure protection.

Expected results

Critical transportation systems have an intrinsic international value, so that the most suitable instrument to achieve advances in the protection of such infrastructures is international co-operation.

NI2S3 cross-border project will give the chance of realizing technology and reference methodology for developing critical infrastructure security systems that can be better accepted by the possible stakeholders, being them designed under the guidelines of each of the participant's country needs.

The realization of a standard VA platform will be able to produce objective measurements of the robustness of heterogeneous networking software and hardware.

This activity is essential to introduce the concept of security metric, that is at the base of any evaluation and certification that is targeted at the security of a network element.

Information

Acronym:
NI2S3

Grant Agreement N°:
225488

Total Cost:
€ 4,325,728

EU Contribution:
€ 2,711,640

Starting Date:
01/07/2009

Duration:
24 months

Coordinator:

VITROCISET S.P.A.

—

Contact:
Walter Matta
phone: +39 06 88202567
Mobile: +39 335 7716488
Fax : +39 06 8820 2288
E-mail: w.matta@vitrociset.it

Website:
http://ni2s3-project.eu/

Partners

NAME	COUNTRY
Vitrociset S.p.A.(VCS)	Italy
Università degli Studi di Firenze (UNIFI)	Italy
HW Communications Limited (HWC)	United Kingdom
AALBORG Universitet (AAU)	Denmark
AGH University of Science and Technology (AGH)	Poland
Comarch S.A. (COMARCH)	Poland

NMFRDisaster / Identifying the needs of medical first responders in disasters

© Dmitry Pistrov - Fotolia.com

Project objectives

Manmade, as well as natural disasters occur more and more often. The medical response is an initial component of the overall response. Medical First Responders are presented daily with new and more complex challenges while preparing for and responding to those disasters

The objective of the project is to identify the needs of the first responders in five key areas, and to match those needs with existing knowledge, technology and products. The end product of the project will be a roadmap, suggested to the European Commission Enterprise General Directorate, pointing out areas where future Research and Developments activities are required.

The 5 Areas are:

1. Training Methodology and Technology
2. The Human Impact of Disasters
3. Law and ethics
4. Personal Protective Equipment
5. Use of Blood and Blood Components in Disasters

Description of the work

The work will be achieved through research activities conducted by the partners in charge, followed by workshops and a final report.

The research aim is to map existing know how and products, as well as lessons learned from real incidents. Then 5 workshops will be conducted. For each subject one workshop will be organised.

During the workshop the results of the research will be presented, and the needs of the first responders will be identified. As a result, a map of needs not covered by current knowledge and products will emerge. The final step will be to prioritise the identified needs. The final report will identify and prioritise the different needs identified as requiring further R&D.

The medical first responders will be invited to the workshops, along with experts in the field and representatives from the industry.

This project is unique since it brings together first responders from different realities in Europe, and the Middle East (Israelis and Palestinians). This broad view of realities, experiences and needs, with be further strengthen through the responders and experts who will be invited to participate in the workshops (Such as the Austrian Red Cross, Turkish Red Crescent, experts from Sarajevo).

The aim of this broad view is to ensure a real European perspective of the work, followed by a real contribution to achieving the of European goal safer communities.

Since this project involves first responders that have never been involved before in EU funded projects, a strong European network will be built, enabling exchange of experience and best practices along with interaction with research institutions, thus focusing researchers on the real needs of the field.

Expected results

The Direct result of this project will be a report suggesting areas where R&D activities are required, in order to have better response capacities, which result in better prepared European Communities. Besides the direct result, the following results are also expected:

» Building a strong network of Medical First Responders, with a broad view of different realities.

» Partnerships between First Responders and research institutes, thus focusing future activities more on identified needs. Giving an opportunity to the European Industry to have a real added value by meeting needs emerging from the grass root level.

» Involving organisations in Europe that did not participate so far in EU activities, in such projects.

In an overall view, in this project a real European impact is expected, providing an opportunity to new players to be involved in EU activities, building a strong network, that should result in cooperation between the end users and industry / researchers, and technology that will be more driven to meet the needs of the field.

Information

Acronym:
NMFRDisaster

Grant Agreement N°:
218057

Total Cost:
€ 815,079

EU Contribution:
€ 815,079

Starting Date:
01/05/2008

Duration:
12 months

Coordinator:

MAGEN DAVID ADOM
Yigal Alon 60
67062 Tel-Aviv
Israel

—

Contact:
Chaim Rafalowski
Tel: +972-36300292
Fax: +972-3-7396541
E-mail: chaimr@mdais.co.il

Partners

NAME	COUNTRY
Magen David Adom in Israel	Israel
SAMUR Proteccion Civil, Ayuntamiento de Madrid	Spain
AmbulanceZorg Nederland	The Netherlands
Danish Red Cross	Denmark
Sinergie S.r.l	Italy
Fundacion Rioja Salud	Spain
Center for Science, Society and Citizenship	Italy
Shield Group Inc.	Aruba
Charles University	Czech Republic
Al-Quds Nutrition and Health Research Institute	Palestinian territory

ODYSSEY / Strategic pan-european ballistics intelligence platform for combating organised crime and terrorism

© Dwight Davis - Fotolia.com

The threat from organised crime and terrorism can undermine the democratic and economic basis of societies. The result is a weakening of institutions and loss of confidence in the rule of law. The Odyssey project will undertake research to design and develop a secure interoperable situation awareness platform for the EU to combat organised crime and terrorism. The Platform will have the ability for information to be obtained using advanced semantic knowledge extraction and data-mining techniques to facilitate fast , responsible decision making. The benefits will be mutual co-operation, security and sustainability across the EU.

Project objectives

To develop a secure interoperable platform for automated information analysis to combat organised crime and terrorism:

» Create European Standards for ballistics data collection, storage and sharing.

» Secure interoperable platform for ballistic information management.

» Automated sharing, processing, and analysis of ballistic data.

» Ability to undertake data-mining and knowledge extraction to tackle organised crime and terrorism across the EU. This will allow com-plex conclusions to be generated for appropriate and fast decision making.

» Ability to exploit automated and semi-automated data processing techniques. This will have the capability to generate a 'Red Flag' situation awareness alert.

» New and improved methods for comparison of micro- and nano-forensics that supplement current approaches.

» The ability for EU Member States to manage security, access and report in cost effective ways.

» Enhance mutual co-operation, security and sustainability across the EU.

Description of the work

The project is divided into seven work packages. This includes work packages for management and dissemination.

The project technical work packages will consist of the following:

» Intelligence Ballistic data capture and knowledge extraction.

» Ballistic risk management process support.

» Extended interoperability layer for semantically managing the Odyssey platform.

The realisation of the above will result in:

» Acquiring integrated data including future multimedia sources and enriching data through a semantically enhanced meta-database.

» Developing knowledge extraction algorithms and defining methodologies for mining and pattern discovery.

» Setting up a ballistic prediction, detection, and monitoring tool.

» Building an info-broker ballistic framework for knowledge process modelling.

» Creating a policy driven data exchange platform.

Expected results

The Odyssey project will deliver a framework that will create a management ballistics information platform within the EU. Proposed outcome:

» An ICT platform for the sharing of ballistic firearms information.

» Improvements in the ballistics data warehousing technologies for investigation purposes.

» The ability to transmit ballistic images and access files across European security organisations.

» The ability to advance in querying, knowledge extraction and intelligence sharing.

» The exploitation of legacy systems.

Information

Acronym :
ODYSSEY

Grant Agreement N° :
218237

Total Cost :
€ 3,821,599

EU Contribution :
€ 2,400,000

Starting Date :
01/11/2008

Duration :
30 months

Coordinator :

SHEFFIELD HALLAM UNIVERSITY
Howard Street
UK - S1 1WB Sheffield
United Kingdom

—

Contact :
Professor B. Akhgar
Tel : +44(0)114 225 6770
Fax : +44(0)114 225 6931
E-mail : b.akhgar@shu.ac.uk

Website :
www.odyssey-project.eu

Partners

NAME	COUNTRY
Sheffield Hallam University	United Kingdom
Atos Origin	Spain
Forensic Pathways Ltd	United Kingdom
EUROPOL	The Netherlands
XLAB	Slovenia
SESA	Austria
Politecnico di Milano	Italy
West Midlands Police	United Kingdom
National Ballistics Intelligence Service Royal Military Academy	Belgium
An Garda Siochana (Police Forensic Service)	Republic of Ireland
SAS Software Limited	United Kingdom
D.A.C. – Servizio Polizia Scientifica	Italy

OPARUS / Open architecture for UAV-based surveillance system

© Netfalls - Fotolia.com

Project Objectives

OPARUS is a Coordination and Support Action. The goal is to propose and elaborate an open architecture for the operation of unmanned air-to-ground wide area land and sea border surveillance platforms in the European Union. This project is based on the statement that EU border protection using comprehensive and improved methods of border observation should be carried out by means of a coordinate policy and procedure. For that purpose the Commission has proposed the creation of a European Border Surveillance System (EUROSUR). Within that context the deployment of Unmanned Aircraft Systems (UAS) of various types and capabilities is anticipated to offer a major increase in the capabilities of border surveillance agencies by increasing the effectiveness and minimizing the cost of surveillance. However the establishment of a common European integrated border information system (known as the "virtual border" concept) requires that intelligence sources like UAS be interoperable and provide information in an open environment using standard interfaces. The definition of such standard interfaces is the central challenge of OPARUS

Description of the work

The project is divided into 5 main technical Work Packages (WP):

- **WP 1 (Concepts and Scenarios)** is dedicated to compilation and analysis of the operational concepts and scenarios of UAS use in the context of maritime and land aerial surveillance of European borders. The border surveillance missions that could be performed by UAS will be identified, and then further refined into scenarios in order to provide an operational framework to the architecture design. This task will propose complete concepts of data / information exchange between scenarios participants, including operational protocols. In this phase the end-user needs will be taken into account through direct exchange (Workshop).
- **WP 2 (Legislation Analysis)** intends to describe the current and emerging regulation framework for insertion of UAS into controlled civil airspace in order to identify its limitations regarding UAS border surveillance operations, and to recommend some legislation evolutions favouring the UAS use in border surveillance.
- **WP 3 (Technical Analysis)** is a central task dedicated to the parallel analysis and synthesis of the technical capabilities available for 4 main UAS components: the surveillance sensors, the aerial platforms, the datalink and communication networks and the ground stations. Generic classes of UAS components will be defined and described in terms of performances and costs.
- **WP 4 (Open Architecture Definition)** is dedicated to the identification of open architecture solutions to perform border surveillance missions. This task particularly focuses on cost-efficient solutions enabling maximum efficiency of UAS operations for European border surveillance.
- **WP 5 (Information Exchange and Dissemination)** is a Work Package dedicated to maintain a close communication level with the end-users, grouped in a User Advisory Board, in order to acknowledge and to check project consistency with the end-users requirements.

Expected results

OPARUS is expected to provide a set of solutions covering both short-term and longer-term perspectives. In both terms, the proposed open architecture will have the following impacts:

- Fostering non-proprietary solutions for equipments and sub-systems (sensors, platforms, data links, and ground stations).
- Allowing smaller companies and SME's from many member countries to enter the market.
- Open-up the market for non-military companies.
- Develop the dialogue between European end-users and make international operations between different nations more feasible.
- Allow companies to share different parts of a more complex system which distributes development costs and risks to a broader basis. This will foster the development of industrial co-operation similar to the "Airbus model".
- Provide an overall benefit to the end-users by optimisation of costs (through lower development costs) and mission efficiency. The customer is expected to get a system of different classes of sub-systems which can be selected for joint operations for more performance instead of having heavily competing single systems.

Overall, OPARUS activities contribute to the development of new markets for UAS by means of harmonized interfaces which both facilitate the standardisation effort and reduce the ownership costs.

Information

Acronym :
OPARUS

Grant Agreement N° :
242491

Total Cost:
€ 1,188,313

EU Contribution:
€ 1,188,313

Starting Date:
01/09/ 2010

Duration:
18 months

Coordinator :

SAGEM DÉFENSE SÉCURITÉ
27 rue Leblanc,
75015 Paris
France
—

Contact :
Olivier REICHERT
Phone : 33 1 40 70 67 26
Mobile : 33 6 30 97 23 37
E-mail : olivier.reichert@sagem.com

Partners

NAME	COUNTRY
Sagem Défense Sécurité	France
AFIT (Air Force Institute of Technology,)	Poland
BAE Systems	UK
Dassault Aviation	France
DLR	Germany
EADS-CASA	Spain
IAI	Israel
INTA	Spain
ISDEFE	Spain
ONERA	France
Selex Galileo	Italy
Thales Communication	France
Thales Systèmes Aéroportés	France

OPERAMAR / An interoperable approach to european union maritime security management

© Bruno Delacotte - Fotolia.com

Project objectives

OPERAMAR Support Action is meant to provide the foundations for pan-European Maritime Security Awareness, as prescribed by the Maritime Policy, by addressing the insufficient interoperability of European and national assets and generating unified data models for seamless exchange, addressing the hurdles raised by the existing different behavioural, organisational, and cultural issues.

It is today recognized, that effective management of Maritime Security activities by the EU requires the capability to collect and fuse available data into a common picture of the relevant maritime environment to be shared among the organizations of participating Member States.

OPERAMAR, networking the competence of national users belonging to EU Member States and Associated countries, European agencies and industrial partners all actively involved in the Maritime domain, will :

» Grasp a better knowledge of Maritime Security users needs and their organizations and define interoperability models and analyse the associated issues, taking into consideration the challenging characteristics of the organizational environment in which they will be implemented,

» Develop common interoperability requirements and translate them into technical requirements, and

» study the consequences and recommend a relevant strategic research roadmap.

Description of the project

OPERAMAR will consist in the establishment of an EU and Associated Countries network of maritime stakeholders, that will identify interoperability challenges, for improving operational coordination.

This study will promote cross fertilization into organizations, structures and systems and will provide, as a result, common requirements and guidelines, to increase situation awareness in maritime environment.

OPERAMAR will also suggest to the EC recommendations in terms of future research programmes, projects and new standards.

OPERAMAR partners have achieved to date 35 visits of Maritime Surveillance Operational Centres of all nature in EU and Turkey, getting direct operator's feddback and observing current tools and procedures in action. They have also presented the project in several workshops, congresses and Maritime Events.

The present situation shows high level of fragmentation, due to many factors: different national procedures, legislations and systems in place, different levels of command and decision making.

OPERAMAR will fill an important gap to solve this issue, by supporting the definition of common requirements and operational procedures, as well as new interoperability standards, at the EU level, that should be adopted at national and local level.

From the analysis of the present situation, the stakeholders network will identify the key interoperability challenges, that will produce significant improvements on the operational performances. The effectiveness of the methodological results will be tested in three scenarios, Mediterranean, Black Sea and Atlantic Ocean (Canary Islands).

Then, the OPERAMAR will translate these interoperability requirements, into guideline for technical requirements, common architectures and systems specifications.

This will include suggestions for improvements in the compatibility of all interfaces for data-exchanges. The ultimate goal is to achieve a common picture of the situations, supporting the end-users decision making process.

OPERAMAR strategic roadmap will describe the evolution of an interoperable approach to the European Union maritime security management from the multiple perspective of organizations, institutions, legislation and regulations.

It will identify priority areas for additional security research to facilitate the development at Regional and European levels. The roadmap will contribute to future FP7 and other European security linked activities taking into account the work of the ESRIF.

Information

Acronym:
OPERAMAR

Grant Agreement N°:
218045

Total Cost:
€ 669,132

EU Contribution:
€ 669,132

Starting Date:
01/03/2008

Duration:
15 months

Coordinator:

THALES UNDERWATER SYSTEMS SAS
Route des Dolines 525
FR – 06903 Sophia Antipolis
France

—

Contact:
Bernard GARNIER
Tel: + 33 4 9296 3000
Fax: + 33 4 9296 4032
E-mail: Bernard.garnier@fr.thalesgroup.com

Website:
www.operamar.eu

Partners

NAME	COUNTRY
Thales Underwater Systems SAS	France
Selex Sistemi Integrati SpA	Italy
Indra Systema SA	Spain
Quintec Associates Ltd	United Kingdom
Alliance of Maritime Regional Interests in Europe	Belgium
Directorate General, Joint Research Centre	Belgium
Instituto Affari Internazionali	Italy
Edisoft	Portugal
Savunma Teknolojieri Muhendislik	Turkey
Thales Systèmes Aéroportés	France

OPTIX / Optical technologies for identification of explosives

© Eline Spek - Fotolia.com

Project objectives

Terrorism, as evidenced by recent tragic events (Madrid 2004, London 2005, New York 2001), is a real and growing threat to Europe and the world. Attacks using Improvised Explosive Devices (IEDs) appear in the news every day. More than 60% of terrorist attacks are carried out by the use of such explosive devices.

Security forces demand new tools to fight against this threat. One of the most demanded capabilities by end users is that of standoff detection and identification of explosives. Today's technologies are not able to provide these capabilities with the required minimum reliability.

The objective of the project is to contribute to increasing the security of the European citizens by the development of a transportable system for the standoff detection and identification of explosives in real scenarios at distances of around 20 metres (sensor to target), using alternative or simultaneous analysis by three different complementary optical technologies (LIBS, RAMAN, IR).

Description of the work

The project activities of OPTIX have been broken down in ten work packages and distributed along 42 months.

OPTIX will perform important progress beyond the state of the art in three different ways:

» Specific developments regarding the individual core technologies (LIBS, RAMAN and IR) for standoff detection and identification of explosives.

» Specific developments of the enabling technologies being addressed in the project: lasers, spectrometry, optics and data fusion and analysis.

» Integration of all technological developments onto a single system to leverage and enhance the individual capabilities for the standoff detection and identification of explosives.

First stage will be dedicated to the System Definition. The project consortium will perform a focused research on the core optical technologies addressed by the project. Scenarios and system requirements will be defined. This is a key stage for the success and final usefulness of the system from the end user's point of view. Workshops with end users will be organised.

Technology development of LIBS, RAMAN, IR (core technologies) and laser, spectrometry, optics and data fusion (enabling technologies) will follow.

Phase three is System Integration, where a single platform will be developed.

Testing will be carried out in laboratories and also in real environment scenarios, adequately supported by end users. Evaluation of results will follow.

Dissemination and Exploitation will provide information of the project's activities, performance and results both at public and restricted levels, as well as definition and carrying out the initial exploitation of the outcomes and foreground of OPTIX. Workshops with end users and other potential stakeholders will take place.

Expected results

» Improved capabilities of LIBS, RAMAN and IR for the detection of explosives at standoff distances.

» Enhanced spectrometrics for an Integrated OPTIX system.

» Advanced data fusion and chemometrics algorithms.

» A technology demonstrator capable of detecting explosive traces at distances of 20 metres.

» Demonstrated capabilities of the developed system to end users and to additional stakeholders as needed.

Information

Acronym:
OPTIX

Grant Agreement N°:
218037

Total Cost:
€ 3,289,855

EU Contribution:
€ 2,487,556

Starting Date:
01/11/2008

Duration:
42 months

Coordinator:

INDRA SISTEMAS S.A
Security Systems
Paseo del Club Deportivo, 1. Edif.5
28223-Pozuelo de Alarcón (Madrid)
Spain

—

Contact:
Carlos de Miguel
Tel :+(34) 91 257 95 73
Mobile: + (34) 650 505 091
Fax :+ (34) 91 257 70 18
E-mail : cdemiguel@indra.es

Website:
www.fp7-optix.eu

Partners

NAME	COUNTRY
Indra Sistemas S.A	Spain
University of Malaga	Spain
FOI	Sweden
EKSPLA UAB	Lithuania
AVANTES BV.	The Netherlands
Technical University of Clausthal	Germany
Vienna University of Technology	Austria
University of Dortmund	Germany
Guardia Civil	Spain

OSMOSIS / Overcoming security market obstacles for SMEs' involvement in the technological supply chain

Project objectives

The OSMOSIS project objective is to foster the involvement of SMEs in the security technology supply chain and to facilitate the collaboration between SMEs and the key stakeholders in the European Security domain.

OSMOSIS will create a nurturing environment for the involvement of SMEs in the overall Security Market, through a set of services including:

- Identification of untapped market potentials in the technology security market supply chain.
- Liaison with large organisations to foster the involvement of SMEs in the security technology supply chain, including the involvement in joint R&D activities.
- The creation of a database of qualified SMEs that will create "meta-clusters" where Large Enterprises could identify partners for their engineering and/or R&D projects.
- Full support to SMEs to favour their involvement in the security supply chain.
- Dissemination and networking events to create a collaborative environment among key stakeholders.

Description of the work

The OSMOSIS method is strongly based on the background of the consortium, and on their unique capabilities and expertise as technology transfer organisations providing services to Large Organisations and SMEs in Europe.

The project methodology will be driven by the following three main pillars:

1. Actions towards Key Stakeholders operating in the Security Technology supply chain, to stimulate and support such organisations in involving SMEs in engineering projects as well as in research projects, and to gather relevant information about untapped market potentials.
2. Actions towards SMEs, to create awareness on technology supply chain opportunities and provide specific services that help SMEs to enter the overall market supply chain.
3. Actions aimed at setting up means to facilitate communication and networking among key stakeholders and organizations.

An added value proposition will be carried out for the engagement of large enterprises. The focus will be placed on the added value that OSMOSIS could provide to them:

- the competitiveness improvement of the Ecosystem of the Large Organization,
- the capability of benefit from innovations and technological expertise offered by SMEs, and
- achievement of Corporate Social Responsibility objectives.

In addition, the OSMOSIS website, will be a reference point for key stakeholders looking for pre-qualified organisations with specific competences/skills in the security sector. The website includes services as:

- Access to a database of SMEs, classified following a specific taxonomy and including only relevant SMEs operating in security related engineering and/or research activities.
- A list of security research opportunities that could be exploited by SMEs to collaborate with Large Organizations.
- Information on security-related grants.
- Interactive communication tools to allow the communication of the identified opportunities and the transfer of specific knowledge to SMEs of the different meta-clusters.

Expected results

- More than 50 key stakeholders involved in the action.
- More than 250 pre-qualified SMEs will be included in the database, and their scientific, technology and engineering skills assessed, as well as technology development plans.
- Information campaign reaching more than 5.000 SMEs and other organisations.
- Support the start up of 20 collaborations among organisations not previously involved in the security technology supply chain with key stakeholders.

Information

Acronym:
OSMOSIS

Grant Agreement N°:
242416

Total Cost:
€ 725,432.60

EU Contribution:
€ 580,889

Starting Date:
01/04/2010

Duration:
24 months

Coordinator :

CiaoTech Srl
Via Palestrina 25
00189 - Rome
Italy
http://www.ciaotech.com

—

Contact :
Mr. Paolo SALVATORE
Tel. +39 06 33268972
Fax + 39 06 33267022
E-mail : p.salvatore@ciaotech.com

Website :
www.osmosisecurity.eu

Partners

NAME	COUNTRY
CIAOTECH S.r.l.	Italy
SESM Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l.	Italy
GMVIS Skysoft, S.A.	Portugal
Consorzio Interuniversitario Nazionale per l'Informatica	Italy
Technische Universität München (TUM)	Germany
INNOSTART Nemzeti Uzleti es Innovacios Kozpont Alapítvany	Hungary
Honeywell, spol. s r.o.	Czech Republic
Instituto Nacional de Tecnica Aeroespacial	Spain
Fundación madrimasd para el Conocimiento	Spain
ELSAG Datamat S.p.a.	Italy
PNO Consultants S.A.S.	France

PANDORA / Advanced training environment for crisis scenarios

© Evan Luthye - Fotolia.com

Project objectives

PANDORA is a crisis management project developing a training toolset and environment, which aims to bridge the gap between table-top exercises and real world simulation exercises. The project proposes a global approach to crises management, providing a near-real training environment at affordable cost.

The project will create an environment that can provide appropriate metrics on the performance of a crisis manager actively engaged in the management of a crisis, with the environment providing:

- A realistic and complete scenario with near real-time action, coherent with that expected in a real-world situation;
- Realistic emotional status, through affective inputs and stress factors;
- The potential to include different crises managers belonging to different sectors.

PANDORA offers a focus on the emotional status of the crisis manager because such knowledge, in all phases of emergency management, is critical to the development of effective emergency policies, plans and training programs.

Description of the work

To achieve the aims of the PANDORA project, the workload has been broken down into 9 work packages:

- **WP1:** User Requirements Analysis and design of PANDORA functional specifications – will provide a definition of both data and workflows needed to specify the proposed system and to clearly identify the processes that are the basis of the system services.
- **WP2:** Behaviour simulation and modelling - split into 5 tasks: the first two consolidate the basic preconditions for the behavioural planner, the third designs the general architecture of the planner, the remaining two provide proactive reasoning services to the planner.
- **WP3:** Crisis simulation and modelling - focused on three main modules: (1) the crisis knowledge base, (2) the crisis planner that generates the conceptual high level network of events that constitutes the plot for the scenario, and (3) the crisis modeller that tracks the evolution in real time of the scenario.
- **WP4:** Environment and Emotion Simulation Engine – seeks to integrate emotional human factors within training programs for crisis managers, taking into account several research topics:
  - Relevant human factors in crisis decision-making
  - Neuro-physiological testing and measures
  - Personalised and flexible training strategies
- **WP5:** Environment design and building – seeks to authentically recreate the dynamic elements of the entire disaster environment, i.e. emulating a complete crisis room with realistic visuals and audio to create an immersive, chaotic and stressful environment.
- **WP6:** Development, integration and testing – will deliver the PANDORA software product that can be considered as a system composed of software subsystems/components implemented on different environments.
- **WP7:** Training testing, evaluation and assessment – will support the development of a robust evaluation methodology that complements the work done to build the PANDORA advanced training environment.
- **WP8:** Dissemination and exploitation
- **WP9:** Project management

Expected results

The project will categorise the current state-of-the-art in crisis management tools and environments.

PANDORA will develop 3 key components:

- The crisis engine, which provides a scenario-based, interactive structure for the crisis management event
- The emotion engine, which tags and manages information for training scenarios on the basis of emotional affect
- The training environment, which integrates multimedia components dynamically to reflect a developing narrative-based crisis scenario

Information

Acronym:
PANDORA

Grant Agreement N°:
225387

Total Cost:
€ 3,995,071

EU Contribution:
€ 2,930,000

Starting Date:
01/01/2010

Duration:
2 years

Coordinator :

University of Greenwich
Old Royal Naval College,
Park Row, Greenwich
UNITED KINGDOM
—

Contact :
Reginald DALY
Tel: +44 02083319685
Fax: +44 02083318665

Website :
http://PANDORAproject.eu/

Partners

NAME	COUNTRY
University of Greenwich	United Kingdom
University of East London	United Kingdom
Cabinet Office - Emergency Planning College	United Kingdom
Consiglio Nazionale delle Ricerche, ISTC	Italy
CEFRIEL Società Consortile a Responsabilità Limitata	Italy
Fondazione Ugo Bordoni	Italy
XLAB Razvoj programske opreme in svetovanje d.o.o.	Slovenia
ORT	France
Business Flow Consulting	France

RAPTOR / Rapid deployable, gas generator assisted inflatable mobile security kits for ballistic protection of European civilians against crime and terrorist attacks

© Ivan Tykhyi - Fotolia.com

Project objectives

The objective of the project is the development of a mobile, rapid deployable and inflatable structure for ballistic protection of European civilians against threat scenarios, such as crime and terrorist attacks.

Tailored solutions are to be developed for supporting the prevention of or the response to, threat scenarios by European security forces. The scope is on protecting:

» individuals,

» general security of events,

» humanitarian workers, e.g. Red Cross, fire brigades, etc.

Description of the work

» Definition of threat scenarios such as acts of terrorism and organised crime. Based on these scenarios, specifications for the development of the security kit are defined and criteria for the demonstration of their effective performance derived.

» Development of textiles and coatings for ballistic protection with respect to foldability, light weight and environmental influence.

» Development of textiles and coatings for inflatable structures and suitable coverings for transport and storage.

» Development and characterization of a gas generator formulation with high mass specific gas output, low gas temperature and non-toxic gas components.

» Evaluation and testing of combustion chamber designs with respect to small size and light weight.

» Consolidation of the demonstrators will comprise the incorporation of all basic systems e.g. gas generator, ballistic protection design and the inflatable structure.

» The final tests of the demonstrators will be done according to the defined threat scenarios. The results will be reviewed according to the goals set out at the start of the project.

» Development of a dissemination plan of the results and knowledge obtained in the project.

Expected results

» Compilation of threat scenarios,

» Performance requirements of protection kit,

» Selection of ballistic protection textiles appropriate to security kits requirements,

» Development of textiles and coatings for inflatable structures,

» Ballistic testing to explore the effectiveness of multi-layer set-up,

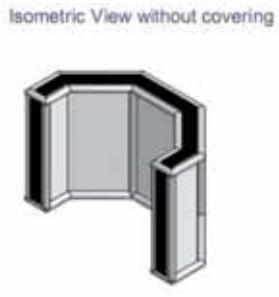
» Gas generator composition characterised by high gas output and fast burning behaviour

» Adjusting of gas generator module to assure reliable inflation,

» Consolidation,

» Final testing of demonstrators, and

» Innovation plan, exploitation plan and feasibility study.



Information

Acronym:
RAPTOR

Grant Agreement N°:
218259

Total Cost:
€ 2,849,867.76

EU Contribution:
€ 2,060,995.13

Starting Date:
01/01/2010

Duration:
48 months

Coordinator:

FRAUNHOFER (FHG-ICT)
Institut für Chemische Technologie ICT
Joseph-von-Fraunhoferstr. 7
76327 Pfinztal, Germany

—

Contact:
Dr. Norbert Eisenreich
Tel +49 (0)721 4640 138
Fax +49 (0)721 4640 538

Dipl.-Ing. Johanna Schubert
Tel +49 (0)721 4640 249
Fax +49 (0)721 4640 111

Website:
http://www.ict.fraunhofer.de

Partners

NAME	COUNTRY
FRAUNHOFER (FHG-ICT)	Germany
Bundeskriminalamt (BKA)	Germany
Explosia	Czech Republic
Fraunhofer (FhG-ICT) (Coordinator)	Germany
Lanco	Germany
P-D Interglas	United Kingdom

SAFE-COMMS / Counter-terrorism crisis communications strategies for recovery and continuity

© Loren Rodgers - Fotolia.com

Project objectives

The goal of the project is to help public authorities in Europe better reacting to terror crises by providing effective communication strategies for the aftermath of terror attacks. Such attacks take place when least expected, as terrorists search for vulnerable targets across Europe and seek to spread fear and panic.

A terror attack instantly becomes breaking news in the media throughout the world. Effective recovery from such an attack depends also on a carefully planned and trained communication strategy which would restore public confidence and enable quick return to normality.

In order to effectively deal with the aftermath of terror attacks, public authorities need a counter-terrorism communication strategy comprised of activities aimed at the relevant audiences. This strategy needs to be trained and adapted before an attack takes place and forms an inherent part of crisis management and continuity plans. SAFE-COMMS aims to provide public authorities throughout Europe with an effective and modular communication strategy for terror crises.

Description of the work

The first stage of the project analyses the communication challenges and problems that terror attacks present to public authorities and the requirements of media coverage of terror attacks on local, regional, national and international levels.

In the second stage of the project, four research groups explore and analyse a wide range of actual terror case studies in Northern Ireland, Spain, Greece and Israel respectively. This analysis examines the communication reactions to each attack, how authorities responded in the immediate hours after the attack, the type and scope of information provided to the media and public, emergency services' press activities, information released about victims, communication activities aimed at reassuring the public and preventing panic and chaos, recovery activities and return to normality.

The third stage of the project then builds upon the case study analysis to develop a terrorism crisis communication strategy. The strategy will comprise short and long-term activities aimed at decreasing the effects of terror attacks on the general public.

Expected results

The outcome of the project will be the Terrorism Crisis Communication Manual and accompanying audiovisual training aids, aimed at easy and effective dissemination of the project's communication strategy to public authorities throughout Europe. The Manual will be made available in three languages. Public authorities will be able to adopt relevant parts of the strategy, incorporate them into their wider crisis recovery plans and train their personnel in effective communications for terror crises. By implementing the SAFE-COMMS strategy, public authorities will be better prepared to respond effectively in case of a terror attack.

© Pakmor - Fotolia.com

Information

Acronym :
SAFE-COMMS

Grant Agreement N° :
218285

Total Cost :
€ 1,397,232

EU Contribution :
€ 1,088,244

Starting Date :
01/04/2009

Duration :
24 months

Coordinator :

BAR-ILAN UNIVERSITY
Department of Political Studies
Bar-Ilan Campus
Ramat Gan 52700, Israel

—

Contact :
Dr. Shlomo Shpiro
Tel : +972-3-531-7061
Mobile: +972-544-550-840
Fax : +972-3-736-1338
E-mail : sshpiro@bezeqint.net

Partners

NAME	COUNTRY
Bar-Ilan University	Israel
A&B One GmbH	Germany
Research Institute for European and American Studies	Greece
University of Ulster	United Kingdom
Universidad de Burgos	Spain
University of Rousse Angel Kunchev	Bulgaria

SAFIRE / Scientific approach to finding indicators and responses to radicalisation

© SAFIRE

Project objectives

The goal of SAFIRE is to improve fundamental understanding of radicalization processes and use this knowledge to develop principles to improve (the implementation) of interventions designed to prevent, halt and reverse radicalization.

Description of the work

SAFIRE develops a process model of radicalization, describing the process from moderation to extremism, based on a non-linear dynamic systems approach and a typology of radical groups. This represents an innovative approach that has not been explicitly applied to this area up until now. We will develop intervention principles in close concert with the models and apply them in a longitudinal, empirical study. We will also address other important aspects of radicalization such as the relationship between national culture and radicalization, radicalization on the Internet, and defining observable indicators of the radicalization process.

Expected results

The results of this project increase the understanding of both conceptual aspects of radicalization (e.g. the psycho-social dynamics of radical groups and individuals), and practical characteristics and modus operandi of radical groups (e.g. recruitment techniques). In addition, the results increase understanding of field efforts and interventions when, why and how they work.

The insights and products resulting from SAFIRE help policy makers, researchers in the field of radicalization and professionals who work with high-risk individuals to better understand the phenomenon with which they are working. This insight combined with the results from the empirical study, also help end-users to better focus and structure the allocation of resources and the implementation of interventions.

Information

Acronym:
SAFIRE

Grant Agreement N°:
241744

Total Cost:
€ 3,681,260.00

EU Contribution:
€ 2,906,600.95

Starting Date:
01/06/2010

Duration:
42 months

Coordinator:

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK - TNO
Schoemakerstraat 97
PO Box 6060
NL-2600 JA Delft
The Netherlands

—

Contact:
Dr. Heather Griffioen-Young
Tel: +31-346356378
Fax: +31-346353977
E-mail: heather.griffioen@tno.nl

Website:
http://www.safire-project.eu

Partners

NAME	COUNTRY
TNO	The Netherlands
Stichting Forum, Instituut voor Multiculturele Ontwikkeling	The Netherlands
International Security and Counter-Terrorism Academy	Israel
Rand Europe Cambridge Ltd	United Kingdom
Stichting Hogeschool Utrech	The Netherlands
Bridge 129 Spa Safety and Security	Italy
Compagnie europeenne d'intelligence stratégique SA	France
Universidade de Coimbra	Portugal
Fondation pour la recherche stratégique	France
Universiteit van Amsterdam	The Netherlands

SAMURAI / Suspicious and abnormal behaviour monitoring using a network of cameras & sensors for situation awareness enhancement

© diego cervo - Fotolia.com

Project objectives

The aim of SAMURAI is to develop and integrate an innovative intelligence surveillance system for monitoring people and vehicle activities at both inside and surrounding areas of a critical public infrastructure.

SAMURAI will provide innovative and critical techniques for permanent monitoring of a critical infrastructure site (e.g. an airport or train station concourse, a football stadium or a shopping mall).

The SAMURAI project is unique in that in addition to project partners, a User Advisory Group provides advice on the user requirements and specifications for the SAMURAI systems by providing a variety of scenarios for data capture and system evaluation.

Description of work

SAMURAI will develop robust moving object, segmentation, categorization and tagging in video captured by multiple cameras from medium-long range distance, e.g. identifying, monitoring and tracking people with luggage between different locations at an airport. Automated focus of attention and identification in a distributed sensor network includes fixed and mobile cameras, positioning sensors and wearable audio or video sensors.

Global situational awareness assessment involves image retrieval of objects by types and movement patterns with incidents across a distributed network of cameras. Online adaptive unusual behaviour monitoring will profile and check inference of unusual behaviours / events captured by multiple cameras. The project will also exploit methods for feeding back into the algorithm human operator's evaluation on any abnormality detection output in order to guide and speed up the incremental and adaptive behaviour profiling algorithm. SAMURAI will allow prevention and rapid-response to events as they unfold.

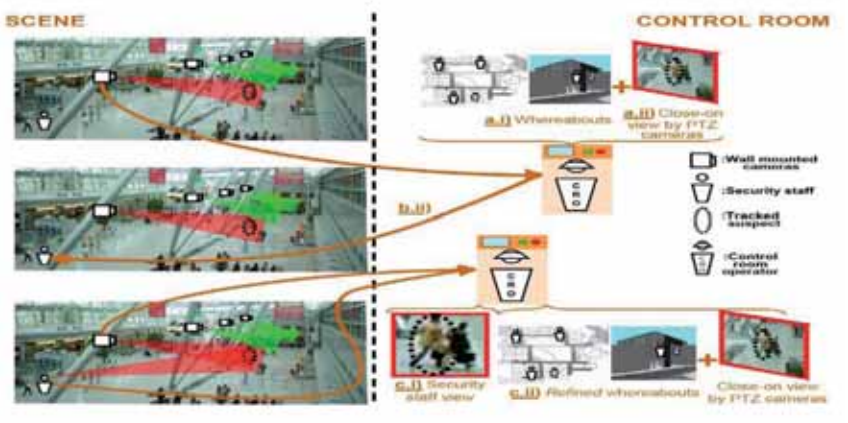
Expected results

SAMURAI will develop groundbreaking technology that can be interfaced with existing CCTV systems already employed widely within the EU. By concentrating the technology developments onto multiple cameras and mobile cameras, many of the limitations of the existing state-of-the-art will be overcome by incorporating strong end-users with a widely deployed CCTV system in the Consortium.

Security in public places is required for the correct functioning of society. However, existing CCTV systems are not effective at prevention of many incidents. Consequently, by improving these current CCTV systems, the main social impact of SAMURAI should be increased public confidence in security systems in public places.

The use of CCTV as a security and management aid is widespread in the EU and offers a huge marketplace for European business.

SAMURAI should provide a higher 'added-value' to installed CCTV system and give European producers a substantial advantage in the marketplace.



Information

Acronym :
SAMURAI

Grant Agreement N° :
217899

Total Cost :
€ 3,638,131

EU Contribution :
€ 2,478,052

Starting Date :
01/06/2008

Duration :
36 months

Coordinator :

QUEEN MARY, UNIVERSITY OF LONDON
Department of Computer Science
Mile End Road
E1 4NS London
United Kingdom

—

Contact :
Shaogang GONG
Tel : +44 20 7882 5249
Fax : +44 20 8980 6533
E-mail : sgg@dcs.qmul.ac.uk

Website :
www.samurai-eu.org

Partners

NAME	COUNTRY
Queen Mary, University of London	United Kingdom
Universita' degli Studi di Verona	Italy
Elsag Datamat S.p.A.	Italy
Waterfall Solutions Ltd	United Kingdom
Borthwick-Pignon OÜ	Estonia
Esaprojekt SP. Z O.O.	Poland
Syndicat Mixte des Transports pour le Rhône et l'Agglomération Lyonnaise	France
BAA Limited	United Kingdom

SEABILLA / Sea border surveillance

© Colette - Fotolia.com

Project objectives

» Define the architecture for cost-effective European sea border surveillance systems, integrating space, land, sea and air assets, including legacy systems.

» Apply advanced technological solutions to increase performances of surveillance functions.

» Develop and demonstrate on the field significant improvements in detection, tracking, identification and automated behaviour analysis of all vessels, including hard to detect vessels, in open waters as well as close to coast.

Description of the work

SEABILLA is based on requirements for sea border surveillance defined by experienced operational users. These requirements have been transformed into scenarios, representative of gaps and opportunities for fruitful co-operative information exchange between Members States:

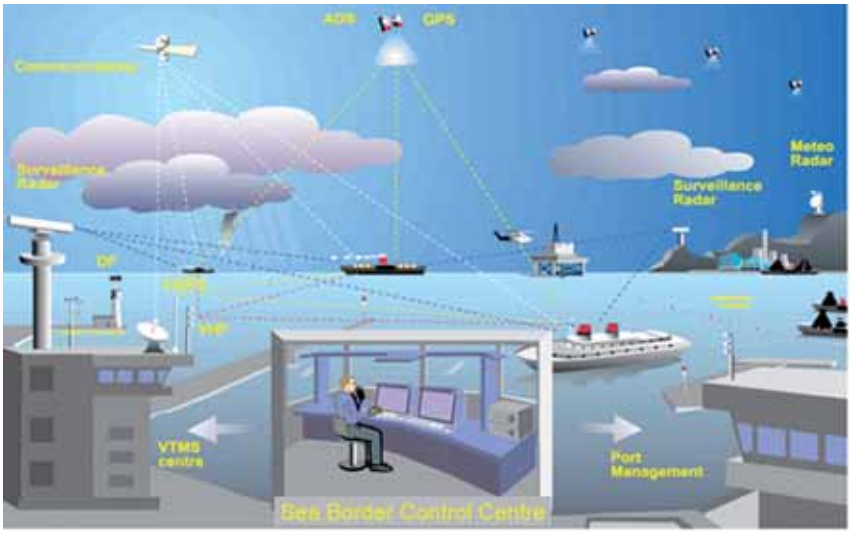
» for fighting drug trafficking in the English Channel;

» for addressing illegal immigration in the South Mediterranean; and

» for fighting illicit activities in open-sea in the Atlantic waters from Canary Islands to the Azores in coherence with the EU Integrated Maritime Policy, with the EU Integrated Border Management Policy (ref. EUROSUR), and in compliance with Member States sovereign prerogatives.

Expected results

The project will provide a feasible, cost effective solution in terms of maritime surveillance, based on best combination of advanced technology in the context of legacy systems, that could be implemented at national and EU level to increase effectiveness, pool resources and address successfully Maritime Security and Safety challenges.



Information

Acronym:
SEABILLA

Grant Agreement N°:
241598

Total Cost:
€ 15,549,679

EU Contribution:
€ 9,843,601

Starting Date:
01/06/2010

Duration:
45 months

Coordinator:

SELEX SISTEMI INTEGRATI SPA
Via Tiburtina km 12,400,
00131 Roma, Italy

—

Contact:
Salvatore RAMPINO
Tel: +39 06 4150 2407
Mobile: +39 3357389405
Fax: +39 06 41502694
E-mail: srampino@selex-si.com

Website:
www.seabilla.eu

Partners

NAME	COUNTRY
SELEX Sistemi Integrati SPA	Italy
ALENIA AERONAUTICA	Italy
BAE SYSTEMS	United Kingdom
CNIT (CONSORZIO NAZIONALE INTERUNIVERSITARIO TELECOMUNICAZIONI)	Italy
CORRELATION SYSTEMS	Ireland
ADS Defence & Security	France
EUROCOPTER ESPANA	Spain
EDISOFT	Portugal
FOI	Sweden
HITT	The Netherlands
INDRA ESPACIO	Spain
INDRA SISTEMAS	Spain
JRC	Europe
MONDECA	France
SAGEM DEFENCE SECURITE	France
SPACE APPLICATIONS SERVICES	Belgium
TELESPAZIO (TPZ)	Italy
THALES ALENIA SPACE FRANCE	France
THALES ALENIA SPACE ITALIA	Italy
THALES DEFENCE DEUTSCHLAND	Germany
TNO	The Netherlands
THALES SYSTEMES AEROPORTES	France
TTI Norte	Spain
UNIVERSITY COLLEGE LONDON	United Kingdom
UNIVERSIDAD DE MURCIA	Spain
UNIVERSITY OF PORTSMOUTH	United Kingdom

SECRICOM / Seamless communication for crisis

© L_PackShot - Fotolia.com

In September 2006 the European Security Research Advisory Board (ESRAB) published a report setting the European security research agenda and the requirements on new communication infrastructures.

These requirements included security, dependability, enhanced connectivity, transmission of multiple formats and advanced search functions.

In response to these ESRAB requirements, the collaborative research project SECRICOM will create and demonstrate a secure communication platform for crisis management in Europe.

Project objectives

Solve problems of contemporary crisis communication infrastructures:

- Seamless and secure interoperability of existing many hundred thousand mobile devices already deployed;
- Smooth, simple, converging interface from systems currently deployed to systems of the new SDR generation;
- Creation of pervasive and trusted communication infrastructure, bring interconnectivity between different networks;
- Provide true collaboration and inter-working of emergency responders; and
- Seamlessly support different user traffic over different communication bearers.

Add new smart functions using distributed IT systems based on an SDR secure agents' infrastructure:

Easier instant information gathering and processing focusing on emergency responders main task – saving lives.

Description of the work

The project work is divided into nine RTD work-packages supported by two work-packages for management and dissemination. Top innovations deal with:

- Creation of secure wireless fault tolerant communication system for mobile devices based on push-to-talk system;
- Secure distributed system; and
- Secure docking module – system on chip design.

These innovations will be extended by:

- IPV6 based secure communication;
- Internetwork interfaces, interoperable, recoverable and extendable network;
- Communication infrastructure monitoring and control centre equipped with localization of actors.

Working infrastructure – the objective of SECRICOM project will be ensured by:

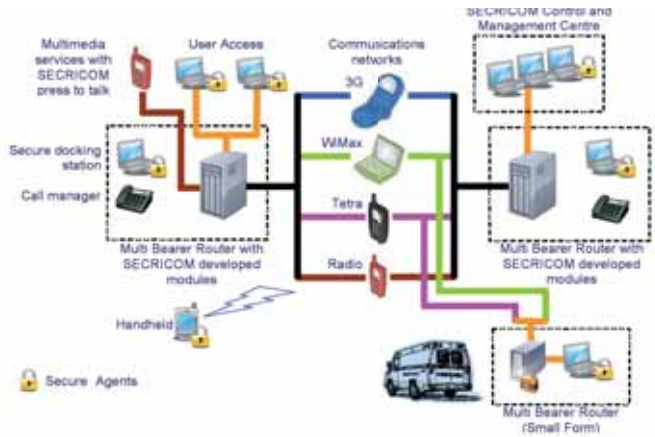
- Integration of research results; and
- Demonstrator creation and presentation.

Expected results

The SECRICOM will develop and demonstrate a secure communications infrastructure for public safety organisations and their users.

Achievements will include:

- The exploitation of existing publicly available communication network infrastructure with interface towards emerging SDR systems.
- Interoperability between heterogeneous secure communication systems.
- A parallel distributed mobile agent-based transaction system for effective procurement.
- Infrastructure based on custom chip-level security.



Information

Acronym :
SECRICOM

Grant Agreement N° :
218123

Total Cost:
€ 12,468,847

EU Contribution:
€ 8,606,791

Starting Date:
01/09/2008

Duration:
44 months

Coordinator :

QINETIQ LTD
Buckingham Gate 85
UK-SW1E 6PD London
United Kingdom

—

Contact :
David Traynor
Tel : +44 (0) 2392 31 2750
Fax : +44 (0) 2392 31 2768
Mobile : +44 (0) 7881846076 / (0) 7590551967
E-mail : dtraynor@qinetiq.com

Website:
http://www.secricom.eu

Partners

NAME	COUNTRY
QinetiQ Ltd	United Kingdom
Ardaco, as.	Slovakia
Bumar Ltd.	Poland
NEXTEL S.A.	Spain
Infineon Technologies AG	Germany
Université du Luxembourg	Luxembourg
Institute of Informatics, Slovak Academy of Sciences	Slovakia
Graz University of Technology	Austria
Smartrends, s.r.o.	Slovakia
ITTI Sp. z o.o.	Poland
British Association of Public Safety Communication Officers	United Kingdom
CEA	France
Hitachi Europe SAS	France

SECTRONIC / Security system for maritime infrastructure, ports and coastal zones

© Fotolia.com

Project objectives

The SECTRONIC initiative addresses observation and protection of critical maritime infrastructures: Passenger and goods transport, Energy supply, and Port infrastructures.

All accessible means of observation (offshore, onshore, air, space) of those infrastructures are networked via an onshore control center.

The end-users themselves or permitted third-parties can access a composite of infrastructure observations in real-time. The end-users will be able to shield the infrastructure by protective means in security-related situations.

The proposed system is a 24h small area surveillance system that is designed to be used on any ship, platform, container/oil/gas terminal or port and harbour infrastructure.

The initiative is an end-users driven R&D activity. The overall objective of the SECTRONIC research project is to develop an integrated system for the ultimate security of maritime infrastructures covering ports, passenger transport and energy supply against being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour.

The project aims to develop an integrated security system that:

» Accurately observes, characterizes and tracks any object of significance, 360 degrees around an infrastructure, 24 h a day in all weather conditions by means of:

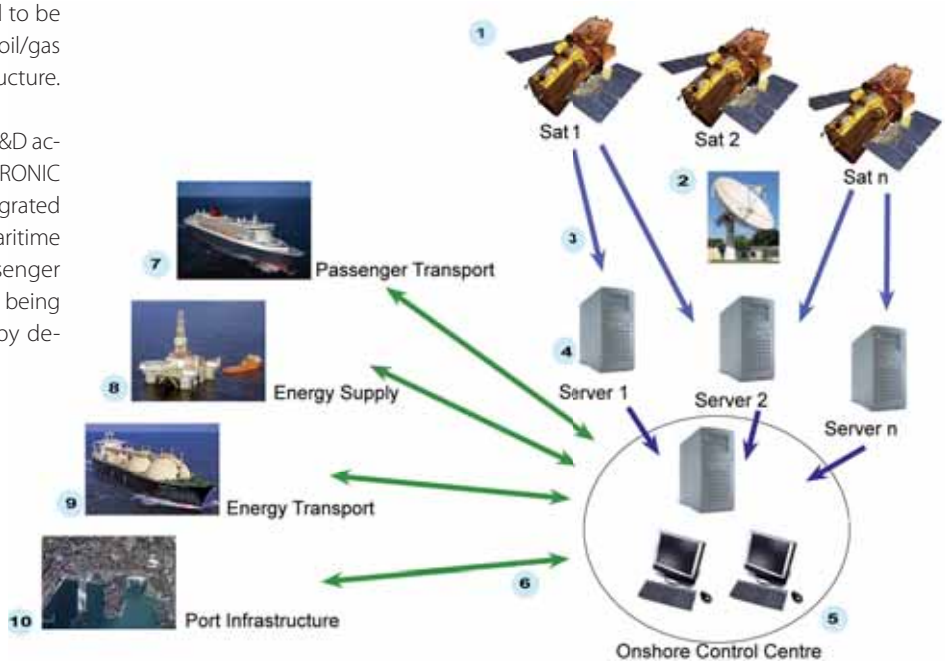
- Near range equipment
- Far range equipment

» Communicates security information of significance to the infrastructure authorities (sea masters, operation control managers, etc.) and to selected authorised third parties of importance for the overall security situation (port authorities, coast guards, etc.) in real time.

» Aggregates, reports and displays any security-related information of significance in an intuitively understandable way. Reliably raises alarms in identified situations.

» Enables response procedures and actions to be undertaken in situations that require effective use of protective measures.

» Demonstrates system effectiveness in real maritime infrastructures.



Information

Acronym:
SECTRONIC

Grant Agreement N°:
218245

Total Cost:
€ 7,080,433

EU Contribution:
€ 4,496,414

Starting Date:
01/02/2008

Duration:
36 months

Coordinator:

MARINE & REMOTE SENSING SOLUTIONS LTD
Suite 100
Saint-James Place 11
UK – SW1A 1NP London
United Kingdom

—

Contact:
Dr. Sverre Dokken
Tel: +44 2078 712 800
E-mail: sdokken@marss.co.uk

Website:
www.sectronic.eu

Partners

NAME	COUNTRY
Marine & Remote Sensing Solutions Ltd	United Kingdom
Uniresearch B.V.	The Netherlands
Det Norske Veritas AS	Norway
Norwegian Defence Research Establishment	Norway
Chalmers University of Technology	Sweden
Advanced Computer Systems ACS S.p.A.	Italy
Nato Undersea Research Centre	Italy
Carnival Corporation.	United Kingdom
BW Offshore AS	Norway
BW Gas ASA	Norway
Havenbedrijf Rotterdam N.V.	The Netherlands
Autorità Portuale della Spezia	Italy

SecureCHAINS / Integration of security technology supply chains and identification of weaknesses and untapped potential

© bisougue - Fotolia.com

Project objectives

The SecureCHAINS project has as a main mission to contribute to a more competitive Security Technology Supply Chains (STSC). The project will cooperate with the industry to gain a better understanding of the nature and structure of the STSC from prime contractors to subcontractors coming from the various tiers of the supply chains.

The SecureCHAINS project will have the following **six main objectives** to:

- identify supply chains and stakeholders;
- detect untapped potential that can be integrated in the European STSC;
- engage innovative low tier suppliers in the STSC;
- contribute to the building of R&D competences in STSC;
- develop awareness building activities in Security related RTD topics; and
- promote and facilitate a communication platform/website and open dialogue in the fields related to Security Technology management, regulation, policy and forecasting.

Description of the work

The SecureCHAINS project will be carried out along the following four main axes of activities:

To identify opportunities and weak spots in the supply chains. The technology tree drawn up for a research project will involve areas of technology of different degrees of maturity. We will apply the concept of 'technology readiness levels ' to determine technical maturity. Immature technology so identified would be considered as a weak spot and the SecureCHAINS project would advise on how this might be strengthened.

- To involve the best intellectual and technological capabilities available throughout Europe in the security technology supply chains.
- To help organisations (SMEs, RTOs, Large Firms, etc.) to understand security related targets, mechanisms and opportunities.
- To facilitate the organisations access to the main stakeholders and integrators, while protecting their intellectual property.

The SecureCHAINS project is structured into 5 workpackages (WP):

- WP1 Security Technology Supply Chains framework setting
- WP2 Analyses of the Supply Chains
- WP3 Increasing SME engagement in the STSC
- WP4 Technology Search & Transfer
- WP5 Dissemination and Future exploitation results and activities

Expected results

The main results are to:

- raise awareness about EU RTD funding programmes and promoting co-operation, exchange of information and networking among them;
- identify weak spots in the security supply chains;
- develop 5 technology trees;
- identify the problems that inhibit the participation of SMEs in RTD activities;
- interview and perform on-site visits to a minimum of 100 SMEs and RTOs;
- organise a minimum of 4 communication exchange fora at European Security related events; and
- produce 10 new RTD project proposals, involving a minimum 20 SMEs.

Information

Acronym:
SecureCHAINS

Grant Agreement N°:
242417

Total Cost:
€ 1,014,344.37

EU Contribution:
€ 820,032

Starting Date:
01/05/2010

Duration:
24 months

Coordinator:

INOVAMAIS SA

—

Contact:
Alexandre Almeida
E-mail: alexandre.almeida@inovamais.pt

Website:
www.securechains.eu

Partners

NAME	COUNTRY
INOVAMAIS - SERVICOS DE CONSULTADORIA EM INOVACAO TECNOLOGICA S.A.	Portugal
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V	Germany
Deutsche Post World Net Market Research and Innovation GmbH (DHL Innovation Center)	Germany
INNOVA SPA	Italy
SOLLERTA Ltd	United Kingdom
FUNDACION ROBOTIKER	Spain
Mr. Juergen K. von der Lippe and Dr. Jean Cornier	Germany
UNIVERSITATEA DIN CRAIOVA	Roumania
ALMA CONSULTING GROUP SAS	France
TECHNICAL SUPPORT FOR EUROPEAN ORGANISATIONS SPRL	Belgium
SOUTHEASTERN EUROPE TELECOMMUNICATIONS & INFORMATICS RESEARCH INSTITUTE	Greece

SecurEau / Security and decontamination of drinking water distribution systems following a deliberate contamination

© Andrey Kiselev - Fotolia.com

Project objectives

The main objective of this proposal is to launch an appropriate response for rapidly restoring the use of the drinking water network after a deliberate contamination and by way of consequence to limit the impact on the population of safe water privation because of contaminated networks. Five main topics will be addressed:

» Detection of unexpected changes in water quality.

» Adaptation of analytical methods to rapidly detect specific CBRN contaminants.

» Localization of the point source (s) of contamination.

» Decontamination procedures of the distribution system.

» Controlling the efficacy of the corrective actions.

Description of the work

SecurEau will implement an effective and timely response on CBRN attack. Questions that will be addressed for successful coordinated response of water utilities and regulatory agencies to contamination include:

» Detection of unexpected changes in water quality which could be in relation with a deliberate contamination event, by applying commercially available or recently developed generic sensors placed throughout the distribution systems.

» Adaptation of known analytical methods to rapidly detect specific CBRN contaminants in water and especially in biofilms and on pipes' walls.

» Localization of the point source(s) of contamination and subsequently the contaminated area (via modelling reactive transport) allowing delimitation of the corrective actions.

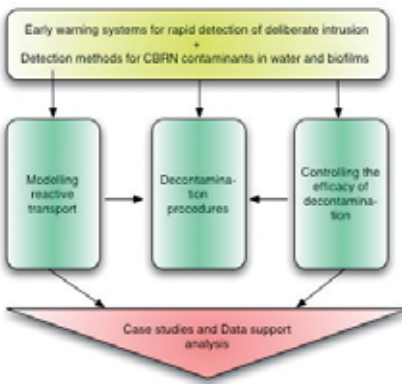
» Decontamination procedures (efficient and realistic) of the distribution system, i.e. adapted to size, age, architecture of the network, including the treatment of water extracted from the system and used for washing the pipe wall.

» Controlling the efficacy of the corrective actions by analysing the water bulk and especially the pipe walls' surface and the deposits.

» The case studies will give the chance for the practitioners to apply on site in realistic conditions the selected sensors, software and remediation technologies. It is a unique occasion to test an emergency procedure on a complicated, quasi directly inaccessible and relatively fragile system, to evaluate its feasibility at field scale and to evaluate the difficulty to apply corrective treatments to the huge water bulk generated by the neutralisation/extraction of contaminants.

Expected results

As a result of this research and methodological effort the consortium plans to develop and validate adapted technologies, analytical tools, sensors and new software, which should reinforce the competitiveness of European Union. These tools and technologies are planned to give results quickly at affordable costs. Case studies will give the chance for the practitioners to apply on site in real conditions the selected sensors, software and remediation technologies.



Information

Acronym:
SecurEau

Grant Agreement N°:
217976

Total Cost:
€ 7,462,072

EU Contribution:
€ 5,269,168

Starting Date:
01/02/2009

Duration:
48 months

Coordinator:

UNIVERSITÉ HENRI POINCARÉ-NANCY 1
Service des Relations Internationales, Cellule Europe
22-30 rue Lionnois
BP 60120
France – 54003 – Nancy cedex

—

Contact:
Dr. Sylvain FASS
Tel : +33 3 54 50 54 37
Fax : +33 3 54 50 54 30
E-mail : sylvain.fass@uhp-nancy.fr

Website:
www.secureau.eu

Partners

NAME	COUNTRY
Université Henri Poincaré - Nancy 1	France
Centre National de la Recherche Scientifique	France
Anjour Recherche / Veolia Environnement	France
Rheinisch-Westfälische Institut für Wasserforschung gemmeinnützige GmbH	Germany
University of Southampton	United Kingdom
National Public Health Institute	Finland
Faculdade de Engenharia da Universidade do Porto	Portugal
Riga Technical University	Latvia
Centre National du machinisme Agricole, du génie rural, des eaux et des forêts	France
Monitoring System Limited	United Kingdom
CEA	France
Veolia Water Central	United KIngdom
Yorkshire Water Sevice Ltd	United Kingdom
STUK-Radiation and nuclear Safety Authority	Finland

SECURENV / Assessment of environmental accidents from a security perspective

© Surrender - Fotolia.com

Project objectives

Environmental security is becoming an important issue for the future development of the European Union. New future threats and the potential consequences of these are becoming more and more difficult to anticipate.

Industrial accidents and natural disasters have repeatedly shown how sensitive the environment is to human negligence. Despite all efforts and advances in security and civil protection, the human habitat remains most vulnerable. The overall objective of the project is to increase the knowledge- base needed to ensure the security of the natural environment.

The project will analyse major industrial and environmental accidents from a security perspective using foresight methods and scenario building techniques to give end-users a better understanding of future environmental risks.

Natural phenomena (fires, floods, etc.), industrial accidents (chemical, biological and other) and other possible threats in a broad perspective will be investigated.

Description of the work

Given the strong uncertainty aspect of the environmental security domain, foresight methods and scenario- building techniques will be employed to a large extent during the implementation of the project. Work will include:

- The review and analysis of past environmental accidents, catastrophes and effects of human actions.
- The establishment of data-bases with relevant information for end-users.
- The identification of novel and emerging threats on the environment as well as the technological opportunities.
- The development of an appropriate foresight methodology and potential scenarios involving future environmental risks and its use for investigating policy options.

Expected results

The project will support the development of policies, programmes and initiatives which aim at further enhancing the security of European citizens. It will provide improved insight and advice for security policy makers, security research programme managers and security researchers.

The project will also contribute to the definition of strategic roadmap for future FP7 Security research and in planning and designing of other future security research programmes and actions.

Information

Acronym:
SECURENV

Grant Agreement N°:
218152

Total Cost:
€ 851,245

EU Contribution:
€ 851,245

Starting Date:
01/04/2009

Duration:
24 months

Coordinator:

GEONARDO ENVIRONMENTAL TECHNOLOGIES LTD.
Záhony utca, 7
Budapest - 1031
Hungary

—

Contact:
Mr. Balázs Bodó
Tel: +36-1-250-6703
Mobile: +36-20-317-2087
Fax: +36-1-436-9038
E-mail: coordinator@securenv.eu

Website:
www.securenv.eu

Partners

NAME	COUNTRY
Geonardo Environmental Technologies Ltd.	Hungary
FOI	Sweden
Adelphi Research gGmbH	Germany

SEREN / Security Research NCP network – Phase 1

© Andres Rodriguez - Fotolia.com

Project objectives

Security Research presents several specificities as compared to other Cooperation's FP7 thematic priorities. Indeed, it is a new theme within FP7 and therefore the Security Research community has only a limited experience gained during the 3 years of the Preparatory Action for Security Research.

Moreover, projects need to be mission-oriented and as such must involve end-users who are not familiar with FP.

Also, the Security products' market is complex, large, and relatively new. Finally, by its very nature, the Security research theme has introduced sensitivity issues into the 7th Framework Programme.

As a consequence, perhaps more than in the other specific programmes and themes, there is a strong necessity to inform and support the European Security Research community in its participation to FP7. One way to facilitate this is through a stronger National Contact Points (NCPs) network.

SEREN will thus aim at strengthening the Security research NCP network by raising the knowledge level of its members, initiate coordination and, as a matter of fact, the ability of its members to deliver a high level of service to the community.

Description of the work

The aim of the SEREN-phase 1 coordination action is to link the different Security Research NCPs, to identify fields of improvement for the structuring of the network, to initiate coordination and to start promoting joint activities. In order to reach those objectives, SEREN will tackle four main issues:

Identification of the network needs and initiation of coordination among its members.
This will be mainly obtained through surveys in order to gain a better understanding of the needs of the Security Research community and of the requirements that NCPs must fulfil in order to deliver a high level of service. Also, coordination will be initiated in order to raise the level of knowledge of NCPs. This will be obtained by making common guides and setting up a website where all the deliverables will be made available.

Increase NCP knowledge and awareness of the European Security landscape.
In order to deliver advices in their respective country, NCPs must have a minimum understanding of the European security landscape. Therefore, a mapping of the Security research programmes launched in Member States will be made. In addition, a mapping of competencies will be initiated. This latter task will aim at the identification of support structures such as government agencies, professional associations, end-users associations, SMEs associations, clusters involved in Security Research across Europe.

Coordination to ease transnational cooperation and training.
The EU community potentially interested in Security Research faces a high level of fragmentation. Therefore, participants are confronted with difficulties finding other potential partners with whom they might collaborate. Hence, it is extremely important that the NCPs network delivers a high level service for the partner searches.

SEREN will initiate coordination in this field by agreeing on standardised partner search templates. In addition one training session focussed on the evaluation will be organised.

This shall enable an increase of the average advice quality delivered by the network and further optimize its services to the Security Research community.

Security research policies.
SEREN will produce synthesis papers on key policies issues related to Security research in order to raise awareness on the contextual framework surrounding ESRP.

Expected results

Thanks to SEREN, the Security research NCPs network will become more efficient and coordinated and therefore will deliver a higher level of service throughout Member and Associated States. As an efficient interface between the European Commission and the Security Research community, SEREN will improve the overall promotion of the FP7 Security theme, and of its specificities and its procedures. As a result, the average quality of proposals submitted to call for proposals should increase.

Information

Acronym:
SEREN

Grant Agreement N°:
217937

Total Cost:
€ 743,597

EU Contribution:
€ 557,692

Starting Date:
01/02/2008

Duration:
18 months

Coordinator:

COMMISSARIAT À L'ENERGIE ATOMIQUE
European Affairs Directorate
91191 Gif-sur-Yvette
France

—

Contact:
Frédéric Laurent
Tel: +33 1 64 50 25 22
Fax: +33 1 64 50 11 57
E-mail: pcn_securite@cea.fr

Website:
www.seren-project.eu/

Partners

NAME	COUNTRY
CEA	France
Tarptautiniu mokslo ir technologiju pletros programu agentura	Lithuania
Achimedes Foundation	Estonia
Foundation For Research & Technology – Hellas	Greece
National Office for Research and Technology	Hungary
Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk	Poland
Matimop, Israel Industry Center For Research & Development	Israel
Agenzia per la Promozione della Ricerca Europea	Italy
Romanian Space Agency	Romania
Norges forskningsråd	Norway
The Scientific and Technological Research Council of Turkey	Turkey
Service d'information scientifique et technique / SPP Politique scientifique – Dienst voor Wetenschappelijke en Technische Informatie/POD Wetenschapsbeleid	Belgium
Österreichische Forschungsförderungsgesellschaft mbH	Austria
Agência de Inovação, Inovação Empresarial e Transferência de Tecnologia, S.A	Portugal
Centro para el Desarrollo Tecnologico Industrial	Spain
SenterNovem	The Netherlands
Technologické centrum	Czech Republic
Research Promotion Foundation	Cyprus
FOI	Sweden
Euresearch	Switzerland
Council for Scientific and Industrial Research	South Africa
Riga Technical University	Latvia
Centre for National Security and Defense Research	Bulgaria
Malta Council for Science and Technology	Malta
Home Office	United Kingdom
Luxinnovation GIE	Luxembourg
Danish Agency for Science Technology and Innovation -Ministry of Science, Technology and Innovation	Denmark
Agentura na podporu vyskumu a vyvoja	Slovakia

SeRoN / Security of road transport networks

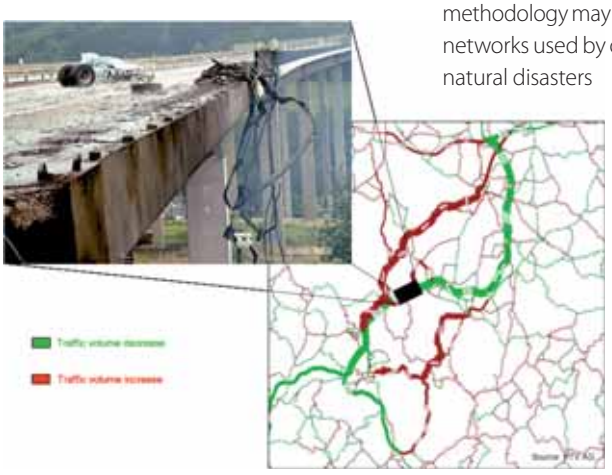
© Frog 974- Fotolia.com

Project objectives

The SeRoN project undertakes a holistic approach both at infrastructure object and road network level. Its main objectives are to investigate the impacts of possible man-made attacks on the transport network, in particular the resulting regional and supra-regional impacts on transport links and their economic impacts. SeRoN focuses on the development and validation of an innovative methodology which is to provide a common framework for the analysis of critical road infrastructure objects or road transport networks with regard to their importance within the European transport network and regard to possible attacks. This methodology is based on an interdisciplinary interaction of expertise and innovative simulation methods. Furthermore, possible protection measures for critical road transport infrastructures can suitably be chosen and evaluated regarding their impact on security and cost-effectiveness.

Description of the work

First a comprehensive threat analysis for transport infrastructures focusing on man-made attacks is carried out. Then data on relevant infrastructure types and classes of the Trans-European road network is gathered, with so-called "partner regions" being more comprehensively covered. Data provided will be evaluated to identify generic infrastructure types and classes which are critical in terms of vulnerability to man-made attacks, e.g. due to their type of construction, and to classify them based on the risk they are exposed to. The results provide the input data for a knowledge database intended to be a means to manage and maintain categorised critical infrastructures and associated protection measures. Such object information is needed for the calculations at network level analysing the importance of individual infrastructures. Their vulnerability will be determined in probable scenarios, studying the impacts of a failure of critical (parts of) infrastructures and the resulting traffic disturbances using scenario analysis and macroscopic traffic flow models. Network data will include information about location and importance of infrastructures in the road network, traffic loads, etc. Thus critical infrastructures of the road network can be identified and ranked according to priority. The risk assessment includes the impact assessment for the respective infrastructure based on different occurrence scenarios with related event sequences. Vulnerabilities are estimated using the local traffic conditions and simulations, e.g. escape simulations, explosives and smoke propagation simulations. Security improvements will be determined and monetary and economic impacts of different measures examined by means of cost-benefit analyses to identify the most effective security measures. Finally at few suitable examples the new developed methodology will be validated before recommendations for infrastructure owners will be formulated taking into account external expert knowledge gained in workshops.



Expected results

The SeRoN results include a knowledge database, an innovative methodology and recommendations covering macro-economic, institutional and organisational and technical issues. They will allow infrastructure owners and operators developing strategies to improve the security of transport structures and to select investments into countermeasures and risk mitigation strategies. The developed methodology may be transferred to transport networks used by other traffic modes and to natural disasters

Information

Acronym:
SeRoN

Grant Agreement N°:
225354

Total Cost:
€ 2,942,113

EU Contribution:
€ 2,246,110

Starting Date:
01/11/2009

Duration:
36 months

Coordinator:

PLANUNG TRANSPORT VERKEHR AG
Dr. Georg Mayer

Contact:
Dr. Georg Mayer
Planung Transport Verkehr AG
Kriegerstr. 15
D-70191 Stuttgart
Germany
georg.mayer@ptv.de

Dr. Christoph Walther
Planung Transport Verkehr AG
Stumpfstr. 1
D-76131 Karlsruhe
Germany
christoph.walther@ptv.de
www.ptv.de

Website:
www.seron-project.eu

Partners

NAME	COUNTRY
PTV Planung Transport Verkehr AG	Germany
Bundesanstalt für Straßenwesen (BASt)	Germany
Parsons Brinckerhoff	United Kingdom
Technische Universität Graz	Austria
Traficon n.v	Belgium
Ernst Basler und Partner	Switzerland
NIRAS A/S	Denmark

SGL for USaR / Second generation locator for urban search and rescue operations

© puck - Fotolia.com

SGL for USaR is mission oriented towards solving critical problems following large scale structural collapses in urban locations. The devotion, courage and expertise of rescuers need to be matched by procedures and technology that will enable safe and effective responses.

This project will combine chemical and physical sensors integration with the development of an open ICT platform for addressing mobility and time-critical requirements of USaR Operations. The project will also focus on medical issues and on the relevant ethical dilemmas.

Project objectives

» To use video images (image analysis), sound (sound signatures), field chemical analysis (marker compounds), optical sensors (spectral analysis), data fusion and wireless communication in order to develop integrated, stand-alone early location devices for entrapped people and dead bodies. Employ the same kind of devices for monitoring and identifying hazardous conditions in voids of collapsed buildings due to construction's physical damage, flaming or smoldering fires and gases released.

» To develop integrated remote early location and monitoring systems for localization purposes based on the deployment of networks of probes. Such systems will also be capable of receiving other type of data (e.g. sonar).

» To integrate early location and monitoring systems with communication and information management applications that can provide with multi-level processing and data fusion and will support relevant USaR services and logistics (medical support, mobilization, tools, transportations, communications) SGL for USaR project will use multidisciplinary approaches, optimize existing cutting-edge technologies and make the best use of available resources.

The project is targeted on delivering next generation systems for USaR operations.

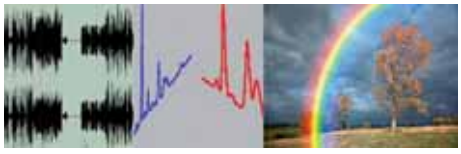
For that purpose, relevant technical, scientific and operational issues will be addressed.

The project focuses on rapid location of entrapped or buried victims (alive or deceased) and the continuous monitoring of the air conditions in the voids of damaged and partially collapsed structures. Entrapped people and voids are associated with characteristic visual, sound and chemical profiles, due to specific images or spectral emissions, to acoustic signatures and chemical markers.

The adaptation of crisis management USaR services (logistics) with the early location and monitoring systems in a mobile command and control operational center is employed.

The project is formed by eight sub-projects (work packages) running in parallel. These WPs address the development of simulation environments; the development and validation of portable devices for location operations; the development and validation of smart sensors environment for monitoring the situation under the ruins; the management of medical information, including privacy and bioethics; and finally the development of an ICT platform that will integrate all the previous data, ensure interoperability and control the flow of the information from the field to the operational center.

SGL for USaR will deliver methods and guidelines, as well as, tangible prototypes: a standalone FIRST responder device that integrates five different location methods; a networked rapid casualty location system (REDS) equipped with wireless sensor probes; an advanced environmental simulator for training and testing search and rescue units, including canine teams; and a prototype mobile operational command and control platform.



Information

Acronym:
SGL for USaR

Grant Agreement N°:
217967

Total Cost:
€ 6,217,478

EU Contribution:
€ 4,859,026

Starting Date:
01/10/2008

Duration:
48 months

Coordinator:

NATIONAL TECHNICAL UNIVERSITY OF ATHENS
Heroon Polytechneiou
15780 Zographou
Greece

—

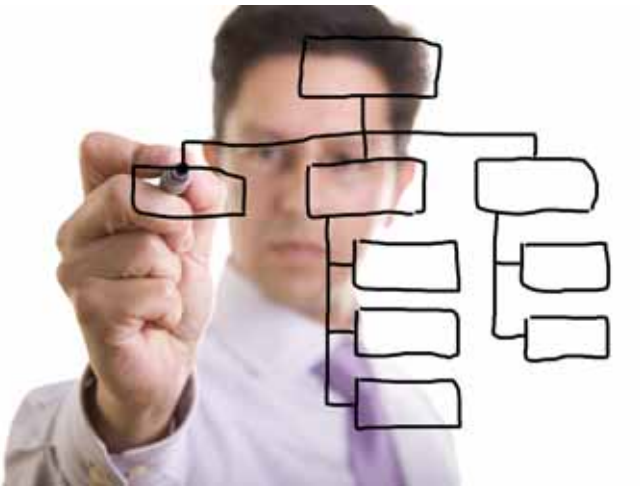
Contact:
Milt Statheropoulos
Tel: + 30 210 7723109
Fax: + 30 210 7723188
E-mail: stathero@chemeng.ntua.gr

Website:
www.sgl-eu.org

Partners

NAME	COUNTRY
National Technical University of Athens	Greece
Service Départemental d'Incendie et de Secours du Vaucluse	France
Direccio General De Prevencio I Extincio D'incendis I Salvaments	Spain
FAENZI s.r.l.	Italy
Valtion Teknillinen Tutkimuskeskus	Finland
Gesellschaft zur Förderung der Analytischen Wissenschaften e.V.	Germany
ECOMED bvba	Belgium
Environics Oy	Finland
Austrian Academy of Sciences	Austria
Entente Interdépartementale en vue de la Protection de l'Environnement et de la Foret contre l'Incendie	France
ANCO S.A. Agencies, Commerce & Industry	Greece
University of Dortmund	Germany
TEMAI Ingenieros S.L.	Spain
G.A.S. Gesellschaft für analytische Sensorsysteme mbH	Germany
Universidad Politecnica de Madrid	Spain
Savox Communications Ltd	Finland
University of Athens	Greece
Markes International ltd	United Kingdom
Bay Zoltan Foundation for Applied Research	Hungary
Critical Links SA	Portugal
The University of Loughborough	United Kingdom

SICMA / Simulation of crisis management activities



© Helder Almeida - Fotolia.com

Project objectives

The SICMA project is a 30 months capability project focused on computer assisted decision making for Health Service crisis managers. It aims at improving decision-making capabilities through an integrated suite of modelling and analysis tools providing insights into the collective behaviour of the whole organisation in response to crisis scenarios.

Mission

The response to the crisis is the result of the activities of:

- Different services (e.g. police, medical care, rescue forces, fire fighting, etc);
- interacting vertically (i.e. with components of the same organization) and horizontally (i.e. with components of other organizations);
- in a complex environment characterized by both "predictable" factors (e.g. the crisis responders' behaviour according to procedures) and "unpredictable" ones (e.g. human/crowd behaviour).

As a consequence, the decision making process both in the preparedness and in the response phase is hard and complex due to the impossibility to estimate the effects of alternative decisions. Within this context, decision making support will be provided addressing the following key aspects:

- "bottom-up" modelling approach building independent model components and then combining them,
- unpredictable factors modelling (e.g. human/crowd behaviour),
- procedure support to provide the user with the correct procedures to solve the problem, and
- computation of the "distribution" of the effectiveness of a certain "decision" rather than the effectiveness of that solution deterministically dependant on the preconceived scenario.

The combined effects of the above points will allow to document both the unexpected bad and good things in the organization(s) thus leading to better responses, fewer unintended consequences and greater consensus on important decisions.

Application scenarios

The following scenarios have been selected:

- Conventional weapons terrorist attack: being the most common and hence the most likely threat in the future, this scenario will be used to evaluate the decision support achievable with the SICMA prototype in the management of casualties. The focus will be on the management of the most likely category of casualties that can be generated by a large number of different types of disasters that is: trauma casualties.
- Chemical weapons terrorist attack: specific types of disasters may result in additional decision making activities to be carried out by the crisis manager. This scenario will be used to highlight the additional support that can be provided to decision making activities specifically related to the kind of accident. The decontamination-station deployment and hazard estimate/update will be used as case study in the chemical attack Scenario.

High level architecture

Even if the high level system design will be defined in the next phase of the project, the presence of the following macro-components is foreseeable:

- Services Models,
- Context Models,
- Effectiveness Distribution Analyser, and
- Procedure Support.

Current achievement

The project has been divided into four phases: User Requirement Analysis, High Level System Design, Prototype Development, Case Study Implementation. At the end of the first phase system scenarios, user requirements and system requirements have been defined.

Expected results

SICMA will deliver a "shoe box" Demonstrator (prototype) comprising the modeling and analysis tools able to prove, on a case-study scenario the need, feasibility, relevance and efficiency of the proposed approach.

Information

Acronym:
SICMA

Grant Agreement N°:
217855

Total Cost:
€ 3,902,580

EC Contribution:
€ 2,566,330

Starting Date:
01/03/2008

Duration:
30 months

Coordinator:

ELSAG DATAMAT SPA
2 Via G. Puccini
IT-16154 Genova
Italy

—

Contact:
Giuseppe La Posta
Tel.: +39 06 5027 2612
Fax: +39 06 5027 2250
E-mail: giuseppe.laposta@elsagdatamat.com

Daniele Cecchi
Tel: +39 06 5027 4629
Fax: +39 06 5027 2250
E-mail: daniele.cecchi@elsagdatamat.com

Website:
www.sicmaproject.eu

Partners

NAME	COUNTRY
Elsag Datamat SPA	Italy
ITTI Ltd	Poland
Consiglio Nazionale delle Ricerche	Italy
SKYTEK Ltd	Ireland
Industrieanlagen Betriebsgesellschaft mbH	Germany
Elbit Systems Ltd	Israel
Centre for European Security Strategies	Germany
IFAD TS A/S	Denmark
Universita' Cattolica del Sacro Cuore Milano	Italy

STAR-TRANS / Strategic risk assessment and contingency planning in interconnected transport networks

© Jean-Paul Bounine - Fotolia.com

Project objectives

The fundamental assumption within STAR-TRANS is that transportation assets, such as airplanes and tunnels, are integral part of larger systems. Taken together, individual transportation networks form a "network of networks". This provides a basis for an integrated EU-wide approach to risk management in transportation networks that would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States.

STAR-TRANS' contribution to the risk assessment process in transportation networks is the recognition of the importance that the impact of a risk incident might have on the assets of the whole 'network of networks'.

The project outcome will offer important aids for decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences, (cost, timing, resources, etc) of proposed actions.

A specialised software system will be developed that will support the end users, and network operators needs.

The objectives of the STAR-TRANS project are:

To produce a security risk assessment framework for European interconnected and interdependent transportation networks and to evaluate the proposed risk assessment framework in two cities.

Description of the work

The aim of proposed transportation security risk assessment framework is to formalise the linkage between risk incidents, transportation network assets and dependency types between assets in order to assess the impact of an incident on the affected interconnected and interdependent networks at the 'network of networks' level. In particular, STAR-TRANS intends to:

- formalise the impact assessment process at the 'network of networks' level;
- develop ICT tools that support the formalised impact assessment process; and
- trial & evaluate the developed impact assessment process and tools.

The STAR-TRANS' comprehensive risk assessment approach targets at the security operation of the European transport networks. STAR-TRANS' will be guided by a holistic risk assessment methodology for critical infrastructure for the analysis and assessment of common issues for risks, threats and vulnerabilities.

Within the STAR-TRANS' framework, security risk in the integrated transportation networks will be defined as the combination of:

1. *Vulnerability*, reflecting the possibility of a risk incident, e.g. terrorist attack, to the interdependent and interconnected European transport networks, compared to the possibility of protecting it through inherent or managed safeguards.
2. *Consequences* of a successful attack, which is defined using (i) the possible number of causalities / fatalities, (ii) disruption and recovery time and (iii) the economic impact.

The combined approach of various transport networks in one risk assessment tool will allow for easy information exchange between different networks and infrastructure elements / facilities.

Expected results

It aims to develop and apply system analysis methods to assess the risk, vulnerability, safety and security elements of complex systems and critical infrastructures supporting road, and inter-modal transport. Emphasis is given on the study and development of open service-oriented architecture and software standards to support risk management and contingency planning.

The proposed STAR-TRANS actions in the area of transportation security will provide the technology basis and relevant knowledge for security capabilities needed in this area, while achieving a significant improvement with respect to performance, reliability, speed and cost and will reinforce the European industry's potential to create important market opportunities.

Information

Acronym:
STAR-TRANS

Grant Agreement N°:
225594

Total Cost:
€ 3,195,188.88

EU Contribution:
€ 2,105,588.94

Starting Date:
01/11/2010

Duration:
30 months

Coordinator:

INTRASOFT INTERNATIONAL S.A.
2 Via G. Puccini
IT-16154 Genova
Italy

—

Contact:
Dr. Antonios Ramfos
E-mail: antonis.ramfos@intrasoft-intl.com

Website:
www.startrans-project.eu

Partners

NAME	COUNTRY
INTRASOFT International SA	Luxembourg
National Centre for Scientific Research Demokritos - Environmental Research Laboratory	Greece
Center for Security Studies	Greece
Confederation of Organisations in Road Transport Enforcement	Belgium
QinetiQ SA	United Kingdom
Fraunhofer Institute for Transportation and Infrastructure Systems	Germany
Centre for Research and Technology Hellas - Informatics & Telematics Institute	Greece
Metropolitan Police Service	United Kingdom
CTL Cyprus Transport Logistics Ltd	Cyprus
SQUARIS Ltd	Belgium

STRAW / Security technology active watch

© Nmedia - Fotolia.com

Project objectives

Europe is confronted with extremely diverse threats backed by unseen command structures and business-like financing mechanisms. Various security agencies concur that information is the key to defeating the enemy. This new environment has not only created a greater need for information but also a greater need to share and effectively control access to that information. This is the single greatest challenge European Security is facing today. STRAW is a Coordination and Support Action under the Security Research Theme that aims at providing a European Service of Technology Watch (TW) on Security Technologies.

The mission of STRAW is not only advicing potencial end-users (public authorities, EU security research community and public at large) about the fundamental technologies but also bring together the defense and security research industry for developing new civil applications.

A main output will be a web-based IT system with a TW list and interface for entering data on user requirements.

Description of the work

Several key milestones are specified to achieve this objective:

» Network and panel of experts constitution: The Consortium will identify the foremost representatives of the Security Sector mainly in Europe. Some of them will be invited to participate in a panel of experts to validate the results of the project. The STRAW network will be growing during the whole project.

» Information Collection: A main task will be the collection of relevant information related to security technologies, stakeholders and initiatives. Members of the network are requested to insert in STRAW any documentation that they consider to be interesting for analysis in STRAW website.

» Information Analysis: In collaboration with the panel of experts, partners will analyze the collected information by means of TW tools in order to present clear snapshot of the relevant security threats and opportunities existing on security.

One of the main outputs will be to release a reviewed taxonomy on Security (based mostly on STACCATO) linked with a Data Base with information of providers, users and technologies.

» Wikibook construction: A wikibook will be developed to present the results of STRAW. The interactive element of the Wikibook will ensure the relevance of the project's results beyond its duration.

» Delivery of information: The project's main results will be delivered to the potential users of the information primarily through the STRAW web page and workshops.

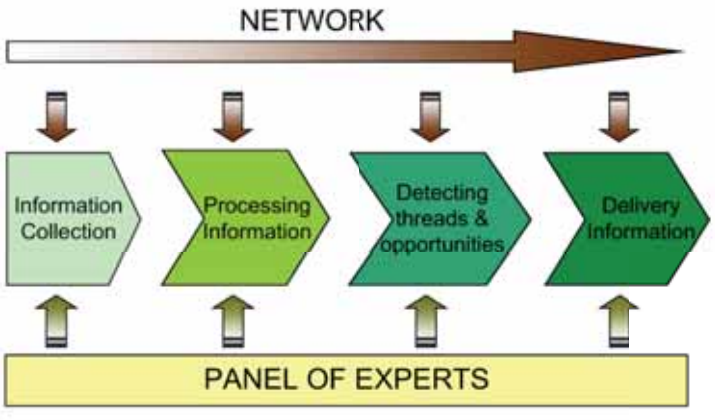
Expected results

Apart from direct results, the following events took place:

» Italian Workshop: This workshop was organized by Fondazione Rosselli in 2009;

» Spanish Workshop: The Instituto Nacional de Técnica Aeroespacial (INTA) was in charge of organizing the workshop in March 2010.

For more information, please visit our website.



Information

Acronym :
STRAW

Grant Agreement N° :
218132

Total Cost :
€ 1,341,933

EU Contribution :
€ 998,537

Starting Date :
01/10/2008

Duration :
18 months

Coordinator :

ATOS ORIGIN SAE
Atos Research & Innovation
Albarracín, 25.
28037 Madrid
Spain

—

Contact :
Aljosa Pasic
Tel : +34 91 214 88 00
Fax : +34 91 754 32 52
E-mail : aljosa.pasic@atosresearch.eu

Website :
www.straw-project.eu

Partners

NAME	COUNTRY
Atos Origin SAE	Spain
Aerospace and Defence Industries Association	Belgium
Thales Services	France
Sitftelsen SINTEF	Norway
Fraunhofer FHG	Germany
Instituto Nacional de Técnica Aeroespacial	Spain
Elsag Datamat S.p.A.	Italy
Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España	Spain
Fondazione Rosselli	Italy
European Organisation for Security	Belgium

SUBITO / surveillance of unattended baggage and the identification and tracking of the owner

© Artsem Martysiuk - Fotolia.com

Project objectives

SUBITO will research and develop automated detection of abandoned luggage, fast identification of the individual responsible and the tracking of their subsequent path.

The consortium, a diverse group of technology and implementation experts from across the EU, will develop an integrated threat detection system that provides a robust, timely alert to security personnel. Working closely with the end users, the team will design a system that is capable of distinguishing between genuine threats and false alarms in order to alert the user to high priority situations.

Key objectives are:

- Find abandoned luggage and identify and track the owner.
- Reduce the number and impact of false alarms.
- Demonstrate automated detection of abandoned goods, fast identification of individual who left them and fast determination of the individual's location or their path.
- Demonstrate a scalable route to implementation.
- Examine the wider user of technologies for explosive threat identification in this context.
- Examine the use of camera technologies to distinguish between threatening and non-threatening goods, and
- Manage public perception of this technology and its implications.

Description of the work

In recent years, there has been a number of incidents where terror organisations have planted explosive devices in ordinary baggage to cause immense disruption in mass transportation networks and other areas of critical infrastructure.

The threat of unattended baggage has led to increased vigilance amongst security personnel and the general public to ensure that unattended baggage is reported and investigated with utmost urgency. In conjunction with the introduction of enhanced CCTV, this has enabled an increase in the breadth and scope of data that can be collected at key locations. Unfortunately, this has not been matched by a corresponding improvement in the capabilities of systems to interpret and filter the data. This has remained the duty of trained human operators who often do not have the capacity to process the breadth of data that is received.

Consequently, the increase in data availability has been met by an increase in the number of false alarms; situations where unattended baggage has been incorrectly considered a potential threat. Often, due to the pressure to act quickly, the situational data is only analysed once a major event has occurred. This has resulted in unnecessary disruption to business operations, with associated cost implications and a lack of confidence regarding security procedures and equipment.

Building upon existing surveillance technology, the SUBITO programme will deliver a demonstration of semi-automated data processing designed to provide real-time detection of goods that have been abandoned. At the same time, the system will identify the individual who left the goods and will utilise the surveillance network to determine the current location of that individual and track their followed path. SUBITO will improve the efficiency of security personnel by automatically filtering out the major false alarms and therefore focusing their attention only on credible threats.

Expected results

With the help of our end user partners, SUBITO will demonstrate that a solution to this problem is achievable using existing infrastructure and security technologies from real locations operating under standard procedures.

SUBITO aims to deliver a generic approach that can be also applied to solve similar problems in more diverse applications. In addition the programme will carry out supporting studies investigating the benefits of incorporating additional sensors and controllable cameras to the system.

© illushooti - Fotolia.com

Information

Acronym :
SUBITO

Grant Agreement N° :
218004

Total Cost :
€ 3,895,730

EU Contribution :
€ 2,581,055

Starting Date :
01/01/2009

Duration :
31 months

Coordinator :

SELEX SENSORS AND AIRBORNE SYSTEMS LIMITED
2 Crewe Road North
Edinburgh - EH5 2XS
Scotland
United Kingdom

—

Contact :
Ms Georgette Murray
Mark Riddell
Tel : +44(0)131 343 5992
Fax : +44(0)131 343 8110
E-mail : mark.riddell@selexgalileo.com

Website:
www.subito-project.eu

Partners

NAME	COUNTRY
SELEX Sensors and Airborne Systems Limited	United Kingdom
ELSAG DATAMAT S.p.A	Italy
Office National d'Etudes et de Recherches Aérospatiales	France
L-1 Identity Solutions AG	Germany
CEA	France
University of Leeds	United Kingdom
University of Reading	United Kingdom
VTT	Finland
Österreichesches Forschungs und Prufzentrum Arsenal Ges.m.bH	Austria
Fiera di Genova S.p.A	Italy

SUPPORT / Security upgrade for ports

© Herbert Rubens - Fotolia.com

Project objectives

SUPPORT aims to raise the current level of port security by integrating legacy port systems with new surveillance and information management systems. SUPPORT will provide the necessary and sufficient security level to satisfy evolving international regulations and standards while efficiently supporting the complexity of the real port environment. As part of this, SUPPORT will also facilitate efficient and, where required, real-time exchange of security related information within the supply chain and between ports and authorities.

One aim of SUPPORT is to provide general methods and technology supported by training services that can be used by any European port to efficiently enhance its security level.

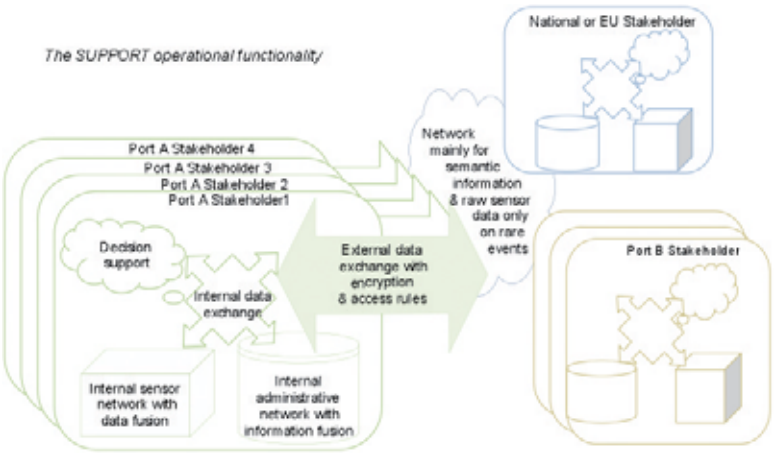
Description of the work

SUPPORT partners include a number of ports that have been selected to represent typical, but different operations. Starting from the perspective of the partner port operations, the project will use a cost-benefit method to identify the main security gaps and will describe security measures to maintain or augment the efficient and secure operation of these ports. The approach will combine creative and analytical techniques to identify as many relevant threats as possible.

After making an inventory of security gaps these will be developed into generic port security models. The models will be used to suggest security upgrade solutions, taking into account the cost-benefit factors of the available technology.

Expected results

Peer-to-peer communication and decision support tools incorporating semantic technologies will be developed, using as far as possible standard open architecture software, accessible to all the port security stakeholders. The results will be demonstrated at the ports of Gothenburg and Piraeus. SUPPORT will include policy and standardisation proposals and training for participating port personnel as well as dissemination activities for other ports and stakeholders.



Information

Acronym:
SUPPORT

Grant Agreement N°:
242112

Total Cost:
€ 14,629,279.69

EU Contribution:
€ 9,920,607

Starting Date:
01/07/2010

Duration:
48 months

Coordinator:

BMT GROUP LIMITED
Goodrich House
Waldegrave Road 1
Teddington TW11 8LZ Middlesex
United Kingdom

—

Contact:
Mr Fernando Caldeira-Saraiva
Tel:+442086144244
Fax:+442089779304
E-mail: fernando@bmtmail.com

Website:
http://www.supportproject.info

Partners

NAME	COUNTRY
BMT Group Limited	United Kingdom
FOI	Sweden
Securitas AB	Sweden
Valtion Teknillinen Tutkimuskeskus	Finland
Marlo A.S	Norway
Inlecom Systems Ltd	United Kingdom
Norsk Marinteknisk Forskningsinstitutt A/S	Norway
Nautical Enterprise Centre Ltd	Ireland
Stena Line Scandinavia AB	Sweden
Ebos Technologies Ltd	Cyprus
Universität Innsbruck	Austria
Cargotec Oyj	Finland
Valsts Akciju Sabiedriba Latvijas Juras Administracija	Latvia
Institut national de recherche en informatique et en automatique	France
Marac Electronics, SA	Greece
Piraeus Port Authority SA	Greece
Gemeente Amsterdam	The Netherlands
Europhar GEIE-AEIE	Spain
Stichting Ecoports	The Netherlands

TALOS / Transportable autonomous patrol for land border surveillance system

© TALOS

TALOS is an innovative, Adaptable Land Border Large Area Surveillance System based on transportable surveillance integrated with fast deployable mobile unmanned ground and air vehicles which will address new challenges of external land borders of the enlarged European Union.

Project objectives

TALOS project proposes to develop an integrated, adaptable land and large area (including devastated environment) surveillance system that:

» Is capable of Detecting, Locating, Tracking and Tracing:
- individuals,
- vehicles,
- hazardous substance.

» Combines remote and autonomous platforms featuring:
- multi sensor data fusion (including biological and chemical),
- active imaging,
- data Fusion,
- command Control & Communication.

The TALOS project main objectives are as follows :

» To design the Integrated, Adaptable Land Border Large Area Surveillance System based on Unmanned Ground and Air Vehicles (TALOS system).

» To run research works in the main topics addressed by TALOS project, i.e.: Unmanned Ground Vehicles, Command and Control, Communication, Virtual prototyping.

» To implement the core components of the designed TALOS system as a proof-of-concept prototype in the Integrated Project (IP).

» To set-up and run the TALOS demonstrator (prototype) that will show the main benefits of the proposed approach.

» To promote the usage of TALOS system concept all over Europe, and to contribute to the on-going efforts of their standardization in Europe.

» To show the cost-effectiveness of the TALOS mobile / transportable concept as opposed to conventional stationary border surveillance solution.

The main TALOS innovation covers :

» Scalability – its ability to change easily system scale due to changes in the requirements and local conditions such as border size, topography, density of surveillance elements etc. ;

» Autonomous capability based on sets of rules (artificial intelligence) - programmed to the computers of the Unmanned ground vehicules and the Command & Control system ;

» Mobility / transportability - the whole system will be Mobile / Transportable installed in standard containers, transported on trailers for fast deployment in selected border zones (according to intelligence) ;

» Tactical learning/adaptation behaviour – during development process, system will be adapted to local operational requirements, operators will be interrogated, and their needs implemented in system mission planning module ;

» No need for fix infrastructure or fences – TALOS system, owing to its mobility and transportability, does not require any fixed infrastructure as well as fences ;

» Enables response to intrusion in minutes – system will respond to intrusion in the matter of minutes, not hours ; and

» Usage of "green" energy – in remote locations (where it is impossible to connect to standard power liens) the energy will be drawn from the natural sources e.g. by means of solar panels (sunny area), wind towers (windy area), water wheels (near to rivers).

Information

Acronym :
TALOS

Grant Agreement N° :
218081

Total Cost :
€ 19,906,815

EU Contribution :
€ 12,898,332

Starting Date :
01/06/2008

Duration :
48 months

Coordinator :

PRZEMYSŁOWY INSTYTUT AUTOMATYKI I POMIARÓW
Aleje Jerozolimskie 202
PL – 02486 Warsaw
Poland

—

Contact :
Mariusz Andrzejczak
Tel : (48 22) 874 01 99
Fax : (48 22) 874 01 13
E-mail : mandrzejczak@piap.pl

Website :
www.talos-border.eu

Partners

NAME	COUNTRY
Przemysłowy Instytut Automatyki i Pomiarów	Poland
ASELSAN Elektronik Sanayi ve Ticaret A.S.	Turkey
European Business Innovation & Research Center S.A.	Romania
Hellenic Aerospace Industry S.A.	Greece
Israeli Aerospace Industries	Israel
ITTI Sp. z o.o.	Poland
Office National d'Etudes et de Recherches Aérospatiales	France
Smartdust Solutions Ltd.	Estonia
Société Nationale de Construction Aérospatiale	Belgium
STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.	Turkey
Telekomunikacja Polska SA	Poland
TTI Norte S.L.	Spain
Technical Research Center of Finland	Finland
Politechnika Warszawska	Poland

TASS / Total airport security system

© Herbert Kratky - Fotolia.com

Project objectives

TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on integrating different types of selected real time sensors & sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions. TASS divides the airport security into six security control segments (environmental, cargo, people, airplanes, vehicle-fleet & facilities) each of them being monitored by various technologies that are fused together, creating a multisource labyrinth fusion logic enabling situational and security awareness of the airport anytime and anywhere. These fused control segments will be accessed through the TASS WEB-based portal by running a suite of applications making the airport security control centralized to all airport authorities. The integration will include the use of in-place technologies that will result in a cost-effective solution.

Description of the work

The overall mission of the TASS consortium is to research, develop and illustrate the capabilities of the data collection tools (which are mainly based on sensing real time technologies), the data fusion mediation system and portal and web based applications. TASS aims to integrate all these elements into one consolidated system where all the collected information is analyzed, alerted and viewed by the airport C3.

Although the array of sensors used in the TASS project consists of sensors based on both new and existing technologies, their integration and the fusion of their data will form an innovative centralized system which will provide an efficient method for securing an airport without affecting the passengers and flow of commerce.

The aim of this multidisciplinary Integrated FP7 Project is to ensure that TASS provides the airports' C3 systems with the actionable information that they seek, in order to allow an effective timely response.

The envisaged TASS system architecture and the research to be performed in TASS consists of 3 main parts: (i) Data collection, sensing and alert technologies which will cover the airport, (ii) Data fusion which will gather the information generated by these sensors and fuse it, to create a comprehensive, real time, security overview of the airport and (iii) a new TASS C2 portal and related Webbased applications which will analyze and display the collected data of each operational area.

During the development stage there will be a strong emphasis on the end-user (airports) insights, needs and remarks. Based on these requirements, TASS will provide the appropriate tools to enable C2 operators to respond in real-time to security situations in the airport.

The TASS consortium brings together European airports, innovative SME's, industrial and academic partners. The TASS solutions will be tested at several European airports including the hub airport Heathrow and Athens airport, in order to cover a wide range of needs at different levels of airport protection. The main test at Heathrow airport will involve scenarios including 2 connected to the upcoming 2012 Olympic Games in London.

Expected results

The TASS project aims to create an entire airport security monitoring solution while increasing the reliability and efficiency of the security screening while respecting the airport passengers' privacy.

TASS will provide real-time accurate situational awareness of all airport facilities and its surroundings (perimeters, terminal, access-points, sensitive areas etc.), as well as of its people (passengers, employees etc.), vehicles, cargo and airplanes.

Information

Acronym :
TASS

Grant Agreement N° :
241905

Total Cost :
€ 15,544,276.60

EU Contribution :
€ 8,986,696.15

Starting Date :
01/04/2010

Duration :
48 months

Coordinator :

VERINT SYSTEMS LTD
Mr. Gideon Hazzani
33 Maskit St Herzliya,
46733 Israel

—

Contact :
Mr. Gideon Hazzani
Phone: +972 9 962 2596
Fax: +972 9 962 4747
E-mail: Gideon.Hazzani@verint.com,

Partners

NAME	COUNTRY
Verint Systems Ltd	Israel
BAA Limited	United Kingdom
Grupo Mecanica del Vuelo Sistemas S.A.	Spain
Rapiscan Systems Limited	United Kingdom
Consorzio per la Ricera Nell' Automatica e Nelle Telecomunicazioni C.R.A.T	Italy
National Center for Scientific Research «Demokritos»	Greece
GMVIS Skysoft SA	Portugal
Mentum SA	France
Vitrociset Spa	Italy
Alcatel-Lucent Italia S.P.A	Italy
The Provost Fellows & Scholars of the College of the Holy and Undivided Trinity of Queen Elizabeth near Dublin	Ireland
IMEGO AB	Sweden
Elbit Security Systems ltd	Israel
Athens International Airport SA	Greece
Real Fusio France	France
Immersion SAS	France
Red-M Wireless Ltd.	United Kingdom
BAE Systems (Operations) Ltd	United Kingdom
Ernst & Young (Israel) Ltd	Israel

TWOBIAS / Two stage rapid biological surveillance and alarm system for airborne threats

© il-fede - Fotolia.com

Project objectives

The project aim is to develop a demonstrable, modular and "close-to-market" demonstrator of a stationary, reliable, vehicle-portable, low false alarm rate Two Stage Rapid Biological Surveillance and Alarm System for Airborne Threats (TWOBIAS) for use at indoor or outdoor public sites regarded as targets for bioterrorist attacks.

The objectives are to:

1. Establish a command and control software system for TWOBIAS in order to reliably function at a real-life site.
2. Test and evaluate biodetectors in large-scale chamber tests, and analyse background interference detection signals at real-life conditions.
3. Enhance the performance of TWOBIAS using advanced data classification methods.
4. Provide a functional combined two stage alarm biological detection and identification system.

Description of the work

TWOBIAS includes both detection (BDU – biological detection unit) and identification (BIU – biological identification unit) schemes:

» *StageONE:* First alarm based on best-in-use optimized optical BDU (detect-to-warn)

» *StageTWO:* Second alarm based on highly automated microfluidic-based platform with a molecular BIU (detect-to-treat).

The project, containing six workpackages, will enhance the progress of the state-of-art technology by developing a reliable biological surveillance system TWOBIAS in order to reduce the total time response for first responders by focusing on:

» assessing the requirements by users;

» reducing false alarm rates by improving current BDUs using complementary orthogonal detector techniques obtaining classification of biological threat agents during detection;

» developing improved alarm algorithms for existing mature and almost mature BDUs;

» combining the improved BDU with a semi-automatic microfluidic on-site molecular identification unit (BIU) for multiplex identification of biological threat agents in air (second innovation);

» integrating the optimized BDU and BIU to obtain a demonstrator of TWOBIAS; and

» using real-life conditions for characterising, improving BDU and performing testing and evaluation of TWOBIAS together with users.

Expected results

» An integrated BDU and BIU system with a two-stage alarm functionality - TWOBIAS.

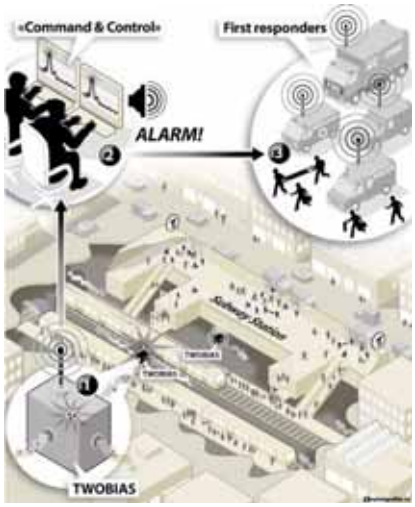
» The best-in-use BDU components with accompanying alarm algorithms (StageONE alarm).

» A reliable BIU component – automatic - microfluidic - molecular (after StageONE alarm).

» No (extremely low) false alarm rates.

» A simulation/model of the real-life test site and BDU/TWOBIAS.

» A demonstration of TWOBIAS at a real-life test.



Information

Acronym:
TWOBIAS

Grant Agreement N°:
FP7 - 242297

Total Cost:
€ 4,935,083.65

EU Contribution:
€ 3,577,834

Starting Date:
01/07/2010

Duration:
3 years

Coordinator :

NORWEGIAN DEFENCE RESEARCH ESTABLISHMENT
FFI
Norway

—

Contact:
Janet Martha Blatny
Tel: +47 63807827
Fax: +47 63807509

Partners

NAME	COUNTRY
FFI	Norway (lead)
Centre d'Etudes du Bouchet, DGA	France
Dycor Global Solutions Ltd , DGS	Cyprus
TNO	The Netherlands
Q-Linea, QL	Sweden
SUJCHBO, SCB	Czech Republic
FOI	Sweden
Thales, TRT og TSS	France
Uppsala University, UoU	Sweden

UNCOSS / Underwater coastal sea surveyor

© Fotolia.com


fig.1


fig.2


fig.2

Project objectives

The waterways are becoming more and crucial for coastal economy and paradoxically, such areas remain very vulnerable to terrorism attacks especially against underwater IED threats. Coastal regions such as in southern Europe and south-east Asia are contaminated by different ammunition left on the sea bottom after war activities from World War I, II and more recent conflicts. This represents a constant threat to the sea traffic, fishermen, tourists and local populations. The objects on the sea bottom are of different nature and include torpedoes, airplane bombs, anti-ship mines, grenades, gun fuses, ammunition and projectiles of different calibers. For example, it is estimated that there are at least 130 000 tons of explosive devices in the eastern coastal waters of the Adriatic Sea. This dramatic pollution weakens the economic development capacity of such regions.

A major challenge is to provide new tools for keeping naval infrastructure safe: harbours, ships, coastal areas, ferry terminals, oil and gas terminals, power/nuclear plants, etc. The main objective of UNCOSS project is to provide tools for the non-destructive inspection of underwater objects mainly based on neutron sensor. This technology used has already been experimented for Land Protection (especially in the frame of FP6/Euritrack project). The application of this technology for underwater protection will be a major achievement.

The classical approach for underwater IED detection is mainly based on sonar detection (derived from military development for mine clearance) which can not guarantee if unattended objects contain explosive. The identification/classification of underwater objects using classical sensors such as sonar and video cameras, becomes more and more difficult when facing asymmetrical attacks. The UNCOSS project is a cost-effective response to new terrorism threats and provides a fundamental technology for the global issue of maritime surveillance and port/naval infrastructure protection.

There is no specific device capable of identifying explosive contents of submerged UneXplode Ordnance (UXO) therefore Explosive Ordnance Disposal (EOD) teams at present have to remove the objects without knowledge of the explosive charge presence.

Expected results

The end product of this project will be a prototype of a complete coastal survey system that will make use of a specifically designed underwater neutron sensor capable of confirming the presence of explosives on the bottom of the sea, either visible or partially covered by sediments. Such a device will allow a safer and more efficient removal of explosive devices from the sea bottom of the ports and elsewhere.

The final demonstration campaign shall perform in Croatia under the supervision of the IRB which shall be responsible for the management of all licensing and authorization issues.


fig.3


fig.4


fig.5

Figure 1: Torpedo from the World War II
Figure 2: Antiship mines
Figure 3: ECA's innovative mine killer with tiltable head
Figure 4: ECA OLISTER MIDS Identification and destruction of mines
Figure 5: H1000, 1000m rated, remotely controlled subsea inspection vehicle (ROV)

Information

Acronym :
UNCOSS

Grant Agreement N° :
218148

Total Cost :
€ 4,520,000

EU Contribution :
€ 2,780,000

Starting Date :
01/12/2008

Duration :
36 months

Coordinator :

CEA
Le Ponant de Paris
25 Rue Leblanc
F-75015 Paris Cedex 15
France

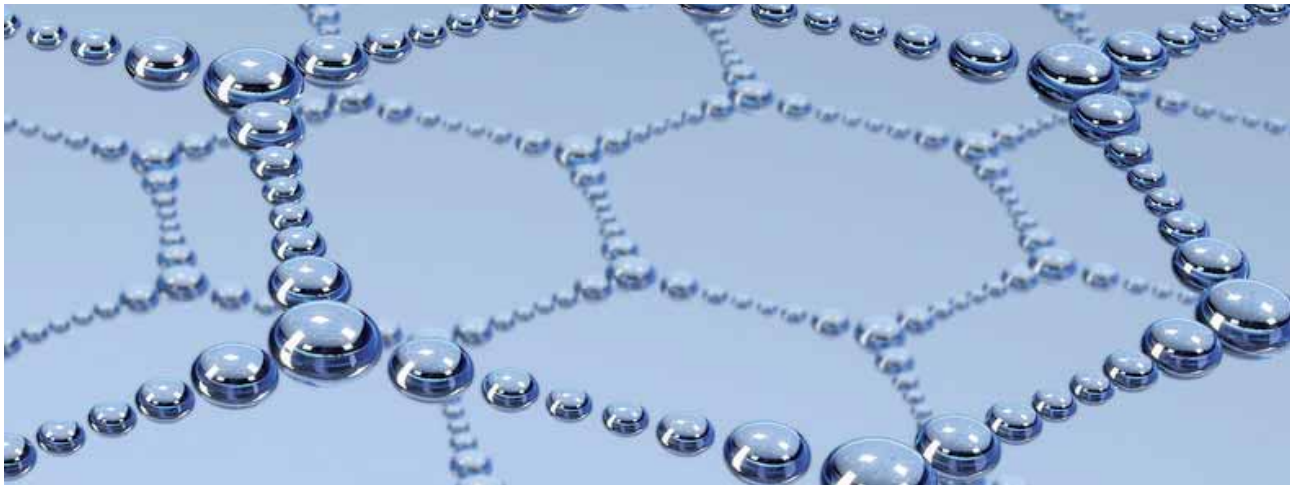
—

Contact :
Guillaume Sannie
Tel: +33169085188

Partners

NAME	COUNTRY
CEA	France
ECA S.A.	France
Ruder Boskovic Institute	Croatia
Laseroptronix	Sweden
Jozef Stefan Institute	Slovenia
A.C.T.d.o.o.	Croatia
Port Authority Dubrovnik	Croatia
Port Authority Bar	Montenegro
Port Authority Vukovar	Croatia

VIRTUOSO / Versatile information toolkit for end-users oriented open sources exploitation



© beawolf - Fotolia.com

Project objectives

The VIRTUOSO Project aims to provide an integrated open source information exploitation (OSINF) toolbox to European authorities working in border security. This toolbox will extend the "security distance" of Europe's borders by allowing EU agencies and member states to anticipate, identify and respond to strategic risks and threats in a timely manner. In short, the project aims to:

1. Improve the situational awareness of those organisations and individuals charged with securing Europe's borders.
2. Help anticipate risks such as terrorism, illegal migration and the trafficking of goods and people using OSINF.
3. Create the kernel of a pan-European technological platform for the collection, analysis and dissemination of open source information, thus ensuring greater interoperability among European actors involved in border security.
4. Provide the tools for crisis management response if anticipation fails or in the event of a rupture scenario.

Description of the work

The VIRTUOSO Project places considerable importance on the involvement of end-users. The project will be developed incrementally in response to their specific requirements.

During the first end-user requirements phase, a state-of-the-art set of tools will be demonstrated to help end-users better understand the utility of the VIRTUOSO toolkit.

Three versions of the VIRTUOSO Toolkit will be delivered:

» *VIRTUOSO-V0:* A very basic version of the framework, integrating basic functions and demonstrating its potential.

» *VIRTUOSO-V1:* A first version of the framework integrating some operational functions.

» *VIRTUOSO-V2:* A second version of the framework with all operational functions adapted and/or developed.

Work Packages:

» *WP0:* Management

» *WP1:* End-users requirements (10 workshops organised with end-users)

» *WP2:* Architecture and infrastructure tools

» *WP3:* Privacy, ethical and legal aspects

» *WP4:* Data acquisition

» *WP5:* Processing

» *WP6:* Knowledge management

» *WP7:* Decision support and visualization

» *WP8:* Integration and demonstration

» *WP9:* End-Users validation (10 workshops organised with end-users)

» *WP10:* Dissemination

Expected results

This seamless OSINF platform will aggregate, in realtime, content from the internet, leading subscription providers, and broadcast media. This content will be filtered and analysed using text mining and other decision support technologies to improve situational awareness and provide early warning to end-users.

The project's deliverables include a demonstrator of the VIRTUOSO toolkit (one that integrates various information services and intelligence applications) and full documentation on the platform itself.

The core platform will be freely available as open source software at the end of the project.

Information

Acronym:
VIRTUOSO

Grant Agreement N°:
242352

Total Cost:
€ 11,510,542.25

EU Contribution:
€ 7,999,182.55

Starting Date:
01/05/2010

Duration:
36 months

Coordinator:

CEA LIST
Commissariat a l'énergie atomique
Centre de Saclay- Bât 476
F91191 Gif-Sur-Yvette Cedex
France

—

Contact:
Géraud Canet
Tel: +33 1 46 54 82 59
Fax: +33 1 46 54 75 80
E-mail: geraud.canet@cea.fr

Partners

NAME	COUNTRY
CEA	France
EADS Defence and Security Systems	France
ATOS Origin Sociedad Anonima Espanola	Spain
Mondeca	France
Newstin a.s	Czech Republic
SAIL Technology AG	Austria
Aalborg University	Denmark
Thales CommunicationsBertin Technologies	France
Stichting Katholieke Universiteit / Brabant Universiteit Van Tilburg	The Netherlands
TNO	The Netherlands
Ingeniería de Sistemas Para la Defensa de Espana SA – ISDEFE	Spain
Hawk Associates Limited	United Kingdom
Compagnie Européenne d'Intelligence Stratégique – CEIS	France
Universita Degli Studi di Modena e Reggio Emilia	Italy
Columba Global Systems Ltd.	Ireland
Thales Research and Technology	France

WIMA²S / Wide maritime area airborne surveillance

© WIMA²S

Project objectives

WiMA²S addresses primarily the urgent need to control illegal immigration and human trafficking by sea, in the context of the Integrated Border Management. In line with the EU Maritime Policy, it also contributes to other public service missions: shipping safety, search and rescue, protection of the marine environment, fisheries monitoring, interception of illegal trade and smuggling arriving by sea.

WiMA²S aims in particular at developing key technologies to prepare the future for the operational use of Unmanned Air Vehicles (UAVs) and innovative mission aircraft

WiMA²S takes into account the operational end-user requirements and the need to develop strong European capabilities in maritime surveillance.

Taking into account that:

» To build a maritime picture, detection and identification phases are mandatory.

» Air assets are unique for wide area maritime surveillance: they are the only one which can provide situation awareness over extended areas because of their endurance, speed and their capacity of reliable long distance detection accuracy; they can be directed to areas of interest, as close as possible from the threat point of origin, and have the flexibility to react to the situation, performing close-up inspection when needed.

» Shortfalls of surveillance capacities of EU wide maritime areas concerning responsibilities in border security, illegal immigration, fisheries control, pollution, terrorism,…

» Lack of air assets for surveillance and their relatively high costs.

» UAVs can be a very attractive technical solution for maritime surveillance — however, one of the main obstacles is integration in the European Air Traffic.

Description of the work

WiMA²S proposes solutions to these issues by:

» Developing original and innovative technological solutions to increase airborne maritime surveillance efficiency while reducing costs.

» Filling the gap between Piloted Mission Aircraft and UAVs for maritime surveillance, and preparing concepts for using UAVs with remote control mission system operation and combining these with existing maritime surveillance systems.

» Partly simulating and partly demonstrating — including a flight demo of a UAV — the concept with End-Users feedback.

» Analysing the cost efficiency in support of the feasibility of the concept.

» Reporting a road map in the final report for further technological projects in the priority topic of maritime surveillance.

© Kevin Bourdeaux - Fotolia.com

Information

Acronym :
WIMA²S

Grant Agreement N° :
217931

Total Cost :
€ 3,997,523

EU Contribution :
€ 2,737,169

Starting Date :
01/12/2008

Duration :
36 months

Coordinator :

THALES AIRBORNE SYSTEMS S.A
25 Avenue Gustave Eiffel
FR-33608 Pessac
France

—

Contact :
Gilles JURQUET
Fax : +33(0)5 - 57 26 71 60
E-mail : gilles.jurquet@fr.thalesgroup.com

Website :
www.wimaas.eu

Partners

NAME	COUNTRY
Thales Systemes Aeroportes S.A	France
SELEX GALILEO	Italy
Dassault Aviation	France
SENER Ingeneria y Sistemas	Spain
FOI	Sweden
Fraunhofer IITB	Germany
JRC	Belgium
Air Force Institute of Technology	Poland
EUROSENSE	Belgium
SATCOM1 Aps	Denmark
SETCCE	Slovenia
Aerovisión Vehículos Aéreos S.L	Spain
Thales Communications S.A.	France
Mediterranean Academy Of Diplomatic Studies	Malta

Acknowledgement



ADABTS • AMASS • BIO PROTECT • COCAE • CrisComScore • DETECTER • EFFISEC • ESCoRTS • EULER • FRESP • iDetecT 4ALL • IMSK • ISTIMES • SAFE-COMMS • SECTRONICS • SECURENV • TALOS • TWOBIAS • UNCOSS • WIMA^{2}S

Notes

SECURITY RESEARCH PROJECTS

under the 7th Framework Programme for Research

Investing into security research for the benefits of European citizens

—

Further information available at: http://ec.europa.eu/enterprise/security/index_en.htm

Catalogue number: NB-32-10-383-EN-C

ISBN 978-92-79-16426-2

European Commission
Enterprise and Industry