European Commission

Security Research Projects
under the 7th Framework Programme for Research

EU Research for a Secure Society

July 2012

Enterprise and Industry

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):
00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

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

Luxembourg: Publications Office of the European Union, 2012

ISBN 978-92-79-25113-9
doi:10.2769/38445

Cover picture: © Fotolia/Shutterstock

Printed in Belgium

PRINTED ON RECYCLED PAPER

INTRODUCTION

Investing in security research for the benefit of European citizens, critical infrastructures, SMEs and industry

"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 in security research. This catalogue presents an exhaustive overview of all projects currently supported by FP7's Security Research budget as of May 2012."

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 (> 22%) is going to SMEs. By stimulating research and innovation – and promoting direct cooperation between providers and end-users of security equipment, 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 for fundamental human rights, including privacy, research into the preparedness and response of society in the face of 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.

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

Prepared by the European Commission, Directorate-General for Enterprise and Industry, Unit H3 Security Research and Development,
E-mail: entr-security-research@ec.europa.eu

TABLE OF CONTENTS

AVERT / The Autonomous Vehicle Emergency Recovery Tool (AVERT) provides a capability rapidly to deploy, extract and remove both blocking and suspect vehicles from vulnerable positions and confined spaces.

© Arindam Banerjee - istockphoto.com

Information

Grant Agreement N°
285092
Total Cost
€ 3,685,613.65
EU Contribution
€ 2,810,822
Starting Date
01/01/2012
Duration
34 months

Coordinator

IDUS Consultancy Ltd
10 Lime Close
RG41 4AW, Wokingham,
United Kingdom
Contact
Richard James May
Tel: +44 118 979 1828
Mobile: +44 77 333 20856
E-mail: Richard.may@
idusconsultancy.co.uk
Website: http://avertproject.eu/

Project objectives

Terrorism can lead to horrific loss of life, extensive disruption to city transport and damage to commercial real estate. Vehicles provide an ideal delivery mechanism because they can be meticulously prepared well in advance of deployment and then brought in to the Area of Operations. Furthermore, a real and present danger comes from the threat of Chemical, Radiological, Biological and Nuclear (CRBN) contamination.

Current methods of bomb disruption and neutralisation are hindered in the event that the device is shielded, blocked or for whatever reason cannot be accessed for examination.

The Autonomous Vehicle Emergency Recovery Tool (AVERT) shall provide a unique capability to Police and Armed Services to rapidly deploy, extract and remove blocking vehicles from vulnerable positions such as enclosed infrastructure spaces, tunnels, low bridges as well as under-building and underground car parks. This will then allow access for Explosive Ordnance Disposal (EOD) operation.

Description of the work

The project covers the development and demonstration of a proof of concept for an Autonomous Vehicle Emergency Recovery Tool (AVERT). This is designed to assist EOD teams by locking onto the vehicle(s) which is (are) obstructing the deployment of EOD systems and rapidly and safely removing it (them) from the path to allow speedier access than can currently be achieved.

The AVERT project concept is to automate the placing of lifting bogies, capable of omnidirectional movement, under the road wheels of identified vehicles and to synchronise their lifting and path as a group in order to remove the vehicle without disturbance. Vehicles can be removed from confined spaces (e.g. where the height level is constrained) with delicate handling, swiftly and in any direction to a safer disposal point to reduce or eliminate collateral damage to infrastructure and personnel.

The operational framework is targeted at a system which is deployed alongside current EOD robots and equipment. This system comprises a number of independent lifting bogies, one for each wheel of the blocking vehicle to be moved. The bogies are deployed from a carrier platform (Deployment Unit) and each locks onto a road wheel on the designated vehicle. Once in position, the swarm of bogies acts in synchronisation to raise the road wheels and move the vehicle along a safe path, allowing the existing EOD robot access for neutralising operations.

© Avert

view/plan

© Avert

deploy

© Avert

extract

The concept also includes a Command Console which is detached from the Deployment Unit and held at the command post. This console will be designed to provide the commander with command and executive control of the operation by designating the desired access path and confirming the sequence of vehicles to be moved to achieve it.

AVERT will be commanded remotely and will operate autonomously under its own power and sensor awareness, as a critical tool alongside existing technologies, thereby enhancing bomb disposal response speed and safety.

Expected results

Demonstration of:

- capability to safely extract and remove blocking vehicles in a timely manner;
- delivery of access paths which cannot be provided by EOD robots;
- delivery of a faster and safer removal capability than that which is currently achievable manually;
- provision of effective command and control of the autonomous co-operative elements within a representative EOD operating framework.

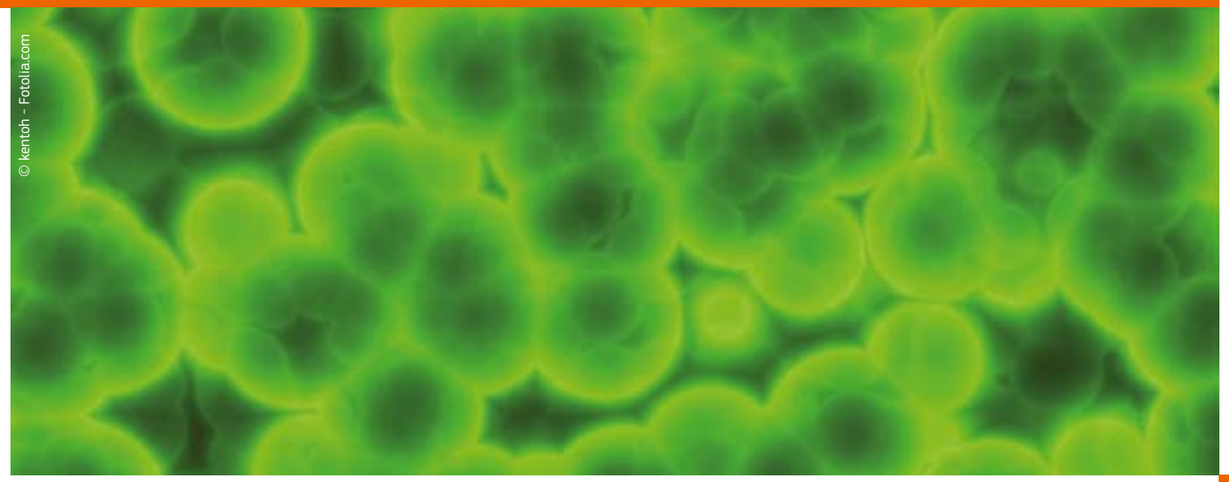
PARTNERS

IDUS Consultancy Ltd (IDUS)
BB-Ingenieure Ingenieurbüro (BBI)
Zurcher Hochschule Fur Angewandte Wissenschaften (ZHAW)
Democritus University of Thrace (DUTH)
Marshall System Design Group Ltd (MSDG)
Force Ware GmbH (FW)

COUNTRY

United Kingdom
Germany
Switzerland
Greece
United Kingdom
Germany

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



Information

Grant Agreement N°
242306
Total Cost
€3,963,556.55
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

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 of 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:

» 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 from heat-decomposed organic matter;

» 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;

» 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;

» 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;

» 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 against 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.

PARTNERS	COUNTRY
LGI Consulting	France
AVSISTA	Lithuania
C-Tech Innovation Ltd	United Kingdom
Environics Oy	Finland
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Institut für Umwelt Technologien GmbH	Germany
Robert-Koch Institut	Germany
University of Aalborg	Denmark
Environics-IUT GmbH (ENIT)	Germany

BONAS / BOmb factory detection by Networks of Advanced Sensors

Information

Grant Agreement N°
261685
Total Cost
€ 4,971,631.81
EU Contribution
€ 3,488,360.01
Starting Date
01/04/2011
Duration
42 months

Coordinator

AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE
Diagnostics and Metrology Laboratory (UTAPRAD-DIM)
Via Enrico Fermi 45
00044 Frascati, Rome
Italy
Contact
Antonio Palucci
Tel: +390694005299
Mobile: +393298313933
Fax: +390694005334
E-mail: antonio.palucci@enea.it
Website: www.bonas-fp7.eu

Project objectives

The BONAS project presents the following objectives:

» To design, develop and test a novel wireless sensor network for increasing citizen protection and homeland security against threats posed by IED devices. The sensor network will focus on the detection of traces of precursors used in IED production (particulates, gases, waterborne) in the vicinity of a "bomb factory". This will contribute to the determination of the "factory's location", allowing an early threat thwart.

» To perform a feasibility study that will assess the usefulness and potential advantages that the BONAS concept will bring about in the future. A cost analysis will be performed in order to foresee the financial effort associated with the field deployment of such a sensor network, its operation and maintenance.

» To demonstrate the BONAS concept in a close to real-life scenario, implementing all developed network sensors with the aim of evaluating their performance and larger scale deployment potentials.

» To investigate and prepare the potential future deployment of key sensors aboard a flying platform with a view towards increasing the BONAS network detection capabilities.

Description of the work

The aim of BONAS is to design, develop and test a novel wireless sensor network for increasing citizen protection and homeland security against terrorist attacks, in particular against the threat posed by IED devices. The sensor network will focus on the detection of traces of precursors used in IED production (particulates, gases and/or waterborne) present in the environment surrounding the vicinity of a "bomb factory". The different sensors are specifically designed to be deployed in sensitive locations and easily camouflaged. This network will help pinpoint the "factory's location", allowing an early threat thwart. A feasibility study will assess the usefulness and potential advantages that the BONAS concept will bring about in the future and the costs of mass production of sensor networks integrating COTS components.

BONAS intends also to investigate and prepare the potential future deployment of key sensors aboard a flying platform with a view towards increasing the BONAS network detection capabilities. The wireless sensor network will feature a variety of sensing devices (in-situ and remote), that will jointly provide broad chemical spread and low false alarm rates through an expert system management of the data collected. In particular, BONAS will develop a Lidar/Dial system; QEPAS sensor; SERS sensor; QCM sensor; and electrochemical sensor.

BONAS includes a multidisciplinary team of leading European research groups together with industrial organizations and end-users with previous experience and activity in the field of specific local and remote sensor development and with experience on security projects. The consortium represents the complete supply chain of the proposed product, which sets good perspectives for exploitation and commercialization of the generated innovations. The consortium will be supported by an already established Advisory Board formed by experts from the various police corps.

Expected results

The BONAS project envisages an innovative, large-scale sensor network in the future, able to detect IED preparation with a minimum rate of false alarms and relying on three different layers. The target substances will comprise explosive and precursor substances contained in IEDs. The concept is based on a series of increasingly specific tests taking place in increasingly smaller areas starting with general tests and then reducing the search area. Each one of the referred layers will correspond to a different phase of threat detection and to different levels of the wireless sensor network.

© Bonas

PARTNERS	COUNTRY
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE (ENEA)	Italy
CONSORZIO CREO-CENTRO RICERCHE ELETTRO OTTICHE (CREO)	Italy
SERSTECH AB (SAB)	Sweden
TEKEVER - TECNOLOGIAS DE INFORMACAO, S.A. (TEK)	Portugal
LASER DIAGNOSTIC INSTRUMENTS AS (LDI)	Estonia
CSEM CENTRE SUISSE D'ELECTRONIQUE ET DE MICROTECHNIQUE SA - RECHERCHE ET DEVELOPPEMENT (CSEM)	Switzerland
EADS DEUTSCHLAND GMBH (EADS)	Germany
UNIVERSITE CLAUDE BERNARD LYON 1 (UCBL)	France
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONE)	France
UNIVERSITE DE LAUSANNE (UNIL)	Switzerland
NATIONAL BUREAU OF INVESTIGATION (NBI)	Finland
KING'S COLLEGE LONDON (KCL)	United Kingdom
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)	France
QUEEN'S UNIVERSITY BELFAST (QUB)	United Kingdom

CAPER / Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime

© Louise Gagnon - Fotolia.com

Information

Grant Agreement N°
261712
Total Cost
€7,143,920.80
EU Contribution
€5,579,346
Starting Date
01/07/2011
Duration
36 months

Coordinator

S21SEC INFORMATION SECURITY LABS S.L.
R&D
Parque empresarial la Muga, 11 1a planta
31160 Orkoien
Spain
Contact
Carlos MONREAL
Tel: +34948100013
Mobile: +34 607 370 017
Fax: +34948336930
E-mail:
cmonreal@s21sec.com
Website:
http://www.s21sec.com/

Project objectives

The goal of the CAPER project is to create a common platform for the prevention of organised crime through sharing, exploitation and analysis of information sources. CAPER will support collaborative multilingual analysis of audiovisual content (video, audio, speech and images) and biometrics information, supported by Visual Analytics and Data Mining technologies. The integration of database technologies, application workflow and semantic modelling of processes, and legal and privacy limitations, will permit participating Law Enforcement Authorities (LEA) to share information and investigative and experiential knowledge. The CAPER platform will be built in close collaboration with the LEA users in order to fulfil their current and forthcoming needs. The project is clearly focused on the fusion and real validation of the existing state of the art, coupled with innovative new technologies, to solve current bottlenecks faced by LEAs.

Description of the work

The CAPER platform will consist of six core elements:
Open and Closed Data Sources: Multi-format, multimedia and multimodal information from open sources, TV and Radio capture, and information in closed legacy systems are the data sources to be mined and evaluated by CAPER.

Data Acquisition: Depending on the information source type, different acquisition patterns will be applied to ensure acquired information has a suitable format for analysis.

Information Analysis: Each analysis module is geared towards a specific content type, i.e. text, image, video, audio and speech or biometric data.

Information and Reference Repositories: Both source data when required, and the information mined by the information analysis modules, will be stored in these repositories, separated by content type.

Interoperability and Management Application: This is the end users' workbench. Built on a web based collaborative platform, it will allow the Law Enforcement Officers to create and configure their monitoring requests and analysis petitions.

Visual Analytics (VA) and Data Mining (DM): Grouped under the management application, the VA and DM elements are key components of the CAPER platform, since they will provide the intelligence necessary to support the outputs of the system.

Expected results

CAPER will support multilingual content analysis from its inception. Its focus will be on the acquisition of information from the Internet, Mass Media and existing LEA information systems. CAPER will include workflow and management applications to allow inter agency and transnational collaboration. The CAPER acquisition and analysis modules will be autonomous and deployable as a geographically distributed system. This provides both technical and operational benefits. CAPER will also comply with present European instruments for Freedom, Security and Justice by addressing the priorities 7 and 8 of The Hague programme.

PARTNERS	COUNTRY
S21Sec Information Security Labs S.L. (S21sec)	Spain
Asociación Centro de Tecnologías de Interacción Visual y Comunicaciones Vicomtech (VICOM)	Spain
Fraunhofer – Gesellschaft zur Foerderung der Angewandt (Fraunhofer-IGD)	Germany
Synthema (Synthema)	Italy
VOICEINTERACTION – Tecnologias de Processamento de Fala, S.A. (VI)	Portugal
ALTIC	France
Technion – Israel Institute of Technology (Technion)	Israel
Angel Iglesias S.A.- IKUSI (IKUSI)	Spain
Alma Consulting Group SAS (Alma)	France
Consiglio Nazionale Delle Ricerche - Institute for Informatics and Telematica (IIT)	Italy
Universitat Autonoma de Barcelona (UAB)	Spain
Studio Professionale Associato a Baker & McKenzie (BAK)	Italy
Ministero dell'Interno - Servizio Polizia Postale e delle Comunicazioni (Postal and Communications Police Service) (PCPS)	Italy
Serviciul de Informații Externe (External Intelligence Service) (SIE)	Romania
Polìcia Judiciària (Judicial Police) (PJ)	Portugal
Guardia Civil (Civil Guard) (GC)	Spain

CBRNEMAP / Road-mapping Study of CBRNE Demonstrator

© Morane- Fotolia.com

RESEARCH **COMPLETED**

Phase two of the CBRNE Demonstrator project will illustrate the usefulness of the system-of-systems approach to counter CBRNE terrorism. This will best be validated in a set of realistic scenarios where vital parameters such as successful denial of access, delay of effect, shortened time for evacuation, shortened response time, more effective health care and other considerations can be observed and quantified.

Information

Grant Agreement N°
242338
Total Cost
€1,662,022
EU Contribution
€1,376,185
Starting Date
01/06/2010
End Date
30/09/2011

Coordinator

EUROPEAN CBRNE CENTER AT UMEÅ UNIVERSITY
KBC Building
90187 UMEA
Sweden
Contact
Agneta H. Plamboeck
E-mail: Agneta.Plamboeck@cbrnecenter.eu
Website:
http://www.cbrnemap.org/

Project objectives

CBRNEmap was a "phase I" Security Research project to define a strategic roadmap that will lead to a subsequent phase II, large-scale CBRNE (chemical, biological, radiological, nuclear, explosive) Demonstrator project. Its goal was to bring together end-users, industry and other stakeholders with Europe's scientific and technical communities to address the cross-cutting activity of such a large-scale effort and to identify potential scenarios and technical solutions.

Its key objective was to evaluate the multi-dimensional challenges of countering CBRNE-based threats. Temporal events (before, during and after) were contrasted against societal targets (mass transport, public spaces, etc.) and societal sectors directly involved in such events (law enforcement, health first-responders, etc.).

These generic needs were matched by technological solutions that will be integrated at a system-of-systems level, leading to the CBRNE Demonstrator.

Results

The project narrowed down CBRNE counter-terrorism to three dimensions: the need to protect society's vital functions, the ability to respond to CBRNE events and the need for resilience to enable society to rebuild capabilities. The generic needs of each dimension were matched with advanced technological solutions and integrated at the system-of-systems level for demonstration during phase II.

CBRNEmap's research identified a number of gaps in CBRNE counter-terrorism and solutions to fill them. Among others, it recommends that:

- more research effort be devoted to the design of buildings and, in particular, to the design of floor plan layouts, escape routes and surface-covering materials;
- recent advances in the material sciences such as nano-technologies argue for the development of new filters and protective equipment;
- the protection of buildings from attack require new modelling techniques to predict the spread of CBRN gas or aerosol agents;
- nano-technologies and new materials be studied for their potential decontamination applications;
- more EU research focus on the use of symbology or simplified language – including animation or other communications channels – to increase the rate, precision and absorption of public messaging about major CBRNE incidents.

PARTNERS	COUNTRY
European CBRNE center at Umeå University	Sweden
Police National CBRN Centre	United Kingdom
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
Totalförsvarets Forskningsinstitut (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

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218000
Total Cost
€2,644,416
EU Contribution
€ 2,031,347
Starting Date
01/10/2008
End Date
31/03/2012

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
Website: www.cocae.eu

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.

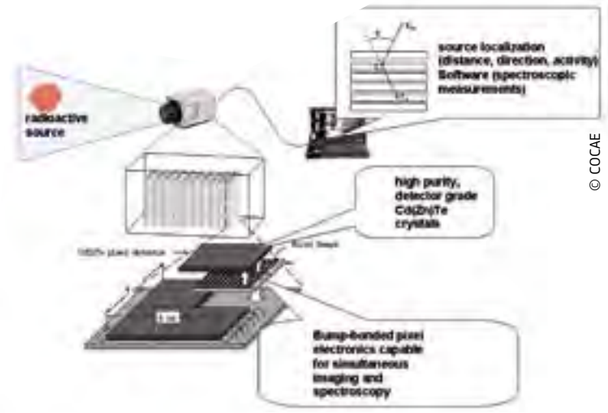
» The design of pixel electronics capable for simultaneous imaging and spectroscopy. The electronics will be bump bonded to the pixel detectors. This is essential for the localization and the identification of the radioactive source.

» 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.

Results

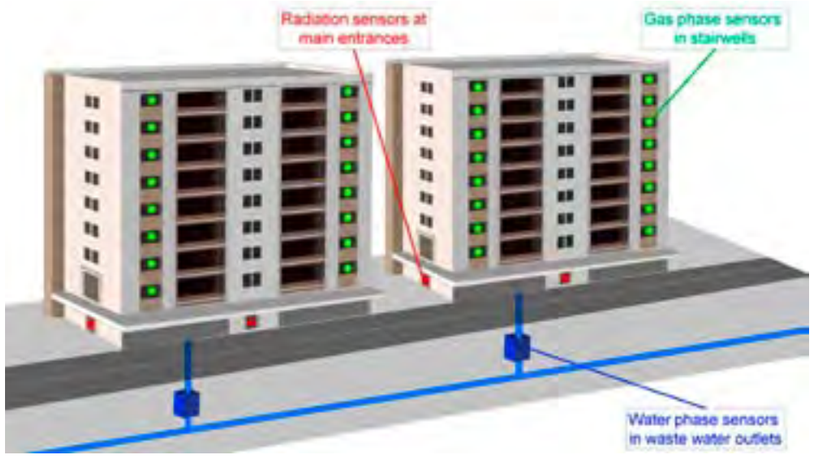
The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.



© COCAE

PARTNERS	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

COMMONSENSE / Development of a Common Sensor Platform for the Detection of IED "Bomb Factories"



Information

Grant Agreement N°
261809
Total Cost
€4,768,992
EU Contribution
€3,404,935
Starting Date
01/01/2011
Duration
36 months

Coordinator

UNIVERSITY COLLEGE CORK, NATIONAL UNIVERSITY OF IRELAND
Tyndall National Institute
Western Road
Cork
Ireland
Contact
Hugh Doyle
Tel: +353 (0)21 490 4177
Fax: +353 (0)21 490 4058
E-mail: info@fp7project-commonsense.eu
Website: www.fp7project-commonsense.eu

Project objectives

The detection of chemical explosives is crucial for homeland security, environmental cleaning, and humanitarian efforts. Chemical explosives encompass a variety of compounds, with different vapour pressures, solubilities and chemical reactivities, making broad-class detection a serious challenge. While many sensing methods currently exist, none is ideal. Principal deficiencies include lack of portability, a susceptibility to false positive results due to environmental contaminants or false negative results to interfering compounds. The need exists for a single distributed network, with a common interface and communications protocol, to manage and communicate with a variety of different sensor technologies, and use the combined sensor data to produce clear results with low false positive/negative readings. The objective of the CommonSense project is to create and demonstrate such a single distributed network, with common interface and communications protocols, to manage and communicate with a variety of different sensor technologies, and to use the combined sensor data to produce clear results with low false positive/negative readings.

Description of the work

The work plan for the CommonSense project is divided into five complementary technical work packages:

Design and Specification
At the start of the project, the partners will specify target IED analytes, detection limits and test conditions relevant to end users. Specification of the common testing and benchmarking procedures, operating protocols, network architectures and communications protocols will also be carried out.

Materials Development and Characterisation
A variety of novel molecular, polymeric and nanostructured sensor materials will be developed and characterised with respect to their optoelectrical and photophysical properties, especially their response to sub-ppb (gas phase) and sub-ppm (liquid) levels of explosive compounds.

Sensor Development
Development of the sensor modules will be carried out at separate partner sites for initial testing and characterisation. A variety of different electrical, opto-electrical and opto-electrochemical devices for gas- and water-phase detection of IED analytes will be developed. A series of radiation detection modules will also be developed.

Software Development and Networking
Development of the common network platform for control and communication of the sensor modules. Driver software for control and read-out from different sensor types will be done at partner sites prior to integration with the network and the chemometric "learning" algorithms.

Integration, Testing and Industrial Validation
Integration of the sensor modules and quantitative testing and validation of the performance of the sensor modules. The final testing and assessment will be carried out in a "real-world" environment.

These are supported by two non-technical work packages focusing on dissemination & exploitation of project results and project management.

Expected results

The expected results from the project are:

» Development of modules for gas-phase detection of explosives with ppb sensitivity;

» Development of modules for water-phase detection of explosives with sub-ppm sensitivity;

» Development of a small form factor low-power gamma radiation sensor with <10% energy resolution and an energy range of 60keV to 2MeV;

» Development of an intelligent learning network, using chemometric algorithms to teach itself to detect explosives and ignore interferents.

PARTNERS	COUNTRY
University College Cork, National University of Ireland (UCC)	Ireland
Israel Institute Of Technology (Technion)	Israel
The University Of Manchester (UNIMAN)	United Kingdom
Alphasense Limited (ALPHA)	United Kingdom
Bundesanstalt Fuer Materialforschung und Pruefung (BAM)	Germany
SensL Technologies Limited (SENSL)	Ireland
Thales Communications S.A. (TCF)	France
Police Service of Northern Ireland (PSNI)	United Kingdom

CONPHIRMER / Counterfeit Pharmaceuticals Interception using Radiofrequency Methods in Realtime

© Elena Aliaga - istockphoto.com

Information

Grant Agreement N°
261670
Total Cost
€3,599,540
EU Contribution
€2,634,489
Starting Date
01/07/2011
Duration
36 months

Coordinator

KING'S COLLEGE LONDON
Engineering
Strand
WC2R 2LS London
United Kingdom
Contact
Kaspar Althoefer
Tel: +44 (0)20 7848 2431
Mobile: +44 (0)77 888 7 555 3
Fax: +44 (0)20 7848 2932
E-mail: k.althoefer@kcl.ac.uk
Website: www.conphirmer.eu

Project objectives

The members of the CONPHIRMER consortium have come together to create a portable and easy-to-use sensor for telling genuine medicines from fakes, which customs officers and other agents of law enforcement can use without having to remove the medicines from their packaging. With this device agencies charged with tackling the growing menace of the trafficking in counterfeit medicines will be able to screen packaged pharmaceuticals at EU borders and airports quickly and accurately, using a non-invasive and non-destructive technology that uses only harmless radio waves.

Description of the work

The consortium will be utilizing a form of radio frequency spectroscopy known as Quadrupole Resonance (QR). This technology has been developed and deployed for the detection of concealed explosives and landmines and is considered human safe.

QR is a radiofrequency (RF) spectroscopic technique that can detect signals through multiple layers of cardboard, glass, plastic and/or wood. QR can analyse any compound containing a quadrupolar nucleus, which accounts for over 50% of elements in the periodic table, and, in particular, it is ideally suited for the analysis of compounds containing nitrogen, chlorine or bromine, sodium and potassium, which includes over 80% of all drugs.

The consortium will develop a portable QR-based medicines authentication device tailored to the needs of customs officers operating at EU borders in parallel with identifying the QR characteristics of medicines that afford the best discrimination between real and fake medicines. QR "fingerprints" based on these key characteristics will be put together to form a database that will be of use not only on the CONPHIRMER device, but in all analytical applications of QR for medicines authentication.

Expected results

A robust, economical, user-friendly and portable prototype system for the non-invasive, non-destructive and highly-specific testing of packaged pharmaceutical products will be produced. The system will quickly give an operator an answer to whether or not a medicine under transport matches that listed on the manifest.

Quadrupole fingerprints of active pharmaceutical ingredients (APIs) and pill formulations will be generated and built up into a database pre-loaded onto the device.

PARTNERS	COUNTRY
King's College London (KCL)	United Kingdom
French-German Research Institute of Saint-Louis (ISL)	France/Germany
University of Ljubljana (IMFM)	Slovenia
Jožef Stefan International Postgraduate School (IPS)	Slovenia
University of Lund (ULund)	Sweden
Rapiscan Systems Ltd (RSL)	United Kingdom
Polish Customs Service (PCS)	Poland
Stelar SRL (STELAR)	Italy
London South Bank University (LSBU)	United Kingdom
Bagtronics Ltd. (BAG)	United Kingdom

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

© morrbyte - Fotolia.com

Information

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

Project objectives

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

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

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.

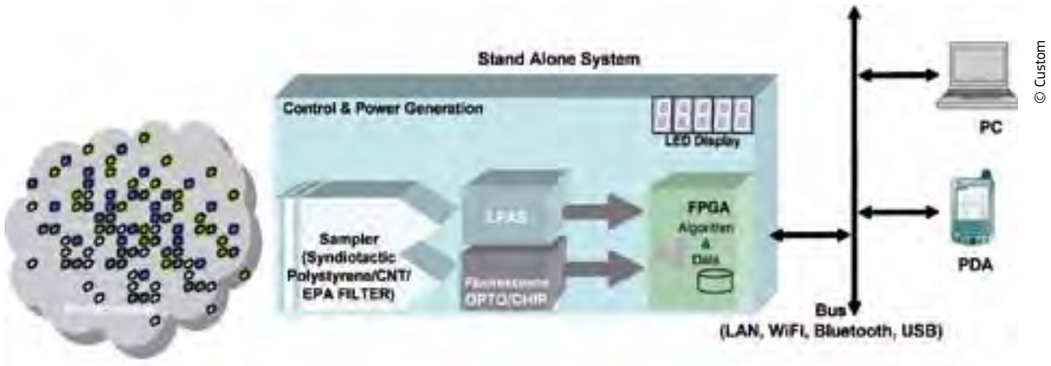
Description of the work

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 happens 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 for both vapour and powder phase compounds; collecting or, where not existing, building up a database of characteristic spectra for both measurement techniques.



© Custom

Expected results

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

PARTNERS	COUNTRY
SELEX Sistemi Integrati S.p.A.	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

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

Information

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

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 fibre IR, will allow for developing a sensor that features hand-portability and prompt response –for field operation– and is able 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 throughout the project.

Expected results

The main output of the project will be the initial prototype of a sensor able 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).

PARTNERS	COUNTRY
Consorzio CREO- Centro Ricerche Elettro-Ottiche	Italy
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Consiglio Nazionale delle Ricerche	Italy
EADS Deutschland GMBH	Germany
Selex Sistemi integrati SpA (SSI)	Italy
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

EMPHASIS / Explosive Material Hidden Agile Search and Intelligence System

© Emphasis

Information

Grant Agreement N°
261381
Total Cost
4,593,273
EU Contribution
3,406,051
Starting Date
01/10/2011
Duration
36 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Defence & Security
Systems and Technology
Department of Energetic Materials
Grindsjön Research Centre
SE-14725, Tumba, Sweden
Contact
Dr. Hans Önnerud
Tel: +46 8 5550 4058
Mobile: +46 709 277386
Fax: +46 8 5550 3949
E-mail: hans.onnerud@foi.se
Website:
www.emphasis-fp7.eu

Project objectives

The goal of the EMPHASIS project is to test a system concept for the surveillance tool of tomorrow for detection and localisation of ongoing illicit production of explosives and improvised explosive devices (IEDs) in urban areas.

The EMPHASIS system is composed of different sensors in a network. Area detectors for the monitoring of explosives or precursors to explosives in the vapour phase will be used. Multiple static sensors, positioned in the sewer, for the monitoring of the sewage for indicative traces will also be used. The total gathered data will be fused and evaluated in a command centre.

If a threat substance is detected in elevated amounts, information about the type, location, time and amount will be registered and sent to a command centre where further evaluation and appropriate actions are undertaken. The intention is first to cover a large area that will be reduced step by step to smaller areas. The search strategy in the smaller area is to increase the number of sensors used in order to localise the bomb factory. The exact pinpointing of the bomb factory will be performed using stand-off detectors in mobile equipped units.

Description of the work

EMPHASIS is a novel way to perform surveillance of a very large area with respect to detecting explosives and precursors to explosives and IEDs.

A key aspect of the EMPHASIS concept is that it will allow efficient intelligence-led assessment of an area of a city in order to establish where, and more crucially when illicit bomb-making activity is occurring. A successful system based on EMPHASIS would lead to a very significant reduction in surveillance man-power of suspect areas. Critically, when a narrow area or house has been identified as being under suspicion, the system will provide invaluable assistance in the timing of police intervention increasing the chance of successful convictions as a consequence.

The area monitoring sensors will be able to cover distances of hundreds of meters thereby facilitating very large area coverage.

Moreover, the stand-off sensors used will have the capacity to detect explosives that have been transferred to surfaces by the touch from people who have handled the explosives. In addition, the combination with electrochemical sensors capable of tracing the explosives present in the sewage will make an extensive system.

A feasibility and cost effectiveness study will be performed in order to ensure a commercially realistic system.

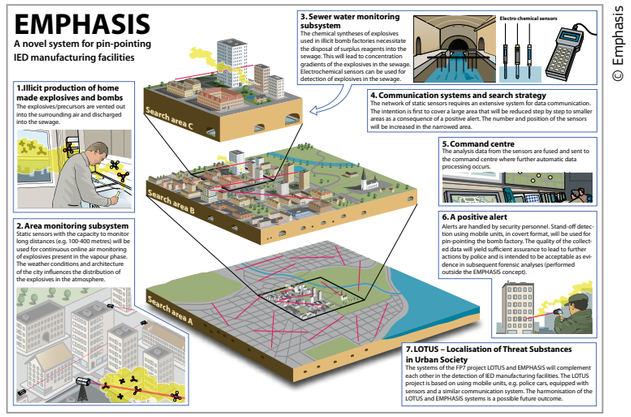
One of the advantages of the EMPHASIS system is the fact that many of the developments achieved in another FP 7 project, LOTUS, can be benefited from. Data and developments can be implemented as much as possible e.g. exploitation of knowledge obtained concerning the central command, threat substance list, dispersion and modelling of threat substances in the air and the already set-up home explosive laboratory.

In EMPHASIS, the focus for the detection will be on three types of cases: i) Detection of explosives/precursors in vapour phase at low concentrations; ii) Detection of explosives/precursors at low concentrations in sewage; and iii) Detection of particles (low concentrations) e.g. door-handles or other covered surfaces.

The fusion of sensor data will lead to potential alerts.

Expected results

On 7 July 2005, three bombs exploded within a very short timeframe on three of the London Underground trains. A fourth bomb exploded somewhat later on a double-decker bus. The bombs were of the home-made explosive types and were packed into rucksacks. The discovery of these types of suicide bomb attacks is very difficult and relies on intelligence and qualified police work. If discovered at a late stage of the criminal activity it is very hard to neutralise the object without consequences for third persons.However, for a system such as EMPHASIS the objective is to discover the illicit activities at a very early stage thus making the neutralisation both easier and with minimum consequence for third persons. This will be one of the strengths of EMPHASIS.



© Emphasis

PARTNERS

Totalförsvarets Forskningsinstitut (FOI)
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT-IAF)
Portendo AB (Portendo)
Cascade Technologies Ltd (Cascade)
Morpho (MPH)
Institut National de Police Scientifique (INPS)
VIGO (VIGO)

COUNTRY

Sweden
The Netherlands
Germany
Sweden
United Kingdom
France
France
Poland

FORLAB / FORensic LABoratory for in-situ evidence analysis in a post blast scenario

© FORLAB

Information

Grant Agreement N°
285052
Total Cost
€ 4,473,920
EU Contribution
€ 3,087,446
Starting Date
01/03/2012
Duration
36 months

Coordinator

INDRA SISTEMAS S.A
Innovation Directorate
Avenida de Bruselas 35
28108 – Alcobendas
Madrid - Spain
Contact
Francisco Javier
Hernández Crespo
Tel: +34 914 808 392
Mobile: +34 620 977 171
Fax: +34 914 806 031
E-mail: fjhernandez@indra.es
Website: www.fp7-forlab.eu

Project objectives

The FORLAB project relates to the problem of evidence collection in the post-blast scene after an IED attack. FORLAB will provide the End Users, the scientific police, with a new tool that will improve their efficiency in the investigation of the crime scene by:

» Providing fast analytical technologies to improve the evidence collection in order to reduce the number of samples to be collected and sent to the reference laboratory for detailed analysis;

» Providing a real time 3D recreation of the scene for identification of areas of the scene of higher interest and helping in the re-creation of the scene for later investigations;

» Establishing bidirectional feedback between the Command and Control Centre (where all the information about the investigation is available) and the field technicians. This will make the investigation more efficient.

FORLAB will be compatible with the in-use forensic procedures and will preserve the chain of custody.

Description of the work

The project activities of FORLAB have been broken down into 11 work packages and distributed in 36 months.

FORLAB will develop a new concept for the investigation of the post-blast scene of an IED based attack, complementing the existing forensic procedures in use by security forces in Europe.

The research in FORLAB is focused on four main areas:

» Quick elaboration of a 3D model of the scene;

» Development of technologies for in-situ searching and screening of evidence;

» Accurate positioning of the evidence and dedicated communication network;

» Information management tools for real time exploitation of the results of the investigation.

The works are structured in four stages:

The first stage will be dedicated to the System Definition with a strong involvement of End Users of the consortium. The procedures already in use by Security Forces around Europe will be reviewed and the concept of the FORLAB will be defined.

The second stage will be the development of the technologies needed based on the operational requirements of the End Users.

» LIF, LIBS, Raman and NLJD will be developed to improve the capability for searching and screening samples;

» A communication and positioning system will be developed to meet the requirements of the investigators;

» A system for real time re-creation of the post-blast scene will be developed;

» Information management tools will be developed to support operations in the Command and Control Centre where all the information on the scene will be available, in real time.

The third phase will be the integration of a subsystem in a two-step approach: Field testing of the individual technologies will be performed to obtain feedback on the achieved performance.

Finally the complete system will be validated in post-blast scenarios to verify the achieved performance. The scenarios will be carefully selected with strong involvement of End Users of the project.

Partial results of the project will be disseminated at public and restricted levels. Workshops with the stakeholders will be organized.

Expected results

» Improve the efficiency of the procedures used by European Security Forces for the investigation of a post-blast scene;

» Reduce the number of samples collected for further processing in the reference laboratory;

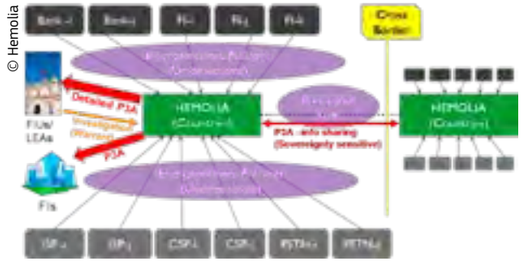
» Improve the capability to re-create the scene during the investigation in the field and for further investigations after clean-up operations;

» Present to the technician in the Command and Control Centre the real time, updated information about the investigation so that he can guide the investigators in the field of the search.

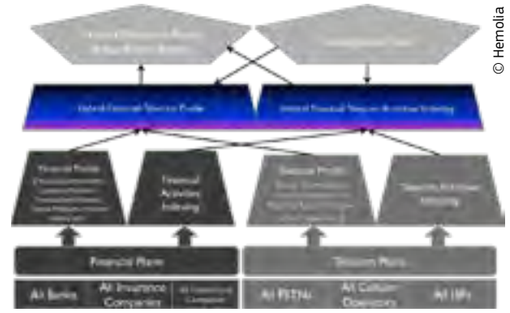
PARTNERS	COUNTRY
INDRA SISTEMAS S.A. (INDRA)	Spain
AGENZIA NAZIONALE PER LE NUOVE ECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE (ENEA)	Italy
ASTRIUM S.A.S. (ASTRIUM)	France
PANEPISTIMIO THESSALIAS (UNIVERSITY OF THESSALY) (UTH)	Greece
SPACE APPLICATIONS SERVICES NV (SAS)	Belgium
ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (APL)	Poland
NATIONAL BUREAU OF INVESTIGATION (NBI)	Finland
MINISTERIO DELLA DIFESA (RACIS)	Italy
PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW (PIAP)	Poland
SOCIETE NUCLETUDES SA (NUCLETUDES)	France
MINISTERIO DEL INTERIOR (CNP)	Spain
MINISTERE DE L'INTERIEUR (LCPP)	France

HEMOLIA / Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts

© brankatekic - istockphoto.com



© Hemolia



© Hemolia

Information

Grant Agreement N°
261710
Total Cost
€4,361,954
EU Contribution
€2,979,390
Starting Date
01/05/2011
Duration
36 months

Coordinator

VERINT SYSTEMS LTD.
33 Maskit St Herzliya,
46733 Israel
Contact
Gideon Hazzani
Tel.: +972 9 9622596
Phone: +972 9 9622596
Fax: +972 9 962 4747
E-mail:
Gideon.Hazzani@verint.com
Website:
http://verint.com/corporate/

Project objectives

HEMOLIA contributes to disrupting, deterring and dismantling criminal financing networks in the fight against terrorist activities by providing a full picture of money laundering networks. It contributes to reveal money laundering criminals and their connections to terrorism and organized crime due to the novel use of telecom information and due to the use, exchange and processing of relevant data according to the Anti Money Laundering legal framework. The enhanced approach of HEMOLIA significantly improves the detection of money laundering by encouraging the sharing of information with better use of the existing legal framework, and by ensuring the transparency and harmonization of the procedures between the Law Enforcement Agencies. The use of financial and telecom data together raise the level of Money Laundering detection. The information sharing is improved by HEMOLIA both at the national and at the international level.

Description of the work

HEMOLIA is a new generation Anti-Money Laundering (AML), intelligent, multi-agent alert and investigation system which in addition to traditional financial data makes extensive use of modern society's huge telecom data source, thereby opening up a new dimension of capabilities to all Money Laundering fighters (FIUs, LEAs) and Financial Institutes (Banks, Insurance Companies, etc.). Adding the Telecom Plane to the existing Financial Plane may improve and dramatically change AML doctrines, since another dimension is added to the analysis and investigation processes.

HEMOLIA, taking into account existing legal frameworks, will hybridize and correlate the Financial and Telecom Planes in order to create richer and more accurate alerts, intelligence and investigation tools, as well as information sharing, both nationally and internationally. A major part of HEMOLIA will be the legal research and provision of legal guidelines to all ML fighters. To respect privacy rights HEMOLIA will bring a new model of Push Privacy Preserving Alerts where all FIUs and FIs are pushed with alerts that mark a transaction or customer with a money laundering / fraud risk level or risk probability, yet without disclosing any private data. This model may have outstanding impact on AML because it means that FIs will be alerted based on data of all other FIs and based on Telecom service providers at the national and international level, opening up a new era of Money Laundering and financial crime reporting by FIs to FIUs.

Expected results

HEMOLIA's technological impact is twofold. On the one hand HEMOLIA generates an intelligent Anti Money Laundering Alerts system based on financial data providing the basis of future AML systems. On the other hand, the hybridization between financial and telecommunication data analysis is a breakthrough approach to Money Laundering prevention and contributes to the technological challenges involved in obtaining and analyzing such data.

PARTNERS	COUNTRY
Verint Systems Ltd.	Israel
MINISTRY OF JUSTICE	Denmark
OFICIUL NATIONAL DE PREVENIRE SI COMBATERE A SPALARII BANILOR	Romania
APLICACIONES EN INFORMATICA AVANZADA SA	Spain
CAPGEMINI NEDERLAND BV	The Netherlands
ZWIAZEK BANKOW POLSKICH IZBA GOSPODARCZA	Poland
UNIWERSYTET WROCLAWSKI	Poland
VERENIGING VOOR CHRISTELIJK HOGER ONDERWIJS WETENSCHAPPELIJK ONDERZOEK EN PATIENTENZORG	The Netherlands
SWITCHLEGAL ADVOCATEN	The Netherlands
TELEKOMUNIKACJA POLSKA S.A.	Poland
Industrial Research Institute for Automation and Measurements PIAP	Poland
Ernst & Young	Israel

HYPERION / Hyperspectral Imaging IED and Explosives Reconnaissance System

© Hyperion

Information

Grant Agreement N°
284585
Total Cost
€4,829,409
EU Contribution
€3,458,969
Starting Date
01/07/2012
Duration
36 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Defence & Security Systems and Technology
Department of Energetic Materials
Grindsjön Research Centre
SE-14725, Tumba, Sweden
Contact
Dr. Hans Önnerud
Tel: +46 8 5550 4058
Mobile: +46 709 277386
Fax: +46 8 5550 3949
E-mail: hans.onnerud@foi.se
Website:
www.hyperion-fp7.eu

Project objectives

The objective of HYPERION project is to develop and test a system concept for the on-site forensic analysis of an explosion. The forensic tools and procedures used will mostly be at safe stand-off detection distances. This will also include tools which can help with the identification of unexploded IEDs. The on-site data provided by the HYPERION system will be the type and amount of explosive used in the attack, the point of origin of the detonation and an assessment of the type of IED. The crime scene will be mapped using 3D-registration and in the map the positions that have been analysed in detail will be marked. The forensic tools and data will be of a quality that can be used as evidence in a court of law. The quality assured data will be electronically documented on-site and sent to the police in a timely manner at the crime scene.

After the crime scene area has been secured, the laboratory forensic sampling and analysis can be started. In HYPERION, new and validated sampling protocols will be developed.

The data from the Hyperion System will supplement the work of the bomb disposal specialist in establishing a safe crime scene.

Description of the work

A rapid response from the forensic investigation to the police is an absolute necessity in order to increase the chance of finding the perpetrators of the attack or for the possibility for the police to be proactive in the case of a series attack such as the London Underground (2005) or Madrid train bombings (2004). For the police, the first 24 hours is of major importance for a successful outcome of the crime investigation. This means that the forensic investigation and analysis of the post-blast scene of the attack has to be carried out quickly. In addition, it is of importance that the analysis data of the crime scene is of a high quality so it can be used as evidence in a trial.

Some of the information the police authorities need to know for facilitating the investigation is the type and amount of explosive that has been used in the attack. The type of explosive will reveal what kind of threat the authorities are facing and will give a hint about where the explosives could have been obtained. Explosives that are of the home-made type require the utilization of a "bomb factory", for the production. This would allow the police the opportunity to use intelligence for the localization of the bomb factory that may finally lead them in the direction of the perpetrators of the attack.

The point of origin for the detonation is needed primarily for assessing the charge size of the bomb and type of IED. It is important for the crime investigation to assess if the IED is of e.g. VBIED (Vehicle Borne IED), PBIED (Person Borne IED) or LBIED (Left Behind IED) types.

The crime scene area also needs to be well documented using ordinary high-resolution 2D photographs but most important using a 3D registration. In this 3D registration the hot-spots that have been analysed using the forensic stand-off detection tools as well as the areas that have been sampled for the laboratory forensic analysis can be marked. The 3D registration contributes to the calculation of the charge size and point of origin for detonation and facilitates the investigation and evidence presentation in the trial. The 3D crime scene registration can also be used to register the typical damage patterns in the direct vicinity of the crime scene, e.g. damage on the buildings.

On-site electronic documentation of forensic data will be performed in order to preserve the chain of custody.

Expected results

A successful system based on HYPERION would lead to a very significant reduction in the time delay of delivered forensic evidence requested by the police.

The fast crime scene investigation that HYPERION will provide can help in rapidly finding terrorists, thus being pro-active in preventing future attacks.

© Hyperion

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IAF)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
ASELSAN Elektronik Sanayi ve Ticaret A.S. (ASELSAN)	Turkey
Selex Sistemi integrati SpA (SSI)	Italy
Morpho (MPH)	France
Bundes Kriminal Amt (BKA)	Germany
VIGO (VIGO)	Poland
Turkish National Police (EGM)	Turkey
Portendo AB (Portendo)	Sweden
Tecnalia (TECNALIA)	Spain
The Swedish National Laboratory of Forensic Science (SKL)	Sweden

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

© Aluke Holwerda - istockphoto.com

Information

Grant Agreement N°
218086
Total Cost
€14,984,466
EU Contribution
€10,906,984
Starting Date
01/01/2009
Duration
60 months

Coordinator

AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY
Department
of Telecommunications
Al. A. Mickiewicza 30
PL-30059 Kraków, Poland
Contact
Prof. Andrzej Dziech
Tel: +48 12 6172616
Mobile: +48 607 720 845
Fax: +48 12 6342372
E-mail: dziech@kt.agh.edu.pl
Website:
www.indect-project.eu/

Project objectives

The **main objectives** of the INDECT Project are:

- to develop an intelligent information system for automatic detection of threats and recognition of criminal behaviour or violence;
- to develop new methods and techniques providing tools to support activities of police officers, including tools for threat detection on the Internet; this includes the development of a new type of search engine combining direct search of images and video based on watermarked contents and storage of metadata in the form of digital watermarks;
- to develop techniques for data and privacy protection in storage and transmission of data based on quantum cryptography and new methods of digital watermarking.

Description of the work

The INDECT Project aims to develop tools for enhancing the security of citizens and protecting the confidentiality of recorded and stored information as well as the privacy of involved persons. INDECT targets threat detection in both real environments (intelligent cameras) and virtual environments (computer networks, especially Internet).

The INDECT methodology addresses, firstly, the detection of specific crimes (such as Internet child pornography, trafficking of human organs, spread of botnets, viruses, malware as well as terrorism, and organised crime), then the detection of the source of the identified crimes (for example, specific criminals responsible for the crimes). It is always a human being (police, security services, etc.) who ultimately decides whether an intervention should take place once a source has been identified.

It should be underlined that the INDECT project is a research project, allowing involved European scientists to develop new, advanced and innovative algorithms and methods aimed at combating terrorism and other criminal activities, such as human trafficking and organised crime, which are affecting citizens' safety.

The INDECT Project ensures strict fulfilment of the EU ethical regulations on privacy, data protection, prevention of dual use, etc. In accordance with these regulations, a great deal of attention is paid to ethical issues, and among others, the INDECT Project will never involve processing of any personal data without the prior written consent of individuals.

Expected results

The **main expected results** of the INDECT project are:

- trial of intelligent analysis of audio-visual data for threat detection in urban environments;
- performing computer-aided detection of threats and targeted crimes in public Internet resources;
- construction of search engines for content related to child pornography and human organ trafficking;
- implementation of a distributed computer system that is capable of effective intelligent processing;
- creation of tools and technology for privacy and data protection using quantum cryptography and digital watermarking.

PARTNERS	COUNTRY
AGH University of Science and Technology (AGH)	Poland
APERTUS Távoktatás-fejlesztési Módszertani Központ Tanácsadó és Szolgáltató Közhasznú Társaság (APERTUS)	Hungary
Gdansk University of Technology (GUT)	Poland
InnoTec DATA G.m.b.H. & Co. KG (INNOTEC)	Germany
Grenoble INP (INP)	France
General Headquarters of Police (GHP)	Poland
INDESOL (INDESOL)	Spain
PSI Transcom GmbH (PSI)	Germany
Police Service of Northern Ireland (PSNI)	United Kingdom
Poznan University of Technology (PUT)	Poland
Universidad Carlos III de Madrid (UC3M)	Spain
Technical University of Sofia (TU-SOFIA)	Bulgaria
University of Wuppertal (BUW)	Germany
University of York (UoY)	United Kingdom
Technical University of Ostrava (VSB)	Czech Republic
Technical University of Kosice (TUKE)	Slovakia
X-Art Pro Division G.m.b.H. (X-ART)	Austria
Fachhochschule Technikum Wien (FHTW)	Austria

LINKSCH / Grasping the Links in the Chain: Understanding the Unintended Consequences of International Counter-Narcotics Measures for the EU


© selimaksan - istockphoto.com

Information

Grant Agreement N°
285073
Total Cost
€ 1,067,166.80
EU Contribution
€ 881,742.20
Starting Date
01/02/2012
Duration
36 months

Coordinator

UNIVERSITY OF GLASGOW
School of Humanities
2 University Gardens
Glasgow University
G12 8QQ Glasgow,
United Kingdom
Contact
Alexander Graham Marshall
Tel: +44 141 330 8581
Mobile: +44 07501986739
Fax: +44 141 330 5000
E-mail: alexander.marshall@glasgow.ac.uk

Project objectives

» design a model of current market dynamics along key illicit commodity chains that currently affect the EU;

» arrive at a typology of unintended consequences generated by current policy as it interfaces at numerous points along these two chains, taking into account both national and international efforts at control and prohibition;

» investigate via empirical investigation (fieldwork) the actual scale and nature of the most harmful of these unintended consequences, with a view to generating policy recommendations for improving them;

» and disseminate the results of this research to a wide variety of key audiences in fora that will also accommodate comparative data from studies of related areas (the cocaine trade for example).

Description of the work

This project aims to develop a model of unintended consequences utilizing the conceptual prisms of global commodity chain theory and hybrid political regimes, and treating the current prohibition regime as a hybrid political system running from closed to open access orders. This process will incorporate both a survey and summary of current state of the art thinking on unintended consequences of the contemporary prohibition regime, and a series of clearly targeted research questions which will then be pursued in active fieldwork across Morocco, Turkey, Russia, Afghanistan and Kazakhstan. Audiences to be engaged with during this process include NGOs, international agencies, government bodies and local communities. The work is novel in the manner that it seeks both to compare the soft and the hard end of the illicit drug spectrum and to look at policy activities beyond the immediately obvious ones of prohibition and harm reduction.

Expected results

The overarching aim of the project is, through examining the interface of current policy stances with current reality, to then develop and disseminate an empirically-based set of policy recommendations for engaging in a more integrated manner with downstream partners in the current drug control regime, with a view to improving unintended consequences. It is anticipated that dissemination itself will occur at a series of workshops, an international conference in Brussels, and in a series of research publications.

PARTNERS	COUNTRY
University of Glasgow (UGLA)	United Kingdom
Virtual Hand Research (VHR)	The Netherlands
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE (CNRS)	France
Coventry University (CBS)	United Kingdom
SCHOOL OF ORIENTAL AND AFRICAN STUDIES, UNIVERSITY OF LONDON (SOAS)	United Kingdom
THORNLEY MANSFIELD LTD (MANSF)	United Kingdom
UNIVERSITAET POTSDAM (POTSDAM)	Germany

LOTUS / Localization of threat substances in urban societies

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217925
Total Cost
€4,298,595
EU Contribution
€3,189,146
Starting Date
01/01/2009
End date
31/12/2011

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
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

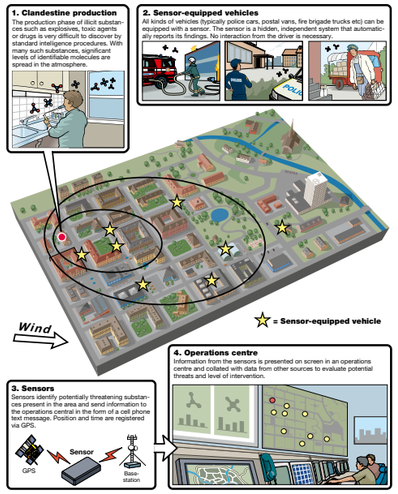
Project objectives

LOTUS set out to develop the software, hardware and concepts of operation needed to deploy an array of mobile and fixed position detection devices to locate explosive precursor chemicals and drugs in urban environments.

The LOTUS team aimed to develop a technical tool for intelligence gathering. This would enable the information obtained to be combined and confirmed with data from other sources (eg. law enforcement investigation) to accurately track and neutralize potential terrorist or organized criminal threats.

The LOTUS early warning system

Prevention and detection of threat substances is a major challenge for intelligence and police authorities. A system of mobile sensors that report significant levels of compounds in a specific or random area will give such authorities new complementary information that will significantly increase their ability to intervene at an early stage.



© Lotus

Results

A range of sensor mounts was developed and tested by LOTUS for this project. The primary detection method used was air sampling by using sensor units mounted on cars or other mobile platforms that traversed urban spaces.

Ion mobility spectrometers (IMS), differential mobility analysis and IR (infrared) absorption spectroscopy technologies were combined to detect trace elements of explosives or drugs found in the air near bomb-making factories and drug manufacturing laboratories.

Field experiments conducted in Stockholm, Helsinki and Madrid found that trace elements could be positively identified up to 45 metres away, depending on wind, temperature and humidity conditions.

In order to process and report the findings of these sensors, GSM-capable transmitters were built into each unit. These sent data reports, including potential threat detection alerts and GPS coordinates, to a central data fusion hub. Advanced analytical tools were developed to allow the hub to process and categorize readings.

If a potential operational intervention was deemed necessary (i.e. a law enforcement raid), analysis could be carried out with a range of tools to further ascertain the exact location of the threat. To avoid signal interception or pattern detection by potential adversaries, reports from each sensor were heavily encrypted and randomly transmitted.

Another element of the LOTUS system was that no interaction between the vehicle driver and the sensor was required. Indeed, the project proposes that sensors could be mounted on civilian vehicles whose users have no knowledge or need to know about what each sensor is doing.

The result would be a network of sensors randomly surveying urban areas, producing GPS pinpointed reports on potential explosive or drug manufacture locations for central assessment.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (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
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Universidad de Barcelona	Spain
Secrab Security Research	Sweden

MIDAS / The development and validation of a rapid millifluidic DNA analysis system for forensic casework samples

Information

Grant Agreement N°
242345
Total Cost
€4,688,674.80
EU Contribution
€3,231,404.60
Starting Date
01/09/2010
Duration
36 months

Coordinator

FORENSIC SCIENCE SERVICE LTD
Research and Development
Birmingham Business Park,
Solihull Parkway
B37 7YN
United Kingdom
Contact
Cecilia Buffery
Tel.: +441256771521
Mobile: +447824 434158
Fax: +441256771521
E-mail: Cecilia.buffery@fss.pnn.police.uk
Website: www.forensic.gov.uk

Project objectives

The objective of the project is to specify and develop a working instrument for the rapid analysis of DNA from samples recovered from a scene of crime. The system will be simple to use and require a single input from the user. The system will be "closed" and will operate on a fully automated basis such that a sample is simply introduced into the instrument and no further sample manipulation is required from the individual. The development of a closed system for the DNA as described above brings a number of advantages to the field of forensic science.

The core scientific and technical objectives of MiDAS are therefore to:

- Develop an agreed technical specification for the instrument and consumables;
- Deliver a prototype integrated instrument for validation;
- Evaluate the instrument in accordance with the validation plan and user requirement;
- Evaluate the instrument and cartridge designs to ensure they are fit for manufacture;
- Evaluate the legal requirements for sample handling and data transfer and protection;
- Determine system validation strategies for each of the participant member states.

Description of the work

Work Package 1 – Technical Specification
Define and agree the specification for a cartridge-based fully integrated millifluidic device for forensic DNA analysis. Calling on all project participants to draw on their own fields of expertise, WP1 will ensure the system is defined so as to fulfil internationally agreed guidelines for the analysis of DNA in a forensic context.

Work Package 2 – Prototype development
Develop and evaluate the prototype DNA analysis device. The instrument will be developed to meet the technical specifications as defined by the Technical Specification Board (TSB) in WP1 and tested against the agreed acceptance criteria. Any optimisation of the final system will take place here and implemented changes will be re-evaluated.

Work Package 3 – Instrument and software validation
Validate the prototype instrument delivered from WP2 in accordance with the validation plan delivered in WP1.

Work Package 4 – Process Integration
Define the process whereby the instrument is integrated into the forensic organisation and how it will integrate with current processes. An understanding of the technological, organisational and human implications of implementation will allow an assessment of the impact to be made.

Work Package 5 – System Validation & Implementation
Define, agree and deliver the system validation. This process is likely to be different in different jurisdictions. It is essential therefore to incorporate knowledge from all the end user partners in the consortium and to identify those parties interested in early implementation of the instrument to their own process.

Work Package 6 – Data Protection
Define, agree and deliver the Data Protection required by the project to industry standards and EU guidelines.

Work Package 7 – Device and System Scalability
Produce a number of strategic plans to allow the device to be developed allowing it to be commercially viable and to consider manufacturability.

Work Packages 8 and 9 – Dissemination and Exploitation; Project Management
Work Package 8 (Dissemination & Exploitation) together with Work Package 9 (Project Management and Reporting to the EC) will ensure effective project management and communication with the EC.

Work in WP8 will also evaluate the impact the successful implementation of a rapid DNA analysis system might have on society as a whole.

Expected results

MiDAS will deliver simple to operate automated DNA analysis technology and will validate this technology and associated processes required for its implementation, enabling forensic DNA analysis to be carried out at the crime scene. With fast results authorities will have the opportunity to rapidly compare the scene samples against DNA profiles from known criminals or results from other crime scenes held in national DNA databases. The project will have dramatic implications for both criminal justice and international security, with the ability to deliver vital intelligence results much more quickly both in a national sense and across the EU.

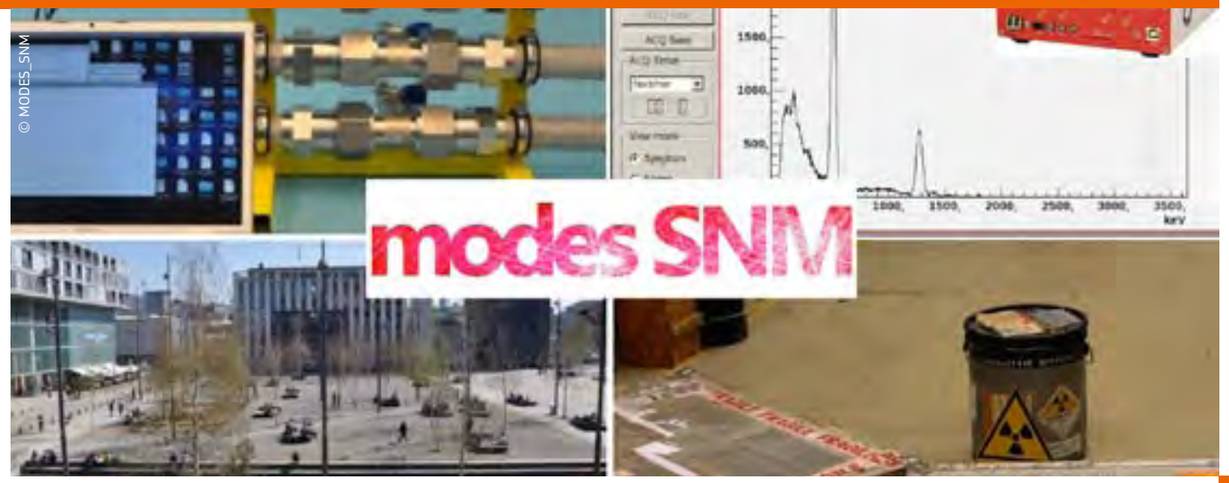
PARTNERS

Forensic Science Service Ltd (FSS)
Grid Xitek Limited (GXD)
Medizinische Universitaet Innsbruck (IMU)
Bundeskriminalamt (BKA)
Netherlands Forensic Institute (NFI)
Arizona Board of Regents (University of Arizona- UoA)

COUNTRY

United Kingdom
United Kingdom
Austria
Germany
Netherlands
United States

MODES_SNM / Modular detection system for special nuclear material



Information

Grant Agreement N°
284842
Total Cost
€ 3,282,051.20
EU Contribution
€ 2,411,633.00
Starting Date
01/01/2012
Duration
30 months

Coordinator

UNIVERSITA' DEGLI STUDI DI PADOVA
Department of Physics and Astronomy
Via Marzolo 8
35131 Padova, Italy
Contact
Giuseppe Viesti
Tel: +390498275933
Mobile: +393484115826
Fax: +390498275961
E-mail:
giuseppe.viesti@unipd.it
Website:
http://www.fisica.unipd.it/

Project objectives

Special Nuclear Materials (Highly Enriched Uranium and Plutonium) are difficult to detect, especially when masked or shielded: gamma rays and neutrons emitted by SNM have to be detected in order to increase the sensitivity against natural backgrounds. These objectives will be pursued by optimizing a novel technology recently developed allowing the detection of all relevant radiation types and the engineering of a prototype of a modular, compact, mobile detection system that will be qualified under laboratory conditions. Moreover, it will be commissioned in an on-field campaign driven by the end-user group established in the project. The campaign will focus on both performance and usability aspects including the verification of the man-machine interface. The MODES_SNM system shall satisfy two major requirements:

» improving the state-of-the-art in detection of radioactive and Special Nuclear Material in terms of sensitivity for shielded SNM;

» being usable by emergency responders in the field filling the gap between Radiation Portal Monitors and hand-held devices.

Description of the work

Starting from the pre-existing know-how of ARKTIS in the field of high pressure noble gas scintillation detectors, the MODES_SNM project aims first at a general optimization of the detector with the goal of designing and realizing the modular mobile system described below. The relevant tasks are:

» Optimization of the mechanical design of the high-pressure gas cells to minimize weight;

» Studies and development geared towards the replacement of the photomultipliers in the current system with solid state devices to reduce the size and increase robustness;

» Design of compact front-end electronics based on CAEN know-how on Digital Pulse Processing.

In parallel with the optimization task, two other tasks will be performed:

» Using ARKTIS technology, new types of detectors will be developed using noble gas cells: a gamma ray sensor and a thermal neutron sensor. The ambitious goal of this task is to develop a suite of detectors capable of gamma, fast and thermal neutron detection, and spectroscopy, all based on the same technology and using the same electronics front-end and DAQ;

» A suitable INFORMATION SYSTEM (IS) will be prepared. The IS will manage and control the detectors, including start-up operations and calibrations. It will manage and analyze the data flow from the detectors to achieve on line: 1) the irate of all radiation species compared with the background level; 2) the application of energy windowing on the fast-neutron and gamma-ray spectra to validate the alarms for weak sources; 3) the analysis of gamma ray spectra for isotope identification; 4) data fusion of all detectors and presentation of the data to the operator through a simple man-machine interface.

This MODES_SNM prototype will represent the final deliverable of the project. It will be modular and scalable, divided into so-called system blocks easily mounted and removed into/onto vehicles:

» *Block A* consists of all system electronics including power supply and battery, signal processing electronics and computing;

» *Blocks B* consists of arrays of four detectors per block, selected from the suite of gamma, fast and thermal neutron. The prototype will consist of one *Block A* and several *Block Bs*, depending on the specific deployment.

Expected results

Improved SNM detection performance to detect weak or well-shielded SNM or SNM at larger stand-off. The proposed technology incorporates thermal and fast neutron detectors along with gamma ray detectors. These measurements are complementary: their combined power is expected to improve the system performances.

Improved usability: the MODES_SNM system will offer single stage screening (rapid primary screening and threat identification), being relocatable, enhancing the portability, and allowing adaptability to varying threat situations.

PARTNERS	COUNTRY
UNIVERSITA DEGLI STUDI DI PADOVA (UNIPD)	Italy
ARKTIS RADIATION DETECTORS LTD (ARKTIS)	Switzerland
Narodowe Centrum Badań Jądrowych - National Centre for Nuclear Research (NCBJ)	Poland
Eidgenössische Technische Hochschule Zürich (ETH)	Switzerland
COSTRUZIONI APPARECCHIATURE ELETTRONICHE NUCLEARI C.A.E.N. SPA (CAEN)	Italy
UNIVERSITA DEGLI STUDI DELL'INSUBRIA (UINS)	Italy
THE REVENUE COMMISSIONERS (RC)	Ireland
THE UNIVERSITY OF LIVERPOOL (UNILIV)	United Kingdom

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

© Dwight Davis - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218237
Total Cost
€3,848,383.54
EU Contribution
€2,395,000
Starting Date
01/11/2008
End date
30/04/2011

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

Project objectives

The ODYSSEY project undertook to research and develop a secure platform for the sharing of information about gun-crime throughout the EU.

The main project objectives were:

» creation of European standards for ballistics data collection, storage and sharing;

» demonstration of a secure, interoperable platform for the management of crime information and the sharing of ballistic intelligence;

» development of techniques for the mining of data and extraction of knowledge about gun crime across the EU;

» exploitation of automated and semi-automated processing and analysis of crime data to generate 'red flags' and analysis of complex data with multiple reference models;

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

Results

The ODYSSEY project established that sharing data about gun crime between authorities and jurisdictions is technically feasible, and would bring operational benefits. These benefits would arise from the creation of trans-national data sets that could be manipulated using advanced data mining techniques to reveal hitherto hidden information.

The bedrock of these findings was the creation of a potential set of new EU standards for gun crime data defined by their own data structures, taxonomies and ontologies. These can now be taken onward to CEN, one of the EU's technical standards organisations, or ISO for evaluation and use.

A working prototype – an automated interoperable platform for data sharing – was also tested. It consisted of a secure platform for the management of crime information and the sharing of ballistics intelligence. It was tested to assess its ability to provide analysis, situation awareness and threat monitoring functionality. This was supported by a distributed technological infrastructure to store metadata in a semantic format for advanced querying and analysis.

As well as demonstrating automated 'red flag' functions, the tests also highlighted the possibility of expanding such a secure platform into other forensic areas such as DNA, fingerprints and physical evidence and other cross border policing domains such as human trafficking.

Odyssey thus demonstrated through its prototype the potential for a federated system to provide cost and time savings, as compared to current cross-EU processes.

PARTNERS	COUNTRY
SHEFFIELD HALLAM UNIVERSITY (SHU)	United Kingdom
AN GARDA SIOCHANA (AGS)	Ireland
ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA (Atos)	Spain
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
EUROPEAN POLICE OFFICE (EUR)	The Netherlands
FORENSIC PATHWAYS LIMITED (FPL)	United Kingdom
MINISTERIO DELL'INTERNO (DAC)	Italy
MIP - CONSORZIO PER L'INNOVAZIONE NELLA GESTIONE DELLE IMPRESE E DELLA PUBBLICA AMMINISTRAZIONE (MIP)	Italy
North Yorkshire Police Authority (North Yorkshire Police)	United Kingdom
SAS SOFTWARE LIMITED (SAS)	United Kingdom
SESA - COMMERCE HANDELSGMBH (SESA)	Austria
WEST MIDLANDS POLICE AUTHORITY (WMP)	United Kingdom
XLAB RAZVOJ PROGRAMSKE OPREME IN SVETOVANJE D.O.O. (XLAB)	Slovenia

OPTIX / Optical technologies for identification of explosives

© Eline Spek - Fotolia.com

Information

Grant Agreement N°
218037
Total Cost
€3,289,855
EU Contribution
€2,487,556
Starting Date
01/11/2008
Duration
54 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

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 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 into ten work packages and distributed across 42 months.

OPTIX will make 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.

The first stage will be dedicated to the System Definition. The project consortium will perform 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 on the project's activities, performance and results both at public and restricted levels, as well as defining and carrying out the initial exploitation of the outcomes and expectations 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.

PARTNERS	COUNTRY
Indra Sistemas S.A.	Spain
University of Malaga	Spain
Totalförsvarets Forskningsinstitut (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

PREVAIL / Precursors of explosives: Additives to inhibit their use including liquids

© Courtesy of Technion-Israel Institute of Technology

Information

Grant Agreement N°
241858
Total Cost
€4,295,469
EU Contribution
€3,343,162
Starting Date
01/09/2010
Duration
36 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Department of Energetic Materials
Grindsjön Research Centre
SE-147 25 Tumba
Sweden
Contact
Malin Kölhed
Tel.: +46 (0)8 5550 4197
Mobile: +46 (0)70 9277010
Fax: +46 (0)8 5550 3949
E-mail: Malin.kolhed@foi.se
Website: www.prevail-fp7.eu

Project objectives

The PREVAIL project is an innovative approach to inhibit the use of some common materials for use as precursors to explosives and to allow for easier detection. Home made explosives are easy to make from readily available materials used for legitimate purposes in everyday life. This availability attracts terrorists and criminals to manufacture and use home made explosives since military and commercial explosives are harder to come by. A great security problem for society today is the availability of these chemicals, since they are very easily attainable.

There are basically three different approaches to increase the security related to these materials: 1) limiting their availability, 2) tracking their use, or 3) limiting their usefulness as explosives or explosives precursors.

This third approach is the way forward and the goal for the PREVAIL project.

Description of the work

The PREVAIL project focuses on finding inhibitors to add to some precursors to prevent them from being used to produce home made explosives or to prevent them from being concentrated by boiling water. A second goal in the PREVAIL project is to find markers to add to certain precursors to ensure easier detection. PREVAIL will perform research into a marker/detection system rather than just the markers, in order to ensure detectability of the markers. The markers found must be environmentally friendly, non-toxic and bio-degradable. Honey bees, micro crystals and fluorescence light will be tested as detectors for these added markers, and micro encapsulation will be used for slow and controlled release. For a successful project, the objectives must be met: without causing any adverse effects on the environment or on people's health and without obstructing the legitimate use of these materials. Since this project will strongly influence manufacturers, users, legislators and governmental security agencies, the ties between the project and the stakeholders are strong. The industrial partners will identify if added inhibitors and markers need extra testing for safety. A road map for future Research and Development work and actions (as well as regulatory) will be prepared.

Expected results

A successful project will make it more difficult for terrorist and other mis-users to use some precursors to manufacture improvised explosive devices. Further, a successful project will also ensure easier detection of some precursors that today are "invisible" by adding markers and by developing a detector to that marker. Also, the usefulness of the developed additives for other precursors not included in this project will be assessed in the road map for future work, and the required future research will be indicated.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Technion – Israel Institute of Technology (Technion)	Israel
Arkema France (Arkema)	France
KCEM AB (KCEM)	Sweden
Yara International ASA (Yara)	Norway
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Wojskowy Instytut Higieny i Epidemiologii (WIHiE)	Poland
SECRAB Security Research (SECRAB)	Sweden
Inscentinel Ltd. (INSC)	United Kingdom

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

© BAYRAM TUNÇ - istockphoto.com

Information

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-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institut für Chemische Technologie (ICT)
Joseph-von-Fraunhofer-Str. 7
76327 Pfinztal (Berghausen), Germany
Contact
Dr. Norbert Eisenreich
Tel +49-721-4640-138
Fax +49-721-4640-538
E-mail: norbert.eisenreich@ict.fraunhofer.de
Website:
http://www.raptor-project.eu/
http://www.ict.fraunhofer.de/

Project objectives

The aim of the RAPTOR project is the development of a mobile, rapidly deployable and inflatable structure for ballistic protection. The project consortium is working on specific solutions to support European security forces in the prevention of, or response to, various threat scenarios. Emphasis is placed on the protection of individuals, general security at events and the protection of humanitarian workers, such as Red Cross employees.

© Raptor

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;

» Overall Project Management and Co-ordination, Accounting, Quality Assurance & Control.

Expected results

» Compilation of threat scenarios;

» Performance requirements of protection kit;

» Selection of ballistic protection textiles appropriate to security kit 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;

» Consolidation and final testing of demonstrators;

» Innovation plan, exploitation plan and feasibility study.

PARTNERS

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT)
Bundeskriminalamt (BKA)
Dr. Lange GmbH & Co KG (LANCO)
Explosia a.s. (EXPLOSIA)
P-D Interglas Ltd. (INTERGLAS)

COUNTRY

Germany
Germany
Germany
Czech Republic
United Kingdom

REWARD / REal-time Wide-Area RaDiation Surveillance System

Information

Grant Agreement N°
284845
Total Cost
€ 4,270,883.00
EU Contribution
€ 3,020,795.00
Starting Date
01/12/2011
Duration
36 months

Coordinator

CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS
Instituto de Microelectrónica de Barcelona, IMB-CNM (CSIC)
Campus Universidad Autónoma de Barcelona
08193 Bellaterra (Barcelona), Spain
Contact
Prof. Manuel Lozano
Tel: (+34) 93 594 77 00
Fax: (+34) 93 580 14 96
E-mail: Manuel.Lozano@csic.es
Website: http://www.reward-project.eu/

Project objectives

The REWARD project will develop portable, intelligent radiation detectors that can determine the flux and energy of the incoming radiation, as well as their own location. Multiple individual detectors will be integrated in a ubiquitous radiation sensing system in order to continuously monitor an area, generate an alarm if an anomalous situation is encountered and locate and identify the radiation sources. The main features of the REWARD system:

» Real-time system with wide area coverage;

» Novel solid-state detector technologies;

» Gamma and neutron detection;

» Scalable in terms of complexity and costs;

» Portable and adaptable to any type of environment.

New methods and tools will be developed for fusion, real-time and offline data mining of the radiation sensor information to discover patterns and associations of background radiation.

Description of the work

REWARD is a novel mobile system for real-time, wide-area radiation surveillance. It is based on the integration of new miniaturized solid-state radiation sensors: a CdZnTe detector for gamma radiation and a high-efficiency neutron detector based on novel silicon technologies. The sensing unit will include a wireless communication interface to send the data remotely to a monitoring base station as well as a GPS system to calculate the position of the tag.

The system will also incorporate middleware and high-level software to provide web-service interfaces for the exchange of information and an expert system to continuously analyse the information from the radiation sensor and correlate it with historical data in order to generate an alarm when an abnormal situation is detected.

REWARD will be useful for many different scenarios such as nuclear terrorism threats, lost radioactive sources, radioactive contamination or nuclear accidents. It can be deployed in emergency units and in general in any type of mobile or static equipment, but also inside public/private buildings or infrastructures. The sensing units will be highly portable thanks to their low size and low energy consumption. The complete system will be scalable in terms of complexity and cost and will offer very high precision in terms of both the measurement and the location of the radiation.

REWARD's goals will be realized by the collaborative effort of eight highly specialized, though synergistic research organizations, wireless sensor networks providers, software developers and application users.

The modularity and flexibility of the system will allow for a realistic introduction to the market. Authorities may start with a basic, low-cost system and increase the complexity based on their evolving needs and budget constraints.

Expected results

» High-efficiency radiation detectors, both for gamma radiation and for neutrons, using state-of-the-art technologies that offer superior performances, lower volume and lower cost compared to conventional sensors;

» A central monitoring and decision support system with the ability to process the data from the sensing units and to compare them with historical records;

» Small size & weight sensing tags, equipped with a positioning and communications unit, resulting in a radiation monitoring network that is capable of autonomous operation, is flexible and can easily be adapted to the needs and conditions of the specific situation;

» A security framework to ensure protection against unauthorized access to the network and data, ensuring the privacy of the communications and contributing to the overall robustness and reliability of the REWARD system.

PARTNERS	COUNTRY
Consejo Superior de Investigaciones Científicas (CSIC)	Spain
Sensing & Control Systems S.L. (S&C)	Spain
Vitrociset S.p.A (VCT)	Italy
Universität Freiburg (ALU-FR)	Germany
Instituto Tecnológico e Nuclear (ITN)	Portugal
XIE. X-ray Imaging Europe (XIE)	Germany
EDISOFT (EDI)	Portugal
Civil Protection Unit of Campania (DIP)	Italy

SALIANT / Selective Antibodies Limited Immuno Assay
Novel Technology

Information

Grant Agreement N°
242377
Total Cost
€4,498,088.80
EU Contribution
€3,362,598.60
Starting Date
01/09/2010
Duration
36 months

Coordinator

UNIVERSITY OF NEWCASTLE UPON TYNE
Institute of Cellular medicine
Kensington Terrace 6
NE1 7RU, Newcastle Upon Tyne
United Kingdom
Contact
Colin Self
Tel.: +44 191 223 5604
Fax: +44 191 223 5601
E-mail: c.h.self@ncl.ac.uk
Website: http://www.saliant.eu/

Project objectives

SALIANT is focussed on developing a hand-held device for real-time analysis of trace levels of explosives, chemicals and drugs. The key innovation is a positive detection lateral-flow test for small molecules that is highly sensitive and simple to use making it ideally suited to deployment by First Responders at crime scenes and terrorist incidents.

SALIANT offers a system based on a small bindable moiety that is first conjugated close to the binding site of a primary antibody against the analyte such that when analyte binds the antibody, the moiety can still be bound by a labelled secondary antibody. A large reagent-analogue of the analyte is also introduced, binding the analyte-unbound primary antibody, and thereby blocking binding of the secondary antibody to the moiety. Thus the more analyte present, the more binding of secondary antibody occurs and more signal is produced.

Description of the work

Lateral flow immunodiagnostics has long offered the promise of fast, high-quality testing for substances of low molecular weight. There have however been very real challenges to bringing the full power of such technology to bear in this area. What is required is a robust system in which there is no observable signal in the absence of analyte, and even low-level samples give an obvious observable signal over this zero background.

The SALIANT project is divided into several technical work packages which comprise research and development of sampling and detection methods, technology integration and demonstration of practical device application in forensic laboratories and first responder scenarios.

An initial specification process will ensure that target molecules and application scenarios are catered for in the development of sampling technologies. This is followed by development of the SAL Universal detection system and in parallel the development of the Apposition detection system to give complementary dipstick and read-out systems respectively. The device will be further developed and integrated with sampling and detection technologies before practical demonstrations in both laboratory and first responder scenarios.

A work package is also dedicated to the dissemination of results which will not only spread awareness of the knowledge gained between project partners and the wider security industry research and technology community but also promote and develop synergy between the security sector, security industry and academia through common training activities and workshops.

Expected results

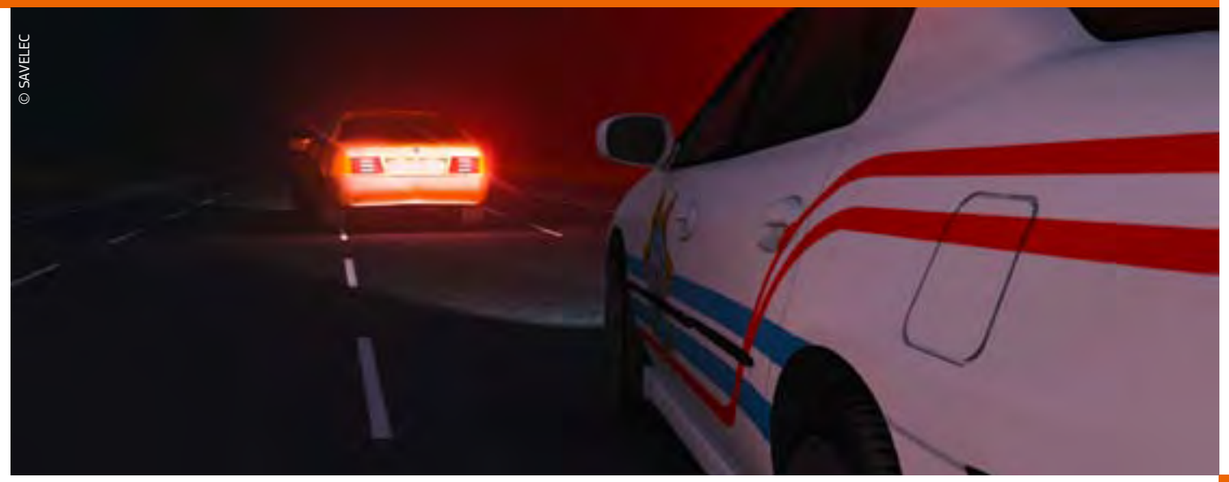
» Demonstrate Immunoassay based technology for detection of small molecular weight analytes relevant to the needs of specific end users targeting explosives and chemical toxins;

» Deliver a mobile, hand-held system for non-invasive sampling, detection, read-out, display, storage, retrieval and secure communication of results;

» Equip First Responders and Forensic Scientists at major crime scenes with high performance, simple to use real-time technology that can support risk assessment, evidence collection and information-guided investigation.

PARTNERS	COUNTRY
University of Newcastle upon Tyne (UNEW)	United Kingdom
Selective Antibodies Limited (SAL)	United Kingdom
OY REAGENA Ltd (REAG)	Finland
Indicia Biotechnology (IND)	France
Department of Justice, Equality & Law reform (FSL)	Ireland
Zilinska univerzita v ziline (UNIZA)	Slovakia
Netherlands Forensic Institute (NFI)	Netherlands
Applikon Analyzers (APP)	Netherlands
Stichting Dienst Landbouwkundig Onderzoek (DLO-FBR)	Netherlands
Centre of Excellence for Life Sciences Ltd (CELS)	United Kingdom
Kite Innovation (Europe) Limited (KITE)	United Kingdom

SAVELEC / Safe control of non-cooperative vehicles through electromagnetic means



© SAVELEC

Information

Grant Agreement N°
285202
Total Cost
€ 4,253,993
EU Contribution
€ 3,321,749
Starting Date
01/01/2012
Duration
40 months

Coordinator

INSTITUTO DE APLICACIONES DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES AVANZADAS
Advanced Projects and Testing Area
Camino de Vera s/n
46022 Valencia, Spain
Contact
Francisco Javier Díaz Jiménez
Tel: +34 963 877 278
Mobile: +34 963 877 278
Fax: +34 963 877 279
E-mail: francisco-javier.diaz@itaca-ct.es
Website: www.savelec-project.eu

Project objectives

SAVELEC aims to provide a solution for the external and safe control of a non-cooperative vehicle with no consequences for the persons inside the vehicle or other persons and objects nearby. The proposed solution is based on the use of electromagnetic means in order to disrupt the correct functioning of the electronic components inside the vehicle, which will make it slow down and stop. The SAVELEC approach is based on the premise of obtaining an optimized solution in terms of field strength, ensuring the solution complies with EU guidelines regarding human exposure to electromagnetic fields.

The ultimate purpose of the project is to design and build a car-stopper prototype to validate the technology. A real demonstration on cars going along a controlled track will be performed to assess the technology in a realistic scenario.

The involvement of security forces as end-users in the project is a key factor as regards the need to have realistic information about the use-cases, scenarios and operational parameters.

SAVELEC will propose a regulatory framework regarding the use of the technology by EU security bodies in their daily missions.

Description of the work

The work programme will start with an assessment of the use-cases and scenarios that will lead to the definition of a set of operational requirements. These activities will be performed in close cooperation with the end-user panel made up of a group of security bodies from Spain, France, Germany and Greece.

An in-depth technology review of the available state-of-the-art technology that may be considered as a reference to follow for generating the signals needed for the project's activities will be performed afterwards. This will consist of waveform generation and modulation, high-power amplifiers, power sources and ultra directional radiating elements, high bandwidth and the ability to withstand high-power signals. In addition, a series of activities are planned to review the electronic architectures and systems in cars and light commercial vehicles, providing a list of vulnerabilities regarding electromagnetic coupling effects ranked according to their expected effectiveness for the following test bench experiments.

The test bench experiments will consist of defining, designing and building automotive test bench architecture for electrical measurements. Additionally, a specific set-up for generating a wide range of electromagnetic signals will be prepared. These two elements will be used to perform a wide range of EMC experiments on sensors, electronics, wires and communications in order to identify the optimized type of signal that could lead to stopping the car as a consequence of the electromagnetic coupling.

Some additional considerations of more legal and safety aspects will be evaluated in the scope of collateral effects regarding the use of this kind of electromagnetic means: human exposure to electromagnetic fields (user, target and persons in close proximity), explosive atmosphere exposure to electromagnetic fields and an assessment of the drivers' reaction once the car goes into abnormal behaviour mode. In addition to this, specific legal and ethical studies will be carried out regarding the use of this kind of electromagnetic means by security forces. A regulatory framework will be sketched out and proposed.

Taking into consideration all the aforementioned outcomes, a breadboard-level prototype car-stopper device will be designed, manufactured and validated in an operational environment.

Expected results

SAVELEC will make technology available that could be used by law enforcement agencies in their daily missions to stop and control non-cooperative land vehicles at distance, safeguarding all the legal and ethical considerations that may arise from the use of this kind of technology. An extrapolation to the case of maritime missions could follow.

SAVELEC will demonstrate the new technology's added value to law enforcement agencies as regards their daily operations. The project will raise awareness among policy-makers and help develop the proper legal framework.

PARTNERS	COUNTRY
INSTITUTO DE APLICACIONES DE LAS TECNOLOGIAS DE LA INFORMACION Y DE LAS COMUNICACIONES AVANZADAS (ITACA)	Spain
DEUTSCHES ZENTRUM FUER LUFT - UND RAUMFAHRT EV (DLR)	Germany
MBDA FRANCE SAS (MBDA)	France
IMST GMBH (IMST)	Germany
TECHNOLOGICAL EDUCATIONAL INSTITUTE OF PIRAEUS (TEIP)	Greece
BCB INFORMÁTICA Y CONTROL S.L. (BCB)	Spain
STATENS VAG- OCH TRANSPORTFORSKNINGSINSTITUT (VTI)	Sweden
OTTO-VON-GUERICKE-UNIVERSITAET MAGDEBURG (OVGU)	Germany
AKADEMIA OZBROJENYCH SIL GENERALA MILANA RASTISLAVA STEFANIKA (AOS)	Slovakia
HELLENIC AEROSPACE INDUSTRY SA (HAI)	Greece

SAVEMED / Microstructure secured and self-verifying medicines

© SAVEMed

Information

Grant Agreement N°
261715
Total Cost
€4,278,114.80
EU Contribution
€3,144,724.50
Starting Date
01/04/2011
Duration
36 months

Coordinator

NANO-4-U GmbH
Mozartstrasse 7
D-76133 Karlsruhe
Germany
Contact
Stefan Klocke
Tel.: +49 (0)
721 182 69 68
Mobile:
+49 (0) 176 608 29 741
E-mail:
stefan.klocke@nano4u.net
Website: www.nano4u.net

Project objectives

Protecting EU citizens from counterfeit pharmaceuticals – SAVEmed offers comprehensive, user friendly and simple to implement solutions.

Counterfeit medicinal products are a threat to the health and safety of patients around the world. They range from drugs with no active ingredients to those with dangerous impurities.

They can be copies of branded drugs, generic drugs or over-the-counter drugs as well as faked implants or diagnostic devices.

In SAVEmed, self-verification security systems highly relevant for a secure track-and-trace system for the whole supply chain of a variety of medical products (e.g. solid dosage forms, pharmaceutical container, medical implants, and sterile pouches) will be developed. The key of the system is that it will work independent of external databases. It will enable the verification of the product's genuineness and its correct supply chain on-site at every step of this chain.

Description of the work

The project aim is to transfer diffractive gratings, random microstructures, micro-barcodes and contrast generating micro-prisms in hard tools. Moreover, algorithm enabling cross checking of the secure microstructures on the product (even through coatings) and on the package will be developed to ensure the highest level of security possible. In SAVEmed, this direct product marking approach will be realised for pharmaceutical tablets, injection moulded pharma caps and laminated sterile pouches.

Nevertheless the approach is applicable to nearly all other types of medical products.

The strategies of criminal organisations will be analysed and the development will be adapted to counteract these strategies. The key advantage of the implementation of secure microstructures directly in or on the medical product itself is that no chemical or biological additives and no costly changes of production lines are needed. Thus no additional approvals from regulatory agencies are required.

Expected results

- Fabrication of novel overt and covered self-verifying security features in medical products;
- Experimental proof of cost-effective manufacturing route of tools equipped with durable micro- and nanostructures;
- Fast measurement devices developed capable of identifying the secure microstructures in a variety of – coated and uncoated – medical products;
- Identification of a technology implementation strategy for different geographic regions which is based on the analysis of weak points in the dissemination of counterfeit pharmaceutical and medical products by organized crime.

PARTNERS	COUNTRY
NANO4U GmbH	Germany
Heliotis AG	Switzerland
Centre Suisse d'Electronique et Microtechnique SA (CSEM)	Switzerland
SteriPack Ltd.	Ireland
Klocke Holding	Germany
Mauer Sp. z o. o,	Poland
United Nations Interregional Crime and Justice Research Institute (UNCRI)	Italy

SCIIMS / Strategic Crime and Immigration Information Management System

Information

Grant Agreement N°
218223
Total Cost
€3,595,562.80
EU Contribution
€2,318,996.45
Starting Date
01/11/2009
Duration
36 months

Coordinator

BAE SYSTEMS INTEGRATED SYSTEM TECHNOLOGIES LIMITED
Commercial Department
Lyon Way, Frimley,
Camberley
GU16 7EX, Surrey
United Kingdom
Contact
Claire Dance
Tel: 01276 603226
Mobile:
+44 (0)7793 423771
Fax: +44 (0)1276 603111
E-mail: claire.dance@baesystems.com
Website: http://www.sciims.co.uk/index.html

Project objectives

» Development and application of Information Management (IM) and Information Exploitation (IX) techniques enabling information to be fused and shared nationally and trans-nationally within a secure information infrastructure in accordance with European crime and immigration agencies' information needs;

» Development and application of tools to assist decision making in order to predict and analyse likely People Trafficking and People Smuggling sources, events and links to organised crime;

» Utilisation and enhancement of existing 'State of the Art' products to develop and incorporate new capabilities, 'Beyond State of the Art' into product baselines in order to speed up the introduction of new innovative techniques, technologies and systems.

Description of the work

People Trafficking and People Smuggling have long been a problem for European Governments, adversely affecting the security of their citizens. In many cases women and children are forced into the sex trade and subjected to labour exploitation. In formulating the SCIIMS project the consortium will focus upon an overarching research question from which the developed capabilities, demonstration and experiments will be focussed:

"In the European Union context how can new capabilities improve the ability to search, mine and fuse information from national, trans-national, private and other sources, to discover trends and patterns for increasing situational awareness and improving decision making, within a secure infrastructure to facilitate the combating of organised crime and in particular people trafficking/ smuggling to enhance the security of citizens?"

The SCIIMS Consortium will utilise 'State of the Art' products which will form the base capability on which to develop new innovative capabilities and technologies. This approach is designed to provide an early exploitation opportunity for the consortium and the user groups involved.

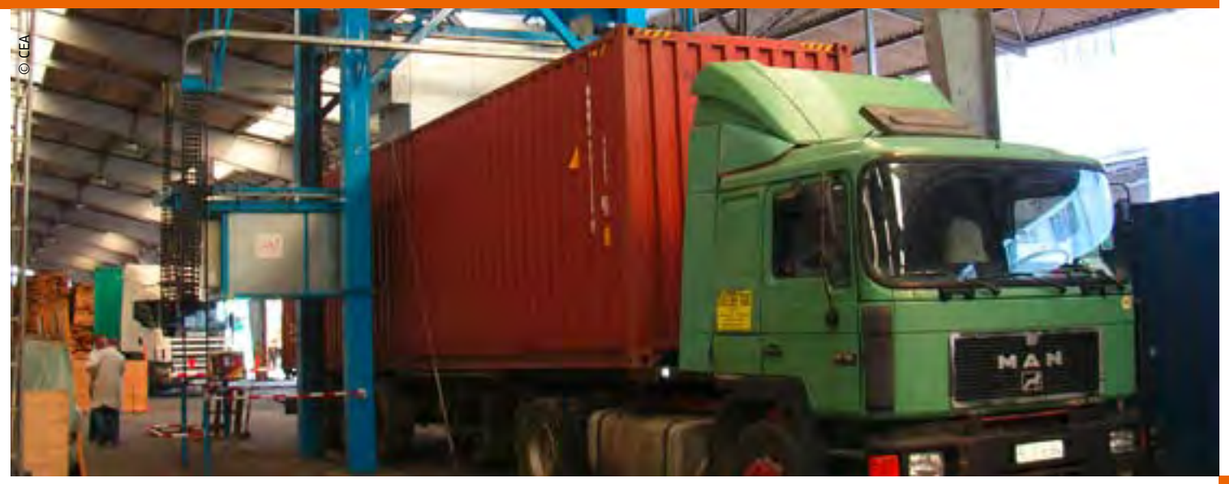
Expected results

Research into Information Management and Information Exploitation techniques to help in combating organised crime. SCIIMS will research and develop 'beyond state of the art' technologies and techniques to search, mine and fuse information from heterogeneous data sets. Visualisation techniques of information for sense-making will be improved in order to conduct analysis, detect trends and improve the understanding and detection of People Trafficking and Smuggling.

SCIIMS will do this through a research capability development and experimentation programme which will investigate both existing technologies and those currently being researched and developed. This will allow European agencies to make more effective decisions and interventions to improve the security of citizens and in particular the fight against organised crime.

PARTNERS	COUNTRY
BAE SYSTEMS INTEGRATED SYSTEM TECHNOLOGIES LTD	United Kingdom
INDRA SISTEMAS S.A. (INDRA)	Spain
COLUMBA GLOBAL SYSTEMS LTD (Columba)	Ireland
ELSAG DATAMAT S.P.A. (ED)	Italy
DENODO TECHNOLOGIES SL (DENODO)	Spain
Magyar Tudomanyos Akademia Szamitastechnikai Es Automatizalasi Kutato Intezet (Sztaki)	Hungary
UNIVERSIDADE DA CORUNA (UDC)	Spain
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
GREEN FUSION LIMITED (DATA FUSION)	Ireland

SCINTILLA / Development of detection capabilities of difficult to detect radioactive sources and nuclear materials



© CEA

Information

Grant Agreement N°
285204
Total Cost
€ 3,867,616.38
EU Contribution
€ 3,023,652.12
Starting Date
01/01/2012
Duration
36 months

Coordinator

COMMISSARIAT À L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
DRT/LIST/ DCSI/ LCAE
CEA Saclay, Bât 516,
Point courier n°72
91191 - Gif sur Yvette - France
Contact
Guillaume SANNIE
Tel: +33 1 69 08 51 88
Fax: +33 1 69 08 60 30
E-mail:
guillaume.sannie@cea.fr
Website: Not available
(public website due month 6)

Project objectives

SCINTILLA aims at building an innovative and comprehensive toolbox of devices and best-of-breed technologies for the enhanced detection and identification of difficult to detect radioactive sources and nuclear material:

» Dealing with the challenge of masked and shielded material;

» Developing effective solutions, which are reliable, portable/mobile and cost effective;

» Finding a reliable replacement for Helium-3, which is the major consumable for today's RPM (Radiation Portal Monitors) devices for neutron detection and has become close to unavailable in the European Union.

Description of the work

SCINTILLA will cover a broad range of different usage cases including automatic screening of moving targets such as people, cars and trucks, the inspection of large containers as well as the detection of radioactive sources in bombs.

The SCINTILLA Test-bed Service and annual Technology Benchmarks will respectively support and select the technologies; they will also be open to third-party developments.

In addition to more technical criteria such as sensitivity, discrimination between neutron and gamma radiation and the minimisation of false alarms, SCINTILLA will assess technologies with respect to practical criteria such as portability, mobility and cost-benefit ratios.

The resulting selection of best-of-breed technologies will then be integrated into full prototype devices, which will be ready for assessment in selected usage cases under (close to) real-life conditions.

To reflect the different TRL of technologies under development the project will proceed in two stages with usage assessments at midterm and project end.

The SCINTILLA Toolbox will be provided with User Guidelines and a Technology Handbook for integrators.

SCINTILLA will also develop and promote communication protocols and standards.

Around the Test-bed and Benchmark services a sustainable SCINTILLA Partnership Network will be built, a worldwide community of technology providers, experts and users, around the topic of detection technologies.

Expected results

SCINTILLA will contribute to minimise the risk of use or dissemination of difficult to detect radioactive sources in the population.

By proposing effective substitutes for Helium-3, SCINTILLA will contribute to the resolution of a strategic threat to Europe: the increasing difficulty to procure Helium-3 for RPMs.

The Test-bed services, Technology Benchmarks and Partnership Network will ensure Europe stays at the front of this area which is critical for the security of Europe and its citizens.

PARTNERS	COUNTRY
COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)	France
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
ISTITUTO NAZIONALE DI FISICA NUCLEARE (INFN)	Italy
ANSALDO NUCLEARE SPA (ANSALDO)	Italy
CENTRE FOR ENERGY RESEARCH – HUNGARIAN ACADEMY OF SCIENCES (IKI)	Hungary
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V (FhG INT)	Germany
ARTTIC (ART)	France
SAPHYMO SAS (SAPHYMO)	France
SYMETRICA SECURITY LTD (SYMETRICA)	United Kingdom

TIRAMISU / Toolbox Implementation for Removal of Anti-Personnel Mines, Submunitions and UXO

Information

Grant Agreement N°
284747
Total Cost
€ 19,798,269.08
EU Contribution
€ 14,934,745.00
Starting Date
01/01/2012
Duration
48 months

Coordinator

ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL
Polytechnic Faculty
30, Avenue de la Renaissance
1000 – Brussels - Belgium
Contact
Yvan Baudoin
Tel: +32 2 7426553
Fax: +32 2 7426547
E-mail:
yvan.baudoin@rma.ac.be
Website: www.rma.ac.be

Project objectives

Anti-personnel landmines and unexploded ordnance (UXOs) represent an important obstacle in the transition from crisis to peace for war-affected countries. They threaten post-conflict development and welfare.

The objective of the TIRAMISU project is to provide the Mine Action community with a toolbox to assist in addressing the many issues related to Humanitarian Demining and thus promoting peace, national and regional security, conflict prevention, social and economic rehabilitation and post-conflict reconstruction.

The tools in development are divided in two main categories:

» Demining planning tools, which will help locate the threats and define the contaminated areas;

» Detection and disposal tools, which will physically neutralise mines and UXOs and improve operators' safety. In this context, in-depth training will be provided to the users.

These tools will be tested and validated in mine-affected countries and will also benefit from state-of-the-art technologies (robots, UAV...).

Description of the work

TIRAMISU is divided into 10 modules that will cover all the different aspects of Humanitarian Demining. They are:

» Land Impact Survey: tools enabling the prioritisation of the areas most affected and the efficient use of the other modules in a given situation. These tools will make use of remote sensing and decision support systems;

» Non-Technical Survey & Advanced General Survey: tools to facilitate land release;

» Technical Survey: tools to detect indicators of probable presence of landmines/UXOs;

» Ground-based Close-in Detection: tools, such as advanced metal detectors, Ground Penetrating Radars and novel chemical sensors;

» Stand-off Detection: tools to detect mines, submunitions or explosives at close range with remotely controlled Micro (Unmanned) Aerial Vehicles (MAV/UAV) or flying biosensors (honeybees);

» Disposal of ERW (Explosive Remnants of War): tools to protect deminers or vehicles against explosions;

» Mine Risk Education: tools to assist in Mine Risk Education activities;

» Training: tools aiming at developing capacity building and enabling the user uptake of the tools developed;

» Mine Action mission management: tools to improve planning and execution of Mine Action missions;

» Standards: this module includes the current and in-progress or proposed CEN Workshop Agreements (CWA).

In order to test the tools and to also increase the confidence of the Mine Action community in these tools, test and validation campaigns will be organised in several mine-contaminated countries.

The project is steered by two boards that will be involved in every step of the development of TIRAMISU to ensure that the tools being developed will really be useful to the Mine Action community. The End-User Board will assist in the definition of the needs and the assessment of the usefulness of the tools. The Project Advisory Board will provide an independent view on the tools' design and development and on any ethical issues that could arise in the course of the project.

Expected results

The TIRAMISU Toolbox will offer a comprehensive modular structure covering the different Mine Action processes, from Land Impact Survey to the safe Mine Clearance Actions and disposal. The tools will be designed with the active participation of end-users, and tested and validated in mine-contaminated countries.

It is expected that these tools will benefit Mine Action Centres and national Mine Action authorities, private companies and NGOs working in Mine Action, as well as European and UN agencies.

PARTNERS	COUNTRY
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
UNIVERSITA DEGLI STUDI DI GENOVA (DIMEC)	Italy
DEUTSCHES ZENTRUM FUER LUFT - UND RAUMFAHRT EV (DLR)	Germany
INSTITUTO DE SISTEMAS E ROBOTICA-ASSOCIACAO (ISR-UC)	Portugal
AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES (CSIC)	Spain
UNIVERSITA DEGLI STUDI DI CATANIA (UNICT)	Italy
INSTYTUT MASZYN MATEMATYCZNYCH (IMM)	Poland
DIALOGIS UG (HAFTUNGSBESCHRANKT) (DIALOGIS)	Germany
SVEUCILISTE U ZAGREBU - GEODETSKI FAKULTET (FGUNIZ)	Croatia
HRVATSKI CENTAR ZA RAZMINIRANJE-CENTAR ZA TESTIRANJE RAZVOJ I OBUKU DOO (CTDT)	Croatia
NOVELTIS SA (NOVELTIS)	France
PARIS-LODRON-UNIVERSITÄT SALZBURG (PLUS)	Austria
WOJSKOWY INSTYTUT TECHNIKI INZYNIERYJNEJ IM PROFESORA JOZEFA KOSACKIEGO (WITI)	Poland
THE UNIVERSITY COURT OF THE UNIVERSITY OF ST ANDREWS (USTAN)	United Kingdom
UNIVERSITE LIBRE DE BRUXELLES (IGEAT)	Belgium
SPINATOR AB (SPINATOR)	Sweden
PROTIME GMBH GESELLSCHAFT FUR INFORMATIONSLOGISTIK (PROTIME)	Germany
SPACETEC PARTNERS SPRL (STP)	Belgium
EUROPEAN UNION SATELLITE CENTRE (EUSC)	Spain
VALLON GMBH (VALLON)	Germany
I.D.S. - INGEGNERIA DEI SISTEMI - S.P.A. (IDS)	Italy
PIERRE TRATTORI DI GIOVANNI BATTISTA POLENTES & C SNC (PIERRE)	Italy
BRIMATECH SERVICES GMBH (BRIMATECH)	Austria
COMITE EUROPEEN DE NORMALISATION (CEN)	Belgium

TWOBIAS / Two stage rapid biological surveillance and alarm system for airborne threats

© il-fede - Fotolia.com

Information

Grant Agreement N°
242297
Total Cost
€4,935,083.65
EU Contribution
€3,577,834
Starting Date
01/07/2010
Duration
36 months

Coordinator

NORWEGIAN DEFENCE RESEARCH ESTABLISHMENT
Norway
Contact
Janet Martha Blatny
Tel.: +47 63807827
Fax: +47 63807509

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:

» Establish a command and control software system for TWOBIAS in order to reliably function at a real-life site;

» Test and evaluate biodetectors in large-scale chamber tests, and analyse background interference detection signals under real-life conditions;

» Enhance the performance of TWOBIAS using advanced data classification methods;

» 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 from 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 the air;

» 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.

© Twobias

PARTNERS

Norwegian Defence Research Establishment (FFI)
Centre d'Etudes du Bouchet (DGA)
Dycor Global Solutions Ltd (DGS)
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Q-linea AB (QL)
Státní ústav jaderné, chemické a biologické ochrany, v. v. i. (SCB)
Totalförsvarets Forskningsinstitut (FOI)
Thales SA (TRT)
Thales Security Solutions and Services S.A.S (TSS)
Uppsala universitet (UoU)

COUNTRY

Norway
France
Cyprus
The Netherlands
Sweden
Czech Republic
Sweden
France
France
Sweden

UNCOSS / Underwater coastal sea surveyor


© Fotolia.com

Information

Grant Agreement N°
218148
Total Cost
€4,119,638.72
EU Contribution
€2,763,818.61
Starting Date
01/12/2008
Duration
44 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Le Ponant de Paris
25 Rue Leblanc
F-75015 Paris Cedex 15
France
Contact
Guillaume Sannie
Tel: +33169085188
Website:
http://www.uncoss-project.org/

Project objectives

The waterways are becoming more and more 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 natures 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 the UNCOSS project is to provide tools for the non-destructive inspection of underwater objects mainly based on neutron sensors. The technology used has already been experimented with for Land Protection (especially in the frame of the FP6/Euritrack project). The application of this technology for underwater protection will be a major achievement.

The classic approach to 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.


fig.1


fig.2


fig.2

© Uncoss

Figure 1: Torpedo from World War II
Figure 2: Antiship mines

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 ports and elsewhere.

The final demonstration campaign shall be carried out 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

© Uncoss

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)

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
ECA S.A.	France
Ruder Boskovic Institute (RBI)	Croatia
Laseroptronix	Sweden
Jozef Stefan Institute (JSI)	Slovenia
A.C.T.d.o.o. (ACT)	Croatia
Port Authority Dubrovnik	Croatia
Port Authority Bar	Montenegro
Port Authority Vukovar	Croatia
Mednarodna podiplomska šola Jožefa Stefana (MPS)	Slovenia

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

© Lv Design - Fotolia.com

Information

Grant Agreement N°
218197
Total Cost
€4,483,794
EU Contribution
€3,229,034
Starting Date
01/08/2009
Duration
48 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
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

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 threatening human behaviour.

ADABTS aims to develop models for threatening 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 the 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 with the defined behaviour primitives, and thus detect the presence of the (potentially) threatening behaviour.

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 to adapt to the context.

ADABTS will adapt the above algorithms to run on commercially available, low-cost hardware architectures consisting of multi-core CPUs combined with several multi-stream GPUs (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 and 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:

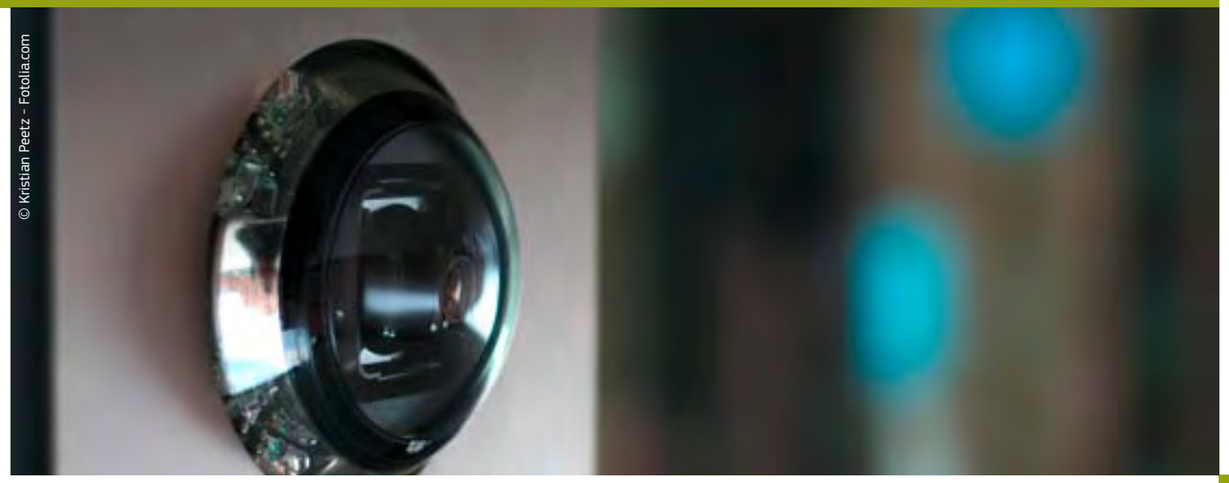
» Understanding of the user needs for automatic detection of threatening behaviour in crowds and new definitions of and methods for describing such behaviour;

» Methods and algorithms for threatening 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.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Stiftelsen SINTEF (SINTEF)	Norway
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Universiteit van Amsterdam (UvA)	The Netherlands
Institute of Psychology – Ministry of the Interior (IPMI)	Bulgaria
BAE Systems (Operations) Ltd (BAE)	United Kingdom
Home Office Scientific Development Branch (HOSDB)	United Kingdom
Detec AS (Detec)	Norway

ARENA / Architecture for the recognition of threats to mobile assets using networks of multiple affordable sensors



© Kristian Peetz - Fotolia.com

Information

Grant Agreement N°
261658
Total Cost
€4,861,867.60
EU Contribution
€3,178,761.00
Starting Date
16/05/2011
Duration
36 months

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
Swedish Defence Research Agency
Gullfossgatan 6
STOCKHOLM, 164 90
Sweden
Contact
Åsa Waern
Tel: +4613378084
E-mail: asa.waern@foi.se
Website: http://www.foi.se/FOI/templates/startpage____96.aspx

Project objectives

The objective of ARENA is to develop methods for automatic detection and recognition of threats, based on multisensory data analysis. Research objectives include:

- To robustly and autonomously detect threats to critical mobile assets in large unpredictable environments;
- To reduce the number and impact of false alarms and work towards optimized decision making;
- To demonstrate automatic threat detection for the land case (truck);
- To demonstrate an integrated, scalable and easy to deploy monitoring system;
- To assess automated threat detection for the land case (train) and the maritime case (vessel, oil rig);
- To evaluate detection performance and contribute to standards;
- To respect and respond to social, legal and ethical issues arising from the design, implementation and deployment.

Description of the work

ARENA addresses the design of a flexible surveillance system for detection and recognition of threats towards deployment on mobile critical assets/platforms such as trucks, trains, vessels, and oil rigs. There is a substantial end-user need for intelligent and continuous proactive monitoring to enable situational awareness and determination of potential threats enabling timely and appropriate response.

ARENA has a stakeholder group which consists of representatives from the land case and the maritime case.

The project will be carried out as an iterative systems development project. First, a threat analysis, development of user scenarios and user interaction will result in user requirements of the ARENA surveillance system for mobile platforms (WP2). The input will be used to develop the generic system architecture (WP3) and the different components necessary for the testbed (developed in WP4); the object assessment (WP5), the situation assessment (WP6), and the threat recognition (WP7). These components will to a large extent be developed in parallel, thus requiring much interaction between the work packages. The results from WP3, WP5, WP6 and WP7 (the latter including inputs from WP5 and WP6) are continuously integrated in the system testbed developed in WP4.

Once the testbed is completed, the remainder of the project deals with demonstrations and evaluations of the ARENA concept and system, providing experiences and feedback on the user requirements, the generic architecture, the different research areas related to the components and the testbed/system itself. Demonstrations will take place using the scenarios as developed in WP2, involving a truck case. Evaluation will be performed by means of testing and experimentation, using a thoroughly designed testing methodology. The Stakeholder Group will be involved throughout the Project.

Expected results

The expected result of ARENA is a system consisting of low cost sensors which are easy to deploy. The system will be adaptable to various platforms and increase the situation awareness.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
BMT GROUP LIMITED (BMT)	United Kingdom
ITTI Sp.zo.o. (ITTI)	Poland
SAGEM DEFENSE SECURITE (Sagem DS)	France
Morpho (MPH)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
THE UNIVERSITY OF READING (UoR)	United Kingdom
PRO DOMO SAS (PRODOMO)	France

BASYLIS / moBile, Autonomous and affordable SYstem to increase security in Large unpredIctable environmentS

© bluefern - Fotolia.com

Information

Grant Agreement N°
261786
Total Cost
€2,989,194.80
EU Contribution
€2,037,265.00
Starting Date
01/05/2011
Duration
24 months

Coordinator

IP SISTEMAS
Calle Anabel Segura
nº 7- Planta B
28108, Alcobendas, Madrid
Spain
Contact
Sonia Gracia Anadón
Tel: +34 91 203 87 09
Mobile: +34-610.201.908
Fax: +34 91 209 78 28
E-mail: sgracia@indra.es
Website: www.basylis.european-project.eu

Project objectives

The general objective of the project is to contribute to increase the security of European citizens by the development of an adaptable and affordable system for temporal or permanent protection of facilities, perimeters and people using a combination of multiple technologies.

The characteristics of the system to be developed will be the following:

- Radar;
- Ladar;
- UGS Acoustic (UNAVE);
- COTS Integration Board;
- UGS Metal;
- Bracelets and panic buttons;
- Seismic UGS Optimization;
- Video Intelligence;
- Behavioural analysis.

The specific objectives leading to the achievement of the general objective of the project are the following:

- To develop the new sensors (radar, ladar, UNAVE, UGS, bracelets, video intelligence), focusing on their potential cross-integration with the others, and devoted to refugee camp protection;
- To develop the main integration software and behavioural analysis enabling the integration of the sensors and the behavioural processing of the data;
- To integrate all the software and hardware developments in the selected demo scenario;
- To test and to improve the whole system in the demo scenarios executing a thorough testing and evaluation program;
- To perform demonstrations of the developed system with the end users involved in the project and with additional stakeholders as needed;
- To elaborate a technological and application roadmap for further research needs and user involvement.

Description of the work

Civil installations such as power plants are often located in wide and remote areas. In the future, the number of small distributed facilities will increase as a direct result of new European environmental policies aimed at increasing societies' resilience to climate change. However, the protection of fragmented assets will be difficult to achieve and will require portable security systems that are affordable to those in charge of their management. The BASYLIS project aims to address these issues by developing a low-cost smart sensing platform that can automatically and effectively detect a range of security threats in complex environments. The principal obstacles to early threat detection in wide areas are of two types: functional (e.g. false-alarm rate) and ethical (e.g. privacy). Both problems are exacerbated when either the installations or the environments are dynamic. Potential solutions are unaffordable for most of the potential users.

The BASYLIS system will consist of a transportable security platform capable of detecting a wide range of predetermined security threats. The prototype design will include five highly sensitive sensors exploiting different parts of the spectrum: radio, magnetic, seismic, acoustic and optical waves, as well as images via intelligent video.

The information gathered by these sensors is then brought together into an information layer composed of three levels: multi-sensor integration, image processing and risk assessment.

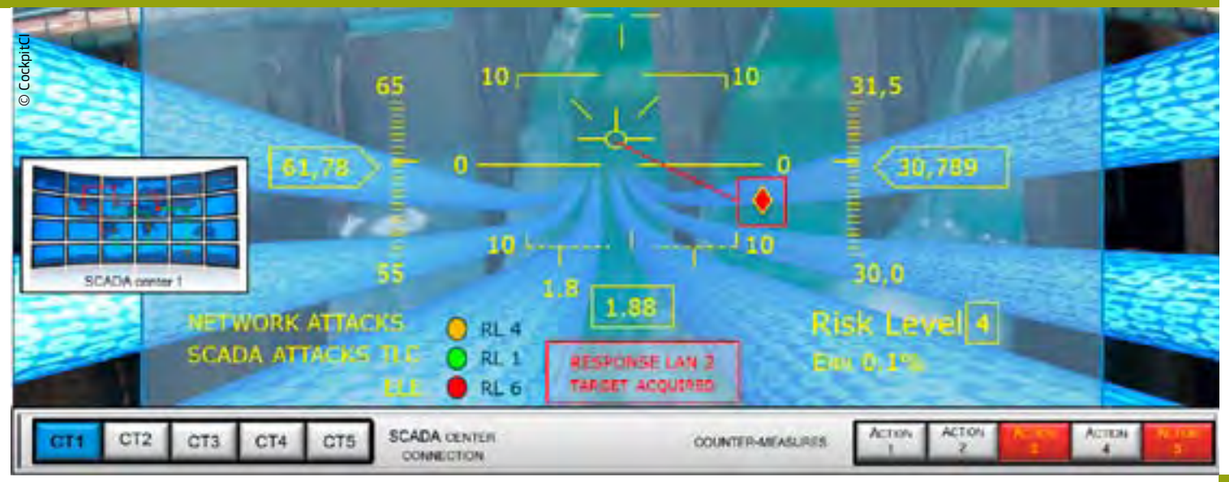
The BASYLIS system will be characterized by a high performance and a high usability index. The engagement of end users in the specification and validation of the design has been considered from the start of the project, ensuring that the design of the final system meets their needs.

Expected results

BASYLIS is a capability project based on the research, development and adaptation of new sensor technologies and processing software for automatic detection and recognition of threats to critical assets in large unpredictable environments.

PARTNERS	COUNTRY
IP SISTEMAS (IP)	Spain
NEW TECHNOLOGIES GLOBAL SYSTEMS (NTGS)	Spain
UNIVERSITA DEGLI STUDI DI FIRENZE (UFL)	Italy
TERMA A/S (TERMA)	Denmark
MICROFLOWN (MICROFLOWN)	Netherlands
MIRASYS OY (MIRASYS)	Finland
UNIVERSIDAD POLITECNICA DE MADRID (UPM)	Spain
UNIVERSITY COLLEGUE LONDON (UCL)	United Kingdom
CENTRO NACIONAL DE PROTECIÓN DE INFRAESTRUCTURAS (CNPIC)	Spain

COCKPITCI / Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures



Information

Grant Agreement N°
285647
Total Cost
€ 4,234,558.35
EU Contribution
€ 2,986,675.00
Starting Date
01/01/2012
Duration
36 months

Coordinator

SELEX SISTEMI INTEGRATI SPA
Large Systems Business Unit
Via Tiburtina Km 12,400
00131 Rome, Italy
Contact
Antonio Graziano
Tel: +39 06 4150 2017
Mobile: +39 331 6231584
Fax: +39 06 4150 2356
E-mail:
agraziano@selex-si.com
Website: www.cockpitci.eu

Project objectives

CockpitCI aims to improve the resilience and dependability of Critical Infrastructures (CIs) by the automatic detection of cyber threats and the sharing of real-time information about attacks among CI owners.

CockpitCI aims to identify, in real time, the CI functionalities impacted by cyber-attacks and assess the degradation of CI delivered services.

CockpitCI aims to classify the associated risk level, broadcast an alert at different security levels and activate a strategy of containment of the possible consequences of cyber-attacks.

CockpitCI aims to leverage the ability of field equipment to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety.

Description of the work

CockpitCI will design and develop a system capable of detecting malicious network traffic which may disrupt the correct functioning of a SCADA system and hamper its normal operability.

CockpitCI will rely on a unifying approach across the Critical Infrastructures modelling domain. Models and software tools will be used to predict the Quality of Services (QoS) delivered by SCADA systems early. Indicators of SCADA QoS will be computed using an adequate representation of the technological networks supporting SCADA services, including including multi-phased cyber attacks and accidental failures.

CockpitCI will aggregate the information of potential cyber-attacks induced on SCADA systems or telecommunication systems used to support the operation of CIs, and identify the potential unsecured area of the CIs.

CockpitCI will research traffic monitoring and attack detection. New machine learning based approaches for unusual traffic event detection will be analysed and several typologies of cyber-threats will be modelled, as will the cyber-interdependencies of the composite CIs system.

CockpitCI will provide a framework to allow the community of CI owners to exchange real-time information about attacks, extending the capabilities developed in the previous MICIE project. It will extend the prediction capabilities by considering cascading events induced by faults and cyber attacks and also develop a strategic analysis tool able to calculate the potential threat of coordinated cyber-attacks on CIs.

Expected results

The main expected result is the demonstration that the convergence among physical security, cyber security and business continuity is possible with positive fallouts for all the involved players. Benefits will arise from the security point of view thanks to the availability of a larger amount of field data, while, from the business point of view, a better real-time risk evaluation will allow a tailored definition of service level agreement and the avoidance of large domino effects.

PARTNERS	COUNTRY
SELEX Sistemi Integrati SpA (SELEX-SI)	Italy
Centre de Recherché Public Henri Tudor (CRPHT)	Luxembourg
Consortium for the Research in Automation and Telecommunication University of Rome - "La Sapienza" (CRAT)	Italy
Dipartimento Informatica e Automazione – Università di Roma Tre (ROMA3)	Italy
Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA)	Italy
Israel Electric Corp (IEC)	Israel
itrust consulting s. à r. l. (ITRUST)	Luxembourg
Multitel asbl (Multitel)	Belgium
University of Coimbra Faculdade de Ciências e Tecnologia (UC)	Portugal
University of Surrey (SURREY)	United Kingdom

COPRA / Comprehensive European Approach to the Protection of Civil Aviation

© Kristian Peetz - Fotolia.com

Information

Grant Agreement N°
261651
Total Cost
€1,303,301.80
EU Contribution
€986,382
Starting Date
01/09/2011
Duration
18 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Ernst-Mach-Institut (EMI)
Hansastr. 27c
80686 Munich
Germany
Contact
Dr. Tobias Leismann
Tel: +49 761 2714 402
Mobile: +49 170 769 5101
Fax: +49 761 2714 1402
E-mail: Tobias.Leismann@emi.fraunhofer.de
Website:
www.emi.fraunhofer.de

Project objectives

Provide the European Commission and Member States with clear guidelines for future RTD activities:

- Compilation of a comprehensive overview of end-user and customer aviation security requirements including boundary conditions like legislation and standardization issues;
- Analysis of new and emerging threats to aviation security using an all-hazard approach. Development of a hierarchy of threats reflecting factors like impact, likelihood and timescale of threats to become relevant for Europe;
- Identification of current and future security technologies taking into account new operational procedures mitigating the new threats;
- Systematic analysis and combination of technologies and procedures into holistic security concepts including organizational paradigms, social acceptability and cost-benefit aspects;
- Creation of a roadmap of the European requirements on future aviation security research and recommendations for standardization, test and certification issues.

Description of the work

Preparedness and protection against new threats while ideally improving the protection of passenger privacy, mobility and public acceptability in the future aviation security system strongly depends on the changing requirements of the stakeholders involved as well as the legal context in the European Union.

Workpackage 1 (WP1) will analyse these requirements (mid-term trends). The starting point is the state of the art description of the security systems. Further, the European legislative context will be described (preparation of standardization questions).

WP2 will identify present, new and emerging threats with impact on the future. Information will be gathered from previous and ongoing European and national research projects. It will also consider new developments for an all-hazard approach to providing a comprehensive prioritized list (e.g. destructive impact, availability) of threats to the aviation system.

WP3 will collect and analyse present security technologies and opportunities arising from new technologies (by state of development, required development costs, maturity and cost estimations of the measures). New concepts (technologies, processes) will be depicted.

WP1, WP2, and WP3 results will be merged in WP4: stakeholder requirements, threats and security solutions will be brought together into a multi-criteria analysis to assess security concepts. Assessment factors: cost-benefit analysis, socio-cultural acceptance and privacy issues, the European legal framework and standards, possible synergistic effects between security concepts and aviation development in general.

In WP5 the results of WP4 will be translated into a research roadmap and recommendations for future RTD activities.

Management (communication/reporting to European Commission, workshop planning) of COPRA is performed in WP6.

The WPs will be supported by expert groups in workshops (WS). WP1 and WP2 through workshop WS1. WP3 will be supported in WS2. WP4 will start with the output of WS2. WP5 results will be presented in WS3.

Expected results

- a comprehensive list of threats to the aviation system through an all-hazard approach;
- a catalogue of security technolgies;
- a roadmap of the European requirements for future aviation security research;
- recommendations for standardization, test and certification issues.

This all takes into account passenger privacy, mobility, public acceptability, stakeholder requirements and the legal context of the European Union.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)	Germany
European Business School (EBS)	Germany
Airbus S.A.S. (AIR)	France
European Organisation for Security (EOS)	Belgium
Fraport AG Frankfurt Airport Services Worldwide (FRA)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Morpho (MPH)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Smith Heimann GmbH (SMI)	Germany
University of Ljubljana (UL)	Slovenia
KLM – Royal Dutch Airlines NV (KLM)	The Netherlands

DEMASST / Demo for mass transportation security: roadmapping study


© NZ photo - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218264
Total Cost
€1,840,549.50
EU Contribution
€956,558.96
Starting Date
12/01/2009
End Date
11/05/2010

Coordinator

TOTALFORSVARETS FORSKNINGSINSTITUT
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

Project objectives

A so-called 'phase one' road-mapping project, DEMASST's goal was to identify the research priorities for a subsequent 'phase two' large scale Demonstration research project in supply chain security.

DEMASST's work aimed at three unique but mutually informative research goals, namely to develop:

» potentially innovative policy instruments, notably in view of the varying degrees of maturity and fragmentation of different national and sectoral areas;

» a road-mapping methodology for the Demo project, notably in the form of system-of-systems models and criteria grids for prioritisation of potential demo tasks;

» a specific road-map for general European mass transport security.

Results

DEMASST set out to articulate an in-depth understanding of 'system-of-systems' approaches to modern transport infrastructure. Mass transportation security was characterised by the DEMASST consortium as a fragmented physical environment, with a multitude of principal actors (i.e. public and private), and no single complete authority or control over the system as a whole. The general public was also identified as the primary end user.

By focusing on these areas, the project developed a series of criteria and analysis frameworks for deciding which tasks and capabilities in mass transportation security require attention from the Demo. Criteria included cost effectiveness, adaptability/applicability to transport security and the social and legal acceptability of a measure.

These were contrasted against a range of tasks in transport security, from situation awareness and command and control to training and staff factors. The tasks were then compared to the three criteria areas in three potential scenarios:

» terrorists who aim to place hazardous material (e.g. a home-made explosive or fire-bomb) in a densely populated area in a mass transport system;

» conflicts between opposing gangs (e.g. football hooligans), which possibly escalate to a fight;

» a mentally disturbed person with a dangerous object (e.g. a knife).

Using a scoring system developed for this purpose, it was concluded that the following task areas should be the focus of the phase two Demo:

» risk assessment-based command and control capabilities;

» interoperability and information interfaces;

» learning and training;

» threat identification and detection capabilities;

» tracking and identification;

» early intervention.

PARTNERS	COUNTRY
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Ansaldo STS (ANSALDO)	Italy
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
EADS Astrium (Astrium)	France
Forsvarets forskningsinstitutt (FFI)	Norway
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-INT)	Germany
Ingeniería y Economía del Transporte SA (INECO)	Spain
Stiftelsen SINTEF (SINTEF)	Norway
Fundación Inasmet (TECNALIA-INAS)	Spain
Thales Security Solutions & Services SAS (T3S)	France
Tecnologia E Investigacion Ferroviaria S.A. (TIFSA)	Spain
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland

DESURBS / Designing safer urban spaces

© Bezalel Academy

Information

Grant Agreement N°
261652
Total Cost
€4,161,929
EU Contribution
€3,208,549
Starting Date
01/01/2011
Duration
48 months

Coordinator

RESEARCH MANAGEMENT AS
Fortunalia 14
NO-7057 Jonsvatnet, Norway
Contact
James Rydock
Tel: +47 73919307
Mobile: +47 95907562
Fax: +47 73918200
E-mail: jrydock@researchmgt.com
Website: www.desurbs.net

Project objectives

» Establish a security events database with a representative number of incidents resulting from security threats in urban areas;

» Create an Integrated Security and Resilience (ISR) design framework that engages local stakeholders in a local forum for finding weak points and strengthening urban spaces;

» Develop GIS-based mapping and visualization tools based on urban design case studies;

» Develop comprehensive supporting models, technologies and tools for quantifying vulnerabilities and strengthening weaknesses;

» Develop and implement a Decision Support System Portal integrating the database, the ISR framework, the mapping and visualization tools and the comprehensive supporting models, technologies and tools;

» Develop an objective rating scale for quantifying safety of different urban space designs and use it to show that the DESURBS solutions result in urban spaces less prone to and less affected by security threats;

» Carry out case studies in Jerusalem, Barcelona and Nottingham.

Description of the work

The project is divided into seven work packages (WPs). WP1 establishes an urban security and resilience database that looks at a range of past urban security incidents and 'near misses'. The database informs the identification of weak points in a variety of urban spaces in cities old and new, as well as the design of more robust and resilient urban spaces. As part of this development, we will create an objective scale for quantifying the safety and security of different urban space typologies and designs. This will be a key feature for showing that DESURBS designs result in urban spaces that are less prone to and less affected by security threats.

WP2 elaborates an Integrated Security and Resilience (ISR) design assessment framework. This will be a multi-disciplinary methodology that engages local stakeholders and focus groups to help recognize and understand the risks and vulnerabilities present, in the context of the competing functionalities (social, economic, aesthetic, managerial) and limitations in a given urban area. WP3 develops mapping and visualization tools to facilitate efficient use of the project's outputs. WP4 develops and adapts supporting models, tools and technologies that advance the state-of-the-art for quantifying different vulnerability aspects of urban spaces to identified threats and risks, to be used to help carry out the ISR design methodology within the framework developed in WP2. The WP2, WP3 and WP4 activities are informed and developed with reference to case studies in Jerusalem, Barcelona and Nottingham, where the project has established ties with local governmental and municipal planning authorities. WP5 combines all of the above into an internet-based, user friendly Decision Support System Portal. WP6 and WP7 are for dissemination and management, respectively.

Expected results

The main result will be an internet portal with the functionality to identify weak spots and to help design more robust and resilient urban spaces. This includes 1) An urban space security events database 2) An integrated security and resilience (ISR) design framework and 3) Comprehensive and generic supporting tools and methodologies, including urban resilient design guidelines and quantitative risk and vulnerability assessment methods to facilitate the qualitative ISR assessment process.

PARTNERS	COUNTRY
Research Management AS (Resman)	Norway
Loughborough University (Loughborough)	United Kingdom
The University of Birmingham (Birmingham)	United Kingdom
The Hebrew University of Jerusalem (HUJI)	Israel
Technical University of Crete (TUC)	Greece
Centre Internacional de Metodes Numerics en Enginyeria (CIMNE)	Spain
University of Southampton (IT Innovation)	United Kingdom
Bezalel, Academy of Arts and Design (Bezalel Academy)	Israel

EMILI / Emergency management in large infrastructures


© TebNad - Fotolia.com

Information

Grant Agreement N°
242438
Total Cost
€3,997,230.40
EU Contribution
€3,139,228
Starting Date
01/01/2010
Duration
36 months

Coordinator

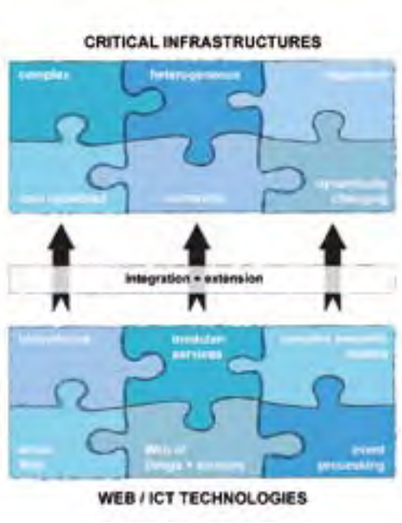
FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Schloss Birlinghoven
D-53754 Sankt Augustin
Germany
Contact
Dr. Rüdiger Klein
Tel.: +49 2241 14 2608
Fax: +49 2241 14 2342
E-mail: Ruediger.Klein@IAIS.Fraunhofer.de
Website: www.emili-project.eu

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, and their methodology and technology.



© Emili

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, and 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, and 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 for all relevant kinds of decision making in critical situations.

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

PARTNERS

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IAIS)
Asit AG
Aplicaciones en Informática Avanzada SA
Skytec AG Consulting in Information Technologies
Stichting Centrum voor Wiskunde en Informatica (CWI)
Institut Mihajlo Pupin
Ludwig-Maximilians-Universität München

COUNTRY

Germany
Switzerland
Spain
Germany
The Netherlands
Serbia
Germany

EURACOM / EUropean Risk Assessment and COntingency planning

Methodologies for interconnected networks

© EURACOM

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225579
Total Cost
€1,038,290
EU Contribution
€833,860
Starting Date
01/07/2009
End Date
31/03/2011

Coordinator

EUROPEAN ORGANISATION FOR SECURITY
Contact
Sophie Batas
E-mail:
Sophie.batas@eos-eu.com
Website:
www.euracom-project.eu

Project objectives

EURACOM addressed the issue of protection and resilience of energy supply for Europe's interconnected energy networks. Its objective was to identify, together with European critical energy infrastructure operators, a common and holistic approach (based on an 'end-to-end energy supply chain' concept) 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 energy infrastructure chain should increase.

Results

In order to develop a common European methodology for risk management and contingency planning, the project began with a research framework to analyse energy networks and their critical elements. This led to two studies of:

» existing risk assessment methodologies, which took stock and analyzed available international and European guidelines and good practices for risk assessment across the whole energy infrastructure chain;

» common areas of contingency planning methodologies, which provided a review of current business continuity management (BCM) practices from various sources. This encompassed international, national and domain-specific standards and guidelines.

The result was a methodology that proposes principles for a wider and consistent adoption of risk assessment and contingency planning approaches in the energy sector. EURACOM's draft outline for a common methodology is available at: https://circa.europa.eu/Members/irc/securejrc/jrc_euracom/home

EURACOM also created a common platform for discussion and future decision-making at European level across all stakeholders of the energy chain. In addition to five stakeholder workshops, the project set up a permanent networking forum. This restricted website offers energy infrastructure stakeholders a place to share their risk management experiences.

EURACOM's findings, including the common methodology, will be fed into policy discussion at EU level, with the long-term goal of incorporating these practices into EU regulatory requirements to encourage further analysis of the legal, technological (especially cyber) and economic implications of common risk management across Europe.

PARTNERS	COUNTRY
European Organisation for Security (EOS)	EU
Altran Technologies SA (ALTRAN)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
European Commission - Joint Research Centre (JRC)	Belgium
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Thales e-Security Ltd (THALES)	United Kingdom
Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)	Portugal

IDETECT 4ALL / Novel Intruder Detection & Authentication
Optical Sensing Technology

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217872
Total Cost
€3,239,571
EU Contribution
€2,298,014
Starting Date
01/07/2008
End Date
30/06/2011

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

Project objectives

This project's overarching objective was to develop and test a system of sensor technologies to protect critical infrastructure. A key driver was to find ways to overcome the high cost and unacceptable false alarm rates that limit the deployment of existing security sensor technologies.

Much of iDETECT4ALL's work focused on prototype sensors to detect intruders and remotely scan/read optical tags worn by authorised personnel and vehicles. A system architecture was defined to capture sensor alert event data, transmit this to a remote control centre and enable an imaging system to view the intruder event.

Work was divided into the following phases:

» review of end user requirements;

» system architecture definition;

» technology R&D until the prototype design and manufacture stage;

» system integration;

» field trials;

» analysis and evaluation.

Results

After consultations with end-users, the consortium developed a technological system consisting of:

» a low-cost prototype communication network to transmit event messages;

» a "back-office" database linked to control centre application software;

» a geographic information system (GIS) to correlate with alerts;

» a high resolution imaging system based on an internet control protocol to accept sensor alerts and pivot to view the event detected.

These elements were integrated and then tested in field experiments at airports in Portugal (Faro) and Belgium (Liege) using representative critical infrastructure protection scenarios. A wide variety of test cases were examined, including authentication and detection of walking and running personnel, and moving vehicles. The tests were carried out both day and night, and in adverse weather conditions such as heavy rain.

The field trial results demonstrated that the sensors and their system delivered useful levels of real world performance, while confirming that the project's objectives of achieving a very low false alarm rate and high detection rates were achieved. A key technological breakthrough was made with the development and successful testing of a single sensor able to both detect intruders and also authenticate personnel and vehicles by reading remote optical tags.

Though the project consortium said there is scope for further improvement of the sensor performance through additional optimisation of the hardware and signal processing algorithms, it argues that there is a good market opportunity to materialise and exploit the know-how gained in the project via a number of products.

According to the project's research partners, suitable levels of investment in optimisation and engineering for production in iDETECT4ALL's sensor and associated system could lead to "improved protection for critical infrastructures in the European Union and the world."

PARTNERS	COUNTRY
Instro Precision Ltd.	United Kingdom
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
Halevi Dweck & Co. Arttic Israel Company Ltd. (ARTTIC)	Israel
Arttic Israel International Management Services 2009 Ltd (AIL)	Israel

INFRA / Innovative & Novel First Responders Applications

© Duncan Noakes- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225272
Total Cost
€3,809,464.91
EU Contribution
€2,642,895
Starting Date
01/04/2009
End Date
31/03/2011

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
E-mail: olaviv@athenaiss.com
Website: www.infra-fp7.eu

Project objectives

INFRA's research goal was to develop new digital-based personal technologies for integration into a secure emergency management system to support first responders (FRs) involved in critical infrastructure incidents.

This encompassed three broad objectives:

» the creation of an interoperable wireless communications system that functions in difficult FR locales such as subway tunnels or buildings with thick concrete walls;

» the development of a robust indoor site navigation system, based on inertial and wireless sensors, a video annotation system for FR digital devices to generate real-time identification of hazardous materials such as gas leakages, and other sensor-based technologies for the individual first-responder;

» demonstration in live environments to prove the concept's feasibility.

End-users were heavily involved throughout INFRA's various work stages, from requirements-gathering to the final demonstration stages.

Results

The culmination of INFRA's integration work was its final field trial. This was held in January 2011 before a stakeholder audience of FR representatives from across Europe and involved an on-site demonstration of INFRA's entire technology at two locations: inside a tunnel of Madrid's M-30 ring road and a C2 centre located five km away.

The technologies and applications demonstrated in Madrid included:

» a robust ad-hoc mesh topology broadband wireless network for interoperability between standard FR radio sets;

» non-invasive biometric sensors integrated onto a wearable "finger clip" (and an early-prototype ear-clip version) to monitor a first-responder's vital signs such as blood haemoglobin and oxygen levels, heart rate and temperature;

» lightweight optical gas sensors for detecting O2, CO2 and methane levels, and radiation sensors for detecting x-rays, alpha and beta rays, among others;

» a video annotation system to enhance visual communications among FRs and the C2 centre;

» the movements of first responders who were tracked effectively in real-time while in the tunnels;

» a PC-based application, based on client-server architecture, to enable the C2 post to send information requests to first-responders.

According to INFRA's research team, their project achieved all of its technical objectives and, with one exception, tested and demonstrated all of the applications it developed. Moreover, it said the project's novel technology solution could help revolutionise the end-user market since it allows all FR teams, command posts and critical infrastructure control centres to communicate with each other and to transfer digital data at high bit rates, including live video images.

"The field test showed that the main features, though far from complete at the time of the test, nevertheless are functional and deemed very useful by FRs," says INFRA.

PARTNERS	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
Arttic Israel International Management Services 2009 Ltd (AIL)	Israel

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

© TOM ANG - Fotolia.com

Information

Grant Agreement N°
225663
Total Cost
€4,367,950.73
EU Contribution
€3,113,460
Starting Date
01/07/2009
Duration
36 months

Coordinator

TECNOLOGIE PER LE OSSERVAZIONI DELLA TERRA ED I RISCHI NATURALI
c/o CNR-IMAA
C.da S. Loja, Zona Industriale
85050 Tito (PZ)
Italy
Contact
Prof. Vincenzo Cuomo
Tel.: +39 0971 427229/208
Fax: +39 0971 427271
E-mail: tem@imaa.cnr.it
Website: www.istimes.eu

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 accurate monitoring as well as the possibility of obtaining quasi real-time information on the scenario of crises.

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 are in terms of detailed real time information and images of the infrastructure status to be used to provide support to the decision of emergency and disaster 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 into five activities:

» ACTIVITY 1 will cover 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-users; infrastructure for enabling remote use of and control of instrumentation and processing of measurements; wireless network services for sensor 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-the-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 an 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 the ISTIMES approach and outcomes to public institutions and private companies.

© Istimes

PARTNERS	COUNTRY
Tecnologie per le Osservazioni della Terra ed i Rischi Naturali (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
Telespazio S.p.A. (TPZ)	Italy

MOSAIC / Multi-Modal Situation Assessment & Analytics Platform

© Mosaic

Information

Grant Agreement N°
261776
Total Cost
€3,606,642.00
EU Contribution
€2,664,559.00
Starting Date
01/04/2011
Duration
36 months

Coordinator

THE UNIVERSITY OF READING
Intelligent Media Systems and Services Research Laboratory, School of Systems Engineering
Whiteknights Campus
PO Box 217
RG66AH Reading,
United Kingdom
Contact
Prof. Atta Badii
Tel: +44 (0) 118 378 7842
Fax: +44 (0) 118 975 1994
E-mail:
atta.badii@readiing.ac.uk
Website:
www.imss.reading.ac.uk

Project objectives

MOSAIC will develop and validate:

» A framework for capturing and interpreting the use-context requirements underpinned by a standard data ontology to facilitate the tagging, search and fusion of data from distributed multimedia sensors, sources and databases;

» A systems architecture to support wide area surveillance with edge and central fusion and decision support capabilities;

» Algorithms, including hardware-accelerated algorithms for smart cameras, which enable disparate multi-media information correlation to form a common operating picture, including representation of the temporal information and aspects;

» Tools and techniques for the extraction of key information from video, uncontrolled text and databases using pattern recognition and behaviour modelling techniques;

» Algorithms and techniques to represent decisions and actions within a mathematical framework, and how this framework can be used to simulate the effects of disturbances on the system.

Description of the work

MOSAIC Platform will involve multi-modal data intelligence capture and analytics including video and text collaterals etc. The distributed intelligence within the platform enables decision support for automated detection, recognition, geo-location and mapping, including intelligent decision support at various levels to enhance situation awareness, surveillance targeting and camera handover; these involve level one fusion, and situation understanding to enable decision support and impact analysis at level two and three of situation assessment. Accordingly MOSAIC will develop and validate: i) A framework for capturing and interpreting the use-context requirements underpinned by a standard data ontology to facilitate the tagging, search and fusion of data from distributed multi-media sensors, sources and databases, ii) A systems architecture to support wide area surveillance with edge and central fusion and decision support capabilities, iii) Algorithms, including hardware-accelerated ones for smart cameras, which enable disparate multi-media information correlation to form a common operating picture, including representation of the temporal information and aspects, iv) Tools and techniques for the extraction of key information from video, un-controlled text and databases using pattern recognition and behaviour modelling techniques, v) Algorithms and techniques to represent decisions and actions within a mathematical framework, and how this framework can be used to simulate the effects of disturbances on the system, vi) An integrated system solution based upon the proposed systems architecture and the above developed enabling technologies including techniques for tagging different multi-media types with descriptive metadata to support multi-level fusion and correlation of surveillance and other data intelligence from distributed heterogeneous sources and networks.

Expected results

Due to the ability to pre-process events on the camera itself, thus allowing for the pre-filtering of unimportant events, the efficacy of wide-area surveillance can be improved. This is enhanced by the fact that the MOSAIC decision support sub-system will support a more focused and targeted approach to surveillance, i.e. informing on the required deployment of cameras as well as informing already deployed cameras to shift attention or to go to temporary sleep mode, thus further enhancing the reduction of network traffic.

© Mosaic

PARTNERS	COUNTRY
The University of Reading (UoR)	United Kingdom
BAE Systems (Operations) Ltd (BAE)	United Kingdom
A E Solutions (BI) (AES)	United Kingdom
SYNTHEMA S.R.L. (SY)	Italy
TECHNISCHE UNIVERSITAT BERLIN (TUB)	Germany
DResearch Digital Media Systems GmbH (DR)	Germany
WEST MIDLANDS POLICE AUTHORITY (WMP)	United Kingdom
INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)	Belgium
WARWICKSHIRE POLICE (WP)	United Kingdom

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


© Aaron Kohr - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225488
Total Cost
€4,325,739.94
EU Contribution
€2,711,640
Starting Date
01/07/2009
End Date
30/09/2011

Coordinator

VITROCISET S.P.A.
Contact
Walter Matta
Tel: +39 06 88202567
Mobile: +39 335 7716488
Fax: +39 06 8820 2288
E-mail: w.matta@vitrociset.it
Website:
http://ni2s3-project.eu/

Project objectives

The main objective of NI2S3 was to research and implement a reference methodology for developing security systems based on networked or electronic information and integration services for critical infrastructure protection (CIP).

A key goal was to integrate information from numerous heterogeneous sensors or sources, in order to build up and improve situational awareness around critical infrastructures.

Results

The basis of NI2S3 was a gap analysis of situational awareness capacities around critical infrastructure protection in Europe.

The goal of this analysis was to identity where a network-centric "information space" could be of use to support CIP decision makers. This space was conceptualised as a layer of interoperable ICT that can support the input of dedicated devices, public information and services to optimise resource management. Such a space can provide superior information on events and conditions surrounding infrastructures in an emergency, or for day-to-day management.

Scenarios and locations considered for this concept included a new command and control (C2) architecture to support Polish police in the city of Kracow, an information service on Kracow's public highways and an information service for the A22 highway in northern Italy.

These scenarios were used to assess potential "spoiler" inputs to an open information system – including such factors as hostile eavesdropping on information traffic, data interception/alteration for malicious purposes and the mass flooding of the system with "spam" or false data or to create denial of service via voluminous spam. False safes such as sensor kill-switches and data encryption were proposed to handle these threats.

The final operational concept has now been submitted for stakeholder examination.

PARTNERS

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

COUNTRY

Italy
Italy
United Kingdom
Denmark
Poland
Poland

PROTECTRAIL / The Railway-Industry Partnership for Integrated Security of Rail Transport

© PROTECTRAIL

Information

Grant Agreement N°
242270
Total Cost
€21,632,880.80
EU Contribution
€13,115,064.00
Starting Date
01/09/2010
Duration
42 months

Coordinator

ANSALDO STS S.P.A.
Via P. Mantovani 3-5
16151 Genova
Italy
Contact
Mr. Vito Siciliano
Tel.: +39-010-6552976
Fax: +39-010-6552006
Mobile: +39-3489895875
E-mail: Vito.Siciliano.
Prof110@ansaldo-sts.com
Website: not yet available

Project objectives

The objective to provide a viable integrated set of security solutions, by considering the extent of the assets involved, the nature of the threats, the amount of requirements and the constraints. The integration will follow an innovative way and will extend the scope of the project beyond the mission addressed by the call.

The PROTECTRAIL will develop mission oriented vs. asset-specific solutions and will make them interoperable by designing a modular architectural framework where each solution can be "plugged". This will provide the basis for a streamlined process of federation, integration and interoperability.

The project will ensure that appropriate solutions and innovations are favoured over isolated questions and solutions, and will represent a comprehensive and scalable answer to rail security.

The dissemination process will initiate a cooperation framework with the National and EU authorities and the standardisation bodies, in view of proposals for recommendations to be adopted.

Description of the work

PROTECTRAIL will tackle the railway security problem from a layered system integration perspective.

The concept of the project is to address this main goal by dividing the global mission into a limited number of submissions that respond to well identified needs of railway protection, within a framework of general coherence and integration of technical and organization solutions.

Each sub-mission oriented solution will cover significant areas of interest, resulting both from risk analysis and rail operator priorities.

By selecting performance goals for sub-missions, effective solutions in terms of architectures, technology deployment, procedures, tools and organizations will be defined and developed to manage specific threat scenarios.

The project has been structured in 7 Sub-Projects and 38 Work Packages.

The 5 technical SPs are supported by the Project Management & Technical Coordination (SP0) and Dissemination and Exploitation (SP1) sub-projects.

For each sub-mission considered, SP2 will define the functional & technical specifications for prevention, mitigation and crisis management for the selected scenarios both at the sub-mission and global integration levels.

In SP3 and SP4, (for fixed asset and transported assets), the feasibility of solving the identified railway protection sub-missions through an efficient and cost effective integration of technologies will be demonstrated. Closely reflecting the main needs in the railway sector, these sub-missions will focus on protection of key assets. The project will be carried out by considering the specificity of rail environments and by monitoring the impact of security measures on ethical issues and citizens rights as well as the positive impacts against other forms of threats and for mitigation of consequences of natural events.

Expected results

The project will show the implementation potential of short/medium term solutions. It will also set out the development of prospective solutions to match future challenges. The market up-take potential is guaranteed by the participation of the main railway and security solutions suppliers, enhancing the capability of producing standard systems and of major railway operators (undertakings and infrastructure managers), guaranteeing that project solutions will satisfy user needs and fulfil railway requirements.

PARTNERS	COUNTRY
Ansaldo STS S.p.A.	Italy
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Elsag Datamat S.p.A.	Italy
Union Internationale Des Chemins De Fer	France
Selex Sistemi Integrati S.p.A.	Italy
Bombardier Transportation GMBH	Germany
Alstom Transport SA	France
Thales Security Solutions & Services SAS	France
Sarad GmbH	Germany
UNIFE – The European Rail Industry	Belgium
Sagem Sécurité SA	France
Ductis GmbH	Germany
Železničná spoločnosť Slovensko a.s.	Slovakia
Joint Stock Company Lithuanian Railways	Lithuania
ItalCertifer S.c.p.a.	Italy
PKP Polskie Linie Kolejowe SA	Poland
D'Appolonia S.p.A.	Italy
Elbit Systems Ltd.	Israel
Facultés Universitaires Notre-Dame de la Paix	Belgium
EPPRA	France
Kingston University Higher Education Corporation	United Kingdom
SODERN	France
Smiths Heimann S.A.S.	France
Rail Cargo Austria	Austria
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Institut Franco-Allemand de Recherches de Saint-Louis	France
Turkish State Railways	Turkey
MER MEC S.p.A.	Italy
Société Nationale des Chemins de Fer	France

RIBS / Resilient infrastructure and building security

© teekid - istockphoto.com

Information

Grant Agreement N°
242497
Total Cost
€4,406,966.80
EU Contribution
€3,321,957.80
Starting Date
01/11/2010
Duration
36 months

Coordinator

UNIVERSITY COLLEGE LONDON
Department of Security and Crime Science
2 - 16 Torrington Place
WC1E 7HN, London,
UNITED KINGDOM
Contact
Dr Hervé Borrion
Tel: +44(0)20 3108 3194
Mobile: n/a
Fax: +44(0)20 3108 3088
E-mail: h.borrion@ucl.ac.uk
Website: www.ribs-project.eu

Project objectives

Objective 1
To characterise a range of existing and emerging (i) security threats and (ii) protection measures, and integrate the results into a single comprehensive multi-layer model that can be used for vulnerability analysis.

Objective 2
To characterise relevant physical and non physical elements of buildings, and integrate the results into a single comprehensive multi-layer model that can be used for vulnerability analysis.

Objective 3
To design and implement an effective vulnerability analysis technique utilizing models of the "complex threat" and the "complex infrastructure" and use this technique to analyse the protection measures of an existing building.

Objective 4
To develop a method for defining suitable requirements for the design of infrastructure-specific protection measures focusing on functions such as detection, identification, and authentication.

Objective 5
To develop and apply a method for assessing the level of protection of buildings provided by additional protection measures against a range of security threats.

Objective 6
To determine, validate and promote the requested design requirements and additional physical protection measurements through a field-study involving an existing building and end-users.

Description of the work

The RIBS-project supports the design of effective and viable integrated security measures aimed at protecting infrastructures without impacting on their business dynamics. In a global context where national interests are increasingly interrelated, the most vulnerable infrastructures in Europe, and particularly the most critical ones, are primary targets for terrorists. Attacks, carried out under a national, political, or religious banner, now strike regularly in our cities, causing deaths, damage and disruption on an unprecedented scale. In the past seven years alone, 1300 terrorist incidents have taken place on European soil.

The RIBS project will deliver more effective and viable security measures by supporting a design process that integrates a broader understanding of the environment (and the contextual factors such as human elements) within which these measures are meant to be implemented.

The particular objectives of the project include a set of functional and non-functional requirements that will drive an effective security system design process, and a set of protection measurement techniques that can be used to assess the level of protection offered by candidate security products proposed to be implemented in buildings and infrastructures.

This work will be carried out for a range of security systems aimed at securing buildings against hostile reconnaissance, intruders and hazardous attack (including chemical, biological and explosive).

Expected results

The RIBS-project will derive a scientific method for security system engineering design that can be challenged and improved over the years, similarly to other areas of engineering and physical sciences. The results include:

» Phase 1: Study of a live building and its 'eco-system', its protection measures, and threats; and integration of these elements into a single multi-layer model;

» Phase 2: Identification of vulnerabilities through incident analysis and protection-measures analysis;

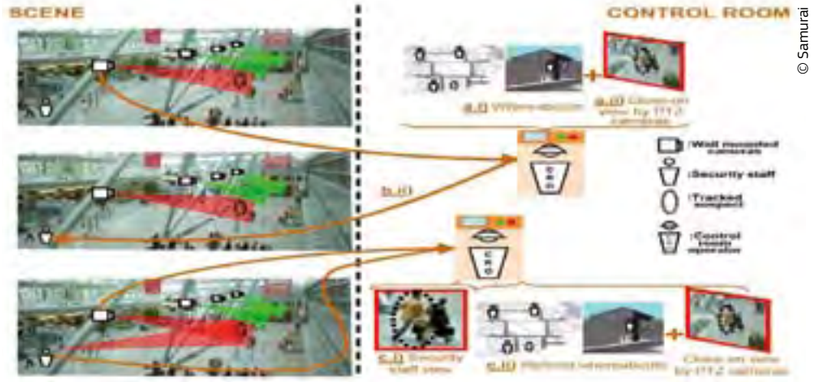
» Phase 3: Development of design requirements.

PARTNERS	COUNTRY
UNIVERSITY COLLEGE LONDON (UCL)	United Kingdom
TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY (TECHNION)	Israel
H.PETROPOULEA&CO (2E)	Greece
KUNGLIGA TEKNISKA HOEGSKOLAN (KTH)	Sweden
DANMARKS TEKNISKE UNIVERSITET (DTU)	Denmark
EFI (Anonymised name of Partner)	Greece
Aedas Architects Limited (Aedas Architects)	United Kingdom

SAMURAI / Suspicious and Abnormal behaviour Monitoring Using a networRk of cAmeras for sItuation awareness enhancement

© diego cervo - Fotolia.com

RESEARCH **COMPLETED**



© Samurai

Information

Grant Agreement N°
217899
Total Cost
€3,723,071.40
EU Contribution
€2,478,051.50
Starting Date
01/06/2008
End Date
30/11/2011

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

Project objectives

The aim of SAMURAI was to develop and integrate an innovative surveillance system for monitoring both the interior and surrounding areas of a critical public infrastructure site.

The project set out to achieve three key innovations:

» combining networked sensors, rather than isolated visual sensors (e.g. standalone CCTV cameras), so that multiple complementary sources of information are fused in order to obtain a complete surveillance picture;

» developing intelligent video analytics, as well as an online adaptive behaviour monitoring system, for real-time abnormal behaviour detection;

» integrating fixed-position CCTV video footage with mobile sensory input from patrolling staff for more effective "man-in-the-loop" decision-making back at the operations centre.

Results

SAMURAI produced a range of new operating concepts, software and hardware to achieve its scientific research goals.

For combining sensor data, SAMURAI produced new visualisation software, the SUMURAI GUI, to display data from different inputs in one window. As well as active 3D image mapping, this includes a background algorithm that automatically filters out "useless" motion from sensor images to leave only relevant, "action needed" highlights.

For abnormal behaviour detection, the project combined multi-sensor source data processing with a series of pre-programmed abnormal, rare or "of interest" behavioural triggers. Data points such as audio abnormalities, obvious attempts to conceal one's identity, or movements against the regular "flow" of crowded area traffic are fed into this system to produce "focus of attention" (FoA) prioritisation for operators.

Finally, to integrate sensory input from patrolling staff, SAMURAI designed and developed the Ninja, a wearable sensor suit with built in data ports for camera and audio inputs. Supported by a wifi-based remote processing unit known as the BPS Ngine system, the project produced 50 operating Ninja units. Each unit can augment fixed position sensors by giving operators an "eyes on target" update to other feeds.

When combined, the results produced by SAMURAI represent a highly integrated and advanced situational awareness system. The use of data fusion algorithms throughout ensures that the SAMURAI system displays only the most pertinent data and knowledge regarding the current situation.

In addition it allows the end-user to alter their awareness picture in real-time, to support almost immediate staff prioritisation during a security incident.

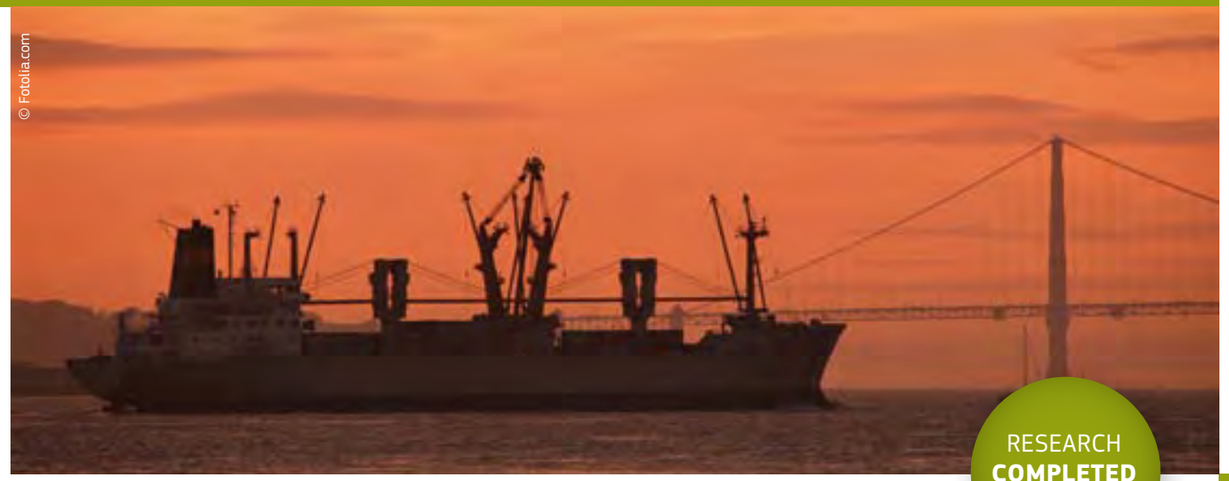
PARTNERS

Queen Mary, University of London
Università degli Studi di Verona
Elsag Datamat S.p.A.
Waterfall Solutions Ltd
Borthwick-Pignon OÜ
Esaprojekt SP. Z O.O.
Syndicat Mixte des Transports pour le Rhône et l'Agglomération Lyonnaise
BAA Limited

COUNTRY

United Kingdom
Italy
Italy
United Kingdom
Estonia
Poland
France
United Kingdom

SECTRONIC / Security system for maritime infrastructure, ports and coastal zones


© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218245
Total Cost
€6,948,326.42
EU Contribution
€4,496,106.41
Starting Date
01/02/2008
End Date
31/01/2012

Coordinator

QUEEN MARY, UNIVERSITY OF LONDON 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

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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

© Sectronic

PARTNERS

Queen Mary, University of London 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

SECUR-ED / Secured urban transportation – European Demonstration


© Paolo Margari

Information

Grant Agreement N°
261605
Total Cost
€40,188,876.20
EU Contribution
€25,468,072.00
Starting Date
01/04/2011
Duration
42 months

Coordinator

THALES SECURITY SOLUTIONS & SERVICES SAS
DOMAIN CTS
20-22 RUE GRANGE DAME ROSE
78141 VÉLIZY-VILLACOUBLAY
FRANCE
Contact
Yves PERREAL
Tel: +33 (0)1 73 32 15 07
Mobile:
+33 (0)6 86 12 70 00
Fax: +33 (0)1 73 32 05 46
E-mail: yves.perreal@thales-group.com
Website: www.secur-ed.eu

Project objectives

SECUR-ED's first objective is to give transport operators of large and medium cities in Europe the means to enhance urban transport security. The second main objective is to enlarge the mass transport security market for the European industry.

SECUR-ED will define a consistent and interoperable mix of technologies and processes, addressing security of people and infrastructures, from minor offences to major terrorism threats, and targeting interoperability and standardisation of solutions.

These mission oriented solutions will be applied in intermodal environments (transport nodes), taking into account various legal, cultural and societal environments.

The demonstrations developed in several cities (Madrid, Paris, Milan, Berlin, Brussels, Istanbul…) will give concrete examples of how to increase the security, and will support the creation of a European common market for security solutions adapted to mass transport.

Description of the work

Security risks in multimodal urban nodes are various and depend on the size of the cities, the modes of transport, and the location of the stations. Severity varies from daily and minor issues (graffiti or verbal insults) to more serious problems (vandalism or physical violence), and even catastrophic damages in case of terrorism attacks. In such situations, and especially in large urban hubs, public transport operators do not act alone and collaborate with a variety of stakeholders in preventive and reactive measures.

It is crucial that the various involved parties exchange relevant information and act in a coordinated way in critical situations. To address this objective, SECUR-ED will define a consistent and interoperable mix of technologies and processes:

» A toolkit of operational procedures aimed at identifying and managing risks, planning operations, and ensuring fast restoration of activities;

» A series of improved technical security solutions:

- Video analytics to analyze threats, monitor situations and anticipate dangerous events;
- Protection, hardening and resilience of critical infrastructures;
- CBRN-E sensor systems to be used prior, during and after a critical event;
- Standardized information management and communication systems controlling exchange of information between the transport actors and the users;
- Intelligent incident prevention and early warning systems using multiple-source correlation.

» Taking into account the importance of the human factor, the project will define extensive training programmes for all types of stakeholders.

All these security capacities will be trimmed and validated in the various real environments of several flagships demonstrations in big European cities: Madrid, Paris, Milan and Berlin.

Additional demonstrations will be proposed to other operators from medium to big size cities (Bucharest, Brussels, Lisbon, Istanbul…). This will demonstrate the applicability of the SECUR-ED toolkit to any mass transport environment, thanks to a strong focus on interoperability. Most of the above demonstrations will be ready for mid 2013.

Dissemination will be achieved through several Advisory Groups, including public transport operators, industries, first responders and users, proposing guidelines and recommendations and sharing the project results.

Expected results

By implementing solutions validated through very concrete experimentations, the project will promote among the operators the importance of conducting risk assessment and investing in security.

Giving to industries the opportunity to validate their solutions in various environments, it will increase the interoperability and standardization of technical solutions.

In stimulating the cooperation between operators and providers of civil security solutions, and delivering mission-oriented solutions, SECUR-ED will reduce the security gaps in the mass transit nodes.

PARTNERS	COUNTRY
Thales Security Solutions & Services SAS (THA)	France
Alstom Transport S.A. (ALS)	France
Ansaldo STS S.p.A. (ANS)	Italy
Azienda Trasporti Milanesi (ATM)	Italy
Bombardier Transportation GMBH (BOM)	Germany
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Consorcio Regional de Transportes de Madrid (CTM)	Spain
Deutsche Bahn AG (DBA)	Germany
European Organisation for Security SCRL (EOS)	Belgium
Edisoft - Empresa de servicios e desenvolvimento de software SA (EDI)	Portugal
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
HAMBURG-CONSULT Gesellschaft für Verkehrsberatung M.B.H. (HCO)	Germany
Ingenieria y Consultoria para el Control Automatico, SL (ICC)	Spain
INOV INESC INOVAÇÃO – Instituto de Novas Tecnologias (INO)	Portugal
European Commission - Joint Research Centre (JRC)	Belgium
Regia Autonoma de Tranport Bucuresti (RTB)	Romania
EMEF, SA - Empresa de Manutenção de Equipamento Ferroviário, SA (EME)	Portugal
MTRS3 Solutions and Services LTD (MTR)	Israel
NICE Systems Ltd. (NIC)	Israel
Universitaet Paderborn (UPB)	Germany
Régie Autonome des Transports Parisiens (RTP)	France
Morpho (MPH)	France
Empresa Municipal de Transportes de Madrid SA (EMT)	Spain
Ministère de l'Intérieur, de l'Outremer et des collectivités territoriales Direction de la défense et de la sécurité civile (STS)	France
Société Nationale des Chemins de Fer Français (SNF)	France
FNM SPA (FNM)	Italy
Universitetet i Stavanger (STA)	Norway
Société des Transports Intercommunaux de Bruxelles SSF (STIB)	Belgium
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	Netherlands
Technische Universitaet Dresden (TUD)	Germany
Union Internationale des Transports Publics - UITP (UIP)	Belgium
Union des Industries Ferroviaires Européennes - UNIFE (UNI)	Belgium
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Julius-Maximilians Universitaet Wuerzburg (WUE)	Germany
Ingenieria y Economia del Transporte S.A. (INE)	Spain
G. Team Security Ltd (GTE)	Israel
AXIS Communications Aktiebolag (AXI)	Sweden
Turkiye Cumhuriyeti Devlet Demir Yollari Isletmesi Genel Mudurlugu (TCD)	Turkey
Selex Elsag S.p.A. (SEG)	Italy

SERON / Security of road transport networks


© Frog 974 - Fotolia.com

Information

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
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

Project objectives

The SeRoN project undertakes a holistic approach at both 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 designed 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 also with 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, using a few suitable examples, the new methodology developed will be validated before recommendations for infrastructure owners will be formulated taking into account external expert knowledge gained in workshops.

Expected results

The SeRoN project 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 in countermeasures and risk mitigation strategies. The developed methodology may be transferred to transport networks used by other traffic modes and to natural disasters.


© Seron

PARTNERS

Planung Transport Verkehr AG (PTV)
Bundesanstalt für Straßenwesen (BASt)
Parsons Brinckerhoff (PB)
Technische Universität Graz (TU Graz)
Traficon n.v (TRFI)
Ernst Basler und Partner (EBP)
NIRAS Rådgivende Ingeniører og Planlæggere A/S (NIR)

COUNTRY

Germany
Germany
United Kingdom
Austria
Belgium
Switzerland
Denmark

SESAME / Securing the European electricity Supply Against Malicious and accidental thrEats

© C. Schiller - www.fotolia.de

Information

Grant Agreement N°
261696
Total Cost
€3,982,815.20
EU Contribution
€2,753,789.80
Starting Date
01/05/2011
Duration
36 months

Coordinator

POLITECNICO DI TORINO
DIPARTIMENTO DI INGEGNERIA ELETTRICA
Corso Duca degli Abruzzi, 24
I-10129, Torino
ITALY
Contact
Prof. Ettore BOMPARD
Tel: +39 011 090 7154
Fax: +39 011 090 7199
E-mail:
ettore.bompard@polito.it

Project objectives

The project targets two key-issues for the security of the European Electric Power Systems: *the decision making related to the assurance of the security of power systems* as critical infrastructure and the design of a *regulatory framework* that allows for covering the cost of security in a market environment.

The project is developing a Decision Support System for the protection of the European power transmission, distribution and generation system. This Decision Support System can be used to:

- identify the vulnerabilities of the analyzed grid and production plants and detect their origins;
- estimate the damage / impact of real or simulated network failures;
- identify the possible measures for prevention of outages and acceleration of automatic restoration;
- rank these measures according to their effectiveness and their cost-benefit ratios;
- carry out contingency analyses of the transmission and distribution network and the generation facilities.

The project, based on the analysis of the impacts of failures in the supply of energy, is designing a set of regulatory rules, based at the national and coordinated at the European level, aiming at assuring an adequate level of security to the European power grid from an economic point of view.

Description of the work

The first step is to analyse the origin of vulnerabilities and how weaknesses of the power transmission / distribution / generation system can be identified. Therefore, the metrics needed for an exhaustive detection and comprehensive rating of the vulnerabilities are being developed. This project not only considers the physical network, with its control and communication structure, as the potential origin of the vulnerabilities, but also incorporates organisational and educative structures.

The second step is to identify effective measures to specifically address each identified kind of vulnerability and threat. These measures are mainly on a technical level, but will also include organisational and educational measures.

The impact of already occurred power interruptions and possible blackout scenarios is then analysed.

The tools developed in the preceding work steps are then integrated into a comprehensive prototype software Decision Support System. In a first step, the tool will be assembled and the developed algorithms and metrics implemented. Then, the DSS will be tested on two actual power grids of two partner power networks, namely Romania and Austria.

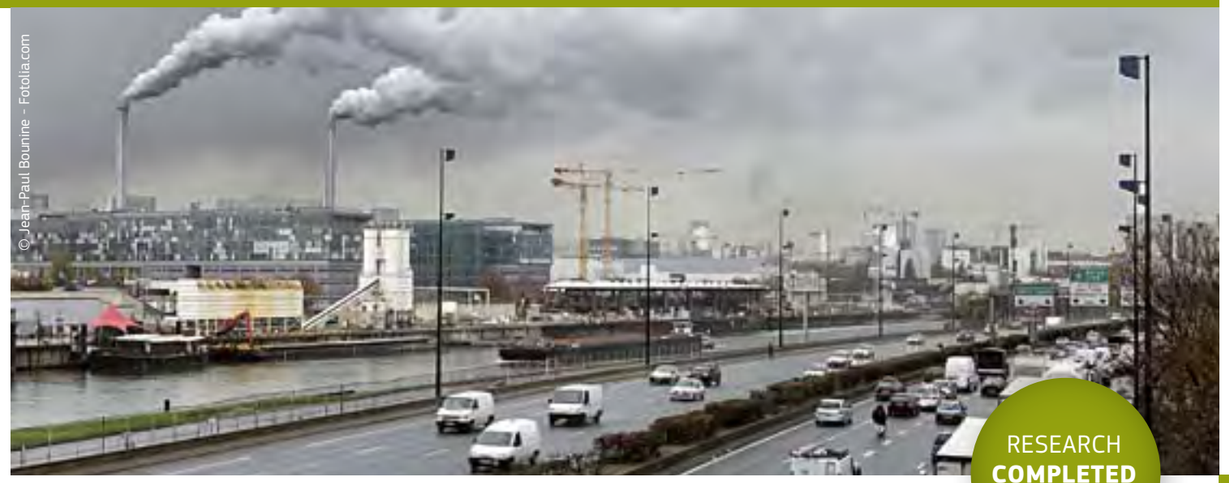
The last work step provides the necessary elements of a comprehensive regulatory policy, which fully incorporates the security of supply.

Expected results

- Risk Assessment System: a set of algorithms and data structures;
- Knowledge base of the impacts of a blackout on society;
- Software tool for the estimation of damage costs caused by a power interruption;
- Assessment of security of electricity supply (SES) indicators as input for rational decisions regarding policy making;
- Comparative view on the different regulatory regimes in Europe;
- Development of a regulatory and policy framework for the security of the energy infrastructure in Europe.

PARTNERS	COUNTRY
Politecnico di Torino (PoliTo)	Italy
Energy Institute at the J. Kepler University Linz (EI-JKU)	Austria
Indra Sistemas SA (INDRA)	Spain
Heriot Watt University (HWU)	United Kingdom
e-Control (Ectrl)	Austria
Deloitte (Delo)	Spain
TU Delft (TUD)	The Netherlands
Transelectrica (TrEI)	Romania
Kudos Research (KUDOS)	United Kingdom

STAR-TRANS / Strategic risk assessment and contingency planning in interconnected transport networks



RESEARCH **COMPLETED**

Information

Grant Agreement N°
225594
Total Cost
€3,296,369.71
EU Contribution
€2,105,588.94
Starting Date
01/11/2009
End Date
30/04/2012

Coordinator

INTRASOFT INTERNATIONAL S.A.
RUE NICOLAS BOVÉ
1253 LUXEMBOURG
LUXEMBOURG
Contact
Dr. Antonios Ramfos
E-mail: antonis.ramfos@intrasoft-intl.com
Website: www.startrans-project.eu

Project objectives

The fundamental assumption within STAR-TRANS is that transportation assets, such as airplanes and tunnels, are an 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 the 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.

STAR-TRANS' comprehensive risk assessment approach targets 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:

» *Vulnerability*, reflecting the possibility of a risk incident, e.g. terrorist attack, for the interdependent and interconnected European transport networks, compared to the possibility of protecting them through inherent or managed safeguards;

» *Consequences* of a successful attack, which is defined using (i) the possible number of casualties / 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	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 Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IVI)	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
SOCIETA RETI E MOBILITA SPA (SRM)	Italy

SUBITO / The Surveillance of Unattended Baggage and the Identification and Tracking of the Owner


© Artsem Martysiuk - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218004
Total Cost
€3,897,587.20
EU Contribution
€2,581,052,60
Starting Date
01/01/2009
End Date
31/10/2011

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@selex-galileo.com
Website:
www.subito-project.eu

Project objectives

SUBITO set out to further develop new technologies for processing visual images and applying threat assessment algorithms for identifying baggage lost by individuals in a crowded public space. The overall objective of the project was to remotely facilitate the:

» fast detection of baggage that has been abandoned;

» fast identification of the individual who left the baggage;

» fast determination of their current location, or path they followed.


© illushooti - Fotolia.com

Results

SUBITO developed its system architecture in the context of existing lost baggage procedures used by stakeholders. It also applied an ethical review related to privacy requirements in EU law, and produced background material on the wider social and legal aspects of visual monitoring technology.

The eventual defined system required novel advancements for visual processing camera technology and for the distributed processing of threat assessment data. These were:

» Visual: image analysis algorithms were combined with improved camera technology to enhance the ability to detect, segment, track and classify moving objects within a scene. This was achieved by using a multi-view approach, which reduced the system's false alarms;

» Threat assessment: processing algorithms were developed to better classify potentially critical situations, by giving positional and classification data about the objects and people within the sensed environment. Research indicates that the inclusion of reasoning about the intentions of individuals within a scene, and the interactions between these individuals, leads to greatly improved performance of the state of the art. In particular, the SUBITO system exceeds the processing achievements of the previous ISCAPS study.

The project culminated in the final demonstration and evaluation of an integrated system, operating in pre-recorded scenarios. The demonstration illustrates advances towards the overall objectives mentioned above.

PARTNERS	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
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
University of Leeds	United Kingdom
University of Reading	United Kingdom
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Österreichesches Forschungs und Prufzentrum Arsenal Ges.m.bH	Austria
Fiera di Genova S.p.A	Italy
The Chancellor, Masters and Scholars of the University of Oxford	United Kingdom

TASS / Total airport security system

© josh webb - istockphoto.com

Information

Grant Agreement N°
241905
Total Cost
€14,966,370.60
EU Contribution
€8,986,696.15
Starting Date
01/04/2010
Duration
48 months

Coordinator

VERINT SYSTEMS LTD
Business Development
33 Maskit st
46733 Herzlia, Israel
Contact
Hazzani Gideon
Tel.: +972 9 9622596
Mobile:+972 54 778 2596
E-mail:
Gideon.hazzani@verint.com
Website: www.tass-project.eu

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 airport security into eight security control segments (environmental, cargo, baggage, people, airplanes, vehicles, facilities and cyberspace) 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 for all airport authorities.

Description of the work

The mission of the TASS consortium is to research, develop and illustrate the capabilities of the data collection tools, data fusion mediation and portal and web based applications. TASS aims to integrate these elements into one consolidated system where collected information is analyzed, alerted and viewed by the airport C3.

Fusion of data collected from an array of sensors 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 TASS system architecture and the research performed in TASS consists of 3 main parts: (i) Data collection, (ii) Data fusion which will gather the information and fuse it, to create a comprehensive, real time, security overview of the airport, and (iii) TASS C2 portal and related Web based applications which will analyze and display the collected data.

The TASS consortium brings together European airports, innovative SMEs and industrial and academic partners. The TASS solutions will be tested at several European airports including the large hub airport Heathrow, the medium Athens airport as well as the small Faro airport (Portugal) in order to cover a wide range of needs at different levels of airport protection.

During the first two years of development a strong emphasis has been placed on the end-user (airports) insights, and requirements. Based on this, TASS partners performed a threat analysis and developed the system architecture and operational scenarios while keeping an emphasis on privacy. TASS started to provide the tools to enable C3 operators to respond in real-time to security situations. More than 35 different sensors have been installed at Heathrow airport.

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.

© Tass

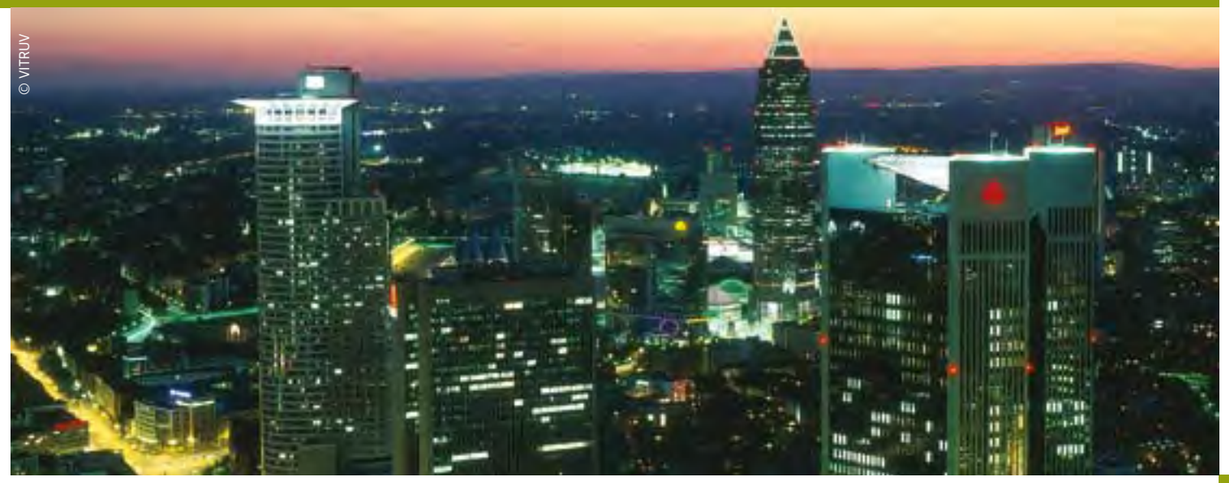
PARTNERS

Verint Systems Ltd (VRNT)	Israel
BAA Limited (BAA)	United Kingdom
Grupo Mecanica del Vuelo Sistemas S.A. (GMV)	Spain
Rapiscan Systems Limited (RSL)	United Kingdom
Consorzio per la Ricera Nell' Automatica e Nelle Telecomunicazioni C.R.A.T (CRAT)	Italy
National Center for Scientific Research "Demokritos" (NCSR "D")	Greece
GMVIS Skysoft SA (SKY)	Portugal
Mentum SA (MTM)	France
Vitrociset Spa (VITRO)	Italy
Alcatel-Lucent Italia S.P.A (ALI)	Italy
The Provost Fellows & Scholars of the College of the Holy and Undivided Trinity of Queen Elizabeth near Dublin (TCD)	Ireland
IMEGO AB (IMEGO)	Sweden
Elbit Security Systems ltd (ELSEC)	Israel
Athens International Airport SA (AIA)	Greece
Real Fusio France (RF)	France
Immersion SAS (IMM)	France
Red-M Wireless Ltd. (RED-M)	United Kingdom
BAE Systems (Operations) Ltd (BAE)	United Kingdom
Ernst & Young (Israel) Ltd (EY)	Israel
ANA - Aeroportos De Portugal, SA (ANA)	Portugal
INOV, Inesc Inovacao, Instituto De Novas Tecnologias (INOV)	Portugal

COUNTRY

Israel
United Kingdom
Spain
United Kingdom
Italy
Greece
Portugal
France
Italy
Italy
Ireland
Sweden
Israel
Greece
France
France
United Kingdom
United Kingdom
Israel
Portugal
Portugal

VITRUV / Vulnerability Identification Tools for Resilience Enhancements of Urban Environments


© VITRUV

Information

Grant Agreement N°
261741
Total Cost
€4,520,921.80
EU Contribution
€3,339,898.00
Starting Date
01/05/2011
Duration
36 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V
Fraunhofer EMI
Hansastrasse 27c
80686 Germany
Contact
Dr. Werner Riedel
Tel: +49 7628 9050 692
Fax: +49 7628 9050 677
E-mail: werner.riedel@emi.fraunhofer.de
Website:
www.emi.fraunhofer.de

Project objectives

With half of the world's population currently living in urban centres, the security of citizens is of paramount importance and a growing concern. Thus, urban planning practice must incorporate appropriate security measures for vulnerability identification and resilience enhancements. Currently no software tool exists that enables urban planners to take these aspects into consideration.

The objective of VITRUV is the development of software tools that can be used for the long and complex urban planning process. These tools address three different detail levels. Based on an all hazard risk approach, the tools will enable planners:

» to make well-considered systematic qualitative decisions (concept level);

» to analyse the susceptibility of urban spaces (e.g. building types, squares, public transport) with respect to new threats (plan level); and

» to perform vulnerability analyses of urban spaces by computing the likely damage on individuals, buildings, traffic infrastructure (detail level).

Description of the work

Based on urban planner requirements, including financial and procedural limitations and preferences, tools will be developed on three different detail levels.

On the concept level, an overarching methodology will be developed to generate suitable city planning alternatives. A computer support tool will assist the use of this method.

On more detailed levels, algorithms are developed to determine weak points in urban environments. On the plan level, this will be achieved by the use of a database of terrorist attacks and expert judgement using empirical risk analysis. This analysis can be used for a quick susceptibility and risk assessment. The second analysis will be at the detail level. Here an automated (hidden) definition of a larger number of possible attack events will be encoded in algorithms and used to assess repeatedly the damage to different urban assets (building / infrastructure types, their structural members, load bearing concepts and functions). The detail level corresponds to an automated vulnerability analysis in technical terms and is based on quantitative risk analysis sizes. Hazard and damage analysis sizes will be computed for explosive, biological and chemical threats.

Case studies will be used to support the development of the tools as well as for the extended testing and evaluation of the results in the project.

Expected results

Within the VITRUV project, tools on three different levels (concept, plan and detail) are developed that will contribute to enabling the development of more robust and resilient space in the field of urban (re)planning/(re)design/(re)engineering. Planners who use VITRUV's tools will be able to develop urban space which is less prone to and less affected by attacks and disasters, thus sustainably improving the security of the citizens.

PARTNERS	COUNTRY
Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung E.V (Fraunhofer-EMI)	Germany
Crabbe Consulting Ltd (CCLD)	United Kingdom
Provincia di Bologna (BOLOGNA)	Italy
West Yorkshire Police Authority (WYP)	United Kingdom
Schussler-Plan Ingenieurgesellschaft mbH (SP)	Germany
Dissing+Weitling Arkitektfirma A/S (D+W)	Denmark
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	Netherlands
Downey Hynes Limited (DHP)	Ireland
Sigmund Freud Privatuniversitat Wien GmbH (SFU-CEUSS)	Austria
Decisio BV (DECISIO)	Netherlands
Thales Security Solutions & Services SAS (THALES)	France
London Borough of Southwark (SOUTHWARK)	United Kingdom

AMASS / Autonomous Maritime Surveillance System

© Volodymyr Kyrylyuk - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218290
Total Cost
€5,551,702.06
EU Contribution
€3,580,550
Starting Date
01/03/2008
End Date
31/08/2011

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

Project objectives

The AMASS project sought to develop a surveillance system for the observation and provision of actionable data for securing critical maritime areas against potential illegal immigration; and to help prevent the trafficking of weapons, drugs and illicit substances.

The project aimed to carry out the key research and technological development required to engineer an unmanned platform capable of remotely monitoring maritime areas a considerable distance from shore.

Results

AMASS produced original research into hardware and software solutions for a range of engineering challenges, including: a flotation platform, optronics, hydrophones, communication circuits, power management, image exploitation and command and control systems.

These innovations were tested on the AMASS Prototype, a sea-worthy buoy developed by the consortia. Sea trials in shallow, deep and far off-shore locations were conducted in both the Baltic Sea and Atlantic. During one trial, a rubber boat was tracked at a distance of 5km. In another, communications signal strength was tested for two weeks.

The range of sensors, on-board processing units, transmission technology and platform stabilisation hydraulics required to operate the buoy led to some novel operational adaptations. AMASS engineers also had to optimise a range of existing products to meet the low power consumption, low weight and long life time criteria required by the project brief. A power control unit for managing consumption was developed to optimise energy usage.

The Prototype is also capable of interaction with a base station for basic command and control (C2) functions. For instance, much of the hardware, such as the hydrophonic sensors, can operate in a low-energy "detection mode", as well as in an on-request high-energy "classification mode" for in-depth analysis of detected signals. Visualisation tools for a C2 hub were also developed, to allow operators to view on-going developments at sea in real-time.

Whilst only one Prototype was actually tested, AMASS has produced a point-to-point radio operating system that can incorporate as many as 65 buoy units with one operating base station.

This highlights the potential to deploy AMASS platforms in an inter-locking network, for 24/7 wide spectrum surveillance of critical maritime areas.

PARTNERS	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 Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)	Germany
IQ-Wireless	Germany
HSF	Czech Republic
University of Las Palmas de Gran Canaria	Spain

ARGUS 3D / AiR GUidance and Surveillance 3D

© Argus - Fotolia.com

Information

Grant Agreement N°
218041
Total Cost
€4,943,520
EU Contribution
€3,262,050
Starting Date
01/12/2009
Duration
36 months

Coordinator

SELEX SISTEMI INTEGRATI SPA
Civil Systems Business Unit
Via Tiburtina, 1231
n.a.
00131 Rome
Italy
Contact
Claudia Fusai
Tel: +39 06 4150 5370
Mobile: n.a.
Fax: + 39 06 4150 2043
E-mail: cfusai@selex-si.com
Website:
http://www.argus3d.eu/

Project objectives

The overall objective of the ARGUS 3D project is to enhance the security of European citizens, as well as of strategic assets by contrasting, over large areas, unpredictable and unexpected terrorist threats that can be delivered by means of small and low-flying (manned or unmanned) aircraft.

In order to achieve this general objective, the project intends to carry out R&D activities aimed at improving the current ATC systems for civil applications, extending their coverage and making them able to detect, recognise and track non-cooperative targets.

The scientific and technical objective of the ARGUS 3D project is studying, designing and implementing an innovative, low-cost, multi-sensor, radar-based system for 3D air guidance and surveillance (the "ARGUS 3D" system) that integrates conventional surveillance systems currently used for civil applications and two classes of non-conventional radar systems: 3D PSR sensors and networks of multi-operational passive/bistatic radar sensors.

Description of the work

The ARGUS 3D project aims at studying, designing and implementing two types of non conventional radar systems:

» The 3D PSR, a solution that, using a monopulse approach which exploits the difference of the gain of two radar beams of a conventional multi-beam 2D PSR, allows for obtaining an estimation of the aircraft altitude;

» The Passive/Bistatic radars, special forms of radar systems that, rather than emitting pulses, rely on sources of illumination already available in the environment to illuminate potential targets and are able to detect and track objects by analysing the way these objects reflect the signals coming from the transmitters of opportunity.

The ARGUS 3D system functionalities will take into account information provided by innovative 3D PSRs and passive radar networks, processing and merging them with existing radar data, thus exploiting and enhancing the performances and capabilities with respect to conventional surveillance and ATC systems.

The presence of new sensors, with respect to conventional ATC systems, and the final goal of the project (the security enhancement) requires the development of:

» a Consistency function to compare the data from the different sensors and check their integrity;

» a Decision Support function to distinguish between cooperative and non-cooperative air traffic, thus providing a warning every time a risk of terrorist attack occurs and suggesting to the operators the right actions;

» a new Data Presentation function to show, in a dedicated display, further information in addition to conventional air traffic information.

The project includes:

» a controlled demonstration in a real environment of the feasibility of the ARGUS 3D approach and the improvement of ATC security, checking the detectability of low flying small-RCS air vehicles (using the passive radar) and the ability to evaluate the altitude of non cooperative vehicles (using only PSR 3D);

» an evaluation, in a simulated environment, of the overall ARGUS 3D integrated system.

Expected results

The integration of 3D PSR sensors will enhance the capability of the ATC systems of getting 3D information also for Non Cooperative Targets; the introduction of passive/bistatic radar sensors will allow for both extending the conventional surveillance coverage into areas typically not well catered for by current systems (considerably reducing if not completely removing the radar blind zones) and improving the recognition capability of the ATC systems also for Non Cooperative Targets.

PARTNERS	COUNTRY
Selex Sistemi Integrati (SELEX-SI)	Italy
SESM Scarl (SESM)	Italy
Università "La Sapienza" di Roma Dip. di Scienza e Tecnica dell'Informazione e della Comunicazione (INFOCOM)	Italy
Przemysłowy Instytut Telekomunikacji S.A. (PIT)	Poland
University College of London (UCL)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
ENAV S.p.A (ENAV)	Italy
ECONET S.L. (ECONET)	Spain
Dependable Real Time Systems Ltd. (DRTS)	United Kingdom
ISO Software Systeme GmbH (ISO)	Germany
REDHADA S.L. (REDHADA)	Spain
CiaoTech Srl (CTECH)	Italy

CASSANDRA / Common assessment and analysis of risk in global supply chains


© CASSANDRA

Information

Grant Agreement N°
261795
Total Cost
€14,813,514
EU Contribution
€9,958,749
Starting Date
01/06/2011
Duration
36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK
Mobiliteit & Logistiek
Van Mourik Broekmanweg 6
PO Box 49
2600 AA Delft
The Netherlands
Contact
Heather Griffioen-Young
Tel: +31 (0)888665931
Mobile: +31 (0)622461065
Fax: +31-346 353 977
E-mail:
heather.griffioen@tno.nl
Website: www.tno.nl

Project objectives

The main objective is to enable and facilitate the combination of existing information sources in supply chains for containers into new and better visibility that allows the assessment of risks by business and government.

CASSANDRA is combining new tools, hardware, visibility platforms and other technical solutions in such a way that business and government are able to fully adopt a risk based approach to their operational activities, and in particular to combine two strategic customs approaches: the Risk-based approach with the System-based audit approach. As such, it is a more balanced approach than the US driven approach aimed at 100% scanning of incoming containers.

CASSANDRA will facilitate the adoption of a risk based approach in designing and managing efficient and secure supply chains by business. In addition, CASSANDRA will facilitate a dialogue between business and government to gain acceptance of the risk based approach and risk self-assessment by business for supervision by government agencies. This principle of governments' piggy backing on businesses' own risk assessment is becoming a central theme in a number of long term strategies among supervision agencies, such as customs and police.

Description of the work

The main activities in the project are the development of risk based approaches in supply chains and the facilitation of information integration and sharing in the supply chain, by building interfaces between existing visibility platforms, and organizing a consensus building process among business and government agencies to arrive at a commonly accepted framework for risk assessment in the supply chain. CASSANDRA follows very much a data integration and business intelligence approach to risk assessment. As much as possible, this approach relies on existing data sources, data sharing and system integration. Hardware oriented solutions, such as satellite tracking and extensive container scanning, or building completely new platforms or tools are not part of this project.

The project will demonstrate and implement this approach to risk assessment in three so-called living labs. These are set up around major European tradelanes: Asia – North West Europe, North Europe – US and North Africa – Southern Europe.

The nine Work Packages are:

- *WP 1:* Inception and user requirements, ensuring that all partners are at the same level in terms of state of the art and user requirements for supply chain visibility;
- *WP 2:* Risk based approach, developing the risk based approach to supply chain management, and defining the first draft of a business government interaction protocol on risk assessment;
- *WP 3:* Design, development and system integration, containing the IT development activities, which consist of interfaces and dashboard development;
- *WP 4:* Living Lab demonstrations, containing the activities to show the proof of concept in a real life environment;
- *WP 5:* Evaluation and deployment;
- *WP 6:* Policy support, privacy and human issues and networking preparations;
- *WP 7:* Dissemination, networking and consensus building, facilitating further discussion on the business-government interaction that is the result of sharing integral data on supply chain operations;
- *WP 8:* Scientific coordination;
- *WP 9:* Administrative management.

Expected results

- Facilitate the combination of information from existing sources in the entire supply chain;
- Develop advanced system integration of risk assessment and analysis tools to generate more information from the available SC data;
- Demonstrate the possibilities to achieve this information combination in three main European trade lanes;
- Evaluate the proposed solutions and informational content and define business drivers that will provide incentives to businesses to adopt the CASSANDRA solutions;
- Build consensus among business and government agencies on risk assessment and the identification of risk mitigating and disruption management measures;
- This project will contribute to combining two fundamental approaches for e-customs in Europe: Risk-based and System-base audit approach;
- Living Lab structure, based on involvement of the key stakeholders, which will be exploited for the successful pilots.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Erasmus Universiteit Rotterdam (EUR)	The Netherlands
Technische Universiteit Delft (TUD)	The Netherlands
Institut fuer Seeverkehrswirtschaft und Logistik (ISL)	Germany
Fundacion Zaragoza Logistics Centre (ZLC)	Spain
Cross-border Research Academy (CBRA)	Switzerland
GS1 AISBL (GS1 GO)	Belgium
IBM Nederland BV (IBM)	The Netherlands
GMVIS Skysoft SA (GMV)	Portugal
Intrasoft International SA (INTR)	Luxembourg
Atos Origin SAE (ATOS)	Spain
Zemblaz NV (DESCARTES)	Belgium
Senator fuer Wirtschaft und Haefen Bremen (SWHB)	Germany
Ministerie van Financien Directoraat Generaal Belastingdienst (DCA)	The Netherlands
HM Revenue and Customs (HMRC)	United Kingdom
Korps Landelijke Politie Diensten (KLPD)	The Netherlands
Portic Barcelona S.A. (PORTIC)	Spain
ECT Participations (ECT)	The Netherlands
Dbh Logistics IT AG (DBH)	Germany
Seacon Venlo Expeditie B.V. (SEACON)	The Netherlands
BAP Logistics Ltd (BAP)	United Kingdom
Kuehne + Nagel GmbH (K+N)	Austria
DHL Management (Switzerland) Ltd (DHL)	Switzerland
North-South Consultants Exchange LLC (NSCE)	Egypt
Port Authority of Setubal and Sesimbra (APSS)	Portugal
Portbase BV (PORTBASE)	The Netherlands
Integrated Solutions for Ports JSC (ISFP)	Egypt

EFFISEC / Efficient integrated security checkpoints

© Natalia Bratslavsky - Fotolia.com

Information

Grant Agreement N°
217991
Total Cost
€16,071,193.27
EU Contribution
€10,034,837
Starting Date
01/05/2009
Duration
54 months

Coordinator

MORPHO
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@morpho.com
Website: www.effisec.eu

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 effective against any kind of threat.

Seaport checkpoints differ strongly from airport 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, providing a higher security level of identity and luggage control of pedestrians and passengers inside vehicles, at land and maritime check points.

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

EFFISEC will benefit from recent progress in e-Gates for Airport. 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 out by those EFFISEC partners interested in providing security solutions.

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

Expected results

EFFISEC will provide border officers with up-to-date 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 subjecting 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.

PARTNERS	COUNTRY
Morpho (MPH)	France
THALES SECURITY SOLUTIONS & SERVICES SAS (THA)	France
THALES ELECTRON DEVICES SA (TED)	France
SELEX GALILEO SPA (GA)	Italy
ELSAG DATAMAT S.P.A. (ED)	Italy
SMITHS HEIMANN GMBH (SDH)	Germany
Sociedad Europea de Analisis Diferencial de Movilidad SL (SEA)	Spain
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Totalförsvarets Forskningsinstitut (FOI)	Sweden
THE UNIVERSITY OF READING (UoR)	United Kingdom
Ministerul Internelor si Reformei Administrative (RBP)	Romania
Microwave Characterization Center SAS (MC2)	France
ADMINISTRAÇÃO DO PORTO DE LISBOA SA (APL)	Portugal
THALES PORTUGAL SA (THP)	Portugal
SECALLIANCE SECURITES INFORMATIQUES SARL (SEC)	France
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
MULTIX SA (MULTIX)	France

FIDELITY / Fast and Trustworthy Identity Delivery and Check with ePassports leveraging Traveller Privacy

© mattjeacock - iStock

Information

Grant Agreement N°
284862
Total Cost
€18,197,463.60
EU Contribution
€12,013,194
Starting Date
01/02/2012
Duration
48 Months

Coordinator

MORPHO
DTS – Technical and Strategic Department
11 Boulevard Gallieni
N/A
92130 – Issy les Moulineaux - France
Contact
Sébastien Brangoulo
Tel: +33(0) 1 58 11 87 29
Mobile: +33 (0) 6 31 50 47 51
Fax: + 33 (0) 1 58 11 87 01
E-mail: sebastien.brangoulo@morpho.com
Website: www.morpho.com

Project objectives

Significant efforts have been invested to strengthen border ID checks with biometrics Travel Documents embedding electronic chips (ePassport). However, problems appeared regarding fraud in the ePassport issuing process, including personal data leaks, difficulties in certificate management, and shortcomings in convenience, speed and efficiency of ID checks, including the access to various remote data bases.

FIDELITY is a multi-disciplinary initiative which will analyze shortcomings and vulnerabilities in the whole ePassport life cycle and develop technical solutions and recommendations to overcome them. The project will demonstrate privacy enhanced solutions to secure issuing processes, improved ePassport security and usability, and improved management for lost or stolen passports.

FIDELITY will provide more reliable ID checks, hence hinder criminal movements, and ease implementation of E/E records.

FIDELITY solutions will be designed for backwards compatibility to be deployed progressively in the existing infrastructure. The consortium is composed of market-leading companies, innovative SMEs, renowned academia, ethical-sociological-legal experts, and end-users.

Description of the work

SP1 contains all transversal activities, lasting the entire project duration. It includes consortium management, study of ethical, legal and societal aspects and dissemination actions targeting stakeholders, exploitation planning, external cooperation, and training.

SP2 is the technical start point of FIDELITY. It focuses on security and usability of ePassports and issuance processes. SP2 will analyse shortcomings and specify requirements that will guide the development and assessment of FIDELITY solutions. It will prepare recommendations for stakeholders on how to address shortcomings in ePassports, which will be updated with the outcome of FIDELITY results assessment.

SP3 handles all research and development work related to safer travel document issuance. It will provide as the main outcome recommendations and technical solutions enabling trust in a claimed identity, trust in the identity claimant, and trust in protection of private data.

SP4 focuses on the chain of trust for ePassports. Fast, protected and reliable security schemes for "trustable" verification is the main objective. SP4 includes innovative architectures, different protocol configurations, and the security of ID check devices, which process personal data. SP4 will also provide innovative alternatives to the current certificate chain.

SP5 develops a one-stop check concept. This concept will cover biographic and biometric data, packaged for protected and non traceable queries in multiple databases. ID inspection terminals will be developed based on privacy-by-design principles, to implement this secure and reliable one-stop ID check concept.

SP6 "Travel document of the future" studies advanced ePassport improvements that would be possible only under the condition of revising the current Logical Data Structure (LDS), access protocols to the ePassport, and chip requirements for ePassports and readers.

SP7 "Assessment" covers the development of demonstrators of FIDELITY solutions and their assessment. It will develop a set of demonstrators corresponding to the typical ePassport use cases and will assess, on the one hand, the components developed in SP3-SP5, and on the other hand, the integrated demonstrator.

Expected results

Recommendations for a reliable breeder document, secure ePassport application processes, and fixed and mobile terminals for border control; user-friendly ID check solutions with advanced "on-the-fly" biometric sensors, Privacy-by-Design based solutions, and concepts of next generation travel documents and on how to improve (end-to-end) security and the usability of ePassports. Architecture and protocols for certificates management is also expected.

PARTNERS	COUNTRY
Morpho (MPH)	France
Gjøvik University College (GUC)	Norway
Bundeskriminalamt (BKA)	Germany
Ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales (FMI)	France
Hochschule Darmstadt (HDA)	Germany
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IGD)	Germany
Alma Mater Studiorum – Università di Bologna (UBO)	Italy
Thales Communications & Security (TCS)	France
Selex Elsag S.p.A. (SEG)	Italy
Central Directorate for Immigration and Border Police (INT)	Italy
Katholieke Universiteit Leuven – COSIC (KUL)	Belgium
Bundesdruckerei GmbH (BDR)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Biometrika (BIO)	Italy
KXEN (KXN)	France
Institute of Baltic Studies (IBS)	Estonia
Centre for Applied Ethics – Linköping University (LiU)	Sweden
ARTTIC (ART)	France

GLOBE / Global Border Environment

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218207
Total Cost
€999,891
EU Contribution
€999,891
Starting Date
01/07/2008
End Date
30/06/2009

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/

Project objectives

The GLOBE project aimed to produce a comprehensive approach to integrated border management in Europe that factors in the internal, border and global aspects of border management. It set out to assess the existing technical, legal, political and societal environment of Europe's borders, and to suggest information management and integration steps to be taken to enhance border security.

GLOBE was a 'phase one' research project, whose feasibility results will inform a subsequent 'phase two' large scale demonstration project on border management, to be funded in the near future.

Results

GLOBE conducted a comprehensive analysis of current European border management practices, which were compiled into a road-map for future enhancement of these networks.

GLOBE focused, in particular, on the role of the EU's border management agency, Frontex, and bilateral arrangements with the EU's external partners that help member states form an overview of their border management situation.

Two key areas were identified as ripe for further development and synergy in Europe: risk analysis and decision making. GLOBE recommends that the 27 Member States adopt common definitions and criteria for sharing source data, risk analysis results and decision making indicators and reports. Convergence and standardisation in these practices would enable automation in areas such as data gathering, risk assessment and the generation of indicators and reports. GLOBE produced its road-map with these goals in mind.

In the area of border checks, GLOBE focused on potential automated processes for sharing document authentication between member state agencies and external partners. Concepts for innovative technologies to check traveler identity and documents before their arrival at the physical border in order to facilitate the processing in advance low risk passengers were suggested. Supported by an information architecture, this mixture of pre-border document checks and information sharing between neighbours will close loop-holes and expedite legitimate travel, GLOBE concluded.

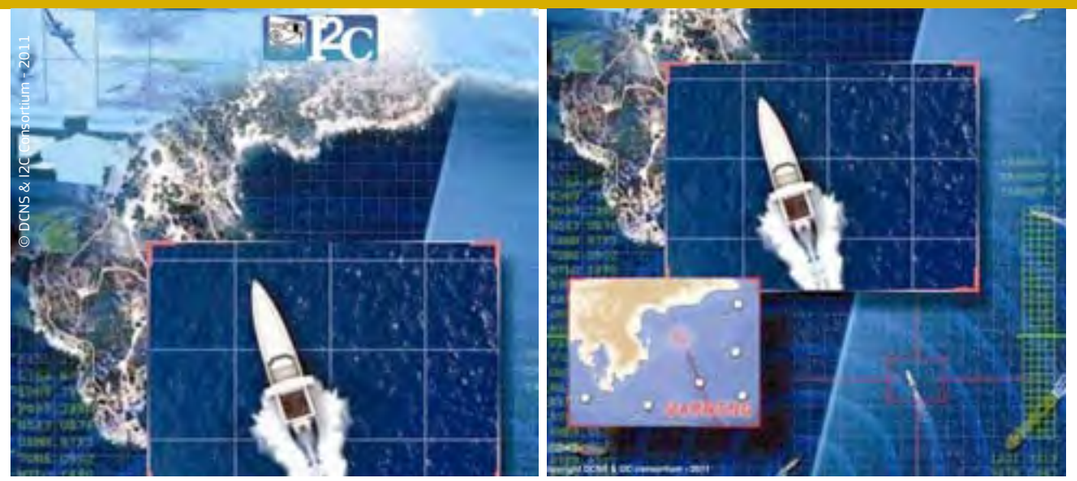
In the area of border surveillance, maritime border monitoring was identified as a priority. GLOBE works to achieve improved situational awareness and assessment via a fusion of surveillance information with information gathered by all relevant monitoring, reporting and information systems – including those of external partners. Modular networks were recommended for this.

In concluding its project road-map, GLOBE suggests that interoperability and dedicated information architecture should be the focus of the phase two Demonstration Project.

© Fotolia.com

PARTNERS	COUNTRY
Telvent Interactiva S.A.	Spain
Amper Sistemas S.A.	Spain
GMV Aerospace and Defence, S.A	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
CIAOTECH Srl (CIAOTECH)	Italy
Fundación Tecnalia Research & Innovation (TECNALIA)	Spain

I2C / Integrated system for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat



Information

Grant Agreement N°
242340
Total Cost
€15,962,707
EU Contribution
€9,869,621
Starting Date
01/10/2010
Duration
48 months

Coordinator

DCNS SA
Direction Systèmes d'Information et de Surveillance
Rond point des artilleurs de marine
B.P 403
83055 Toulon
France
Contact
Michel Morel
Tel: + 33 (0) 498 039 259
Mobile:
+ 33 (0) 699 812 771
Fax: + 33 (0) 498 039 257
E-mail: Michel.Morel@dcnsgroup.com
Website: www.i2c.eu

Project objectives

The I2C new generation of maritime surveillance system must allow:

» Permanent and all weather coverage of border maritime areas;

» Continuous collection and fusion of heterogeneous data provided by various types of sensors deployed on shorelines and on mobile platforms and other information from external sources;

» Supervised automatic detection of abnormal vessel behaviours (in track and performed activity) and generation of justified alarms;

» Understanding of suspicious events and early identification of threats from series of detected spatiotemporal abnormal vessel behaviours (alarms);

» Generation of electronic and formatted interpretation reports on suspicious events to keep decision-making authorities periodically informed.

Description of the work

The tasks to perform in the I2C integration project are:

» To set up an end to end information acquisition and processing system;

» To test the fusion of data from a bench of sensors and other available intelligent information sources in order to perform optimal maritime security awareness.

To do so:

» Two coastal sites are installed with a set of sensors. These shore based platforms provide measurements (AIS messages, radar vessel tracks and optical imageries) to elaborate a maritime situational picture for all vessel types. Platforms at sea will also be deployed (aircraft & vessel patrols, Zeppelin and USV) to provide local node surveillance;

» Fusion of all sensor data with existing information on vessel characteristics (Lloyds Register, Traffic2000, Ship spotting, etc.), on black listed vessels (Paris and Tokyo MOUs), on meteorological conditions (wave height and surface wind speed, etc.) and on geographical data (bathymetry, fishing and protected areas, etc.), will take place to provide an intelligent maritime situational picture;

» Applying rules on verified vessel conditions, to detect abnormal vessel behaviours, then sounding alarms for operators for validation. Examples of rules are:

- Vessels boarding during the night and with low wave height will generate an alarm for a suspect event which can be analysed as trans-boarding of goods such as drugs;
- Vessels stopped in international water for less than thirty minutes and with low surface current speed will generate an alarm for a suspect event which can be analysed as dropping smuggled goods at sea.

» Validated alarms are transferred to experts for understanding and identification of threats. Experts use tool kits to analyse the history of the alarm and its evolution over time with the help of knowledge models on similar past suspicious events already identified.

Expected results

The main outcomes of I2C are:

» Innovative capacities to collect / pre-process / fuse / exploit collected data & information to track all vessel types, and to detect suspicious events and early identification of associated threats;

» Assessments of the added value of the various sensor types and the integrated data processing according to various threats and detection conditions;

» A demonstration showing that the integrated system fulfils the operational needs with prototypes installed in a few operational centres.

PARTNERS	COUNTRY
DCNS SA (DCNS)	France
ROCKVELL COLLLINS France (ROC)	France
FURUNO FINLAND OY (FUR)	Finland
SES ASTRA TechCom SA (AST)	Luxembourg
KONGSBERG NORTCONTROL IT A/S (KON)	Norway
KONGSBERG SPACETEC A/S (KSPT)	Norway
CLEARPRIORITY SA (CLE)	Belgium
ZLT ZEPPELIN LUFTSCHIFFTECHNIK GMBH ET CO KG (ZLT)	Germany
METEOSIM SL (MET)	Spain
AJECCO OY (AJE)	Finland
AIRSHIPVISON INTERNATIONAL SA (AVI)	France
ECOMER (ECO)	France
INTUILAB (INT)	France
SOFRESUD (SOF)	France
ERIC VAN HOOYDONK ADVOCATEN (HOO)	Belgium
ASSOCIATION POUR LA RECHERCHE ET LE DEVELOPPEMENT DES METHODES ET PROCESSUS INDUSTRIELS - ARMINES (ARM)	France
UNIVERSITE PAUL SABATIER TOULOUSE III (IRI)	France
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES - ONERA (ONE)	France
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
DEUTSCHE ZEPPELIN REDEREI GMBH (DZR)	Germany

IMCOSEC / IMprove the supply chain for COntainer transport and integrated SECurity simultaneously


© Netfalls - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242295
Total Cost
€1,142,591
EU Contribution
€930,718
Starting Date
01/04/2010
End Date
31/03/2011

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

Project objectives

This project's main aim was to define a basic concept and strategic roadmap for a large scale Demonstration project for security of supply chains to reconcile the global transportation sector's two conflicting trends: free trade vs transport security.

IMCOSEC opted for an approach that minimises the impact of cost and time, thus making it practicable for commercial operators and enterprises, while creating a "win-win" solution between industry and regulatory authorities. Its concept reached for security that balances effectiveness with practicality within a regulatory framework.

The project analysed security regulations, standards and trends, identified security gaps via a generic model of supply chains based on resilience and threat "trees" or charts, referenced security projects, technologies and industry needs and, finally, defined a roadmap for demonstration activities.

Results

The results of IMCOSEC's six work packages can be summarised as the following:

» A generic transport model was created to represent the essential processes and activities of inter-modal transport chains;

» The security aspects of 42 national and international security programmes were compared to determine what new procedures, if any, were needed for the future Demonstration project. IMCOSEC's researchers concluded that no new regulations are needed, but mutual recognition and standardization among national governments should be the goal;

» Security threats along supply chains were identified and folded into a matrix tool that reflects inter-dependencies and interactions between different supply chain arrangements and each kind of threat. The matrix enables threats to be weighted in importance;

» The project's gap analysis to identify the weakest points of the supply chain concludes there are very few single measures that can improve security and efficiency at the same time. However, it argues that a combination of measures could improve both, thus increasing the competitiveness of both industry and the supply chain;

» IMCOSEC's analysis of security projects, technologies and industry needs revealed that many projects focus on either security or efficiency, but not on security and efficiency at the same time. As for technology, it concludes that the most cost-effective and logical combination of technologies to track cargo shipping would be mobile phone-based ones for the identification, positioning and communications;

» Finally, the project's road-map rests on two broad conclusions. First, it insists that human factors (e.g. employee selection, recruitment and training criteria, responsibility for identification and control processes, etc.) are the biggest issues for supply chain security. "This is of primary importance to successfully reduce the other gaps," says IMCOSEC.

Second, it says security-efficiency measures should take into account the views of all supply chain stakeholders, including shipping consignors and consignees, while promoting technologies that use international standards.

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

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


© Kaarsten - istockphoto.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
241676
Total Cost
€800,047
EU Contribution
€753,372
Starting Date
01/04/2010
End Date
31/03/2011

Coordinator

EFP CONSULTING (UK) LTD.
MOTHERWELL
BRANDON STREET -
OAKFIELD HOUSE
ML1 1XA
UK
Contact
Dana Remes
Phone: +44 141 649 3244
E-mail:
dana@efpconsulting.com
Website: www.logsec.org

Project objectives

The LOGSEC project had the following three main objectives:

» 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.

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

» 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 consisted 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 included:

» literature and project reviews,

» end-user expert interviews,

» user surveys, and

» user workshops.

Results

The LOGSEC project delivered a 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 identified the most relevant/promising research areas and research gaps, to be addressed in a possible follow-up demonstration project. An instrumental part of the roadmap project was to build a basis for future metrics necessary to evaluate supply chain and security performance and to monitor supply chain vulnerabilities.

PARTNERS	COUNTRY
EFP Consulting (UK) Ltd (EFPC)	United Kingdom
ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA (ATOS)	Spain
Cross-border Research Association (CBRA)	Switzerland
European Council of Transport Users (ESC)	Belgium
SZKOLA GLOWNA HANDLOWA W WARSZAWIE (POL)	Poland
Clecat - European Association for Forwarding, Transport, Logistics and Customs Service (CLECAT)	Belgium
Innovative Compliance Europe Ltd (ICE)	United Kingdom
Eidgenössische Zollverwaltung (SC)	Switzerland

OPARUS / Open Architecture for UAV-based Surveillance System

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242491
Total Cost
€1,405,309.68
EU Contribution
€1,188,312.75
Starting Date
01/09/2010
End Date
31/05/2012

Coordinator

SAGEM DÉFENSE SÉCURITÉ
27 rue Leblanc,
75015 Paris
France
Contact
Mr Fernando Barbero
Olivier REICHERT
Phone: 33 1 40 70 67 26
Mobile: 33 6 30 97 23 37
E-mail:
olivier.reichert@sagem.com

Project objectives

OPARUS aimed to define an open architecture for operating unmanned aerial systems (UAS) for wide-area land, coastal and sea border surveillance in Europe. This took into account emerging legislation for the safe deployment of UAS platforms across Europe's controlled civil airspace – a regulatory and technical concept known as "air insertion".

The project's technical work focused on surveillance sensors, aerial platforms, secure data links, communication networks and generic ground control stations. Directly connected to the needs of end-users such as Frontex and national Border Guard authorities, OPARUS also looked at cost-efficient solutions to promote maximum efficiency for UAS-based border surveillance operations.

Results

The project held three workshops to define operational scenarios with end-users and receive their feedback on the project results. The first Workshop focused on technology reviews, operational concepts and the definition of scenarios. Based on answers from end-users regarding 29 missions and 15 scenarios, OPARUS identified 26 user requirements that applied to three main geographical scenarios: Poland for land borders, South Mediterranean for coastal and Canary Islands for sea surveillance.

The second workshop proposed architectures for the three missions, with the third presenting the project's final architecture solutions and associated regulatory framework.

Ethical aspects were presented during workshops with close attention paid to identifying applicable European legislation, operational recommendations and proposal for a future roadmap.

For each of OPARUS' four key UAS technologies – sensors, platform, data link and ground control station – a list of generic products and their technical characteristics and performances was defined and classified, including purchase cost estimates. For example, regarding sensors it looked at electro-optical and infrared detection as well as several types of radar.

In the end, OPARUS came up with a set of solutions covering both short-term and longer-term border surveillance needs. Its open architecture includes:

» cost effective surveillance for "typical" border scenarios;

» room for non-proprietary solutions regarding equipment and sub-systems;

» room for SMEs from many member countries to enter the market;

» the ability of companies to share different parts of a complex system which distributes development costs and risks on a broad basis – an advantage that would foster the development of industrial co-operation similar to the Airbus model.

The project's approach to UAS border surveillance architecture, if commercialised, would deliver a system of different classes of technological sub-systems, which end-users could select for joint operations, leading to "more performance instead of heavily competing single systems".

OPARUS proposed innovative solutions for UAS flight operations with today's technology that could be approved by authorities for land or maritime European border surveillance missions.

PARTNERS	COUNTRY
Sagem Défense Sécurité (SAGEM)	France
Instytut Techniczny Wojsk Lotniczych (AFIT)	Poland
BAE Systems (Operations) Ltd (BAE)	United Kingdom
Dassault Aviation S.A.	France
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
Construcciones Aeronáuticas S.A. (EADS-CASA)	Spain
Israel Aerospace Industries Ltd. (IAI)	Israel
Instituto Nacional de Técnica Aeroespacial (INTA)	Spain
Ingeniería de Sistemas para la Defensa de España S.A. (ISDEFE)	Spain
Office national d'études et de recherches aérospatiales (ONERA)	France
Selex Galileo (SG)	Italy
Thales Communications & Security S.A. (TCF)	France
Thales Systèmes Aéroportés (Thales Syst Aero)	France
Tony Henley Consulting Limited (THL)	United Kingdom

PERSEUS / Protection of European seas and borders through the intelligent use of surveillance

© PERSEUS

Information

Grant Agreement N°
261748
Total Cost
€43,644,979.60
EU Contribution
€27,847,579
Starting Date
01/01/2011
Duration
48 months

Coordinator

INDRA SISTEMAS, S.A.
Security Systems
Av. de Bruselas, 35
28108 Alcobendas (Madrid)
Spain
Contact
Mr Fernando Barbero
Tel: +34 91 2097937
Mobile: +34 647 624 121
E-mail: fbarbero@indra.es
Website:
http://www.perseus-fp7.eu/

Project objectives

The PERSEUS scope is three-fold:

- Design of a system of systems architecture that integrates existing and upcoming surveillance systems as well as innovations created within PERSEUS and those originating from other projects. The goal of the system of systems is to address the complex security missions, focusing on irregular migration and trafficking;
- Validation and demonstration of the system of systems through six exercises representing specific surveillance missions, instantiated in the Western and Eastern regions of the Mediterranean sea;
- Strong involvement of end users to warrant a realistic step by step approach to reach an efficient operational cooperation among the Member States while preserving the national prerogatives;
- In this environment, the PERSEUS demonstration is the most ambitious European research and development project to date, embracing the widest possible list of needs and regulatory contexts and taking into account both the pre-existing initiatives and the foreseen innovations.

Description of the work

PERSEUS contributes to Europe's efforts to monitor illegal migration and combat related crime and goods smuggling by proposing a large scale demonstration of an EU Maritime surveillance System of Systems, on the basis of existing national systems and platforms, enhancing them with innovative capabilities and moving beyond EUROSUR's 2013 expectations, addressing key challenges:

- Supporting the network created by National Contact Centres, Frontex and EMSA through a communication infrastructure and increased surveillance capabilities;
- Implementing transnational exchange of information, and associated procedures and mechanisms, thereby supporting the creation of a common information sharing environment;
- Generating and enhancing a Common Situational Information Picture (CSIP), incorporating tools for surveillance mission planning, providing decision and interception support and providing quasi real-time sharing of information;
- Improved detection and identification of non collaborative/suspicious small boats and low flying aircraft;
- Enhanced and increasingly automated detection of abnormal vessel behaviours, identification of threats and tracking.

Expected results

PERSEUS will deliver:

- A system of systems representative of what will be available from 2015 onwards;
- A target vision for an integrated European maritime border surveillance system;
- A set of recommendations and best practices to instantiate this target vision in different contexts and to extend it to more countries, based on the user and provider feedbacks acquired through two real-life exercises operating in the Western and Eastern Mediterranean regions.

PARTNERS	COUNTRY
INDRA SISTEMAS S.A. (INDRA)	Spain
EADS DEFENCE AND SECURITY SYSTEMS (EADS-DS)	France
DCNS SA (DCNS)	France
ENGINEERING INGEGNERIA INFORMATICA SPA (ENGINEERING)	Italy
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA (ISDEFE)	Spain
EADS - CONSTRUCCIONES AERONAUTICAS S.A. (EADS-CASA)	Spain
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSRD)	Greece
GUARDIA CIVIL ESPAÑOLA (GUARDIA CIVIL)	Spain
INSTITUTT FOR FREDSFORSKNING STIFTELSE (PRIO)	Norway
SAAB AKTIEBOLAG (SAAB)	Sweden
SES ASTRA TECHCOM SA (SES-ASTRA)	Luxembourg
AJECO OY (AJECO)	Finland
INTUILAB (INTUILAB)	France
METEOSIM SL (METEOSIM)	Spain
LUXSPACE SARL (LUXSPACE)	Luxembourg
SOFRESUD (SOFRESUD)	France
INOV, INESC INOVAÇÃO, INSTITUTO DE NOVAS TECNOLOGIAS (INOV)	Portugal
SKYTEK LTD (SKYTEK)	Ireland
LAUREA-AMMATTIKORKEAKOULU OY (LAUREA)	Finland
DFRC AG (DFRC)	Switzerland
BOEING RESEARCH & TECHNOLOGY EUROPE S.L. (BR&TE)	Spain
ECORYS NEDERLAND B.V. (ECORYS)	Netherlands
CORK INSTITUTE OF TECHNOLOGY (CIT)	Ireland
MINISTERE DE L'INTERIEUR, DE L'OUTREMER ET DES COLLECTIVITES TERRITORIALES DIRECTION DE LA DEFENSE ET DE LA SECURITE CIVILES (MOI FRANCE)	France
FORÇA AÉREA PORTUGUESA (FAP)	Portugal
SATWAYS - PROIONTA KAI YPIRESIES TILEMATIKIS DIKTYAKON KAI TILEPIKINONIAKON EFARMOGON ETAIRIA PERIORISMENIS EFTHINIS EPE (SATWAYS)	Greece
MINISTRY OF NATIONAL DEFENCE, GREECE (HMOD)	Greece
NATO UNDERSEA RESEARCH CENTRE (NURC)	Italy
MINISTRY OF CITIZENS PROTECTION (MCP-HCG)	Greece

SEABILLA / Sea border surveillance

© Colette - Fotolia.com

Information

Grant Agreement N°
241598
Total Cost
€15,558,125.80
EU Contribution
€9,841,603.55
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

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 in 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 the coast.

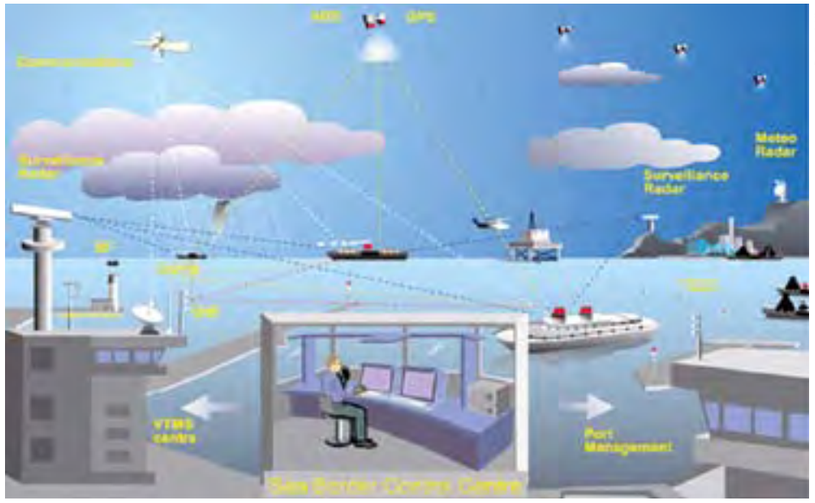
Description of the work

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 cooperative 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 the Canary Islands to the Azores in line with the EU Integrated Maritime Policy and the EU Integrated Border Management Policy (ref. EUROSUR), and in compliance with Member States' sovereign prerogatives.



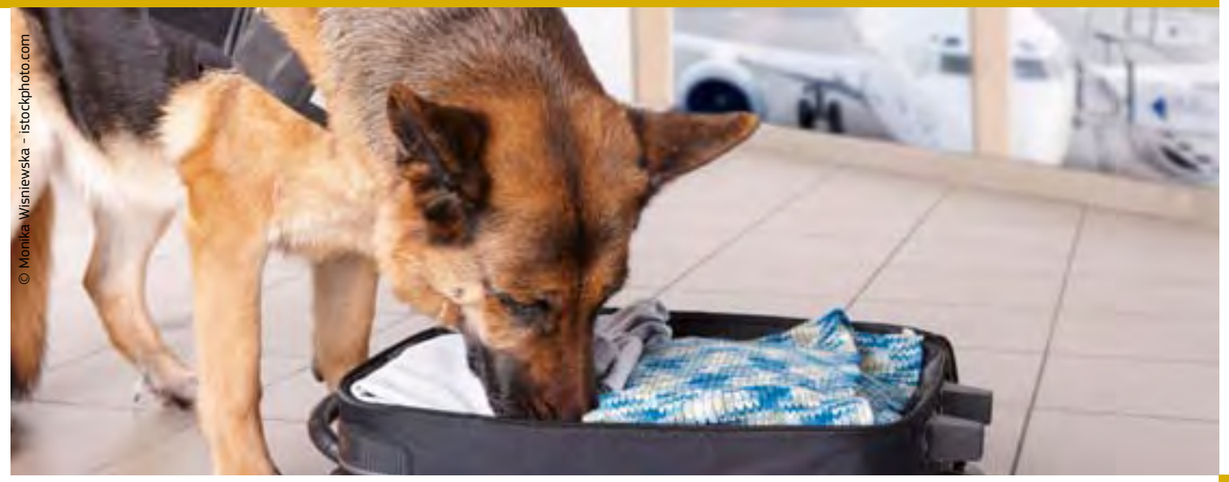
© Seabilla

Expected results

The project will provide a feasible, cost effective solution in terms of maritime surveillance, based on the 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 successfully address Maritime Security and Safety challenges.

PARTNERS	COUNTRY
SELEX Sistemi Integrati SPA (SSI)	Italy
Alenia Aeronautica	Italy
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)	Italy
BAE Systems (Operations) Ltd (BAES)	United Kingdom
Correlation Systems (CorrSys)	Israel
Cassidian S.A.S. (EADS DS)	France
Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)	Portugal
Eurocopter España (ECE) (ECE)	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Holland Institute of Traffic Technology BV (HITT Traffic)	The Netherlands
Indra Espacio S.A. (IE)	Spain
Indra Sistemas S.A. (INDRA)	Spain
European Commission - Joint Research Centre (JRC)	Belgium
Mondeca S.A. (Mondeca)	France
Sagem Défense Sécurité (SAGEM)	France
Space Applications Services N.V./S.A (SpaceApps)	Belgium
Thales Alenia Space Italia S.p.A. (TASI)	Italy
Thales Defence Deutschland GmbH (TMSS)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Telespazio S.p.A. (TPZ)	Italy
Thales Systèmes Aéroportés S.A. (TSA)	France
TTI Norte (TTI)	Spain
University College London (UCL)	United Kingdom
Universidad de Murcia (UMU)	Spain
University of Portsmouth Higher Education Corporation (UoP)	United Kingdom
Thales Alénia Space France (TASF)	France
Thales Communications & Security S.A. (TCF)	France

SNIFFER / A bio-mimicry enabled artificial sniffer



© Monika Wisniewska - istockphoto.com

Information

Grant Agreement N°
285203
Total Cost
€ 4,837,982.97
EU Contribution
€ 3,493,820.72
Starting Date
01/02/2012
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Diamond Sensors Laboratory
Centre d'Etudes de Saclay
91191 Gif-sur-Yvette,
France
Contact
Emmanuel Scorsone
Tel: +33 1 6908 6934
Fax: +33 1 6908 7819
E-mail:
emmanuel.scorsone@cea.fr
Website: Not available
(due month 3/end of April)

Project objectives

The SNIFFER project proposes a highly innovative one-stop shop approach to complement sniffer dogs and leverage their capabilities. This approach is based on state-of-the-art technologies centred on a new generation of olfactory biosensors. The SNIFFER devices to be developed integrate sampling, pre-concentration and pre-treatment with bio-mimicry, synthetic diamond sensor technology and multi-parametric training software. This will enable the detection of odours arising out of security threats which may occur in a panel of border security applications, such as the detection of illegal substances carried by people and in suitcases (open or on a luggage belt) and cars or the detection of hidden people in containers.

Description of the work

The SNIFFER project will be pulled and driven by concrete usage cases corresponding to major border security applications of artificial sniffing. To make sure that the SNIFFER project is efficiently managed, the consortium will work against common global milestones which structure the project in a set of V1 solutions (at midterm) and V2 solutions (at the end of the project).

A first work package will define the usage cases and corresponding metrics, validate them at midterm and at the end of the project and cover the societal and ethical implications of introducing SNIFFER technology in the respective usage contexts.

A second work package will deal with the integration and testing of different sub-systems, namely the sampling, pre-concentration and pre-treatment of target analytes module developed in a third work package, as well as the multisensory array developed in a fourth work package.

Multi-parametric training software will also be adapted in order to cover the broad range of different odours targeted by the SNIFFER project.

A whole work package will also be dedicated to odorant proteins engineering which is one of the core technologies of the SNIFFER project along with the innovative diamond based transducers.

Finally another work package will investigate different aspects of self-diagnostics for artificial sniffers.

SNIFFER is a two-step incremental project. A first version of the SNIFFER devices will be developed to answer the needs expressed by the users at the beginning of the project (month 1 to 23). A second version will then be consolidated taking into account the feedback given by the users on V1 (month 24 to 36).

Expected results

SNIFFER devices cover the variety of border security situations in which dogs are used today. Their capabilities will allow security forces to operate 24/7, while saving the use of real dogs for cases in which they can potentially make a difference.

Thanks to the SNIFFER devices, border security, especially at airports, will be significantly enhanced as regards illegal trafficking of all kinds (drugs, tobacco, illegal immigration…) as well as terrorist acts (thanks to explosive detection).

PARTNERS

Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LIST/LCD)	
The University of Manchester (UNIMAN)	
Ministère de l'Intérieur - Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure (ST(SI)²)	France
Association pour la Recherche et le Développement des Méthodes et Processus industriels (ARMINES)	France
EADS Deutschland GmbH – Innovation Works (EADS)	Germany
Ecole Polytechnique Fédérale de Lausanne (EPFL)	Switzerland
Centre for Science, Society and Citizenship (CSSC)	Italy
The University of Padua (UNIPD)	Italy
Chambre de Commerce et d'Industrie de Paris (ESIEE)	France
GTP Technology (GTP)	France
TraceTech Security (TTS)	Israel
3D General Aviation Applications SA (3DSA)	Greece
Israel National Police (INP)	Israel
ARTTIC Belgium (ART)	France

COUNTRY

France
United Kingdom

SNIFFLES / Artificial sniffer using ion trap technology

© WAGTAIL

Information

Grant Agreement N°
285045
Total Cost
€ 5,226,007.41
EU Contribution
€ 3,493,625.00
Starting Date
01/01/2012
Duration
36 months

Coordinator

TWI LTD
Commercial Group
Granta Park
Great Abington. CB21 6AL.
Cambridge.
United Kingdom.
Contact
Debbie McConnell
Tel: +44 (0)1223 899000
Fax: +44 (0)1223 890952
E-mail:
debbie.mcconnell@twi.co.uk
Website: www.twi.co.uk

Project objectives

The goal of the SNIFFLES project is to develop a Linear Ion Trap Mass Spectroscopy (LIT MS) based device that has a mass range larger than other comparable MS techniques. Additionally, methods for miniaturisation and modularisation will be applied to allow reduced vacuum demand and upgradeability. Miniaturisation will be made possible through improved designs based on results from modelling, implementation of novel manufacturing techniques and improvements in the MS drive electronics and vacuum system.

The objectives of the SNIFFLES system are to be able to detect weapons, drugs and hidden persons at border crossings; identifying in parallel the elemental, molecular or biological composition all at a high speed of detection.

To ensure the suitability for real world applications the system will have a stand-off capability whilst being a complementary technique to that of sniffer dogs.

Description of the work

The areas of work that will: be undertaken within the project will be carried out in 3 phases:

» Phase 1 will concentrate on project road mapping that will provide a holistic overview of the gas sensor device development, within the context of creating a robust and reliable artificial sniffer. This will specify the device performance and enable all of the individual technical sub-system activities to be undertaken. After this initial output, it will continue to run, focussing on forming a structured approach to define the operational procedures of the final device;

» Phase 2 will be the technical development of each of the sub-systems that will be implemented into the artificial sniffer. Ion trap development will ensure a device with high sensitivity whilst using novel manufacturing techniques to create a device with a small footprint and small cost.

The electronic control unit development will ensure that the ion trap functions to its highest specification and the measurements taken are accurate and reliable.

The vacuum sub system will be technologically advanced to enable the high performance of the system whilst ensuring that the whole system can be contained within the smallest footprint possible.

The operating conditions of the linear ion trap will be adjusted to confirm that each stage of the mass spectrometer is operating at its highest performance with the best sensitivity and resolution. The sample inlet operation will be designed, enabling the correct operation of the device whilst sampling the multiple substances required.

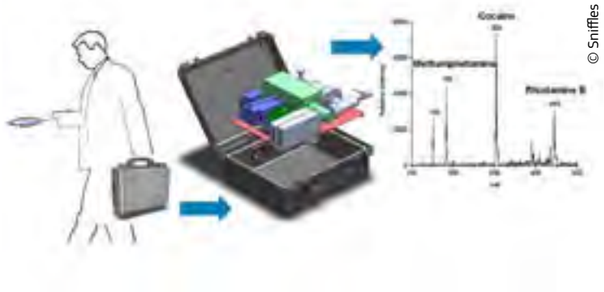
The end stage of phase 2 is the system integration to ensure that each sub system is working in synchronicity with its partners;

» Phase 3 is where the device will undergo its testing and validation program so that the SNIFFLES device is optimised for border control points. The testing will integrate a number of development stages including feedback from live field testing trials.

Expected results

The main outcome of the project will be a device that can work in collaboration with existing sniffer dog teams at border check points; this includes high speed detection and continuous monitoring of air and surfaces to prevent transport of illegal substances at crossing points on land and at airports and seaports.

The overall device will be a portable system aided by the integration of the vacuum system using new materials.



© Sniffles

PARTNERS

TWI Ltd (TWI)
The University of Liverpool (UOL)
Université Aix-Marseille 1 Provence (UdP)
DSM R&D Solutions BV (DSM)
Q Technologies Ltd (Qtec)
SAES Getters S.p.A (SAES)
Envisiontec GMBH (ENV)
Xaarjet AB (XAAR)
Wagtail UK Ltd (WAG)

COUNTRY

United Kingdom
United Kingdom
France
Netherlands
United Kingdom
Italy
Germany
Sweden
United Kingdom

SUPPORT / Security UPgrade for PORTs

© Herbert Rubens - Fotolia.com

Information

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 LTD
Research Directorate
Goodrich House, 1 Waldegrave Road
TW11 8LZ, Teddington
UK
Contact
Jenny Gyngell
Tel: +44 (0)1933 625958
Mobile:
+44 (0)7717 803105
Fax: +44 (0)1933 625958
E-mail:
jgyngell@bmtmail.com
Website:
http://www.support-project.eu/

Project objectives

The primary project objective is to support the principal stakeholder groups involved in the security of European main sea and/or inland ports to build distributed cooperative security systems. SUPPORT will facilitate optimised interchange of surveillance and administrative information as well as threat alerts between port stakeholders, thus enabling cost effective, multiple use of available data in tailored decision support systems.

SUPPORT solutions will: provide integrated state-of-the-art surveillance/security systems for border control; assist port security operators in decision making; take into account the port's organisational structure and operational modalities; and ensure that differing legal and regulatory constraints and standards for security are met in a cost effective manner.

Description of the work

The work programme will start with requirements analysis including Gap and Threat Scenario Analysis, Regulatory and Stakeholder Analysis and Security Technology Assessment and Forecasting. The output from these activities will direct the development of Generic Models for EU Ports Security. These will be validated by operational experts from the SUPPORT participants and will be used to support a 'European standardised approach for port security information exchange and training'. The Generic Models will be installed in the SUPPORT Models Repository and will be used to produce service registries for specific ports. These registries will support their specific circumstances and will contain the information they wish to share with whom on a peer-to-peer basis. Each peer will have its own (possibly unique) view on the total security information and will hence need its own tailored decision support system. The Generic Models will also provide the basis for assessing existing systems and simulating appropriate upgrade solutions.

Evaluation will be undertaken in terms of both improvements in security performance and cost benefit analysis.

Two full scale demonstrators have been planned, one to represent a state of the art situation and the second to represent typical conditions in European ports.

These demonstrators will simulate a full scale installation of the SUPORT Platform with integration with existing systems facilitating measurements of the impact on both the security and efficient operation of the port.

Expected results

SUPPORT will deliver:

» 'validated' generic port security management models (capturing reusable state-of-the-art and best practices) that can be customised for specific ports;

» training and open standards based tools to aid security upgrade in EU ports.

These will be complementary to, and usable by, other EU projects and initiatives.

© Support

PARTNERS

BMT Group Ltd. (BMT)
Totalförsvarets Forskningsinstitut (FOI)
Securitas (Securitas)
Technical Research Centre of Finland (VTT)
MARLO (Marlo)
INLECOM Systems (ILS)
MARINTEK (Marintek)
Nautical Enterprise (NECL)
STENA (Stena)
eBOS Technologies (eBOS)
University of Innsbruck (UIBK)
Cargotec Port Security (CA)
Maritime Administration of Latvia (MAL)
INRIA (Inria)
MARAC Electronics (ME)
Port of Piraeus (PPA)
EUROPHAR - EEIG Port of Valencia - Marseille – Genoa (PV)
Gemeente Amsterdam (PA)
Stichting Ecoports (EP)

COUNTRY

United Kingdom
Sweden
Sweden
Finland
Norway
United Kingdom
Norway
Ireland
Sweden
Cyprus
Austria
Finland
Latvia
France
Greece
Greece
Spain
The Netherlands
The Netherlands

TALOS / Transportable autonomous patrol for land border surveillance system


© TALOS

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218081
Total Cost
€19,878,692
EU Contribution
€12,898,332
Starting Date
01/06/2008
End Date
31/05/2012

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

Project objectives

TALOS is an innovative, Adaptable Land Border Large Area Surveillance System, based on transportable surveillance integrated with rapidly deployable, mobile, unmanned ground and air vehicles, which will address new challenges of external land borders of the enlarged European Union.

The 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's 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 the 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 the TALOS system concept all over Europe, and to contribute to the ongoing efforts of their standardization in Europe;

» To show the cost-effectiveness of the TALOS mobile/transportable concept as opposed to conventional stationary border surveillance solutions.

The main TALOS innovation covers:

» Scalability – its ability to change system scales easily 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 vehicles and the Command & Control system;

» Mobility/transportability – the whole system will be Mobile/Transportable, installed in standard containers, and transported on trailers for fast deployment in selected border zones (according to intelligence);

» Tactical learning/adaptation behaviour – during the development process, the system will be adapted to local operational requirements, operators will be interrogated and their needs implemented in a system mission planning module;

» No need for fixed infrastructure or fences – the TALOS system, owing to its mobility and transportability, does not require any fixed infrastructure or fences;

» Enables response to intrusion in minutes – system will respond to intrusion in a matter of minutes, not hours; and

» Usage of "green" energy – in remote locations (where it is impossible to connect to standard power lines) the energy will be drawn from natural sources e.g. by means of solar panels (sunny area), wind towers (windy area), water wheels (near rivers).

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	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

VIRTUOSO / Versatile information toolkit for end-users oriented open sources exploitation

Information

Grant Agreement N°
242352
Total Cost
€11,497,567.53
EU Contribution
€7,999,182.55
Starting Date
01/05/2010
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
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
Website:
http://www.virtuoso.eu/

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:

» Improve the situational awareness of those organisations and individuals charged with securing Europe's borders;

» Help anticipate risks such as terrorism, illegal migration and the trafficking of goods and people using OSINF;

» 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;

» 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.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LIST)	France
Defence and Security Systems (EADS)	France
Origin Sociedad Anonima Espanola (ATOS)	Spain
Mondeca SA (Mondeca)	France
Newstin a.s (NWT)	Czech Republic
SAIL Technology AG (SailLabs)	Austria
Aalborg University (AAU)	Denmark
Thales Communications (TCF)	France
Bertin Technologies (Bertin)	France
Stichting Katholieke Universiteit / Brabant Universiteit Van Tilburg (TILT)	The Netherlands
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Ingenieria de Sistemas Para la Defensa de Espana SA (Isdefe)	Spain
Hawk Associates Limited (HAWK)	United Kingdom
Eidgenössische Technische Hochschule Zürich (ETH Zurich)	Switzerland
Compagnie Europeenne d'Intelligence Strategique (CEIS)	France
Universita Degli Studi di Modena e Reggio Emilia (CRIS/UoM)	Italy
Columba Global Systems Ltd. (Columba)	Ireland
Thales Research and Technology (THALES)	France

WIMAAS / Wide maritime area airborne surveillance

© WIMAAS

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217931
Total Cost
€4,001,123
EU Contribution
€2,737,169
Starting Date
01/12/2008
End Date
30/11/2011

Coordinator

THALES SYSTEMES AEROPORTES 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

Project objectives

WIMAAS aimed to assess the potential cost reduction, efficiency and enhanced border control benefits for European maritime domain surveillance to be gained via a large-scale integration of unmanned or otherwise remotely piloted airborne vehicles. The project explored the application of such systems for tracking illegal immigration, illegal fishing, smuggling, pollution and terrorist threats.

The final outcome aimed to develop simulation models based on operational scenarios, innovative concepts and technologies for unmanned systems, in-flight experiments, a detailed cost benefit analysis and, finally, a roadmap for the wider use of unmanned aerial vehicles (UAVs), including R&T priorities and future program suggestions.

Results

The primary outcome of the project was the exploration of a future "system of systems" (SoS) architecture incorporating UAVs to produce complete maritime domain awareness.

The first step of the project was to gather and analyze the future needs of potential End-Users in charge of maritime surveillance on European borders. End-user consultations included 10 national and military authorities, plus Frontex. This led to the generation and simulation of scenarios such as drug trafficking between North Africa and Spain, illegal fishing in the Aegean, illegal immigration between Libya and Italy and a theoretical terrorist hijacking in the strait between Cyprus and Turkey.

WIMAAS was considered as a generic system including all airborne platforms (PF) in the maritime 3rd dimension. The notion of system covers the platforms, their sensors, airborne or ground Command and Control system to coordinate PF tasks, to exploit data before transmission to SoS, and the communication system enabling data exchange between platforms with crews, and between PF and SoS.

Further research aimed to develop the multi-sensor concepts required to integrate UAVs into existing maritime domain awareness processes.

On board processing and fusion is analysed for observation payloads to reduce data throughput transmission, to improve levels of automation, to decrease the amount of exchanged data and to reduce data link bandwidth, paving the way for miniaturisation of the airborne mission segment.

The Sensor and data fusion concepts on the ground address the definition of a solution to reach a level of situation awareness, which allows the timely detection and prevention of events threatening maritime security and the environment. The challenge is rather to process and represent them in an intelligent and meaningful way to give sufficient information support to human decision-makers.

Dynamic tasking provides an aid to decide the path of aircraft in the area of interest. The issue is to dynamically plan the path of the airborne platform in order to comply with the mission objective (reach in a specified time an observation position) periodically updated by real time detection or objects of interest generated by its own sensor or by an external sensor. An algorithm has been developed and experimented.

A crew concept was also developed to assess the personnel requirements and workload management needed to operate UAVs from a central base station. An optimal mission length and crew size was aggregated from a series of mission scenarios.

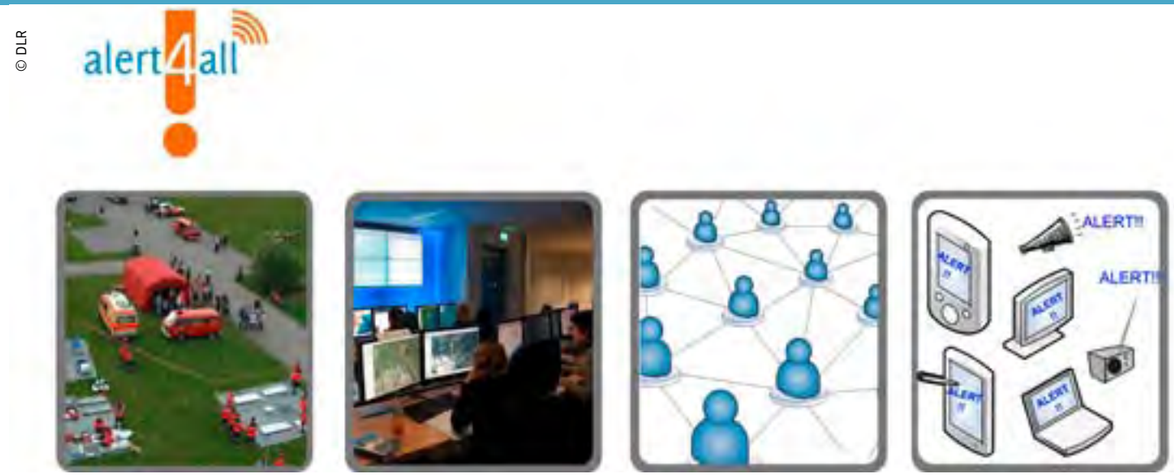
A communication study has defined an innovative architecture for complete data communications between air vehicles and the ground segment, introducing innovative access techniques and interfaces.

The project concludes that there is no single multi-purpose UAV platform capable of covering every altitude and maritime environment. A multi-platform category system-of-systems would be required.

To facilitate further research into this, WIMAAS concluded with a cost estimate based on varying degrees of mission intensity and the use of multiple (up to 10) types of UAV platforms. These cost estimates, excluding training and maintenance expenses, can now form the basis of a policy assessment for implementing a wide maritime area surveillance network based on UAVs.

PARTNERS	COUNTRY
Thales Systemes Aeroportes S.A	France
SELEX GALILEO	Italy
Dassault Aviation	France
SENER Ingeneria y Sistemas	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)	Germany
European Commission - Joint Research Centre (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

A4A / Alert for All



Information

Grant Agreement N°
261732
Total Cost
€4,881,506
EU Contribution
€3,497,469
Starting Date
16/03/2011
Duration
30 months

Coordinator

DEUTSCHES ZENTRUM FÜR LUFT- UND RAUMFAHRT E.V.
Institute of Communications and Navigation
Linder Hoehe
51147 Cologne
Germany
Contact
Cristina Párraga Niebla
Tel: +49 (0) 8153 282824
Mobile:
+49 (0) 1727134781
Fax: +49 (0) 8153 282844
E-mail:
Cristina.Parraga@dlr.de
Website: www.alert4all.eu

Project objectives

The overall objective of A4A is to improve the effectiveness of alerts and communication to the population in crisis management.

To achieve this goal, A4A will provide an extensive and interdisciplinary alerting framework that integrates the key enablers to achieve significant improvements in terms of the level of alert penetration, cost-benefit ratio and intended vs. actual impact of alert strategies. With the project results, A4A aims at contributing to lay the foundations of an effective alert and communication paradigm that is scalable from the regional to pan-European range.

A4A will provide solutions to align alert procedures and processes in contemporary crises (natural or man-made) with available and emerging information management and communication technologies, emerging information sources and trends in social and human behaviour.

Description of the work

A4A builds its alerting concept on five research areas that are key enablers to achieve the aimed effectiveness improvements: authorities' and responders' operations, human behaviour, the role of new media, information management and communications technologies.

As a multi-disciplinary alerting framework, A4A will develop and exploit synergies among its research areas. In particular, the A4A work plan foresees the following research activities:

» To develop a suitable communications protocol and a scalable alert message dispatcher that connects several mass market communications technologies to disseminate alerts in a multi-channel approach, including satellite components, to consumer devices, providing ubiquitous penetration of the alert system and resilience in the face of major disasters;

» To develop a portal for efficient information management that enables the coordination and common situational awareness of involved authorities and responders, enhancing the (common) operational picture for optimizing the alert strategies;

» Situational awareness and trends in social behaviour will be addressed from two different perspectives: (i) understanding the impact of alerts in the population and (ii) understanding the role of new media, such as social networks, during the crisis. The first aspect will be tackled by research and modelling of social behaviour in crisis. From this research, an alert impact simulation tool will be developed to support decision making processes in crisis management. The second aspect will be tackled by investigating the information flows and their timing during crisis to understand the role of new media and by developing tools to efficiently monitor the information exchanges within new media to improve the situational awareness of authorities, especially on the perception of the society of the crisis situation;

» The integration of these research activities will allow for defining recommendations for the improvement of operational concepts that make use of and benefit from the A4A tools. Furthermore, the development of training material for authorities and responders will contribute to the end user acceptance.

Investigations on organisational, institutional and funding aspects for the deployment of A4A and a final showcase will complete the A4A activities.

Expected results

Through its research activities A4A will provide an extensive and scalable alerting and communications concept that is capable of optimising the penetration and impact of alerts and can be incrementally deployed, both in terms of technologies/features and in terms of operating range, from a regional to a pan-European scope.

PARTNERS	COUNTRY
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
German Red Cross (DRK)	Germany
Avanti Communications Ltd. (AVA)	United Kingdom
BAPCO LBG (BAPCO)	United Kingdom
TECNOSYLVA S.L. (TSYL)	Spain
Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)	Portugal
Fundación Tecnalia Research & Innovation (Tecnalia)	Spain
Universität Stuttgart (USTUTT)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	Germany
Eutelsat S.A. (EUT)	France
Institut fuer Rundfunktechnik GmbH (IRT)	Germany

ACRIMAS / Aftermath Crisis Management System-of-systems Demonstration - Phase I

© Federal Office of Civil Protection and Disaster Assistance (BBK) Germany

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261669
Total Cost
€1,666,022
EU Contribution
€1,109,381
Starting Date
01/02/2011
End Date
31/05/2012

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Technological Trend Analysis (INT), Department for Meta-Analyses and Planning Support
Appelsgarten 2
PO Box 14 91,
53879 Euskirchen
Germany
Contact
Hans-Martin Pastuszka
Tel: +49 (0)2251 18 298
Fax:
+49 (0)2251 18 38 298
E-mail: hans-martin.pastuszka@int.fraunhofer.de
Website: www.acrimas.eu

Project objectives

The Phase I project ACRIMAS, a 15-month Support Action with 15 partners from 10 European countries, elaborates a systematic integration process for crisis management (CM) systems, procedures and technologies in Europe, to be implemented within a Phase II demonstration programme. The process will allow for gradual evolvement of CM capabilities through demonstration and experimentation (DE) activities, facilitating Europe wide collaboration, cooperation and communication in CM at different levels of decision making, and respecting the different CM approaches and ambitions of the EU Member States. This process will improve the transfer of related knowledge between stakeholders and promoting an environment for co-development of CM technology and methodology in R&D where users and providers work together.

ACRIMAS further emphasises community-building which will be considerably supported by the execution of the subsequent Phase II, bringing together the various key stakeholders and the available DE infrastructures in a case-by-case demonstration or experimentation activity.

Description of the work

Large-scale incidents (man made and natural) inside and outside the EU require a coordinated response from crisis managers and first responders across Europe and with resources from all levels of government. Among others, a common operational picture, well trained and equipped teams, secure communications, and mission flexibility are core assets for successful CM.

Currently, CM in the EU can be regarded as a highly diversified 'system-of-systems' integrating organisations and components with different cultures, policies and assets, and various stakeholders and procurement schemes. This 'system-of-systems' incorporates technology, procedures, organisational concepts, and human factors. To identify the relevant/critical/ urgent areas and topics within this current CM 'system-of-systems' which need to be addressed by the demonstration programme in Phase II, ACRIMAS follows a scenario-based and user-centric work approach.

ACRIMAS is scenario-based in the sense that characteristic CM scenarios will be identified, selected and developed to constitute a sound basis for ensuring the work of posing user needs and requirements, identifying current weaknesses and gaps in CM in Europe, looking at potential solutions and documenting corresponding demonstration topics and R&D needs to be integrated in a roadmap for Phase II. The scenario approach embraces an all-hazard view, including the EU external dimension.

ACRIMAS is user-driven in the sense that users and other stakeholders in terms of first responders, authorities and governmental bodies as well as the supply side are actively involved throughout the project process, some of them as full partners, most of them linked to the project through a supporting Expert Group and dedicated project workshops. They play a central part in complementing and validating the scenario analysis by expressing their needs and requirements regarding the identification of relevant CM topics, which should be addressed by DE activities in Phase II, and the demonstration concept to be elaborated.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-INT)	Germany
CRISIS MANAGEMENT INITIATIVE (CMI)	Finland
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSRD)	Greece
NEDERLANDS INSTITUUT FYSIEKE VEILIGHEID (NIFV)	The Netherlands
T-SOFT AS (TSOFT)	Czech Republic
TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)	Sweden
EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)	Belgium
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (TNO)	The Netherlands
TURKIYE KIZILAY DERNEGI (TRCS)	Turkey
TECHNOLOGIES SANS FRONTIERES ASBL (TSF)	Belgium
UNITED NATIONS UNIVERSITY (UNU-EHS)	Germany
Cassidian S.A.S. (EADS)	France
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
PUBLIC SAFETY COMMUNICATION EUROPE FORUM AISBL (PSCE)	Belgium

ANTIBOTABE / Isolation of recombinant antibodies neutralizing botulinum toxins A, B and E

Information

Grant Agreement N°
241832
Total Cost
€3,896,416
EU Contribution
€2,966,386
Starting Date
01/09/2010
Duration
48 months

Coordinator

CENTRE DE RECHERCHE DU SERVICE DE SANTÉ DES ARMÉES
Unité de biotechnologie des anticorps, et des toxines
24, avenue des Maquis du Grésivaudan
B.P. 87
38702
Contact
Philippe Thullier
Tel: + 33 (0)4 76 63 69 14
Mobile:
+ 33 (0)6 86 74 75 66
Fax: + 33 (0)4 76 63 69 17
E-mail: pthullier@yahoo.com
Website:
http://www.antibotabe.eu

Project objectives

Botulinum neurotoxins (BoNTs) are among the most toxic substances known, whether of biological or chemical origin, and they are part of the "dirty dozen" agents listed as possible bioweapons. Beside voluntarily contamination, naturally-occurring food intoxications, though rare but often severe, are still encountered and intoxication due to the cosmetic use of an unauthorized BoNT has also been reported. Despite extensive research, no small synthetic molecule has been validated for therapeutic use against BoNTs, and Europe relies on an old stockpile of horse polyclonal antibodies as the sole BoNTs-neutralizing medicines. Recombinant antibodies are a highly successful new class of therapeutic molecules, produced by biotechnologies, showing an exponential-like growth. The goal of AntiBotABE is to isolate recombinant antibodies neutralizing BoNT A, B and E as these types are lethal for humans. The heavy and light chains will be targeted for a synergistic effect, thus six recombinant antibodies have to be isolated. For this project, the strategy that allowed prior isolation of neutralizing antibodies against ricin and the lethal toxin of anthrax will be re-utilized.

Description of the work

This project will start with recombinant proteins, part of the light or heavy chains of BoNT A, B and E and utilized as immunogens. The lymphocytes of NHPs immunized up to a high titer with these immunogens, will be used for the construction of immune phage-displayed libraries. These libraries will be screened to isolate high-affinity antibody fragments (scFvs), which will be human-like due to the phylogenetic proximity between NHPs and humans. BoNTs present sub-types (A1 and A2, B1 and B2 for instance), and scFvs reacting with these various sub-types will be isolated with a specially-designed panning procedure. To test for neutralization capacities, scFvs directed against heavy chains will be tested in *ex vivo* assays, and the scFvs directed against the heavy chains will be tested *in vitro*. At the end of these steps, the scFvs with best neutralizing profile will be selected and super-humanized.

The super-humanization of NHP antibodies has been described as an approach that allowed for obtaining a "better than human antibody". In effect, due to the physiology of the immune system, human antibodies undergo affinity maturation processes, that bring mutations in antibody regions involved in tolerance. These mutations cause differences between the human germline encoded segments, part of the immunological self, and those of the immunoglobulins G (IgG). We have shown that "super-humanization" (also called "germline humanization") of NHP antibodies is possible, by reversing most of these mutations while respecting the affinity. This process will be applied to the neutralizing scFvs isolated in the course of the project.

In the third part of the project, neutralizing, super-humanized scFvs will be expressed as full-sized IgGs and tested in a standardized protection model to verify their efficacy against several strains for each targeted serotype. At various steps of the project, our results will be communicated to the first responders more particularly involved against biothreats.

Expected results

The ideal result is an oligoclonal cocktail of 6 recombinant, super-humanized IgGs, neutralizing the neurotoxins secreted by all strains of Clostridium botulinum A. B and E. These IgGs will then be developed as medicine with the intent to be registered by the European Medicines Agency (EMEA). This medicine is to become available for biodefense primarily, but also for natural cases of botulinum intoxications in Europe. This dual-use availability, and information given to practitioners in the course of the project, will ensure real improvement in botulism treatment and its perception by EU citizens.

PARTNERS	COUNTRY
Centre de Recherche du Service de Santé des Armées (CRSSA)	France
Ministere de la défense (MLD)	France
Technische Universität Braunschweig (TUBS)	Germany
Institut Pasteur (Pasteur)	France
Health Protection Agency (HPA)	United Kingdom
Centre National de la Recherche Scientifique (DNRS)	France
LFB Biotechnologies (LFB)	France
University of Helsinki (UoH)	Finland
VITAMIB (VITAMIB)	France

BOOSTER / Bio-dosimetric tools for triage to responders

© Tommy Windecker- Fotolia.com

Information

Grant Agreement N°
242361
Total Cost
€4,583,559.24
EU Contribution
€3,284,291
Starting Date
01/07/2010
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
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/

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 designed to develop new bio-dosimetric tools and to integrate them into a toolbox in order to quickly evaluate the level of potential casualties and allow for 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 for 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 for optimising the strategy for the use of the devices. In this respect a decision-aiding component will be developed to help 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 training the responders in several languages.

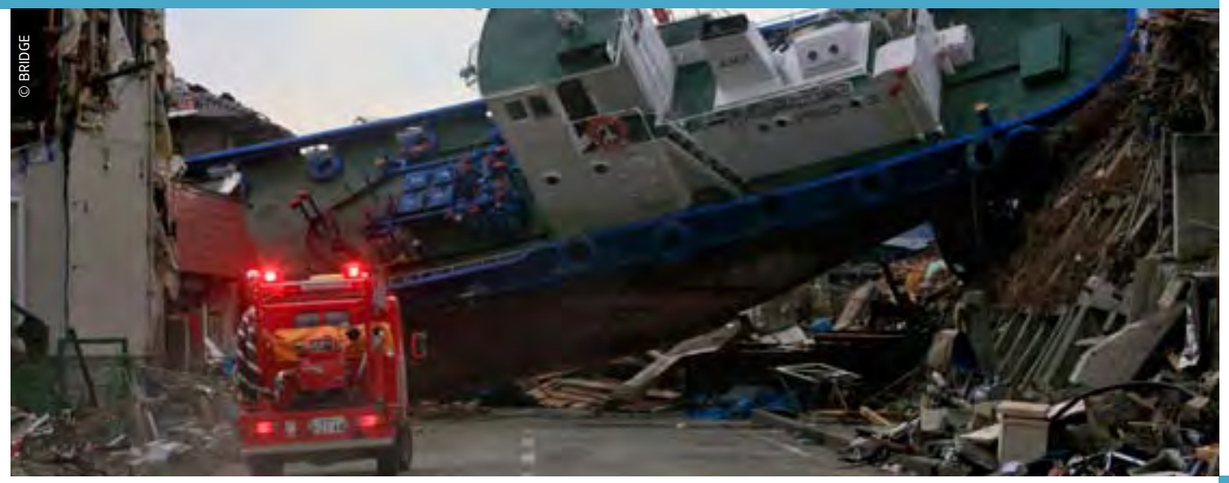
Expected results

The development of the proposed device will provide security personnel with a viable tool for taking fast, effective countermeasures against biological threats. This will drastically reduce the potential impact of terrorist attacks or accidental release of bio-agents from laboratories, as well as detecting the 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.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (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

BRIDGE / Bridging resources and agencies in large-scale emergency management



© BRIDGE

Information

Grant Agreement N°
261817
Total Cost
€18,075,144.20
EU Contribution
€12,983,143.75
Starting Date
01/04/2011
Duration
48 months

Coordinator

STIFTELSEN SINTEF
Forskningsveien 1
P.O. Box 124 Blindern
0314 Oslo
Norway
Contact
Geir Horn
Tel: +47 22067561
Mobile: +47 93059335
Fax: +47 22067350
E-mail: geir.horn@sintef.no
Website: www.sintef.no

Project objectives

The goal of BRIDGE is to increase the safety of citizens by developing technical and organisational solutions that significantly improve crisis and emergency management. A BRIDGE platform will provide technical support for multi-agency collaboration in large-scale emergency relief efforts. The key to this is to ensure interoperability, harmonization and cooperation among stakeholders on the technical and organisational level. The vision of the BRIDGE project is to:

» facilitate cross-border and cross-agency collaboration;
» allow the creation of a common, comprehensive, and reliable operational picture of the incident site;
» enable integration of resources and technologies into workflow management;
» enable active ad-hoc participation of third parties.

Social practices, ethical concerns and legal and bureaucratic demands must be taken into consideration during the realization of this vision. Therefore, BRIDGE will facilitate constructive deep integration of multi-dimensional social, legal and ethical analysis into ambitious interdisciplinary user-led socio-technical innovation.

Description of the work

The BRIDGE consortium consists of a well-balanced mix of cross-disciplinary academics, technology developers, domain experts and end-user representatives. An established End-User Advisory Board guarantees an active end-user involvement during the whole project. Participatory design and agile software development allow for a close collaboration with the targeted end-user groups. BRIDGE is also committed to an iterative user-centred approach incorporating and validating user/domain requirements.

Social, legal and ethical experts investigate the mutual dependence of technology, organisational dynamics, and human factors, and study existing and emergent future practices of managing opportunities, risks and difficulties. This steers the far-reaching synchronization between technical and social innovations as well as public life, most importantly in the areas of privacy, trust in technology, and inter-organisational collaboration.

BRIDGE elaborates solutions for the generation and distribution of 3D simulations of emergency situations for use in training and in case of an emergency. The visual presentation of threat scenarios and their consequences help bridge the differences in technical and operational backgrounds between the parties involved. In addition, BRIDGE develops technical solutions in three different areas:

» Interoperability of data, systems & technology:

- Manage heterogeneous ad-hoc networks;
- Handle information in different formats & from different sources;
- Collect & manage context information.

» Exploration of a common operational picture:

- Develop intelligent, adaptive & multimodal user interfaces;
- Obtain, filter, share, & annotate information;
- Provide a decision support tool for crisis management.

» Runtime inter-agency & inter-agent collaboration:

- Allow the dynamic creation & composition of inter-agency workflows;
- Actor-agent networks & agent-based simulations;
- Facilitate a shared situational awareness.

Realistic scenarios in real-world environments lead to yearly demonstrations of the BRIDGE platform under different foci. BRIDGE's exploitation activities target three groups: emergency management end-user communities in different European countries, industrial BRIDGE partners, and non-BRIDGE technology and solution providers in Europe.

Expected results

BRIDGE will deliver socio-technical innovation in multi-agency emergency collaboration. Ethnographical work will construct a deep understanding of the first responders' domain, also in terms of social, legal and ethical issues. The technical platform will deliver:

» methods and tools that support run-time intra- & inter-agency collaboration;
» a middleware allowing data, system & network interoperability;
» advanced human-computer interaction techniques for effortless exploration of high-quality information;
» enhanced organizational workflows & communication processes.

PARTNERS	COUNTRY
Stiftelsen SINTEF (SINTEF)	Norway
Almende B.V. (Almende)	The Netherlands
CNet Svenska AB (CNET)	Sweden
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FIT)	Germany
Lancaster University (ULANC)	United Kingdom
Crisis Training AS (CTAS)	Norway
SAAB Training Systems (SAAB)	Sweden
THALES Nederland BV (THALES NL)	The Netherlands
Universität Klagenfurt (UNIKLU)	Austria
Paris-Lodron-Universität Salzburg (PLUS)	Austria
VSH Hagerbach Test Gallery LTD (VSH)	Switzerland
Technische Universiteit Delft (TUDelft)	The Netherlands
Stockholms Universitet (US)	Sweden
Helse Stavanger (RAKOS)	Norway

CATO / CBRN crisis management: Architecture, Technologies and Operational procedures

© Bruno Vincent - Getty Images

Information

Grant Agreement N°
261693
Total Cost
€14,148,292.23
EU Contribution
€10,278,062
Starting Date
01/01/2012
Duration
36 months

Coordinator

NESS A.T LTD
Ness Technologies and Systems Group (TSG)
Kiryat Atidim
P.O.B. 58180
Tel Aviv 61581, Israel
Contact
Victor Remez PhD.
Tel: +972-3-5483664
Mobile: +972 52 6076516
Fax: +972 3 5483578
E-mail:
Cato-coordinator@eurtd.com
Website: www.cato-project.eu

Project objectives

» **To deliver a comprehensive Toolbox addressing the needs of all stakeholders:** Policy Makers, Incident Managers, Healthcare providers, the Population and Responders.

CATO addresses the entire disaster life cycle: preparedness, monitoring and detection (alerts and early assessment), response and recovery;

» **To develop a flexible, open, and innovative approach** to cope with the issue of fragmentation between current approaches, systems, and organisational set up.

The CATO Toolbox should provide the means to build a dedicated customised DSS (Decision Support System) adapted to local and national organisational, political and financial constraints as well as different levels of exposure to CBRN threats;

» **To create an Open DSS-Architecture for the CATO CBRN Toolbox** to be adaptable to the specific context of the CATO-DSS's owner;

» **To Focus on Users and Organisational Learning:**

CATO is to set up a **CATO Laboratory**, a simulation based environment where Policy Makers can see scenarios in action, evaluate their impact and develop strategies, and CBRN experts can validate and demonstrate new CBRN scenarios etc.

Description of the work

CATO is organised in 8 Sub-Projects (SPs):

» *SP 1* **"Planning, Response & Ethics"** gathers the main effort from the "user partners" and provides requirements and feedback through validation & testing;

» *SP 2* **"CBRN Expertise"** gathers the CBRN scientific experts together, to support the project with advice on hazardous materials, and systematically collect and provide best practice references;

» *SP 3* **"CATO Core and Knowledge Base"** focuses on the central architecture of the CATO system;

» *SP 4* **"Algorithms"** focuses on CBRN algorithms for data and information fusion, threat detection, propagation & evaluation, holistic situation assessment and decision support;

» *SP 5* **"CATO Interfaces"** covers both the user and the system interfaces providing the basic infrastructure for interoperability with existing systems;

» *SP 6* **"Integration"** puts together the CATO Laboratory to validate the CATO approach with users and the CATO Proof of Concept;

» *SP 7* **"Dissemination"** aims to build a dedicated user and expert community, and establish a regular and deep dialogue with this community;

» *SP 8* is dedicated to **Management**.

CATO pursues several strands creating a virtuous learning process:

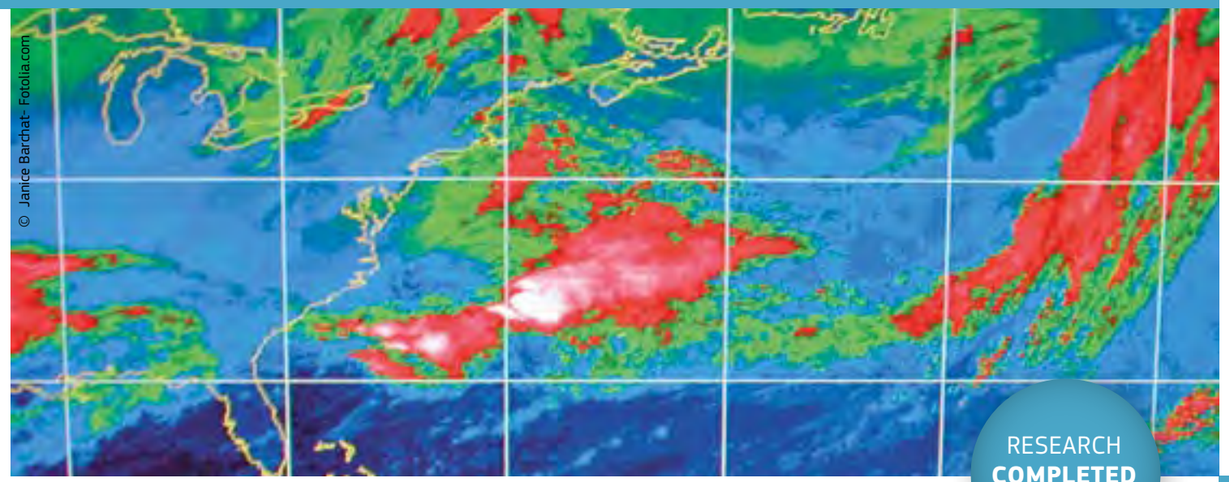
» Dialogue on CBRN crisis management between stakeholders and experts, leading to a deeper understanding of the issues at stake and influencing the developments. CATO, by design, will be open to collaboration with third parties on a mutual benefit basis. CATO expects progressively to have access to a broad range of results in return for access to the CATO Toolbox;
» Development of sub-systems of the CATO Toolbox;
» Research activities in exploiting written input from the population, correlating multiple data analysis of fuzzy data, and data and information fusion;
» Implementation of a first prototype DSS which will serve several purposes:
- Allow for the validation of the CATO approach with different CBRN scenarios;
- The "field based proof of concept" will allow the CATO project to test the CATO approach for the entire life cycle and especially the debriefing and "feedback" added into the CATO knowledge base;
- The CATO Laboratory will provide a strong basis for **validation, testing, dissemination** and future **exploitation of results**;
- A continuous stream of dialogue with the stakeholder community.

Expected results

» Create a basis for the production of more effective operational CBRN toolboxes, by progressively incorporating results of tests and simulations;
» Facilitate knowledge collection and sharing around a "simulation based" dialogue;
» Improve the capability to manage the complexity of CBRN crises by fusing heterogeneous multi-source information into a common picture and offering alternatives for reaction;
» Enable policy makers and managers to go through accelerated learning, and testing of response strategies for given scenarios and facilitate the exchange of best practices.

PARTNERS	COUNTRY
Ness A.T. Ltd. (Ness TSG)	Israel
VectorCommand Ltd (VCL)	United Kingdom
Police National CBRN Centre (PNCBRNC)	United Kingdom
Prolog Development Center (PDC)	Denmark
Technical University of Denmark (DTU)	Denmark
Danish Emergency Management Agency (DEMA)	Denmark
Studiecentrum voor Kernenergie/Centre d'Etude de l'Energie Nucléaire (SCK-CEN)	Belgium
ARTTIC (ART)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Service de Santé des Armées (SSA)	France
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Centre for European Security Studies (CESS)	Germany
Robert Koch Institute (RKI)	Germany
Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)	Germany
Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH) (HMGU)	Germany
Hospital University of Bonn (UKB)	Germany
University of Jyväskylä (JyU)	Finland
Technical Research Centre of Finland (VTT)	Finland
University of Salzburg (PLUS)	Austria
National Radiation Protection Institute (SURO)	Czech Republic
VÚJE Trnava (VUJE)	Slovakia
Inconnect (INCONNECT)	The Netherlands
Magen David Adom (MDA)	Israel
Center for Science Society and Citizenship (CSSC)	Italy
Peace Research Institute Oslo (PRIO)	Norway

COPE / Common Operational Picture Exploitation



© Janice Barchat- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217854
Total Cost
€3,886,574
EU Contribution
€2,535,049
Starting Date
01/02/2008
End Date
31/01/2011

Coordinator

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/

Project objectives

First responders are a heterogeneous group regarding their emergency environments, their roles, command structures, and organisational and national frameworks.

COPE's goal was to improve the performance reliability and cost of emergency response management "C2" (command and control) systems by combining user-oriented human factors with technology development. A central aim was to strengthen information flow from and to first responders to boost situational awareness across agencies and at all levels of the C2 chain in emergency management situations.

A user-driven approach therefore drove COPE's development of new technologies that support information requirements at the scene of an event. The project applied a wide range of human-factor methods – from functional task modelling to end-user simulations – to better understand individual agencies, and to ensure that new systems match requirements and can be integrated with legacy processes and technologies.

Results

COPE's obtained its results from its key work packages, which focused on:

» a generic concept for a common operational picture (COP);

» analysis of first responder activity (fire fighters, sector commanders and incident commanders) in three countries;

» technology mapping to align user requirements with hardware solutions;

» definition of user-driven scenarios and key performance indicators.

These led to two exercises: a live one involving first responders and actual fire and hazards events, and a tabletop one with end-users involved in additional C2 and decision-making tasks.

The culmination of COPE's work packages resulted in end-user assessment of technology-in-design using trials and questionnaires. Based on a set of criteria for modern and future COP systems derived from leading international projects, a detailed evaluation of the state of the art achieved was produced, which takes into account technological, operational, and end-user evaluations.

For example, COPE studied the use and benefits of wearable displays, sensors and locational technologies to support first-responders. The advantages and disadvantages of such technologies were identified. According to feedback from first responders and external stakeholders, the system and its components produced "good" to "very good" levels of satisfaction. Though there were certain temporary failures and reductions in functionality, these did not undermine the validity of the project's overall research results, according to the COPE consortium.

PARTNERS	COUNTRY
TECHNICAL RESEARCH CENTRE OF FINLAND (VTT)	Finland
UTI SYSTEMS S.A. (UTI)	Romania
CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)	Germany
Pelastusopisto, Emergency Services College (ESC)	Finland
Ministry of Interior and Administration Reform (IGSU)	Romania
BAE Systems C-ITS (BAE Systems C-ITS)	Sweden
THE PROVOST, FELLOWS AND SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY COLLEGE DUBLIN (TCD)	Ireland
BAE SYSTEMS (OPERATIONS) LIMITED (BAE Systems UK)	United Kingdom
SKYSOFT PORTUGAL - SOFTWARE E TECNOLOGIAS DE INFORMAÇÃO SA (Skysoft)	Portugal

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

© Francois Doisnel - Fotolia.com

Information

Grant Agreement N°
242474
Total Cost
€4,593,444.66
EU Contribution
€3,495,611.99
Starting Date
01/05/2010
Duration
36 months

Coordinator

MIDDLESEX UNIVERSITY HIGHER EDUCATION CORPORATION
School of Engineering & Information Sciences, London NW4 4BT
Contact
Prof. William Wong, BCom (Hons.) PhD FN-ZCS – 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/

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, for 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 draw on insights derived from the research team covering 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.

PARTNERS	COUNTRY
Middlesex University Higher Education Corporation (MU)	United Kingdom
SHELTERLAND ApS - 3D CONNECTION (CRI)	Denmark
National Aerospace Laboratory (NLR)	The Netherlands
ObjectSecurity Ltd (OS)	United Kingdom
Space Applications Services (SAS)	Belgium
VSL Systems AB (VSL)	Sweden
Linkoping University (LiU)	Sweden
Haskoli Island - University of Iceland (HI)	Iceland
A E Solutions (BI) Ltd (AES)	United Kingdom
Aeroportos de Portugal, SA (ANA)	Portugal
British Transport Police Authority (BTP)	United Kingdom
Flugstodir (ISAVIA)	Iceland

CRISMA / Modelling crisis management for improved action and preparedness


© GYI NSEA - istockphoto.com

Information

Grant Agreement N°
284552
Total Cost
€14,397,298
EU Contribution
€10,107,160
Starting Date
01/03/2012
Duration
42 months

Coordinator

VALTION TEKNILLINEN TUTKIMUSKESKUS
Tekniikankatu 1
P.O. Box 1300
FI-33101 Tampere, Finland
Contact
Anna-Mari Heikkilä
Tel: +358 20 722 3490
Mobile: +358 20 722 3490
Fax: +358 20 722 3499
E-mail:
Anna-mari.heikkila@vtt.fi
Crisma.coordinator@vtt.fi
Website: www.crismaproject.eu

Project objectives

CRISMA IP focuses on large scale crisis scenarios with immediate and extended human, societal, structural and economic, often irreversible, consequences and impacts. These crisis scenarios cannot be managed alone with regular emergency and first responder resources, but require multi-organisational and multi-national cooperation including humanitarian aid.

A common set of criteria and performance indicators for crisis management simulation and optimisation provided by CRISMA modelling system shall enable decision makers and crisis managers to: (1) model possible multi-sectoral crisis scenarios and assess the consequences of an incident, (2) simulate possible impacts resulting from alternative actions, (3) support strategic decisions on capabilities, related investments, reserves and inventories, (4) optimise the deployment of resources dedicated to crisis response in line with the evolvement of a crisis, and (5) improve action plans for preparedness and response phases of the crisis management.

© Crisma

Description of the work

CRISMA builds upon the existing tools and facilities provided by its research, industry, SME and end-user partners, and takes into account the existing structures and practices as well as the research and development work done in the EU and its member states. The work is carried out in close cooperation with the end-user partners who have wide experience in crisis management in complex situations, including national disasters and global response activities.

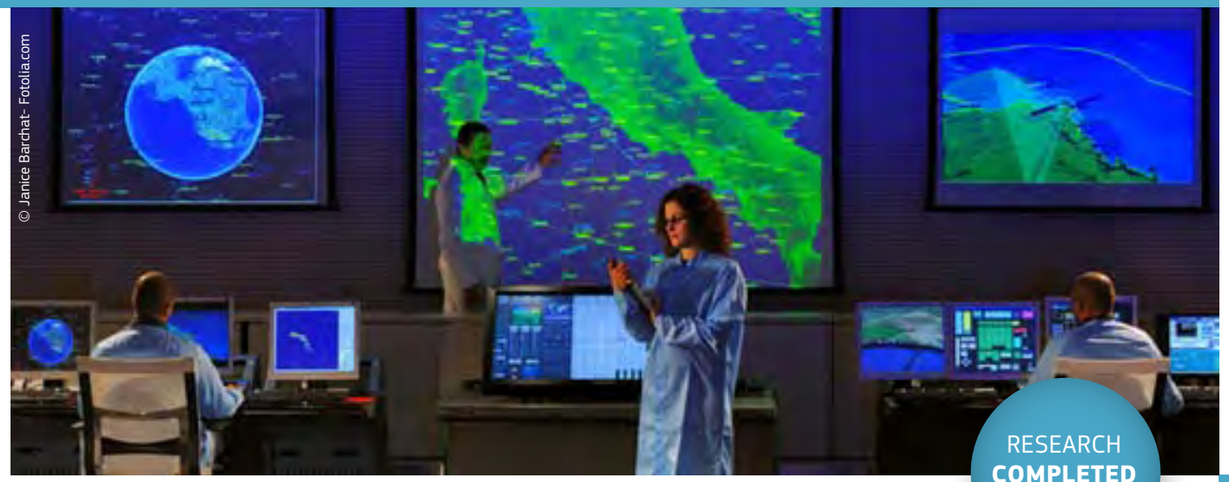
The CRISMA work plan consists of several sub-projects (SP) that are divided into several work packages. Those SPs define Scenarios, Requirements and Criteria for Crisis Management Modelling for the development of CRISMA, and develop components for the Integrated Crisis Modelling System (ICMS) and Models for Multi-Sectoral Consequences. In the middle of the project, the first version of the CRISMA system components will be tested and validated by the end-user pilots. End-User pilots shall test and validate the CRISMA system and its components in two sequences, which provides feedback for the development work. The mid-term and final validation of CRISMA's results are performed in cooperation with the End-User Advisory Board.

Expected results

The CRISMA project shall develop a simulation-based decision support system for modelling crisis management, improved action and preparedness. The CRISMA system shall facilitate the simulation and modelling of realistic crisis scenarios, possible response actions, and the impacts of crisis depending on both the external factors driving the crisis development and the various actions of the crisis management team.

PARTNERS	COUNTRY
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Analisi e Monitorraggio del Rischio Ambientale (AMRA)	Italy
AIT Austrian Institute of Technology GmbH. (AIT)	Austria
Association for the Development of Industrial Aerodynamics (ADAI)	Portugal
Tallinna Tehnikaulikool - Tallinn University of Technology (TTU)	Estonia
NICE Systems Ltd (NICE)	Israel
European Aeronautics Defence and Space Company – CASSIDIAN Division (EADS)	Germany
Insta DefSec (INS)	Finland
Spacebel S.A (SpB)	Belgium
Cismet GmbH (CIS)	Germany
Pelastusopisto - The Emergency Services College (ESC)	Finland
Magen David Adom (MDA)	Israel
Public Safety Communication Europe Forum (PSCE)	Belgium
Ilmatieteen laitos - Finnish Meteorological Institute (FMI)	Finland
Deutsches Rotes Kreutz (DRK)	Germany
ARTELIA Eau & Environnement (AEE)	France

CRISYS / Critical Response in Security and Safety Emergencies



RESEARCH **COMPLETED**

Information

Grant Agreement N°
261682
Total Cost
€805,852
EU Contribution
€740,945
Starting Date
01/02/2011
End Date
31/05/2012

Coordinator

EUROPEAN ORGANISATION FOR SECURITY
Avenue de Tervuren 270
B-1150 Brussels,
Belgium
Contact
Nicola Iarossi
Tel: +32 (0)2 7770255
Mobile: +32 (0)472990751
Fax: +32 (0)2 7758112
E-mail:
nicola.iarossi@eos-eu.com
Website:
www.crisys-project.eu

Project objectives

To build in this Phase (Phase I) a roadmap capable of full implementation to show specific demonstration actions in Phase II, whilst establishing contacts and awareness with the main public and private stakeholders in the field of Crisis Management.

The work done in the actual phase is aimed at full understanding of the issues surrounding effective operational needs (e.g. interoperability of technical solutions, commonality of procedures, decision and crisis decision tools, the importance of languages; common training approaches; homogeneous risk assessment methodologies etc.) for the most significant demonstration actions.

Description of the work

It is imperative to understand how the civil protection sector operates. Firstly we need to review presently adopted solutions, procedures and the operational, legal, societal, political and, legacy environments in which those mechanisms are set. We can then establish parameters of operations, not simply scenarios but how to create wider capability and capacity.

Users and citizens are the critical success key for the project. Building a respected relationship is a vital part of the project. That requires the creation of a public-private dialogue with local, national and international users, first responders and national governments and citizens.

The role of CRISYS Partners is therefore to gather these requirements via specific MEETINGS with USERS and SUPPLIERS around Europe, thus establishing a sound network of contacts for Phase II whilst also gathering the key elements to develop the requirements for the Roadmap.

This process will be followed by a gap analysis activity of the collected results, in two steps, from a preliminary roadmap to a final roadmap which will be presented at a final conference.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
European Organization for Security (EOS)	Belgium
EDISOFT SA (EDI)	Portugal
Center for Security Studies (KEMEA)	Greece
National Center for Scientific Research, “Demokritos” (NSCRD)	Greece
ALTRAN BV (ALTRAN)	The Netherlands
International Association of Fire and Rescue Services (CTIF)	France
Teletron Euroricerche SRL (TLT)	Italy
Compania nationala de transport al energiei eletrice Transelectrica SA (TRA)	Romania
Société Françoise de Medicine de Catastrophe (SFMC)	France
THALES Security Solution & Service SAS (T3S)	France
Indra Sistemas S.A (INDRA)	Spain
Istituto Affari Internazionali (IAI)	Italy
University of Central Lancashire (UCLAN)	United Kingdom
Ministry of the Interior, Department for Rescue Services, SISAASIAINMINISTERIO (FMOI)	Finland
Zanasi Alessandro SLR (ZAN)	Italy

DARIUS / Deployable SAR Integrated Chain with Unmanned Systems (SAR = Search and Rescue)

© alxpin - istockphoto.com

Information

Grant Agreement N°
284851
Total Cost
€10,688,505
EU Contribution
€7,475,830
Starting Date
01/03/2012
Duration
36 months

Coordinator

BAE SYSTEMS (OPERATIONS) LTD
BAE Systems, Engineering
Marconi Way
Rochester, Kent, ME1 2XX,
United Kingdom
Contact
Richard Cross
Tel: +44-1634-844400
E-mail: contact@darius-fp7.eu
Website: www.darius-fp7.eu

Project objectives

» Interoperability of the unmanned platforms;

» Seamlessly integrate the unmanned platforms in the command and control loop (i.e. C2/C4I platforms);

» Provide the necessary communication structure without relying on existing infrastructure;

» Support the interaction between humans and systems, i.e. FRs, victims, unmanned vehicles and payloads;

» Develop a Generic Ground Station;

» Define the capability, deployability and sustainability requirements for future SAR unmanned vehicles;

» Define and evaluate operational performance improvements of current deployed solutions;

» Reduce the cost of unmanned SAR solutions.

Description of the work

The DARIUS project is broken down into seven work packages (WPs).

WP1 deals with project management.

The other six work packages are designed around the development and testing in real conditions of a real interoperability capability of the unmanned systems, in terms of both sharing the utilisation in the same operation, and integrating them in the legacy command and control systems.

WP2 User Needs and Concept of Operations: This work package is responsible for the understanding of the user needs for the deployment and use of unmanned systems for search and rescue organisations.

WP3 Integration Design: This work package involves the generation of the requirements and interoperability standards for the DARIUS system based upon the outputs in WP2.

WP4 Components Development: This work package involves the adaptation of the existing unmanned platforms and ground system to meet the DARIUS requirements.

WP5 Integration: This work package involves the integration and testing of the DARIUS platforms and ground stations to prove the system prior to the evaluation and trials.

WP6 Evaluation and Trials: This work package involves the evaluation of the DARIUS solution in urban/indoor, forest fire and maritime SAR scenarios.

WP7 Exploitation: This work package involves the management of a User Advisory Board, the dissemination of project results, the exploitation issues and the final standards and legal recommendations emerging from DARIUS' results.

Expected results

DARIUS is expected to lead to improved citizen security and safety through enhanced capabilities and more extensive use of unmanned air, land and waterborne vehicles and payloads in search and rescue operations, with enhanced operational, procedural and technical interoperability.

PARTNERS	COUNTRY
BAE Systems (Operations) Ltd (BAES)	United Kingdom
Cassidian S.A.S. (CASS)	France
DFRC AG (DFRC)	Switzerland
SKYTEK LTD (SKY)	Ireland
TELINT RTD Consultancy Services LTD (TEL)	United Kingdom
FUTURE INTELLIGENCE EREVNA TILEPIKINONIAKON KE PLIROFORIAKON SYSTIMATON EPE (FINT)	Greece
OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONE)	France
STIFTELSEN SINTEF (SIN)	Norway
ECA SA (ECA)	France
NATIONAL TECHNICAL UNIVERSITY OF ATHENS (NTUA)	Greece
CENTER FOR SECURITY STUDIES (KEM)	Greece
ECOMED bvba (ECO)	Belgium
CORK INSTITUTE OF TECHNOLOGY (NMCI)	Ireland

DECOTESSC1 /DEmonstration of COunterTErrorism System-of-Systems against CBRNE phase 1

© Martijn Smeets - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242294
Total Cost
€1,587,642
EU Contribution
€1,001,627
Starting Date
01/04/2010
End Date
30/06/2011

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK
Department of CBRN Protection
Schoemakerstraat 97
PO Box 6060
NL-2600 JA Delft
The Netherlands
Contact
Nicola Iarossi
Mark van den Brink
Tel: +31 8886 63898
Mobile: +31 6 3015 8707
Fax: +31 8886 66938
E-mail: mark.vandenbrink@tno.nl
Website: www.decotessc1.eu

Project objectives

DECOTESSC1 – a so-called 'phase one' project – set out to provide a research road-map for priorities and structures for a subsequent 'phase two' large scale Demonstration Project project, which will test effective methods for countering chemical, biological, radiological, nuclear and explosive (CBRNE) terrorist threats.

The basic idea behind DECOTESSC1 was analysis and subsequent prioritization of CBRNE counter-measure security gaps, taken as a comparison between the current situation and a theoretical ideal situation.

An in-depth background study supported this analysis, including interviews and workshops to ascertain the current threat environment and technical state-of-the-art.

Results

As well as identifying relevant research actors, technology providers, end users and other stakeholders for consultation, the project created a comprehensive Multidimensional Taxonomy System (MTS) in order to aggregate common technical terminology for this study.

This fed into a gap analysis, which eventually produced a list of 150 potential gaps in current CBRNE counter-measures. Using a ranking system, these were narrowed down to just 25 "serious" gaps in European CBRNE counter-measures.

These gaps are subdivided into five categories to be prioritized in the 'phase two' Demonstration project:

» Fusion of information and situational picture. This includes detection, identification and monitoring of actors, agents, means of delivery, targets and effects in the CBRNE field. The validity of the perceived threat and its consequences needs to be measured and verified;

» Communication. In addition to general disaster management strategies, CBRNE awareness and resilience should be increased. Aspects such as education, the role of local, regional, national and European authorities and the passive and active use of (social) media should be covered by a dedicated communication strategy;

» Cooperation. This requirement includes priorities to pool resources, share (classified) information and use best practices among separate C, B, RN and E actors;

» Consequence management. Mostly post-incident activities (the response and recovery phases), but also the relationship between pre-incident activities and preparedness;

» Realistic training and exercise. In particular, new techniques (such as the use of virtual reality and serious gaming) need to be further explored, developed and demonstrated to meet both needs and restrictions.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
European Commission - Joint Research Centre (JRC)	Europe
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Fundación Tecnalia Research & Innovation (TEC)	Spain
Seibersdorf Labor GmbH (SLG)	Austria

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


© E-SPONDER

Information

Grant Agreement N°
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

Project objectives

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 crisis 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 brigade crews;

» *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.

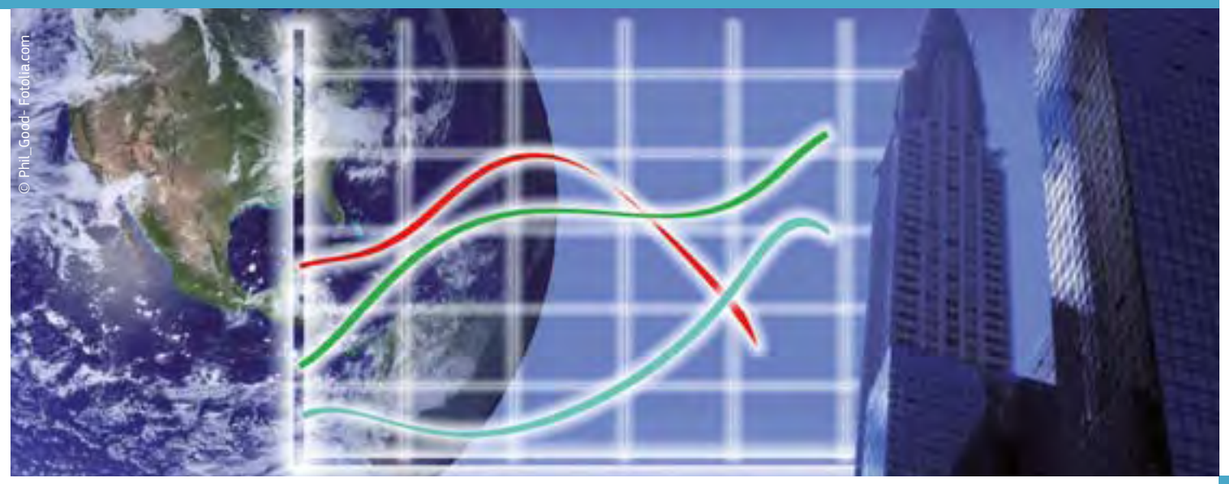
Expected results

Measures	Metrics
Preparedness	
Percent of responders trained to respond to anticipated emergencies (e.g. 15 planning scenarios)	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, which may hold this role for a period of time)	Within 30 minutes of 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 of 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 of arrival of responders 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%

PARTNERS

Exodus S.A.(EXO)	Greece
University of Modena and Reggio Emilia (UNIMORE)	Italy
CrisisPlan B.V. (CPLAN)	The Netherlands
Prosyst Software GmbH (PROS)	Germany
Immersion S.A. (IMM)	France
Rose Vision (ROSE)	Spain
Telcordia Poland Sp. z.o.o. (TARC-PL)	Poland
Centre Suisse d'Electronique et de Microtechnique S.A. (CSEM)	Switzerland
Smartex Srl (SMTX)	Italy
Technische Universität Dresden (TUD)	Germany
YellowMAP AG (YA)	Germany
PANOU S.A. (PANOU)	Greece
Telcordia Taiwan (TARC-TW)	Taiwan
Institute for Information Industry (III)	Taiwan
Entente pour la forêt Méditerranée (EPLFM)	France

ESS / Emergency support system



Information

Grant Agreement N°
217951
Total Cost
€14,025,624.80
EU Contribution
€9,142,126
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

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 fuses in real-time various forms of field-derived data including video, audio, weather measurements, location tracking, radioactivity, bio-chemical, 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 Vehicles (UAV), Unmanned Ground Systems (UGS), air-balloons 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 at 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 perspectives.

Expected results

First and foremost, ESS will aid in the development of novel tactical intelligence systems 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.

PARTNERS	COUNTRY
VERINT SYSTEMS LTD (VRNT)	Israel
Wind Telecomunicazioni SpA (WIND)	Italy
International Geospatial Services Institute GMBH (IGSI)	Germany
Intergraph CS (ING)	Czech Republic
GMV Sistemas S.A. (GMV)	Spain
CS Systèmes d'Information (CS)	France
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IAIS)	Germany
ITIS Holdings plc. (ITIS)	United Kingdom
Algosystems SA (ALGO)	Greece
Alcatel-Lucent Italia (ALI)	Italy
APD Communications Ltd. (APD)	United Kingdom
Anonymos Etaireia Antiprosopeion Emporiou Kai Viomichanias (ANCO)	Greece
FAENZI srl. (FNZI)	Italy
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
The Imego Institute (IMEGO)	Sweden
Magen David Adom (MDA)	Israel
Ernst & Young (EY)	Israel
Aeronautics Defense Systems (AERO)	Israel
DIGINEXT SARL (DXT)	France
Entente pour la forêt méditerranéenne (CEREN)	France

FASTID / Fast and efficient international disaster victim identification


© FASTID

Information

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

Project objectives

» Development of an information management and decision support system for disaster victims 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;

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

» To test and evaluate the system;

» 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 with 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 to 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 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 with 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.

PARTNERS	COUNTRY
International Criminal Police Organization - I.C.P.O. (INTERPOL)	France
Bundeskriminalamt (BKA)	Germany
Plass Data Software A/S (Plass Data)	Denmark
University of Dundee (UNIVDUN)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Crabbe Consulting Ltd (CCLD)	United Kingdom

FRESP / Advanced first response respiratory protection


© Loren Rodgers - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218138
Total Cost
€4,074,891.01
EU Contribution
€3,029,967
Starting Date
01/06/2008
End Date
31/05/2012

Coordinator

ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL
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

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 a commercialisation procedure for 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:

» *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.).

» *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.

» *System development*

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

» *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.

» *Economic feasibility and manufacturability, exploitation and dissemination, IPR policy*

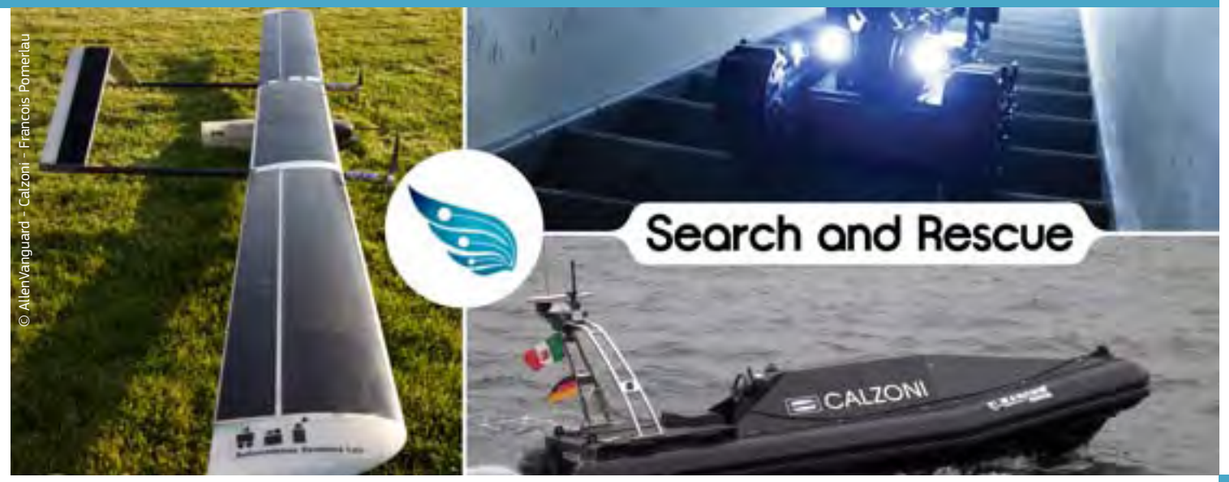
Examination of viability of a full scale production of the nanoporous adsorbent, the filter canister and the hood.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Ecole Royale Militaire - Koninklijke Militaire School (RMA)	Belgium
Budapest University of Technology and Economics (BME)	Hungary
University of Brighton (UoB)	United Kingdom
University of Alicante (UALI)	Spain
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
High Technology Filters s.a. (HTF)	Greece
MAST Carbon (MAST)	United Kingdom
NORIT Nederland B.V (NORIT)	The Netherlands
Laser Optical Engineering Ltd. (LOE)	United Kingdom
ProQares BV (ProQares)	The Netherlands

ICARUS / Integrated Components for Assisted Rescue and Unmanned Search operations



© AlenVanguard - Calzoni - Francois Pomerlau

Information

Grant Agreement N°
285417
Total Cost
€17,554,528.49
EU Contribution
€12,584,933.45
Starting Date
01/02/2012
Duration
48 months

Coordinator

ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL
Department of Mechanics
Av. De La Renaissance 30
1000 Brussels, Belgium
Contact
Geert De Cubber
Tel: +32 2 7426553
Mobile: +32 478 640652
Fax: +32 2 7426547
E-mail:
geert.de.cubber@rma.ac.be
Website:
http://www.fp7-icarus.eu/

Project objectives

- Development of a light sensor capable of detecting human beings;
- Development of cooperative Unmanned Aerial System (UAS) tools for unmanned SAR;
- Development of cooperative Unmanned Ground Vehicle (UGV) tools for unmanned SAR;
- Development of cooperative Unmanned Surface Vehicle (USV) tools for unmanned SAR;
- Heterogeneous robot collaboration between Unmanned Search And Rescue devices;
- Development of a self-organising cognitive wireless communication network, ensuring network interoperability;
- Integration of Unmanned Search And Rescue tools in the C4I systems of the Human Search And Rescue forces;
- Development of a training and support system for the developed Unmanned Search And Rescue tools for the Human Search And Rescue teams;
- Communication and dissemination of project results.

Description of the work

In the event of a large crisis, a primordial task of the fire and rescue services is the search for human survivors on the incident site. This is a complex and dangerous task, which often leads to loss of lives. The introduction of unmanned search and rescue devices can offer a valuable tool for saving human lives and speeding up the search and rescue process. Therefore, ICARUS concentrates on the development of unmanned search and rescue technologies for detecting, locating and rescuing humans. In this context, there is vast literature on research efforts towards the development of unmanned search and rescue (SAR) tools. However, in the field, unmanned SAR tools still have great difficulty finding their way to the end-users.

The ICARUS project addresses these issues, aiming to bridge the gap between the research community and end-users, by developing a toolbox of integrated components for unmanned search and rescue. The objective of the ICARUS project is to develop robots which have the primary task of gathering data. The unmanned SAR devices are foreseen to be the first explorers of the area, as well as in situ supporters to act as safeguards for human personnel. In order not to increase the cognitive load of the human crisis managers, the unmanned SAR devices will be designed to navigate individually or cooperatively and to follow high-level instructions from the base station. The robots connect wirelessly to the base station and to each other, using a wireless self-organising cognitive network of mobile communication nodes which adapts to the terrain. The unmanned SAR devices are equipped with sensors that detect the presence of humans. At the base station, the data is processed and combined with geographical information, thus enhancing the situational awareness of the personnel leading the operation with in-situ processed data that can improve decision-making. The Haitian experience has shown the importance acquired by the geographic component in the management of human and technical resources in crisis situations. Similarly, it has highlighted that a suitable distribution of thematic maps allows optimisation and interoperability of these resources and accelerates the access to victims. All this information will be integrated in existing C4I systems, used by the forces involved in the operations.

Expected results

The overall purpose of the ICARUS project is to apply its innovations for improving the management of a crisis and by doing so to reduce the risk and impact of the crisis on citizens. The use of unmanned search and rescue devices embedded in an appropriate information architecture and integrated into existing infrastructures will help crisis personnel by providing detailed and easy to understand information about the situation. The proposed system will inform crisis personnel about real dangers present on the ground, and will thus increase their performance in resolving the situation.

PARTNERS	COUNTRY
ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
SPACE APPLICATIONS SERVICES NV (SPACE)	Belgium
ESTUDIOS GIS S.L. (E-GIS)	Spain
Centre de Tecnologia aerospacial (CTAE)	Spain
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IZM)	Germany
INSTYTUT MASZYN MATEMATYCZNYCH (IMM)	Poland
JMDTHEQUE SARL (JTH)	France
TECHNISCHE UNIVERSITAET WIEN (TUV)	Austria
INTEGRASYS, S.A. (ISYS)	Spain
Skybotix AG (SBX)	Switzerland
QUOBIS NETWORKS SL (QUOBIS)	Spain
INESC PORTO - INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES DO PORTO (INESC)	Portugal
ALLEN-VANGUARD LIMITED (AV)	United Kingdom
UNIVERSITE DE NEUCHATEL (UNINE)	Switzerland
Eidgenössische Technische Hochschule Zürich (ETH)	Switzerland
ATOS SPAIN SA (ATOS)	Spain
TECHNISCHE UNIVERSITAET KAISERSLAUTERN (UKL)	Germany
NATO Undersea Research Centre (NURC)	Italy
CALZONI SRL (CAL)	Italy
METALLIANCE SA (META)	France
ESRI PORTUGAL - SISTEMAS E INFORMACAO GEOGRAFICA SA (ESRI)	Portugal
SPACETEC PARTNERS SPRL (STP)	Belgium
ESCOLA NAVAL (CINAV)	Portugal
Federale overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking (BFAST)	Belgium

IDIRA / Interoperability of data and procedures in large-scale multinational disaster response actions

Information

Grant Agreement N°
261726
Total Cost
€10,925,164.35
EU Contribution
€8,032,971.06
Starting Date
01/05/2011
Duration
48 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V
Hansastrasse 37C
80686 - Muenchen
Germany
Contact
Andreas Kuester
Tel: +49 (0) 351 4640 667
Mobile: +49 (0) 172 4117655
Fax: +49 (0) 351 4640 803
E-mail: Andreas.Kuester@ivi.fraunhofer.de
Website: http://www.ivi.fraunhofer.de

Project objectives

There are currently no disaster management procedures, tools and systems in the EU which fully take into account the specific requirements of large-scale international cooperation in emergency situations. Those actions are distinguished by many diverse emergency response organisations that need to collaborate across technological systems, organisational borders and language and cultural barriers. Technologies and procedures used and researched so far have provided many solutions for single aspects, but there is no concept available yet which supports the entire process.

In IDIRA we follow the vision of providing a conceptual framework that allows for supporting and augmenting regionally available emergency management capacities (including the existing IT systems) with a flexibly deployable Mobile Integrated Command and Control Structure. This system of technologies and guidelines is designed to help in optimal resource planning and operations across national and organisational borders.

Description of the work

As part of the analysis of the state of the art, the workflow in multinational disaster response actions is being modelled, and based on that a high-level specification of supporting technological components and a system integration concept for interoperability and interfaces is being designed.

As interoperable communication is a prerequisite for successful disaster management, the Consortium works on the integration of communication protocols for data exchange and voice communication interoperability. Furthermore data models for tasks and resources and the quick integration of geographic and attribute data as well as sensor data are being improved.

A core step is the provision of a common operational picture, including structured text communication over language barriers and information interchange for the provision of early situational awareness to unit leaders before leaving their home country. Planning and optimisation tools for missing persons' tracing are being integrated.

In the field of interoperable response management, a decision support system for coordinated multinational response planning and optimisation is provided. This includes micro simulation as an up-to-date technology for decision support. Additional fields of work are improvements in international donation management and multinational resource management for disaster response.

For training and dissemination purposes, local and binational field training sessions are carried out. Finally, three multi-national and multi-organisational exercises are being planned, covering flood, large-scale fire and earthquake or pandemic events.

At the final stage, a description of successful rules and procedures, the Architectural Reference for the Mobile Integrated Command & Control Structure and recommendations for harmonization and standardization in the European Union are being presented.

Expected results

The set of tools, interfaces and procedures developed in IDIRA provides services for data integration, information exchange, resource planning and decision support to disaster response units and decision makers. It is an architectural framework and an exemplary implementation of a Mobile Integrated Command and Control Structure supporting co-ordinated large-scale disaster management. The IDIRA solutions are building on and are being integrated with existing infrastructure and response procedures.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IVI)	Germany
Salzburg Research (SRFG)	Austria
Frequentis (FRQ)	Austria
Brimatech Services GmbH (BRI)	Austria
National and Kapodistrian University of Athens (NKUA)	Greece
Earthquake Planning and Protection Organization (EPPO)	Greece
German Red Cross (branch of the state of Saxony) (DRK-SN)	Germany
University of Greenwich (UOG)	United Kingdom
IES Solutions (IES)	Italy
Flexit Systems (FLEXIT)	Austria
Austrian Red Cross Headquarters (ORK-HQ)	Austria
Hellenic Ministry of Defence (HMOD)	Greece
Department of Fire Brigade, Public Rescue and Civil Defence – Ministry of Interior (CNVVF)	Italy
Satways Ltd. (STWS)	Greece
TLP, spol. s r.o. (TLP)	Czech Republic
World Agency of Planetary Monitoring & Earthquake Risk Reduction (WAPMERR)	Switzerland
Local Government of Achaia Prefecture (NEA)	Greece
Center for Security Studies (KEMEA)	Greece

IFREACT / Improved First Responder Ensembles Against CBRN Terrorism

© IFREACT

Information

Grant Agreement N°
285034
Total Cost
€5,475,980.60
EU Contribution
€3,394,615.40
Starting Date
01/01/2012
Duration
36 months

Coordinator

UNIVERSITE PARIS XII- VAL DE MARNE
SAMU 94
51 Avenue de Lattre de Tassigny
94000, Creteil, France
Contact
Dr. Catherine Bertrand
Tel: +33 1 45 17 95 29
Mobile: + 33 6 82 82 24 11
Fax: + 33 1 45 17 95 30
E-mail: catherine.bertrand@hmn.aphp.fr
Website: www.ifreact.eu

Project objectives

IFREACT aims to provide the next generation of protective clothing for first responders. Bringing together leading protective technology and blending it with some of the latest software, it will enhance the chemical, biological and radiological protection of European first responders. European major cities continue to face the threat of terrorism and, in the near future, may be subject to a serious chemical, biological or radiological terrorist attack. When the time comes it will be the brave men and women of the various emergency services who will answer the call – and they need to be adequately protected and prepared.

Description of the work

The consortium will deliver qualitative and quantitative evaluation of existing Personal Protective Equipment (PPE) by both a laboratory and end-users and will focus its research on the most emergent threats in order to best fulfil the needs of those end-users who are in the greatest need of protection from both terrorist and non-terrorist related crises. Once this preparatory work has been completed, it will be tempered by direct feedback from the user community, and the team will begin to work on prototype ensembles that:

» address the real protection needs of conventional users, with regards to both the level of protection and its total capacity;

» provide adequate protection, while keeping the burden of the system as low as possible;

» include solutions for hand and foot protection, whilst taking safety, ergonomic and logistic aspects of the conventional user group into consideration;

The protective system will provide added functionality regarding the C4I needs of the first responder. Typical tactical needs such as communication, (indoor) localisation & situational awareness, will be enabled by affordable, robust and easy to use technology. Wearability, graceful degradation and logistics will dictate innovative approaches to the material as well as to the system level;

The suit will be configured as a platform that carries the energy and the connections to the components of the sensor subsystem. The sensors itself will be housed in the suit as well as in the respirator, depending on their function. The configuration of the system will enable other / new energy cells and sensors to be connected whenever required;

This platform will be interfaced with the external infrastructure to get extra capabilities/situation awareness without constraints and cost as regards the suit itself.

Moreover, the project will develop a platform that allows end-users and procurement staff to best select the PPE system needed for the mission of the first responder and the expected threat.

Expected results

The ensemble will incorporate next-generation skin protection, a head-up display, a biodosimeter, audio/voice technology, and a GPS self-localisation device; it will also incorporate three types of respiratory protection, heightened situational awareness and agility, as well as comfortable, yet safe, protection against CBRN threats. With injections of knowledge from the users themselves the suit will exceed their demands, in terms of both protection and usability. It will be a prêt-à-porter Personal Protective Equipment!

PARTNERS	COUNTRY
Universite Paris XII- Val de Marne (SAMU)	France
IB Consultancy BV (IBC)	The Netherlands
NBC-SYS SAS (NBC Sys)	France
Blücher GmbH (Blücher)	Germany
Astrium SAS (Astrium)	France
Falcon Communications Limited (CBRNe World)	United Kingdom
Bertin Technologies SAS (Bertin)	France
Statni Ustav Jaderne, Chemicke a Biologicke Ochrany vvi (SUJCHBO)	Czech Republic
Drzavna Uprava za Zastitu i Spasavanje (DUZS)	Croatia
Prometech BV (Prometech)	The Netherlands
Hotzone Solutions Benelux (Hotzone Solutions)	The Netherlands

IMSK / Integrated mobile security kit

Information

Grant Agreement N°
218038
Total Cost
€23,485,135.25
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

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, and 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 full 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.

PARTNERS	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'énergie atomique et aux énergies alternatives (CEA)	France
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)	Germany
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (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
Joint Research Centre (JRC)	Belgium
Deutscher Fußball-Bund e.V.	Germany
AirshipVision International S.A	France
University of Reading	United Kingdom
The Chancellor, Masters and Scholars of the University of Oxford	United Kingdom

INDIGO / Crisis management solutions

© Galina Pankratova- Fotolia.com

Information

Grant Agreement N°
242341
Total Cost
€3,835,727
EU Contribution
€2,787,672
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

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 analysing events after the crisis;

» The involvement of multiple participants (field units as well as 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:

» 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.

» The mobile INDIGO system that enables first responders and other field units to participate in INDIGO crisis exercises;

» 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;

» The Real-time Simulation Services that can simulate the scenario or be used to support decisions during real crises;

» The portable map table that will offer an extremely innovative and intuitive means to interact with the Common Operational Picture in mobile crisis centers;

» The standard proposition for a European 2D/3D emergency symbology.

PARTNERS	COUNTRY
Diginext SARL	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

L4S / Learning for security project

© fotografiche.eu - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225634
Total Cost
€3,471,413.41
EU Contribution
€2,415,768
Starting Date
01/07/2009
End date
31/07/2011

Coordinator

DELOITTE BUSINESS SOLUTIONS ANONYMI ETAIREIA SYMVOULON EPICHEIRISEON
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

Project objectives

The L4S project sought to develop an easily deployable life-long learning service to improve the crisis management skills and competencies of security personnel (notably top management). L4S simulation-based crisis management exercises focused particularly on air and sea transport disaster scenarios.

The project's target audience for improved crisis management skills comprised European corporate personnel, decision-makers and academic learners, with an eye to strengthening the resilience of private and public organsiations in Europe. Three types of crisis management-relevant competencies were addressed: cognitive abilities, affective and normative aspects of learning, and the ability to perform an action.

Results

The project designed and developed the "L4S learning experiences service" consisting of advanced simulation games and learning/networking applications. The L4S portfolio includes the following air and sea transport crisis management simulation exercises:

» "IMPACT: The Crisis Readiness Online Simulation Experience";

» "RECKON&CHOOSE! Air Simulation";

» "CRISIS TEAM".

Apart from simulation games, the L4S portfolio also contains a WEB 2.0 advanced networking and sharing tool named "CRISIS TUBE Leadership Learning Network", as well as a supportive online workshop tool known as "OWL4S".

The individual exploitation plans of the partners explored the potential use of three different types of L4S applications:

» *Internal:* organisations that integrate the L4S applications portfolio in their internal executive training programs, offering employees and executives the opportunity to take part in this type of learning experience;

» *External:* commercial entities that distribute the L4S applications portfolio to their customers in various industries, with possibilities for learning experiences to be bundled with existing business products or services;

» *Academic:* educational and academic institutions that integrate L4S training applications in their curricula. The L4S portfolio could also serve as basis for executive and vocational training.

The consortium believes that L4S simulation games and applications can provide impact and visibility, along with the generation of a strong stream of revenue for those organisations choosing to implement them. The long-term strategy is to set up an efficient Europe-wide B2B Channel for the diffusion of similar game-based learning experiences.

PARTNERS	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

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

© rolffimages - Fotolia.com

Information

Grant Agreement N°
241536
Total Cost
€4,580,243.01
EU Contribution
€3,493,199
Starting Date
01/05/2010
Duration
36 months

Coordinator

STOCKHOLM UNIVERSITY 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

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 the 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 automation 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.

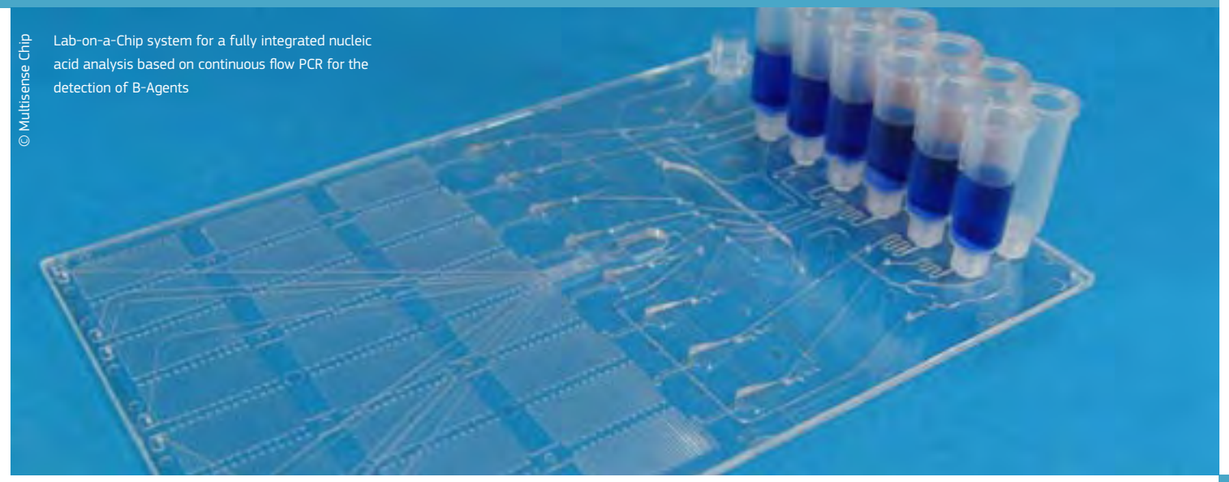
The project beneficiaries will be supported by an advisory committee that will include experts in bio-dosimetric tools and management of radiation accidents.

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 the 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.

PARTNERS	COUNTRY
Stockholm University Centre For Radiation Protection Research (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)	United Kingdom
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
University of Oxford (UOXF)	United Kingdom
EURADOS (EURADOS)	Germany

MULTISENSE CHIP/ The lab-free CBRN detection device for the identification of biological pathogens on nucleic acid and immunological level as lab-on-a-chip system applying multisensor technologies



© Multisense Chip

Lab-on-a-Chip system for a fully integrated nucleic acid analysis based on continuous flow PCR for the detection of B-Agents

Information

Grant Agreement N°
261810
Total Cost
€8,986,775.00
EU Contribution
€6,619,399.50
Starting Date
01/06/2011
Duration
48 months

Coordinator

MICROFLUIDIC CHIPSHOP GMBH
Stockholmer Str.20
07747 Jena, Germany
Contact
Andrzej Wojcik
Dr. Claudia Gärtner
Tel: +49 3641 3470511
Mobile: +49 172 52 58 506
Fax: +49 3641 3470590
E-mail: Claudia.Gaertner@microfluidic-ChipShop.com
Website:
www.multisense-chip.com

Project objectives

The goal of Multisense Chip is the development of a detection and identification system for biological pathogens, which shall include both the sample preparation stage, during which target molecules are extracted directly, and the nucleic-acid-based and/or immunological detection and identification steps.

The chosen technologies offer several advantages: on the one hand, a small, portable, and easy-to-use device can be realized due to miniaturization; on the other, the so-called lab-on-chip technology enables operation outside of lab settings, meaning that the complete analysis including sample preparation, extraction of target molecules, etc. will be carried out in a small device the size of a microtiter plate with all necessary reagents on board. This includes dry reagent storage of lysis reagents, master mixes for the PCR, antibodies, and liquid storage of buffers. The overall target is a "sample in, result out"-type handling procedure.

Description of the work

The overall goal is the realization of a complete analysing system for biological pathogens consisting of a micro-nano-based consumable chip with integrated sensor technology, an innovative instrument to run the chip, as well as the respective biological assays themselves.. Finally this will be embedded in advanced information and communication technologies. To cope with this multidisciplinary work from the technical and application side and to ensure full compliance with ethical aspects connected to the intended use of the system, the work will be arranged in thirteen work packages. A detailed requirement specification combined with regular design reviews will guide the way to a proper project run. The technical work packages are grouped around the biological assay, the sensor technology and micro- and nanofabrication technologies. The system and integration tasks will be covered within the microfluidics, software, communication and instrumentation work packages. An important aspect within the project is the validation and demonstration task for ensuring a proper performance and usability of the system. The training aspect in particular of future users to get them in touch with lab-on-a-chip technology as early as possible is an important aspect as well. To guarantee the awareness and proper handling of ethical issues an independent work package was installed.

To realize the integrated system, the following latest enabling technologies will be applied:

- **Sample enrichment: Novel air sampling technologies** and sampling procedures easily combinable with a chip;
- The target material for the biological assays and tests will be extracted on-chip via **novel micro-nanotechnological devices** combined with advanced biochemistry;
- **Microfluidics** allows for fast and efficient hybridization of the PCR products on the capture microarray, implementing **3D-nanotechnology**;
- **Electrochemiluminescence-based** detection or **electrochemical sensors** ensure ultrasensitive detection.

Expected results

The aim is to produce a portable analytical instrument for the detection and identification of biological pathogens on the molecular and immunological levels. This system will be based on a portable instrument and a lab-on-a-chip as a consumable. It will combine sample enrichment, extraction of the target molecules from the sample, the biological reaction and finally the carrying out of the detection reaction via innovative sensor technologies.

PARTNERS	COUNTRY
Microfluidic ChipShop GmbH (MFCS)	Germany
Bertin Technology (BT)	France
Friedrich Loeffler Institut (FLI)	Germany
Integrated Microsystems for quality of Life SL (iMicroQ)	Spain
Institut für Mikrotechnik Mainz (IMM)	Germany
Universitat Rovira i Virgili (URV)	Spain
Institute of Physical Biology (IFB)	Slovenia
Cedralis (CED)	France

OPTI-ALERT / Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication

© S. Hofschlaeger / pixelio.de

Information

Grant Agreement N°
261699
Total Cost
€3,543,462
EU Contribution
€2,531,122
Starting Date
01/01/2011
Duration
36 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Institute for Software and Systems Engineering ISST, Department of Targeted Alerting Systems
Steinplatz 2
10623 Berlin
Germany
Contact
Dr. Michael Klafft
Tel: +49 (0) 30 24306-365
Fax: +49 (0) 30 24306-599
E-mail: Michael.Klafft@isst.fraunhofer.de
Website: www.opti-alert.eu

Project objectives

The Opti-Alert project strives to improve the alerting of the general public in crisis situations through personalized, culturally sensitive multi-channel communication. The objective of this project is to develop an alerting suite that:

» allows for a rapid simulation of the impact of different alerting strategies (depending on the selected media-mix and current availability of communication media);

» supports the composition of the optimal mix of communication channels (individualized alerting channels and mass media);

» improves alert compliance through social and cultural adaptation and personalization of alert messages and communication channels;

» supports the rapid and automated implementation of a selected alert strategy;

» can simultaneously address a large variety of communication channels to facilitate efficient high-throughput alerting; and

» can be integrated with existing tools and legacy systems via well-defined interfaces.

Description of the work

The objectives of the Opti-Alert project are supported by the following key research activities:

» an in-depth analysis of the impact that social and cultural and regional factors have on risk perception and risk communication;

» an analysis of the influence which the observed socio-cultural differences have on regional alerting strategies;

» an analysis of the impact of individualized alerting (via SMS, E-Mail, etc.) and alerting via the mass media;

» the identification of best-practices in alerting via mass media;

» a definition of appropriate algorithms for the simulation of alert propagation within the population (in general, but also inside critical infrastructures such as metro stations), depending on the selected mix of communication channels and communication patterns between humans.

One goal of Opti-Alert is to improve the impact of alerts by developing alerting strategies that take socio-cultural characteristics of the message recipients into account. This can refer to both differences in risk perceptions and different usage patterns with respect to media and communication channels. Based upon the situational and socio-cultural context of an alert situation, the authorities will be able to simulate different alerting strategies (in terms of communication channels and media mix). This will allow authorities to re-assess alert procedures and processes and to improve impact and coverage of alerts. Another goal of Opti-Alert is the adaptation of alert content to the socio-cultural milieu of the message recipients. This refers, e.g., to the wording of the messages, or layout and design. The idea is to improve the compliance of alert recipients with the proposed protective actions by creating trust and, if necessary, a sense of urgency (or calm) among those who have been warned.

Expected results

In addition to in-depth and interdisciplinary studies of sociologists and media scientists on the perception of crisis communication, Opti-Alert will develop a demonstrator to test the proposed socio-culturally adaptive alerting tool and the corresponding alert simulation component in practice. Furthermore, an interface definition will be specified so that existing as well as new and emerging communication channels can be connected to the Opti-Alert toolsuite. The goal is to provide an alerting platform that can later be used internationally in order to efficiently address the information needs of the population in times of crisis.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FHSS)	Germany
e*Message Wireless Information Services Deutschland GmbH (EMESS)	Germany
UBIMET GmbH (UBIMET)	Austria
Proteo S. p. A. (PROTEO)	Italy
UNIQA Versicherungen AG (UNI)	Austria
Göteborgs Universitet (UGOT)	Sweden
Süddeutsches Institut für empirische Sozialforschung e.V. (SINE)	Germany
Regione Sicilia (SIC)	Italy
Nederlands Instituut Fysieke Veiligheid (NIFV)	The Netherlands
Università degli Studi di Perugia (UNIPG)	Italy
THALES Services SAS (THALES)	France

PANDORA / Advanced training environment for crisis scenarios

© Evan Luthye - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
225387
Total Cost
€3,997,166.21
EU Contribution
€2,930,000
Starting Date
01/01/2010
End Date
31/03/2012

Coordinator

UNIVERSITY OF GREENWICH
Old Royal Naval College,
Park Row, Greenwich
UNITED KINGDOM
Contact
Reginald DALY
Tel: +44 02083319685
Fax: +44 02083318665
Website: http://PANDORA-project.eu/

Project objectives

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

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
University of Greenwich (UoG)	United Kingdom
Consiglio Nazionale delle Ricerche (CNR-ISTC)	Italy
Società Consortile a Responsabilità Limitata (CEFRIEL)	Italy
Razvoj programske opreme in svetovanje d.o.o. (XLAB)	Slovenia
Fondazione Ugo Bordoni (FUB)	Italy
ORT FRANCE (ORT)	France
University of East London (UEL)	United Kingdom
Business Flow Consulting (BFC)	France
Emergency Planning College (EPC)	United Kingdom

PEP / Public Empowerment Policies for Crisis Management

© James Brey - istockphoto.com

Information

Grant Agreement N°
284927
Total Cost
€1,065,206
EU Contribution
€950,023
Starting Date
01/01/2012
Duration
36 months

Coordinator

UNIVERSITY OF JYVÄSKYLÄ
Agora Center
Seminaarinkatu 15
PO Box 35
40014 University
of Jyväskylä, Finland
Contact
Prof. Marita Vos
Tel: +358 50 4410 358
Mobile: +358 50 4410 358
Fax: +358 14 260 1021
E-mail: marita.vos@jyu.fi
Website: www.projectPEP.eu

Project objectives

The purpose is to investigate how the crisis response abilities of the public can be enhanced and identify what public empowerment policies can be utilised for this purpose. The project has the following objectives.

» To identify potential key enablers for public empowerment for crisis management, by 3 studies:

- providing an overview of best practices showing strategies and tools used by authorities to enhance individual, family and community crisis response;
- clarifying in depth how community approaches, involving social groups in crisis preparedness and response, are used, including success factors in how to connect with community needs;
- assessing how and what technologies can enhance human resilience in crisis situations taking perceptions and social acceptance of the technologies and mobile services into account.

» To construct a Road Map charting promising areas for future R&D and implementation, supporting human resilience;

» To ensure dissemination of the project results in order to raise awareness of the importance of public resilience, and how this can be achieved.

Description of the work

In work package 1 the aim is to provide *best practices* in how authorities currently enhance human resilience and what strategies and tools are used to promote individual and community crisis response. A desk study will be conducted and an online questionnaire sent to international experts.

In work package 2 the focus is on *community approaches* involving social groups in crisis preparedness and response. An analysis of quantitative data and in-depth interviews will be done in Sweden, focusing on remote areas where storms may cause long power cuts and isolation. Interviews with members of the International Expert Panel will also be conducted to scrutinise international applicability.

In work package 3 the aim is to assess how and what *technologies* can enhance human resilience in crisis situations, taking into account technology acceptance models and inclusion requirements (diversity of publics). In Finland focus group interviews will be organised to clarify what kind of communication technology citizens prefer for this purpose. The applicability of the conclusions will be scrutinized in interviews with members of the International Expert Panel.

In work package 4 the focus is on constructing a *Road Map* charting directions for further research and implementation supporting human resilience. A preparation workshop will be organised at the International Disaster and Risk Conference (IDRC) 2012. In addition, a web platform will be used to expose the preliminary conclusions for review. During an *international symposium* within the framework of IDRC Davos 2014 the future orientation of the Road Map will be discussed.

In work package 5 the dissemination gets attention. An online toolbox will be produced with the *guides* about key enablers for public empowerment in crisis situations, concentrating on a) best practices, b) community approach and c) human technology. Furthermore, a *theme issue* of the open access journal 'Human Technology' will be prepared to disseminate the project results to crisis managers and communication experts working for public authorities and non-governmental organizations, as well as European policymakers in the security area.

Expected results

The project will address future directions for research to enhance public resilience and bring a European 'enabled public' closer. It will clarify how a community approach can be effective in strengthening abilities and social structures for resilience and what technologies strongly contribute to public resilience.

The project will develop policies from the perspective of coproducing safety with citizens and communities. Furthermore, through the Road Map the project will produce innovative ways to increase cooperation with and by citizens.

PARTNERS

University of Jyväskylä (JyU)
Mid Sweden University (MIUN)
Global Risk Forum (GRF)
Inconnect (Inconnect)
Emergency Services College Finland (ESC)

COUNTRY

Finland
Sweden
Switzerland
Netherlands
Finland

PLANTFOODSEC / Plant and food biosecurity

Information

Grant Agreement N°
261752
Total Cost
€5,609,529.69
EU Contribution
€4,624,499.00
Starting Date
01/02/2011
Duration
60 months

Coordinator

UNIVERSITA DEGLI STUDI DI TORINO
Centro di Competenza per l'innovazione in campo agro-ambientale (AGROINNOVA)
Via Leonardo da Vinci, 44
10095, Grugliasco (Torino)
Italy
Contact
Maria Lodovica Gullino
Tel: +39 011 670 8539
Fax: +39 011 6709307
E-mail: marialodovica.gullino@unito.it
Website: www.plantfoodsec.eu

Project objectives

PLANTFOODSEC is a Network of Excellence aiming to enhance preparedness for preventing, responding and recovering from the possible use of plant pathogens as biological weapons against crops, and the microbiological contamination of feed and food in the European agrifood system.

PLANTFOODSEC pursues the following specific objectives:

- obtaining scientific knowledge on plant disease epidemiology;
- enhancing the prevention, recognition, response and recovery from foodborne illness due to the contamination of fresh produce;
- improving planning of effective and efficient national and regional responses to agro-terrorism acts;
- improving disease surveillance and detection systems by facilitating international laboratory cooperation and by developing diagnostic tools;
- preventing the establishment and spread of deliberately-introduced pathogens;
- building a strong culture of awareness and compliance with plant and food biosecurity for those with responsibilities in all sectors of agriculture and food production;
- improving awareness among stakeholders and the general public on biosecurity issues;
- overcoming the fragmentation of partners' research.

Description of the work

This project will focus on biological threats having the capacity to affect and damage agriculture, infect plants and ultimately affect food and feed at any stage in the food supply chain. These threats are multifaceted, interrelated, complex and increasingly transnational in their impact.

Recent trends in biosecurity recommend a shift from a largely national approach towards greater international cooperation.

The Network of Excellence will renew and reinforce already established partnerships and enlarge them by including new countries, institutions and topics to establish a virtual Centre of Competence. It will be able to deal with issues of crop and food biosecurity and become a Centre of reference at the European level.

The project strategy is based on the bio-preparedness approach to prevent, respond and recover from a biological incident or deliberate criminal activity threatening European agrifood systems, thus including:

- actions to identify and update the biology, epidemiology and impacts of high priority pathogens also through the optimization of detection and diagnostic tools;
- actions to develop effective responder strategies by defining specific protocols on emergent pest and disease management;
- actions to enhance knowledge of target groups and to inform relevant stakeholders taking into account the balance between confidentiality and public access;
- actions to overcome the fragmentation of partners' research and to facilitate and coordinate responder networks.

Expected results

A more risk-based approach will move biosecurity from a reactive towards a proactive position which focuses more on prevention and better anticipates emergences of entirely new threats.

By following this strategy, PLANTFOODSEC will increase the quality and impact of plant and food biosecurity training and research in Europe thus providing timely scientific inputs to respond to biosecurity threats posed to the European agriculture, farming and agrifood industry.

PARTNERS	COUNTRY
Università degli Studi di Torino (UNITO-AGROINNOVA)	Italy
National Institute of Agricultural Botany	United Kingdom
The Secretary of State for Environment, Food and Rural Affairs	United Kingdom
Rheinische Friedrich-Wilhelms-Universitaet Bonn	Germany
Institut National de la Recherche Agronomique	France
Regional Environmental Center for Central and Eastern Europe	Hungary
Imperial College of Science, Technology and Medicine	United Kingdom
Middle East Technical University	Turkey
SPIN-TO Srl	Italy
United Nations Interregional Crime and Justice Research Institute	Italy
The Agricultural Research Organisation of Israel – The Volcani Centre	Israel
Oklahoma State University	United States
Kansas State University	United States

PRACTICE / Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment PRACTICE


© PRACTICE

Information

Grant Agreement N°
261728
Total Cost
€11,695,072
EU Contribution
€8,424,029
Starting Date
01/05/2011
Duration
42 months

Coordinator

UMEA UNIVERSITY
European CBRNE Centre
Linneaus väg 6
90187 Umea
Contact
Dzenan Sahovic
Tel: +46 (0) 90 786 5774
Mobile: +46 (0) 73 073 5303
Fax: +46 (0) 90 786 6681
E-mail: dzenan.sahovic@cbrne.umu.se
Website: www.umu.se/cbrne

Project objectives

The objective of the PRACTICE project is to improve the preparedness and resilience of the Member States and Associated Countries countries to an attack from a terrorist group using non-conventional weapons such as CBRN (Chemical, Biological, Radiological and/or Nuclear agents) materials. This will be done with the help of a newly developed integrated CBRN incident management toolbox.

Description of the work

The development of a new toolbox will be based on:

» identification, organization and establishment of knowledge of critical elements in the event structure through studies of a wide selection of scenarios, real incidents and exercises;

» analysis and identification of gaps in the current response situation and organization and integration of the allocated response capabilities or functions in a toolbox of equipment, procedures and methods; and

» an allocated system or kit for public information, decision-support, first-responder training and exercises.

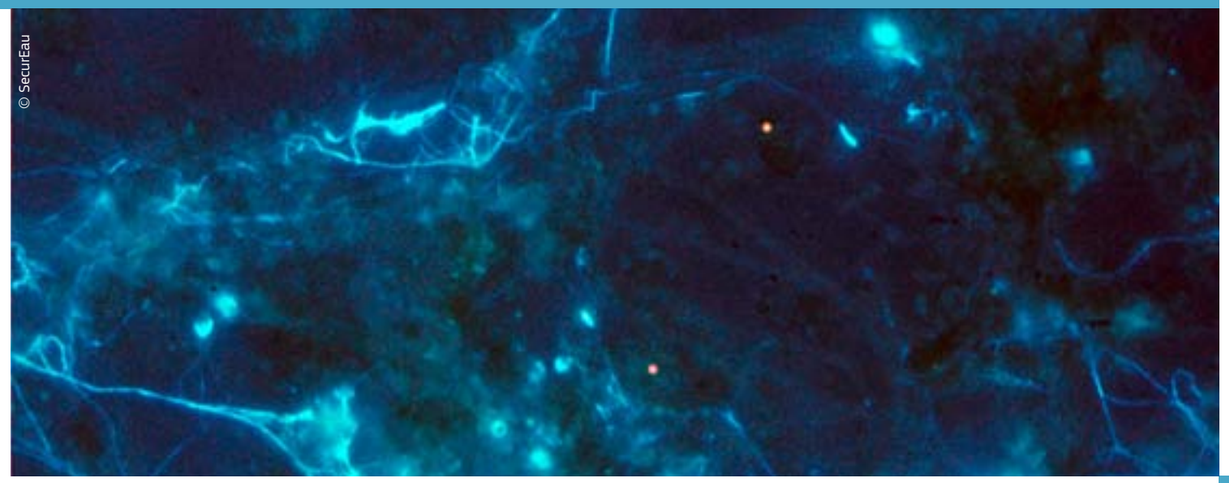
These response capabilities functions are to a great extent universal in character and independent of national organizational structures. Particular attention will be given to integration and understanding of human factors and societal aspects in all the parts of the project. The final concept and integrated response system (toolbox) and subsystems will be tested and validated. A whole system demonstrator will be shown and tested in the final phases of the project.

Expected results

The concept and developed system will provide the EU and its Member States with a flexible and integrated system for a coordinated response to a CBRN terrorist attack, which is easy to adapt to various national organizations and regulations.

PARTNERS	COUNTRY
Umea University (UmU)	Sweden
Forsvarets forskningsinstitutt (FFI)	Norway
ASTRIUM S.A.S. (AST)	France
Cassidian S.A.S. (EADS)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
KING'S COLLEGE LONDON (KCL)	United Kingdom
IB Consultancy BV (IBC)	The Netherlands
CBRNE Ltd (CBRNEltd)	United Kingdom
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSRD)	Greece
Totalförsvarets Forskningsinstitut (FOI)	Sweden
UNIVERSITE CATHOLIQUE DE LOUVAIN (UCL)	Belgium
Netherlands Forensic Institute (NFI)	The Netherlands
STATNI USTAV JADERNE, CHEMICKE A BIOLOGICKE OCHRANY vvi (SUJCHBO)	Czech Republic
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy
SELEX GALILEO LTD (SELEX)	United Kingdom
ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (AstriPL)	Poland
COMITE EUROPEEN DE NORMALISATION (CEN)	Belgium
Szkola Glowna Sluzby Pozarniczej (SGSP)	Poland
MITTUNIVERSITETET (MIUN)	Sweden
Prometech BV i.o. (PRO)	The Netherlands
BRUHN NEWTECH A/S (BNT)	Denmark
HEALTH PROTECTION AGENCY (HPA)	United Kingdom
SODERSJUKHUSET AB (SPC)	Sweden

SECUREAU / Security and decontamination of drinking water distribution systems following a deliberate contamination



© SecurEau

Information

Grant Agreement N°
217976
Total Cost
€7,481,418.73
EU Contribution
€5,266,871
Starting Date
01/02/2009
Duration
48 months

Coordinator

UNIVERSITE HENRI POINCARE - NANCY 1
Service des Relations Internationales, Cellule Europe
22-30 rue Lionnois
60120
54003 Nancy cedex
FRANCE
Contact
Sylvain FASS
Tel: +33 (0)3 54 50 54 37
Fax: +33 (0)3 54 50 54 01
E-mail:
sylvain.fass@uhp-nancy.fr
Website:
http://www.secureau.eu/

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 to a 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 to 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 pipe 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 in applying 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 the 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.

© SecurEau

PARTNERS	COUNTRY
Université Henri Poincaré – Nancy 1 (UHP)	France
Centre National de la Recherche Scientifique (CNRS)	France
Veolia Environnement Recherche et Innovation (VERI)	France
Rheinisch-Westfälisches Institut für Wasserforschung gemeinnützige GmbH (IWW)	Germany
University of Southampton (SOTON)	United Kingdom
Faculdade de Engenharia da Universidade do Porto (FEUP)	Portugal
Riga Technical University (RTU)	Latvia
Centre national du Machinisme Agricole, du Génie Rural, des Eaux et des Forêts (CEMAGREF)	France
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Monitoring Systems Ltd. (MSystems)	United Kingdom
Veolia Water Central (VWC)	United Kingdom
Radiation and Nuclear Safety Authority (STUK)	Finland
Kelda Group PLC (YWS)	United Kingdom
National Institute for Health and Welfare (THL)	Finland

SECURENV / Assessment of environmental accidents from a security perspective

© SECURENV

RESEARCH **COMPLETED**

© SECURENV

Information

Grant Agreement N°
218152
Total Cost
€1,205,870
EU Contribution
€850,596.50
Starting Date
01/05/2009
End Date
30/04/2011

Coordinator

Geonardo Environmental Technologies Ltd.
Záhony utca, 7
1031 - Budapest
Hungary
Contact
Balazs Bodo
Tel: +36 1250 6703
Mobile: +36 20 317 2087
Fax: +36 1 436 9038
E-mail: coordinator@securenv.eu
Website: www.securenv.eu

Project objectives

SECURENV aimed to develop a knowledge base and research agenda for future threats associated with possible deliberate attacks on the environment – including 'environmental terrorism' or attempts to amplify the damage inflicted on environmental elements by conventional security incidents.

The ultimate goal of the project was to catalogue and prioritise potential threats in this area, support the development of appropriate policy counter measures and mitigation strategies.

Results

The initial project output was a review and assessment of past environmental accidents, catastrophes and examples of deliberate attacks on the environment. This created a database of 330 entries. Though this database catalogued substantial anecdotal evidence of deliberate environmental destruction throughout history, the actual number of incidents described as direct 'environmental terrorism' is limited.

However, environmental damage as the result of organised crime appears to be an emerging phenomenon, whilst increasingly strict environmental regulations are generating larger numbers of notable incidents: ie., the threshold of tolerance for incidents has been lowered, with a corresponding decrease in investment for causing such an incident.

Several examples of environmental warfare were also identified, with special attention being given to incidents such as the potential release of invasive species by a would-be attacker. These findings have been integrated to a 'foresight model', through which the inherent risk and likelihood of an incident manifesting can be calculated.

These models were used to develop a systematic security foresight approach. The resulting methodology is a combination of assessment methods including input and expertise from a survey addressing more than 600 experts in Europe and beyond, as well as scenario-building workshops involving 15-20 consortia experts.

The policy recommendations and mitigations strategies related to these findings, due to the sensitive nature of this topic area, are largely classified.

PARTNERS

Geonardo Environmental Technologies Ltd.
Adelphi Research
Totalförsvarets Forskningsinstitut (FOI)

COUNTRY

Hungary
Germany
Sweden

SGL FOR USAR / Second generation locator for urban search and rescue operations


© puck - Fotolia.com

Information

Grant Agreement N°
217967
Total Cost
€6,218,278
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

Project objectives

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.

Description of the work

» 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, and to employ the same kind of devices for monitoring and identifying hazardous conditions in voids of collapsed buildings due to the 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 types of data (e.g. sonar);

» To integrate early location and monitoring systems with communication and information management applications that can provide multi-level processing and data fusion and will support relevant USaR services and logistics (medical support, mobilization, tools, transportations, communications). The 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 at delivering next generation systems for USaR operations.

For that purpose, relevant technical, scientific and operational issues will be addressed.

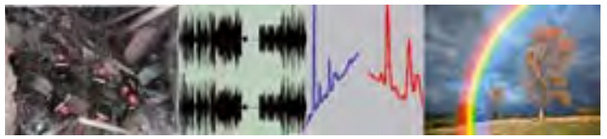
The project focuses on rapid location of entrapped or buried victims (alive or deceased) and the continuous monitoring of the air conditions in the voids of damaged and partially collapsed structures. Entrapped people and voids are associated with characteristic visual, sound and chemical profiles, due to specific images or spectral emissions, and 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 a 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.

Expected results

SGL for USaR will deliver methods and guidelines, as well as tangible prototypes: a stand-alone 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.


© SGL for usar

PARTNERS	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

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217855
Total Cost
€3,902,633.33
EU Contribution
€2,566,330
Starting Date
01/03/2008
End Date
31/08/2010

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
Website: http://www.sicma-project.eu/SicmaProject-Site2008/index.html

Project objectives

The SICMA project was a 30 months capability project focused on computer assisted decision making for Health Service crisis managers. It aimed 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.

Description of the work

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).

© Sicma

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 was 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 allowed a documentation of 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 were selected:

Conventional weapons terrorist attack: being the most common and hence the most likely threat in the future. This scenario was used to evaluate the decision support achievable with the SICMA prototype in the management of casualties. The focus was 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 was 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 was used as case study in the chemical attack Scenario.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
ELSAG DATAMAT S.P.A. (ED)	Italy
SKYTEK LTD (SKYTEK Ltd)	Ireland
Centre for European Security Strategies GMBH (CESS)	Germany
IFAD TS A/S (IFAD)	Denmark
ELBIT SYSTEMS LTD (ESL)	Israel
ITTI Ltd (ITTI)	Poland
INDUSTRIEANLAGEN BETRIEBSGESELLSCHAFT MBH (IABG)	Germany
UNIVERSITA CATTOLICA DEL SACRO CUORE (UCSC)	Italy
CONSIGLIO NAZIONALE DELLE RICERCHE (CNR-IASI)	Italy
SELEX SISTEMI INTEGRATI SPA (SSI)	Italy

S(P)EEDKITS / Rapid deployable kits as seeds for self-recovery


© s(p)eedkits

Information

Grant Agreement N°
284931
Total Cost
€9,021,302
EU Contribution
€6,117,066
Starting Date
01/03/2012
Duration
48 months

Coordinator

CENTRE SCIENTIFIQUE & TECHNIQUE DE L'INDUSTRIE TEXTILE BELGE
Technologiepark 7
BE-9052 Zwijnaarde,
Belgium
Contact
Guy Buyle
Tel: +32-9-220 41 51
Mobile: +32-492-73 76 19
Fax: +32–9-220 49 55
E-mail: gbu@centexbel.be
Website: www.speedkits.eu

Project objectives

The main objective of S(P)EEDKITS is to develop kits for emergency response units, i.e. *SPEED*KITS. Following best practice guidelines from humanitarian organisations, these solutions will also be *SEED*KITS, i.e. kits that form the seeds for the long term self-recovery process after a disaster strikes.

Humanitarian organisations like the Red Cross or MsF have sleeping emergency response units which start acting immediately after disaster strikes. Each unit has a specific function, e.g. medical care, sanitation, energy provision, or water supply.

S(P)EEDKITS targets a smart (re-)design of existing / novel kits via smart packaging and via introduction of the latest technological developments from a wide range of domains like coated textile materials, ICT, material development, tensile structures and construction.

Some examples: lightweight, durable and thermally isolating tent materials, novel concepts for energy supply (biogas from sanitation), smart packaging (matryoshka doll principle), kits for debris recuperation, and rapidly deployable container solutions for a mobile hospital or command centre.

Description of the work

S(P)EEDKITS will design, develop, test and demonstrate units for emergency response in the following four domains:

Shelters:

Design and development of novel shelter kits for four different basic shelters:

» *ultra lightweight safe house unit*, a short term solution for the very first hours, to be deployed by the affected communities;

» *collective unit*, an emergency shelter which could be removed or re-used for other purposes later;

» *family house unit*, the first version of a real house, to be used in the transitional period and later;

» *multipurpose unit* for the humanitarian organizations, to be used for storage, offices and medical centres.

Water and Sanitation:

Research, development and testing of prototypes of flexible sanitation systems and low tech, low cost, small scale potable water kits, based on the use of "add-ons" for tuning to local needs and future application.

Sustainable infrastructure:

Develop container-based command, communication and medical centre units, based on existing prototypes. The units can be reused or handed over to the local medical authorities.

Design and testing of a biogas system for energy for ca.200 people based on faeces and household kitchen waste collection.

Development of mobile debris recycling kit for producing easily usable building materials from the existing debris.

Deployment and Tracking:

Development of a deployment decision tool (DDT) to determine immediately which kits and support have to be deployed. As well as the development of a tracking system, tagging the individual transported packages – suitable for central operational planning & for local assessment of the situation.

For the different kits, the goal is to (re-)design existing and novel emergency response kits using the Matryoshka doll principle; this nesting principle will inspire the packaging optimization of smaller robust packages in large ones, allowing splitting up according to the transportation means available.

Three different levels of packaging are anticipated within S(P)EEDKITS: container-level, pallet-level and bag-level based as much as possible on the use of flexible textile materials.

We aim mostly at the bag-level, i.e. solutions for where more conventional transport means fail.

Expected results

The expected outcomes are novel emergency kits that are modular and adaptable, low-cost, and high-tech in their conceptions yet low-tech in their use. The planned kits have the potential to improve the lives of millions of people during the first hours, days and weeks after a major disaster.

PARTNERS	COUNTRY
CENTRE SCIENTIFIQUE & TECHNIQUE DE L'INDUSTRIE TEXTILE BELGE (CTB)	Belgium
AIDE INTERNATIONALE DE LA CROIX-ROUGE LUXEMBOURGEOISE ASBL (SRU)	Luxembourg
HET NEDERLANDSE RODE KRUIS (NLRC)	The Netherlands
SIOEN INDUSTRIES NV (SIOEN)	Belgium
VRIJE UNIVERSITEIT BRUSSEL (VUB)	Belgium
TECHNISCHE UNIVERSITEIT EINDHOVEN (TU/e)	The Netherlands
POLITECNICO DI MILANO (POLIMI)	Italy
De Mobiele Fabriek B.V (DMF)	The Netherlands
STICHTING WASTE (WASTE)	The Netherlands
STICHTING PRACTICA (PRACTICA)	The Netherlands
D'APPOLONIA SPA (DAPP)	Italy
IBBK FACHGRUPPE BIOGAS GMBH (IBBK)	Germany
MILLSON BV (MIL)	The Netherlands
ARTSEN ZONDER GRENZEN (MEDECINS SANS FRONTIERES NEDERLAND) VERENIGING (MSF)	The Netherlands
STIFTELSEN FLYKTNINGERADET (NRC)	Norway

SPIRIT / Safety and Protection of built Infrastructure to Resist Integral Threats

© SPIRIT

Information

Grant Agreement N°
242319
Total Cost
€4,885,951.00
EU Contribution
€3,497,684.50
Starting Date
01/08/2010
Duration
36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK
Physical Protection and Survivability
Lange Kleiweg 137
PO Box 45
2280 AA Rijswijk
The Netherlands
Contact
Ms Jolanda van Deursen
Tel: +31 (0) 888 66 1289
Mobile: +31 (0) 630 72 7331
Fax: +31 (0) 888 66 6932
E-mail:
Jolanda.vandeursen@tno.nl
Website: http://www.infrastructure-protection.org

Project objectives

The project SPIRIT (Safety and Protection of built Infrastructure to Resist Integral Threats) is a capability project. The aim of this project is to provide the technology and know-how for the protection of buildings and people against terrorist threats and to minimize the consequences of a terrorist attack in terms of number of casualties/injuries, damage and loss of functionality and services, by providing:

» tools to quantify the vulnerability of built infrastructure;

» a portfolio of protective products;

» a guidance tool for safety based engineering to realize a required built infrastructure protection and resilience level;

» a proposal on how to take a CBRE-threat into account in the building guidelines.

Description of the work

Terrorist attacks with explosives (E) or chemical, biological or radiological (CBR) agents are threats with a low probability but with disastrous consequences. People, critical infrastructures and utilities have to be protected. The societal community should not be disrupted by acts of terrorism.

SPIRIT works on solutions to realize sufficient resilience of the urban infrastructure for rare occasions with minimum effect on normality. Hitherto, normal regulations and building guidelines do not take into account the CBRE threat.

The required specialist knowledge on explosion dynamics, response of structures, dispersions of toxic agents and injuries is available within the SPIRIT Consortium. Making this knowledge available and finding solutions that can be integrated into normal planning and building procedures is part of the work to be carried out.

Expected results

The project will contribute to people safety and increase the resilience of built infrastructure against a terrorist threat by providing an integrated approach to counter CBRE-threats, including proposed guidelines for an EU Regulatory Framework. With this approach, government, end users of buildings and designers can define and achieve a desired level of protection.

© Spirit

PARTNERS

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)	Germany
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Schüßler-Plan Engineers Ltd (SP)	Poland
Arup Group Ltd (ARUP)	United Kingdom
Hamilton Erskine Ltd (HE)	United Kingdom
Artemis control AG (ART)	Switzerland
Ducon GmbH (DUC)	Germany
Ionicon Analytik GmbH (ION)	Austria
Corsmit Raadgevend Ingenieurs BV (CORS)	The Netherlands
European Commission - Joint Research Centre (JRC)	Italy

ADVISE / Advanced Video Surveillance archives search Engine for security applications

© AVC Group - Defence & Security

Information

Grant Agreement N°
285024
Total Cost
€4,237,304.80
EU Contribution
€2,989,761.60
Starting Date
01/03/2012
Duration
36 months

Coordinator

ENGINEERING - INGEGNERIA INFORMATICA S.P.A.
R&D Laboratory
Via Riccardo Morandi, 32
00148 – Rome - Italy
Contact
Carmela Occhipinti
Tel: +39.06.83074971
Mobile: +39.335.1328411
Fax: +39.06.83074200
(Please, write "For the attention of Carmela Occhipinti")
E-mail: carmela.occhipinti@eng.it
Website: www.eng.it

Project objectives

ADVISE aims to design and develop a unification framework for surveillance-footage archive systems, in an effort to deal with the increasingly critical need to provide automated and smart surveillance solutions. This need arises due to the continuous growth of surveillance systems in scale, heterogeneity and utility. There are two major obstacles: the variety of the technical components of the surveillance systems, producing video repositories with different compression formats, indexing systems, data storage formats and sources, and the fact that such a system should take into careful consideration the legal, ethical and privacy rules that govern surveillance and the produced content. Towards both, ADVISE has been formed by experts on both technological and legal, ethical and privacy aspects, with valuable experiences in the security field. For this purpose, the consortium includes some major European security agencies, though it will collaborate with plenty of others through its Advisory Boards.

Description of the work

ADVISE will analyse and geo-register surveillance video archives of different agencies, and extract statistical patterns of activity and search (context-based and content-based) for specific events, people and objects through ontologies and semantic representations. In effect, the ADVISE system will enable interoperability beyond the boundaries defined by different compression formats, indexing systems, data storage formats and access systems, offering valuable insights and help during investigations of law enforcement authorities. In order to realise this aim, the following concrete goals have been identified:

» Legal and ethical exchange of data to offer secure and legally/ethically compliant inter-organisation communication;

» Video Analysis & Recognition to design, develop and validate novel, beyond SoTA, video analysis and recognition algorithms that will offer semantic search and analysis capabilities for various patterns (e.g. events, persons, cars, objects);

» Geo-registration assisted video archives analysis to support efficient time and camera indexing, thus empowering the tracing back of an object/person in time and in localisation, from surveillance system to surveillance system (and the corresponding video archives);

» Interoperability and Scalability to design and develop an open and extensible framework that will offer search capabilities for various patterns (e.g. objects, persons, events), into various video archives, independently from their different technological standards and ethical/privacy and legacy issues, focusing on improving the interoperability between infrastructure operators and between law enforcement agencies. The interoperability will cover the technical layer (aiming to solve the problems related to different formats of video archives and the communication format) and the semantic one (aiming to improve the search with an understanding of what happens in the footage, what is being looked for and who can access the information).

Expected results

The ADVISE system will result in two major components. The first will perform the semantically enriched, event based video analysis, offering efficient search capabilities into video archives and sophisticated result visualisation. The second will enforce the legal/ethical/privacy constraints that apply to the exchange and processing of the surveillance data. A Dedicated Engine will be developed to efficiently deal with each peer authority's technical and legal/ethical/privacy specificities.

PARTNERS	COUNTRY
ENGINEERING - INGEGNERIA INFORMATICA SPA (ENG)	Italy
SEMANTIX TECHNOLOGIES PLIROFORIKIS TILEPIKOINONION ANONYMOS ETAIREIA (SEM)	Greece
CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS/INFORMATICS & TELEMATICS INSTITUTE (CERTH/ITI)	Greece
QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)	United Kingdom
SINGULARLOGIC ANONYMOS ETAIRIA PLIROFORIAKON SYSTIMATON & EFARMOGON PLIROFORIKIS (SL)	Greece
VRIJE UNIVERSITEIT BRUSSEL (IES/VUB)	Belgium
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA-ISDEFE (ISDEFE)	Spain
ALMAVIVA - THE ITALIAN INNOVATION COMPANY SPA (Almaviva)	Italy
INNOVATION ENGINEERING SRL (INNEN)	Italy
AYUNTAMIENTO DE MADRID (ADM)	Spain

BEAT / Biometrics Evaluation and Testing

© yewkeo - iStockphoto

Information

Grant Agreement N°
284989
Total Cost
€4,738,788.40
EU Contribution
€3,499,784
Starting Date
01/03/2012
Duration
48 months

Coordinator

IDIAP RESEARCH INSTITUTE
RUE MARCONI 19
592
1920 Martigny, Switzerland
Contact
Sebastien Marcel
Tel: +41 27 721 7727
Fax: +41 27 721 7712
E-mail: marcel@idiap.ch
Website:
https://www.beat-eu.org

Project objectives

The goal of BEAT is to propose a framework of standard operational evaluations for biometric technologies.

The BEAT project will provide standardized criteria (and metrics) to evaluate biometric systems for both academic and commercial entities. This standardization is currently lacking and would likely lead to: an improved communication between academic and commercial entities in the field of biometrics by providing a common basis for comparison, and an improvement in the state-of-the-art for biometric systems by providing a fair and centralized method to evaluate systems.

The standardization would include methods to evaluate: 1) the performance (accuracy) of a biometric system, 2) the vulnerability of a biometric system to direct attacks (spoofing) or indirect attacks (hill-climbing attacks), and 3) the performance of privacy preservation techniques.

Description of the work

Identity management using Biometrics is a reality because of the e-passport (Biometric passport). Similar biometric technology has also become more prevalent on personal computers with more biometric-enabled functions, and soon applications to recognize nomadic users through biometrics will also emerge as mobile devices are equipped with more sensors. Unfortunately the reliability of these biometric technologies is not always known and therefore can not be guaranteed. In particular the three criteria of (1) the performance of the underlying biometric system, (2) the robustness regarding vulnerabilities such as direct (spoofing) or indirect attacks, and (3) the strength of privacy preservation techniques, are often unknown or impossible to compare to competitors.

The lack of standard operational evaluations is the reason that we cannot measure the reliability of these biometric technologies. Some initiatives exist in Europe, the United States of America, and Asia. However, these initiatives are: isolated (focusing only on one or two biometric modalities), disorganized (teams from the same institution can work on different biometrics without talking to each other), or limited in time (very few are organizing ongoing evaluations). This leads to discontinuous and non-integrated efforts which have a limited life span. Thus the BEAT project will establish a framework to evaluate, in a systematic way, the performance of biometric technologies using several metrics and criteria (performance, vulnerability, privacy).

The goal of BEAT will be achieved by (1) developing an online and open platform to transparently and independently evaluate biometric systems against validated benchmarks, (2) designing protocols and tools for vulnerability analysis, and (3) developing standardization documents for Common Criteria evaluations.

Additionally, legal aspects will be considered to address the issues of both privacy data protection and Intellectual Property and so ensure that the BEAT framework can be used by the research community and companies.

Expected results

There will be three outcomes of this project. The first is that the reliability of biometric systems will be measurable and thus should lead to a meaningful increase in performance. The second is that technology transfer from research to companies will be much easier as there will be an interoperable framework. Finally, decision-makers and authorities will be informed about the progress that is made in biometrics as the results will have an impact on standards. Given these outcomes we expect that BEAT will significantly contribute to the development of a European Identification Certification System.

PARTNERS	COUNTRY
Idiap Research Institute (IDIAP)	Switzerland
Universidad Autonoma de Madrid (UAM)	Spain
University of Surrey - CVSSP (UNIS)	United Kingdom
Ecole Polytechnique Federale de Lausanne - LASEC (EPFL)	Switzerland
TURKIYE BILIMSEL VE TEKNOLOJIK ARASTIRMA KURUMU (TUBITAK)	Turkey
Commissariat à l'énergie atomique et aux énergies alternatives - LETI (CEA)	France
Morpho (MPH)	France
TÜViT (TUVIT)	Germany
Katholieke Universiteit Leuven (KULeuven)	Belgium

CREATIF / CBRNE related testing and certification facilities - A networking strategy to strengthen cooperation and knowledge exchange within Europe


© CREATIF

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217922
Total Cost
€831,279.79
EU Contribution
€831,279.79
Starting Date
01/02/2009
End Date
31/07/2011

Coordinator

SEIBERSDORF LABOR GMBH
Radiation Safety and Applications
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@seibersdorf-laboratories.at
Website: http://www.creatif-network.eu

Project objectives

CREATIF's overall aim was to explore how to promote the harmonisation of national testing procedures and facilities across Europe for detection products and services in the CBRNE (chemical, biological, radiological, nuclear and explosive) sector. Among other tasks, this called for the creation of a communication platform to enable technology users, decision makers, technology providers and testers to discuss the future development of this sector. An advisory group of end-users and industrial experts was established to help shape the project's deliverables and workshops were held in which certification and testing issues regarding CBRNE detection equipment were discussed.

One of CREATIF's key objectives was to review existing testing protocols and standards in order to suggest ways to harmonise CBRNE testing, both on a geographic and technical level across the 27 EU nations, leading to a roadmap.

Results

The project's stakeholder groups agree that testing of detection systems and comparability of testing results are needed and should be based on EU agreed standards, with certification of products based on independent third party evaluation.

CREATIF's research demonstrated that complementary testing should focus on the use of real agents (or simulants) carried out in realistic operational scenarios. Training exercises for end-users should be organised to get hands-on realistic experience with detection systems. This would enhance security by providing feedback to industry to develop better detection systems and, ultimately, save public money by enabling public authorities to select the most suitable equipment.

The project also concluded that pan-EU certification would support the development of a European market for CBRNE detection systems and reduce the costs of testing.

CREATIF's main results include:

- a glossary of terms as the basis for a common language for CBRNE detection testing;
- a database on test facilities for CBRNE detection equipment;
- a report on available standards and protocols used for testing CBRNE detection systems;
- a road map for a European certification system for CBRNE sensor systems and devices, covering the following: stakeholder assessments, terminological and system descriptions, assessment of means and methods, and certification and accreditation.

In conclusion, CREATIF's research produced a broad stakeholder consensus that standardisation of testing methods is needed to boost the quality and comparability of testing results and instruments across Europe. This should be based on the development of EU-wide testing standards, followed by either international standardisation or full mutual recognition of the standards.

PARTNERS

Seibersdorf Labor GmbH (SLG)
DGA Ministère de la Defense (DGA/MD)
Cotecna Inspection S.A. (COT)
Federal Institute for Materials Research and Testing (BAM)
Totalförsvarets Forskningsinstitut (FOI)
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)

COUNTRY

Austria
France
Switzerland
Germany
Sweden
The Netherlands

DISASTER / Data Interoperability Solution At Stakeholders Emergency Reaction

© PHOTOPQR - LE TELEGRAMME - Francois Destoc

Information

Grant Agreement N°
285069
Total Cost
€3,573,156
EU Contribution
€2,783,970
Starting Date
01/02/2012
Duration
36 months

Coordinator

TREELOGIC TELEMÁTICA Y LÓGICA RACIONAL PARA LA EMPRESA EUROPEA S.L.
R&D
Parque Tecnológico de Asturias, parcela 30
E33428 Llanera, Asturias, Spain.
Contact
Marcos Sacristán Cepeda
Tel: +34 985 966 136
Mobile: +34 663 246 699
Fax: +34 985964190
E-mail: marcos.sacristan@treelogic.com
Website: www.treelogic.com

Project objectives

» Designing a reference architecture to solve interoperability problems in data exchange in SOA-based Emergency Management Systems (EMS), addressing interdisciplinary environments at a European level;

» Designing and developing an integrative and modular interoperable data model. This objective may be split into two sub-objectives:

- The core framework data model, common to every stakeholder involved in emergency management;
- Complementary transversal (spatial and temporal) & vertical (domain-specific) modules.

» Designing and developing mediation techniques, a set of bridges, enabling a transparent integration of the data model within already-existing SOA-based EMSs;

» Developing and executing a validation pilot phase in an actual environment, based on a representative scenario, in order to get feedback from end-users, and evaluating the project's outcomes and their benefits to the European multicultural domain related to emergency management.

Description of the work

Emergency management and information exchange become more challenging in an international crisis episode because of cultural, linguistic and legal differences between all stakeholders, especially first responders. Misunderstandings between first responders slow down decision-making and make it more difficult. The recent spread and development of networks and Emergency Management Systems (EMS) has facilitated communication and improved emergency responses, allowing them to become more coordinated and successful in overcoming distance issues, and allowing decentralized decision-making when necessary and appropriate. However, EMSs have still not solved problems related to cultural, legal and linguistic differences which are the greatest cause of slow decision-making. In addition, from a technical perspective, the consolidation of current EMSs and the limitations of their exchanged data formats offer significant problems to be solved in any solution proposing information interoperability and understanding between heterogeneous Emergency Management Systems located in different countries, and operating within different contexts.

To overcome this complicated situation, a two step solution is proposed: (i) As the main objective and foundation of the DISASTER project, the development of a common and modular ontology shared by all the stakeholders is proposed to offer the best solution to gather all stakeholders' knowledge in a unique and flexible data model, taking into account different countries' cultural, linguistic and legal issues; (ii) Then, taking advantage of the fact that most legacy Emergency Management Systems are based on Service-Oriented-Architectures (SOA), i.e. those systems compile information from distributed and specialized systems (e.g. Geographic Information Systems). The interoperability information burden will be addressed by means of transparent SOA mediation algorithms compliant with current data formats and existing solutions.

Taking into account the heterogeneity and diversity of all existing scenarios in crisis episodes, potential results of the ontology-based interoperability solution proposed will be validated through the design and development of a realistic prototype scenario, which will actively involve both emergency managers and emergency first responders from organisations with significant experience in developing capability in technologies and organisational structures towards increased interoperability.

Expected results

The project's target outcome is an integrative and modular ontology for establishing a common knowledge structure between all the first responders involved in an emergency, but being compliant with legacy international data formats exchanged in the European Union as long as they are seamlessly integrated within current SOA-based Emergency Management Systems.

PARTNERS	COUNTRY
Treelogic Telemática y Lógica Racional para la Empresa Europea S.L. (TREE)	Spain
Fachhochschule Köln (CUAS)	Germany
Fundación CTIC Centro Tecnológico para el desarrollo en Asturias de las Tecnologías de la Información (CTIC)	Spain
Dansk Brand-Og Sikringsteknisk Institut Forening (DBI)	Denmark
Aimtech Consulting Limited (AIM)	United Kingdom
Veiligheidsregio Kennemerland (VRK)	The Netherlands
Antworting Ingenieurburo Weber Schutte Kaser partnerschaft (ANT)	Germany

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

Information

Grant Agreement N°
225404
Total Cost
€4,180,383.81
EU Contribution
€2,798,517.50
Starting Date
01/01/2010
Duration
36 months

Coordinator

SAGEM DEFENSE SECURITE
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/

Project objectives

One of the main problems of First Responders (FR) (fire fighters, police, etc.) in the case of a crisis occurring at critical infrastructures is the availability of relevant information for the First Responder itself and for the local manager. The loss of communication 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 FR 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 headquarters.

DITSEF aims at increasing the effectiveness and safety of First Responders through 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 workshops:

» *First Workshop:* The first workshop is dedicated to the common and usual scenarios which drive FR interventions (analysis of potential threats, typical emergency operations with a definition of the role of FRs according to their defined missions);

» *End-user inputs:* Presentation of some typical infrastructures (arrangement of the buildings, legal constraints, emergency measures) and of typical iinterventions of FRs;

» *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);

» *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;

» *End-user inputs:* Analysis and comments with the R&D team regarding the proposed solutions and first view of the integration in a systemic approach;

» *Fifth Workshop:* Demonstration with FR in a 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.

PARTNERS	COUNTRY
Sagem Défense Sécurité (SDS)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Cassidian S.A.S. (EADS)	France
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Elsag Datamat spa (ED)	Italie
National Centre for Scientific Research "Demokritos" (DEM)	Greece
INFITHEON Technologies Ltd (INFI)	Greece
T - SOFT spol. s r.o. Praha (TSOFT)	Czech Republic
National Civil Protection Service Directorate General (MES-TDCP)	Bulgaria
SELEX Sistemi Integrati S.p.A. (SSI)	Italie

EQUATOX / Establishment of Quality Assurances for the Detection of Biological Toxins of Potential Bioterrorism Risk

Information

Grant Agreement N°
285120
Total Cost
€1,591,305.10
EU Contribution
€1,338,634
Starting Date
01/01/2012
Duration
36 months

Coordinator

ROBERT KOCH-INSTITUT
Center for Biological Security, Microbial Toxins (ZBS3)
Nordufer 20
13353 Berlin, Germany
Contact
Dr. Brigitte G. Dorner
Tel: +49 30 18754 2500
Fax: +49 30 18754 2501
E-mail: DornerB@rki.de
Website: www.rki.de

Project objectives

The features of biological toxins like ricin, botulinum toxins, staphylococcal enterotoxins and saxitoxin place them at the interface of biological and chemical agents. They could be used for terrorist attacks on the basis of their availability, ease of preparation, their toxicity or the lack of countermeasures. Some of the toxins are considered among the most relevant agents in the field of bioterrorism, for which the current preparedness within European countries should be further improved to limit casualties in the case of an intentional release. While different technologies for toxin detection have been established, hardly any universally agreed "gold standards" are available, and reference materials as well as proficiency tests are generally lacking.

To address these issues EQuATox will create a network of experts among EU 27 and Associated Countries, focussing on biological toxins and integrating experts from the security, verification, health and food sector.

Description of the work

The main objectives of EQuATox are the following:

» Establishment of an EU-wide network focussing on the detection and identification of biological toxins which are at the interface of classical B- and C-agents and are highly relevant in terms of a potential biothreat attack;

» Screening for information within Europe: who is responsible for the detection of biological toxins of potential bioterrorism risk in each country? Currently 32 laboratories from 20 countries are interested in taking part in the EQuATox project, and the network is open for further laboratories to join us;

» Generation and characterisation of toxin reference material, in case it is not accessible from certified sources. Four independent proficiency tests are planned to compare diagnostic results attained by different analytical approaches (one proficiency test on ricin, saxitoxin, staphylococcal enterotoxin B and botulinum toxins, respectively);

» Identification of "best practices" for the analysis of the different biological toxins based on the results obtained in the proficiency tests. Recommendations will be given on how to close any gaps identified in order to minimise potential health and security risks for European citizens;

» Exchange of information and know-how between all network partners, including information on protocols, reagents etc. in order to optimize analytical procedures within the network's laboratories.

Expected results

By creating a network of experts the project will substantially help to minimise security and health threats posed by biological toxins. Based on the status quo of toxin detection described in EQuATox, good practices and critical gaps in detection technology will be identified as foundations to harmonise and standardise detection capabilities.

PARTNERS	COUNTRY
Robert Koch-Institut (RKI)	Germany
European Commission - Joint Research Centre (JRC)	Belgium
Institut Scientifique de Santé Publique (WIV-ISP)	Belgium
University of Helsinki, Finnish Institute for Verification of the Chemical Weapons Convention, VERIFIN (UH/VERIFIN)	Finland
French agency for food, environmental and occupational health safety (Anses)	France
Toxogen GmbH (Toxo)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Federal Department of Defence, Civil Protection and Sport - SPIEZ LABORATORY (VBS-LS)	Switzerland
ChemStat (CHS)	Switzerland

EULER / European software defined radio for wireless joint security operations

© RCP Photo - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218133
Total Cost
€15,468,483
EU Contribution
€8,720,692
Starting Date
01/03/2009
End Date
30/04/2012

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

Project objectives

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.

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 reusability of these elements across platforms from different organisations and suppliers.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

© wayne ruston - Fotolia.com

PARTNERS	COUNTRY
Thales Communications S.A	France
Cassidian S.A.S. (EADS DS)	France
Astrium Ltd. (EADS-Astrium)	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
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Indra Sistemas S.A.	Spain
Rohde & Schwarz gmbh.	Germany
Center for Wireless Communications, University of Oulu	Finland
Prismtech Limited	United Kingdom
Interuniversitair Micro-Electronica Centrum VZW (IMEC)	Belgium
European Commission - Joint Research Centre (JRC)	Belgium
Ecole Superieure d'Electricite	France
Elektrobit Wireless Communications	Finland
SELEX Sistemi Integrati S.p.A. (SELEX)	Italy

FREESIC / Free Secure Interoperable Communications

Information

Grant Agreement N°
285205
Total Cost
€4,338,320
EU Contribution
€3,284,040
Starting Date
01/02/2012
Duration
30 months

Coordinator

ARDACO, A.S.
Polianky 5
84101 – Bratislava - Slovakia
Contact
Miroslav Konecny
Tel: +421 232 212 311
Mobile: +421 910 889 650
Fax: +421 232 212 312
E-mail: miroslav.konecny@ardaco.com
Website: www.freesic.eu

Project objectives

The main objective of FREESIC is to validate an innovative interoperability ICT concept for better cooperation of various emergency responders (both public services and private grid services).

FREESIC investigates barriers to interoperability of emergency services, proposes a communication solution supporting information exchange through heterogeneous communication systems, deploys the interoperability platform into three countries and evaluates its operation.

Security aspects and user requirements are both essential and shape the delivery of the project.

Description of the work

The FREESIC project creates a solution that will allow highly secure and cost effective interoperability between communication infrastructures right across Europe. The project has been inspired by legal, organizational and operational barriers the consortium has encountered during its previous activities (i.e. the project Secricom).

Approach

Existing interoperability solutions such as gateways are the right approach and will simplify FREESIC's adoption and in return FREESIC will open broader possibilities for them. It will be operated free-of-charge and will offer an open source gateway, documentation and operational guidelines for others to use. It is the project's ambition to continue the free-of-charge operation after the project's end as well. The operational costs will be covered by the new business opportunities.

Operation

The system should motivate end users outside the consortium to request the integration from their system vendors or integrators. The architecture will take into account ongoing standardization research (e.g.: NCOIC Interoperability Framework) to reduce the integration time and costs. The integration process will be simple; the system integrator takes the gateway and modifies it as needed. The gateway remains the property of the integrator. The integrators do not have to worry about disclosing any know-how or information. The communication between gateways will be end-to-end encrypted and the gateway will be under full control of end users to avoid security concerns.

Workpackage structure:

» *WP1* – Project management;

» *WP2* - Requirements and limiting factors analysis;

» *WP3* - Definition of technical and non-technical solutions;

» *WP4* - Implementation of the interoperability platform;

» *WP5* - Integration of end user systems;

» *WP6* - Acceptance and scenario testing by users;

» *WP7* - Dissemination and exploitation.

Expected results

The FREESIC project investigates and proves ways to provide the secure and cost effective interoperability between as many communication systems as possible without having to do the Sisyphean task of never-ending one-to-one integration.

FREESIC will be cost effective, based on EU standards and standard protocols so effort needed to integrate is minimal. The motivation for system integrators is in the form of new services they can provide to their users.

PARTNERS	COUNTRY
Ardaco, a.s. (ADO)	Slovak Republic
National Security Authority of the Slovak Republic (NSA)	Slovak Republic
Université du Luxembourg (UL)	Luxembourg
British Association of Public Safety Communication Officers (BAPCO)	United Kingdom
ITTI Ltd. (ITTI)	Poland
NEXTEL S.A. (NEX)	Spain
Centre de Communications du Gouvernement (CCG)	Luxembourg
World Consult, a.s. (WCT)	Slovak Republic
Pramacom Prague (PCM)	Czech Republic

GERYON / Next generation technology independent interoperability of emergency services

© GERYON

Information

Grant Agreement N°
284863
Total Cost
€3,590,730.20
EU Contribution
€2,512,308.65
Starting Date
01/12/2011
Duration
30 months

Coordinator

UNIVERSIDAD DEL PAIS VASCO EHU UPV
Faculty of Engineering of Bilbao
Alameda Urquijo s/n
48013 Bilbao, Spain
Contact
Fidel Liberal
Tel: +34 946014129
Fax: +34 946014259
E-mail: fidel.liberal@ehu.es
Website: www.sec-geryon.eu

Project objectives

GERYON proposes seizing the existing window of opportunity due to the convergence of commercial LTE networks, IMS as a predominant enabler for multimedia networks, and uncertainty about the future of classic emergency networks due to spectrum scarcity, digital dividend issues and economic crisis.

The project aims at unifying technical and operational logic of first responder communications by providing an IMS based technology independent system. GERYON will ensure seamless operation regardless of the access technology and take advantage of the coverage and responsiveness of existing PMRs and broadband data services of 4G networks.

Intermediate objectives include the design and development of:

- A fully operational IMS-driven emergency services management platform;
- An emergency services central management system and associated transcoding and security gateways.
- Advanced decision support logic for multimedia emergency communications;
- A technology agnostic TETRA-IMS interconnection gateway;
- A software client that will allow for using a subset of GERYON services through non-GERYON access networks;
- A transnational TETRA and 4G based testbed.

Description of the work

GERYON proposes an innovative emergency interworking system capable of connecting existing first responder communication systems and enabling the integration of next generation mobile networks by defining technology independent standardized interfaces and autonomic configuration and adaptation techniques under the umbrella of IMS.

GERYON will demonstrate both classic (i.e. PTT, MTP and preemptive calls) and enhanced emergency services (i.e. multimedia streaming and data services) over an across-frontier testbed. Furthermore, its capability for including general purpose IMS terminals and GERYON enhanced ones will allow an easy access to first responder networks to general purpose devices.

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

Specifications and system design.
The initial stage is dedicated to the definition of the overall system architecture and the specifications of the GERYON interfaces between different modules and systems, including internal ones and those related to IMS signalling. The trial plan and tests to be conducted will be also specified. End users will take an active role in the requirements gathering stage of this WP.

GERYON management system design and development.
This WP deals with the design and implementation of the hardware and software modules of the central management system, as well as the considered emergency services and transcoding and security gateways.

Interconnection gateway design and development.
A technology independent reference interconnection gateway will be designed in this WP. Later, a working prototype considering TETRA, LTE and IMS will be developed according to a GERYON specific testbed.

GERYON-enabled LTE emergency communications.
The GERYON testbed will demand basic technology dependent interfaces to be developed for the LTE scenario.

Integration, Field Trials and Evaluation.
The final WP is dedicated to the integration of all the systems, components, hardware and software modules that have been developed in previous WPs into a complete system, in order to demonstrate the whole GERYON ecosystem. Again, end users will take part significantly in trial and evaluation tasks.

Expected results

Apart from the development and deployment of the needed technological modules considered as the main objectives of the project, a particularly important expected outcome of GERYON lies in the approach itself: "IMS based technology agnostic emergency services as enablers of interoperable current and future PMRs".

Indeed, although specific modules in the GERYON testbed will depend on a current PMR (and vendor specific issues may also arise), the "reference gateway" will allow the interconnection of different technologies towards the Next Generation Networks paradigm.

PARTNERS	COUNTRY
Universidad del Pais Vasco EHU UPV (UPV/EHU)	Spain
Itelazpi SA (ITEL)	Spain
Grupo Comunicaciones y Sonido SL (CYS)	Spain
University of Plymouth (UoP)	United Kingdom
Viotech Communications SARL (VIO)	France
National Center for Scientific Research "DEMOKRITOS" (NCSRD)	Greece
Cosmote Kinites Tilepikoinonies AE (COS)	Greece

HELP / Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261659
Total Cost
€1,352,219
EU Contribution
€991,255
Starting Date
01/02/2011
End Date
30/04/2012

Coordinator

UNIVERSITAT POLITÉCNICA DE CATALUNYA
Signal Theory and Communications
Jordi Girona 31
08034- Barcelona-Spain
Contact
Oriol Sallent
Tel: +34 93 4017197
Mobile: +34 619 35 16 54
Fax: +34 93 4017200
E-mail: sallent@tsc.upc.edu
Website: www.fp7-sec-help.eu

Project objectives

It is generally acknowledged that existing wireless communication networks frequently fall short of meeting users' needs and cannot properly support the management of emergency and disaster relief scenarios. HELP will establish a comprehensive solution framework for supporting public safety communications aspiring to significantly enhance the communications in emergency situations. The envisioned solution framework consists of significantly strengthening the role and commitment of commercial wireless infrastructures in the provision of public safety communications. Only a solution framework targeted at creating and exploiting synergies of composite radio systems encompassing commercial and professional mobile radio networking technologies can address the complex requirements of modern emergency communications. HELP will define and establish the foundations for the development of network and spectrum sharing concepts between networks. HELP will identify the key features and functional building blocks of the operations and management system needed to achieve a synergic and holistic operation of the composite radio systems.

Description of the work

HELP will firstly identify operational user requirements, scenarios and overall system requirements. The scenarios will be created jointly with a User Advisory Board (UAB), formed by public safety users from diverse emergency service organisations. Then, HELP will define a solution framework (system concept) for the provision of public safety communications over diverse wireless infrastructures.

This will include, e.g.:

» determining internetworking solutions,

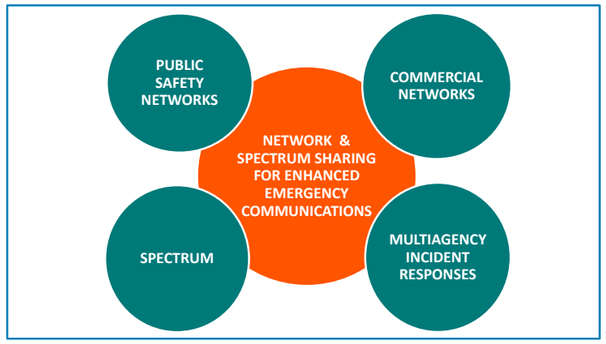
» determining the required features and functionalities that will enable the use of commercial systems for public safety communications in emergency and disaster relief operations, and

» determining new spectrum usage models to enhance communications in emergency scenarios by means of proper spectrum management mechanisms.

An Operator Advisory Board (OAB) will be established to validate the envisioned system concept. Following this, a framework for the management of the composite emergency network will be defined. Besides, the economic impact that the novel technical solutions proposed in HELP may have on the involved stakeholders will be investigated. HELP will eventually establish a consolidated basis and roadmap for the realisation of the envisioned solution framework.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.



PARTNERS

Universitat Politècnica de Catalunya (UPC)
DataX Sp. z o.o. (DTX)
Cassidian S.A.S. (EADS DS)
BAPCO LBG (BAPCO)
European Commission - Joint Research Centre (JRC)

COUNTRY

Spain
Poland
France
United Kingdom
Belgium

SAVASA / Standards Based Approach to Video Archive Search and Analysis

© Mike Zakharov - Fotolia.com

Information

Grant Agreement N°
285621
Total Cost
€4,061,085
EU Contribution
€3,166,266.58
Starting Date
01/12/2011
Duration
30 months

Coordinator

ANGEL IGLESIAS S.A. - IKUSI
R&D
Paseo Miramon
20009, San Sebastian
Contact
Gorka Peréz
Tel: +34 943 44 88 00
Mobile: +34 650 15 69 56
Fax: +34 943 44 88 20
E-mail:
gorka.perez@ikusi.com
Website: http://www.ikusi.com/

Project objectives

The SAVASA project proposes the creation of a video archive search platform that allows authorised users to perform semantic queries over different, remote and non-interoperable video archives. This project will exploit the current trends in computer vision, video retrieval and semantic video analysis. It is also a goal of the project to ensure that its results are capable of deployment in distributed systems and as software services.

However, technology for technology's sake is of little value. Therefore the involvement of ethicist, legal experts and, those users who must operate Video Archive installations and services to meet the needs of law enforcement agencies and judicial authorities, as well as those of civil protection and day-to-day organisational needs, is required. The SAVASA consortium covers each of these roles.

At its core, SAVASA will use existing reference technologies from the ICT field that have overcome the barrier of system interoperability/compatibility, i.e. between container and compression formats. The project will implement a prototype platform capable of demonstrating unified archive integration and an approach to common search and indexing. The project will also provide a set of tailored video analytics and semantic analysis tools that will provide added value to end-users, but which can also function within a legal and ethical framework. The project will provide an analysis of existing technical barriers/requirements in the standardisation of technologies and procedures, via the validation testing of a prototype platform with end users.

Description of the work

The SAVASA project plan will focus on the following objectives:

Interoperability:
» Application of semantic technologies to enhance the analysis of video archive content;
» Compliance with national and European regulations applicable to video surveillance.

Open standards:
» Definition of a migration path from proprietary technologies to open standards;
» Propose best practices and procedural approaches in the absence of defined standards;
» Participation in standards bodies relevant to the results of the project;
» Leverage existing Open and International Standards, and open source initiatives.

User focused applied research:
» Focus on the real user needs, such as operators and law enforcement agencies that make intensive use of video archives;
» The introduction of high level and rich information to video sources to boost data mining from video archives, as well as keeping protected privacy data through the application.

Ethical and privacy protection:
» Address issues that video surveillance inevitably implies; ethically sensitive issues related to personal data beyond what is established by law;
» Operational restrictions controlled by rules on conducting situational assessments to ensure that required control levels are reached.

Video analytics:
» Application of the latest trends in object detection and tracking, based on probabilistic inference and models, to enhance robustness and accuracy of elements of interest descriptions within videos;
» Use of signal encryption and cryptographic methods to protect private elements of the video;
» Exploitation of visual features to identify object properties in order to enrich the metadata descriptions;
» Development of video analysis tools to automatically annotate video with semantic concepts and scenarios.

Contribution to Standards:
» Contribution to standards related to video surveillance, storage, secure communications and metadata indexing;
» Development of a set of operational best practices derived from the results of end-user validation tests.

Multiple Archive Integration:
» Integration of multiple video archive systems (remote or local), under a single technology that presents these archives as a homogenous logical system vis-à-vis an indexing and search system;
» Multi-modal search across multiple video archives tailored to the requirements of end users of surveillance video archives;
» Implementation of the core technological deliverables as a set of distributed applications suitable for deployment as software services.

Expected results

SAVASA will provide a step forward in Video Surveillance Archive Exploitation by providing capabilities for seamless integration archives, widened archive search enabling semantic analysis, enhanced metadata tagging, integration of ethical, legal and privacy controls, contribution to standards, reduction of manual intervention in archive analysis and technology to support judicial requests. SAVASA will achieve these results through three formal prototypes with end user validation.

PARTNERS	COUNTRY
Angel Iglesias S.A.- IKUSI (IKUSI)	Spain
Asociación Centro de Tecnologías de Interacción Visual y Comunicaciones Vicomtech (VICOM)	Spain
Studio Professionale Associato a Baker & McKenzie (BAK)	Italy
HI-Iberia Ingeniería y Proyectos S.L. (HIB)	Spain
Dublin City University (DCU)	Ireland
University of Ulster (UU)	United Kingdom
INECO (INECO)	Spain
Demokritos (NCSRD)	Greece
Sintel Italia (SINTEL)	Italy
Dirección General de Tráfico – Ministerio del Interior (DGT)	Spain
RENFE Operadora (RENFE)	Spain

SECRICOM / Seamless communication for crisis

© L_ PackShot - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218123
Total Cost
€12,424,827.51
EU Contribution
€8,606,568.20
Starting Date
01/09/2008
End Date
30/04/2012

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

Project objectives

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.

Solve problems of contemporary crisis communication infrastructures:

» Seamless and secure interoperability of the several 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, bringing 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 a secure wireless fault tolerant communication system for mobile devices based on a 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, an interoperable, recoverable and extendable network;

» Communication infrastructure monitoring and control centre equipped with localization of actors.

Working infrastructure – the objective of the SECRICOM project will be ensured by:

» Integration of research results; and

» Demonstrator creation and presentation.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

© Secricom

PARTNERS

QinetiQ Ltd
Ardaco, as. (ADO)
Bumar sp. z o.o. (BUM)
NEXTEL S.A. (NEX)
Infineon Technologies AG (IFX)
Université du Luxembourg (Uni Lu)
Ustav Informatiky, Slovenska Akademia Vied (UI SAV)
Technische Universität Graz (TUG)
Geothermal Anywhere, s.r.o. (SMT)
ITTI Sp. z o.o. (ITTI)
British Association of Public Safety Communication Officers (BAPCO)
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
Hitachi Europe SAS (HIT)
University of Patras (UOP)

COUNTRY

United Kingdom
Slovakia
Poland
Spain
Germany
Luxembourg
Slovakia
Austria
Slovakia
Poland
United Kingdom
France
France
Greece

SLAM / Standardisation of Laboratory analytical methods


© SLAM

Information

Grant Agreement N°
285410
Total Cost
€1,237,261.33
EU Contribution
€1,117,608.41
Starting Date
01/04/2012
Duration
24 months

Coordinator

UMEÅ UNIVERSITY
European CBRNE Center
Umeå University campus
90187 Umeå, Sweden
Contact
Dr Agneta H. Plamboeck
Tel: +46 (0) 90 10 67 34
Mobile: +46 (0) 73 211 10 00
E-mail: Agneta.plamboeck@cbrne.umu.se

Project objectives

The purpose of the present project is to propose a system view on the need for quality control (i.e. standards) on the European capability for CBRN analysis. Discussing the needs at different levels and for different purposes the SLAM project will invite representatives from relevant laboratories of the EU Member States in order to achieve a widespread understanding and approval of the differentiated needs of the CBRN analytical capability. Tutorial tabletop inter-calibration laboratory exercises will become a useful instrument in this process. The final outcome of the project is a road-map for the development of European CBRN laboratory standards.

The objectives are:

» To suggest and seek agreement between the EU 27 on differential needs for CBRN laboratory standards;

» To motivate and initiate a discussion on different CBRN networks depending on the role and requirement of laboratories;

» To engage and educate relevant laboratories in the EU 27 on inter-calibration exercises for CBRN analytical laboratories as requested in the call;

» To produce a road-map for correct and efficient standardisation of the European CBRN laboratory capability as requested in the call.

Description of the work

The SLAM project is a two-year project that is broken down into six work packages (WP). WP0 contains the management and coordination efforts of this project, which also includes arranging a kick-off meeting and a workshop for WP1-WP3 to facilitate the harmonisation process between those work packages.

WP1, WP2 and WP3 cover Chemical Analysis, Biological Analysis and Radio Nuclear Analysis, respectively and will together, in coordination, generate an overview of European laboratories analysing CBRN substances and background materials like CBRN threat agents, existing procedures and protocols relevant for the threat agents. This also involves an overview and comparison of different standard regimes for the full analytical cycle, i.e. from sampling to the interpretation of data. Transportation regulations, guidelines and systems in place among European laboratories are also part of the background material needed for the final road-map.

WP4 will illustrate relevant cases of mixed or unknown samples. An inventory will be made of different methods that have been developed and applied for unknown samples suspected to contain highly toxic and/or highly infectious and/or dangerous radioactive material. WP4 will depend on input from WP1–WP3 and thereafter similarly to these WPs perform a full cycle analysis, from sampling to interpretation of data.

WP5 will collate inventories of existing initiatives (regimes), and their protocols and methods from WP1-4 and develop a workshop programme based on that information. WP5 will promote the interaction with neighbouring Member States and will, through a workshop with co-beneficiaries and stakeholders, analyse the outputs of WP1 to 4 and discuss and propose the most suitable standard operating procedures for Member States reference laboratories to follow for CBRN incidents. This involves agreeing on the best practices as well as issues relevant to surveillance, alert and response at local and national level. The outputs of the workshop will in turn be tested through a Round Robin inter-calibration exercise.

Finally, WP6 will use all available inputs, internal (WP1 to WP4), external and WP5, to suggest a road-map for needs and means to achieve systematic standardisation of European CBRN analytical capability.

Expected results

Enhancing the competence in Member States in the development of common methods, procedures and protocols for the detection, analysis and identification of CBRN substances allowing for a significant comparison of results from different laboratories and operators within Europe.

A road-map suggesting methods of choice and processes and means to implement necessary standards to CBRN analysis will be presented and reported. A functional standardisation of CBRN analysis at the necessary level of stringency will become an important component of a Europe more resilient to CBRN incidents.

PARTNERS

Umeå University (UmU)
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
Forsvarets forskningsinstitutt (FFI)
Totalförsvarets Forskningsinstitut (FOI)
Health Protection Agency (HPA)
Robert Koch-Institut (RKI)
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)

COUNTRY

Sweden
France
Norway
Sweden
United Kingdom
Germany
The Netherlands

VIDEOSENSE / Virtual Centre of Excellence for Ethically-guided and Privacy-respecting Video Analytics in Security

© iofoto - Pavel Losevsky - Hunta - NZphotos - Fotolia.com

Information

Grant Agreement N°
261743
Total Cost
€6,412,895
EU Contribution
€5,282,366
Starting Date
01/05/2011
Duration
48 months

Coordinator

THE UNIVERSITY OF READING
Intelligent Media Systems and Services Research Laboratory, School of Systems Engineering
Whiteknights Campus
PO Box 217
RG66AH Reading
United Kingdom
Contact
Prof. Atta Badii
Tel: +44 (0) 118 378 7842
Fax: +44 (0) 118 975 1994
E-mail:
atta.badii@readiing.ac.uk
Website:
www.imss.reading.ac.uk

Project objectives

The objectives of VideoSense are to investigate Video Analytics RTDI and Ethical issues and update the stakeholders including both citizens and implementers on the latest actionable insights regarding the optimisation of acceptable and effective Video Analytics adoption including how best to:

- Implement Ethical and Privacy Safeguards;
- Minimise False Alerts;
- Minimise Network (data) traffic bandwidth demand arising from VA deployment;
- Minimise the required human attention bandwidth in using VA surveillance;
- Ensure easy, cost-effective, efficient and effective deployment of VA systems;
- Establish a sustainable business case and revenue model for VA technology uptake;
- Minimise the storage requirements for VA deployment;
- Integrate with identification technologies;
- Trust interoperability between VA systems;
- Conduct benchmarking and comparative evaluation of alternative products.

VideoSense, through its joint programme of research studies will seek to examine: a) the recent achievements, b) the breakthroughs that are needed to achieve the expected results, c) the disciplines that are relevant and need to be applied to problems, and d) the best approach for establishing and managing a benchmarking and evaluation framework.

Description of the work

VideoSense will integrate leading European research groups to create a long-term open integration of critical mass in the twin areas of Ethically-Guided, and, Privacy Preserving Video Analytics where the advent of new data intelligence technologies against the background of dynamic societal and citizen goals, norms, expectations, safety and security needs and thus surveillance requirements have all contributed to a complex interplay of influences which deserve in-depth study and solution seeking in order for European society, citizens and industry to strike the optimal balance in resolution of the various challenges in this arena. Accordingly VideoSense provides for: i) Fostering increased sustainable relationships between existing national research groups; ii) Momentum building by integrating existing researchers and resources to push forward new paradigms and the knowledge basis for the resolution of ethically guided, sensible, selective, useful, cost–effective solutions to society's surveillance needs; iii) Establishing a Virtual Centre of Excellence and expandable framework, based on Pan-European integration of complementary expertise and optimisation of shared, flexible, modular and interconnected resources including knowhow, laboratories and people to support collaborative research and agenda setting; iv) Two external Boards of Industrial and Scientific Advisors to keep the targeted research focused and responsive to the needs of European citizens, society and industry; v) Establishing a standard framework for Ethical Compliance Audit Management based on a suitably evolved Compliance Audit Maturity Model (CAMM) and associated Training and Certification services as both a service to organisations and revenue streams to ensure longer-term sustainability of the Video-Analytics Centre of Excellence.

Expected results

The VideoSense Virtual Centre of Excellence will play a significant role by bringing together a critical mass of leading experts and resources that will foster significant advances in the domain of ethically-aware data and video analytics with a synergic and integrated approach. VideoSense efforts will fill capability gaps and provide clear added-value to security needs both from the technical perspective as well as from the ethical and regulatory one; in VideoSense the respect of privacy and civil liberties will be both a guiding principle as well as part of the delivered results.

PARTNERS	COUNTRY
THE UNIVERSITY OF READING (UoR)	United Kingdom
QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)	United Kingdom
EURECOM (EURECOM)	France
THALES SECURITY SOLUTIONS & SERVICES SAS (THALES)	France
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA- ISDEFE (ISDEFE)	Spain
TECHNISCHE UNIVERSITAET BERLIN (TUB)	Germany
ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE (EPFL)	Switzerland
INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)	Belgium

ADDPRIV / Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance

© Andrey Maslennikov - istockphoto.com

Information

Grant Agreement N°
261653
Total Cost
€4,077,720.40
EU Contribution
€2,818,338.00
Starting Date
01/02/2011
Duration
36 months

Coordinator

ANOVA IT CONSULTING, SL
Avda. Punto Mobi, 4 - Parque Científico Tecnológico de la Universidad de Alcalá
28805 – Alcalá de Henares
Spain
Contact
Paolo D'Arminio
Tel: +34 918 305 977
Mobile: +34 634 933 543
Fax: +34 918 305 928
E-mail: paolo.darminio@anovagroup.es
Website: www.addpriv.eu

Project objectives

The ADDPRIV project proposes novel knowledge and developments to better comply with citizens' privacy rights through limiting the storage of unnecessary data throughout existing multicamera networks.

It addresses the challenge of determining in a precise and reliable manner private data captured by video surveillance systems that are not relevant from a security perspective.

ADDPRIV proposes solutions for automatic discrimination of relevant data recorded on a multicamera network, related to an individual whose suspicious behaviour triggered an alert. Relevant data not only corresponds to video scenes capturing individuals' suspicious behaviour (smart video surveillance), but also automatically extracting images of these individuals recorded before and after the suspicious event and across the surveillance network.

Description of the work

The project is divided into 8 work packages, 6 devoted to R&D and 2 devoted to Management Activities:

» **Requirements for better compliance with privacy rights:** precise definition of all legal and ethical specifications that the solution has to fulfil; preliminary definition of the system compliance with citizens' privacy evaluating criteria;

» **Definition of technical specifications:** detailed definition of the ADDPRIV solution's technical specifications; definition of the standards to be used in order to ensure interoperability; precise definition of the real life scenarios for testing;

» **Data relevancy discrimination algorithms:** generation of new algorithms for Automatic Data Relevancy Discrimination capable of reconstructing the route followed by a suspicious person throughout a camera network, automatically triggered by smart surveillance algorithms and capable of adapting to different scenarios;

» **Intelligent storage and secure deletion technologies:** development of intelligent storage algorithms and methodologies for the automatic browsing and retrieval of all the relevant data related to a suspicious event (automatic processes that avoid a manual handling of the recorded images that lead to privacy infringements); development of secure erase technologies specific for SSDs to be applied on images that are not relevant from a security perspective;

» **Implementation and validation of developed solutions in a real life scenario:** design and implementation of the developed solution in a real application context along with the already existing video surveillance systems;

» **Analysis of the impact of the proposed solutions on human rights and organizational processes:** analysis of ADDPRIV's impact on the organizations involved in surveillance and security in order to look for possible amendments to the technological solution; development of a strong and detailed understanding of the current public concerns with privacy, security and surveillance in order to address them;

» **Project Coordination and Quality Management;**

» **Dissemination, Exploitation and Ethical Management.**

Expected results

ADDPRIV aims to find a balance between security needs and citizens' privacy through limiting the collection and storage of unnecessary data. This will pave the way towards an approach to video surveillance where the respect for human rights will be central.

It also aims to improve the competitiveness of the European Industry in the video surveillance sector by developing new solutions for the mid-term future that meet the society demands and are therefore committed to lead a change in the European legislation to enforce the use of privacy-sensitive systems whenever possible.

PARTNERS	COUNTRY
ANOVA IT CONSULTING, SL	Spain
KINGSTON UNIVERSITY HIGHER EDUCATION CORPORATION	United Kingdom
POLITECHNIKA GDANSKA	Poland
LANCASTER UNIVERSITY	United Kingdom
AVANZIT TECNOLOGIA, S.L.	Spain
HEWLETT PACKARD ITALIANA SRL	Italy
SOCIETA PER AZIONI ESERCIZI AEROPORTUALI SEA SPA	Italy
Renfe Operadora	Spain
THE PROVOST FELLOWS & SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN	Ireland

ALTERNATIVE / Developing alternative understandings of security and justice through restorative justice approaches in intercultural settings within democratic societies

Information

Grant Agreement N°
285368
Total Cost
€4,354,777.60
EU Contribution
€3,423,262.00
Starting Date
01/02/2012
Duration
48 months

Coordinator

KATHOLIEKE UNIVERSITEIT LEUVEN (KU LEUVEN)
Leuven Institute of Criminology (LINC)
Hooverplein 10
3000 Leuven, Belgium
Contact
Inge Vanfraechem
Tel: +32 16 32 5277
Fax: +32 16 32 5463
E-mail: inge.vanfraechem@law.kuleuven.be
Website: www.law.kuleuven.be/linc

Project objectives

The overall objective of this project is to provide an alternative and deepened understanding based on empirical evidence of how to handle conflicts within intercultural contexts in democratic societies in order to set up security solutions for citizens and communities. From this general objective several specific objectives are derived :

» To develop a coherent theoretical framework for an alternative understanding of security and justice,

» To develop empirically applicable knowledge on conflict and conflict transformation in intercultural settings,

» To design, apply and evaluate concrete action models in four different intercultural conflict settings, based on an alternative understanding of justice and security and on existing restorative justice (RJ) models, and

» To analyse the findings from the four pilot settings in a comparative way and to advance knowledge by integrating the empirical results into theoretical insights and by adapting the latter where appropriate.

Description of the work

The project is set up in different work-packages (WP). Three work-packages focus on the theoretical development of the concepts: WP1 will: critically analyse the existing epistemologies of thinking, talking about, and doing justice in current democratic societies, especially in relation to the discourse on human security; offer a new theoretical understanding based on alternative epistemologies on how to tackle conflict, especially in intercultural settings in a constructive and transformative way; and analyse RJ as an alternative academic and policy oriented discourse to the current dominant discourses on justice and human security. WP2 will: undertake an analysis of 'conflict' in intercultural contexts, conflict transformation mechanisms and security perceptions; study the role of dialogical processes and possible contributions from civil society in conflict transformation at individual and societal level; study the role of gender and age in conflict resolution approaches; and investigate conflict transformative processes in an intercultural context at three different levels (micro-meso-macro) in four different settings. WP3 will study the existing RJ models and their potential application and relevance to conflicts in an intercultural context and possible implications for European policies.

Four more practice-oriented WPs will apply action research in different settings. WP4: Dealing with everyday conflicts at the micro-level between local residents and residents with migrant backgrounds in public/social housing (Vienna); WP5: Dealing with meso-level conflicts in a small town with tensions between Roma and non-Roma inhabitants (Hungary); WP6: Dealing with interethnic conflicts at meso- and macro-level (Serbia); and WP7: Dealing with civil conflicts at meso- and macro-level (Northern Ireland).

WP 8, 9 and 10 deal respectively with comparative research, dissemination of the results, and the management of the whole project.

Expected results

At the end of the project, innovative and exemplary RJ based models and procedures of conflict resolution will be available to statutory and non-statutory agencies which are confronted daily with problems of intercultural/interethnic conflicts throughout Europe. The project will demonstrate in a very concrete and visible way how alternative understandings of security and justice issues in democratic societies can be constructed through participatory processes with citizens.

PARTNERS

Katholieke Universiteit Leuven (KU Leuven)
Institute for the Sociology of Law and Criminology (IRKS)
European Forum for Restorative Justice (EFRJ)
Foresee Research Group (Foresee)
Norwegian Social Research (NOVA)
Victimology Society of Serbia (VDS)
University of Ulster (UU)

COUNTRY

Belgium
Austria
Belgium
Hungary
Norway
Serbia
Northern Ireland

ANVIL / Analysis of Civil Security Systems in Europe

© Larissa Belova - iStock

Information

Grant Agreement N°
284678
Total Cost
€2,202,702.60
EU Contribution
€2,009,228.00
Starting Date
01/03/2012
Duration
24 months

Coordinator

RESEARCH MANAGEMENT AS
Fortunalia 14
7057 Jonsvatnet, Norway
Contact
James P. Rydock
Tel: +47 7391 9307
Mobile: +47 9590 7562
Fax: +47 7391 8200
E-mail:
jrydock@researchmgt.com
Website:
www.anvil-project.net

Project objectives

The ANVIL project has six main objectives:

» To pinpoint essential similarities and differences between civil security systems across Europe, through mapping and comparing, especially with regard to relevant cultural phenomena and legal determinations;

» To study a representative number of security regional architectures in a comparative analysis regarding the sharing of responsibilities between public and private bodies and the role that citizens play in regional security architectures;

» To determine whether these systems are efficient and effective in protecting their citizens (i.e. to determine what works and what doesn't work in existing civil security systems);

» To provide advice about what changes or modifications could result in improvements to the security situation in regions or countries where this is desired by EU policymakers;

» To ensure that the project gives EU-added value to policy stakeholders;

» To link to future research needs where possible.

Description of the work

To reach these objectives, ANVIL has formulated three sub-strategies (encompassing the first five of in all seven work packages) for each project pillar: design, mapping and analysis, each of which is informed by policy stakeholders. Each pillar is essential to the outcome of the project.

» *WP1: Clever design*

The strategy is to organize a focused and intense design phase at the start. Existing literature will be used to formulate a framework for design, which will be translated into a "mapping manual". This will involve experts with different backgrounds (civil security, public administration, crisis management) to make sure the proposed mapping method is feasible in all selected regions;

» *WPs 2 and 3: Accurate and efficient mapping*

The strategy will be to identify what the best sources of existing data are and how we can access these. ANVIL will make use of our extended network (of both practitioners and academics) to identify these data sources. In addition, it is important that all partners collect data in the same way to ensure comparability (which is necessary for the analytical phase). Part of this strategy is to organize several meetings (in person and using video networking) to discuss and compare data collection processes, and jointly devise solutions for emerging data-related problems;

» *WPs 4 and 5: EU-focused analysis, dissemination and impact*

ANVIL will draw on previous research into the growing role of the EU and the existing constraints on developing EU crisis and disaster management capacities. This will provide a clear overview of the needs at the EU level. In addition, ANVIL will create a policy stakeholder group in WP5 to inform and provide feedback to our work, and who can ultimately validate our findings and function as an additional avenue for dissemination of ANVIL results;

» *Finally, WP6 is for overall dissemination, both during and after the project, and WP7 is for project management.*

Expected results

The project will develop consensus definitions of effectiveness and efficiency (in consultation with our end-user policy stakeholder advisors) and then apply them to the different country and regional security systems looked at in the project. Additionally, ANVIL will provide specific advice, based on those objective indicators and analysis, about what changes or modifications could result in improvements to the security situation in certain regions or countries where this might be desired by EU policymakers.

PARTNERS	COUNTRY
Research Management AS (Resman)	Norway
Universiteit Utrecht (Utrecht)	Netherlands
Ideella Foreningar Utrikespolitiskainstitutet, Informationsavd (UI)	Sweden
University of Essex (UEssex)	United Kingdom
Institut za Medunarodne Odnose (IMO)	Croatia
Hellenberg Oy (HI)	Finland
Istituto Affari Internazionali (I.A.I.)	Italy
Institut fur Friedenforschung und Sicherhetspolitik an der Universitat Hamburg (IFSH)	Germany
Försvarshögskolan, Swedish National Defence College (SNDC)	Sweden
Univeristet u Beogradu, Fakultet Bezbednosti (FB)	Serbia
Fondation pour la Recherche Strategique (FRS)	France
Uniwersytet im. Adama Mickiewicza w Poznaniu (AMU)	Poland

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

© Louise Gagnon - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218324
Total Cost
€2,705,344.54
EU Contribution
€2,093,808
Starting Date
01/05/2008
End Date
31/12/2011

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

Project objectives

Floods, fires, earthquakes or terrorist events in Europe raise important questions about human behaviour in crisis situations. Does culture play a role in how people respond to these events? More important: could a better understanding of cultural responses help define better emergency communication and evacuation procedures?

That was the goal of BeSeCu: to investigate cross-cultural and ethnic differences in human behaviour during crisis situations to produce tailor-made security-related communications, instructions and procedures. Its field work involved 1130 survivors and 3011 first responders.

Focused on eight European countries, BeSeCu carried out:

» video-tape analysis and the simulation of real-time evacuation scenarios;

» assessment of first responder roles and how communities were affected;

» standardized evaluation of survivors' cognitive, behavioural and emotional response to fires, terrorist attacks, floods or earthquakes.

Results

One of BeSeCu's discoveries was that it is possible to cross-culturally assess different types of incidents using a set of standard psychological tools. The project also discovered that different crisis situations incite different psychological impacts, with fires and building collapses producing the highest post-traumatic stress symptoms and floods the lowest.

Survivors with high post-traumatic stress levels reported significantly higher risk perception, levels of dissociation, panic and physiological reactions. They also had less time to inform themselves about the situation or to prepare for evacuation. As a result, they acted "automatically" or instinctively during the crisis. However, all survivors reported a common impulse toward supportive social behaviour such as helping other victims, sharing food and water, etc.

Among other findings, BeSeCu's research:

» produced a set of scientifically sound and cross-culturally validated instruments ("BeSeCu-S") to assess human behaviour in security-relevant crisis situations across cultures of survivors of disasters;

» extracted original data from 300 firefighters per country regarding their professional experience in crisis situations and culturally-relevant concepts of emergency operations, leading to new evidence about non-verbal communication by first responders;

» confirmed that information about the crisis itself is critical for occupants to response appropriately;

» developed two comprehensive evacuation model validation data sets from Turkish and Polish evacuation trials;

» confirmed that while behaviour and cognitions differ across cultures, common indices were identified regarding prevention, knowledge and safety culture habits.

BeSeCu's work will inform future R&D efforts focused on improving communication and emergency procedures regarding the links between culture and evacuation behaviour.

© Besecu

PARTNERS	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
Alma Mater Studiorum - Università di Bologna (UNIBO)	Italy

BESECURE / Best practice Enhancers for Security in Urban Regions

© TNO

Information

Grant Agreement N°
285222
Total Cost
€4,321,420.40
EU Contribution
€3,468,092.00
Starting Date
01/04/2012
Duration
36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK
TNO Behavioural
and Societal Sciences
Schoemakerstraat 97
PO Box 6060
2600 JA Delft,
The Netherlands
Contact
Heather Griffioen-Young
Tel: +31 8886 65931
Mobile: +31 6224 61065
Fax: +31 3463 53977
E-mail:
heather.griffioen@tno.nl
Website:
www.besecure-project.eu

Project objectives

Urban security is a complex challenge to modern urban environments. Many factors influence urban security, from the physical layout to the social and economic makeup of urban zones, from the national landscape to the daily practices of local public services. Europe has seen rapid expansion of its urban environments, and the rise of new types of communities due to migration, economic tensions and social developments. Unfortunately, this has also resulted in recent instances of urban unrest and failing urban regeneration plans. These developments demand a better understanding of urban security throughout Europe, and a more sensible policy development to create safer urban environments.

The BESECURE project aims to contribute to this challenge through comparative exploration of urban security in Europe, and providing policy makers with shared knowledge and informative policy support tools.

Description of the work

Recent instances of urban unrest have once again shown that seemingly small events can trigger a sudden escalation of unrest in neighbourhoods that have been under social tension for a prolonged period of time. In order to prevent such escalations, policy makers should understand the interdependency of factors that affect the urban area in question, and base their policies on that comprehension. However, in reality, most decisions are made on the basis of local, long-standing best practices. Given the universal importance of urban security, it is vital to share knowledge and practices among stakeholders throughout Europe, and to jointly work on a better common understanding of urban security.

The project 'Best practice Enhancers for Security in Urban Regions' (BESECURE) will work towards a better understanding of urban security through examination of different European urban areas. In each area, the BESECURE project will interact with local policy makers and stakeholders to learn local best practices on urban security, and on which basis they are made. This will include an appreciation of the data and background information available to policy makers, and a characterisation of the area on aspects relevant to urban security, such as social and cultural makeup of the target area, the economic state, crime rates and the public perception of security. By comparing the outcomes of the case studies, the BESECURE project will gain a comprehensive understanding of the underlying factors that impact the effectiveness of urban security policies. The knowledge and data gathered throughout the project will be used to devise tools that can alert policy makers to security issues in their target area and help them comprehend the effectiveness of their interventions.

The BESECURE project will work with the following urban regions: Belfast (UK), The Hague (NL), Freiburg (GER), London Tower Hamlets (UK), London Lewisham (UK), Naples (IT), Reggio di Calabria (IT), Poznan (PL).

Expected results

The BESECURE project will a) collect and share best practices in use throughout Europe, b) provide visualisation and assessment tools, driven by locally available data, and c) guidelines that will help local policy makers to assess the impact of their practices using the BESECURE tools and accompanying knowledge on the urban security landscape.

Together, these results provide a valuable evidence-base to policy makers, and give them new means to improve their urban security decision making.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
University of Ulster (UU)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)	Germany
Albert-Ludwigs-Universität Freiburg (ALU)	Germany
ITTI Sp.z.o.o. (ITTI)	Poland
The Stephen Lawrence Charitable Trust (SLCT)	United Kingdom
Downey Hynes Limited (DHP)	Ireland
JVM Limited (JVM)	United Kingdom
Crabbe Consulting Ltd. (CCLD)	United Kingdom
Consiglio Nazionale delle Ricerche (CNR)	Italy
Università degli Studi Mediterranea di Reggio Calabria (UMRC)	Italy
Experian Nederland BV (EXP)	The Netherlands
Stichting Dr. Hilda Verwey-Jonker Instituut (VJI)	The Netherlands
Institute for Housing and Urban Development Studies B.V. (EUR)	The Netherlands

CAST / Comparative Assessment of Security-Centered Training Curricula for First Responders on Disaster Management in the EU

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218070
Total Cost
€2,719,068.55
EU Contribution
€1,974,620
Starting Date
01/07/2009
End Date
30/06/2011

Coordinator

UNIVERSITAT SALZBURG
Office of the Rectorate
Research Support Unit
Kapitelgasse 4-6
A-5020 Salzburg
Austria
Contact
Prof. Friedrich Steinhäusler
Tel: +43 (0) 662 8044 5700
Mobile: +43-680-123 7158
Fax: +43-662-8040 150
E-mail: Friedrich.steinhaeusler@sbg.ac.at
Website:
www.research.sbg.ac.at/cast

Project objectives

The CAST project aimed to address the future needs of EU first responders (FR) from across the 27 Member State for handling a disaster scenario that exceeds in severity any existing training assumption – i.e., a catastrophic terrorist incident or an extremely large-scale "once in a life-time" natural or man-made disaster.

The project sought to identify and categorise a range of unusually extreme disaster scenarios of natural, man-made or terrorist origins. It then aimed to map and evaluate existing training and equipment preparation, and to produce a standardised modular training curriculum to prepare FR staff for these threats. Finally, it tried to streamline and standardise current cross-border preparation in these areas, to avoid pan-European duplications of effort.

Results

This project's deliverables included a range of new research in the field of disaster preparedness and training.

For identifying potential threat scenarios, the consortia created DERMI – the Database on Emergency Response Major Incidents. Containing 110 real-life incidents from across Europe, Russia and the US, DERMI provided a comprehensive catalogue of disaster scenarios to support the project's analysis.

A comprehensive survey of existing training programmes for disaster management was also conducted. Featuring 80 responses from across 25 EU Member States, covering themes such as the division of responsibility during a terrorist attack and procedures for the use of protective equipment.

Utilizing the surveys and reports, CAST then formulated a series of "best practice" procedural guides to form the basis of common training curricula for FR staff.

Low probability-high consequence threat scenarios that were explored included the wide area synchronised use of improvised explosive devices, large-scale chemical, biological or radiological releases in urban environments and chemical fires. These were then compared to existing equipment and training procedures to evaluate overall preparedness.

The recommendations and new procedural priorities suggested include:

- making the DERMI database available to all stakeholders;
- preplanning risk assessment in industrial facilities;
- focusing on control room design, structure, future development and management;
- enhancing communication technologies;
- developing new support technologies for CBRNE detection, mobile labs, drone surveillance and protective equipment;
- basing preparation for future large scale accidents based on lessons-learnt from disasters in the 21st century.

PARTNERS	COUNTRY
Universität Salzburg (PLUS)	Austria
DSTS-Advisers to Executives (DSTS)	Austria
Fire Service Academy Hamburg (FSAH)	Germany
Research Institute of Red Cross (FRK)	Austria
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT)	Germany
BMLVS / Heereslogistikschule (HLogS)	Austria
International Security Competence Center (ISCC)	Austria
University of Defense Brno (UDB)	Czech Republic
Corvinus University Budapest (VGT)	Hungary
SAAB Training Systems AB (SAAB)	Sweden
Swedish Counter Terrorist Police (SCTU)	Sweden
Diamond Aircraft Industries (DAI)	Austria
Tecnatom (TEC)	Spain
Sigmund Freud Privatuniversität Wien (SFU)	Austria
Police Service of Northern Ireland (PSNI)	United Kingdom

COMPOSITE / Comparative Police Studies in the EU

© Hans van Rhoon – Erasmus University Rotterdam

Information

Grant Agreement N°
241918
Total Cost
€8,904,352.73
EU Contribution
€6,623,303
Starting Date
01/08/2010
Duration
48 months

Coordinator

ERASMUS UNIVERSITY ROTTERDAM
Rotterdam School of Management
Postbus 1738
3000 DR, Rotterdam
The Netherlands
Contact
Gabriele Jacobs
Tel: +31(0) 10 4082061
Mobile: +31(0) 6 57559341
Fax: +31(0) 10 4089015
E-mail: gjacobs@rsm.nl
Website:
www.composite-project.eu

Project objectives

Police forces all over Europe are faced with major challenges: new types of crime, open borders, new technologies, the threat of terrorism and tighter financial resources are but a few of the changes in European societies that affect the police. Many police forces react by changing their administrative structure, merging forces and modernizing tools and processes. Some of these changes reach their goals, but many fail or face serious problems along the way.

Within this context, the COMPOSITE project brings together a network of European academic and police institutions, to investigate how organizational and cultural factors facilitate or hinder successful change implementation in European policing.

In doing so, the COMPOSITE project aims to contribute to improvements in the planning and execution of change initiatives in the police, showing how these projects can be better aligned with the cultural and societal context per country, as well as how negative processes can be mitigated. In this way COMPOSITE seeks to enhance police capability and performance, both within individual police forces and across European joint operations.

Description of the work

The COMPOSITE project investigates change management practices in the police across 10 European countries. Based around 11 interconnecting work-packages, COMPOSITE seeks to identify the key triggers of change as well as the determinants of change processes and outcomes.

The project consists of two phases. In the first phase, work-packages investigate the *content* of current change programs in European policing, by analyzing the police's external challenges and identifying the internal resources and capabilities that serve to counter such threats. Other work packages in this phase research knowledge sharing and technology trends, providing insights into the organizational structures that promote change initiatives. The second phase of the research project focuses on change *processes* and on understanding the role of specific organizational features, national and organizational culture, identity, and leadership in the management of change.

The goal of COMPOSITE is not restricted to the extension of scientific knowledge and theory building. The project also aims to have strong practical outcomes, bringing about concrete improvements in the conception, planning, organization and implementation of change processes in European police forces. Thus COMPOSITE includes work packages focusing on dissemination, training and consultancy in order to reach relevant police communities and the general public alike. This dissemination process is further enhanced by the COMPOSITE photo project which runs alongside the main project, enriching the research process and facilitating the dissemination of results.

Expected results

The COMPOSITE project aims to provide a richer understanding of the key processes involved in police organizational change, as well as a range of practical tools and training solutions for police agencies, including:

» A comparative strategic analysis of strengths, weaknesses, opportunities and threats for police organizations in 10 European countries;

» Analysis of the planning and execution of change processes and best practices to meet current and future challenges;

» An annual European Police Monitor tracking how police forces across Europe are developing and improving.

PARTNERS	COUNTRY
Erasmus Universiteit Rotterdam	The Netherlands
University of Utrecht	The Netherlands
Police Academy, Apeldoorn	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Police Academy, Brandenburg	Germany
University of Durham	United Kingdom
Sheffield University	United Kingdom
University of Antwerp	Belgium
CNRS, Paris	France
Capgemini Telecom Media defence	France
University St. Kliment Ohridski, Skopje	Republic of Macedonia
Masaryk University, Brno	Czech Republic
Formit, Rome	Italy
Babes-Bolyai University, Cluj	Romania
Esade Business School, Barcelona	Spain

COREPOL / Conflict Resolution, Mediation and Restorative Justice and the Policing of Ethnic Minorities in Germany, Austria, and Hungary

© Merijn van der Vliet - iStockphoto

Information

Grant Agreement N°
285166
Total Cost
€1,775,192
EU Contribution
€1,429,681
Starting Date
01/01/2012
Duration
36 months

Coordinator

GERMAN POLICE UNIVERSITY
Police Science Department
Zum Roten Berge 18-24
D-48165 Münster, Germany
Contact
Professor Joachim Kersten
Tel: +49 2501 806295
Mobile: +49 172 260 3860
Fax: +49 2501 806 226
E-mail:
Joachim.Kersten@dhpol.de
Website: www.corepol.eu

Project objectives

The proposed research will use a comparative design (Germany, Austria, Hungary) to establish whether better police - minority relations can be achieved through means of a Restorative Justice (RJ) approach.

The main objective of the COREPOL project will be:

» To provide a basis for coordinated research activities in the area of police-minority relations using a comparative method of data analysis; the findings will further police science research in this crucial area of peace building as part of a democratic process within European societies;

» To address the practical issue of effective dissemination of research findings to improve police-minority interaction making use of the realm of police tertiary education and in-service staff training but also involving other agencies including NGOs;

» To serve as a principal network for a practice oriented dissemination of RJ strategies and peace building in the conflict zone of police and minorities. In the area of police education, this concerns CEPOL course curricula (e.g. TOPSCOP) and course material and curricula for similar influential target groups, and also civil and public sector agencies.

Description of the work

The extent and cultural particularities of RJ programs and their affiliation to the criminal justice system will be ascertained. Then, specific minority populations (Turks in Germany, Roma in Hungary, Africans in Austria) will be examined in regard to the country's security context. The involvement of police in RJ programs for minority populations will be explored. Finally, the proposed research will exemplify the scope of RJ approaches for the improvement of police-minority communication and interaction. Based on the legality principle and on an inquisitorial civil law tradition of policing and criminal justice, the partner countries' legal and policing systems differ substantially from the Anglo-American-Australian hemisphere of restorative justice.

Expected results

It is one of the objectives of the proposed research to spread basic knowledge about the concept of RJ, its practical implementation, its varieties across the legal cultures, and its impact on different security contexts, the policing in general, and the policing of minorities in particular: RJ's potential for handling conflicts and peace building within democratic societies. The findings will have a wider impact on the Central and Eastern EU situation. The research will include open questions of gender, age and cultural compatibility of RJ.

PARTNERS

German Police University (DHPOL)
Rendőrtiszti Főiskola (RTF)
Bundesministerium für Inneres (SIAK)
Verein für Rechts- und Kriminalsoziologie (IRKS)
European Research Services GmbH (ERS)

COUNTRY

Germany
Hungary
Austria
Austria
Germany

CPSI / Changing perceptions of security and interventions

© Zoe - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217881
Total Cost
€2,712,487
EU Contribution
€2,165,637
Starting Date
01/04/2008
End Date
31/03/2010

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK
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

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 were 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Totalförsvarets Forskningsinstitut (FOI)	Sweden
University of Kent (UniKent)	United Kingdom
Sogeti Nederland B.V. (Sogeti)	The Netherlands
Temis S.A. (Temis)	France
European Commission - Joint Research Centre (JRC)	Belgium
WWEDU World Wide Education GmbH (CESS)	Austria
Ministerie van Volksgezondheid, Welzijn en Sport (SCP)	The Netherlands
VLC Projects B.V. (VLC)	The Netherlands
Sigmund Freud Privatuniversitat Wien GmbH (SFPUW)	Austria

CRISCOMSCORE / Developing a crisis communication scorecard

© volant - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217889
Total Cost
€1,013,207
EU Contribution
€799,174
Starting Date
01/02/2008
End Date
30/04/2011

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
Website: http://www.crisis-communication.fi

Project objectives

The purpose of this project was to improve public and media crisis communications during natural or man-made security incidents, disasters and emergencies.

To meet this goal the project had four key objectives:

» identify critical factors for an effective media strategy before, during and after crisis situations;

» identify critical factors for communication with citizen groups before, during and after crisis situations;

» construct a scorecard for public authorities to measure and improve their readiness to communicate in crisis situations;

» stimulate implementation by hosting and encouraging the use of the Crisis Communication Scorecard and the Strategy Guides.

Results

CRISCOMSCORE's conclusions were based on extensive best practice studies, assessments of scientific literature, empirical research to clarify existing communications co-operation in end-user response networks and an overview of the current level of reception to such information in stressful situations. These were reported in published strategy guides and academic journals.

These findings then formed the basis for measurable performance indicators in the Crisis Communications Scorecard – an online auditing tool that can be accessed free of charge by all crisis management professionals at: http://www.crisiscommunication.fi/criscomscore/

The scorecard presents critical factors in the communication of public authorities with stakeholders such as citizens, news media, and other response organisations before, during and after emergencies. It separates its analytics into three separate categories, focused on steps which can be taken before, during and after a crisis. In each category, a range of table-top exercises, planning meetings and outcome studies are required to feed into the auditing process.

The final analysis gauges the effectiveness of an organization's communications strategy using a system inspired by business efficiency auditing techniques. It concentrates on key success factors and reveals strong and weak points in performance, thereby enabling the prioritization of resource allocation by participants.

As well as the published strategy guides and scorecard, the website platform hosts a range of advice and recommendations for improving crisis communications.

PARTNERS

University of Jyväskylä Yliopisto
Ben Gurion University of the Negev
University of Tartu
Norwegian University of Science and Technology
Emergency Services College Finland

COUNTRY

Finland
Israel
Estonia
Norway
Finland

DESSI / Decision Support on Security Investments

© Jesus Conde - istockphoto.com

Information

Grant Agreement N°
261718
Total Cost
€1,902,303
EU Contribution
€1,561,095
Starting Date
01/01/2011
Duration
30 months

Coordinator

DANISH BOARD OF TECHNOLOGY
Toldbodgade 12
DK-1253 Copenhagen
Denmark
Contact
Ida Leisner
Tel: +45 3345 5355
Mobile: +45 3345 5355
Fax: +45 3391 0509
E-mail: il@tekno.dk
Website: www.securitydecisions.org, www.tekno.dk

Project objectives

The DESSI project will develop a tool that will support decision-makers in situations, where different possible solutions for a perceived security-problem are available. It will enable a comparison and evaluation of different security investments and serve as a way to achieve transparency of the security decisions.

Description of the work

The post-9-11 era is still upon us. Investments in safeguarding the security of European citizens have increased dramatically. Often the security dimension overshadows other critical aspects of decisions, i.e. political, ethical, and social. This has led to a securitization of several areas of society, such as transport, public space, health care, etc. Decisions are seemingly immediate responses to specific security issues. They tend to be technology driven. There is an urgent need for a political framework that directs all processes that lead to decisions on security investment to be transparent and participatory, and that accounts for the context and multi-dimensionality of society.

Security investments are made to avoid known or perceived threats. Threats could be conventional crime, cyber-crime, inner security, international conflicts, environmental hazards, and mixed forms of these. It is important to first understand the nature of the threat and the consequences, probability and impact of the threat and who is affected by it.

Security investment includes a choice between different approaches to increasing security, and DESSI makes this choice explicit by describing and evaluating the security investment alongside its alternatives. In almost any security related decision-making, implicitly or explicitly a range of alternatives is considered. The DESSI tool will ensure this aspect is explicit. The alternatives are identified or developed in a participatory process, including experts and stakeholders, which are informed by the threat description.

Security investments are often highly controversial and disputed decisions. This is not only because of political differences between actors but mostly because the societal phenomena involved (threat perception, technology insight, belief in alternative investments, etc.) are differently distributed and valued among the actors. Accordingly, a rigorous investment assessment method needs to make use of a participatory approach, which ensures that a range of relevant actors is taken on board in the assessment procedure.

Expected results

The DESSI project will provide a decision support system to decision makers and users of security investments. The system will give insight into the pros and cons of specific security investments. It will contribute to a transparent and participatory decision making that accounts for the context and multi-dimensionality of society. It will be useful for public authorities, developers of security solutions, commercial enterprises and social organizations that can use the DESSI tool to make their own comprehensive assessment as an input to strategic discussions or public debate.

PARTNERS	COUNTRY
Teknologiraadet - Danish Board of Technology (DBT)	Denmark
Peace Research Institute, Oslo (PRIO)	Norway
Teknologiraadet – Norwegian Board of Technology (NBT)	Norway
Verein für sozialwissenschaftliche Forschung und Beratung e.V. (SWFB)	Germany
Austrian Academy of Sciences, Institute of Technology Assessment (ITA)	Austria

DETECTER / Detection technologies, ethics, human rights and terrorism

© V. Yakobchuk - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217862
Total Cost
€2,424,419
EU Contribution
€1,869,684
Starting Date
01/12/2008
End Date
31/01/2012

Coordinator

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

Project objectives

The overall objective of DETECTER was to identify appropriate human rights, legal and moral standards for detection technologies in counter-terrorism. This assessment took into account the effectiveness of these technologies as judged by law enforcement bodies responsible for counter-terrorism, and other relevant authorities.

DETECTER aimed to do this in three ways:

» by surveying current and foreseeable applications of detection technologies in counter-terrorism;

» by conducting legal and philosophical research into the implications of human rights and ethics for counter-terrorism, and the use in counter-terrorism of technologies for the surveillance, identification or tracking of people and places; and

» by engaging directly and continuously with developers and users of detection technologies.

Results

DETECTER conducted a comprehensive review of the latest developments in detection technologies, resulting in five technology review reports, a series of day-long meetings with technology developers and users, and focus-groups with counter-terrorism professionals. The feedback and analysis of these groups will be released in academic publications.

A further series of research papers examined the ethical norms of counter-terrorism, including the extent of intrusion that can be justified for investigating terrorist threats and the moral hazards of profiling as a counter-terrorism tool. One paper on the ethics of special investigative techniques has already been published and one proposing a novel theory of privacy is in the process of being published, both in academic journals. Another study, focused on border security ethics and the rights of refugees, will also be released via academic publication.

Yet another of DETECTER's studies examined permissible limitations to the human right of privacy and recommended six universal safeguards that should be adopted to avoid abuses of power when undertaking surveillance. These include categories of offence liable for surveillance investigation, limitations on data dissemination and storage, and guarantees of due process.

Other work packages focused on data mining and electronic surveillance of internet activity. New insights were gained by assessing relevant practices in EU Member States and comparing them against US case studies. The findings fed into a series of research meetings on the judicial implications of such technology in counter-terrorism activities, including the need for a regular review of practices by national courts and the UN Human Rights Committee.

Many of these reports, including multi-media presentations and digestible summaries of key research findings, are available for public review and discussion on the DETECTER project website - http://www.detecter.bham.ac.uk/index.html

PARTNERS

University of Birmingham
Åbo Akademi University
University of Nottingham
University of Zurich
University of Oslo, Centre for Human Rights
Raoul Wallenberg Institute of Human Rights and Humanitarian Law
Danish Institute for Human Rights
European University Institute

COUNTRY

United Kingdom
Finland
United Kingdom
Switzerland
Norway
Sweden
Denmark
Italy

ETTIS / European security trends and threats in society

© alexander kirch - istockphoto.com

Information

Grant Agreement N°
285593
Total Cost
€2,823,373.40
EU Contribution
€2,285,586.13
Starting Date
01/01/2012
Duration
36 months

Coordinator

PEACE RESEARCH INSTITUTE OSLO
Security Dimensions Department
Hausmannsgate 7
PO Box 9229 Grønland
NO-0134 Oslo
0186 – Oslo – Norway
Contact
J. Peter Burgess
Tel: +47 22 54 77 38
Mobile: +47 909 23 949
Fax: +47 22 54 77 01
E-mail: peter@prio.no
Website: www.ettis-project.eu

Project objectives

The main goal of the project is to provide the means to establish a sustainable process of anticipating emerging threats to society and to societal security, and to translate them into research priorities. In the identification of research priorities, particular emphasis will be put on the role of European policy to support the realisation of these collective priorities.

The ETTIS project will meet these objectives through the following substantive and methodological sub-objectives. It will:

» Carry out an identification, integration and scenario-based assessment of:

- possible future **threats** resulting from trends, trend breaks and weak signals in technology and society;
- security-related **needs** of first responders, policy-makers and society at large;
- research-based **security opportunities** (using portfolio analysis, robust and adaptive strategies of priority-setting, new intelligence tools);
- comprehensive analysis of results and approaches of completed, ongoing and – to the extent possible - planned security research projects.

» Systematically derive a portfolio of **research priorities** that is geared towards the needs of user organisations, and rationales for policy intervention and the respective roles of European and national research and innovation policy;

» Develop a **methodological approach** for threat- and needs-based identification of research priorities, and generalize it as part of a continuous monitoring and assessment process and test its applicability with stakeholder organisations;

» Help increase the awareness of and attention to new insights generated by research among **first responders, policy-makers and industrial strategists**, as well as in wider **societal debates about civil security**. This includes the identification of barriers and limitations to the uptake of research results;

» Assess the relevance and success of the research.

The approach to be developed in ETTIS aims to leave an imprint on the way future threats are to be dealt with in the future.

Description of the work

The underlying strategy of the ETTIS work plan has three main approaches:

» It takes a broad and integrated approach to security that considers shifts in human/societal systems, reflecting the approach increasingly evident in the security strategies of more Member States and the EU;

» It seeks to adapt available research tools and results to better understand emerging threats and needs;

» It adopts an adaptive planning paradigm that addresses the security challenges in the dynamic, uncertain and complex security environment that our societies face, both in concept and in practice.

The project's work plan also includes various dissemination activities as well as an important task devoted to identifying individual stakeholders, creating a taxonomy of stakeholders and identifying their interests, needs and drivers. This task, carried out early on, will provide the basis for engaging stakeholders by means of interviews, focus groups, workshops and other means throughout the project and will ensure that the consortium's analyses, findings and recommendations are based on stakeholder reality.

Expected results

The work undertaken as part of the ETTIS project will make a high quality contribution to the impacts expected not only of this call, but also the security programme more generally. Firstly, the research undertaken in WP1 will provide a firm platform from which to bring forward a comprehensive understanding of 'security' that will inform later work packages as well as encourage a shared understanding of security in conversation with other stakeholders, such as other project partners, industry representatives, user organisations and policy makers. The review of other security projects undertaken in WP2 will specifically integrate the results of various FP 7 security research projects. These results will be fed into WPs 3-6, which will design and promulgate a series of tested methodologies and tools, useful for a range of categories of stakeholder. These will improve the situation awareness of administrations, end users and the population by assisting them in continually identifying and evaluating emerging trends and threats. Research undertaken in this project will also assist policy makers in maintaining an up-to-date security research agenda through evaluating and testing methodologies for identifying user needs and gaps created between threats and needs in the development of new technology. The use of participatory methods will ensure that these methodologies and tools are useful to different categories of stakeholder, as they will be evaluated in workshops, user reflection groups and project events. Creating a specific strategy for implementing a broad range of dissemination activities in WP7 will also increase the awareness of a range of categories of stakeholder about not only our project's research results, but also the results of other FP 7 security projects that may have relevance for those stakeholders. A targeted but wide dissemination strategy will also publicise the needs of policy makers and end-users, as well as the opportunities presented by new or emerging technological innovations and research priorities.

PARTNERS	COUNTRY
Peace Research Institute Oslo (PRIO)	Norway
Totalförsvarets Forskningsinstitut (FOI)	Sweden
DEN HAAG CENTRUM VOOR STRATEGISCHE STUDIES (HCSS)	Netherlands
TRILATERAL RESEARCH & CONSULTING LLP (TRI)	United Kingdom
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ISI-INT)	Germany
CENTRE FOR IRISH AND EUROPEAN SECURITY (CIES)	Ireland
AUSTRIAN INSTITUTE OF TECHNOLOGY GmbH (AIT)	Austria
Morpho (MPH)	France
MAGEN DAVID ADOM (MDA)	Israel
Police Service of Northern Ireland (PSNI)	United Kingdom

EUSECON / A new agenda for european security economics

Information

Grant Agreement N°
218105
Total Cost
€3,009,542.74
EU Contribution
€2,357,188
Starting Date
01/03/2008
End Date
30/04/2012

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

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 intranational 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	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
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
Athens University of Economics and Business - Research Center (AUEB-RC)	Greece

FESTOS / Foresight of Evolving Security Threats Posed by Emerging Technologies

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217993
Total Cost
€971,799.62
EU Contribution
€824,552.7
Starting Date
01/03/2009
End Date
31/12/2011

Coordinator

INTERDISCIPLINARY CENTER FOR TECHNOLOGY ANALYSIS AND FORECASTING
Tel-Aviv University
69978 RAMAT AVIV, TEL AVIV
Israel
Contact
Yair Sharan
Tel: +97236407574
Mobile: +972544381600
Fax: +97236410193
E-mail: sharan@post.tau.ac.il
Website: www.festos.org

Project objectives

Analysing technological and societal developments over the next 20 years and beyond, this foresight study aimed to identify and assess security threats that could stem from recently developed or upcoming science and technology (S&T) breakthroughs.

FESTOS' overall strategy was based on three pillars of research:

» horizon scanning: identification of potentially threatening new technologies and field of techno-science research;

» evolving threats: assessment of emerging threats, construction of related threat scenarios, their impact on society and development of early-warning indicators;

» pathways towards solutions: developing preparedness measures and policy guidelines.

Results

FESTOS mainly focused its research on the fields of nanotechnology, biotechnology, robotics, new materials and information and communications technology (ICT). It also examined crime and terrorism as potential threats, but excluded industrial accidents or other potential disasters.

The project carried out a comprehensive literature scan of current and upcoming emerging technology research. This resulted in a report that categorised and provided an initial threat assessment of 80 potential technologies of interest. Some 288 experts participated in a survey where they were asked to assess the risk potential of leading future technologies, and to estimate a timeframe for each threat's realisation.

The result is a database of potentially abusable technologies, including a potential timeframe for their entry into the market. Potential misuse falls into three categories, namely the:

» the disruption of certain technological applications for malicious purposes;

» increased access to technologies previously confined to the military, specialist industry or unique heavily funded laboratories;

» surprising malicious use of new technologies developed for completely different, beneficial purposes.

Each category of threats was divided into short, medium and long term timeframes of concern, with Category 3 ("surprising malicious uses") deemed as the high priority area since it can include a "wild card" exploitation of new technologies not previously associated with a security risk.

The potential wild card scenarios that were examined include a large-scale nano-technology out-break, swarms of robotic "cyber insects", the use of genetic engineering for personal blackmail and the creation of infectious viruses capable of altering human behaviour (eg. heightened aggression or depression).

By applying these assessments to different national contexts across the EU, the consortium came up with a series of policy recommendations and guidelines for national authorities and the EU on how to conduct their own risk assessments in these fields.

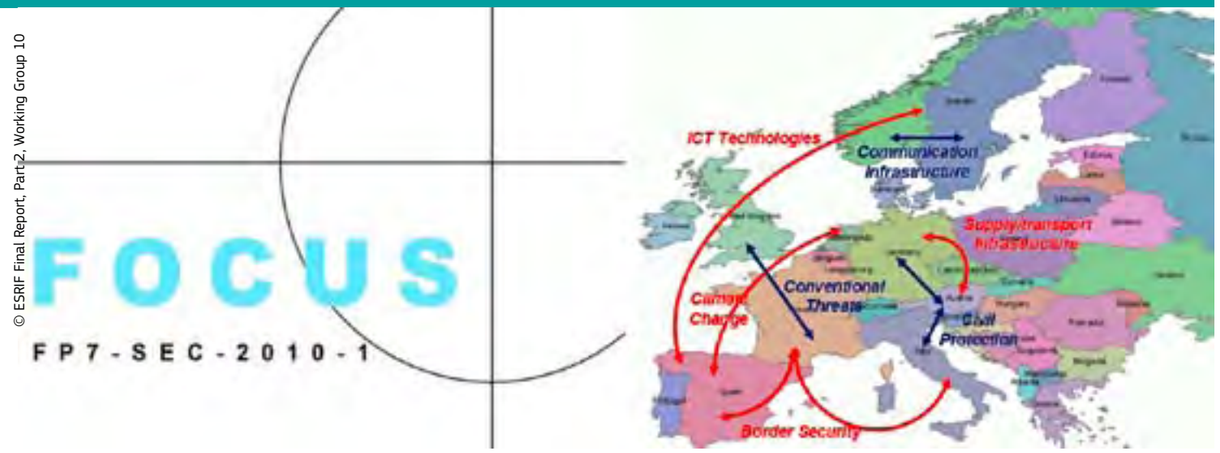
PARTNERS

Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF)
Turku School of Economics, Finland Futures Research Centre
Foundation for European Scientific Cooperation
EFP Consulting
Technical University of Berlin
Uniwersytet Lodzki

COUNTRY

Israel
Finland
Poland
United Kingdom
Germany
Poland

FOCUS / Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles



Information

Grant Agreement N°
261633
Total Cost
€4,372,012
EU Contribution
€3,407,075
Starting Date
01/04/2011
Duration
24 months

Coordinator

SIGMUND FREUD PRIVATUNIVERSITAT WIEN GMBH
CEUSS | Center for European Security Studies
Schnirchgasse 9a
1030 Vienna
Austria
Contact
Alexander Siedschlag
Tel: +43 (0) 1 798 62 90 50
Mobile:
+43 (0) 699 113 69 717
Fax:
+43 (0) 1 798 62 90 52
E-mail: siedschlag@european-security.info
Website:
http://www.focusproject.eu

Project objectives

FOCUS will help shape European security research to enable the EU to effectively respond to tomorrow's challenges stemming from the globalization of risks, threats and vulnerabilities.

FOCUS will concentrate on alternative future EU roles to prevent or respond to incidents situated on the "borderline" between the internal and external dimensions of the security affecting the Union and its citizens. It will do so by elaborating multiple scenarios, based on IT-supported foresight, in the form of alternative futures. These will be plausibility-probed versus mere threat scenarios.

The main contribution of FOCUS is to develop an effective long-term foresight and assessment tool at the EU level, populated with the analyses carried out by the project. Moreover, FOCUS will deliver tangible products (such as an IT platform) and contents (i.e., a roadmap) for planning research and deciding on priorities. These products are usable beyond the project.

Description of the work

FOCUS will design and apply an "embedded scenario" method of integration. This will delineate options for future tracks and broadened concepts of security research within broader scenarios that involve EU roles for responding to transversal challenges (whose causes are external but whose effects are internal to the EU). This will be performed along five big themes:

» different tracks regarding the comprehensive approach as followed by European institutions, Member States and international strategic actors – including links between the internal and external dimension of security;

» natural disasters and environment-related hazards, with an emphasis on comprehensive risk reduction, civil protection and reconstruction;

» critical infrastructure and supply chain protection, centred on preventing, mitigating and responding to exogenous threats that could have a significant impact on EU citizens;

» the EU as a global actor regarding the so-called "wider Petersberg Tasks", and building on EU and member state instruments and capability processes;

» the evolution of the EU's internal framework and prerequisites for delivering a comprehensive approach, including Lisbon treaty provisions and relevant strategies (e.g. for engagement with other international actors) as well as ethical acceptability and public acceptance.

The "embedded scenario" method and IT-based tools will be adjusted and sharpened as applied to these five thematic scenarios. Interrelations among themes and scenarios will be particularly addressed: FOCUS will investigate cross-cutting issues that constitute transversal key drivers/constraints. The project will explore interfaces and translation mechanisms by which exogenous threats – such as those stemming from global change – directly confront EU citizens, their perception and their actual state of security. It will also take into account the differential impact of external threats on national and European research programmes designed to enhance capabilities.

Expected results

FOCUS will deliver (a) an IT Platform with tools and infrastructure for designing, applying, evaluating and managing scenarios for research planning, all of which is (b) populated with scenarios and analyses; and, finally, (c) a roadmap with new tracks for security research.

In particular, FOCUS will identify and assess alternative sets of future tracks for security research in FP7 and subsequent programmes that will support the EU in adopting new roles in dealing with external threats, risks and vulnerabilities.

PARTNERS	COUNTRY
SIGMUND FREUD PRIVATUNIVERSITAT WIEN GMBH (SFU-CEUSS)	Austria
ATOS ORIGIN SOCIEDAD ANONIMA ESPAÑOLA (ATOS)	Spain
BOC ASSET MANAGEMENT GMBH (BOC)	Austria
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (CSDM)	Bulgaria
CROSS-BORDER RESEARCH ASSOCIATION (CBRA)	Switzerland
INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPAÑA SA (ISDEFE)	Spain
CESKE VYSOKE UCENI TECHNICKE V PRAZE (CVUT)	Czech Republic
SECEUR SPRL (SECEUR)	Belgium
UNIVERSITAET FUER WEITERBILDUNG KREMS (DUK)	Austria
UNIVERSITY OF HAIFA (U HAIFA)	Israel
UNIVERSITAET FUER BODENKULTUR WIEN (BOKU)	Austria
INSTITUTO NACIONAL DE TECNICA AEROESPACIAL (INTA)	Spain
CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)	Germany

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

© Cornelius - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218199
Total Cost
€942,202
EU Contribution
€942,202
Starting Date
01/02/2008
End Date
30/11/2009

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

Project objectives

FORESEC was a foresight project aimed at assessing the evolution of Europe's security landscape in the coming decade. Its goal was to identify likely upcoming security threats, and to categorise the potential added value in EU-level action for tackling such threats. Finally, the project sought to suggest research priorities to support these goals.

To fulfil this objective, FORESEC decided to create – or where it already existed strengthen – networks of experts from across various professions and backgrounds in European security.

Results

The main output of FORESEC was a series of specialist reports. These included 12 country reports on national security strategies, a global trends report, a concept paper on European security, a threat taxonomy assessment and a scenario development report.

These key publications can be found for public consumption at: www.foresec.eu

The development of an interactive web site for stakeholders and the professional networking undertaken during the projects workshops can also be seen to have contributed to the development of security expert groups at the EU level.

A particular focus of this research was on the potential added value of EU level cooperation in security. FORESEC research shows that the EU's combination of "effective multilateralism" – the benefits of international institution membership, resource and knowledge sharing – combined with the EU's natural comparative advantage in combining civilian, military and diplomatic spheres, are all positive contributions to Member State security policy. EU level policy also allows smaller states to benefit from capabilities and insights beyond their individual means.

Yet despite these advantages, FORESEC research – including six national research workshops – shows that a shared concept of security does not yet exist amongst Member States. An appreciation of national approaches is thus encouraged.

Looking forward, FORESEC recommends that future security research should shift from a state centric approach to one that acknowledges the comprehensive and citizen-centred strategies now advocated in most national security strategies.

PARTNERS

Crisis Management Initiative
Austrian Research Centres System Research
International Institute for Strategic Studies
Totalförsvarets Forskningsinstitut (FOI)
Centre for Liberal Studies
European Commission - Joint Research Centre (JRC)

COUNTRY

Finland
Austria
United Kingdom
Sweden
Bulgaria
Italy

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

© quayside - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218265
Total Cost
€2,422,082
EU Contribution
€1,890,248
Starting Date
01/04/2008
End Date
31/03/2011

Coordinator

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

Project objectives

This project set out to analyse the value assumptions and ethical consequences of the internal/external security continuum in Europe of trans-border security initiatives. Its goal was to better understanding the role of values in security measures and to frame recommendations for strengthening the coherence, effectiveness and justice of security policy in the EU.

The work of INEX project was designed around thematic and geopolitical research axes. The thematic axes explored four fields of knowledge relating to value-laden tensions that arise from internal/external security continuum:

- ethical consequences of the proliferation of security technologies;
- legal dilemmas linked to transnational security arrangements;
- ethical and value questions stemming from the shifting role of security professionals;
- consequences of the changing role of foreign security policy in an era when the distinction between external and internal borders grows less distinct.

Along the geopolitical axis, the project studied the aims and outcomes of the EU's Eastern European and Mediterranean neighbourhood policies.

Results

INEX's research concluded that ethical concerns and the value assumptions should play a central role in the formation of European security policy.

The study of internal and external security measures suggests the need for careful consideration of the ethical assumptions behind security technological, for new interpretations of conventional legal documents, for attention to the values informing the work of security professionals and the shifting forces of the foreign policy arena.

The project's results indicate that these new needs have consequences for the external policing policies of the EU in an age of rapid security sector reform. The ambitions of the EU's European Neighbourhood Policy and Mediterranean policies have been challenged by inadequate attention to the geopolitical, cultural, religious and economic dimensions of rapidly changing events.

The project's results suggest that security cannot be reduced to a single political approach, institutional orientation or sole dependence on scientific means. They indicate that reliance on security technologies as the default approach to security challenges is not only an inadequate solution to the threats European society faces, but can, at times, stand in the way of suitable solutions.

PARTNERS	COUNTRY
International Peace Research Institute	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

PACT / Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action


© PACT

Information

Grant Agreement N°
285635
Total Cost
€3,237,736.40
EU Contribution
€2,675,107.85
Starting Date
01/02/2012
Duration
36 months

Coordinator

VITAMIB SAS
Rue Colonel Dumont 26
38000 Grenoble, France
Contact
Xavier Fabre
Tel: + 33 4861 10185
Mobile: + 33 6768 42877
Fax: + 33 4765 18491
E-mail: xfabre@vitamib.com
Website: www.vitamib.com

Project objectives

PACT is a collaborative project, which aims:

» to assess existing knowledge about public perception of the tension between security and privacy and the role played by social trust and concern,

» to collect empirical evidence about the way in which European citizens perceive and assess in real life novel surveillance technologies,

» to analyze the main factors that affect public assessment of the security and privacy implications of given security technology.

On the basis of such an investigation, the project will develop and validate a prototype Decision Support System (DSS), which may help end users to evaluate pros and cons of specific security investments also on the basis of the societal perception of privacy and liberty.

Description of the work

The first year of the project is devoted to creating the baseline knowledge and designing a pan European survey on privacy and security; the second year is entirely devoted to carrying out and analysing the survey; the third year is devoted to developing a new Privacy Reference Framework for security technologies and the DSS.

WP1 explores the existing gaps in current approaches, available evidence, and modeling of public perception of privacy and security through a literature review from a number of domains, also taking into account deliverables of previous and current EC funded projects.

In *WP2*, the consortium designs and pilots the survey consisting of three real life scenarios - in which security technologies might affect privacy and fundamental rights - and background questions such as socio economic characteristics, perceptions of security and privacy as well as attitudinal and life style indicators.

In *WP3*, the consortium carries out the fieldwork by interviewing twenty-seven thousand individuals in the 27 EU countries. The fieldwork will be conducted via a self administered methodology using a combination of online methodologies and face to face approaches.

WP4 will focus on the analysis of the collected data using both descriptive and advanced quantitative techniques.

WP5 will exploit results from the previous WPs to develop a new conceptual Privacy Reference Framework for Security Technology (PRFST) covering levels of respect for privacy and liberty in different aspects of its descriptive scheme with illustrative descriptors scale.

WP6 will develop the PACT DSS, through a series of sessions among partners, with direct involvement of stakeholders.

WP7 is devoted to dissemination and the involvement of stakeholders.

Finally, *WP8* deals with project management and quality control.

Expected results

The PACT project is expected to provide a Decision Support System to decision makers giving them insight into the pros and cons of specific security investments taking into account a wider societal context. Furthermore, a Pan-European survey carried out in PACT will allow citizens, policy makers, scholars and other stakeholders to better grasp democratic questions of privacy, surveillance, and security and better understand the relationship between privacy and security.

PARTNERS	COUNTRY
VITAMIB SAS (VITAMIB)	France
ATOS SPAIN SA (ATOS)	Spain
CENTRE FOR IRISH AND EUROPEAN SECURITY LIMITED (CIES)	Ireland
MARKET & OPINION RESEARCH INTERNATIONAL LIMITED (IPSOS MORI)	United Kingdom
CENTER FOR SECURITY STUDIES (KEMEA)	Greece
MINISTRY OF PUBLIC SECURITY (MOPS/IP)	Israel
NATIONAL CENTER FOR SCIENTIFIC RESEARCH “DEMOKRITOS” (NCSR Demokritos)	Greece
RAND EUROPE CAMBRIDGE LTD (RAND)	United Kingdom
INSTITUTT FOR FREDSFORSKNING STIFTELSE (PRIO)	Norway
UPPSALA UNIVERSITET (UU)	Sweden
CENTRE FOR SCIENCE, SOCIETY AND CITIZENSHIP (CSSC)	Italy

PRISMS / The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making

© kyoshino - istockphoto.com

Information

Grant Agreement N°
285399
Total Cost
€3,561,935
EU Contribution
€2,985,744
Starting Date
01/02/2012
Duration
42 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48
76139 Karlsruhe, Germany
Contact
Dr. Michael Friedewald
Tel: +49 (0) 721 6809 146
Fax: +49 (0) 721 6809 315
E-mail: michael.friedewald@isi.fraunhofer.de
Website: http://www.prismsproject.eu

Project objectives

The PRISMS project will analyse the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It will examine how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance. PRISMS will determine the factors that affect public assessment of the security and privacy implications of a given security technology. The project will use these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Description of the work

The first phase of PRISMS begins with a multidimensional analysis of the relation between privacy and security from the different perspectives of technology, policy, media, criminology and law. These diverse perspectives offer an analytical background against which perceptions and attitudes of citizens can be studied. The consortium will determine the factors that affect public assessment of the security and privacy implications of a given security technology. Having analysed the conceptualisations of and interrelations between privacy and security, the consortium will test and validate its analysis in interviews, focus groups and workshops which will bring together various stakeholder groups (citizens, policy advisors, security people, societal organisations, criminologists, scientists).

The main outcome of the first project phase will be hypotheses about the relationship between privacy and security, trust and concern. These hypotheses will form the basis of a pan-European survey in the project's second phase. The survey will investigate the opinions, attitudes and behaviour of a representative sample of citizens on privacy and security. It will include 1,000 telephone interviews in each of the 27 Member States of the Union. This survey will allow us to identify the main driving factors that influence the forming of citizens' opinions on privacy and security and to make consistent comparisons between countries or regions in the EU.

In its third phase PRISMS will use these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives, taking into account a wide societal context. The decision support system will need to reconcile the various dimensions such that the results can be understood in terms of discriminating between options for security investments.

Expected results

- A better understanding of the iridescent terms "security" and "privacy" and their interrelationship;
- A model of how privacy and security attitudes of citizens are formed;
- A proposal for a participatory decision support process for an early assessment of emerging security technologies based on reconciling security, privacy and trust;
- Improving decision makers awareness of critical aspects of security technologies;
- Policy recommendations for ensuring human rights by design.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ISI)	Germany
Trilateral Research and Consulting LLP (Trilateral)	United Kingdom
Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (VUB-LSTS)	Belgium
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
The University of Edinburgh (UEdin)	United Kingdom
Eötvös Károly Public Policy Institute (EKINT)	Hungary
Zuyd University of Applied Sciences (Zuyd)	The Netherlands
Market & Opinion Research International Ltd. (Ipsos MORI)	United Kingdom

RECOBIA / Reduction of Cognitive Biases in Intelligence Analysis

© Yury Kuzmin - istockphoto

Information

Grant Agreement N°
285010
Total Cost
€4,294,081.40
EU Contribution
€3,215,454
Starting Date
01/02/2012
Duration
36 months

Coordinator

COMPAGNIE EUROPÉENNE D'INTELLIGENCE STRATÉGIQUE (CEIS)
European Office
Boulevard Charlemagne 42
1000 Brussels, Belgium
Contact
Frederik Schumann
Tel: +32 2 646 70 43
Mobile: +32 488 372 959
Fax: +32 2 646 70 22
E-mail: fschumann@ceis.eu
Website: www.recobia.eu

Project objectives

The aim of the RECOBIA project is to improve the quality of intelligence analysis by reducing the negative impact of cognitive biases upon intelligence analysis. To this end, we will make an assessment of cognitive biases and on how these biases affect the practice of intelligence.

Building on this initial assessment, best practices to reduce the negative impact of cognitive biases will be defined. Solutions are likely to be found in the following domains:

» Software tools;

» Training of analysts;

» Analytic techniques and methodologies;

» Organisational and operational processes.

Description of the work

The RECOBIA project is a three-year initiative intended to find solutions to reduce the negative impact of cognitive biases in intelligence analysis.

Building on an initial assessment, best practices to reduce the negative impact of cognitive biases will be defined. Solutions are likely to be found in the following domains:

» Software tools;

» Training of analysts;

» Analytic techniques and methodologies;

» Organisational and operational processes.

To this end, the project is structured into four key phases:

» *Step 1:* An audit and assessment of cognitive biases: the project will undertake an audit of the many biases that affect the process of intelligence. The objective here is to rigorously catalogue the cognitive pathologies that undermine the analytic process;

» *Step 2:* A review of the intelligence process: RECOBIA will conduct a full review of the intelligence process, from the identification of requirements to the dissemination and evaluation of intelligence products;

» *Step 3:* A mapping of cognitive biases to the intelligence process to identify how such biases might be reduced: so far, no attempt has ever been made to map the many biases that impact intelligence to specific phases of the intelligence process. RECOBIA will be the first attempt to do so. This will go as far as identifying the potential impacts of each bias, as well as identifying possible solutions (whether technical, methodological, operational or otherwise);

» *Step 4:* Formulation of a catalogue of solutions (requirements for software tools, draft of a curriculum for training, and proposals for organisational/methodological modifications).

Through the organisation of six workshops with end-users, the project will maintain a close dialogue with intelligence professionals. The network of the EUROSINT Forum, which is a pan-European not-for-profit association that maintains contact with over 400 intelligence professionals working in agencies and administrations across Member States and EU institutions, will facilitate the link with and involvement of the end-user community.

The results of the RECOBIA project will be a catalogue of solutions for end-users of how to reduce the negative impact of cognitive biases upon intelligence analysis.

Expected results

RECOBIA's value is both immediate and apparent. The project would result in a significant advance over the current "state of the art", as well as provide tangible benefits to those organisations and individuals engaged in intelligence or related work. Finally, it would go to improving: the practice of intelligence; the quality of its outputs; and the communication of risks and opportunities to decision makers across the EU.

PARTNERS	COUNTRY
Compagnie Européenne d'Intelligence Stratégique (CEIS)	France
Hawk Associates Limited (HAWK)	United Kingdom
Thales SA (THALES)	France
Atos Spain SA (ATOS)	Spain
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
ISEA Psy (ISEA)	France
EUROSINT Forum (EUROSINT)	Belgium
Zanasi Alessandro (ZANASI)	Italy
University Konstanz (UKON)	Germany
Technische Universitat Graz (TUG)	Austria

SAFE-COMMS / Counter-terrorism crisis communication

© Loren Rodgers - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218285
Total Cost
€1,397,232
EU Contribution
€1,088,244
Starting Date
01/04/2009
End Date
31/03/2011

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
Website:
http://faculty.biu.ac.il/~sshpiro

Project objectives

The goal of this project was to help public authorities in Europe better react to terror incidents by providing effective communication strategies for the aftermath of terror attacks.

Results

During the initial stages of the project, the SAFE-COMMS partners undertook a comprehensive review of literature already published on the topic. The review examined articles in the area of crisis communication and those focused on communication following a terrorist attack.

This provided an overview of the key terms and variables relevant to this area. The project also conducted stakeholder interviews with police, fire brigades, armed forces officers, emergency medical services personnel, government officials, journalists from both public and private TV stations, and spokespersons of major hospitals.

In the next stage of SAFE-COMMS' research, actual examples of terrorist incidents in Europe were selected for incorporation into the project's case-study phase. The case studies were chosen to reflect the full range of possible terrorist attacks.

Conclusions drawn by the project's consortium partners from their analysis argue that:

» there is a need for a coherent crisis management plan that includes clear strategies for communication with other emergency services;

» plans should be effectively and widely disseminated in preparation for an attack;

» it is important to develop strategies to protect victims from the media;

» time, space and support are needed for public authorities to assess and come to terms with traumatic incidents.

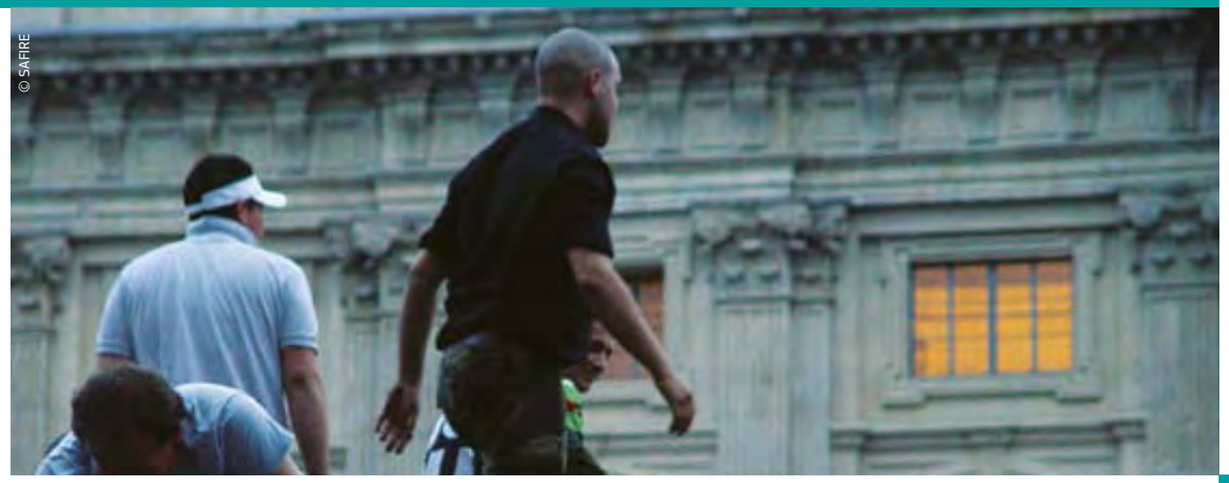
PARTNERS

Bar-Ilan University
A&B One GmbH
Research Institute for European and American Studies
University of Ulster
Universidad de Burgos
University of Rousse Angel Kunchev

COUNTRY

Israel
Germany
Greece
United Kingdom
Spain
Bulgaria

SAFIRE / Scientific approach to finding indicators and responses to radicalisation


© SAFIRE

Information

Grant Agreement N°
241744
Total Cost
€3,681,260
EU Contribution
€2,906,600.95
Starting Date
01/06/2010
Duration
42 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK
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

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. The project will develop intervention principles in close concert with the models and apply them in a longitudinal, empirical study. It 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, notably 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.

PARTNERS	COUNTRY
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Stichting Forum, Instituut voor Multiculturele Ontwikkeling (FORUM)	The Netherlands
International Security and Counter-Terrorism Academy (ISCA)	Israel
Rand Europe Cambridge Ltd (RAND)	United Kingdom
Stichting Hogeschool Utrecht (Hogeschool Utrecht)	The Netherlands
Bridge 129 Spa Safety and Security (Bridge)	Italy
Compagnie europeenne d'intelligence stratégique SA (CEIS)	France
Universidade de Coimbra (UC)	Portugal
Fondation pour la recherche stratégique (FRS)	France
Universiteit van Amsterdam (UvA)	The Netherlands

SAPIENT / Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies

© Sapient

Information

Grant Agreement N°
261698
Total Cost
€1,539,687
EU Contribution
€1,248,577
Starting Date
01/02/2011
Duration
36 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Systems and Innovation Research
Breslauer Straße 48
76139 Karlsruhe,
Germany
Contact
Michael Friedewald
Tel: +49 (0) 721 6809 146
Fax: +49 (0) 721 6809 315
E-mail: michael.friedewald@isi.fraunhofer.de
Website:
www.sapientproject.eu

Project objectives

SAPIENT aims to specify how and when smart surveillance should be used (or not) and its characteristics to be effective and scalable to rapidly adapt to changing situations. It will provide stakeholders with a set of criteria for data protection and integrity that can be used to verify that surveillance systems and the sharing of information respect the privacy of citizens. The project will develop and provide a privacy impact assessment methodology, which is tailor-made for surveillance projects and technology developments and, in so doing, the use of the methodology will provide means for limiting the collection and storage of unnecessary data. It will focus on the necessity and proportionality of data collection needs, in order to avoid undue threats to data protection and privacy. SAPIENT will pave the way towards an approach of surveillance where the respect of the privacy of the citizen will be central.

Description of the work

The SAPIENT project will define and characterize smart surveillance within technological, social, political, legal, and ethical contexts, bridging from current studies of state-of-the-art of surveillance to emerging technologies and related applications expected over the next decade.

The second step will begin the process of active stakeholder engagement within SAPIENT, through convening focus groups with participants representing various views and interests on different applications of smart surveillance.

Then the SAPIENT team will examine existing privacy impact assessment (PIA) methodologies and propose a methodology that is suitable for the assessment of state-of-the-art and emerging surveillance technologies and related applications.

The validation of the suggested PIA is done by three distinct field studies. These cases may focus upon technologies such as RFID, biometrics, or smart CCTV. A "lessons learned" evaluation will be completed at the conclusion of the case study test, and these will be used to revise the PIA methodology, resulting in the Surveillance Privacy Impact Assessment Manual.

Moreover a series of policy meetings will be held over the course of the project to present results of research. At the conclusion of the project, a final conference will be held to present the main findings and recommendations. It is expected to pave the way towards an approach of surveillance where the respect for privacy will be central.

Expected results

The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizens.

PARTNERS

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FhG)
Trilateral Research & Consulting LLP (Trilateral)
Centre for Science, Society and Citizenship (CSSC)
Vrije Universiteit Brussel, Research Group on Law Science Technology & Society (VUB-LSTS)
University of Lugano, Faculty of Informatics (USI)
King's College London, Department of War Studies (KCL)
Centre for European Policy Studies (CEPS)

COUNTRY

Germany
United Kingdom
Italy
Belgium
Switzerland
United Kingdom
Belgium

SECONOMICS / Socio-Economics meets Security

© Ulrich Mueller - istockphoto.com

Information

Grant Agreement N°
285223
Total Cost
€4,723,323.44
EU Contribution
€3,451,096.14
Starting Date
01/02/2012
Duration
36 months

Coordinator

UNIVERSITÀ DEGLI STUDI DI TRENTO
Department of Information Engineering
and Computer Science
Via Sommarive 14
38123 Povo, Trento, Italy
Contact
Fabio Massacci
Tel: +39-0461-282086
Mobile: +39-329-2105004
Fax: +39-0461-283987
E-mail:
Fabio.Massacci@unitn.it
Website: www.seconomics.eu

Project objectives

Policy makers are often in the unenviable position of having to make regulatory and investment decisions on security based on incomplete information about the risk structure, and unknown or unknowable preferences of their stakeholders. The presence of Knightian uncertainty (i.e., uncertainty of uncertainty and uncertainty of the outcomes in security problems) renders many conventional "rules of thumb", or "broad policy generalizations", unworkable.

SECONOMICS is a collaborative project on the socio-economics of security, with a specific focus on the interplay between information security and physical security, driven by three key cases studies in critical infrastructure protection: in international air transportation, in local transportation and in energy distribution. These sectors are all critical to the economic and social lives of EU member states. The scientific approach will integrate expertise into social, economic, system and risk modelling and will provide a basis for initial developments of decision-support methodologies and tools for policy makers.

Description of the work

The SECONOMICS project is primarily structured around three case studies that are designed to address the core themes of the call and can be applied to the majority of the missions that are outlined within the CORDIS Cooperation Security Theme. They cover:

» *WP1:* Airports and airport security;

» *WP2:* Critical Power Infrastructure;

» *WP3:* Regional and Urban Transport.

The initial task would be to identify the concrete issues in security missions for these case studies. Once the menu of security missions has been characterized, R&D work-packages (WP4, WP5, WP6), will then begin to characterize the threats and distillate socio-economic methodologies based on rigorous and well-developed methodologies from the social sciences, risk and operations research, and economics and systems models.

» *WP4* will identify the qualitative societal impact scenarios, from the future or emergent threat. Quantification of the social cost is made by contingent valuation;

» *WP5*'s role is in the identification of the outcome space and associated risk measures. In addition WP5 will analyse the threat environment and potential security measures and their effectiveness;

» *WP6* develops economic and systems models of the policy interactions with the architecture of the physical and ICT system under threat and develops an optimal set of policy tools and control instruments designed to optimally deal with the future or emergent threat, subject to social cost constraints;

» *WP7* will consolidate the results of the three case studies to cross-mission relevance results and will assist in consolidating the validation assessment between WP4, WP5 and WP6. Loosely speaking it will be "hand-booking" the results of the concrete case studies;

» *WP8* will provide the necessary computer-aided support to manage real data, by providing tools that map the research models either to collected or to simulated data (for instance backing out the policy parameters from structural models of economic risk and risk preferences);

» A specific WP (*WP9*) is devoted to the issue of dissemination and exploitation.

Expected results

The models developed are distilled into cross-mission policy toolkits that make it possible for decision makers to adapt the general socio-economic methodologies to their concrete problems.

© Seconomics

PARTNERS

UNIVERSITA' DEGLI STUDI DI TRENTO (UNITN)
DEEP BLUE SRL (DBL)
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
UNIVERSIDAD REY JUAN CARLOS (URJC)
THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN (UNIABDN)
FERROCARRIL METROPOLITA DE BARCELONA SA (TMB)
ATOS SPAIN SA (ATOS)
SECURENOK AS (SNOK)
INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC
PUBLIC RESEARCH INSTITUTION (ISAS CR)
NATIONAL GRID ELECTRICITY TRANSMISSION PLC (NGRID)
ANADOLU UNIVERSITY (AU)

COUNTRY

Italy
Italy
Germany
Spain
United Kingdom
Spain
Spain
Norway

Czech Republic
United Kingdom
Turkey

SIAM / Security Impact Assessment Measures

© L Robert Wilson - Fotolia.com

Information

Grant Agreement N°
261826
Total Cost
€2,777,307.68
EU Contribution
€2,168,640
Starting Date
01/02/2011
Duration
36 months

Coordinator

TECHNICAL UNIVERSITY BERLIN
Centre for Technology and Society
Human Technology Lab
Hardenbergstraße 16-18
10623 Berlin,
Germany
Contact
Dr. Leon Hempel
Tel: +49 (30) 314-25373
Mobile:
+49 (0) 176 111 20 400
Fax: +49 (30) 314-26917
E-mail:
hempel@ztg.tu-berlin.de
Website:
www.siam-project.eu

Project objectives

The SIAM decision support system will ease the complexity associated with the assessment of security measures and technologies. Where today decision makers have to oversee a wide range of relevant knowledge from different academic fields and national and cultural interests, SIAM will provide knowledge needed for assessing security technologies in a structured manner. The objective of SIAM is to produce a SIAM database and guidelines that allow quick access to information, not only on the effectiveness and the cost-benefit ratio but also on societal, ethical and legal aspects of security technologies. The interdisciplinary character of SIAM makes it unique. The participation of seven leading academic institutions from five countries and partners in the security research guarantees a high level of variety of perspectives. Additionally, the involvement of end users provides an empirical base for the theoretical research.

Description of the work

SIAM will combine various methodologies to conduct the research. SIAM entails four case study partners to gather field information in security measures and technologies (SMTs) as well as counter infringement technologies (CITs). The new capital airport Berlin Brandenburg International (BBI) will introduce state of the art technologies and will be one of the most modern airports on the European continent. SIAM will also compare airport security with the well established Ben Gurion Airport Tel Aviv, which uses a different approach in airport security. As a contrasting case, SIAM also focuses on the public transportation systems of London and Turin. SIAM will compare the London transportation, which is large and long standing, with the newly constructed full automatic transportation system in Turin. By conducting these four case studies featuring a significant level of security measures and technologies, SIAM integrates the practical experience with such technologies into the decision support system, as it will be flanked by extensive literature reviewing and the gathering of the knowledge of Europe's leading security and civil rights experts. The practitioner perspective will be extended by state of the art knowledge. SIAM will also complement the state of the art of SMTs and CITs by analyzing research projects for future technologies. This will be accomplished by conducting Delphi studies and interviews with leading experts in this domain of research.

SIAM is also analyzing threats towards SMTs and its efficiency and effectiveness to counter them. By analyzing past incidents, SIAM will develop threat scenarios on which it will test the implemented and future technologies.

Focus is also directed at freedom infringements by SMTs and at how effective CITs can be implemented. The legal dimension of technology assessment will be scrutinized in order to take accountability and transparency criteria into account when assessing SMTs.

Beyond that, SIAM is building an actor network to initialize the relationships needed for sustained cooperation and future fruitful interaction in the field of security. Participative elements such as stakeholder conferences open up the security field to a wider public and include more actors in the process.

Expected results

To decide on new SMTs is a complex task that requires the decision maker to evaluate a great number of heterogeneous aspects. SIAM ties together these aspects and reduces their complexity by providing a number of guidelines and a database for easy decision making. One major impact is that SIAM will continue to close this gap between the threat perspective and the freedom perspective that still characterizes the security field strongly. This will help to protect the freedom of European citizens and passengers, foster accountability and transparency in the use of security technology and help to avoid economic loss caused by investment flops and a lack of acceptance.

PARTNERS	COUNTRY
Technical University Berlin (TUB)	Germany
University of Kassel (UNIKASSEL)	Germany
University of Newcastle (UNEW)	United Kingdom
Kingston University London (KU)	United Kingdom
Higher Institute on Territorial System for Innovation Torino (SITI)	Italy
Tel Aviv University (ICTAF)	Israel
Vrije Universiteit Brussels (VUB)	Belgium

SMART / Scalable Measures for Automated Recognition Technologies

© kalafoto - Fotolia.com

Information

Grant Agreement N°
261727
Total Cost
€4,202,156
EU Contribution
€3,456,017
Starting Date
01/06/2011
Duration
36 months

Coordinator

UNIVERSITY OF CENTRAL LANCASHIRE
Centre for Law, Information and Converging Technologies
PR1 2HE, Preston,
The United Kingdom
Contact
Joseph Cannataci
Tel: +44 79 208 42745
Mobile: +356 99 42 61 33
Fax: +356 21 34 56 55
E-mail:
joe.cannataci@yahoo.co.uk

Project objectives

The project's objectives are to:

» Determine the state of the art and likely future trends of smart surveillance, its proportionality and its impact on privacy;

» Identify the dependency and vulnerability of smart surveillance on underlying technology infrastructures and explore system integrity and privacy issues;

» Identify and explore smart surveillance and privacy issues in cyberspace;

» Map out characteristics of laws governing surveillance and identify lacunae as well as best practices;

» Explore the attitudes and beliefs of citizens towards smart surveillance;

» Map out characteristics of laws governing interoperability, and data exchange, and identify lacunae while identifying new safeguards as well as best practices;

» Establish best-practice criteria developed on the basis of operational efficiency, established legal principles and citizen perceptions;

» Develop a toolkit for policy-makers, police and security forces to implement and promote the best practice approach.

Description of the work

» **Status quo analysis:** The project brings together serving or ex-police and intelligence officers with engineers, security specialists, IT and privacy lawyers, sociologists and experts in consumer behaviour, marketing and e-government identifying key sectors where smart surveillance technologies may find or are already finding application in four key areas: border control, counter-terrorism and law-enforcement, consumer sector multi-purpose mobile devices and e-Government. The status quo analysis also maps out characteristics of laws governing surveillance and identifies lacunae/new safeguards and gives special attention to mapping out characteristics of laws governing interoperability and data exchange;

» **Infrastructure analysis:** The project carries out risk analysis of the technologies utilised in underlying telecommunications network technology infrastructures as well as cyberspace;

» **Citizen attitudes:** Part of the project carries out qualitative research on the attitudes of citizens to smart surveillance and privacy. In addition, analytical bibliography as well as a literature review is carried out on the sociology of surveillance in order to inform the overall analysis of citizen attitudes as well as the impact assessments produced in other streams in an effort to identify criteria for best practices;

» **Best practice and development of the toolkit for policy makers:** The SMART project will develop a toolkit for policy-makers, system designers, decision-makers and police/security forces to implement and promote best practices.

Expected results

The expected results of this project include:

» A complete survey of smart surveillance techniques especially those used in EU Member States;

» Further understanding of current citizen attitudes toward privacy, especially in relation to smart surveillance technology;

» Best practices in relation to processing citizen information, respecting privacy whilst balancing the need for surveillance in modern European society;

» A toolkit for policy makers based on the findings of this project.

PARTNERS	COUNTRY
University of Central Lancashire (CLICT)	United Kingdom
University of Malta (UoM)	Malta
University of Ljubljana (UL)	Slovenia
Laboratorio di Scienze della Cittadinanza (LSC)	Italy
Babeș-Bolyai University of Cluj-Napoca (BBU)	Romania
Universitetet i Oslo (UiO)	Norway
Universidad de Leon (ULE)	Spain
Law and Internet Foundation (LIF)	Bulgaria
Masarykova univerzita (MU)	Czech Republic
Edith Cowan University (ECU)	Australia
Georg-August-Universitaet Goettingen Stiftung Oeffentlichen Rechts (UGOE)	Germany
Sheffield University (SHEFU)	United Kingdom
Gottfried Wilhelm Leibniz Universität Hannover (LUH)	Germany
CNR National Research Council (CNR)	Italy
Universzita Komenskeho v Bratislave (FMUNIBA)	Slovakia
Rijksuniversiteit Groningen (RuG)	The Netherlands
University of Vienna (UNIVIE)	Austria
Morpho (MPH)	France
International Criminal Police Organization - I.C.P.O. (INTERPOL)	France
Metropolitan Police Service (MET)	United Kingdom

SURPRISE / Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe

© Manuel Gutjahr - istockphoto.com

Information

Grant Agreement N°
285492
Total Cost
€4,396,297.56
EU Contribution
€3,424,109
Starting Date
01/02/2012
Duration
36 months

Coordinator

OESTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
Institute of Technology Assessment
Strohgasse 45/5
A-1030 Vienna, Austria
Contact
Johann Čas
Tel: +43 1 51581 6581
Fax: +43 1 7109883
E-mail: jcas@oeaw.ac.at
Website: http://www.oeaw.ac.at/ita/welcome.htm

Project objectives

» Map key security challenges and related security policies and technologies;

» Identify factors influencing acceptability and acceptance of these security technologies;

» Identify technical design and legal/regulatory options and non-technical alternatives;

» Develop models and hypotheses about relations between privacy and security;

» Select two cases for empirical testing and perform a large scale participatory empirical testing of models;

» Synthesize empirical findings with theoretical models and practical options to design security solutions;

» Transform results into smaller scale participatory methods;

» Disseminate the findings widely throughout Europe and beyond.

Description of the work

SURPRISE re-examines the relationship between security and privacy, which is commonly positioned as a 'trade-off'. Where security solutions involve the collection of information about citizens, questions arise as to whether their privacy has been infringed. This infringement of individual privacy is sometimes seen as an acceptable cost of enhanced security. Similarly, citizens are seen as willing to trade-off their privacy for enhanced personal security in different settings. These common understandings of the security-privacy relationship, at both state and citizen levels, have informed policymakers, legislative developments and best practice guidelines concerning security developments across the EU. However, an emergent body of work questions the validity of the security-privacy trade-off, suggesting that this has over-simplified the consideration of the impact and acceptability of security solutions on citizens in current security policy and practice. Thus, the more complex issues underlying privacy concerns and public scepticism towards surveillance-oriented security solutions (SOSSs) may not be apparent to legal and technological experts.

In response to these developments, this project will consult with citizens from several EU Member and Associated States on the question of the security-privacy trade-off as they evaluate different security solutions. Through extensive preparatory work, the project will identify and empirically examine the influence of a broad range of issues upon their evaluations. Using large scale citizen consultation meetings, a representative, fine-grained picture from across Europe will be provided. Furthermore, citizens' understanding of privacy protection laws, their enforcement, and the acceptance levels of SOSSs, will be explained. Finally, a set of context-dependent dimensions for decision support concerning the acceptability of new SOSSs which promotes civil rights protection will be produced.

Expected results

Provision of a framework to evaluate security solutions and technologies to be highly relevant for taking investment and policy decision related to security issues.

Provision of insight to understand the drivers of insecurity and the ways to prevent it; allowing governments to distribute resources in a more efficient and comprehensible way.

Improving social inclusion by highlighting potential sources of discrimination, unintended consequences produced by the introduction of security solutions and other aspects that threaten social cohesion with respect to security issues.

PARTNERS	COUNTRY
Oesterreichische Akademie der Wissenschaften (OEAW)	Austria
Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)	Spain
Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC)	Spain
Teknologiradet - The Danish Board of Technology (DBT)	Denmark
European University Institute (EUI)	Italy
VEREIN FUR RECHTS-UND KRIMINALSOZIOLOGIE (IRKS)	Austria
Medián Opinion and Market Research Ltd. (Median)	Hungary
Teknologiradet - Norwegian Board of Technology (NBT)	Norway
The Open University (OU)	United Kingdom
Akademien der Wissenschaften Schweiz Verein (TA-Swiss)	Switzerland
Unabhaengiges Landeszentrum fuer Datenschutz (ULD)	Germany

SURVEILLE / Surveillance: Ethical Issues, Legal Limitations, and Efficiency

© Surveille

Information

Grant Agreement N°
284725
Total Cost
€4,382,719.80
EU Contribution
€3,382,354
Starting Date
01/02/2012
Duration
39 months

Coordinator

EUROPEAN UNIVERSITY INSTITUTE
Research Administration
Via dei Roccettini 9, San Domenico Di Fiesole
50014 Firenze, Italy
Contact
Ms. Serena Scarselli
Tel: +39 055 4685 204
Fax: +39 055 4685 293
E-mail: serena.scarselli@eui.eu
Website: www.surveille.eu

Project objectives

SURVEILLE systematically reviews the impacts of different surveillance systems, and also helps manufacturers and end-users better develop and deploy these systems. It is a multidisciplinary project combining law, ethics, sociology and technology analysis. SURVEILLE assesses surveillance technology for its effectiveness in fighting crime and terrorism and its social and economic costs; it will assess perceptions of surveillance in the general public and certain identified target groups. SURVEILLE addresses legal limitations on the use of surveillance technologies as well as ethical constraints. SURVEILLE analyses the potential of 'privacy by design' and privacy-enhancing technologies in the context of surveillance systems and interacts with technology developers and manufacturers through a systematically delivered advisory service. SURVEILLE engages with law enforcement officials to seek their feedback as results emerge from the research. The project aims at wide dissemination, including amongst European and national decision-makers and will contribute to the field of training of judges, prosecutors and the police.

Description of the work

SURVEILLE is an interdisciplinary programme of research that will help decision makers to make better choices concerning the development, deployment and use of surveillance technologies. SURVEILLE conducts a comprehensive survey of surveillance systems and technologies that are currently used in Europe or that are likely to be introduced and addresses the legal limits on surveillance and the ethical issues it raises. It will also assess the effectiveness of surveillance technologies in improving security. SURVEILLE examines perceptions of surveillance and surveillance technologies amongst the general public and specific target groups, and informs decision-makers and other relevant stakeholders about the public acceptability of these technologies. Interactions between SURVEIILLE and developers and end-users will help manufacturers to adapt their systems to public concerns, and will help users to deploy systems more effectively. SURVEILLE builds upon the work of DETECTER – an FP7 Security funded project involving some of the members of this consortium that successfully experimented with the use of closed meetings between law enforcement officials, technology developers and human rights lawyers and ethicists to discuss how products could be developed in line with human rights and ethical standards. SURVEILLE further innovates by piloting an advisory service for technology developers using teleconferencing for virtual meetings and a telephone help-line as a potential advance in best practice. The concerns of technology developers will also serve as an input to research on ethical and legal constraints; here SURVEILLE also adds value to other projects funded under FP7 Security calls. SURVEILLE's interaction with technology developers, end-users and the data gained on perceptions of surveillance will be combined with the theoretical research to produce the best possible academic input for policy makers. SURVEILLE includes cutting edge expertise in ethics and human rights law.

Expected results

SURVEILLE provides a comprehensive survey of surveillance technology deployed in Europe and appraises security concerns, economic cost, public perceptions, and infringement of fundamental rights, and examines the legal and ethical issues of surveillance technology in the prevention, investigation and prosecution of terrorism and other serious crimes. SURVEILLE will continuously communicate results with stakeholders - European decision-makers, law enforcement, local authorities and technology developers - and receive feedback to inform ongoing research.

PARTNERS	COUNTRY
EUROPEAN UNIVERSITY INSTITUTE (EUI)	Italy
UNIVERSITY OF BIRMINGHAM (UOB)	United Kingdom
RAOUL WALLENBERG INSTITUTE OF HUMAN RIGHTS AND HUMANITARIAN LAW (RWI)	Sweden
TECHNISCHE UNIVERSITEIT DELFT (TU DELFT)	The Netherlands
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IOSB)	Germany
UNIVERSITE LIBRE DE BRUXELLES (ULB)	Belgium
FORUM EUROPEEN POUR LA SECURITE URBAINE (EFUS)	France
MERSEYSIDE POLICE AUTHORITY (MERPOL)	United Kingdom
ALBERT-LUDWIGS-UNIVERSITAET FREIBURG (ALU-FR)	Germany

VALUESEC / Mastering the Value Function of Security Measures

Information

Grant Agreement N°
261742
Total Cost
€4,473,885
EU Contribution
€3,443,210.10
Starting Date
01/02/2011
Duration
36 months

Coordinator

FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer Institute for Factory Operation and Automation IFF
Sandtorstrasse 22
39106 Magdeburg
Germany
Contact
Christian Blobner
Tel: +49 391 4090 371
Fax: +49 391 4090 93 901
E-mail: Christian.blobner@iff.fraunhofer.de
Website: http://www.valuesec.eu/

Project objectives

The objective of the ValueSec project is to develop a tool-set to support decision makers with overall policy objectives, political and ethical values as well as societal concerns. To achieve this, the consortium will develop means to make costs and benefits associated with decisions on security more transparent. The objectives of the project are:

» *Objective 1:* To survey the field of security economics, and the field of applicability of cost-benefit-tools and their links to societal issues relevant to security;

» *Objective 2:* To provide a tool-set for the analysis of cost and benefits of security measures, based on explicit requirements of policy level end-users;

» *Objective 3:* To test and validate the developed tool-set in realistic use cases;

» *Objective 4:* To evaluate the results from different perspectives of decision makers in security, from the policy, economic and societal point of view; and

» *Objective 5:* To determine the research needs and to give recommendations for further R&D.

Description of the work

ValueSec brings together an interdisciplinary team of researchers and end-users to generate a knowledge base of the current state and trends in theory and in practical applications of methods of economics, applied to security decision making. The project's main challenge will be to combine economic factors and societal effects of security measures into a "value function" to establish a basis for a cost-benefit approach. In effect, the project will bring together quantitative and qualitative information and combine it in a common methodological framework and integrate it into a decision support tool.

The consortium will be gathering inputs from public decision makers regarding their requirements for an efficient cost-benefit analysis in a security framework. Additionally, current approaches in cost-benefit analysis and in how far they are applicable to meet the decision maker's requirements will be surveyed and mapped onto available methodologies. This will be a major research effort for the subsequent integration into a software-based decision support tool.

ValueSec ensures the applicability of the developed approach and the subsequent software tool through validation in realistic use cases. These use cases will be built around typical scenarios for decisions in a security context. These use cases will be developed in close cooperation with end-users and external stakeholders to guarantee maximum relevance. End-user input will be provided by the Valencia Local Police, which will also provide an application scenario for a use case validation. Valencia provides ample opportunities to validate the developed approach and the subsequent support tool, e.g. in a use case comprising strategic planning elements for the Formula One Grand Prix organized in the city.

Expected results

The ValueSec project's main output will be a tool-set to support the systematic analysis and assessment of decisions of policy level stakeholders in a security context. Innovative approaches to cost-benefit analysis will be developed, making the effects of decisions more transparent and enabling decision makers to carry out trade-offs with respect to different decision making criteria, such as different priorities regarding security, political, economic or social goals.

PARTNERS	COUNTRY
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IFF)	Germany
VTT Technical Research Centre of Finland (VTT)	Finland
Centre for European Security Strategies (CESS)	Germany
International Peace Research Institute (PRIO)	Norway
University of Stavanger (UIS)	Norway
ATOS Origin S.A. (Atos)	Spain
Institute of Innovative Technologies (EMAG)	Poland
White Cyber Knight (WCK)	Israel
Policía Local de Valencia (VPD)	Spain

ARCHIMEDES / Support to security end users

© Cristian Baitg - istockphoto.com

Information

Grant Agreement N°
285061
Total Cost
€1,539,056
EU Contribution
€1,353,848
Starting Date
01/01/2012
Duration
36 months

Coordinator

EUROPEAN ORGANISATION FOR SECURITY
Avenue de Tervuren 270
B-1150 Brussels, Belgium
Contact
Moureen Schobert
Tel: +32 2 775 82 97
Mobile: +32 483 227 941
Fax: +32 2 775 81 12
E-mail: moureen.schobert@eos-eu.com
Website: www.eos-eu.com

Project objectives

ARCHIMEDES' mission is to increase the R&T uptake in Europe by focusing on end-users & operators' needs and involvement in the innovation cycle. To do that it aims at promoting a sustainable public – private dialogue between the demand and the supply side, and at making European research activities more end-user friendly, for a better identification of capability gaps and operational needs. ARCHIMEDES will facilitate end-users & operators' participation in security Research & Innovation programmes and make recommendations on how the innovation process from basic research through to development, standardization, certification and validation and finally deployment could be improved.

Description of the work

ARCHIMEDES will carry out research on Innovation Management tools, procedures and best practices (e.g. on Pre-Commercial Procurement, regulations, standardisation, etc.), end-users & operators' early R&T demand and common operational needs. In addition to testing, validation and certification issues in the security domain, it will also look into possible improvements of the legal and operational environment.

The results will consist of recommendations that will be explored, refined and validated with end-users & operators during several sector-specific roundtables. These roundtables will be held in different EU countries and gather existing networks of end-users and operators to support a dialogue and exchange information.

These networks will further be organised and linked through a "Virtual Forum for Security End-Users & Operators." This forum will continuously inform and encourage the debate among end-users on R&T activities, funding, new EU regulations and other developments that might impact their ability to innovate.

ARCHIMEDES will have the unique opportunity to maximise its impact on the planning of European and national security research activities by leveraging its Partners' established links with policy-makers. ARCHIMEDES will guarantee the follow-up of the project results by making them available to the broadest network of European, local and national stakeholders.

Expected results

- Development of an Innovation Management methodology to provide end-users with tools, procedures and best practices on how to efficiently benefit from R&T results;
- Launch of a sustainable process for an end-user & operator driven definition of common operational needs & early R&T demands;
- Recommendations for Horizon2020 that are in line with EU & national security policies, while reflecting end-users' needs;
- Enhancement of end-users & operators' participation in European research and innovation activities by looking at those stages where their involvement would be beneficial for improved R&T results and better deployment;
- Establishment of a sustained public-private dialogue among end-users & operators through the creation of a Forum for European Security End-Users & Operators to promote their networking.

PARTNERS	COUNTRY
European Organisation for Security (EOS)	Belgium
Ministerio Del Interior (MIR-ES)	Spain
Ingeniera De Sistemas Para La Defensa De España SA-ISDEFE (ISDEFE)	Spain
Universite catholique De Louvain (UCL)	Belgium
Haut Comite Francais Defense Civile (HCFDC)	France
German European Security Association EV (GESA)	Germany
Przemyslowly Instytut Automatyki I Pomiarow (PIAP)	Poland
@ Mediaservice.Net SRL (MEDIASERVICE)	Italy

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

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218026
Total Cost
€521,281
EU Contribution
€499,523
Starting Date
01/07/2009
End Date
30/06/2011

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
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

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 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 the 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique (CEA-LIST)	France
European Aeronautics Defence and Space Company EADS France SAS	France
Astrium SAS	France
Finmeccanica- Societa Per Azioni	Italy
Morpho (SGM)	France
Thales avionics SA	France
Österreischiches Forschung- und Prüzentrum Arsenal GesmbH	Austria
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Valtion Teknillinen Tutkimuskeskus (VTT)	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
European Commission - Joint Research Centre (JRC)	Belgium
European Biometrics forum limited	Ireland
Association française de normalisation	France
Ministère de l'intérieur	France
Center for Security Studies	Greece
AIT Austrian Institute of Technology GmbH (AIT)	Austria

DITAC / Disaster Training Curriculum

© Arkadi BojarUinov - iStockphoto

Information

Grant Agreement N°
285036
Total Cost
€4,466,505.80
EU Contribution
€3,498,668
Starting Date
01/01/2012
Duration
36 months

Coordinator

UNIVERSITY CLINIC BONN GERMANY
Department of Orthopaedics and Trauma Surgery
Sigmund Freud Street. 25
53127 Bonn, Germany
Contact
Dr. Philipp Fischer
Tel: +491607234539
Mobile: +491607234539
Fax: +491607234539
E-mail: philipp.fischer@ukb.uni-bonn.de
Website: www.ditac.info

Project objectives

The DITAC Project will:

- analyse concepts, methods, and doctrines of crisis response and identify the relevant European competences of crisis management;
- analyse existing initiatives on generating curricula for crisis management;
- identify the requirements of the local actors in crisis management education;
- identify the needs of relevant actors and the resulting stakeholder requirements for significant improvement of trainings in international disaster response and crisis management;
- develop a didactic concept to transmit common standards for crisis management education, using state of the art methods for teaching and training;
- organize a pilot study course for suitable participants from European countries;
- prove an evaluation tool for the course based on the developed curriculum.

Description of the work

The DITAC project proposes to develop a holistic training curriculum for first responders and strategic crisis managers dealing with international crises. The DITAC Curriculum will address the key challenges for the management of disaster incidents.

It will develop a standardised strong, comprehensive and efficient EU wide approach to crises and disasters to feature the added value by EU coordinated actions in the field of crisis response. The curriculum will improve the preparedness and availability of trained personnel by providing a common language, common objectives and common tools leading to better results in the protection and assistance of people confronted with large scale crises.

The focus is on international crisis management, but the benefit of a standardised training programme in crisis and disaster response can also be used to increase Europe's resilience in facing disasters and crises within the European Union. Establishing curricular training on how to respond to an international crisis and making it accessible to pertinent organizations throughout the EU will be a first step towards building a European Emergency Response Centre. Collaboration of specialists for disaster response as single experts in the field of international crisis management with local, regional and international authorities, NGOs, training institutes, scientific societies, research institutes and the cooperation of experts with backgrounds in medical, psychological and technical emergency assistance, logistics, conflict analysis and security challenges will create synergies towards improved disaster response capacity in the European Union.

The DITAC Project will use open sources for dissemination during the project period in order to get continuous feedback, and will organize public meetings and congresses to reach a consensus about the curriculum's content.

Expected results

- addresses the overall effectiveness and performance of the response and not just of the individual agencies;
- can be adapted to different geopolitical, organisational and geographic settings;
- creates an environment supporting progressive learning and enrichment, even beyond the scope of the project;
- supports effective collaboration and dialogue between EU member states and beyond;
- defines and develops educational tools which allow for preparing for and responding to major disasters in general.

PARTNERS	COUNTRY
University Clinic Bonn Germany (UKB)	Germany
Prehospital and Disaster Medicine Centre (PKMC)	Sweden
Hanover Associates (HA)	England
Center for Research in Emergency and Disaster Medicine (CRIMEDIM)	Italy
Clinical Emergency Hospital Bucharest (URGENTA)	Romania
Nations Health Career School of Management gGmbh (NHSC)	Germany
General and Teaching Hospital Celje (SBC)	Slovenia
Istanbul Aydin University (AFAM)	Turkey
Croatian urgent medicine and surgery association (CROUMSA)	Croatia
German Aerospace Center (DLR)	Germany
Bonn International Center for Conversion (BICC)	Germany
GABO:mi Gesellschaft für Ablauforganisation:milliarium mbH & Co. KG (GABO)	Germany

ESC / European Security Challenge

© Lom - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
261566
Total Cost
€527,034
EU Contribution
€468,279
Starting Date
01/03/2011
End Date
29/02/2012

Coordinator

GLOBAL SECURITY CHALLENGE LLP
57 Gloucester Place,
London W1U 8JJ
United Kingdom
Contact
Mr Simon Schneider
Tel: +44 (0) 207 224 0110
Email: schneider@globalsecuritychallenge.com
Website:
www.omnicompete.com

Project objectives

Other regions of the world, particularly the US, use competitive incentives such as awards and prizes to encourage innovation in security research, but Europe has lagged in this area.

The focus of this one-year project was to examine how such a model could be used to Europe's advantage. ESC's three-member consortium, consisting of Global Security Challenge LLP (UK), Jožef Stefan Institute (Slovenia) and PR agency 3D Communications (France), was tasked to design prize competitions that encourage innovators (from industry, academia, etc.) to deliver innovation solutions in European security – and to provide ideas and guidelines to the European Commission for doing so.

A parallel objective was to examine how competitions could visibly involve EU citizens in the innovation process.

Results

The ESC team conferred with experts, policymakers, companies and other stakeholders to shape its work, surveying 523 SMEs and interviewing 24 international innovation decision-makers from both public and private sectors, for example.

This led to the definition of three competition packages as options for the Commission to use in the future. The three are:

» the "UAV Crisis Response Challenge", designed to advance unmanned aerial systems (UAS) technology for emergency response to disasters;

» the "Citizens' Frontline Emergency Management Competition" to create open source software applications for emergency management, based on use of social media and modern communications technology;

» the "Cloud Castle Challenge" to encourage the creation of an open source software repository, or 'toolbox', for cyber security and the protection of cloud computing.

ESC's final report will allow European policy-makers to assess the potential for using prize competitions to boost innovation in security.

"Our analysis has shown that both applicants/innovators and prize promoters/sponsors can benefit from prizes," says the team. It adds that contest applicants and winners profit from wide media coverage and easier access to funding for the commercialisation of their research, while contest promoters and sponsors pull in participants from non-conventional fields that traditional methods fail to reach. Indeed, other methods for attracting innovation such as research grants or patents are discussed in the report and compared to prize competitions.

The report ends with a suggestion to integrate prize competitions in the EU's existing funding schemes.

PARTNERS

Global Security Challenge LLP (GSC)
3D Communications
Institute Jozef Stefan (JSI)

COUNTRY

United Kingdom
France
Slovenia

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

© TebNad- Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218217
Total Cost
€1,108,701.75
EU Contribution
€673,603.47
Starting Date
16/06/2008
End Date
15/12/2010

Coordinator

COMITÉ EUROPÉEN DE NORMALISATION (CEN)
Rue de Stassart 36
BE – 1050 Bruxelles
Belgium
Contact
Luc Van den Berghe
Tel: +32 2 550 09 57
E-mail:
luc.vandenberghe@cen.eu
Website:
www.escortsproject.eu/

Project objectives

ESCoRTS was 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 addressed 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 aimed at the dissemination of best practices on Supervisory Control And Data Acquisition (SCADA) security implementation, thus 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
COMITÉ EUROPÉEN DE NORMALISATION (CEN)	Belgium
AREVA T&D SA (Areva)	France
Enginet srl (EngiNet)	Italy
UNINFO - Associazione di Normazione Informatica (UNINFO)	Italy
OPUS PUBLISHING GENERAL PARTNERSHIP (OPUS)	United States
COMPANIA NATIONALA DE TRANSPORT AL ENERGIEI ELECTRICE TRANSELECTRICA SA (Transelectrica)	Romania
ENEL PRODUZIONE. S.P.A. (ENEL)	Italy
MEDITERRANEA DELLE ACQUE S.p.A. (Med-d-Acque)	Italy
SIEMENS AG (Siemens)	Germany
European Commission - Joint Research Centre (JRC)	Belgium
ABB SCHWEIZ AG (ABB)	Switzerland
Enel Ingegneria e Innovazione SpA (ENEL spa)	Italy

ETCETERA / Evaluation of critical and emerging technologies for the elaboration of a security research agenda

© ETCETERA

Information

Grant Agreement N°
261512
Total Cost
€1,996,728
EU Contribution
€1,512,742
Starting Date
01/10/2011
Duration
24 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen
Appelsgarten 2
53879 Euskirchen,
Germany
Contact
Joachim Burbiel
Tel: +49 2251 18-213
Fax: +49 2251 18-38-213
E-mail: joachim.burbiel@int.fraunhofer.de
Website:
www.etcetera-project.eu

Project objectives

The ETCETERA project is a contribution to effective and efficient security research planning on a European level. Its aim is three-fold:

» to develop novel methodologies for future strategic research planning;

» to identify risks and potential benefits associated with Critical Dependencies and Emerging Technologies with security implications; and

» to recommend a research agenda to deal with these risks and potential benefits.

Description of the work

ETCETERA's structure is separated into strands, one for Critical and the other for Emerging Technologies. These strands are separate but interrelated. Each strand is further divided into three Work Packages that will be carried through in a sequential manner. Two consultation campaigns will generate input from technical experts, end-users, and public authorities.

Strand 1: Critical Technologies

The first research strand (Work Packages 1 to 3) can be envisaged as a filtering exercise. Starting from all possible technologies, technologies indispensible for European security now and in the near future will be identified through extensive consultations within the consortium and with external experts.

In the second work package, the validated list of Critical Technologies will be checked for Critical Dependencies. Critical Dependencies arise if European industry is not self-sufficient in providing critical technologies/systems/capabilities to end users. Those dependencies could be caused by extra-European intellectual property rights (IPR), trade and academic restrictions, restrictions due to high classification in dual-use technologies, and economic challenges (e.g. shifting production sites, hindering or underdeveloped norms and standards, failing business models).

The last work package of Strand 1 will propose and prioritise alternative solutions to alleviate the Critical Dependencies identified. Strand 1 is associated with the 1st Consultation Campaign which includes five parallel workshops held at five locations and in six languages.

Strand 2: Emerging Technologies

In the first work package of Strand 2, Emerging Technologies are scanned for their security implications in 10 to 20 years time. Three scanning methods are implemented in a parallel fashion by AIT, Fraunhofer INT, and Isdefe. A comparative analysis of the results of these three methods will then be performed.

Emerging Technologies identified to be most relevant will be analysed in depth in the second work package of this strand. Furthermore, it is envisaged to adapt the originally military Disruptive Technology Assessment Game (DTAG) to civil scenarios and to set up an evaluative scenario workshop.

In the last work package of the strand, all results on Emerging Technologies will be considered when developing recommendations for an Emerging Security Technology Research Agenda (ESTRA).

Expected results

Several new approaches for research planning will be developed. This includes synthesising an enhanced and novel technology scanning method by taking the best of three methods already in use.

Furthermore, recommendations for strategic security research plans will be made. Measures will be taken to ensure that these plans are compatible with existing national and European research strategies. A new economic model to analyse high risk, high pay-off research priorities will also be developed. Ethical aspects will be taken into account at all levels of the project.

PARTNERS	COUNTRY
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fundación Tecnalia Research & Innovation (Tecnalia)	Spain
Ingeniería de Sistemas para la Defensa de España, S.A. (Isdefe)	Spain
Universität Duisburg-Essen (UDE)	Germany
AIT Austrian Institute of Technology GmbH (AIT)	Austria
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
VDI Technologiezentrum GmbH (VDI-TZ)	Germany
Morpho (MPH)	France
Ansaldo STS S.p.A. (ASTS)	Italy
COMSEC Unternehmensgruppe (COMSEC)	Germany
Centre for Science, Society and Citizenship (CSSC)	Italy
Storstockholms brandförsvar (SSBF)	Sweden

EUROFORGEN – NOE / European forensic genetics network of excellence

© Euroforgen

Information

Grant Agreement N°
285487
Total Cost
€8,192,996.63
EU Contribution
€6,613,680
Starting Date
01/01/2012
Duration
60 months

Coordinator

UNIVERSITÄTSKLINIKUM KÖLN
Institute of Legal Medicine
Melatengürtel 60/62
50823 Köln (Cologne),
Germany
Contact
Peter M. Schneider
Tel: +49 221 478 88345
Fax: +49 221 478 88370
E-mail: peter.schneider@uk-koeln.de
Website: www.euroforgen.eu

Project objectives

This initiative aims to achieve **long lasting cooperation leading to the emergence of a virtual research centre in forensic genetics embedded in the security domain.** For the implementation, a series of specific actions is needed such as:

- To establish a directory of forensic genetics research institutions across Europe;
- To identify the processes involved in handling and analyzing forensic genetic evidence from crime scene to courtroom;
- To facilitate the exchange of information between research institutions, stakeholders and end users;
- To integrate research needs and capacities into a sustainable virtual network.

EUROFORGEN-NoE - will serve to connect the efforts named above and to lay the foundations of a European virtual centre of research in forensic genetics aimed at introducing an international, self-sustained body fully supported by national activities.

Description of the work

EUROFORGEN-NoE comprises 12 partners from 8 countries, among them some of the leading groups in European forensic genetic research. The network initiative proposes an integration of existing cooperation, as well as establishing new ones, in this security field by integrating all the relevant parties and stakeholders.

Stimulating cooperation between research centres and industry is key to continued success. Thus, the main thrust of activities is aimed towards exchange of information, dissemination of knowledge, and networking. EUROFORGEN-NoE will carry out a series of actions in this regard. One of these actions is the execution of **three short exemplar projects**, where leading European research groups are collaborating as an example for other groups. These exemplar projects will prepare the ground for the publication of a **competitive call for additional projects** to be funded and subsequently integrated into the second phase of the project period.

Furthermore, forensic genetic research has to be **embedded into an ethical and societal framework** required for a positive acceptance of this relatively new technology by the public. An adequate response to public concerns regarding a potentially too intrusive use of new forensic DNA applications is seminal for a wider application of these methods in the near future. Only then can the consequences and future perspectives be addressed adequately. The essential development and **publication of an ethical guideline on forensic genetics** will be a major element of this process.

Finally, **educational structures will be established** both at the local as well as at the European level ensuring that scientists applying the forensic genetic technology in the context of security and the justice system are in line with the most recent scientific developments.

An **advisory board** with highly recognized experts from the fields of ethical, legal, and forensic sciences ensures that the challenges defined in the network programme will be met.

Expected results

EUROFORGEN-NoE will have **a long-lasting societal effect** by building an efficient research network – a **European Virtual Centre for Research in Forensic Genetic**: It enables the **most important stakeholders** to meet, to exchange and to disseminate information, to develop **new directions in research**, and to integrate its output into **outstanding new training concepts**. It will identify public perception of genetic forensic technologies and its potential for ethical conflicts - resulting in the development of **ethical guidelines**.

PARTNERS	COUNTRY
Universitätsklinikum Köln (UHC)	Germany
Universidade de Santiago de Compostela (USC)	Spain
Nasjonalt Folkehelseinstitutt (NIPH)	Norway
Queen Mary and Westfield College, University of London (QMUL)	United Kingdom
Københavns Universitet (UCPH)	Denmark
Netherlands Forensic Institute (NFI)	Netherlands
Medizinische Universitaet Innsbruck (IMU)	Austria
Universitetet for Miljø og Biovitenskap (UMB)	Norway
Uniwersytet Jagiellonski (JU)	Poland
University of Northumbria at Newcastle (UNN)	United Kingdom
Epiontis GmbH (EPTS)	Germany
GABO:mi Gesellschaft fuer Ablauforganisation:milliarium mbH & Co. KG (GABO:mi)	Germany

EU-SEC II / Coordinating National Research Programmes and Policies on Security at Major Events in Europe

© Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218076
Total Cost
€2,829,013.06
EU Contribution
€2,527,000
Starting Date
01/07/2008
End Date
31/10/2011

Coordinator

UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE
Security Governance and Counter-Terrorism Laboratory
10127- Turin
Italy
Contact
Alberto Pietro Contaretti
Tel: +39 011 6537 111
Fax: +39 011 6313 368
E-mail: contaretti@unicri.it
Website: www.eu-secii.org

Project objectives

EU SEC II was a coordination action organized by the United Nations Inter-regional Crime and Justice Research Institute (UNICRI), Europol and 22 European countries to develop the research cooperation begun by the first EU-SEC project (concluded in 2008).

EU-SEC II aimed to establish a comprehensive EU-wide network of national authorities in the field of Major Event security as well as common security planning standards to foster future European coordination in this area.

Its ultimate goal was the creation of the "European House of Major Events Security" (known as "the House") – a coordination tool to provide technical assistance to Major Event security planners on the basis of commonly elaborated planning methodologies. In this way, the House will contribute to the realization of the objectives of the EU Internal Security Strategy and the Stockholm Programme: the achievement of a common European policing approach.

Results

A key component of the project was the desire to avoid duplication of efforts and to incorporate the lessons learned and best practices already established into the House. A series of meeting allowed partners to elaborate common research priorities and policies endorsed by the whole research consortium.

One of EU-SEC II's objectives was to investigate which services the House could offer, focusing in particular on public-private partnerships (PPPs), common research standards and media management. The final output was a pilot research strategic roadmap to direct future research priorities.

To validate these ideas, EU-SEC II tested the services to be offered by the House in relation to seven Major Events. These were: the 2009 Champions League Final held in Rome, Italy; the Climate Change Conference 2009 held in Copenhagen, Denmark; the Pope's 2010 visit to Cyprus; the 2011 Champions League Final held in Madrid, Spain; the EU Presidencies of Hungary in 2011 and Cyprus in 2012; and, the 2011 G20 meeting held in France.

Finally, a manual was produced to guide ownership and operation of the House. The Manual lays the foundations for the further development of international coordination services aimed at improving and strengthening European level cooperation in Major Event security research and planning. It includes a detailed description of the Coordination Tools and Methodologies (CTMs) to be made available to European security planners via the House.

These efforts produced the following benefits:

» stronger cooperation and coordination among the relevant security stakeholders, including the private sector, to develop integrated and comprehensive operational security plans;

» implementation of specific training curricula to disseminate common policing methods and a culture of increased attention to the development of relationships with the general public and the media.

© EU-SEC II

PARTNERS

United Nations Interregional Crime and Justice Research Institute
Europol
Bundesministerum für Inneres/Ministry of the Interior
German Police University
Cuerpo Nacional de Policía
Ministry of the Interior/Police Department
Direction Générale de la Police Nationale
Metropolitan Police Service
An Garda Siochana
Ministero degli Interni
Ministry of Justice
Ministry of the Interior/Higher Institute on Police Sciences and Internal Security
Centre for Security Studies
Police Academy of Latvia
Ministry of Interior and Administration Reform General Inspectorate of the Romanian Police
Ministry of Interior of the Slovak Republic
Academy of the Ministry of the Interior
Policijska uprava Maribor
Personal Protection and Law Enforcement Police
Cyprus Police
Hungarian National Police Headquarters
Malta Police Force
Swedish National Police Board
National Police Department/National Police College
Ministry of the Interior of the Republic of Latvia (State Police)

COUNTRY

Italy
The Netherlands
Austria
Germany
Spain
Finland
France
United Kingdom
Ireland
Italy
The Netherlands
Portugal
Greece
Latvia
Romania
Slovakia
Bulgaria
Slovenia
Estonia
Cyprus
Hungary
Malta
Sweden
Denmark
Latvia

INNOSEC / Innovation management models for security organisations

© Cristian Baitg - istockphoto.com

Information

Grant Agreement N°
285663
Total Cost
€1,651,765
EU Contribution
€1,289,778
Starting Date
01/02/2012
Duration
24 months

Coordinator

FUNDACIÓN TECNALIA RESEARCH & INNOVATION
Innovation and Society Division
Parque Tecnológico de Bizkaia. Edificio 204
E-48170, Zamudio (Bizkaia), Spain
Contact
Amaia Sopelana
Tel: +34 946 400 450
Mobile: +34 667 17 89 33
E-mail: amaia.sopelana@tecnalia.com
Website: www.innosec-project.eu

Project objectives

The aim of the Project is to develop a novel innovation model for the security sector based on networked relationships between the actors and its associate organisational framework that will allow end-users to develop the ability to handle and utilise currently available and forthcoming innovations. It will foster the balance between innovation strategies, creating dynamic capabilities, and including absorptive capacity, allowing adequate structural and cultural organisational conditions that permit them to handle real environmental threats. This balance between a flexible model for implementing innovation management and the respect for current practices in general management and operation will be called the InnoSec paradigm.

Description of the work

In order to achieve the objectives of the project the consortium will:

» Analyse the end-user organisations' environment and innovation management processes. By analysing the operating environment and identifying end-users' current practices of innovation management, lessons will be drawn for the development of an innovation model;

» Analyse models of innovation and innovation management processes in non-security sectors. A development of a typology of these innovation models and practices will be conducted, in respect of their suitability for different types of embedding organisational environments;

» Develop a modular innovation model for security organisations (Innosec Model). This model aims at helping these organisations to design and implement innovation management processes and practices;

» Test the Innosec model. The modular innovation model previously developed will be customised and tested in end-user organisations;

» Develop an Implementation Roadmap that will guide public and private security providers as well as their regulatory bodies and other stakeholders towards a successful implementation of the novel model.

Expected results

The project expects to:

» Understand how security organisations are interpreting most critical needs of change, how they address innovation management, and how their conditions facilitate or impede successful innovation initiatives;

» Develop a methodological framework that allows for applying a new concept development addressing conceptualisation and innovation design issues in security organisations;

» Develop a supporting model for innovation management in security organisations that will be integrated by different modules;

» Transfer and share the insights and knowledge elaborated with security organisations.

PARTNERS	COUNTRY
Fundación Tecnalia Research & Innovation (TECNALIA)	Spain
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	Germany
Valtion Teknillinen Tutkimuskeskus (VTT)	Finland
Ministerio de Defensa de España (MDE)	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Austrian Institute of Technology GmbH (AIT)	Austria
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
The University of Manchester (UNIMAN)	United Kingdom
Österreichisches Rotes Kreuz – Austrian Red Cross (ÖRK ARC)	Austria
Prosegur Compañía de Seguridad SA (PROSEGUR)	Spain

INSEC / Increase Innovation and Research within Security Organisations

© mtrommer - fotolia.com

Information

Grant Agreement N°
285287
Total Cost
€1,576,867.60
EU Contribution
€1,126,862
Starting Date
01/04/2012
Duration
24 months

Coordinator

ALMA CONSULTING GROUP SAS
Innovation Department
55, Rue René Cassin
CP 418
69338 Lyon France
Contact
Michel MOULINET
Tel: +33 (0)4 72 35 89 04
Mobile:
+33 (0)6 22 92 98 12
Fax: +33 (0)4 72 35 80 31
E-mail:
mmoulinet@almacg.com
Website:
www.insec-project.eu

Project objectives

The INSec project is striving to improve the Innovation and Research processes within the security organisations, so that they can integrate new technologies, enabling them to evaluate novel approaches and services dedicated to the safety of citizens.

The project will focus on two main areas:

» The development of a new internal innovation management model. This will allow the security organisations to better manage both the financial impacts and the added value of innovating projects;

» The development of an external innovation platform in order to promote the networking between European security SMEs and public/private security organisations. This will increase the visibility of SMEs among security organisations and hence diversify the range of services and technologies for them.

Two major European-scale events will be organised to share good practices in the field of innovation management, and dissemination will be done though e-learning training modules developed within the project.

Description of the work

With a consortium of consulting companies and security end-users (public and private security organisations), the INSec project focuses on the existing needs and practices of four types of organisations:

» Rescue Services;
» Police and National Security Office;
» Academies of Security Sciences;
» National Security Infrastructures (port, border control).

As described below, eleven main tasks grouped by the following type of activities will be implemented:

Activity 1 - Analysis and Studies

» Analyse the main aspects of Innovation Management in the security-related operators (end-users), both public and private;

» Assess the Level of Innovation inside the organisation;

» Foster new business models for Security;

» Promote the security and privacy requirements at the early stages of systems development (“Security and Privacy by design”);

» Analyse and evaluate the impact of new technologies and review their legal implications.

Activity 2 - Innovation Ideas and Technology boost

» Create a new innovation model based on the needs of security organisations identified during the creativity sessions;

» Build an open platform which will integrate effective tools for technology watch, forecasting and roadmapping for the security sector. The aim is to provide an integrated framework for technology screening activity at European level in order to identify weak spots and early demand in R&D;

» Find services related to the platform tools which will encourage an appropriate use of technology or the implementation of innovative ideas for responding to new threats, in the medium to long-term.

Activity 3 - Best practices and networking

» Create networking activities and exchanges of best practices between security end-users in Europe;

» Establish for the four types of management systems a European best practices list.

Activity 4 - Training

» Define training needs and create an ‘innovation’ vocational training system framework for end-users available for the entire European Security Organisation.

Expected results

The implementation of INSec will enable Security organisations to:

» Use new innovation management models to improve internal innovation processes in order to maximise their added value and contribute to economic and social wealth;

» Develop networking with external actors, in particular European SMEs, for mutual benefits;

» Promote dissemination of the innovation management models and best practices through networking events and training, and facilitate internal cultural change.

PARTNERS	COUNTRY
ALMA CONSULTING GROUP SAS (Alma)	France
EFPC (UK) LTD (EFPC)	United Kingdom
FM MANAGEMENT CONSULTANCY SRL (FMMC)	Romania
PROXIMA CENTAURI SAS (KAOS)	France
ADVISIO OU (ADVISIO)	Estonia
GLOBAZ SA (GLOBAZ)	Portugal
EVERIS SPAIN SLU (EVR)	Spain
INOGATE- CONSULTORIA EM INOVACAO EMPRESARIAL SA (INOGATE)	Portugal
SISEKAITSEAKADEEMIA (EASS)	Estonia
ACADEMIA DE POLITIE ALEXANDRU IOAN CUZA (AICPA)	Romania
GRAD SKOPJE (CoS)	Former Yugoslav Republic of Macedonia
AUTORIDAD PORTUARIA DE GIJON (PAG)	Spain
HUNGARIAN MINISTRY OF INTERIOR (ORFKV)	Hungary
OU BALTIC INNOVATION AGENCY B.I.A. (BIA)	Estonia
ROMANIAN MINISTRY OF ADMINISTRATION AND INTERIOR (MAI)	Romania

NMFRDISASTER / Identifying the Needs of Medical First Responders in Disasters


© Dmitry Pistrov - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218057
Total Cost
€815,079.25
EU Contribution
€815,079.25
Starting Date
01/05/2008
End Date
30/06/2009

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
Website:
http://www.mdais.org

Project objectives

NMFRDISASTER aimed to research and recommend new methodologies for medical first-response organisations, so as to allow them to better train and prepare for disaster response tasks. It also sought to identify appropriate medical tools.

This research focused on five key areas:

» training methodology and technology used to train medical first responders for disasters;

» understanding the human impact of disaster on medical first responders;

» ethical and legal issues influencing the medical response to disasters;

» personal protective equipment (PPE) used in chemical, biological and radiological (CBR) incidents;

» use of blood and blood products in disasters.

Results

A key finding of NMFRDISASTER was that although medical preparedness for disasters in most organisations surveyed was high, evidenced-based material for training was limited.

NMFRDISASTER thus proposes the creation of a formal, evidence-based curriculum based on successful case studies, determined evaluation criteria and a training simulation programme for both medical treatment and management issues.

In view of the fact that employment frameworks for the use of medically trained volunteers are highly irregular across Europe, the project recommends creating and adopting a basic charter in this area. Provisions of the charter would include common minimum standards and a "rights and duties" agreements that could be signed between volunteers and medical organisations.

NMFRDISASTER also found a lack of procedural preparation for the use of personal protective equipment to shield medical first-responders from chemical, biological or radiological contamination. The project thus proposes the development of standard decontamination procedures, enhanced communications regimes and more stringent safety procedures for handling CBR incidents.

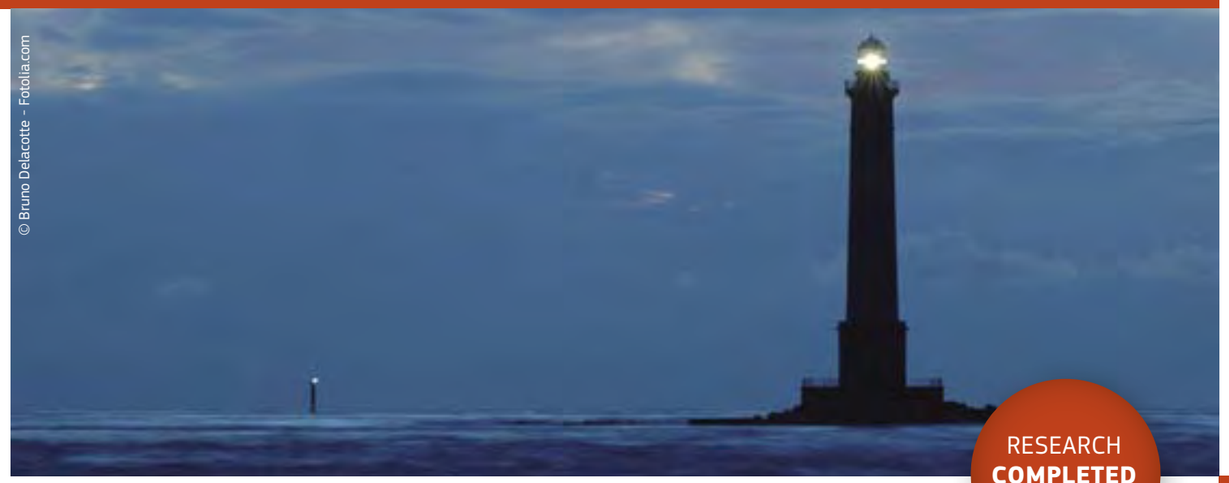
The project also proposed the development of new portable blood delivery technologies, and the formal set-up of emergency blood donation schemes to overcome the rapid decline in blood stocks instigated by a large-scale medical incident.

Finally, the project considered some of the ethical, emotional, legal and media communication aspects of medical first response tasks. NMFRDISASTER concludes that a lack of public understanding of medical tasks in an emergency, combined with sensitivity towards issues such as blood donation and medical "triage" prioritisation, may place medical responders at great risk of legal liability charges and emotional trauma.

Public awareness campaigns, cultural sensitivity training and further legal research is encouraged in these areas.

PARTNERS	COUNTRY
Magen David Adom	Israel
SAMUR Protección Civil, Ayuntamiento de Madrid	Spain
AmbulanceZorg Nederland	The Netherlands
Danish Red Cross	Denmark
Sinergie S.r.l	Italy
Fundación 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-administered areas

OPERAMAR / An interoperable approach to European Union maritime security management



RESEARCH **COMPLETED**

Information

Grant Agreement N°
218045
Total Cost
€669,134
EU Contribution
€669,134
Starting Date
01/03/2008
End Date
31/05/2009

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

Project objectives

OPERAMAR aimed to assess the challenges of boosting the seamless exchange of information and ensuring a sufficient level of interoperability between current maritime security management systems amongst EU Member States.

This study had a specific emphasis on technical constraints and legacy systems, but did not ignore organisational and institutional obstacles to information sharing such as legislation and regulations within particular states.

Results

OPERAMAR undertook 40 field visits and stakeholder surveys, which were used to ascertain the current state of information gathering, integration and dispatch between stakeholders in the maritime surveillance field.

The range of actors surveyed included: sea border and port control, customs, fisheries, marine transport and traffic control, marine pollution control, suppression of criminal activities, military actors and marine search and rescue.

In each instance, stakeholders were examined in terms of overall awareness and information management practices during both routine and emergency response activities.

OPERAMAR concluded from these assessments that, given the large number of legacy systems current in operation (estimated at 20 Europe-wide), the following two-pronged approach is recommended:

» A secure and interoperable ICT environment, dubbed the "Common sEcuRe and selective Information Sharing Toolbox" (CERIS.Tbox), should be used as the basis for a shared information sharing protocol that can accept inputs from a variety of existing systems. CERIS Tbox should prioritise common data standards and secure connections – and it should be based on the principle of information "push", whereby data owners retain control over what data is shared with specific end-users;

» Structured around CERIS Tbox, a medium-to-long term vision of operational concepts and technical solutions should be nurtured. OPERAMAR argues that this will encourage future harmonisation and interoperability when managing maritime surveillance activities and response operations.

Overall, OPERAMAR concluded that getting information-sharing to become routine while also developing a common Concept of Operations ("ConOps") are more of an impediment in this domain than the actual technological obstacles.

Next steps:

OPERAMAR recommends that an action plan and roadmap be developed for two reasons to:

» encourage convergence of member state, stakeholder and EU project efforts related to information sharing, co-ordination and management;

» provide Member States with guidance to enhance their maritime surveillance capabilities, for example in the framework of the EU's External Border Fund.

An over-arching ConOps to create a structured system of integrated maritime management for a European Maritime Domain should also be considered.

PARTNERS	COUNTRY
Thales Underwater Systems SAS (THALES)	France
SELEX Sistemi Integrati S.p.A. (SELEX)	Italy
Indra Sistemas S.A. (INDRA)	Spain
Quintec Associates Ltd. (QUINTEC)	United Kingdom
The Alliance of Maritime Regional Interests in Europe (AMRIE)	Belgium
European Commission - Joint Research Centre (JRC)	Belgium
Istituto Affari Internazionali (IAI)	Italy
Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)	Portugal
STM Savunma Teknolojileri Muhendislik ve Ticaret A.S. (STM)	Turkey
Thales Systemes Aeroportes S.A. (TAS)	France

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

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242416
Total Cost
€726,706.60
EU Contribution
€580,889
Starting Date
01/04/2010
End Date
31/03/2012

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

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:

» 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;

» 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;

» 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
CiaoTech Srl (CTECH)	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

SECURECHAINS / Integration of security technology supply chains and identification of weaknesses and untapped potential

© bisougue - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
242417
Total Cost
€1,082,006.63
EU Contribution
€820,032
Starting Date
01/05/2010
End Date
30/04/2012

Coordinator

SERVIÇOS DE CONSULTADORIA EM INOVAÇÃO TECNOLÓGICA, S.A.
Contact
Alexandre Almeida
E-mail: alexandre.almeida@inovamais.pt
Website: www.securechains.eu

Project objectives

The SecureCHAINS project's main mission is to contribute to 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**:

» 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 the 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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Serviços de Consultadoria em Inovação Tecnológica, S.A. (INOVAMAIS)	Portugal
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)	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	Romania
ALMA CONSULTING GROUP SAS	France
TECHNICAL SUPPORT FOR EUROPEAN ORGANISATIONS SPRL	Belgium
SOUTHEASTERN EUROPE TELECOMMUNICATIONS & INFORMATICS RESEARCH INSTITUTE	Greece

SEREN / Security Research NCP network – Phase 1

© Andres Rodriguez - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217937
Total Cost
€743,597.40
EU Contribution
€557,692.04
Starting Date
01/02/2008
End Date
31/07/2009

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
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/

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.

Results

The results of the project are available on the CORDIS website http://cordis.europa.eu/fp7/security.

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (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
Totalförsvarets Forskningsinstitut (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

SEREN2 / SEcurity REsearch Ncp network – phase 2

Information

Grant Agreement N°
261814
Total Cost
€1,801,696.23
EU Contribution
€1,499,546.21
Starting Date
01/04/2011
Duration
24 months

Coordinator

ROMANIAN SPACE AGENCY
Headquarters
21-25 Mendeleev Street
010362 – Bucharest
Romania
Contact
Anca Liana RACHERU
Tel: +40 (0) 21 3168722
Fax: +40 (0) 21 3128804
E-mail: Anca.racheru@rosa.ro
Website: www.rosa.ro

Project objectives

The main objective of this project is to continue promoting and enhancing trans-national cooperation among Security National Contact Points (NCP) (at the level of both people and institutions appointed in this respect), by reaching a balanced distribution of proficient services to be delivered by Security NCPs to their clients while assisting them to write high quality proposals to be submitted in the future calls.

Description of the work

WP1 – Capacity Building aims at *improving the Security NCPs' capabilities and reinforcing the network to become more efficient and effective. Technical trainings on general and specific issues, twinning schemes and staff exchange* are focused on sharing experiences, expertise and good practices, by promoting intensive trans-national cooperation.

WP 2 – Joint Brokerage Events aims at *improving the quality of the cooperation between security research stakeholders* (researchers, large companies, SMEs, end-users) by *providing the necessary support* to ease the process of finding appropriate partners for *building successful consortia*. Trans-national events shall be organised to the benefit of cross-border audiences.

WP 3 – Mapping of security research competencies focus on the identification of Security Research Competencies in Europe, to *increase the visibility of security related research in Europe and to optimize the networking* between research facilities, universities, public authorities, end users and suppliers of security solutions and operators of critical infrastructures.

WP 4 – Partner Search is dedicated to *promote transnational cooperation by facilitating the access of potential participants to future Security calls*.

WP 5 - Monitoring of Security research area aims at *providing both NCPs and stakeholders with an improved flow of security research area information*. An *in-depth mapping of security research systems and programmes* is foreseen.

WP 6 – Communication and dissemination has as the objective to oversee and organize all aspects which are related to communication and dissemination of the project results and activities. A scientific approach of communication and dissemination will be applied for this project by stimulating and strengthening the relationship between persons and problems. Making project achievements and activities widely accessible and easily exploitable by project customers will be a challenge for this WP.

Expected results

Results from SEREN2 will help decision making related to:

» Underpinning the realization of NCP value chains in the security topic for simplifying access to FP7 calls, for lowering the entry barriers for newcomers and raising the average quality of submitted proposals;

» Improve and increase the effectiveness of third country organizations' participation alongside European organizations;

» Strengthen the competitiveness of the European R&D in the Security theme.

PARTNERS	COUNTRY
Romanian Space Agency (ROSA)	Romania
Foundation for Research & Technology – HELLAS (FORTH)	Greece
Agenzia per la Promozione della Ricerca Europea (APRE)	Italy
Österreichische Forschungsförderungsgesellschaft mbH (FFG)	Austria
Euresearch Head Office Berne (EURESEARCH)	Switzerland
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)	France
Mokslo Inovaciju Ir Technologiju Agenturaa (MITA)	Lithuania
SIHTASUTUS ARCHIMEDES (Archimedes)	Estonia
Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk (IPPT PAN)	Poland
MATIMOP - Israel Industry Center for Research & Development (MATIMOP-ISERD)	Israel
Norges forskningsråd – Research Council of Norway (RCN)	Norway
The Scientific and Technological Research Council of Turkey (Tubitak)	Turkey
Dienst voor Wetenschappenlijke en Technische Informatie / Service d'Information scientifique et technique (STIS)	Belgium
Centro para el Desarrollo Tecnologico Industrial (CDTI)	Spain
Technologické centrum Akademie ved Ceske republiky (The Technology Centre of the Academy of Science - TC AS CR)	Czech Republic
Research Promotion Foundation (RPF)	Cyprus
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Council for Scientific and Industrial Research (CSIR)	South Africa
Riga Technical University (RTU)	Latvia
Centre for National Security and Defense Research (CNSDR)	Bulgaria
Malta Council for Science and Technology (MCST)	Malta
Zilinska Univerzita v Ziline (UNIZA)	Slovakia
Finnish Funding Agency for Technology and Innovation (TEKES)	Finland
Hrvatski institut za tehnologiju/ Croatian Institute of Technology / Odjel za međunarodnu suradnju/ International Cooperation Unit (HIT)	Croatia
Fundacao para a Ciencia e Tecnologia (FCT)	Portugal
National Institute of Aerospace Technology of Spain (INTA)	Spain

STRAW / Security Technology Active Watch

© Nmedia - Fotolia.com

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218132
Total Cost
€1,341,933.33
EU Contribution
€998,537
Starting Date
01/10/2008
End Date
31/05/2010

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@atos-research.eu

Project objectives

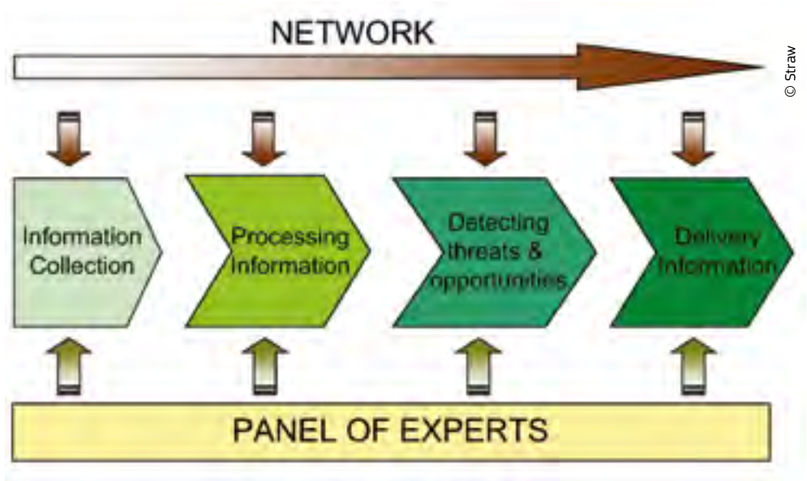
The STRAW project aimed to enhance European civil security by facilitating cooperation amongst various stakeholders, including researchers, technology providers and end-users.

Its mission was to monitor the security domain in order to detect relevant and applicable security technology developments, knowledge, experience and stakeholders. It also strove to deliver this information to the right audience at the right time to better exploit the information.

Results

The project began by creating a comprehensive review and cataloguing framework for evaluating thematic, technical and structural developments in security technology. This included creating a taxonomy structure for defining a concept map composed of classes, sub¬classes and name relations between technology areas. This served as the core of the semantic processing tool for the project's Security Technology Watch.

The main outcome of the project was "STRAWiki", an online portal tool based on wiki software that allows users to constantly update technology information in an online depository.



© Straw

PARTNERS

Atos Origin SAE
Aerospace and Defence Industries Association
Thales Services
Sitftelsen SINTEF
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
Instituto Nacional de Técnica Aeroespacial
Elsag Datamat S.p.A.
Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España
Fondazione Rosselli
European Organisation for Security

COUNTRY

Spain
Belgium
France
Norway
Germany
Spain
Italy
Spain
Italy
Belgium

THE HOUSE / Enhancing European Coordination for National Research Programmes in the Area of Security at Major Events

© Louise Gagnon - Fotolia.com

Information

Grant Agreement N°
285099
Total Cost
€3,105,925.27
EU Contribution
€2,774,300
Starting Date
01/03/2012
Duration
24 months

Coordinator

UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE
Security Governance
Counter-Terrorism
Via Maestri
del Lavoro 10,
10122 Turin, Italy
Contact
Alberto Contaretti
Tel: +390116537136
Fax: +390116313368
E-mail: contaretti@unicri.it

Project objectives

The main objective of the project 'THE HOUSE' is to provide assistance to EU countries hosting a Major Event through the European House of Major events (the House), in the application of the research[1] coordination methodologies identified, developed and tested by the Consortium of end-users of EU-SEC II.

While initially open to its 24 participating EU members only, the House is designed to be an inclusive tool at the disposal of all EU Member States and Associated Countries. By assisting them to coordinate their Major Events security plans, the House will help the partners to advance towards the adoption of a common European approach to Major Event security planning.

In addition, the House will serve as a tool to further improve security in the EU in line with the Stockholm Programme objective of protecting the lives and safety of European citizens by strengthening cooperation in police matters and law enforcement thus making Europe more secure. The enhancement of mutual trust between authorities and services in the different Member States, as well as decision-makers, is the basis for efficient cooperation.

Description of the work

The Project is organized in four thematic Work Packages (WPs), each of them envisaging different Tasks. The implementation of each Task is carried out by the respective Task Leader, with the support of other Consortium partners, under the overall coordination of UNICRI.

The envisaged *joint activities* aim to apply THE HOUSE coordination tools/methodologies (CTMs) to four thematic areas of real Major Events security planning: Common research and technology taxonomy; Common planning standards; Common evaluation standards; Networking and training. Each CTM is "looked after" by a dedicated member of the Consortium who acts as CTM Owner, providing assistance to the hosts of selected Major Events. The hosting Member State facilitates the Consortium Members' access to the planning/evaluation process of the Major Event, whilst UNICRI, in addition to its Coordinator role and in its capacity as WP leader, coordinates the organization of the planned use of the CTMs with the activities of the respective Task leaders. In this way, the House encourages the national security practitioners of the participating countries to foster the application of its EU-wide coordination standards and ensure the highest level of security at Major Events.

The *transnational activities* carried out by THE HOUSE Consortium aim to assess the impact of the coordination tools/methodologies (CTMs) provided by the House on the implementation of the Stockholm Programme and the Internal Security Strategy (ISS). These activities are intended to contribute to the adoption of a common policing approach by the European security policy-makers, to develop policy suggestions and ensure the effectiveness and long-term sustainability of these advancements.

The main project output will be a set of *User Guidelines* aimed at providing security planners with practical tips on the use and application of the research CTMs offered by the House in respect of the security planning of Major Events taking place in Europe.

Finally, specific *Dissemination* activities are envisaged to raise awareness about the House and the main products of its Consortium among relevant targeted audiences and the general public.

[1] Security Research for Major Events concerns the process by which knowledge of either 'security threats' or the capacity of 'security tools' (which includes plans) to provide 'security' (i.e. actually prevent the potential harm of a 'threat') at a Major Event, is produced.

Expected results

Security in the EU requires an integrated approach where professionals share a common culture, effectively pool information and have appropriate technological infrastructure to support them. THE HOUSE provides a response to these needs as well as answering to an identified European requirement to advance the coordination of security planning in the field. All this is in line with the recommendation included in the Stockholm Programme that consideration be given to the establishment of ad hoc law enforcement cooperation at sporting events or large public gatherings.

PARTNERS	COUNTRY
United Nations Interregional Crime and Justice Research Institute (UNICRI)	Italy
Bundesministerium für Inneres-Ministry of the Interior (BM.I)	Austria
Deutsche Hochschule der Polizei (DHPol)	Germany
Ministerio del Interior (MIR-CNP)	Spain
Ministere de l'Interieur (D.G.P.N.)	France
Metropolitan Police Service (MetPol)	United Kingdom
An Garda Síochána (AGS)	Ireland
Ministero dell'Interno (MinInterno)	Italy
Ministry of Security and Justice (MinJus)	The Netherlands
Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI/MAI)	Portugal
Center for Security Studies (KEMEA)	Greece
State Police of Latvia (SP)	Latvia
Ministry of Administration and Interior-Inspectorate General of Romanian Police (MoAI-GIRP)	Romania
Ministry of Interior of the Slovak Republic (MINV-APZ SK)	Slovakia
Academy of the Ministry of the Interior (Academy of MOI)	Bulgaria
Ministry of the Interior of the Republic of Slovenia (MOI SI)	Slovenia
Ministry of the Interior of the Republic of Estonia (MOI)	Estonia
Cyprus Police (Cyprus Police)	Cyprus
Hungarian National Police (HNP)	Hungary
Malta Police Force (MPF)	Malta
Swedish National Police Board (Polisen)	Sweden
The Danish National Police (DNP)	Denmark
Police department under the Ministry of the Interior of the Republic of Lithuania (PD)	Lithuania
Police College of Finland (Polamk)	Finland
Wyzsza Szkola Policji W Szczytnie (WSPol)	Poland

LIST OF PROJECTS

European Commission

Enterprise and Industrie

Luxembourg: Publications Office of the European Union, 2012

2012 — 352 pp. 21 cm x 29.7 cm

ISBN 978-92-79-25113-9
doi:10.2769/38445

NB-32-12-224-EN-C

Security Research Projects
under the 7th Framework Programme for Research

EU Research for a Secure Society

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

Publications Office

ISBN 978-92-79-25113-9

doi:10.2769/38445