



European
Commission



*Security Research Projects
under the 7th Framework Programme for Research*

EU Research for a **Secure** Society

May 2014



*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, 2014

ISBN 978-92-79-43792-2
doi:10.2769/52221

© European Union, 2014
Reproduction is authorised provided the source is acknowledged.

Cover picture: © Fotolia/Shutterstock

Printed in France

Printed on a CONDAT silk paper, certified by the PEFC™ and ECF

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/dgs/home-affairs/innovation-and-industry/>

Prepared by the European Commission, Directorate-General for Enterprise and Industry, Unit G4 Policy and Research in Security, E-mail: HOME-INNOVATIONANDINDUSTRY@ec.europa.eu

TABLE OF CONTENTS

INTRODUCTION 1

TABLE OF CONTENTS 2

Security of the Citizens

■ CBRN PROTECTION

BIO-PROTECT	6
CBRNEMAP	8
COCAE	10
CREATIF	12
DECOTESC1	14
EDEN	16
ISIS	18
MODES_SNM	20
REWARD	22
SAFEWATER	24
SCINTILLA	26
SECUREAU	28
SNIFFER	30
SPICED	32
TAWARA_RTM	34
TWOBIAS	36

■ EXPLOSIVES

AVERT	38
BONAS	40
COMMONSENSE	42
D-BOX	44
EMPHASIS	46
ENCOUNTER	48
FORLAB	50
HOMER	52
HYPERION	54
LOTUS	56
OPTIX	58
PREVAIL	60
SALIENT	62
SUBCOP	64
TIRAMISU	66

■ INTELLIGENCE AGAINST TERRORISM

IMSK	68
RAPTOR	70
TACTICS	72
UNCOSS	74
VIRTUOSO	76

■ ORDINARY CRIME AND FORENSIC

AEROCEPTOR	78
EVIDENCE	80
LINKSCH	82
MEPROCS	84
MIDAS	86
ODYSSEY	88
SAVELEC	90

SMARTPRO 92

■ ORGANISED CRIME

CAPER	94
CONPHIRMER	96
CUSTOM	98
DIRAC	100
HEMOLIA	102
SAVEMED	104
SCIIMS	106

■ INFORMATION GATHERING

CRIMTRACK 108

Security of infrastructures and utilities

■ CYBER CRIME

CAMINO	110
COCKPITCI	112
E-CRIME	114
HYRIM	116
PREEMPTIVE	118
SAWSOC	120
SECCRT	122

■ DESIGN, PLANNING OF BUILDINGS AND URBAN AREAS

DESURBS	124
HARMONISE	126
RIBS	128
SECUR-ED	130
SPIRIT	132
VASCO	134
VITRUV	136

■ ENERGY, TRANSPORT, COMMUNICATION GRIDS

COPRA	138
CWIT	140
DEMASST	142
DITSEF	144
EURACOM	146
EUROSKY	148
GAMMA	150
INFRA	152
ISTIMES	154
L4S	156
NI2S3	158
PANDORA	160
PROTECTRAIL	162
SECTRONIC	164
SERON	166
SESAME	168
SPARKS	170
STAR-TRANS	172
STRUCTURES	174
TASS	176
XP-DITE	178

■ SUPPLY CHAIN

IMCOSEC	180
IPATCH	182
LOGSEC	184
PROMERC	186
SAFEPOST	188

■ SURVEILLANCE

ADABTS	190
ARENA	192
ARGOS	194
BASYLIS	196
IDETECT 4ALL	198
INDECT	200
MOSAIC	202
P5	204
SAMURAI	206
SUBITO	208

Intelligent surveillance and border security

■ AIR BORDERS

ARGUS 3D	210
--------------------	-----

■ BORDER CHECKS

ABC4EU	212
ACXIS	214
CONSORTIS	216
DOGGIES	218
EFFISEC	220
FASTPASS	222
FIDELITY	224
HANDHOLD	226
INGRESS	228
SNIFFER	230
SNIFFLES	232
SNOOPY	234
TERASCREEN	236

■ BORDER SURVEILLANCE

OPARUS	238
SUNNY	240

■ LAND BORDER

CONTAIN	242
GLOBE	244
TALOS	246

■ SEA BORDERS

AMASS	248
CASSANDRA	250
CLOSEYE	252
I2C	254
OPERAMAR	256

PERSEUS	258
SEABILLA	260
SUPPORT	262
TRITON	264
WIMAAS	266

Restoring security and safety in case of crisis

■ CBRN RESPONSE

ANTIBOTABE	268
BOOSTER	270
CATO	272
COUNTERFOG	274
FRESP	276
IFREACT	278
MIRACLE	280
MULTIBIODOSE	282
MULTISENSE CHIP	284
PRACTICE	286

■ PREPAREDNESS, PREVENTION, MITIGATION AND PLANNING

A4A	288
BESECU	290
BRIDGE	292
CASCEFF	294
CAST	296
COPE	298
CRISCOMSCORE	300
CRISIS	302
CRISMA	304
EMILI	306
IDIRA	308
INDIGO	310
OPSIC	312
OPTI-ALERT	314
POP-ALERT	316
PREDICT	318
PSYCRIS	320
SECURENV	322
S-HELP	324
SICMA	326
SNOWBALL	328

■ RECOVERY

ACRIMAS	330
CAERUS	332
COBACORE	334
DESTRIERO	336
HELP	338
RECONASS	340
SAFE-COMMS	342
CRISYS	344

■ RESPONSE

DARIUS	346
ELITE	348

TABLE OF CONTENTS

E-SPONDER	350
ESS	352
EVACUATE	354
FASTID	356
ICARUS	358
NMFRDISASTER	360
PEP	362
SGL FOR USAR	364
SPARTACUS	366
S(P)EEDKITS	368

Security systems integration, interconnectivity and interoperability

■ INFORMATION MANAGEMENT

BEAT	370
FORTRESS	372
REDIRNET	374

■ INTEROPERABILITY

ADVISE	376
C2-SENSE	378
DISASTER	380
ESENET	382
ISITEP	384
SALUS	386
SAVASA	388
UNSETH	390

■ SECURE COMMUNICATIONS

EULER	392
FREESIC	394
GERYON	396
HIT-GATE	398
PPDR-TC	400
SECRICOM	402

■ STANDARDISATION

CRISP	404
EQUATOX	406
SLAM	408

Security and society

■ CITIZENS, MEDIA AND SECURITY

ANVIL	410
ATHENA	412
COSMIC	414
CPSI	416
EMERGENT	418
IMPACT EUROPE	420
ISAR+	422
PARIS	424
RECOBIA	426
SAFIRE	428

SLANDAIL	430
SUPER	432
SURVEILLE	434

■ ETHICS AND JUSTICE

ADDPRIV	436
ALTERNATIVE	438
COREPOL	440
DETECTOR	442
INEX	444
PACT	446
PRISMS	448
SAPIENT	450
SMART	452
SURPRISE	454

■ FORESIGHT, SCENARIOS AND SECURITY AS AN EVOLVING CONCEPT

ASSERT	456
COMPOSITE	458
DESSI	460
EPOOLICE	462
ETTIS	464
FESTOS	466
FOCUS	468
FORCE	470
FORESEC	472
SIAM	474

■ ORGANISATIONAL STRUCTURE AND CULTURES OF PUBLIC USERS

BESECURE	476
--------------------	-----

■ SECURITY ECONOMICS

EUSECON	478
SECONOMICS	480
VALUESEC	482

Security Research coordination and structuring

■ END USER

ARCHIMEDES	484
EU-SEC II	486
INNOSEC	488
INSEC	490

■ ERA-NET

THE HOUSE	492
---------------------	-----

■ OTHER COORDINATION

EU-CIPRNET	494
EUROFORGEN - NOE	496
PLANTFOODSEC	498
SEREN	500

SEREN2 502
SOURCE 504
VIDEOSENSE 506
VOX-POL. 508

■ **SMALL AND MEDIUM ENTERPRISES**

3D-FORENSICS 510
GRAFFOLUTION 512
MISAFE. 514
OSMOSIS 516
P-REACT 518
ROSFEN 520
SMARTPREVENT. 522

■ **STUDIES**

CRESCENDO. 524
ESC. 526
ESCORTS. 528
ETCETERA 530
SECURECHAINS 532
STRAW. 534

■ **TRAINING**

DITAC 536
LEILA. 538
SAFECITI. 540

LIST OF PROJECTS 542

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

© kentoh - Fotolia.com

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@](mailto:vincent.chauvet@lgi-consulting.com)

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

LGI Consulting
AVSISTA
C-Tech Innovation Ltd
Environics Oy
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
Institut für Umwelt Technologien GmbH
Robert-Koch Institut
University of Aalborg
Environics-IUT GmbH (ENIT)

COUNTRY

France
Lithuania
United Kingdom
Finland
France
Germany
Germany
Denmark
Germany

CBRNEMAP / Road-mapping Study of CBRNE Demonstrator



**RESEARCH
COMPLETED**

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@](mailto:Agneta.Plamboeck@cbnecenter.eu)

cbnecenter.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.

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.

PARTNERS

European CBRNE center at Umeå University
 Police National CBRN Centre
 National Institute for NBC Protection
 Robert Koch Institute
 DGA Maîtrise NRBC
 Lindholmen Science Park
 French High Committee for Civilian Defence
 Compagnie Industrielle des Lasers
 European Aeronautic and Space Company
 Totalförsvarets Forskningsinstitut (FOI)
 Foundation for Strategic Research
 Istituto Affari Internazionali
 Selex Galileo
 Catholic University of Louvain

COUNTRY

Sweden
 United Kingdom
 Czech Republic
 Germany
 France
 Sweden
 France
 France
 Germany
 Sweden
 France
 Italy
 Italy
 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 borders 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

COCAE's works focused on two areas. The first was to develop a high-energy resolution and efficiency image device. The second applied techniques to locate and identify the types of radiation sources in cargo or during emergency situations.

The project resulted in the design – but not the complete construction – of a portable spectroscopic instrument focused on

accurate identification and localization of radioactive sources. The instrument uses the Compton imaging technique, which deduces the energy of incident gamma ray photons and their origins by measuring energy depositions and the positions of Compton scattering interactions.

COCAE centered on the development of several core technologies

- » the growth of high purity, detector grade Cd(Zn)Te crystals and the development of the first high quality ingots in Europe
- » the creation of pixel detectors
- » development of pixel electronics capable of recording the spatial coordinates, time of conversion, and energy levels of converted photons
- » hybridization of the detectors, electronics, design, and

construction of an instrument to explore the capabilities of the proposed method of radioactive source localization and identification

The intermediate results of COCAE were focused on several sectors

- » Crystal growth of CdTe and CdZnTE crystals
- » Device processing using the p-i-n diode structure
- » Semiconductor technology for processing pixel detectors with 75 mm wafers
- » Read-out electronics for pixel detectors
- » Exploitation of the complete system

COCAE was tested via a large simulation effort and the development of algorithms. In the future, the project could potentially lead to the creation of a pan-European

PARTNERS

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

COUNTRY

Greece
 Greece
 Greece
 Finland
 Germany
 Spain
 Latvia
 Ukraine
 Ukraine

CREATIF / CBRNE related testing and certification facilities - A networking strategy to strengthen cooperation and knowledge exchange within Europe



**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

DECOTESSC1 / DEmonstration of COunterTErrorism System-of-Systems against CBRNE phase 1

© Marijijn 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.

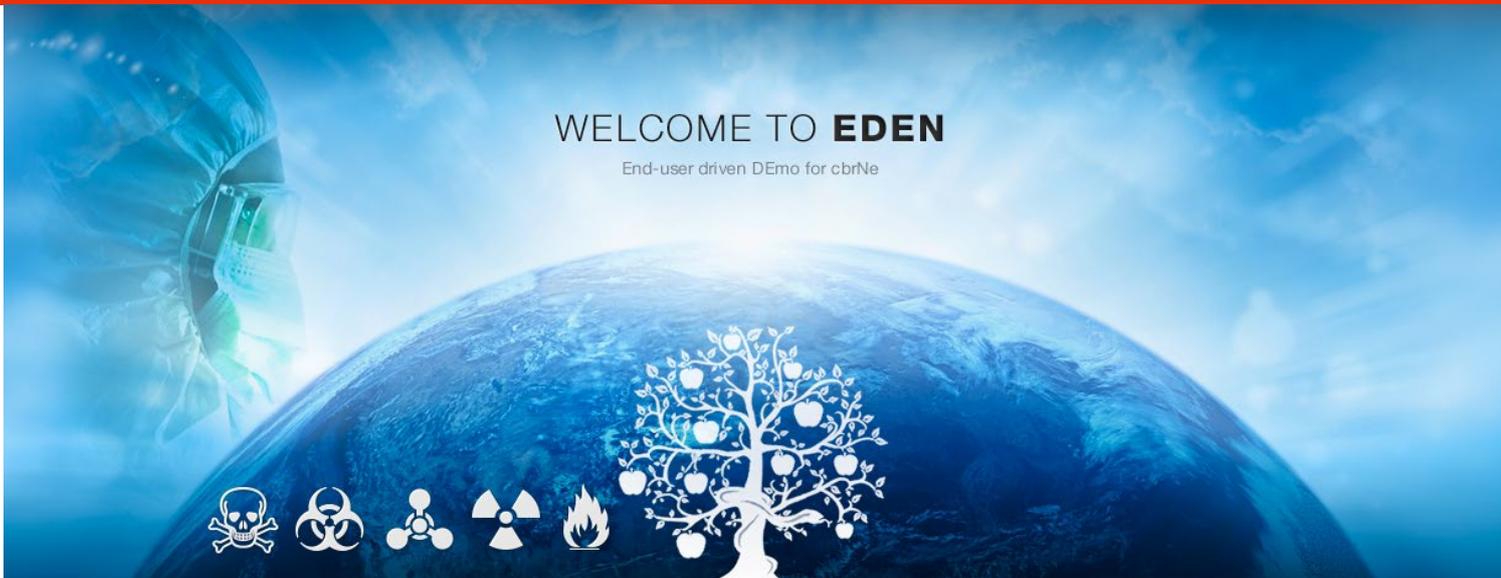
PARTNERS

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
AIT Austrian Institute of Technology GmbH (AIT)
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
Totalförsvarets Forskningsinstitut (FOI)
European Commission - Joint Research Centre (JRC)
Valtion Teknillinen Tutkimuskeskus (VTT)
Fundación Tecnalia Research & Innovation (TEC)
Seibersdorf Labor GmbH (SLG)

COUNTRY

The Netherlands
Austria
France
Germany
Sweden
Europe
Finland
Spain
Austria

EDEN / End-user driven DEMO for cbrNe



Information

Grant Agreement N°
313077

Total Cost
€36,075,401.17

EU Contribution
€24,826,823.91

Starting Date
01/09/2013

Duration
36 months

Coordinator

**BAE SYSTEMS
(OPERATIONS) LTD
(BAES)**

Electronic Systems
Airport works
T1F3
Rochester, ME1 2XX,
United Kingdom

Contact
Clive Goodchild
Tel: +44 (0)1634 204727
Mobile:
+44 (0)773 681 0656
Fax: +44 (0)1634 204715
E-mail: clive.goodchild@
baesystems.com

Project objectives

This project intends to raise the level of maturity of the resilience capacity of EU society when it comes to CBRNe events. The project will build on the results and successful completion of previous projects and will test in the field, through key demonstrations, the validity of the solutions sought. The 36 partners of the EDEN consortium will cooperate to achieve the development of a “multi-facetted system of systems approach” that will provide an EU-tailored solution able to enhance interoperability between CBRNe operators.

A distinctive feature of the EDEN project is the activation of its end-user, SME and suppliers’ platforms. These are open bodies where end-users, SMEs or industry external to the EDEN consortium can actively take part in the project with advice and feedback. Suppliers and SMEs can offer their equipment, technologies and services relevant for CBRNe contingency plans to the EDEN project for inclusion in the “EDEN Store” and for potential demonstration during the project.

Currently, the end user platform includes 60 end users from 20 countries, while the SME platform has 34 participants and the supplier platform has 19. All platforms are expanding their capabilities by recruiting new organisations via their contact points.

Description of the work

The strategy of the work plan has been conceived along three lines, namely to:

- » Allow end-users to pilot and control the whole process
- » Avoid replicating topics already covered in previous projects dealing with CBRNe and thus make best use of existing projects
- » Evaluate the achievements (services and performances) with concrete tests and trials essentially based on real environments and data to demonstrate affordable improvements in resilience.

The project has 4 major phases:

In the first phase end-users will define and specify the performances they need and baseline the current resilience of legacy systems. The initial societal, ethical and legal aspects will be considered.

In the second – main – phase the RTD partners will expand the PRACTICE system into the EDEN Store. Elements from other projects and new tools will be developed/ matured for the EDEN demonstrations.

The third phase will entail the preparation, system integration and execution of demonstrations. There will be a combination of small, medium and large scale demonstrations based on detailed scenarios.

The fourth phase is evaluation of the demonstrations, and the societal and exploitation activities.

To exploit feedback, these 4 phases will overlap to some extent.

Expected results

The EDEN project will provide solutions to improve CBRNe resilience and allow for enhanced interoperability and effectiveness between CBRNe operators to boost the resilience of EU society.

The EDEN solutions will demonstrate the added value of large scale integration of CBRNe counter-terrorism and security solutions by improving effectiveness, efficiency, coherence, and cooperation/coordination at the national, European and international levels.

As a result, Member States and their preparedness and response organizations, large operators and local populations and media will benefit from improved integration and information sharing in countering CBRNe threats. The project will develop a “Toolbox of Toolboxes” (ToT), accessible by an exchange platform: the EDEN Store. The ToT will leverage other EU-funded CBRNe projects as well as projects funded by national research programmes and the European Defence Agency while also including new tools when needed.

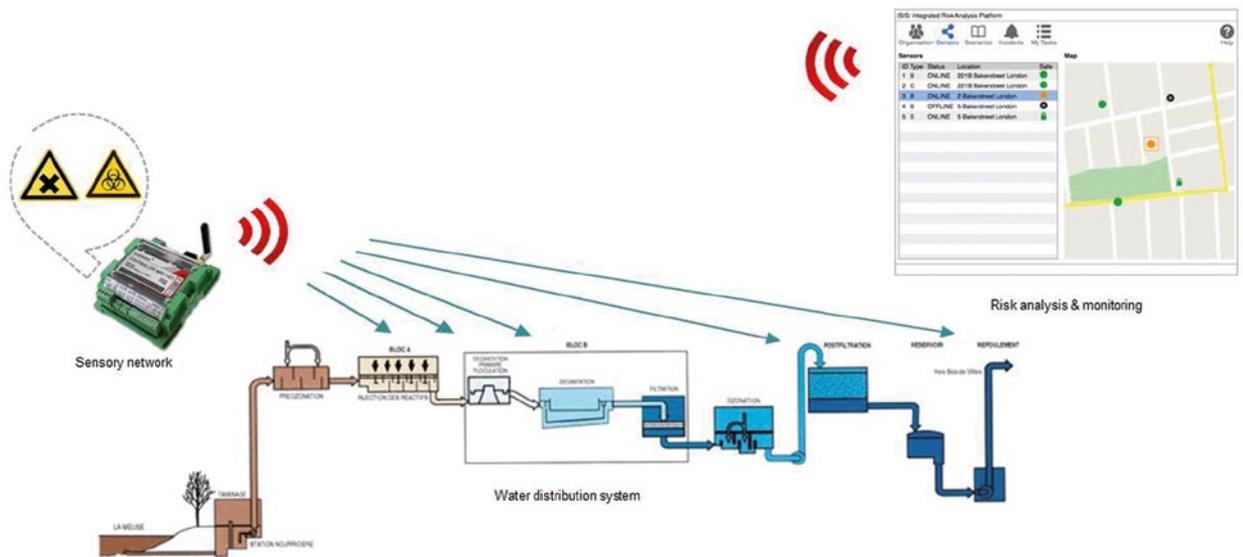
PARTNERS

European Commission (EC)
 BAE Systems (Operations) Ltd (BAES)
 Astrium SAS (AST)
 Forsvarets Forskninginstitut (FFI)
 Tecnoalimenti S.C.P.A (TCA)
 Selex ES SPA (SES)
 Université Paris XII Val de Marne (SAMU)
 Szkoła Główna Służby Pożarniczej (SGSP)
 Centre for Science, Society and Citizenship (CSSC)
 Astri Polska Sp. z o.o. (APL)
 Istituto Affari Internazionali
 CBRNE Ltd (CBRNELTD)
 Université Catholique de Louvain (UCL)
 LDI Innovation OU (LDI)
 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Teknologian Tutkimuskeskus VTT (VTT)
 Fondation pour la Recherche Stratégique (FRS)
 Indra Sistemas S.A.
 L'Institut National de l'Environnement Industriel et des Risques INERIS (INR)
 SICPA SA (SICPA)
 Magen Davis Adom in Israel (MDA)
 Przemysłowy Instytut Automatyki i Pomiarów PIAP (PIAP)
 HotZone Solutions Benelux BV (HZS)
 Agenzia Nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA)
 Societe NUCLETUDES SA (NUC)
 OMNIDATA S.A. (OMNI)
 Universidad del País Vasco EHU UPV (UPV/EHU)
 The University of Reading (UREAD)
 Bruker Daltonics Limited (BRU)
 Ldiamon AS (LDIAMON)
 Microfluidic Chipshop GMBH (MCG)
 Robert Koch - Institut (RKI)
 European virtual institute for integrated risk management (EU-VRI)
 Centrum Badan Kosmicznych Polskiej Akademii Nauk (SRC)
 Asociación de Investigación de la Industria Agrolimentaria (AINIA)
 Università Cattolica Del Sacro Cuore (UCSC)
 UMEA Universitat (UMU)
 Department of Health (PHE)

COUNTRY

Belgium
 United Kingdom
 France
 Norway
 Italy
 Italy
 France
 Poland
 Italy
 Poland
 Italy
 United Kingdom
 Belgium
 Estonia
 Germany
 Finland
 France
 Spain
 France
 Switzerland
 Israel
 Poland
 The Netherlands
 Italy
 France
 Romania
 Spain
 United Kingdom
 United Kingdom
 Estonia
 Germany
 Germany
 Germany
 Poland
 Spain
 Italy
 Sweden
 United Kingdom

ISIS / Integrated intelligent sensor system for improved security of water supplies



Information

Grant Agreement N°
312330

Total Cost
€4,790,621.90

EU Contribution
€3,484,929.00

Starting Date
01/01/14

Duration
36 months

Coordinator

C-TECH INNOVATION LTD + (CTECH)
Strategic Research
Unit 2 Capenhurst
Technology Park
CH1 6EH – Capenhurst –
United Kingdom

Contact
Domenico Cupertino
Tel: +44 151 347 2965
Fax: +44 151 347 2901
E-mail: dom.cupertino@
ctechinnovation.com
Website:
www.ctechinnovation.com

Project objectives

ISIS will provide public security by developing an advanced monitoring system for drinking water networks that instantly detects chemical or biological contamination and gives clear indication of the risk level.

Description of the work

The ISIS project will combine state of the art advances in four main areas: sensors, wireless networks, intelligent surveillance strategies and integrated risk analysis software.

Expected results

- » Sensors: develop four complementary innovative sensor methods. Each will have adaptable selectivity, through tailored sensing surfaces, so that collectively they can cover major potential contaminants, both chemical and biological
- » Wireless network: apply new methods to achieve effective sensor distributions within the constraint of existing water system architectures
- » Intelligent monitoring strategies: develop novel decision software to ensure the integrity of the monitoring system
- » Integrated risk analysis software: develop risk analysis software, which will be implemented in two ways.
 - (1) integrated into the monitoring strategy to provide a reliable model-based architecture;
 - (2) modelled on the existing architecture of water treatment and distribution systems in order to optimise the positioning and implementation of the sensor network.

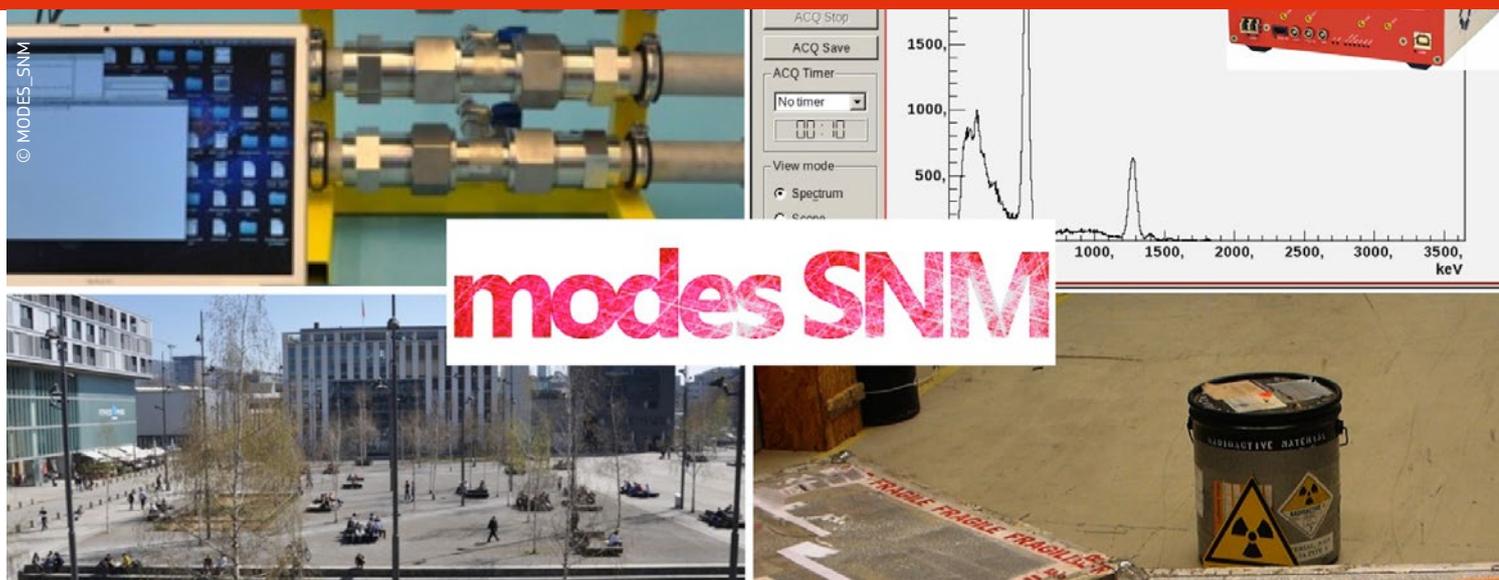
PARTNERS

- European Commission (EC)
- C-Tech Innovation Ltd. (CTECH)
- Kauno Vandenys Uab (KV)
- Vivaqua Scrl (VVQ)
- Cniguard Ltd (CNIG)
- Advantic Sistemas Y Servicios (ADVAN)
- Aleksandro Stulginskio Universitetas (ASU)
- Commissariat à L' Energie Atomique et Aux Energies Alternatives (CEA)
- Universitaet Wien (UNIVIE)
- Universita Degli Studi Di Roma Tor Vergata (UTOV)
- IOS International NV (IOS)

COUNTRY

- Belgium
- United Kingdom
- Lithuania
- Belgium
- United Kingdom
- Spain
- Lithuania
- France
- Austria
- Italy
- Belgium

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

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: +39 0498275933

Mobile: +39 3484115826

Fax: +39 0498275961

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

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

COUNTRY

Italy
 Switzerland
 Poland
 Switzerland
 Italy
 Italy
 Ireland
 United Kingdom

REWARD / REal-time Wide-Area RaDIation Surveillance System



© Andrea Dami, Benjamin Haas @ fotolia.com

Information

Grant Agreement N°

284845

Total Cost

€4,270,883

EU Contribution

€3,020,795

Starting Date

01/12/2011

Duration

36 months

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.

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/>

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

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

COUNTRY

Spain
 Spain
 Italy
 Germany
 Portugal
 Germany
 Portugal
 Italy

SAFEWATER / Innovative tools for the detection and mitigation of CBRN related contamination events of drinking water



Information

Grant Agreement N°

312764

Total Cost

€4,776,382.20

EU Contribution

€3,494,338.25

Starting Date

01/10/2013

Duration

39 months

Coordinator

ARTTIC (ART)

ARTTIC

58A rue du Dessous des

Berges

75013 Paris, France

Contact

Anna Ellinge Madar

Tel: +97233732010

Mobile: +972526604919

Fax: +9723732009

E-mail: elling@arttic.eu

Website: www.arttic.eu

Project objectives

The overarching aim of the SAFEWATER project is to develop a comprehensive and pragmatic platform to manage the safety and security of drinking water, reducing the time to react and effectively respond to a crisis. SAFEWATER will thus cover the detection, response, and recovery stages of potential events.

SAFEWATER will pursue the following objectives:

- » OB1: Improve preparedness through enhanced event detection capabilities, including virtual sensors machine learning algorithms and unsupervised learning capabilities to train the system;
- » OB2: Strengthen current response & recovery capacities of security and safety management systems for drinking water through a new generation of real-time decision support systems;
- » OB3: Develop new and improve current CBRN sensors for drinking water;
- » OB4: Develop adequately focused solutions for different usage contexts;
- » OB5: Optimise internal efficiency and external impact.

Description of the work

The SAFEWATER project will be driven by concrete usage cases corresponding to potential water security events. To make sure that the project is efficiently managed, the consortium will work according to common global milestones, which structure the project in a set of V1 solutions (Release 1 at midterm), including:

- » the integration and development of partial capabilities (sensors, system, and Event Management System);
- » Initial testing results, including a SAFEWATER user workshop and V2 solutions (Release 2 at the end of the project), including;
- » the integration and development of full capabilities (sensors, system, and Event Management System) based on the outcomes of testing and further technological developments;
- » physical trials;
- » final results culminating in a final workshop.

Expected results

The SAFEWATER solution fully covers the variety of drinking water security management situations (detection, response, and mitigation) and develops cutting-edge modelling methods, which will enable a near real-time overview of the water networks in large urban areas.

With the development of better and smarter technological solutions such as online CBRN detection, spatial modelling and look-ahead simulations, SAFEWATER will provide reliable tools for the management of drinking water crises.

During its second and final release of technology, SAFEWATER will provide adequate tools to enhance the online detection capabilities of the presence of contaminants in all water networks, and to effectively

alert crisis managers, decision makers, and the general public in due time.

Additionally, it will introduce a paradigm shift in the overall management of water quality parameters by investigating the domestic sensors solution – through the testing and selection of adequate low cost, and low maintenance sensors, and by adjusting the Event Detection System capacities to handle signals from a large number of distributed domestic sensors

The expected impact of SAFEWATER will, however, go far beyond water security: its open systems approach and deployed technologies will be useful for drinking water quality management in general. Indeed, aside from CBRN attacks perpetrated by malevolent actors,

whose probability is low, the contamination of drinking water by sewage or human error is more likely but no less disastrous. Thus SAFEWATER can respond to the needs of utilities to protect their networks from all kind of contaminations.

PARTNERS

ARTTIC (ART)
 Hagihon Company Ltd. (Hagihon)
 3S Consult GMBH (3S)
 Fraunhofer-Gesellschaft Zur Foerderung der Angewandten Forschung E.V (Fraunhofer IOSB)
 Aguas do Algarve, SA (AdA)
 Commissariat A L Energie Atomique et aux Energies Alternatives (CEA)
 ACREO Swedish ICT AB (ACREO)
 Decision Maker Ltd (DM)
 BioMonitech Ltd (BM)

COUNTRY

France
 Israel
 Germany
 Germany
 Portugal
 France
 Sweden
 Israel
 Israel

SCINTILLA /

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



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'ÉNERGIE ATOMIQUE ET**

**AUX ÉNERGIES
ALTERNATIVES**

DRT/LIST/ DCSI/ LCAE
CEA Saclay, Bât 516,
Point courrier 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

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

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

COUNTRY

France
 Belgium
 Italy
 Italy
 Hungary
 Germany
 France
 France
 United Kingdom

SECUREAU / Security and decontamination of drinking water distribution systems following a deliberate contamination

© SecurEau

RESEARCH
COMPLETED

Information

Grant Agreement N°

217976

Total Cost

€7,481,418.73

EU Contribution

€5,266,871

Starting Date

01/02/2009

End Date

31/01/2013

Coordinator

**UNIVERSITE HENRI
POINCARÉ - 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 modeling 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.

Results

The project developed sensors and specific contingency plans to identify and address the contamination of water in urban and rural water distribution networks.

SECUREAU achieved 10 important technological advancements:

1. sensors that detect any abnormal changes in water quality and provide assistance to the operator to manage the drinking water network
2. software that identifies the optimal location of water quality sensors and data treatment
3. mathematical models to find the optimal distribution of sentinel coupons
4. mathematical approaches to identify sources of contamination and the contaminated areas
5. CBRN pollutant analytical methods
6. modeling sorption and desorption to predict the spread of contamination
7. pipe wall cleaning and decontamination
8. methods of handling of decontamination sludge and water
9. verification of decontamination by deposits, biofilms or scale analysis, or by using sensor signals
10. decision tools within organizational frameworks and methodologies to follow in specific crisis situations.

Building on the above tasks during its fourth and final year, SECUREAU carried out experiments on wall deposits and biofilms to determine the kinetic parameters for absorption and desorption of contaminants, and methods for decontaminating water and cleaning pipes. It also used software to model the contamination of drinking water networks and identify contamination sources.

Finally, the research team installed two networks – one rural, one urban – comprised of 40 sensors to collect field information and to create an early warning system of contamination.

PARTNERS

Université Henri Poincaré – Nancy 1 (UHP)
 Centre National de la Recherche Scientifique (CNRS)
 Veolia Environnement Recherche et Innovation (VERI)
 Rheinisch-Westfälisches Institut für Wasserforschung gemeinnützige GmbH (IWW)
 University of Southampton (SOTON)
 Faculdade de Engenharia da Universidade do Porto (FEUP)
 Riga Technical University (RTU)
 Centre national du Machinisme Agricole, du Génie Rural, des Eaux et des Forêts (CEMAGREF)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Monitoring Systems Ltd. (MSystems)
 Veolia Water Central (VWC)
 Radiation and Nuclear Safety Authority (STUK)
 Kelda Group PLC (YWS)
 National Institute for Health and Welfare (THL)

COUNTRY

France
 France
 France
 Germany
 United Kingdom
 Portugal
 Latvia
 France
 France
 United Kingdom
 United Kingdom
 Finland
 United Kingdom
 Finland

SNIFFER /

Securing the food chains from primary production and animal feeds to consumer-ready food against major deliberate, accidental or natural CBRN contamination.

© Thinkstock



Information

Grant Agreement N°

312411

Total Cost

€3,632,513

EU Contribution

€2,720,029

Starting Date

01/05/2013

Duration

36 months

Coordinator

TEKEVER ASDS (TEK)

TEKEVER ASDS

Rua das Musas 3.30

1990-113, Lisboa

Portugal

Contact
André Oliveira

Tel: +351 213 304 300

Fax: +351 213 304 301

E-mail:

andre.oliveira@tekever.com

Project objectives

Project SNIFFER envisions the design and development of a network of distributed detection devices, capable of rapid, on-site detection of multiple kinds of agents and CBR agents with high sensitivity and specificity throughout the most vulnerable stages of the food supply chain (such as farms, large collection centers, wholesalers, etc...).

The project will address both available sensor technology and new, complementary sensor devices that shall be used for the detection of hazardous CBR agents within the food supply chain. The sensor devices to be developed are characterised by their portability, ease of use and reusability. Another important feature of the new device will be its modular design, i.e. the device is formed by several independent modules (sensors, communication device, on-board computing, etc), combined through generalized and standardized connections.

The network of sensor devices will be designed as a centralised architecture, in which all the data from the devices will be sent to a command center. An operator of the SNIFFER system will also have the ability to remotely control and command the sensor devices using a specific interface from the command center.

Project SNIFFER also envisions the creation of a set of guidelines, which presents the countermeasures and procedures that shall be used within the European Union whenever a food or feed borne incident is detected within the food supply chain. The guidebook will provide help to the appropriate entities in employing the corrective counter-measures in order to mitigate, restrain or ultimately eradicate the hazardous agent.

The aforementioned objectives of the project will be directed to achieve the final goal of providing means of countermeasure to mitigate a possible incident of CBR

health hazardous agents in the food supply chain and to increase the security within all the steps that constitute the food supply chain.

Description of the work

The SNIFFER consortium has established a precise and main objective for this project which is to:

» Increase the security of the food supply chain by developing a network of detection devices to detect CBR agents introduced in food either by accidental, natural or intentional means.

This achievement will be pursued by providing specific outcomes from the activities identified below:

» Development of a new sensor (MIPs technology) with a faster detection time, and improved re-usability

» Combination of MIPs with fluorogenic probes to reduce false positive rates and improve sensor robustness

» Provide the capability to network different sensors at different stages/locations of the food supply chain (vertical and horizontal dimensions)

» Development of the capability to improve the quality of detection through data fusion

» Definition of a set of sample preparation procedures

» Definition of a set of recommendations to policy makers (specific recommendations to food security agencies and European authorities)

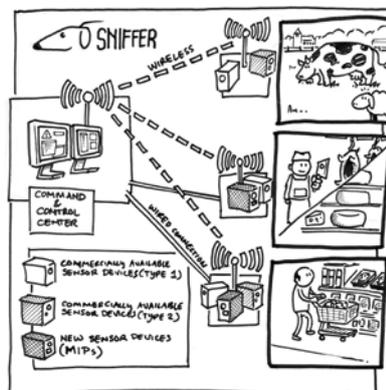
» Definition of a set of scenarios specifically adapted to food supply chain and the SNIFFER validation methodology

Expected results

The capability to network different devices with different functionalities (i.e. capable of detecting different agents) throughout the entire food supply chain will undoubtedly reduce the detection time (the time between contaminating a specific food and detecting this contaminated food somewhere along the chain) of contaminant agents, introduced either deliberately, accidentally or through natural sources.

By providing users with the ability to perform tests at any stage across the entire food chain (which is basically already possible but not with the technology proposed in SNIFFER), the probability of detecting contamination earlier will increase.

Additionally, the faster detection time and higher rate of re-usability introduced by the MIPs technology will enable users to perform more tests/hour and wait less time for the results which again results directly in lower detection times.



PARTNERS

- Tekever ASDS (TEK)
- Ministério da Defesa Nacional (LBDB)
- Umea Universitet (UMU)
- INESC Porto – Instituto de Engenharia de Sistemas e Computadores do Porto (INESC)
- Universidad de Burgos (UBU)
- Osterreichische Agentur für Gesundheit und Ernährungssicherheit (AGES)
- Centre Suisse d’électronique et de microtechnique SA – Recherche et developpement (CSEM)
- Forvarets Forskninginstitut (FFI)

COUNTRY

- Portugal
- Portugal
- Sweden
- Portugal
- Spain
- Austria
- Switzerland
- Norway

SPICED / Securing the spices and herbs commodity chains in Europe against deliberate, accidental or natural biological and chemical contamination

© BFR



Information

Grant Agreement N°

312631

Total Cost

€4,586,455.60

EU Contribution

€3,499,942.35

Starting Date

01/07/2013

Duration

36 months

Coordinator

FEDERAL INSTITUTE FOR RISK ASSESSMENT (BFR)

Department Biological Safety

Max-Dohm-Straße 8-10
Postfach 126942, 10609
Berlin
10589 Berlin
Germany**Contact****Prof. Dr. Bernd Appel**

Tel: +49 30 18412 2151

Fax: +49 30 18412 2951

E-mail:

spiced@bfr.bund.de

Website: www.spiced.eu**Project objectives**

Securing food chains against deliberate, accidental or natural contaminations is directly related to the safety of food products.

Many alerts from European countries via the Rapid Alert System of Food and Feed (RASFF) over the past years have included spices and herbs. Additionally, these components are contained in almost every processed food, including ready-to-eat products. Thus consumers can be directly exposed to contaminated spices and herbs. There is a need to monitor these commodities. SPICED's objectives are to:

- » characterize the heterogeneous matrices of spices and herbs and their respective production and supply chains regarding relevant biological and chemical hazards that can lead to major deliberate, accidental or natural contaminations in the food supply chain;
- » improve the knowledge of biological hazard properties as well as on-site and high throughput diagnostic methods for appropriate detection;
- » reduce (industrial) chemical adulterations and ensure authenticity of spices and herbs by evaluating and improving non-targeted fingerprinting methods;
- » improve alerting, reporting and decontamination systems as well as techniques to ensure prevention and response on high quality level.

The consortium will evaluate the most important spices and herbs that could be the source for natural, accidental or deliberate contaminations.

Description of the work

WP1, "Management and Coordination", includes scientific management and assessment of progress and results, financial and administrative management, intra-consortium communication and management of gender issues.

WP2, "Matrix Chains and Modelling", will systematically collect and evaluate information about spices and herbs production steps and the potential hazard of contamination. Vulnerable points along the spices and herbs production chain will be identified. An evaluation of various parameters will determine the risks and the potential of possible interventions.

WP3, "Biological Hazards", will improve the knowledge about microorganism properties (e.g. tenacity) and their detection. Current microbiological and molecular techniques, including existing sample preparation, purification and detection methods will be investigated for the development of reliable and standardized cultural, on-site screening as well as high throughput approaches. A database will be created to include data on biological hazard properties and diagnostic methods.

The aim of WP4, "Chemical Hazards", is to develop a rapid and cost-efficient set of methodologies for the detection of spices and herbs contamination with (unexpected) chemical agents. Fingerprinting data will be used to develop and evaluate various chemometric (one-class) classification techniques that allow distinguishing authentic (non-adulterated) samples from adulterated/contaminated samples.

In WP5, "Prevention and Response", alerting and reporting systems and decontamination techniques will be investigated, with recommendations to be published. Moreover, a guideline for differentiation between natural and intentional incidents will be developed.

WP6, "Sustainability and Dissemination", deals with the dissemination of knowledge to the public, governmental institutions and scientific and industrial communities.

Expected results

The SPICED project will lead to a better and more comprehensive view of the heterogeneous matrix of spices and herbs. Its approach should lead to improved food safety and food security aspects in the spices and herbs food chain, and to reduce human casualties and the economic impact. The EU level of expertise in this field will be significantly increased.

PARTNERS

Federal Institute for Risk Assessment (BfR)
 Austrian Agency for Food and Health (AGES)
 Institute of Food Safety, Animal Health and Environment (BIOR)
 DLO foundation - RIKILT (DLO)
 Fuchs Gewürze GmbH (FUCHS)
 National Agricultural Research and Innovation Center (KEKI)
 RTD Services (RTDS)
 University of Limerick (UL)
 National Agricultural and Food Center (VÚP)
 Bundeswehr Research Institute for Protective Technologies & NBC-Protection (WIS)
 Wageningen University (WU)

COUNTRY

Germany
 Austria
 Latvia
 The Netherlands
 Germany
 Hungary
 Austria
 Ireland
 Slovakia
 Germany
 The Netherlands

TAWARA_RT M / Tap Water Radioactivity Real Time Monitor



Information

Grant Agreement N°

312713

Total Cost

€3,414,864.80

EU Contribution

€2,564,554.00

Starting Date

01/12/2013

Duration

30 months

Coordinator

UNIVERSITA' DEGLI

STUDI DI PADOVA

(UNIPD)

Department of Physics and

Astronomy

via Marzolo, 8

I-35131 – Padova - Italy

Contact

Marcello Lunardon

Tel: +39 049 827 5643

Fax: +39 049 827 7102

E-mail:

marcello.lunardon@unipd.it

Website: www.tawara-rtm.eu

Project objectives

The main purpose of the TAWARA_RT M project is to create a platform for drinking water security against deliberate or accidental radiological or nuclear threats.

This goal will be pursued by targeting the needs of the Warsaw Waterwork Company MPWIK, but it will be easily adapted to other large municipalities in Europe and abroad.

The proposed prototype will be composed of two main radioactivity detection systems: a real-time monitor system (RTM) for the measurement of the gross alpha and beta activity in the water, and a spectroscopic system (SPEC) for the identification of the radioactive contaminant by exploiting the recognition of its characteristic gamma lines. An additional gamma detection system for early alarm in case of strong radioactive contaminations of raw water will be added to the monitoring network in order to preserve as much as possible the water treatment plant by blocking the contaminated water at its intake.

As required in the call topic, the project will cover the development, assessment, demonstration, deployment and monitoring phases of the new monitoring system at the North Warsaw site where the prototype will be deployed.

TAWARA_RT M's mechanical lay-out, electronics architecture and information system will be specifically conceived for easy integration of additional specialized sensors for chemical or biological threats.

In this way TAWARA_RT M will offer a system for real time on-site monitoring of water quality that will be useful in the following tasks:

- » early warning in case of changes in the radioactive content of water and time reading of the changes;
- » fast alarm for crossing thresholds that require rapid

actions for the tap water distribution system;

- » in case of alarm, starting the spectroscopic investigation to determine the type of contamination and decide the appropriate and effective countermeasures (response and mitigation measures).

Description of the work

Starting from the project consortium's pre-existing know-how regarding the use of scintillation detectors in nuclear physics applications, TAWARA_RT M's work plan foresees first an R&D phase where available detectors and technologies will be optimized for integration into this new application.

The relevant tasks comprise:

- » design and production of TAWARA_RT M's prototype RTM detector to continuously measure on site the water's gross alpha and beta activity. The detector is based on an array of commercially available plastic scintillators that distinguish between alpha and beta signals. However, these kind of detectors have never been used so far for such application. The optimal read-out scheme and a suitable water-protection and functionalization treatment of the scintillator surface will be realized during the initial R&D phase of this task. Moreover, the additional gamma detection system for early alarm in case of strong radioactive contamination will be developed and tested in this phase.
- » design and production of a low-background gamma spectroscopy system attached to a chemical concentration system (SPEC) that will analyse the water after a triggered RTM alarm, thus providing information on the nature of the radioactive contaminant. New-generation inorganic gamma scintillation crystals will be evaluated in order to guarantee the expected sensitivity in the required timescale.

» design of compact front-end electronics based on CAEN know-how on digital pulse processing and radiation detector power supply systems.

» dedicated software for the automatic control of the prototype and analysis of raw data will be developed. It will be coupled to a suitable ICT infrastructure for collecting information from all monitoring nodes scattered along the tap water plant, allowing complete supervisory control via a remote web interface. The operator will be alerted in case of alarm from any of the nodes and will be able to inspect and configure each node.

The second phase of the project foresees integration of the previous tasks' results, a complete characterization test of the prototype at the Italian National Institute of

Ionizing Radiation Metrology of ENEA and final installation and demonstration phase at the Warsaw Waterwork Company site.

Expected results

Improve drinking water security against deliberate or accidental radiological or nuclear threats via a new real-time alpha and beta radioactivity monitor system installed at water treatment plants.

Improve water plants' protection by offering the possibility of quickly blocking water flow at intake points in case of strong radioactive contamination.

PARTNERS

Università degli Studi di Padova (UNIPD)
 Costruzioni Apparecchiature Elettroniche Nucleari C.A.E.N. SpA (CAEN)
 SCIONIX Hollande BV (SCIONIX)
 Narodowe Centrum Badan Jadrowych (NCBJ)
 Agenzia Nazionale per le Nuove Tecnologie, l'Energia e lo Sviluppo Economico Sostenibile (ENEA)
 Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w M. St. Warszawie Spółka Akcyjna (MPWIK)
 Università di Pisa (UNIFI)
 Wardynski i Wspólnicy SPK (WIW)

COUNTRY

Italy
 Italy
 The Netherlands
 Poland
 Italy
 Poland
 Italy
 Poland

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);

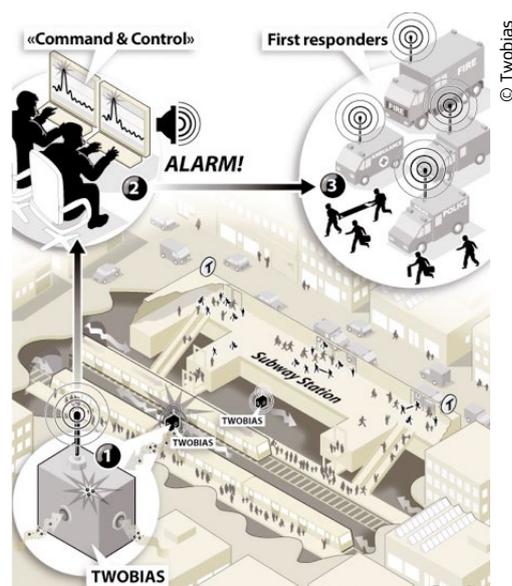
» **StageTWO:** Second alarm based on highly automated microfluidic-based platform with a molecular BIU (detect-to-treat).

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.



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

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

[idusconsultancy.co.uk](http://avertproject.eu/)

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.

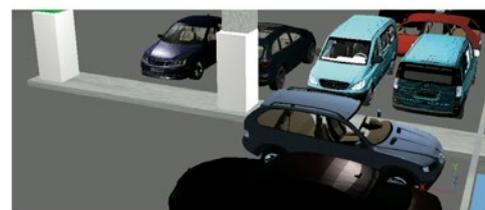
Description of the work

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

BONAS / B0mb factory detection by Networks of Advanced Sensors

© Robert Reich - istockphoto.com



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 TECNO- LOGIE, 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.



PARTNERS

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

COUNTRY

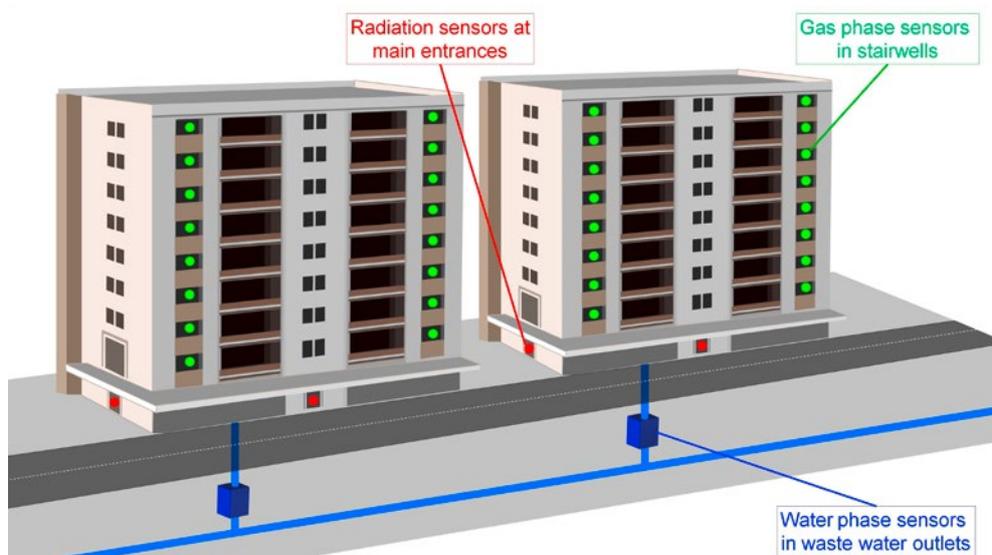
Italy
Italy
Sweden
Portugal
Estonia

Switzerland
Germany
France
France
Switzerland
Finland
United Kingdom
France
United Kingdom

COMMONSENSE /

Development of a Common Sensor Platform for the Detection of IED “Bomb Factories”

© Created by Hugh Doyle, Tyndall National Institute, 2011



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 interferences.

PARTNERS

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

COUNTRY

Ireland
 Israel
 United Kingdom
 United Kingdom
 Germany
 Ireland
 France
 United Kingdom

D-BOX / Comprehensive toolbox for humanitarian clearing of large civil areas from anti-personal landmines and cluster munitions



Information

Grant Agreement N°

284996

Total Cost

€9,909,587.90

EU Contribution

€6,898,085.95

Starting Date

01/01/2013

Duration

36 months

Coordinator

Astrium SAS (ASTRIUM)

ASTRIUM SPACE TRANSPORTATION

51-61 route de Verneuil

PO Box 3002

78133 Les Mureaux

France

Contact

Bruno Esmiller

Tel: +33 1 39 06 29 66

Mobile: +33 6 15 18 39 97

Fax: + 33 1 39 06 14 40

E-mail: bruno.esmiller@astrium.eads.net

www.d-boxproject.eu

Website:

www.d-boxproject.eu

Project objectives

Landmines and cluster munitions continue to kill or maim civilians every day in countries all around the world, even long after conflicts are over. Assuming no additional mines are laid from now on, at the current rate of clearance of some 500,000 mines per year it could still take hundreds of years to find and clear all the landmines around the world.

D-BOX will tackle this burning issue of anti-personal landmines and cluster munitions inherited from armed conflicts. This will be achieved through the development of innovative solutions that will be interfaced and integrated in a comprehensive toolbox to provide demining stakeholders with the best tools, methods and procedures for:

- » Mapping and localization (long distance) of hazardous areas
- » Close-in detection (short distance)
- » Risk management
- » Human, ethical and legal factors (including procedures and best practices)
- » Neutralization of anti-personal landmines and cluster munitions in an open and civil environment,
- » Protective equipment for operators and population
- » Training solutions for personnel

This “smart” toolbox could be used during all demining activities (from the mission’s preparation to the elimination of mines, including communication to general public and donors). It could also help operators and end users get the most suitable answers to technical problems

and, finally, find the lowest cost and “easy to use” tools for specific tasks during demining activities that are adapted to different scenarios and conditions.

D-BOX Toolbox will help them choose the most suitable solutions, taking into account the environment (terrain, vegetation, age of mines, local population, culture, etc.) and thus enabling an optimization of operations in the field faster demining and a lower cost per square meter.

Description of the work

The development of D-BOX is mainly based on the assessment of past and ongoing activities and legacy tools. Completion of the project concept will lead to development of the actual D-BOX Toolbox. Before populating the latter with real functions (tools and procedures), an advanced information system will be developed to organize the Toolbox. This will provide an easily understandable user interface for access to all functions in the Toolbox, where data collection will be very important.

In parallel, innovative tools, methods and procedures will be developed or improved in the following domains: human, ethical and legal factors, mapping and localization of hazard zone, close-in detection, neutralization in a civil environment, protective equipment for personnel and population, training solutions and mine risks population education.

The Toolbox’s components will be carefully tested tool by tool, by function and as groups of functions. Finally, an assembled complete version of the integrated Toolbox will be subject to full scale field validation via different relevant demining scenarios.

End users and stakeholders will provide their experience and requirements during the whole process from concept design, Toolbox development, development of information and training kit to the Toolbox’s testing and validation.

When needed, the industrial stakeholder platform will be called upon to carry out integration, modifications and development of technology.

Expected results

The D-BOX Toolbox will significantly increase the humanitarian demining capability. It will be modular and upgradable, and its deployment will be adapted to each situation and user.

It will provide various toolboxes with different complexity and completion to be used in different places by a variety of users. Furthermore, the D-BOX solution will improve significantly demining productivity and safety by increasing the current rate of clearance and cost-effectiveness. It will also allow for more effective application of solutions that encompass simple and advanced technologies.

The D-BOX Toolbox will meet the most recent needs of demining stakeholders: mapping of hazard zone and close-in detection with low cost and easy to use tools.

The D-BOX Toolbox will tackle the main challenges for the development of new de-mining technologies:

- » the tremendous diversity of environmental conditions in which landmines are employed and the variety of these mines and cluster munitions
- » different training levels, cultural backgrounds, and educational levels of deminers
- » detection of mines made with plastic and low metal content, while at the same time discriminating them from non-explosive debris.

PARTNERS

Astrium SAS (ASTRIUM)
 Astri Polska Spolka z ograniczona odpowiedzialnoscia (APL)
 Bactec International Limited (BACTEC)
 CBRNE Limited (CBRNE)
 Comité Européen de Normalisation (CEN)
 Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)
 Technische Universiteit Delft (TUD)
 Totalforsvarets Forskningsinstitut (FOI)
 Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V (FRAUNHOFER)
 Infoterra Limited (INFOTERRA)
 Instytut Technologii Bezpieczeństwa MORATEX (MORATEX)
 Consorzio Università Industria – Laboratoria di Radiocomunicazioni RADIOLABS (RADIOLABS)
 Selex ES S.P.A. (SELEX)
 TerraSpatium SA (TERRASPATIUM)
 Telespazio SPA (TELESPAZIO)
 Netherlands Organisation for Applied Scientific Research (TNO)
 University of Surrey (SUR)
 Teknologian Tutkimuskeskus VTT (VTT)
 University of Leicester (ULEIC)
 e-GEOS S.p.A. (E-GEOS)

COUNTRY

France
 Poland
 United Kingdom
 United Kingdom
 Belgium
 Italy
 The Netherlands
 Sweden
 Germany
 United Kingdom
 Poland
 Italy
 Italy
 Greece
 Italy
 The Netherlands
 United Kingdom
 Finland
 United Kingdom
 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.

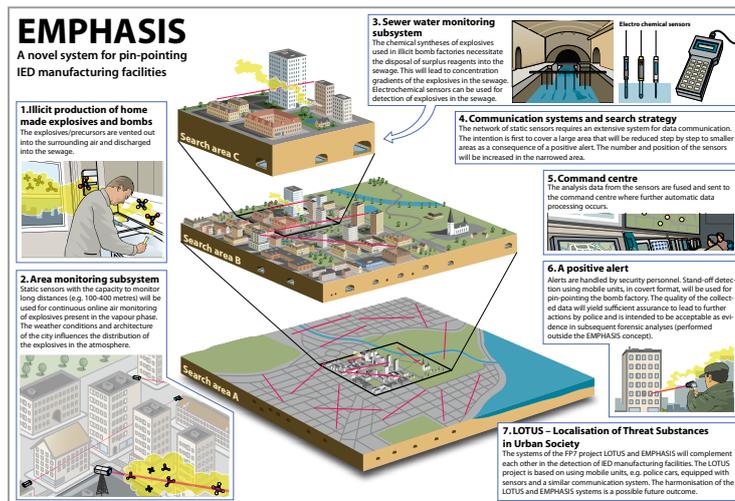
One of the advantages of the EMPHASIS system is the fact that many of the developments achieved in another FP 7 project, LOTUS, can be benefited from. Data and developments can be implemented as much as possible e.g. exploitation of knowledge obtained concerning the central command, threat substance 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.



PARTNERS

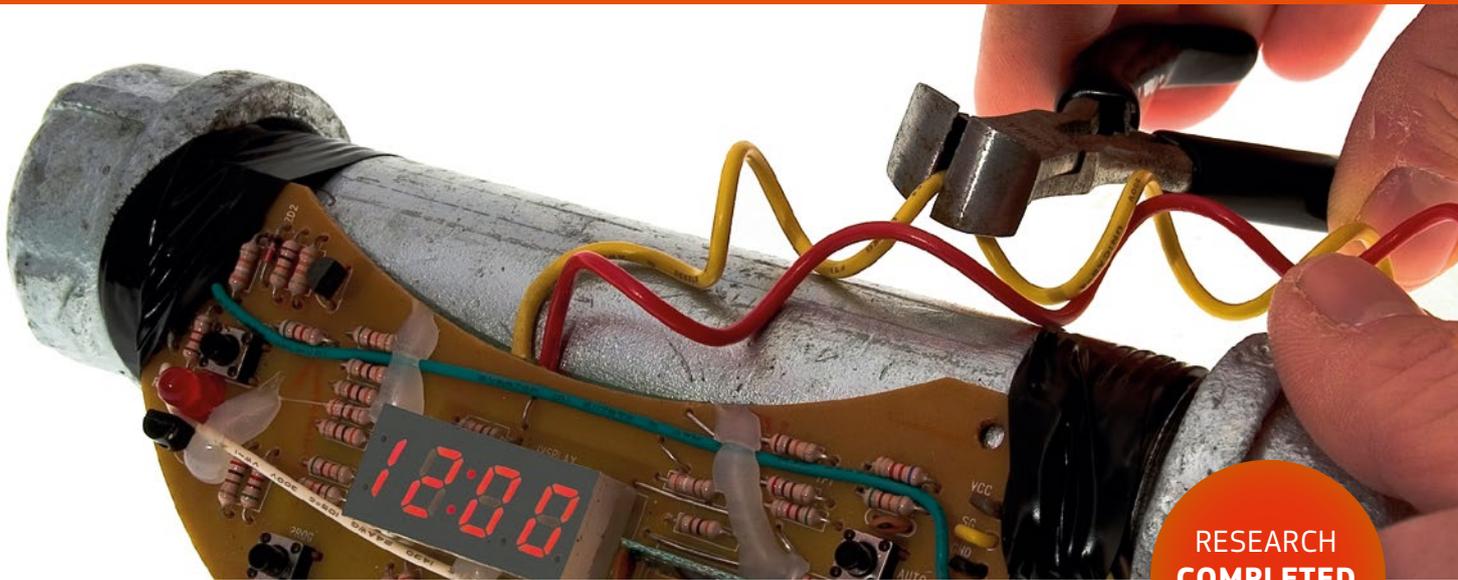
Totalförsvarets Forskningsinstitut (FOI)
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT-IAF)
Portendo AB (Portendo)
Cascade Technologies Ltd (Cascade)
Morpho (MPH)
Institut National de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

COUNTRY

Sweden
The Netherlands
Germany
Sweden
United Kingdom
France
France
Poland

ENCOUNTER / Explosive Neutralisation and Mitigation Countermeasures for IEDs in Urban/Civil Environment

© istockphoto


**RESEARCH
COMPLETED**
Information

Grant Agreement N°
285505

Total Cost
€4,412,123

EU Contribution
€3,313,630

Starting Date
01/05/2012

End Date
31/08/2015

Coordinator

**SWEDISH DEFENCE
RESEARCH AGENCY
(FOI)**

Department of Physical
Protection and Weapons
Effects
Grindsjön Research Centre
SE-14725 Tumba, Sweden

Contact

Pernilla Magnusson
Tel: +46-8 5550 3939
Mobile: +46 709277209
Fax: +46 855504180
E-mail:
pernilla.magnusson@foi.se
encounter@foi.se
Website:
<http://www.encounter-fp7.eu>

Project objectives

The ENCOUNTER project will consider threats from Improvised Explosive Devices (IED) in the urban environment. The project objectives are to:

- » Increase urban security through improved procedures for dealing with an IED.
- » Prevent IED explosion after discovery through new technologies for their neutralisation. This would mean most people need never be aware an IED was present, reducing the impact of the IED in achieving the terrorists' aims.
- » Drastically reduce damage if the IED is triggered, through development of explosion-mitigating and fragment-prevention technologies. This will enable the urban environment to 'bounce-back' to normal life as quickly as possible.
- » Consider the ethical, societal and financial aspects of new ways to dealing with IEDs to ensure the response is in proportion to the threats, and that the response does not create any additional problems.

In summary, the ENCOUNTER project will identify, explore and validate existing and innovative techniques for mitigation and neutralisation of already discovered IEDs in the urban/civil environment. The results will be summarised in a recommendation matrix and used to develop a software tool to assist clearing forces.

Description of the work

The concept of the ENCOUNTER project is based on:

Review of practices and state of the art.

This part deals with the operational and technical aspects associated with the neutralisation of IEDs and the actions and means that mitigate the damage they will cause if detonated:

- » Review of the practices, policies and procedures of the police and security units responsible for Explosive Ordnance Disposal (EOD).
- » State of the art review of the existing technologies for neutralisation of IEDs and the means and tools for the mitigation of damage.
- » Identification of scenarios and design basis threats for the work packages focusing on R&D and on the examination and evaluation of technologies.

Development of technological capacities in two areas:

- » Development and assessment of IED neutralisation technologies and assessment of EOD response bodies' practices.
- » Development and assessment of damage mitigation means and decision support tools for EOD response bodies.

Ethical and societal aspects.

Consider the ethical, societal and financial aspects of new ways to deal with IEDs to ensure the response is in proportion to the threat, and that the response does not create any additional problems. This will:

- » Give stakeholders guidelines for evaluating and improving acceptance of IED neutralisation techniques

- » Reduce worries of citizens regarding the application of IED neutralisation
- » Understand how techniques are perceived and which techniques have a positive impact on the population's perception of security
- » Cost-benefit assessment of the technologies used for IED mitigation and neutralisation

Experiments, tests and evaluation.

Review, tests and evaluation of the range of means, tools and practices that will be developed within the framework of the project's R&D work packages. This includes tests of neutralisation technologies and IED damage mitigation experiments in the laboratory and

field conditions, with the use of live IEDs.

Results

The project outcome will describe the practices, tools and procedures for neutralising (N) or mitigating (M) the effects of IEDs and how to respond appropriately and effectively to the threat they present in the urban environment. The N/M technologies will be assessed in relation to the threat and their effectiveness in dealing with the various scenarios that EOD bodies and police units address.

The capability to review and evaluate the various technologies in relation to the concept of operation (CONOP) of the EOD bodies and the police units operating in the urban environment will be developed.

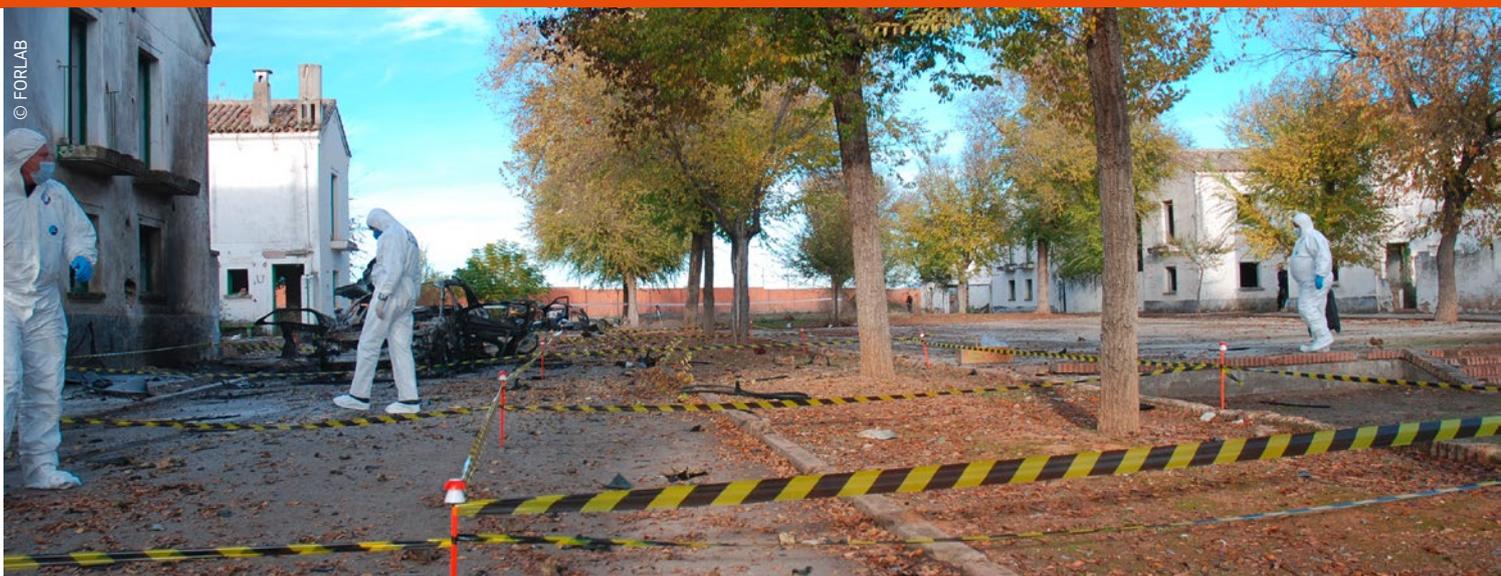
PARTNERS

Totalförsvarets forskningsinstitut (FOI)
 Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung E.V (EMI)
 The University of Sheffield (USFD)
 Ingenieria de Sistemas Para La Defensa de Espana SA (ISD)
 Tamar Israeli Advanced Quarrying Co Ltd (TMR)
 Albert-Ludwigs-Universität Freiburg (ALU-FR)
 Blastech Ltd (BLT)

COUNTRY

Sweden
 Germany
 United Kingdom
 Spain
 Israel
 Germany
 United Kingdom

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



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

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

COUNTRY

Spain
 Italy
 France
 Greece
 Belgium
 Poland
 Finland
 Italy
 Poland
 France
 Spain
 France

HOMER / Homemade explosives (HMEs) and recipes characterisation - Capability



Information

Grant Agreement N°

312883

Total Cost

€4,474,991.50

EU Contribution

€3,436,875.00

Starting Date

01/11/2013

Duration

36 months

Coordinator

POLICE SERVICE OF NORTHERN IRELAND

Una Williamson

Head of EU Programme Office

65 Knock Road

Belfast

BT5 6LE

Contact

Una Williamson

Tel: +44 (0)28 90 90 1155

Mobile: +447734909685

E-mail: una.williamson@

psni.pnn.police.uk

Website:

www.homer-project.eu

Project objectives

The goal of the HOMER project is to implement a study to mitigate the threat of home made explosives (HMEs) from criminal and terrorist elements.

The objectives of the HOMER project are to:

1. Expand the knowledge of European bodies: map and analyse the sources of information that instruct how to prepare HMEs, the required raw materials and precursors, their technical characteristics and the possibilities of their detection using existing technologies.
2. Mitigate the threat presented by HMEs: expand and enhance knowledge on HMEs to serve security and law enforcement agencies in their quest to prevent the use of HMEs to perpetrate attacks.
3. Work to prevent the use of HMEs: detect and classify HMEs in instances when they are used.
4. Deliver sustainable HME content for use: a knowledge management platform – securely accessible by security and law enforcement agencies – flowing from our study.
5. Draft a standard on HME vocabulary and definitions suitable for Europe.
6. Promote the work of the project.

Description of the work

The HOMER project will implement a comprehensive, European study on HMEs including their identification and detection and the prevention of HME threats. The

project will establish basic knowledge hitherto unknown about HMEs and develop a knowledge management platform for use by European police and security services to protect the safety of the EU citizen.

The Project has four main pillars:

Data Collection and Analysis. This work area focuses on the collection and analysis of HME information using a HME literature study and internet empirical study to mine and collect publicly available information on HME recipes to establish answers for the most fundamental questions on HMEs. Data collection will also gather information from industry best practices, expert knowledge within the HOMER consortium and experts across Europe.

Knowledge Management focuses on the sustainability of HME knowledge content relating to manufacturing methods, technical characteristics of HMEs, the required raw materials and their impact, detection and classification. This information will be folded into a knowledge management platform to serve law enforcements agencies, European defence and manufacturers.

Case study experiments and validation will demonstrate the use of the project's research for detecting and classifying the HME data. This pillar will involve the project's main end users for developing case studies to test the platform and the information in laboratory conditions and in the field.

Standardisation, dissemination and exploitation will deliver a standardised HME vocabulary and definitions across precursor manufacturers, security providers and law enforcement agencies. This work will provide a recognised standard of vocabulary to assist agencies in working collaboratively to defeat the HME threat.

Expected results

The HOMER project will deliver three main results:

1. A measured step towards a common HME knowledge management base for Europe's law enforcement, security, defence and manufacturers of fertilisers and chemicals.
2. Better knowledge of the chemicals involved in HMEs, and their components and composition.
3. End user access to HME researched content, strengthening their innovation capacity.

The detection of detonators and chemical compositions for bomb making is crucial for homeland security, environmental clean-up and humanitarian efforts.

PARTNERS

POLICE SERVICE OF NORTHERN IRELAND
 TAMAR ISRAELI ADVANCED QUARRYING CO LTD.
 THE PROVOST, FELLOWS, FOUNDATION SCHOLARS & THE OTHER MEMBERS OF BOARD
 OF THE COLLEGE OF THE HOLY & UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN
 BUNDESANSTALT FUER MATERIALFORSCHUNG UND-PRUEFUNG
 BULGARIA DEFENSE INSTITUTE
 THE QUEEN'S UNIVERSITY OF BELFAST
 CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS
 KENTRO EREVNON NOTIOANATOLIKIS EVROPIS ASTIKI MI KerdoskopiKI ETAIREIA
 YARA SA
 MINISTERIO DEL INTERIOR

COUNTRY

United Kingdom
 Israel
 Ireland

 Germany
 Bulgaria
 United Kingdom
 Greece
 Greece
 Belgium
 Spain

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 Önnnerud

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.

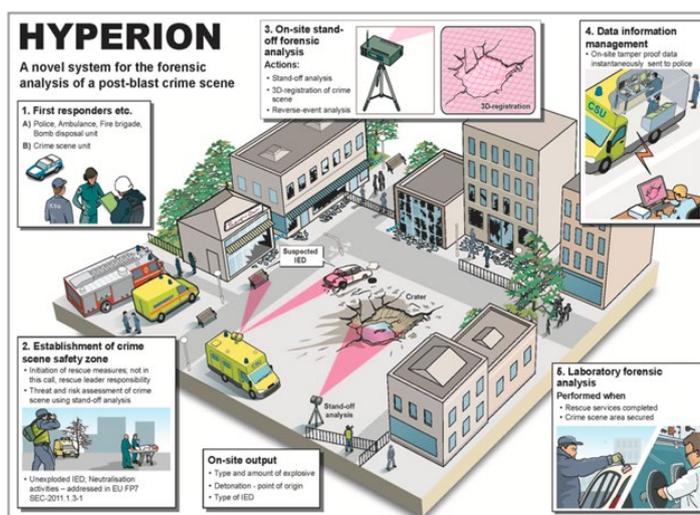
The crime scene area also needs to be well documented using ordinary high-resolution 2D photographs but most important using a 3D registration. In this 3D registration the hot-spots that have been analysed using the forensic stand-off detection tools as well as the areas that have been sampled for the 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

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

COUNTRY

- Sweden
- Germany
- The Netherlands
- Turkey
- Italy
- France
- Germany
- Poland
- Turkey
- Sweden
- Spain
- Sweden

LOTUS / Localization of threat substances in urban societies

© paolo toscani - Fotolia.com

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

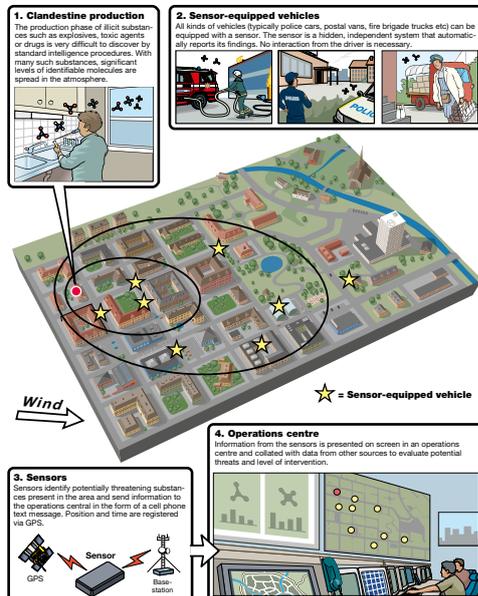
Project objectives

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.

**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

Totalförsvarets Forskningsinstitut (FOI)
 Portendo AB
 Saab AB
 Bruker Daltonik GMBH
 Ramem S.A.
 Bruhn NewTech A/S
 Research and Education Laboratory in Information Technologies
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Universidad de Barcelona
 Secrab Security Research

COUNTRY

Sweden
 Sweden
 Sweden
 Germany
 Spain
 Denmark
 Greece
 The Netherlands
 Spain
 Sweden

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.528223-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

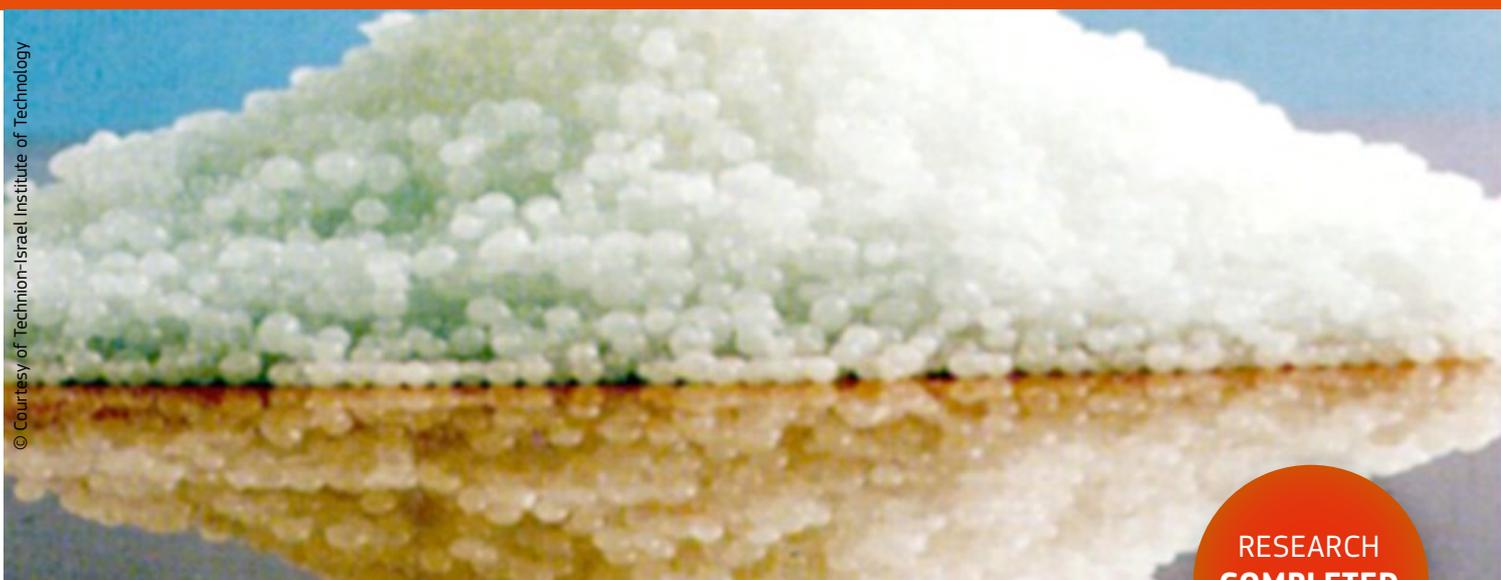
Indra Sistemas S.A.
 University of Malaga
 Totalförsvarets Forskningsinstitut (FOI)
 EKSPLA UAB
 AVANTES BV.
 Technical University of Clausthal
 Vienna University of Technology
 University of Dortmund
 Guardia Civil

COUNTRY

Spain
 Spain
 Sweden
 Lithuania
 The Netherlands
 Germany
 Austria
 Germany
 Spain

PREVAIL / PRecursors of Explosives: Additives to Inhibit their use including Liquids

© Courtesy of Technion-Israel Institute of Technology



RESEARCH
COMPLETED

Information

Grant Agreement N°

241858

Total Cost

€4,296,266.87

EU Contribution

€3,343,162

Starting Date

01/09/2010

End Date

31/10/2013

Coordinator

TOTALFORSVARETS

FORSKNINGSINSTITUT

Department of Energetic

Materials

Gullfossgatan 6

164 90 Stockholm

Sweden

Contact

Malin Kölhed

Tel.: +46 (0)8 5550 4197

Mobile: +46 (0)70 9277010

E-mail: Malin.kolhed@foi.se

Website: www.prevail-fp7.eu

Project objectives

The goal was to prevent or at least make it much more difficult to manufacture explosives. Another part of the project focused on finding a suitable marker/detection system to facilitate detection of illegal use of fertiliser-based homemade explosives, a task that today is very difficult to perform. These objectives had to be met without obstruction of the legitimate use of these products and without causing any adverse effects on the environment or on people's health.

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.

Results

Results regarding selected project objectives:

» Inhibitors to prevent the concentration of a precursor

The final candidate was tested for inhibition activity, stability and removal in lab scale and was finally validated in large scale and long-term testing. This showed that it is possible to find chemicals that function in the desired temperature range. The inhibition activity of these chemicals will make it much more difficult to construct bombs using the precursor under study. However, the stability should be further improved. Future research methods have been identified.

» Inhibitors for preventing the formation of some home-made explosives crystals

These inhibitors were tested for activity and removal on lab scale and were finally validated on a realistic scale and the results are promising.

If this measure is implemented, we all shall benefit from the fact that terrorists will encounter major difficulties when attempting to prepare this HME.

» Novel Markers for fertiliser-based homemade explosives

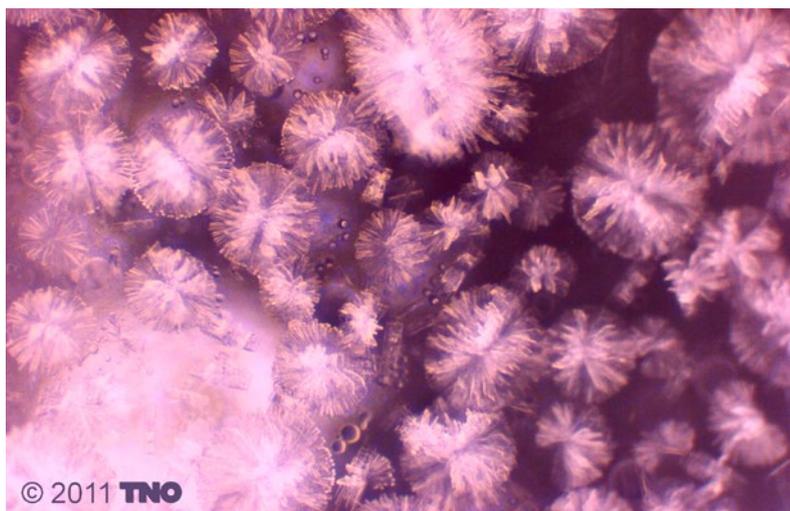
These markers were developed to suit specific detectors, as well as to be environmentally friendly, non-toxic and bio degradable.

The work has found technical solutions of where to add a chemical marker in order to be able to detect illegal uses of fertilisers. The work has also resulted in a unified work with the European coatings industry. Further

research will be necessary to find technological detection solutions that can be implemented.

» Roadmap for future work

A roadmap for future Research and Development work and actions (as well as regulatory) was prepared. Criteria for the industrial implementation of inhibitors and markers were drafted. The usefulness of the developed additives for other precursors was also assessed and required future research was indicated.



PARTNERS

Totalförsvarets Forskningsinstitut (FOI)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Technion – Israel Institute of Technology (Technion)
 Arkema France (Arkema)
 KCEM AB (KCEM)
 Yara International ASA (Yara)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Wojskowy Instytut Higieny i Epidemiologii (WIHiE)
 SECRA Security Research (SECRA)
 Inscintinel Ltd. (INSC)

COUNTRY

Sweden
 The Netherlands
 Israel
 France
 Sweden
 Norway
 France
 Poland
 Sweden
 United Kingdom

SALIENT / Selective Antibodies Limited Immuno Assay

Novel Technology

© SALIENT

RESEARCH
COMPLETED

Information

Grant Agreement N°

242377

Total Cost

€4,498,088.80

EU Contribution

€3,362,598.60

Starting Date

01/09/2010

End Date

31/12/2013

Coordinator

**UNIVERSITY OF
NEWCASTLE UPON TYNE**Institute of Cellular me-
dicine

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.ukWebsite: <http://www.salient.eu/>**Project objectives**

SALIENT 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.

SALIENT 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 immunodiagnosics 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 SALIENT 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.

Results

SALIENT has been highly successful in meeting its objectives of designing and developing an ultra-rapid testing platform for the high explosives RDX, PETN, HMX and TNT that is very simple to deploy and complementary to physical methods of detection. A key feature of the system is that the presence of explosive is positively seen on a dipstick simply as a positive red line, over a white zero background, that is easy to see by eye or read with a hand-held reader. The lateral flow dipstick systems that have been developed are capable of simple visual detection within seconds of sample application and quantitative detection within a few minutes. This capability has been complemented by development of highly efficient

sampling means, including rapid surface-wipe and air sampling devices and protocols. The programme has also facilitated development of a hand-held reader allowing rapid quantification, storage and controlled broadcasting of results. Extensive laboratory and field-testing, following controlled explosions, have clearly shown the robustness and excellent performance of the systems. The high sensitivity (to parts per billion) speed and simplicity of use of the devices allows their application to both post-blast incidents and pre-blast screening applications by personnel such as first responders and security staff. The SALIENT consortium has developed the complete high performance detection package to a fully developed pre-manufacturing production prototypic stage.

PARTNERS

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

COUNTRY

United Kingdom
 United Kingdom
 Finland
 France
 Ireland
 Slovakia
 Netherlands
 Netherlands
 Netherlands
 United Kingdom
 United Kingdom

SUBCOP / Suicide Bomber Counteraction and Prevention

© freeimages – Andreas Krappweis



Information

Grant Agreement N°

312375

Total Cost

€4,601,647.25

EU Contribution

€3,486,040.00

Starting Date

01/06/2013

Duration

36 months

Coordinator

SWEDISH DEFENCE

RESEARCH AGENCY (FOI)

Department of Weapon
Effects and Security of
Explosives

Gullfossgatan 6
SE-164 90 Stockholm,
Sweden

Contact

Anna Pettersson

Tel.: +46 8 5550 4027

Mobile: +46 709 277224

Fax: +46 8 5550 3949

E-mail:

anna.pettersson@foi.se

Website: www.subcop.eu

Project objectives

SUBCOP addresses the extraordinary challenge of how to intervene in a suicide bombing event using non-lethal means.

SUBCOP sets out to develop technologies and procedures that can be applied by police security forces when responding to a suspected person-borne improvised explosive device (PBIED). The core objectives for SUBCOP are to consider the:

- » available technological tools for less than lethal PBIED intervention,
- » novel procedures for their application, and
- » development of new technological capabilities.

SUBCOP addresses the course of action to take when an alert to a possible PBIED has been issued and an attack may be imminent. The project recognises that an alert may only give cause for suspecting the presence of a PBIED, and that this suspicion can be of lower or higher confidence. SUBCOP will develop guidance for responses to a PBIED that are ethically and socially justifiable, given the context. SUBCOP is insensitive to how the alert is raised, whether based on detection of explosives or explosive devices, informants' reporting or other intelligence sources.

Description of the work

The selection of tools and technologies for countering a PBIED event requires an understanding of the operational and situational requirements for end-user intervention. In the first phase of the project, requirements are collected from end users that either have or would be responding to a PBIED event. In parallel, previous PBIED events are analysed in detail in order to gain a deeper understanding about the underlying factors in PBIED attacks. The selection of tools and technologies are further supported by a technical capability and gap analysis.

The project focuses its technical work on three different areas:

- » Supporting and softer methods encompasses situational awareness tools, psychological approaches and methods to direct the crowd away from the danger;
- » Mitigation and containment brings rapidly deployable physical protection from the effects of the IED in case of an explosion. It also surveys possible electronic warfare measures that can be used in an urban environment to mitigate remote initiation of the IED;
- » Less than lethal methods focuses on existing and emerging tools and technologies for engaging with the suspect to achieve immediate but reversible incapacitation. Evaluation of promising tools and new developments are part of the project objectives in this area.

The selection of tools to be further investigated and developed within SUBCOP is based not only on the efficiency of the countermeasures to handle the PBIED, but also on the medical risks and risks of collateral injuries to the suspect, law enforcement personnel or bystanders caused by countermeasures. It must be understood that

the outcome of a PBIED situation can be highly lethal.

The potential responses to PBIED situations can be assessed by end users in a preparatory phase through the toolbox model, which incorporates the tools' efficiency, utility and safety when applied in a PBIED context.

The project embeds ethical aspects into the tools' selection and their modelling. Ethical and legal aspects of research and deployment are also part of the project work plan.

Expected results

SUBCOP will develop technology demonstrators and suggest tools and procedures for use in PBIED situations. A response guidance training tool for assessing response strategies applied in the separate-, protect- and engage-phases of PBIED intervention is another major output of the project.

In the final phases, the outcome of SUBCOP will be a training-and-validation exercise for end users.

In the long term, the project will help prepare police forces throughout the EU in dealing with PBIED terrorist attacks.

PARTNERS

Swedish Defence Research Agency (FOI)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 ASELSAN Elektronik Sanayi ve Ticaret A.s. (ASELSAN)
 RAND Europe Community Interest Company (RAND)
 Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V. (FhG-ICT)
 CBRNE Ltd. (CBRNE)
 Cerberus Black Ltd. (CB)
 Karolinska institutet (KI)
 Icisleri Bakanligi (EGM)
 Technische Universiteit Eindhoven (TU/e)
 Ministry of Public Security (MOPS-IMP)

COUNTRY

Sweden
 The Netherlands
 Turkey
 United Kingdom
 Germany
 United Kingdom
 United Kingdom
 Sweden
 Turkey
 The Netherlands
 Israel

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

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

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

COUNTRY

Belgium
 Italy
 Germany
 Portugal
 Spain
 Italy
 Poland
 Germany
 Croatia
 Croatia
 France
 Austria
 Poland
 United Kingdom
 Belgium
 Sweden
 Germany
 Belgium
 Spain
 Germany
 Italy
 Italy
 Austria
 Belgium

IMSK / Integrated mobile security kit



RESEARCH
COMPLETED

Information

Grant Agreement N°

218038

Total Cost

€23,485,135.25

EU Contribution

€14,864,308

Starting Date

01/03/2009

End Date

28/02/2013

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

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.

Results

IMSK designed a system to optimally integrate different sensor information feeds to produce a common operational picture for area surveillance checkpoint control and detection of CBRNE (chemical, biological, radiological, nuclear, explosive) threats during large-scale events. The goal was also to provide security support to protect important public figures and others who might be present during such event.

Sensor data was integrated via a secure communication module and a data management module and output to a command & control centre. The technologies' sensor data was fed into a single information platform and fused to create a common picture for rapid distribution at event sites (hotels, sport or festival arenas, etc.) which temporarily need enhanced security.

IMSK developed an information model – the “Mobile Situation Object” – used for information-gathering from all its subsystems and their sensors.

The project's heart is its command and control subsystem (C2), which allows authorities to monitor a site and activity by humans, vehicles and other factors. The “position” of a threat could be continuously updated as well as that of security forces.

IMSK also developed sensors for CBRNE detection, 3D face recognition and the detection of hidden weapons via passive THz technology. It studied security procedures currently used across Europe in order to better frame future European standard operating procedures.

The IMSK team says its technology could increase the volume of visitors moving through security checks, while allowing for a reduction in the number of security personnel required.

PARTNERS

Saab AB
 Selex Sensors and Airborne Systems Limited
 Selex Communications S.p.A.
 Telespazio S.p.A.
 Cilas
 Diehl BGT Defence GmbH & CO KG
 Thales Security Systems SA
 Bruker Daltonik GmbH
 Totalförsvarets Forskningsinstitut (FOI)
 Valtion Teknillinen Tutkimuskeskus (VTT)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Ministère de l'intérieur- STSI
 Università Degli Studi Di Catania
 Thyia Tehnologije d.o.o.
 AS Regio
 EPPRA S.A.S
 Qascom S.r.l
 Rikskriminalpolisen - Swedish National Police Board
 Regione Lombardia
 Thales Research and Technology Ltd
 TriVision ApS
 Joint Research Centre (JRC)
 Deutscher Fußball-Bund e.V.
 AirshipVision International S.A
 University of Reading
 The Chancellor, Masters and Scholars of the University of Oxford

COUNTRY

Sweden
 United Kingdom
 Italy
 Italy
 France
 Germany
 France
 Germany
 Sweden
 Finland
 France
 Germany
 Germany
 France
 Italy
 Slovenia
 Estonia
 France
 Italy
 Sweden
 Italy
 United Kingdom
 Denmark
 Belgium
 Germany
 France
 United Kingdom
 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 FORS-
CHUNG 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/>

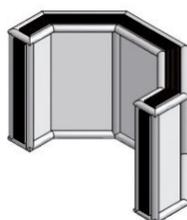
Project objectives

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



Isometric View without covering



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

TACTICS / Tactical Approach to Counter Terrorists in Cities



Information

Grant Agreement N°
285533

Total Cost
€4,466,999.07

EU Contribution
€3,478,464.00

Starting Date
01/09/2012

Duration
36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUUR-WETENSCHAPPELIJK ONDERZOEK TNO (TNO)

Human Behaviour and Organisational Innovations
Brassersplein 2

Postbus 5050, 2600 GB,
Delft

2612CT, Delft,
The Netherlands

Contact

Sharon Prins

Tel +31 88 86 67766

Mobile: +31 6 53715812

E-mail: sharon.prins@tno.nl,

info@fp7-tactics.eu

Website: www.tno.nl,

http://www.fp7-tactics.eu

Project objectives

The objective of TACTICS is to identify, research and develop tools, technologies and methods to improve the effectiveness of security forces in preventing and mitigating an urban attack or threat, while fully considering legal requirements, democratic and ethical principles.

The goals of TACTICS are to:

1. Improve the threat decomposition process
2. Improve the capability management process
3. Support the threat management process
4. Develop a three-levelled facilitation approach
5. Implement legal requirements, democratic and ethical principles into the research and development process within TACTICS

TACTICS will support actors in reacting quickly and in a more structured, efficient way to a specific threat by delivering a decision support system that responds to threats and minimises the consequences of a terrorist attack in an urban environment.

Description of the work

A common definition for the problems that TACTICS aims to solve was created, along with possible attack scenarios. Two were chosen by consulting with end users during the End User workshop in December 2012 which also simulated TACTICS operations. This work led to the TACTICS system's user-centred design, including privacy-by-design and concrete validation systems.

TACTICS was evaluated by the end users again in a validation workshop in September 2014.

Throughout the project ethical aspects were taken into account and this is reflected in an ethical paragraph in the majority of the deliverables.

Expected results

TACTICS aims at increasing effectiveness and efficiency for end users and stakeholders:

End user focus:

TACTICS increases effectiveness and efficiency of the following end user responsibilities in the case of the prevention of a specific threat or dealing with an actual attack:

- » Police officers: patrolling the streets and other public places, maintaining public order, providing assistance in emergencies.
- » Military Police: maintaining public order, providing assistance in ceremonial duties, personal protection.

» Private security: personal protection, protection of small companies, protection of bigger closed urban environments.

TACTICS increases effectiveness and efficiency of the following stakeholder responsibilities that are relevant for the prevention of a specific threat or dealing with an actual attack:

» National Coordinators for Counterterrorism: analysing intelligence and other information, policy development, coordinating anti-terrorist security measures.

» Local Municipalities: managing safety and security in their own town or city.

» National Security Services: investigating individuals and organisations, promoting the security of vital sectors, gathering international intelligence and compiling risk and threat analyses.

» Pan-European Authorities: promoting information sharing to address free movement of persons and ensure European-wide public safety.

PARTNERS

European Commission (EC)
 Rand Europe (RAND)
 Korps Landelijke Politiediensten (KLPD)
 Peace Research Institute Oslo (PRIO)
 ITTI Sp. Z o.o. (ITTI)
 LERO @ TRINITY COLLEGE DUBLIN (TCD)
 International Security and Counterterrorism Academy (ISCA)
 Universidad Politécnica de Valencia (UPV)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (FHG)
 Koninklijke Marechaussee (KMAR)
 Morpho (MPH)

COUNTRY

Belgium
 United Kingdom
 The Netherlands
 Norway
 Poland
 Ireland
 Israel
 Spain
 Germany
 The Netherlands
 France

UNCOSS / Underwater coastal sea surveyor

© COCAE

Information

Grant Agreement N°
218148

Total Cost
€4,119,638.72

EU Contribution
€2,763,818.61

Starting Date
01/12/2008

End Date
31/07/2012

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: +33 1 69 08 51 88
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 Unexploded 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

Figure 1: Torpedo from World War II

Figure 2: Antiship mines

RESEARCH
COMPLETED

© Uncoss

Results

The project's main objective was to provide tools for the non-destructive inspection of underwater objects based on a neutron generator and gamma sensor. The technology's application for underwater protection is one of its major achievements.

UNCOSS designed, manufactured and tested a remotely operated vehicle (ROV) to inspect suspicious objects lying on the seafloor or riverbed. The ROV hovers over an object and reads its chemical make-up using the neutron generator and gamma sensors. The range of the reading depends on the salt content of the water and varies from several centimetres in very salty water to several meters in freshwater.

The project's underwater neutron inspection system was tested in Croatia's Punt Seaport to prove its ability to distinguish explosive surrogates from sediments in metallic objects lying on the seafloor. A further demonstration was performed along Slovenia's Adriatic seacoast, which demonstrated that the ROV can detect metallic objects potentially buried in the seabed.

PARTNERS

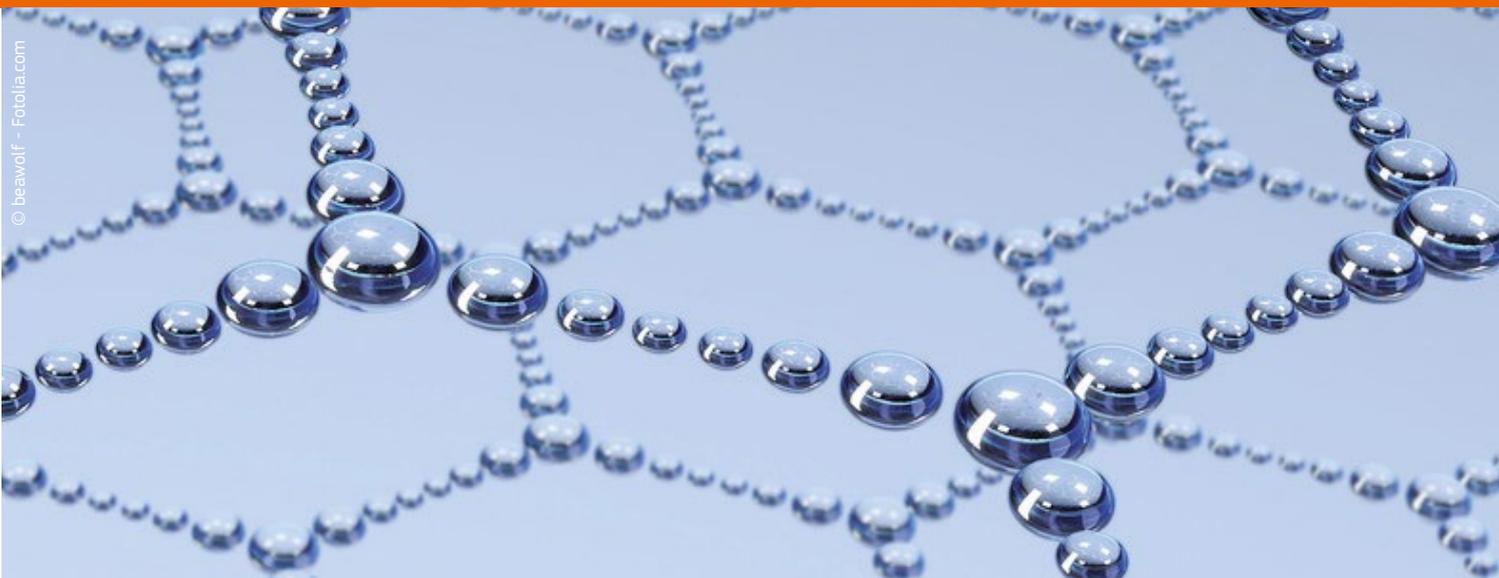
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 ECA S.A.
 Ruder Boskovic Institute (RBI)
 Laseroptronix
 Jozef Stefan Institute (JSI)
 A.C.T.d.o.o. (ACT)
 Port Authority Dubrovnik
 Port Authority Bar
 Port Authority Vukovar
 Mednarodna podiplomska šola Jožefa Stefana (MPS)

COUNTRY

France
 France
 Croatia
 Sweden
 Slovenia
 Croatia
 Croatia
 Montenegro
 Croatia
 Slovenia

VIRTUOSO / Versatile information toolkit for end-users oriented open sources exploitation

© beawolf - Fotolia.com



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

Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LIST)
 Defence and Security Systems (EADS)
 Origin Sociedad Anonima Espanola (ATOS)
 Mondeca SA (Mondeca)
 Newstin a.s (NWT)
 SAIL Technology AG (SailLabs)
 Aalborg University (AAU)
 Thales Communications (TCF)
 Bertin Technologies (Bertin)
 Stichting Katholieke Universiteit / Brabant Universiteit Van Tilburg (TILT)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Ingenieria de Sistemas Para la Defensa de Espana SA (Isdefe)
 Hawk Associates Limited (HAWK)
 Eidgenössische Technische Hochschule Zürich (ETH Zurich)
 Compagnie Européenne d'Intelligence Strategique (CEIS)
 Universita Degli Studi di Modena e Reggio Emilia (CRIS/UoM)
 Columba Global Systems Ltd. (Columba)
 Thales Research and Technology (THALES)

COUNTRY

France
 France
 Spain
 France
 Czech Republic
 Austria
 Denmark
 France
 France
 The Netherlands
 The Netherlands
 Spain
 United Kingdom
 Switzerland
 France
 Italy
 Ireland
 France

AEROCEPTOR / UAV BASED INNOVATIVE MEANS FOR LAND AND SEA NON-COOPERATIVE VEHICLES STOP

© Jonoman1 Dreamstime.com



Information

Grant Agreement N°

285144

Total Cost

€4,839,873

EU Contribution

€3,468,859.75

Starting Date

01/01/2013

Duration

36 months

Coordinator

INSTITUTO NACIONAL DE TÉCNICA AEROESPACIAL (INTA)

Aeronautic Programs

Department

Crtra Ajalvir km 4

28850

Torrejón de Ardoz, Madrid,

Spain

Contact

Vicente de Frutos

Cristóbal

Tel: +34 91 587 66 58

Fax: +34 91 520 16 16

E-mail: frutoscv@inta.es

Website: www.aeroceptor.eu

Project objectives

When approaching the problem of non-cooperative vehicles in Europe two different groups are in focus: land and sea vehicles (such as: motorbikes, cars, trucks and maritime boats). These vehicles are considered non-cooperative, when the Law Enforcement Agents are trying to stop them but the vehicle drivers do not obey the orders and signals of the agents. Maritime scenarios include the use of speedboats by organised crime groups for border crossing, drugs and weapons smuggling. Ground vehicles can be found also in a wide number of scenarios. These scenarios embrace situations ranging from routine traffic control attempts, to stolen or hijacked car pursuits, crime scene escapes and, the most complex ones, complicated and dangerous hostage situations. Law enforcement officers always seek for means to perform the stop and arrest procedure in the safest way for both the law enforcement officers, the offenders, and the rest of the people involved.

AEROCEPTOR project aims at increasing the capability of Law Enforcement Authorities (LEA) to remotely, safely and externally control and stop non-cooperative vehicles in both land and sea scenarios, by means of a Remote Piloted Aerial System (RPAS), the subset of Unmanned Aerial vehicles (UAV). Full consideration will be given to legal and human rights aspects, which are an integral part of the project. The scenarios will moreover be audited from the ethics point of view before their implementation.

RPAS consists of an aerial vehicle that is remotely piloted. This solution has several advantages, such as:

- » Higher security level for law enforcement agents and lower error rate;

- » Increasing the efficiency and effectiveness of interception operations, since RPAS are quickly deployable and have an all-weather and 24/7 operation capability;
- » Decreasing the risk of human overreaction in interception operations;
- » Offering a cost effective and environmentally friendlier solution due to their reduced weight and therefore less fuel consumption;
- » and last but not least, being humans still the best decision makers, RPAS offers a solution able to combine the human capability for decision making with a high automated operation capability owing to the continuous monitoring of the operation and fulfilling "state of the art" privacy respect legal requirement.

Description of the work

The project will cover different types of activities:

1. Research and Technological Development activities:
 - » Electromagnetic jamming payload equipment development;
 - » Development of an innovative RPAS control system;
 - » Technological development to adapt existing payloads
2. Systems engineering activities to integrate the different subsystems, technologies, new developments and Components Off The Shelf (COTS) into the new system.
3. Legislation and regulatory assessment activities, to study the needed regulatory framework allowing this kind of RPAS to operate (certification and integration into aerospace).

4. Safety, Security and ethical issues assessment, in order to ensure that the proposed system complies with the necessary safety and security levels and is compliant with the European regulations.

Expected results

Interception of non-cooperative vehicles by law enforcement agencies is often a very dangerous task. Accident may occur that threatens the lives of those who intercept, for example the police or border guards. At the same time it can also result in the loss of life of the offenders, which is of course not intended. Moreover, often innocent third parties are involved in accidents occurring in vehicular pursuits, that is, people who just happen to stand or pass by. That's the reason why current interception means are neither safe nor effective. I. AEROCEPTOR will develop a concept that will increase effectiveness and safety of these procedures, enhancing also the capability range by developing a technology that will allow LEAs to monitor, track and stop land and maritime non cooperative vehicles owing to an automated aerial system.

PARTNERS

Instituto Nacional de Técnica Aeroespacial (INTA)
 Ingeniera de Sistemas para la Defensa de España SA (ISDEFE)
 Aerospace and Defence SAU (GMV)
 Office National d'Etudes et de Recherches Aérospatiales (ONERA)
 Przemysłowy Instytut Automatyki i Pomiarów piap (PIAP)
 Alma Mater Studiorum-Università di Bologna (UNIBO)
 Austrian Institute of Technology GMBH (AIT)
 Israel Aerospace Industries LTD. (IAI)
 Turk Otomobil Fabrikası Anonim Şirketi (TOFAS)
 Sigmund Freud Privatuniversität Wien GMBH (SFU)
 Ministerio del Interior (MIR)
 Rotem Technological Solutions LTD (ROTEM)
 Etienne Lacroix Tous Artifices SA (LACROIX)
 Ministry of Public Security (MOPS/INP)
 Zabala Innovation Consulting, SA (ZABALA)

COUNTRY

Spain
 Spain
 Spain
 France
 Poland
 Italy
 Austria
 Israel
 Turkey
 Austria
 Spain
 Israel
 France
 Israel
 Spain

EVIDENCE / European Informatics Data Exchange Framework for Courts and Evidence



Information

Grant Agreement N°

608185

Total Cost

€2,303,648

EU Contribution

€1,924,589

Starting Date

01/03/2014

Duration

30 months

Project objectives

The EVIDENCE project aims to provide a road map (guidelines, recommendations, and technical standards) for creating the missing Common European Framework for the systematic and uniform application of new technologies in the collection, use and exchange of evidence. This road map would enable policy makers to create an efficient system of regulation, treatment and exchange of digital evidence.

Law enforcement agencies (LEAs) as well as judges/magistrates, prosecutors and lawyers practising in the criminal field would have at their disposal a Common European Framework, allowing them to gather, use and exchange digital evidences according to common standards and rules. EVIDENCE activities will enable the implementation of a stable network of experts in digital forensics communicating and exchanging their opinions.

The following objectives are considered essential

- » Developing a common and shared understanding on what electronic evidence is and which are the relevant concepts of electronic evidence in involved domains and related fields;
- » Defining rules and criteria utilized for processing electronic evidence in EU Member States, and how the exchange of evidence is regulated;
- » Developing the existence of criteria and standards for guaranteeing reliability, integrity and chain of custody requirement of electronic evidence in the EU Member States and eventually in the exchange of it;
- » Defining operational and ethical implications for LEAs all over Europe;

- » Identifying and developing technological functionalities for a Common European Framework in gathering and exchanging electronic evidence

Description of the work

In order to achieve the objectives of the project, EVIDENCE has several research work packages. Each work package is led by an experienced project member who is responsible for clearly delineated, measurable deliverables. The work packages are carried out in the context of four distinct project streams which build on and inform each other:

- » Status Quo Analysis (WP2, WP3, WP4, WP6, WP8),
- » Technical Functionalities development (WP5),
- » Impact and Testing (WP5, WP7), and
- » Road Map (WP9).

The project moves from an 'as is' analysis to the envisioning of future counter measures and research.

The EVIDENCE project will be co-managed through a Steering Committee on the basis of the joint responsibility principle. External input, advice and feedback will be provided by members of the External Advisory Group (EAG). Dissemination of the project outcomes will be carried out in the context of a dedicated work package (WP11) that will be in close cooperate with all other work packages to achieve the widest possible dissemination of information to the relevant stakeholders and policy makers.

Coordinator

CONSIGLIO NAZIONALE DELLE RICERCHE - NATIONAL RESEARCH COUNCIL OF ITALY (CNR-ITTIG)

Institute of Legal Information Theory and Techniques of the National Research Council of Italy (ITTIG)

Via De' Barucci 20
50127 - Florence

Italy

Contact

Maria Angela Biasiotti

Tel: +39 055 4399683

Mobile: +39 3393511657

Fax: +39 055 4399605

E-mail: mariaangela.biasiotti@ittig.cnr.it

ittig.cnr.it

Website: www.ittig.cnr.it

Expected results

EVIDENCE will create a common European framework in regards to electronic evidence.

More specifically, the EVIDENCE Road Map will greatly impact on the existing scenario by:

- » Positively influencing judges, who are the key actors in admitting electronic evidence and police experts holding the main position in gathering evidence;
- » positively influencing the perceptions of security and reliability held by different agents by adjusting and creating national and supranational legislation;
- » enhancing confidence in the experts related to the collection, analysis and conservation of electronic evidence;
- » supporting training, knowledge and experience for experts;
- » improving communication between the actors related to electronic evidence, at the national, European and international level;
- » foreseeing uses for the EVIDENCE road map.

PARTNERS

Consiglio Nazionale delle Ricerche (CNR-ITTIG and CNR-IRPPS)
 Rijksuniversiteit Groningen (RUG)
 International Criminal Police Organization (Interpol)
 Leibniz Universität Hannover (LUH)
 Laboratorio di Scienze della Cittadinanza (LSC)
 Università Malta (UoM)
 Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC)
 Law and Internet Foundation (LIF)
 Conseil des Barreaux Européens AISBL (CCBE)

COUNTRY

Italy
 The Netherlands
 France
 Germany
 Italy
 Malta
 Belgium
 Bulgaria
 Belgium

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.

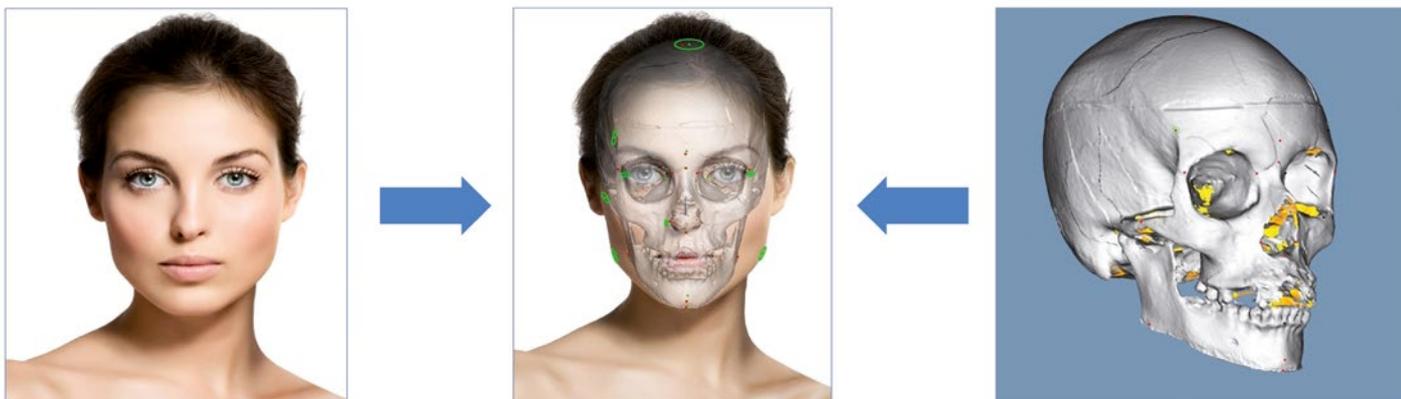
PARTNERS

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

COUNTRY

United Kingdom
 The Netherlands
 France
 United Kingdom
 United Kingdom
 United Kingdom
 Germany

MEPROCS / New methodologies and protocols of forensic identification by craniofacial superimposition



Information

Grant Agreement N°

285624

Total Cost

€1,199,750

EU Contribution

€1,005,800

Starting Date

01/02/2012

Duration

24 months

Coordinator

Fundación para el

Progreso del Soft

Computing (ECSC)

Applications of Fuzzy Logic

and Evolutionary

Algorithms Research Unit

C/ Gonzalo Gutiérrez

Quirós, s/n

33600, Mieres, Asturias,

Spain

Contact

Sergio Damas Arroyo

Tel: +34 985 45 65 45

Fax: +34 985 45 66 99

E-mail: sergio.damas@

softcomputing.es

Website: www.meprocs.eu

Project objectives

The MEPROCS project aims to propose a common EU framework to allow the extensive application of the craniofacial superimposition (CS) technique in practical forensic identification scenarios commonly tackled by European scientific police units.

This framework will include:

- » the implementation of an existing semi-automatic method to assist the forensic experts in the application of the CS technique, resulting in a simple, quick, and systematic approach;
- » the definition of standard protocols at European level, leading to the objective application of the CS technique in different forensic identification scenarios; and
- » the specification of a forensic science methodology to provide an objective evaluation of the forensic identification results achieved by CS, avoiding particular assumptions that could bias the process. Hence, the project clearly promotes the validation and exchange of CS protocols and methodologies among different organisations.

Description of the work

1. Analysis of the existing methods and procedures in the field of CS-based forensic identification.

A review of the state of the art in forensic identification from skeletal remains by CS will be addressed, identifying all the reported applications of the CS technique, including materials, protocols, methods and tools used.

2. Consolidation of the network.

Engage new stakeholders by contacting the most representative forensic anthropology labs, researchers, and end-users, in order to expand the implementation of the network and widen its scope.

3. Establishment of specific protocols for the application of CS to different scenarios.

Identify the different scenarios where CS has been applied, reporting common problems, number of tackled and solved cases, predominant scenarios and reliability. Advantages and disadvantages of the different procedures followed by the end-users in the network will be discussed. Standard protocols for each kind of scenario (missing people, mass disasters, etc.) will be defined.

4. Specification of validation techniques.

Study previous approaches to propose semi-automatic methods to assess CS results. Special focus will be placed on analysing ethical and legal issues concerning scientific use of identification cases. Finally, the robustness and accuracy of the automatic CS method will be assessed through experiments over all the identification cases available.

5. Global CS forensic identification framework definition.

Design of a CS-based methodological framework that can be easily distributed and accessed by stakeholders, and evaluation of its performance.

6. Dissemination and training.

We will work on improving communication between the different communities involved. Events to train end-users in the proposed automatic CS-based forensic identification framework will be organised. The visibility of the project results will be promoted, and a handbook on the CS identification framework published.

Expected results

- » Definition of standard protocols for the application of CS to different scenarios;
- » Specification of objective and automatic validation techniques for the CS identification results
- » Promotion of the application of the resulting CS-based forensic identification methodological framework
- » Enhancement of the cooperation among forensic anthropologists, technical researchers, and end-users
- » Enhancement of the CS forensic identification technique

PARTNERS

European Centre for Soft Computing - ECSC
 Consorci di Ricerca Sistemi ad Agenti - CORISA
 European Council of Legal Medicine - ECLM
 University of Granada - UGR
 Israel National Police (Ministry of Public Security) - INP
 Forensic Sciences Centre (Universidade de Coimbra) - FSC
 Guardia Civil (Ministerio del Interior) - GC

COUNTRY

Spain
 Italy
 Portugal
 Spain
 Israel
 Portugal
 Spain

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

© rolffimages - Fotolia.com



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,
Solithull Parkway

B37 7YN

United Kingdom

Contact

Cecilia Buffery

Tel.: +44 1256771521

Mobile: +44 7824 434158

Fax: +44 1256771521

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

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

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

COUNTRY

United Kingdom
 Ireland
 Spain
 Belgium
 The Netherlands
 United Kingdom
 Italy

 Italy
 United Kingdom
 United Kingdom
 Austria
 United Kingdom
 Slovenia

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 AreaCamino 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

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

COUNTRY

Spain
 Germany
 France
 Germany
 Greece
 Spain
 Sweden
 Germany
 Slovakia
 Greece

SMARTPRO /

Lightweight, flexible and smart protective clothing for law enforcement personnel



Information

Grant Agreement N°

607295

Total Cost

€3,777,451.27

EU Contribution

€2,741,826.52

Starting Date

01/04/2014

Duration

42 months

Coordinator

MATERIALS INDUSTRIAL RESEARCH AND TECHNOLOGY CENTER S.A. (MIRTEC)

R&D – Athens Branch

Eleftheriou Venizelou 4

176 76, Kallithea, Athens,

Greece

Contact

Silvia Pavlidou

Tel: +30 210 9234932

Mobile: +30 6944639248

Fax: +30 210 9235603

E-mail:

s.pavlidou@ebetam.gr

Website: www.ebetam.gr

Project objectives

The concept of SMARTPRO lies in the development of lightweight and flexible protective clothing, incorporating smart functionalities and designated for law enforcement authorities.

Modern body armours still have some of the same drawbacks as the old ones, as they are mostly heavy, bulky and rigid. They limit the wearer's mobility and agility and are impractical for use on joints, arms, legs, etc. Also, body armours have traditionally been designed to protect the wearer against ballistic threats and, thus, they provide only a limited level of protection against knives, sharp blades or sharp-tipped weapons.

Recent studies reveal that stab and puncture have become a main cause of police officers' injuries. There is an obvious need to develop materials that combine stab and ballistic protection, while retaining their flexibility and low weight.

Description of the work

The work in SMARTPRO addresses the following:

- » Development of optimized protective (ballistic/ stab resistant) textile and composite structures, including woven and 3D knitted textiles structures, fish scale-type composites and innovative hybrid structures made of synthetic polymer nanofiber composites.
- » Development and application of innovative surface treatments aiming to improve textiles performance on an areal density basis. These include surface application of shear thickening fluids, ceramic coatings, dilatant powders, carbide nanoparticles and cross-linkable side-functionalized aromatic polymers.
- » Optimized assembly of the protective panel aiming to achieve maximum protection at minimum weight and cost.
- » Development and integration of smart systems, including wearable GPS, electrocardiogram, temperature and gas sensors.
- » Ergonomic design of the body armour, considering also modularity.
- » Prototypes development.

Expected results

The project is expected to lead to new body armours and protective gear for body parts other than the torso, characterized by low weight and increased flexibility and incorporating smart functionalities that may increase awareness of law enforcement personnel. The new PPE will be ergonomically designed, take into account the importance of modularity, and is expected to find wide acceptance by the end-users.

PARTNERS

European Commission (EC)
 Materials Industrial Research and Technology Center S.A. (MIRTEC)
 Acondicionamiento Tarrasense Associacion (LEITAT)
 Next Technology Tecnotessile Società Nazionale di Ricerca r.l. (NTT)
 Foundation for Research and Technology Hellas (FORTH)
 Kostas Siamidis AE (SIAMIDIS)
 Rheinisch-Westfaelische Technische Hochschule Aachen (RWTH)
 B.C.B International Limited (BCB International Lt)
 Soliani EMC SRL (SOLIANI)
 E. CIMA SA (CIMA)
 Departament d'Interior - Generalitat de Catalunya (INT)

COUNTRY

Belgium
 Greece
 Spain
 Italy
 Greece
 Greece
 Germany
 United Kingdom
 Italy
 Spain
 Spain

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



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, multi-media 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

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

COUNTRY

Spain
 Spain
 Germany
 Italy
 Portugal
 France
 Israel
 Spain
 France
 Italy
 Spain
 Italy
 Italy
 Romania
 Portugal
 Spain

CONPHIRMER / Counterfeit Pharmaceuticals Interception using Radiofrequency Methods in Realtime



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

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

COUNTRY

United Kingdom
 France/Germany
 Slovenia
 Slovenia
 Sweden
 United Kingdom
 Poland
 Italy
 United Kingdom
 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 06 4150 3104

Mobile: + 39 3351379733

E-mail:

afilello@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.

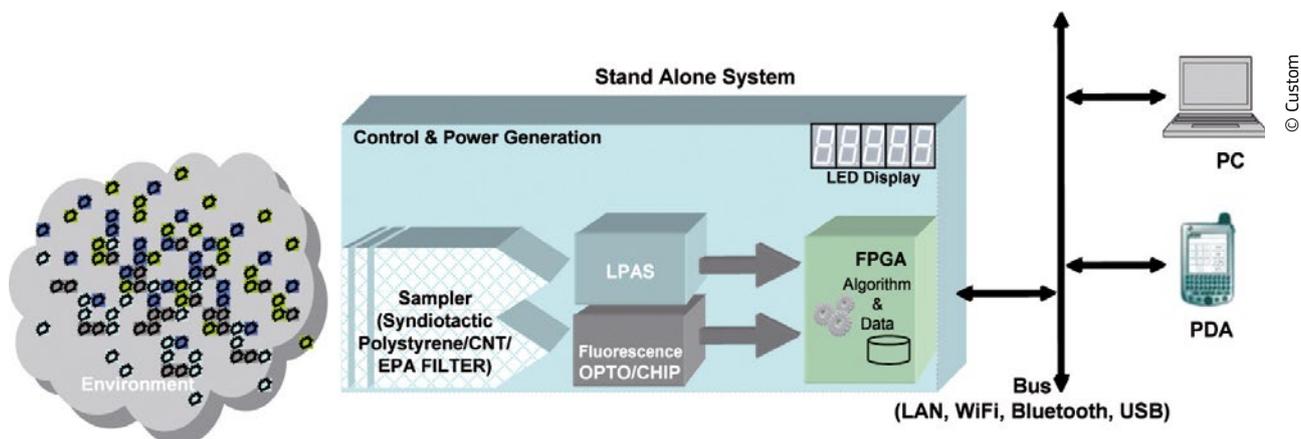
The project will focus on employing multiple techniques, integrating them in a complex system in a complementary approach, in order to identify an optimum trade-off between opposite requirements: compactness, simplicity, low cost vs. sensitivity, low false alarm rate, selectivity.

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.



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

SELEX Sistemi Integrati S.p.A.
GASERA
University of TURKU
INAS-Tecnalia
Alcatel-Thales III-V Lab
CNR IBP
ENEA
INSTM
Aalto University Foundation
Direction Nationale du Renseignement et des Enquêtes Douanières

COUNTRY

Italy
Finland
Finland
Spain
France
Italy
Italy
Italy
Finland
France

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



© G.K. - Fotolia.com

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
ELETTRICO-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 **WPO** (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:

- » 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).
- » Reliability (ability to reject interferents);
- » Hand portability;
- » Fast response (few minutes);

PARTNERS

Consorzio CREO- Centro Ricerche Elettro-Ottiche
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Consiglio Nazionale delle Ricerche
 EADS Deutschland GMBH
 Selex Sistemi integrati SpA (SSI)
 ELSAG DATAMAT S.p.A.
 Universite de Lausanne
 Universitatea Dunarea de Jos Din Galati
 Institut National de Criminalistiek en Criminologie
 National Bureau of Investigation
 Consorzio Interuniversitario Nazionale per la Scienza e la Tecnologia dei Materiali

COUNTRY

Italy
 Germany
 Italy
 Germany
 Italy
 Italy
 Switzerland
 Romania
 Belgium
 Finland
 Italy

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

© brankatekic - istockphoto.com

RESEARCH
COMPLETED

Information

Grant Agreement N°

261710

Total Cost

€4,361,954

EU Contribution

€2,979,390

Starting Date

01/05/2011

End Date

30/04/2014

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**

The overall mission of HEMOLIA is to research and develop an innovative anti-money laundering (AML) intelligent, multi-agent alert and investigation system.

Description of the work

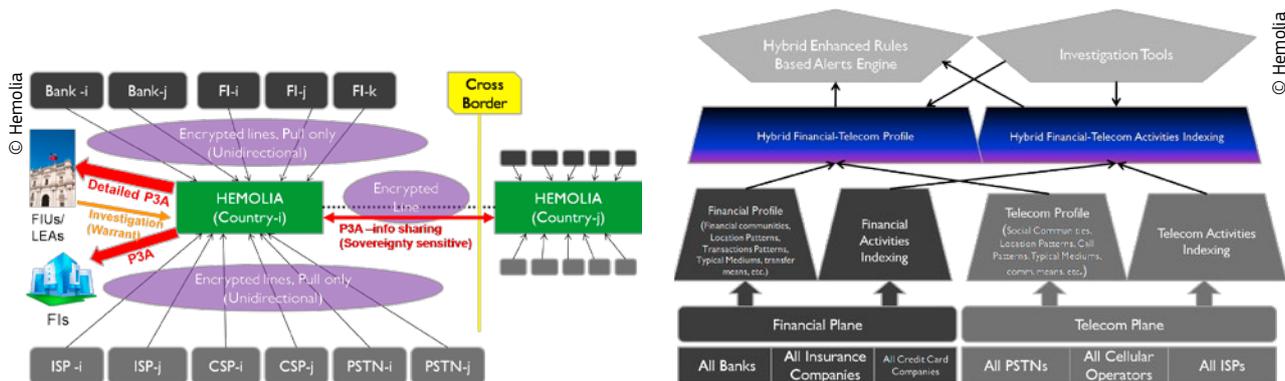
The research to be performed in HEMOLIA can be divided into 3 categories:

1. Technological objectives: The technological research will be based on the envisaged HEMOLIA architecture composed of two main parts: (i) Data-collection and data-mining from the Financial Plane and from the Telecom Plane and (ii) the HEMOLIA Core Modules which will analyse the Telecom Plane and Financial Plane Data Sources and will create enhanced alerts.
2. Legal framework of AML Systems: The legal research will include several areas: Telecom Plane Legal Framework and the "Financial Plane Legal Framework" for different categories of end users (banks and financial institutes versus FIUs/LEAs). This will also include analysis of the content of alerts and harmonisation of AML-related data and boundaries.
3. AML end-users good practice and communication strategies including the definition of methodology and guidelines for an optimal use of the HEMOLIA system, information sharing methodologies between different authorities, at the national level and at the international level.

Results

The HEMOLIA functionalities support not only the internal processes of a FIU (Financial Investigation Unit) or LEA (Law Enforcement Agency), but also the relationship with the information providers. For instance, the system identifies cases of reporting where the information is not correct or complete and where it should be sent back to the reporting entity to be returned more accurate and value-added.

By using the alerting system, the end-user would be able to identify cases where the regulated entities should have provided the information. This will improve the relationship of the FIU with the reporting entities, by organizing more targeted training sessions and by providing more appropriate feedback.



PARTNERS

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

COUNTRY

- Israel
- Denmark
- Romania
- Spain
- The Netherlands
- Poland
- Poland
- The Netherlands
- The Netherlands
- Poland
- Poland
- Israel

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

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

COUNTRY

Germany
 Switzerland
 Switzerland
 Ireland
 Germany
 Poland
 Italy

SCIIMS / Strategic Crime and Immigration Information Management System

© khwi - Fotolia.com


**RESEARCH
COMPLETED**
Information
Grant Agreement N°

218223

Total Cost

€3,595,562.80

EU Contribution

€2,318,996.45

Starting Date

01/11/2009

End Date

31/10/2012

Coordinator
BAE SYSTEMS
INTEGRATED SYSTEM
TECHNOLOGIES LIMITED

Commercial Department

Lyon Way, Frimley,

Camberley

GU16 7EX, Surrey

United Kingdom

Contact
Claire Dance

Tel: +44 (0)1276 603226

Mobile:

+44 (0)7793 423771

Fax: +44 (0)1276 603111

E-mail: [claire.dance@](mailto:claire.dance@baesystems.com)[baesystems.com](http://www.baesystems.com)Website: [http://www.sciims.](http://www.sciims.co.uk/index.html)[co.uk/index.html](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.

Results

The project developed technology that collects information and fuses it to present a clearer picture of criminal activity and movements such as human trafficking.

According to the SCIIMS team, their project's technology could be very useful in detecting unusual and criminal behavior and preventing crime in Europe.

The team focused on computer-based technology to strengthen the ability of LEAs to search, mine and fuse information from massive datasets obtained from diverse sources. Taking into account how investigators construct and represent data for an investigation, the research team produced an integrated demonstration system to show the effectiveness of their technologies, which support the various stages of an investigation, from the foraging for information to making sense of it.

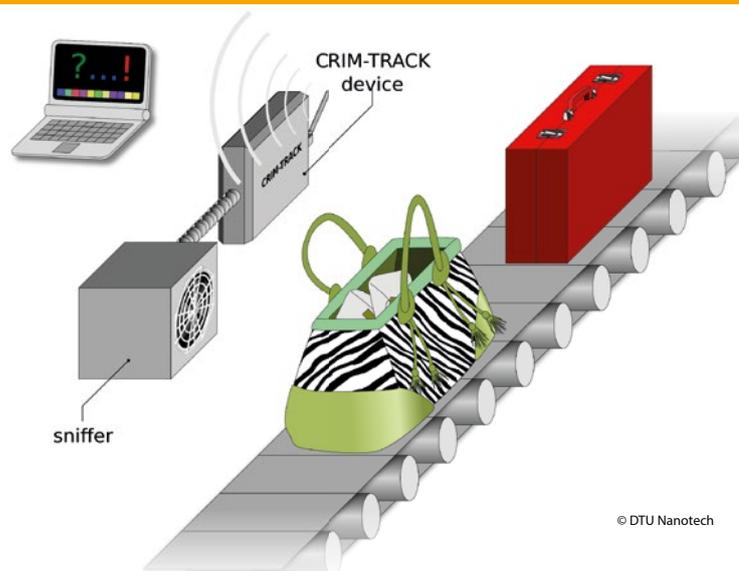
PARTNERS

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

COUNTRY

United Kingdom
 Spain
 Ireland
 Italy
 Spain
 Hungary
 Spain
 Italy
 Ireland

CRIM-TRACK / Sensor system for detection of criminal chemical substances



© DTU Nanotech

Information

Grant Agreement N°

313202

Total Cost

€4,844,602

EU Contribution

€3,583,940

Starting Date

01/01/2014

Duration

36 months

Coordinator

TECHNICAL UNIVERSITY OF DENMARK (DTU)

Department of Micro- and Nanotechnology

Ørsteds Plads 345

DK-2800 - Kgs. Lyngby -

Denmark

Contact**Mogens Havsteen****Jakobsen**

Tel: +45 45255772

Mobile: +45 51801482

Fax: +45 45887762

E-mail: Mogens.Jakobsen@nanotech.dtu.dk

Website:

<http://www.nanotech.dtu.dk/english><http://www.crimtrack.eu/>**Project objectives**

The detection of illegal compounds is an important analytical problem which requires reliable, selective and sensitive detection method that provides the highest level of confidence in the result. Moreover, to contribute to its successful development, automated target acquisition, identification and signal processing of data from the sensor are mandatory. Enhancements to sensing methods, recognition ability and timely target detection should improve sensors in both aspects, software and hardware. In the end, the sensing device should be portable, rapid, easy to use, highly sensitive, specific (minimal false positives), and low cost.

CRIM-TRACK - Sensor system for detection of criminal chemical substances aims to demonstrate a sensing device that can be further developed into a portable, miniaturized, automated, rapid, low cost, highly sensitive and simple, "sniffer". This detection unit will be based on a disposable micro-colorimetric chip that can be used for identification of illegal drugs, drug precursors and home-made explosives.

The project will combine advanced disciplines such as organic chemistry, micro fabrication and hardware technology, machine learning and signal processing techniques to support the development of a miniaturized sensor system to identify illegal drugs or drug precursors. This will provide custom officers, police forces, etc. with an effective tool to control trafficking of illegal drugs and drug precursors.

Description of the work

- » WP5 Micro-colorimetric chip for Sniffer system;
- » WP7 Air sampling;
- » WP8 Monitoring station;
- » WP9 System integration;
- » WP10 LEA Demo 1: Border control - Hidden drugs;
- » WP11 LEA Demo 2: Checkpoint security - Hidden drugs;
- » WP12 LEA Demo 3: Forensic investigation - Explosives.

Expected results

Development of Sniffer (prototype)

Road map for exploitation and protection of IPR

PARTNERS

Technical University of Denmark (DTU)
Cranfield University (CRA)
Securetec GmbH (SEC)
Pro Design Electronic GmbH (PDE)
Gammadata Instruments AB (GIAB)
Ministerie van Financien Directoraat Generaal Belastingdienst (DCA)
Mykolas Romeris University (MRU)
Danish Emergency Management Agency (DEMA)

COUNTRY

Denmark
United Kingdom
Germany
Germany
Sweden
The Netherlands
Lithuania
Denmark

CAMINO / Comprehensive Approach to cyber roadMap coordINation and develOpment



Information

Grant Agreement N°

607406

Total Cost

€1,157,666

EU Contribution

€1,036,888

Starting Date

01/04/2014

Duration

24 months

Coordinator

ITTI SP. Z O.O. (ITTI)

ITTI Sp. z o.o.

Ul. Rubież 46

61-612 Poznań, Poland

Contact

Michał Choras

Tel: +48 61 6226 985

Fax: +48 61 6226 973

E-mail:

Michal.choras@itti.com.pl

Website: www.itti.com.pl

Project objectives

The major goal of the project is to provide a realistic roadmap for improving resilience against cyber crime and cyber terrorism. Its strategic objectives are to:

- » develop a comprehensive cyber crime and cyber terrorism research agenda;
- » initiate long term activities providing a stable platform of security research experts and organisations.

Description of the work

The main aim of the CAMINO project is to establish a research agenda on cyber crime and cyber terrorism in order to fully accomplish a trustworthy information society as depicted by the Digital Agenda 2020.

The work of the project is divided into the following activities:

- » Project Management - WP1 will ensure the overall management of the project tasks in terms of effective completion, progress reporting, accountability and quality assurance. WP1 will be responsible for all contacts with the European Commission (deliverables delivery, reporting) and also with the project's advisory board, composed of external experts. A project handbook will be published that will guide the participants on administrative tasks and procedures for IPR, data handling, quality assurance, etc.
- » Identification and Analysis of Main Research Gaps and Challenges - WP2 aims to identify key research

gaps and challenges through analysis of existing cyber security-related guidelines, roadmaps and strategies. Promising results of current cyber security research projects will be identified and analysed.

- » Workshops, Seminars and Consultations - WP3 will ensure the organisation of necessary activities and meetings for the consultation with experts, working groups and all involved stakeholders.
- » Guidelines and Roadmap Development - WP4 will aim to develop cyber security guidelines, which will reflect the expectations and needs of key stakeholders. WP4 will identify key stakeholders and the scope of cyber security related problems. WP4 will also develop research roadmaps in the areas of cyber crime and cyber terrorism. This work is based on the activities of the other WPs. It will be based on commonly agreed needs among the stakeholders to provide effective guidelines and actions. Alignment with national initiatives is also planned.
- » Community Building, Dissemination and Sustainability - WP5 will provide analysis and determination of the most appropriate strategies for dissemination and exploitation of the project results and products.

Expected results

- » the definition of a concept and terminology of cyber security, cyber crime and cyber terrorism;
- » the identification of current cyber threats (including cyber crime and cyber terrorism) and corresponding state-of-the-art identification, protection and defence mechanisms, including appropriate risk analysis methodologies;
- » the definition of research gaps and stakeholders needs;
- » the guidelines, recommendations and a comprehensive research agenda (roadmap) regarding cyber security, cyber-crime and cyber terrorism;
- » a long term cyber research community on the basis of the IMG-S Cyber Security Thematic Area (TA7).

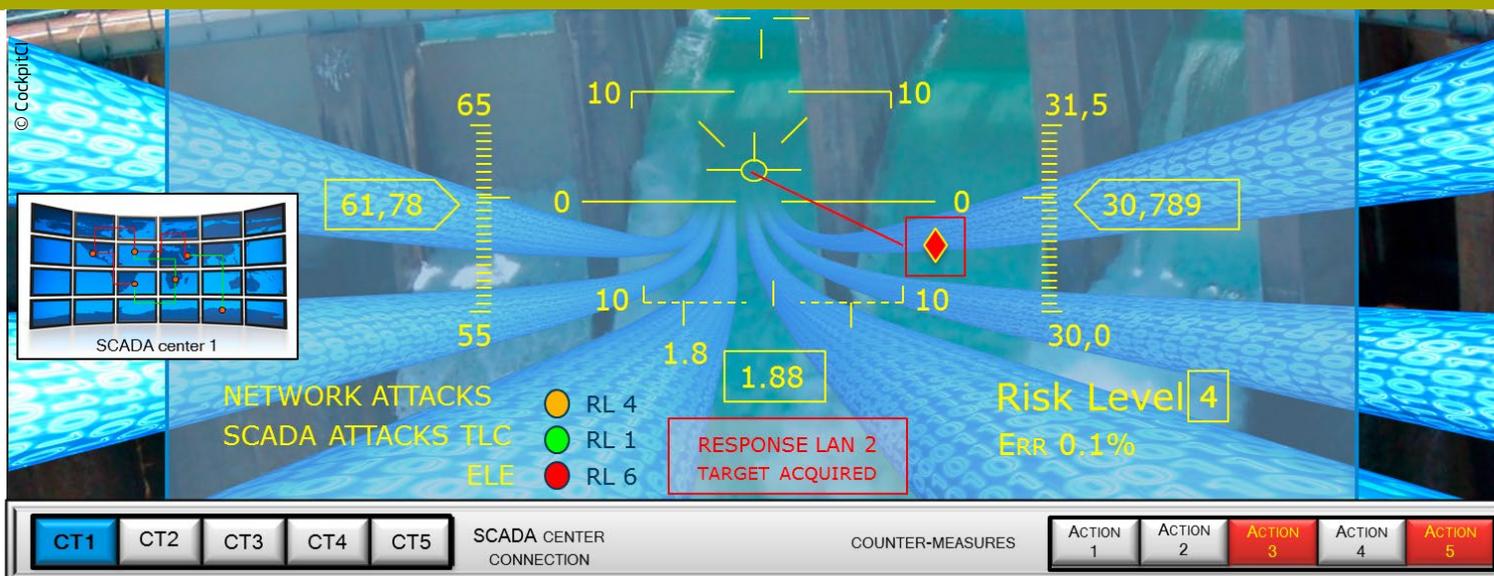
PARTNERS

ITTI Sp. z o.o. (ITTI) - Coordinator
 CBRNE Ltd. (CBRNE Ltd)
 Consiglio Nazionale delle Ricerche (CNR)
 Data Fusion Research Center AG (DFRC)
 Espion Ltd (Espion)
 Everis Aerospace and Defense S.L.U. (EADE)
 Montpellier 1 University (UM1)
 Police Academy in Szczytno (WSPol)
 S21SEC Information Security Labs S.L. (S21SEC LAB)
 Sec-Control Finland (Sec-Control Finland)

COUNTRY

Poland
 United Kingdom
 Italy
 Switzerland
 Ireland
 Spain
 France
 Poland
 Spain
 Finland

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

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

COUNTRY

Italy
 Luxembourg
 Italy
 Italy
 Italy
 Israel
 Luxembourg
 Belgium
 Portugal
 United Kingdom

E-CRIME / The Economic Impacts of Cyber Crime



Information

Grant Agreement N°

607775

Total Cost

€3,749,289

EU Contribution

€3,004,180

Starting Date

01/04/2014

Duration

36 months

Coordinator

TRILATERAL RESEARCH & CONSULTING (TRI)

Crown House, 72 Hammersmith Road

W14 8TH, London, UK

Contact

Dr. Monica Lagazio

Tel: +44 207 559 3550

Mobile: +44 790 370 3051

E-mail: monica.lagazio@trilateralresearch.com

trilateralresearch.com

Website:

<http://ecrime-project.eu>

Project objectives

E-CRIME has two primary objectives:

1. Measure and analyse the economic impact of cyber crime on non-ICT sectors (e.g., transport, energy, finance, health etc) and analyse the criminal structures and economies behind such crimes.
2. Develop concrete measures and methods to deter possible criminals and to drastically limit the attractiveness of such crimes.

Description of the work

Progress has been made in understanding and managing cyber crime as well assessing its economic impact. Yet much remains to be done. Lack of co-ordination in law enforcement and legislation, lack of common consensus on the nature of cyber crime and lack of knowledge sharing and trust are just some of the issues that afflict cyber crime responses and cloud our understanding of cyber crime.

E-CRIME addresses these problems, while analysing the economic impact of cyber crime and developing concrete measures to manage risks and deter cyber criminals in non-ICT sectors. E-CRIME uses an interdisciplinary and multi-level-stakeholder focused approach that integrates a wide range of stakeholders' knowledge and insights into the project.

First, the project will develop a detailed taxonomy and inventory of cyber crime in non-ICT sectors and analyse cyber criminal structures and economies by combining

the best existing data sources with specialist new insights from key stakeholders and experts.

Second, it will assess existing counter-measures against cyber crime in these sectors via current technology, best practices, policy and enforcement approaches, and awareness and trust initiatives.

Third, having mapped the as-is of cyber crime, the project will use available information and new data to develop a multi-level model to measure the economic impact of cyber crime on non ICT-sectors.

Fourth, it will integrate all the findings to identify and develop diverse, concrete counter-measures, combined in portfolios of inter-sector and intra-sector solutions, including enhancement for crime-proofed applications, risk management tools, policy and best practices, and trust and confidence measures.

Expected results

E-CRIME's work aims for the following durable impacts:

1. Increasing awareness of policy makers
2. Helping businesses to provide crime-proofed applications
3. Increasing the trust and confidence of EU citizens in using cyber applications
4. Making the European Union's security work programme more effective

PARTNERS

Trilateral Research & Consulting (TRI)
 Technische Universiteit Delft (TUD)
 Universite De Lausanne (UNIL)
 Westfaelische Wilhelms-Universitaet Muenster (WWU)
 The University of Warwick (WARWICK)
 Rijksuniversiteit Groningen (RUG)
 Global Cyber Security Center (GCSEC)
 IPSOS Belgium SA (IPSOS)
 Tallinna Tehnikaulikool (TUT)
 The International Criminal Police Organisation (INT)

COUNTRY

United Kingdom
 The Netherlands
 Switzerland
 Germany
 United Kingdom
 The Netherlands
 Italy
 Belgium
 Estonia
 France

HYRIM / Hybrid Risk Management for Utility Networks



Information

Grant Agreement N°

608090

Total Cost

€4,657,587.60

EU Contribution

€3,387,085.00

Starting Date

01/04/2014

Duration

36 months

Coordinator

**AIT – AUSTRIAN
INSTITUTE OF
TECHNOLOGY GMBH
(AIT)**

Safety & Security

Department

Donau-City-Strasse 1

1220 Vienna, Austria

Contact
Stefan Schauer

Tel: +43 50 550 4055

Mobile: +43 664 825 14 55

Fax: +43 50 550 4150

E-mail:

hyrim-mgmt@ait.ac.at

Website:

www.hyrim.net

Project objectives

HYRIM hopes to accomplish the following objectives:

- » Definition of hybrid risk metrics and risk assessment processes to enable comprehensive risk management for dealing with threats in multiple aspects of utility network infrastructures and to support categorisation of utility infrastructures to prioritise countermeasures development.
- » Evaluation of hybrid risk metrics to cope with attacks targeted specifically at utility network controls.
- » Development of tools and methods for risk assessment, which extend existing methodologies towards the handling of new threats to interconnected utility networks.
- » Definition of security architectures and guidelines to mitigate threats related to human and organisational risk.
- » Enhancing network and infrastructure surveillance systems using novel, on-demand technologies in the extended perimeter of utility networks.
- » Demonstration and Evaluation of Project Results in Simulated and Real Testing Environments.
- » Increase awareness of policy makers and pave the way for new legislation and pre-standardisation efforts.

Description of the work

Risk management is a core duty in critical infrastructures as operated by utility providers. Despite the existence of numerous risk assessment tools to support the utility providers in estimating the nature and impact of possible incidents, risk management is mostly a matter of best practice approaches. Risk management tools are mostly focused on one of two major topics:

- » the utility network physical infrastructure, consisting of gas, water pipes or power lines
- » the utility control network including Supervisory Control and Data Acquisition (SCADA) networks and business and information systems.

In the context of utility providers, these network types exhibit a significant interaction, and therefore risk management methods that focus on just one of these network types might be insufficient.

The main objective of this project is to identify and evaluate 'Hybrid Risk Metrics' for assessing and categorizing security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms.

Expected results

The HYRIM project will provide utility network providers with a risk assessment tool that supports qualitative risk assessment based on numerical (quantitative) techniques. Our method will explicitly account for the infrastructure's two-fold nature in terms of the utility network and the control network alongside it. The expected impact is a movement away from best practice only, towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation. The project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

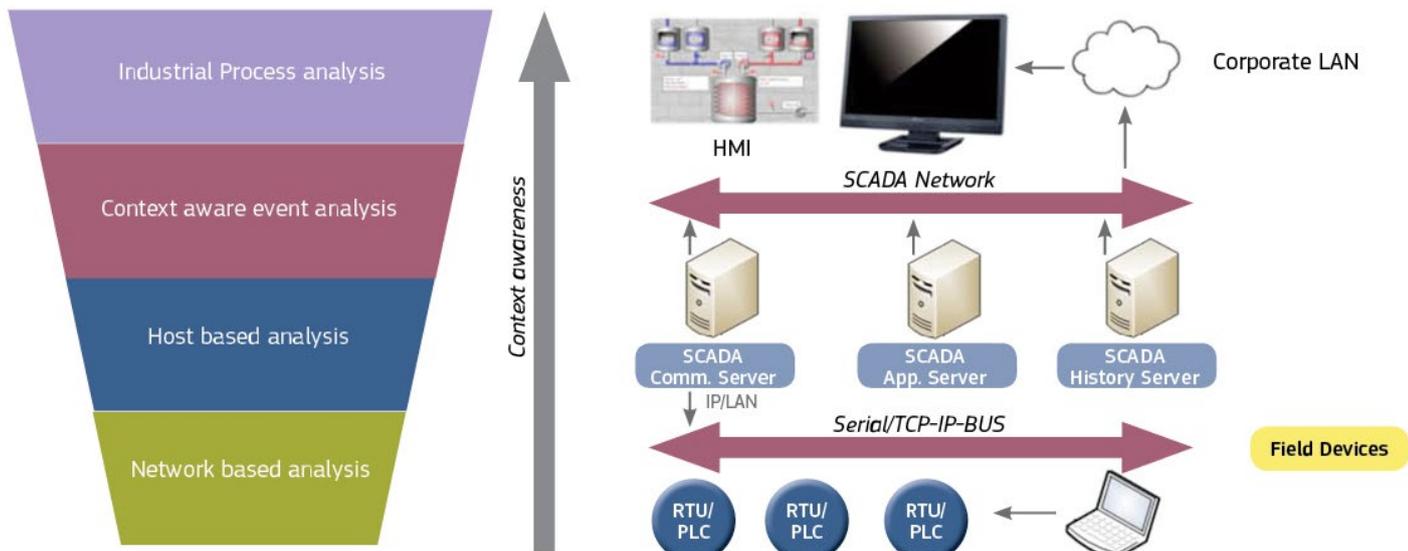
PARTNERS

Universität Passau (UNI PASSAU)
 Lancaster University (ULANC)
 ETRA Investigacion y Desarrollo SA (ETRA)
 Akhela SRL (AKH)
 Suministros Especiales Alginetenses COOP. V. (ECA)
 Linz AG für Energie, Telekommunikation, Verkehr und kommunale Dienste (LINZ)

COUNTRY

Germany
 United Kingdom
 Spain
 Italy
 Spain
 Austria

PREEMPTIVE / Preventive Methodology and Tools to Protect Utilities



Information

Grant Agreement N°

607093

Total Cost

€5,204,569.68

EU Contribution

€3,831,016.24

Starting Date

01/03/2014

Duration

36 months

Coordinator

VITROCISSET S.P.A.

(VITRO)

Giorgio Sinibaldi

Via Tiburtina, 1020

00156 – Rome – Italy

Contact

Giorgio Sinibaldi

Tel: +39 068820 4394

Mobile: +39 3346196030

Fax: +39 068820 4269

E-mail:

g.sinibaldi@vitrociset.it

Website:

www.vitrociset.com

Project objectives

PREEMPTIVE's goal is to provide an innovative solution against cyber attacks that target utility networks by enhancing existing methods and conceiving new tools. PREEMPTIVE addresses the prevention of cyber attacks against hardware and software systems such as DCS, SCADA, PLC, networked electronic sensing, and monitoring and diagnostic systems used by the utilities networks. Moreover, the research aims to implement detection tools based on a dual approach comprised of low direct detection and process misbehavior detection.

PREEMPTIVE proposes to enhance existing methodological security and prevention frameworks with the aim of harmonizing Risk and Vulnerability Assessment methods, standard policies, procedures, and applicable regulations or recommendations to prevent cyber attacks. Its dual approach takes into account both the industrial process misbehavior analysis (physical domain) and the communication & software anomalies (cyber domain).

Description of the work

PREEMPTIVE proposes to face the new threats trends against SCADA and industrial networks, using jointly a methodology framework and innovative techniques; both will be strongly related in order to fill the existing gaps among security policy, practices and technologies. The heavy involvement of the utility companies partnered within the consortium assures the feasibility of this goal.

A specific "host based" technique will be developed in order to contrast transmission through personal devices. The impact of the "host based" tool envisaged will also be within the sector of the "cloud technologies" especially for securing storage spaces.

PREEMPTIVE enhances existing security frameworks with the aim of harmonizing Risk and Vulnerability Assessment methods, standard policies and procedures and applicable regulations or recommendations. In details ISO/IEC 27000 family of standards will be considered as well as the outcomes coming from other FP7 projects: N1253, MICIE and COCKPITCI dealing with Cyber Security and Critical Infrastructure protection.

Expected results

We expect to have a high impact on utility companies and related industry and it is highly likely that future attacks will be thwarted with the help of PREEMPTIVE project results.

The outcomes envisaged in PREEMPTIVE shall improve the awareness in legal and regulatory organizations as well as for operators managing critical infrastructure assets.

PARTNERS

Vitrociset SpA (Vitro)
 Universiteit Twente (UT)
 SecurityMatters BV (SM)
 Aplicaciones en Informática Avanzada S.L. (AIA)
 Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (IOSB)
 HW Communication Limited (HWC)
 Università degli studi Roma Tre (UNIROMA)
 European Network for Cyber Security U.A. (ENCS)
 Israel Electric Corporation Limited (IEC)
 Katholieke Universiteit Leuven (KU Leuven)
 Fundacio Institut de Recerca de l'energia de Catalunya (IREC)
 Harnser Ltd (HARNSER)

COUNTRY

Italy
 The Netherlands
 The Netherlands
 Spain
 Germany
 United Kingdom
 Italy
 The Netherlands
 Israel
 Belgium
 Spain
 United Kingdom

SAWSOC / Situation AWare Security Operations Center



Information

Grant Agreement N°
313034

Total Cost
€5,406,398.00

EU Contribution
€3,491,379.00

Starting Date
01/11/2013

Duration
30 months

Coordinator

SELEX ES SPA (SELEX ES)
Cyber Security & Information
Assurance
Via Tiburtina Km 12 400
00131 – Roma - Italy

Contact
Giuseppe La Posta
Tel: +39 06 5027 4742
E-mail: Giuseppe.laposta@selex-es.com
Website:
www.selex-es.com
www.sawsoc.eu/

Project objectives

The objective of SAWSOC is to identify, implement, and validate techniques to achieve the convergence of physical and logical solutions for security monitoring. This entails the following:

1. Advancing and modernising some of the key physical and logical security technologies (namely: SOC, SIEM, Video Surveillance, PSIM, IM, Forensics, and Building Automation)
2. Developing techniques for correlating physical and logical security services from the physical and electronic domains to achieve a consistent view and to be able to produce an irrefutable record of who did what, where, and when
3. Implementing those techniques in an integrated platform for providing sophisticated security services combining in modular way diverse information from multiple sources

Description of the work

SAWSOC aims to effect a significant advancement in the convergence of physical and logical security, meaning effective cooperation among previously disjointed functions. The project is implemented in 3 main steps.

The first phase, basically consisting in detailed definition/ planning of project objectives and activities, started in November 2013 and ended in late April 2014. As an important milestone, the requirements have been identified and the techniques which will have to be implemented by the SAWSOC components and platform have been defined. Second, the project will focus on the prototype implementation until mid-2015. Then, a first workshop will then be organized, to present preliminary results to a wider audience, and collect feedback. The final workshop will take place at the end of the project in 2016.

Expected results

Demonstrating and validating the proposed techniques and the framework by performing a thorough experimental campaign with respect to three substantial case studies, namely: “maintenance impacts and attack recognition on critical infrastructures” (MIARCI); “energy production and distribution critical infrastructure” (EPDCI); and “crowded events safety & security” (CES&S).

In addition to experimental evaluation in the domains of the three use cases, the consortium will study the applicability of the proposed solutions to a wider scope, i.e. to critical infrastructure domains other than air traffic management and energy production, and to crowded events in contexts other than sports.

Experiments will also be used to derive best practices for optimal deployment of the security technologies in real world settings.

PARTNERS

Selex ES (SELEX)
 Consorzio Interuniversitario Nazionale per l'Informatica (CINI)
 Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (FhG-IOSB)
 The Israel Electric Corporation Limited (IEC)
 Enav SPA (ENAV)
 Intercede Limited (INTRCED)
 Espion Limited (ESPION)
 Lonix Oy (LONIX)
 Bergische Universitaet Wuppertal (BUW)
 Esaprojekt SP Z OO (ESA)
 Comarch S.A. (CMR)

COUNTRY

Italy
 Italy
 Germany
 Israel
 Italy
 United Kingdom
 Ireland
 Finland
 Germany
 Poland
 Poland

SECCRIT / Secure Cloud Computing for Critical Infrastructure IT

© Thinkstock



Information

Grant Agreement N°

312758

Total Cost

€4,802,313

EU Contribution

€3,397,319

Starting Date

01/01/2013

Duration

36 months

Coordinator

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT)

Safety & Security Department

Donau-City-Straße 1
1220 Vienna

Contact

Thomas Bleier (Thematic

Coordinator ICT Security)

Tel: +43 664 8251279

Fax: +43 50550 2813

E-mail:

thomas.bleier@ait.ac.at

Markus Tauber (Project Manager SECCRIT)

Tel: +43 664 8251011

Fax: +43 50550 2813

E-mail:

markus.tauber@ait.ac.at

Website: www.seccrit.eu

Project objectives

The SECCRIT project is a multidisciplinary research project with the mission to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments. It will develop methodologies, technologies and best practices for creating a secure, trustworthy and high assurance cloud computing environment for critical infrastructure IT.

Description of the work

Cloud computing is a style of computing where elastic IT-related capabilities are provided as optimized, cost-effective, and on-demand utility-like services to customers using Internet technologies. Being one of the major trends in the IT industry recently, it has gained tremendous momentum and started to revolutionize the way enterprises create and deliver IT solutions.

As more sectors adopt cloud services in their computing environment, the trend will also reach ICT services operating critical infrastructures (CI), such as transportation systems or infrastructure surveillance. Hosting CI services in the cloud brings with it security and resilience requirements that existing cloud offerings are not well placed to address.

Due to the opacity and elasticity of cloud environments, the risks of deploying CI services in the cloud are difficult to assess – specifically on the technical level, but also from legal or business perspectives. Traditional IT security measures cannot fully tackle the issues (e.g. risk, trust, and resilience) arising from this paradigm shift, especially for operators and manufacturers of CI IT systems.

Therefore, the mission of the SECCRIT project is to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for CI.

To accomplish this, the objectives of the SECCRIT project are:

- » identification of the relevant legal framework and establishment of respective guidelines, provision of evidence and data protection for cloud services;
- » understanding and managing risk associated with cloud environments;
- » understanding cloud behaviour in the face of challenges;
- » establishment of best practice for secure cloud service implementations;
- » demonstration of SECCRIT research and development results in real-world application scenarios

Expected results

- » Establishment of legal fundamentals by identification and techno-legal modelling of legally subsumable scenarios
- » Methodologies and tools for risk assessment, policy specification and enforcement and assurance evaluation
- » Techniques for cloud analysis and forensics, frameworks for resilience management
- » Process-oriented security guidelines for critical infrastructure cloud services
- » Evaluation and application of SECCRIT results in two real-world pilot scenarios dealing with hosting of video surveillance and critical mobility services

PARTNERS

AIT Austrian Institute of Technology GmbH (AIT)
 ETRA Investigacion y Desarrollo, S.A. (ETRA)
 Fraunhofer IESE (IESE)
 Karlsruhe Institute of Technology (KIT)
 NEC Europe Ltd. (NEC)
 Lancaster University (LANC)
 Mirasys Ltd. (MIRASYS)
 Hellenic Telecommunications Organization S.A. (OTE)
 Ajuntament De Valencia (VALENCIA)
 Amaris (AMARIS)

COUNTRY

Austria
 Spain
 Germany
 Germany
 United Kingdom
 United Kingdom
 Finland
 Greece
 Spain
 Austria

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

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

COUNTRY

Norway
 United Kingdom
 United Kingdom
 Israel
 Greece
 Spain
 United Kingdom
 Israel

HARMONISE / Holistic Approach to Resilience and Systematic Actions to make Large Scale Urban Built Infrastructure Secure



Information

Grant Agreement N°
312013

Total Cost
€4,144,140.52

EU Contribution
€3,493,771.00

Starting Date
01/06/2013

Duration
36 months

Coordinator

FUTURE ANALYTICS CONSULTING LTD (FAC)
23 Fitzwilliam Square
(South)
Dublin 2, Ireland

Contact
Dr. William Hynes
Tel: +353 (0) 1 639 4836
Mobile:
+353 (0) 86 852 4438
Fax: +353 (0) 1 554 7334
E-mail: william.hynes@futureanalytics.ie
futureanalytics.ie
Website:
<http://futureanalytics.ie/>

Project objectives

The HARMONISE project will assess the vulnerability of urban infrastructure and will forge new opportunities for enhancing resilience of large scale urban built infrastructure. The concept will be designed for use by civil authorities/municipalities and other key stakeholders involved in the design, planning, construction, operation or use of large scale urban built infrastructure.

Specifically, HARMONISE will:

- » Deliver supporting tools (hosted within the platform) for the design/planning stage of large scale urban built infrastructure development; these will be tested/enhanced through quality case studies;
- » Provide an integrated approach to sharing building infrastructure and security information including critical flows of materials/energy and sensor technologies etc., while recognising the important role of security culture and societal acceptance aspects;
- » Be conducive to complementarities with other EU FP7 projects, not least VITRUV, BESECURE, RIBS and DESURBS;
- » Advocate and promote a significant exploitation programme to capitalise on new market opportunities, thus enhancing the pool of European expertise supported by a comprehensive education/training curriculum; and, ultimately,
- » Improve the design of urban areas and systems by increasing their security against, and resilience to, new threats.

Description of the work

The project will culminate in a holistic concept of innovative technology exploitation. This will be achieved by the development of a versatile, intuitive and interactive intelligence platform, with semantic data processing capabilities. Within this, all aspects of urban security and resilience are enshrined.

Developing a practical and holistic concept which addresses the range of complexities inherent in urban resilience, while fulfilling the objective of enhanced resilience in a sustainable way (and also ensuring acceptability by citizens).

HARMONISE will be a milestone project in the field of resilience, making a major contribution toward minimising the destruction and lethality arising from a range of potential disasters. It will provide solutions for adapting and responding to disaster scenarios, while also integrating aspects for the long term sustainability of large scale urban built infrastructure such as energy efficiency and multi-functionality.

Expected results

The final validated version of the HARMONISE platform is an interactive, holistic approach providing versatile support for end-users. The platform will contain relevant urban resilience information and host a portfolio of search, diagnostic, scenario modelling and management tools. Moreover, the platform will include educational elements that provide a 'virtual centre of excellence', and self-assessment tools that help end-users to assess the general resilience and security level of an existing

or proposed large scale infrastructure.

Within the portfolio catalogue end-users will have access to the “Harmonised Resilience Toolkit”. This suite of tools will include:

- » Dynamic approaches to Risk Assessment Methodologies;
- » Integration software (integrated management systems to combine previously isolated building systems);
- » Design and planning guidelines for resilience of large scale urban built infrastructure;
- » Socio-economic tools (includes societal acceptance

and adaptive governance measures);

- » Engineering/construction/retrofit tools (for best placement of sensor technologies, causal relationship analysis for non-compatible building system elements etc);
- » Critical flows (sustainability) tools for energy efficiency, smart grids and multi-functionality etc);
- » Educational multimedia tools (for promotion and dissemination of HARMONISE concept).

PARTNERS

Future Analytics Consulting Ltd (FAC)
 Teknologian Tutkimuskeskus VTT (VTT)
 University of Ulster (UU)
 Selex ES SPA (SXE)
 Fundacion Tecnalia Research & Innovation (Tecnalia)
 Bergische Universitaet Wuppertal (UW)
 Lonix OY (Lonix)
 Building Design Partnership Ltd. (BDP)
 LeighFisher Ltd. (LeighFisher)
 Ayuntamiento De Bilbao (Bilbao Council)
 Comune di Genova (CDG)
 University of Warwick (UoW)

COUNTRY

Ireland
 Finland
 United Kingdom
 Italy
 Spain
 Germany
 Finland
 United Kingdom
 United Kingdom
 Spain
 Italy
 United Kingdom

RIBS / Resilient infrastructure and building security



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 Borrión

Tel: +44 (0) 20 3108 3194

Fax: +44 (0) 20 3108 3088

E-mail: hborrión@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

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

COUNTRY

United Kingdom
 Israel
 Greece
 Sweden
 Denmark
 Greece
 United Kingdom

SECUR-ED / Secured urban transportation – European Demonstration



Information

Grant Agreement N°

261605

Total Cost

€40,188,876.20

EU Contribution

€25,468,072

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 flagship 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, SECUR-ED will reduce the security gaps in the mass transit nodes.

PARTNERS

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

COUNTRY

France
 France
 Italy
 Italy
 Germany
 France
 Spain
 Germany
 Belgium
 Portugal
 Sweden
 Germany
 Germany
 Spain
 Portugal
 Belgium
 Romania
 Portugal
 Israel
 Israel
 Germany
 France
 France
 Spain

 France
 France
 Italy
 Norway
 Belgium
 Netherlands
 Germany
 Belgium
 Belgium
 Finland
 Germany
 Spain
 Israel
 Sweden
 Turkey
 Italy

SPiRiT / Safety and Protection of built Infrastructure to Resist Integral Threats



Information

Grant Agreement N°
242319

Total Cost
€4,885,951

EU Contribution
€3,497,684.50

Starting Date
01/08/2010

End Date
31/07/2013

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: 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.

Results

The scope of SPiRiT concerned resilience against CBRE terrorist threats to large modern buildings where significant numbers of people may be present. Based on a preliminary threat assessment, a representative range of potential scenarios (20 chemical, 12 biological, 9 radiological and 14 explosive) was defined. Together with two concrete buildings whose structures are typical of urban landscapes, these scenarios formed the basis for the quantitative vulnerability study carried out by the project.

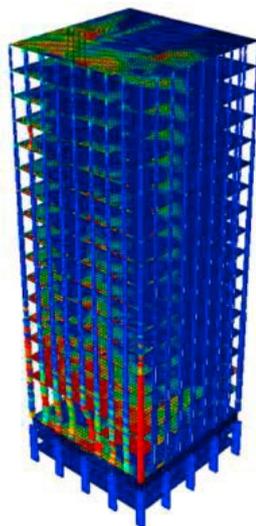
Extensive damage and consequence calculations (including loading predictions, dispersion calculations, injury and lethality predictions and finite element simulations) were performed to generate a database of results. These extend beyond the initially defined scenarios and buildings, offering options for applying the results to additional threats and structures.

With regard to the protective solutions, multiple tests and extensive assessments were conducted, thus yielding quantitative information about the protection level provided by the tested products. Designs of the studied protection products were improved and optimized, and their costs were studied. Other available protective solutions were identified through: internet searches, the

RESEARCH
COMPLETED

previous experience of consortium members and expo visits. All available information is gathered in a portfolio of protection products.

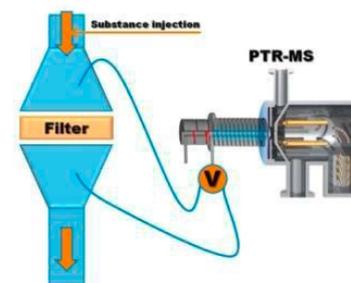
Recommendations for a regulatory framework and a guidance tool were also developed based on the risk assessment methodology, consequence models and data obtained. The guidance tool enables a user to quantitatively estimate the risks and consequences of chemical, biological, radiological and explosion (CBRE) attacks on new or existing buildings and to optimize their protective design. There are two versions of the guidance tool: a publically available demo version and the classified full tool.



Numerical simulation



Blast testing of glazing



Filter and detection system for C-threats

PARTNERS

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Schüßler-Plan Engineers Ltd (SP)
 Arup Group Ltd (ARUP)
 Hamilton Erskine Ltd (HE)
 Artemis control AG (ART)
 Ducon GmbH (DUC)
 Ionicon Analytik GmbH (ION)
 Corsmit Raadgevend Ingenieurs BV (CORS)
 European Commission - Joint Research Centre (JRC)

COUNTRY

The Netherlands
 Germany
 France
 Poland
 United Kingdom
 United Kingdom
 Switzerland
 Germany
 Austria
 The Netherlands
 Italy

VASCO / Virtual Studio for Security Concepts and Operations



Information

Grant Agreement N°
607737

Total Cost
€4,151,940.00

EU Contribution
€3,037,341.00

Starting Date
01/03/2014

Duration
36 months

Coordinator

DIGINEXT (DXT)

RTD Department / Simulation and Virtual Reality Division
ZAC de la Grande Plaine
5, rue Brindejonc des Moulinais
BP 15872
31506 TOULOUSE Cedex 5
FRANCE

Contact

Stéphane Collins

Tel: +33 5 61 17 66 66
Fax: +33 5 61 17 65 78
E-mail:
stephane.collins@diginext.fr
Website:
<http://vasco.diginext.fr/>

Project objectives

The concentrated localisation of government buildings and critical infrastructure sites, within or close to dense urban environments, is a source of serious security risks that are hard to anticipate: attacks on consulates and embassies, violent demonstrations near parliamentary buildings; attacks on government buildings or educational institutions; or the paralysing effects of natural disasters.

VASCO aims to:

1. develop a system to enable security professionals to construct and assess security concepts and measures, leading to an evidence-based, all-risk approach for the protection of government buildings of critical importance;
2. build a knowledge and best practice database to capture dynamic and visual reference scenarios based on VASCO's work.

VASCO will offer security experts:

- » a realistic visual representation of buildings within an urban environment, combining geographic details (roads, nearby buildings of potential relevance, critical infrastructures) with architectural information (lay-out of the building, exits, windows, garden entrances, roof top access, parking garage etc.);
- » capabilities to create dynamic scenarios, allowing security experts to employ their toolbox of virtual security devices (e.g. cameras, sensors) and security personnel in the virtual environment, and to simulate their behaviour and assess their effectiveness.

Description of the work

VASCO will develop the following:

- » a new-generation tool based on "serious game" principles and using the latest technologies for the study and assessment of security concepts and measures related to the protection of government building;
- » an automated software solution for rapidly reconstructing digital 3D mock-ups of buildings, including interiors from a series of photographs;
- » simulation capabilities to help users create dynamic scenarios that identify resources (e.g. security equipment and units), strategies, events, and threats ;
- » new interaction techniques such as tangible interfaces coupled with multitouch multiuser surfaces;
- » a VASCO software developer kit to enable third-parties to extend the system by implementing additional modules or gateways to other services and simulators;
- » the ability of the whole system to run on entry-level PCs or laptops, with the appropriate graphic board and hard drive.

Expected results

VASCO will help complete the product line for security and crisis management developed by DIGINEXT in the frame of the CRIMSON and INDIGO EC projects (<http://crimson.diginext.fr>, <http://indigo.diginext.fr>).

VASCO's expected results will:

- » enable users to rapidly and cheaply create a 3D digital model of a building, including interiors, and its environment from series of photographs;
- » offer a natural user interface, based on a set of real objects (e.g. rulers, pencils, erasers) to be used in conjunction with a multitouch multiuser table. This will allow users to intuitively edit the DMU, control simulations, or make annotations and measurements without having to learn a software user interface;
- » enable the creation and simulation of custom-made event- and threat-scenarios such as hostage-takings, fire, earthquakes and demonstrations, bomb blasting and architectural damages – and the response to these;
- » sensitize decision-makers, security teams and building owners to the security issues related to critical structures in dense urban environments through visual and educational scenarios;
- » allow use of visual reference scenarios to study and assess new security concepts, which are stored in a knowledge database. The latter will hold a wide variety of security concepts whose scenarios users can manipulate to test certain security concepts while holding other features constant. Thus, managers will be able to search the database for feasible strategies and learn from the experiences of other users. This will encourage users to store scenarios – fictitious and real – together with assessed security concepts. Future users will be able to access the scenario and the concepts, watching with detailed precision how a given threat evolved and what was done (or not) to counter it;

PARTNERS

DIGINEXT SARL (DXT)
 Consiglio Nazionale Delle Ricerche (CNR)
 Centro Di Ricerca, Sviluppo E Studi Superiori In Sardegna (CRS4)
 Immersion Sas (ISA)
 Center For Security Studies (KEMEA)
 Crisisplan B.V. (CRISP)
 Försvarshögskolan, Swedish National Defence College (CRISM)

COUNTRY

France
 Italy
 Italy
 France
 Greece
 The Netherlands
 Sweden

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

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

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

COUNTRY

Germany
 United Kingdom
 Italy
 United Kingdom
 Germany
 Denmark
 Netherlands
 Ireland
 Austria
 Netherlands
 France
 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

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 technologies;
- » 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

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

COUNTRY

Germany
 Germany
 France
 Belgium
 Germany
 The Netherlands
 France
 France
 Germany
 Slovenia
 The Netherlands

CWIT / Countering WEEE Illegal Trade



Information

Grant Agreement N°

312605

Total Cost

€1,868,303

EU Contribution

€1,868,303

Starting Date

01/09/2013

Duration

24 months

Coordinator

INTERNATIONAL CRIMINAL POLICE ORGANISATION (INTERPOL)

Environmental Security
Sub Directorate
INTERPOL General
Secretariat
200 Quai Charles de Gaulle
69006 Lyon, France

Contact

Laurent GROSSE

Executive Director,
Resource Management
Tel: +33 472 44 70 88
E-mail: lgrosse@interpol.int

David HIGGINS

Assistant Director,
Environmental Security
Sub-Directorate
Tel: +33 472 44 76 23
Fax: +33 472 44 73 51
E-mail: dhiggins@interpol.int

Therese SHRYANE

CWIT Project Coordinator
Tel: +33 472 44 71 60
Fax: +33 472 44 73 51
E-mail: tshryane@interpol.int
Website: www.cwitproject.eu

Project objectives

The aim of the CWIT – Countering WEEE Illegal Trade – project is to provide a set of recommendations to support the European Commission, law enforcement authorities, and customs organizations, countering the illegal trade of e-waste/WEEE (waste electrical and electronic equipment or e-waste) in and from Europe. The project will collect, study, and identify gaps in the current legislation in place at the International and European level.

Only around 3 million tons of an estimated total of 8 million tons in WEEE was officially collected, treated, and reported to authorities across Europe in 2010. WEEE contains materials such as gold, copper, and palladium which makes it very valuable on the black market; attracting not just illegal single operators but serious organised crime groups. However this waste also contains hazardous substances such as mercury and cadmium.

The CWIT project was established to identify the policy, regulatory, procedural, and technical gaps as observed in today's business environment, and to suggest tangible improvements.

Description of the work

Gap analysis

The project will collect, study, and identify gaps in the current legislation at the international and European level:

- » The Directive on Waste Electrical and Electronic Equipment (WEEE) (Recast) WEEE Directive 2012/19
- » The Directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) Directive Recast 2011/65/EU
- » Regulation 1013/2006 on Shipments of Waste

Illegal trade

In addition, the CWIT project will carry out intensive data collection and an intelligence-based approach to:

- » analyse the involvement of organized crime in the global distribution of WEEE;
- » analyse criminal activity and crime types associated with illegal WEEE shipments, drawing on other work carried out to target illegal e-waste exports on an international scale;
- » estimate the true volume of WEEE generated and the amounts inappropriately disposed of;
- » assess the typology of companies (and brokers) involved in the export market and identifying those with a criminal history; and
- » develop a detailed understanding of the destinations and routes used to carry illegal shipments.

Expected results

The CWIT project will develop a set of recommendations:

- » for the end user community that could improve the response to the illegal trade in WEEE;
- » for the European Commission and its member states related to future research and technologies

Finally the CWIT project will ensure a multi-layer platform for the exchange of information among law enforcement authorities, customs organisations, policy makers, etc. to enable them to improve their prevention and respond to the illegal trade of WEEE.

PARTNERS

International Criminal Police Organization (INTERPOL)
WEEE Forum
United Nations University (UNU)
Zanasi & Partners
Compliance & Risks
Cross Border Research Association (CBRA)
United Nations Interregional Crime and Justice Research Institute (UNICRI)

COUNTRY

France
Belgium
Japan
Italy
Ireland
Switzerland
Italy

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

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

COUNTRY

Sweden
 Italy
 France
 France
 Norway
 Germany
 Spain
 Norway
 Spain
 France
 Spain
 The Netherlands
 Finland

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



© sonya etchison - Fotolia.com

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 interventions 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

Sagem Défense Sécurité (SDS)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Cassidian S.A.S. (EADS)
 CENTER FOR SECURITY STUDIES (KEMEA)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Elsig Datamat spa (ED)
 National Centre for Scientific Research "Demokritos" (DEM)
 INFITHEON Technologies Ltd (INFI)
 T - SOFT spol. s r.o. Praha (TSOFT)
 National Civil Protection Service Directorate General (MES-TDCP)
 SELEX Sistemi Integrati S.p.A. (SSI)

COUNTRY

France
 The Netherlands
 France
 Greece
 France
 Italie
 Greece
 Greece
 Czech Republic
 Bulgaria
 Italie

EURACOM / European Risk Assessment and COntingency planning Methodologies for interconnected networks



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.

**RESEARCH
COMPLETED**

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

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

COUNTRY

EU
France
France
Belgium
The Netherlands
United Kingdom
Portugal

EUROSKY / Single European Secure Air-cargo Space



Information

Grant Agreement N°

312649

Total Cost

€19,086,960.06

EU Contribution

€11,708,124

Starting Date

01/05/2013

Duration

48 months

Coordinator

BMT GROUP LTD (BMT)

Research Directorate

Goodrich House,

1 Waldegrave Road

TW11 8LZ – Teddington

UK

Contact

Dr Fernando Caldeira-

Saraiva

Tel: +44 208 6144 244

Mobile: +44 7785 310 334

Fax: +44 208 977 9304

E-mail:

fernando@bmtmail.com

Website:

www.euroskyproject.eu

Project objectives

EUROSKY will deliver a high impact programme for improved air-cargo security and facilitation to safeguard international supply chains and the security of citizens whilst fostering international co-operation and a broad stakeholder engagement from all segments of the industry. The main project objectives are to:

- provide systemic solutions for European air cargo security that address prevailing complexities and vulnerabilities aligned with international initiatives, while building on complementary on-going projects
- offer different stakeholder groups enhanced capabilities for integrating preventive and reactive controls that address their threats in a timely and effective manner with optimised cost
- secure air cargo supply chains whilst facilitating the overall process (i.e. achieving security without stoppages, keeping the cargo movements unimpeded at all times).

Description of the work

Requirements analysis from security, legal, policy, market and technology perspectives will be undertaken and guided initially by the EUROSKY Demonstrators. Subsequently, stakeholder surveys and workshops will be used to broaden the coverage. An important outcome will be a detailed survey of security gaps and threats across the complete air cargo supply chain.

The results of the requirements analysis will be used to produce the EUROSKY blueprints. These will address:

- » integrated model of air-cargo security management including an air-cargo threat taxonomy
- » operational model for detection and targeting/detection prioritization
- » supervisory strategic management model

The EUROSKY solutions (Next Generation Screening Solutions, EUROSKY Ecosystem and Integrated Air-cargo Security Solutions) will be produced during the second year by leveraging the complementary competencies of the consortium partners and outputs from other related projects.

The Demonstrators will be used to validate the EUROSKY solutions under realistic conditions, to ascertain feasibility and benefits of the solutions and to provide feedback for improvements.

Expected results

EUROSKY will raise the bar in air cargo security to safeguard international supply chains and the security of citizens in general and that of air travellers across European states by: a comprehensive list of threats to the aviation system through an all-hazard approach;

- » contributing to the development of a unified European aviation security approach in a global supply chain context - the 'Single European Secure Air-cargo Space';
- » developing a strategic set of effective innovative measures (concepts, processes, technologies), centred on next-generation detection systems, to improve security whilst maintaining flows and optimising costs.

EUROSKY will:

1. Support European and international programmes aimed at:
 - a. Establishing a common approach and associated infrastructure for international co-operation and for enforcing air-security regulations and risk-based approaches in a uniform manner across the EU States;
 - b. Specifying detection technology requirements and future research areas;
 - c. Monitoring the effectiveness of regulations, standards and enforcement controls to fuel continuous improvement;
 - d. Managing changes, due to new or updated regulations, in a timely and cost effective manner.
2. Provide innovative aviation security solutions to implement EU policy addressing requirements from different industry stakeholder groups, including:
 - a. Fast screening approaches, facilitating planning and optimisation of resources;
 - b. Tools for managing compliance with changing regulatory requirements for both security and transport legislation, irrespective of destination and transit airports;
 - c. Integration capabilities for the optimisation of security and operational efficiency, utilising the latest technologies and best practices with clear and measurable benefits.

PARTNERS

BMT Group Limited (BMT)
 Swissport International AG (SWP)
 Athens International Airport SA (AIA)
 Department for Transport (DfT)
 Conzorzio IB Innovation (IBI)
 Urbanos-Group SGPS SA (URB)
 Geopost UK Ltd (GEO)
 Fast Freight Marconi SPA (FFM)
 Heavyweight Air Express Ltd (HWE)
 Rapiscan Systems Ltd (RSL)
 MULTIX SA (MLX)
 Totalforsvarets Forskningsinstitut (FOI)
 Inlecom Systems Ltd (ILS)
 Conceptivity SARL (CPT)
 Mass Spec Analytical Ltd (MSA)
 ENIDE Solutions SL (ENID)
 Commissariat a l'Energie Atomique et aux Energies Alternatives (CEA)
 MJC2 Ltd (MJC2)
 European Organisation for Security SCRL (EOS)
 Ingenieria IDOM Internacional SA (IDOM)
 CLMS (UK) Ltd (CLMS)

COUNTRY

United Kingdom
 Switzerland
 Greece
 United Kingdom
 Italy
 Portugal
 United Kingdom
 Italy
 United Kingdom
 United Kingdom
 France
 Sweden
 United Kingdom
 Switzerland
 United Kingdom
 Spain
 France
 United Kingdom
 Belgium
 Spain
 United Kingdom

GAMMA / Global ATM security management



Information

Grant Agreement N°

312382

Total Cost

€14,837,981.60

EU Contribution

€9,124,760.00

Starting Date

01/09/2013

Duration

48 months

Coordinator

SELEX ES S.P.A. (SELEX)

Air & Vessel Traffic Management Systems

Via Tiburtina, km 12.400

00131 - Rome - Italy

Contact
GIULIANO D'AURIA

Tel: +39 06 41504448

Mobile: +39 335 1629954

Fax: +39 06 41503156

E-mail: giuliano.dauria@

selex-es.com

Website: <http://www.gamma-project.eu/>

Project objectives

The GAMMA project stems from the growing need to address new air traffic management (ATM) threats and vulnerabilities due to the increased reliance on distributed enterprise computing and the automated flow of information across a ground and airborne network. In addition, there is a clear need to establish and implement a comprehensive framework for managing ATM security to minimise the effects of ATM crises brought about by security incidents.

For this purpose GAMMA aims to reach the following main objectives:

- » Extend the scope of security risk assessment performed within SESAR (Single European Sky ATM Research) to a more comprehensive system-of-systems level for a global approach to ATM security
- » Develop a global ATM security management framework, representing a concrete proposal for the day-to-day operation of ATM security and the management of crises at European level.
- » Define the requirements and architecture of an ATM security solution, suitable to support the security management of the global ATM system, in line with the directions and European regulatory baseline identified by the security management framework
- » Design and implement representative prototype components of the ATM solution to demonstrate, the functionalities and operations proposed for future European ATM
- » Set up a realistic validation exercises, representative

of the target ATM solution, through which to validate the feasibility and assess the adequateness of the procedures, technologies, and human resources issues proposed.

Description of the work

To reach these goals, GAMMA will first perform a comprehensive security risk assessment, by taking into account present and emerging set of threats and vulnerabilities affecting the existing ATM system. This analysis will provide the basis for GAMMA to develop a security management framework: a concrete proposal for the day-to-day operation of ATM security. It will also define the requirements and architecture of a security solution which will include the ability to manage incidents and crises spreading throughout the system. The solution will then be tested in exercises using a validation platform to include prototypes and demonstrators developed within the project.

GAMMA will approach the security aspects of the future ATM from an end-to-end perspective, consistent with the full SESAR vision, covering the following domains:

- » Airspace security incident management
- » Cyber security in ATM information flows
- » Communication, navigation and surveillance technologies
- » Ground Infrastructure security management

Expected results

The GAMMA project will produce solutions to emerging air traffic management vulnerabilities, backed up by practical proposals for their implementation.

The initial security risk assessment will result in threat scenarios, security objective reports and associated security controls. This will then be elaborate in a proposed solution covering both operational and technological elements to increase the capability of the ATM system to respond to attacks and manage any crises of the ATM service. The solution developed by GAMMA will be aligned with a proposed institutional framework for ATM security that reflects the interfaces and constraints of stakeholders.

Finally, GAMMA's solutions will be validated via exercises based on prototypes and via validation environments representative of the target architecture.

PARTNERS

Selex ES S.p.A. (SELEX)
 Airbus Prosky Sas (AIRBUS)
 Thales Alenia Space España, SA (TASE)
 Boeing Research & Technology Europe S.L.U. (BRTE)
 Enav S.p.A. (ENAV)
 Lancaster University (ULANC)
 Cassidian Sas (CASS)
 Cassidian Cybersecurity Sas (CYB)
 Deutsches zentrum fuer Luft – und Raumfahrt EV (DLR)
 RNC Avionics Limited
 Thales Research & Technology (UK) Limited (TRT)
 Società per azioni Esercizi Aeroportuali SEA S.p.A (SEA)
 42 Solutions BV (42S)
 Ingenieria de Sistemas para a Defensa de España SA (ISDEFE)
 Administratia Romana a Serviciilor de Trafic Aerian (ROMATSA)
 Ustav Informatiky, Slovenska Akademia Vied (SAV)
 Thales Avionics Sas (THALES)
 European Aeronautic Defence and Space company EADS France Sas (EADS)
 CiaoTech Srl (CTECH)

COUNTRY

Italy
 France
 Spain
 Spain
 Italy
 United Kingdom
 France
 France
 Germany
 United Kingdom
 United Kingdom
 Italy
 The Netherlands
 Spain
 Romania
 Slovakia
 France
 France
 Italy

INFRA / Innovative & Novel First Responders Applications



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.

RESEARCH
COMPLETED

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

Athena GS3 Security Implementations Ltd.
 Halevi Dweck & Co. ARTTIC Israel Company Ltd.
 University of Limerick
 ISDEFE Ingeniería de Sistemas S.A.
 Democritus University of Thrace
 Rinicom
 Everis Spain S.L.
 Hopling Networks B.V.
 Opgal Optronics Industries Ltd.
 Research and Education Laboratory in Information Technologies
 Arttic Israel International Management Services 2009 Ltd (AIL)

COUNTRY

Israel
 Israel
 Ireland
 Spain
 Greece
 United Kingdom
 Spain
 The Netherlands
 Israel
 Greece
 Israel

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



© TOM ANG - Fotofra.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.

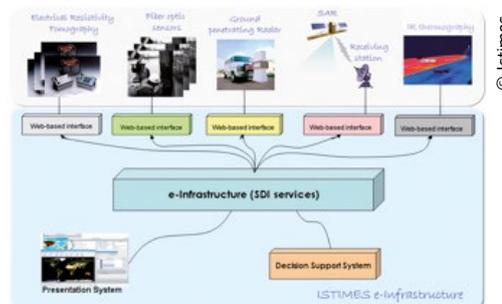
The project activities of ISTIMES have been broken down into five activities:

- » **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-infrastructure: 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.



PARTNERS

- Tecnologie per le Osservazioni della Terra ed i Rischi Naturali (TeRN)
- Elsag Datamat (ED)
- Dipartimento di Protezione Civile (DPC)
- Eidgenoessische Materialpruefungs- und Forschungsanstalt (EMPA)
- Laboratoire Central des Ponts et Chaussées (LCPC)
- Lund University (ULUND)
- Tel Aviv University (TAU)
- Territorial Data Elaboration SRL (TDE)
- Norsk Elektro Optikk (NEO)
- Telespazio S.p.A. (TPZ)

COUNTRY

- Italy
- Italy
- Italy
- Switzerland
- France
- Sweden
- Israel
- Romania
- Norway
- Italy

L4S / Learning for security project



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 organisations 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

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

COUNTRY

Greece
 Austria
 France
 Germany
 Greece
 Italy
 Italy
 Greece
 Spain
 Austria
 Germany

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

© Aaron Köhr - 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
VITROCISSET S.P.A.
Contact
Walter Matta

Tel: +39 06 88202567

Mobile: +39 335 7716488

Fax: +39 06 8820 2288

E-mail: w.matta@vitrocisset.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 identify 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 Krakow, an information service on Krakow'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

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

University of Greenwich (UoG)
 Consiglio Nazionale delle Ricerche (CNR-ISTC)
 Società Consortile a Responsabilità Limitata (CEFRIEL)
 Razvoj programske opreme in svetovanje d.o.o. (XLAB)
 Fondazione Ugo Bordoni (FUB)
 ORT FRANCE (ORT)
 University of East London (UEL)
 Business Flow Consulting (BFC)
 Emergency Planning College (EPC)

COUNTRY

United Kingdom
 Italy
 Italy
 Slovenia
 Italy
 France
 United Kingdom
 France
 United Kingdom

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

© PROTECTRAIL

RESEARCH
COMPLETED

Information

Grant Agreement N°
242270

Total Cost
€21,632,880.80

EU Contribution
€13,115,064

Starting Date
01/09/2010

End Date
30/06/2014

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

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 designed an interoperability framework built on a system-of-systems approach into which asset-specific and interoperable security solutions can be "plugged". This gives operators and infrastructure managers the possibility to adapt their security systems to changing security needs with minimal non-recurring costs. This framework consists of a set of rules and standards which facilitate the integration and communication amongst various security technologies. It is based on three concepts, namely that:

1. interoperability is improved through standardisation
2. re-use of existing and relevant international standards are preferred
3. simplicity is the key to long-term adoption.

Results

PROTECTRAIL tested this interoperability framework during field demonstrations at the main test site in Zmigrod, Poland and at satellite sites in Villecresnes, France and Palermo, Italy). These tests concentrated on four priority facets: an event-driven Service-Oriented Architecture (SOA), network communications, video management, and security technologies. PROTECTRAIL has met the challenges of both combining a large variety of technological and procedural security solutions, and reinforcing the strength of these solutions in a global and coherent system.

The methodology for the integration of security technologies in PROTECTRAIL has worked and has shown to be efficient, scalable and able to evolve with time. This is due to its simplicity, non-proprietary nature and standardisation. The integration of security technologies in the railway sector has thus been confirmed to be a complex but achievable goal, facing a broad spectrum of threats, from low-probability-high-impact events (e.g. terrorist attack) to high-probability-low-impact events (e.g. copper theft).

PARTNERS

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

COUNTRY

Italy
 The Netherlands
 Italy
 France
 Italy
 Germany
 France
 France
 Germany
 Belgium
 France
 Germany
 Slovakia
 Lithuania
 Italy
 Poland
 Italy
 Israel
 Belgium
 France
 United Kingdom
 France
 France
 Austria
 France
 France
 Turkey
 Italy
 France

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

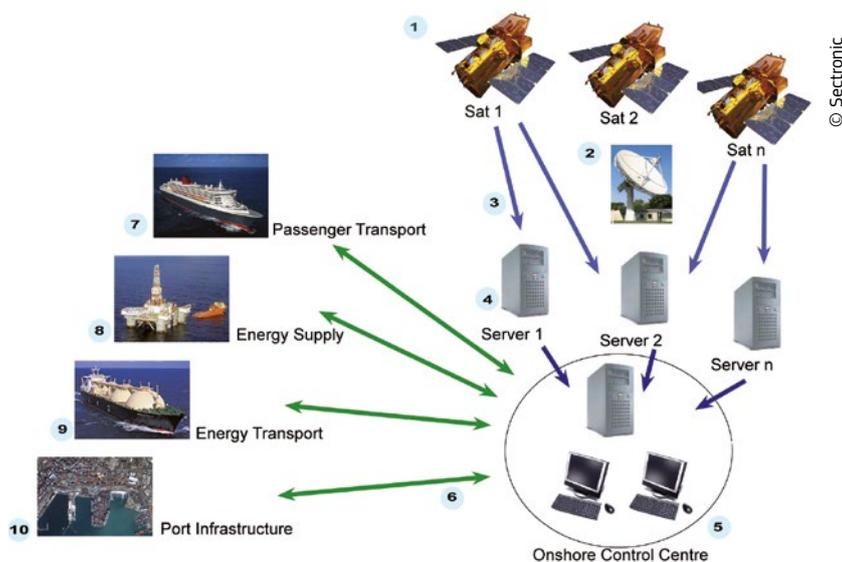
The project aimed to develop an integrated system for the security of maritime facilities: ports, passenger transport and energy supply. Project partners combined various observation systems (radar, sonar and Earth Observation (EO) satellites) to develop an early warning system that can be installed on a ship's bridge or in port control rooms.

This early warning system tracks and characterises objects of significance in a 360 degree radius around the infrastructure. Any identified threats are then communicated to the managers of the infrastructure and relevant authorities. The SECTRONIC system also facilitates responses to the identified threat(s).

As part of this work, the project analysed performance gaps in existing monitoring facilities, based on user-defined scenarios, and recommended new sensors and

algorithms. SECTRONIC also assessed current security alert reporting and operational performance practices. In addition, to make the system as user friendly as possible and to minimise response time, the project team identified optimal ways to integrate security information into the graphical user interface.

SECTRONIC's findings will help facility managers and emergency services to keep Europe's marine infrastructures safe from harm by identifying risks and responding to them effectively.



PARTNERS

Queen Mary, University of London Marine & Remote Sensing Solutions Ltd
 Uniresearch B.V.
 Det Norske Veritas AS
 Norwegian Defence Research Establishment
 Chalmers University of Technology
 Advanced Computer Systems ACS S.p.A.
 Nato Undersea Research Centre
 Carnival Corporation.
 BW Offshore AS
 BW Gas ASA
 Havenbedrijf Rotterdam N.V.
 Autorità Portuale della Spezia

COUNTRY

United Kingdom
 The Netherlands
 Norway
 Norway
 Sweden
 Italy
 Italy
 United Kingdom
 Norway
 Norway
 The Netherlands
 Italy

SERON / Security of road transport networks



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

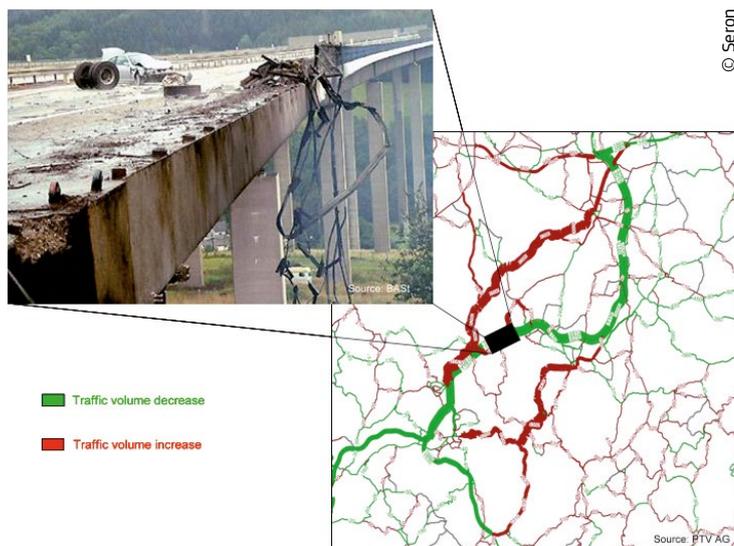
The SeRoN project undertakes a holistic approach at both infrastructure object and road network level. Its main objectives are to investigate the impacts of possible man-made attacks on the transport network, in particular the resulting regional and supra-regional impacts on transport links and their 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.



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

Politecnico di Torino (PoliTo)
 Energy Institute at the J. Kepler University Linz (EI-JKU)
 Indra Sistemas SA (INDRA)
 Heriot Watt University (HWU)
 e-Control (Ectrl)
 Deloitte (Delo)
 TU Delft (TUD)
 Transelectrica (TrEI)
 Kudos Research (KUDOS)

COUNTRY

Italy
 Austria
 Spain
 United Kingdom
 Austria
 Spain
 The Netherlands
 Romania
 United Kingdom

SPARKS / Smart Grid Protection Against Cyber Attacks



Information

Grant Agreement N°
608224

Total Cost
€4,913,955.40

EU Contribution
€3,429,551.00

Starting Date
01/04/2014

Duration
36 months

Project objectives

The aim of the SPARKS project is to promote awareness of existing and emerging smart grid cyber-security risks to stakeholders, including energy network operators, industry and policy makers. It will develop procedural and technical countermeasures, and provide cost assessments of key smart grid security technologies that are developed in the project. The project will also investigate privacy issues related to smart grid development.

Description of the work

The project will investigate risk assessment methods that are tailored to the smart grid. Tools will be developed to support these methods, including a novel cyber-attack simulation environment that can be used to measure the impact of an attack. Moreover, SPARKS will make recommendations about security architectures and standards for smart grids.

A number of key security technologies and measures will be developed via a set of mini-projects:

- » cyber-attack resilient control systems,
- » real-time network monitoring of SCADA-based control systems,
- » novel hardware security technologies for smart metering applications, and
- » security analytics techniques for smart grid.

Business cases for these technologies will be developed to support the case for their deployment. Additionally, the societal acceptance of smart grid security technologies will be investigated, along with the legal directives and regulatory requirements.

The research outcomes of the project will be demonstrated in a number of testbed and real-world deployment facilities. There will be a series of workshops across the project's lifetime to engage with stakeholders.

Coordinator

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT)

SAFETY &
SECURITY DEPARTEMENT
DONAU-CITY-STRASSE 1
1220 VIENNA, AUSTRIA

Contact
Dr Paul Smith
Tel: +43 664 88390031
Fax: +43 50550 2813
E-mail: paul.smith@ait.ac.at
Website:
<https://project-sparks.eu>

Expected results

The main impact of the SPARKS project is ensuring the security and resilience of future smart grid infrastructures.

SPARKS will deliver important new knowledge about vulnerabilities, attack vectors, security risks, legislation, and consequential costs to business and society.

To maximise our impact, SPARKS has identified a number of technology development areas that offer significant advances in the state of the art. With experienced technology experts working in the domains of SCADA intrusion detection, new methods for smart meter authentication, security information analytics and resilient power control systems, SPARKS will deliver impact right across the smart grid spectrum.

PARTNERS

AIT Austrian Institute of Technology GmbH (AIT)
 Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung e.V (Fraunhofer AISEC)
 Queen's University Belfast (QUB)
 Energieinstitut an der Johannes Kepler Universität Linz (EI)
 EMC Information Systems International Ltd (EMC)
 Kungliga Tekniska Hoegskolan (KTH)
 Landis + Gyr AG (L+G)
 United Technologies Research Centre Ireland, Limited (UTRC)
 SWW Wunsiedel GmbH (SWW)

COUNTRY

Austria
 Germany
 United Kingdom
 Austria
 Ireland
 Sweden
 Switzerland
 Ireland
 Germany

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



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.

RESEARCH
COMPLETED

Results

STAR-TRANS created models that can represent possible risk incidents, the structure and assets of Europe's heterogeneous transport systems, and the relationship between the different assets in the networks. In this regard, the project developed a STAR-TRANS modelling language and an impact-assessment modelling language.

PARTNERS

INTRASOFT International SA
 National Centre for Scientific Research Demokritos - Environmental Research Laboratory
 Center for Security Studies
 Confederation of Organisations in Road Transport Enforcement
 QinetiQ SA
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IVI)
 Centre for Research and Technology Hellas - Informatics & Telematics Institute
 Metropolitan Police Service
 CTL Cyprus Transport Logistics Ltd
 SQUARIS Ltd
 SOCIETA RETI E MOBILITA SPA (SRM)

COUNTRY

Luxembourg
 Greece
 Greece
 Belgium
 United Kingdom
 Germany
 Greece
 United Kingdom
 Cyprus
 Belgium
 Italy

STRUCTURES / Strategies for the Improvement of Critical Infrastructure Resilience to Electromagnetic Attacks



Information

Grant Agreement N°

285257

Total Cost

€4,797,731.63

EU Contribution

€3,497,673.54

Starting Date

01/07/2013

Duration

36 months

Project objectives

The aim of the STRUCTURES project is to analyze the possible effects of intentional electromagnetic interference (IEMI) on civilian infrastructures (power plants, communication systems, computer networks, etc.) and assess the related impact for defense and economic security. Innovative awareness and protection strategies will be identified and an outline of the actual threats and consequences of an electromagnetic attack will be provided to policy makers.

Description of the work

The Project is part of the more general theme of "Critical Infrastructures Protection", focusing in particular on the "Intentional ElectroMagnetic Interference" (IEMI) threat.

Such a threat is going to become in the next future more and more dangerous due to the largest availability of low/medium cost electromagnetic sources and to the increasing technical level of terrorism and organized crime.

The project will go through a number of steps to develop new capabilities and technologies and acquire information on IEMI effects in order to help civil society and policy makers to fight such a threat.

A first step will be the assessment of the scenarios of interest and the identification, preparation and validation of analytical/numerical and experimental methodologies for risk assessment and design of protection devices.

An investigation on IEMI effects on the critical infrastructures and sub-systems will follow, as well as the identification and testing of cost-effective technologies able to improve the infrastructure resilience.

Finally Guidelines and methodologies for IEMI protection will be developed and organised in pre-regulatory documentation.

Coordinator

INGEGNERIA DEI SISTEMI

S.P.A. (IDS)

Business Development

VIA FLAMINIA, 1068

00189 ROME,

ITALY

Contact

Aldo Bonsignore

Tel: +39 0633217414

Mobile: +39 3357458088

Fax: +39 0633217402

E-mail: abonsignore@idscorporation.com

[idscorporation.com](http://www.idscorporation.com)

Website:

<http://www.idscorporation.com>

Expected results

The Project is expected first of all to provide improved comprehension of the problems and risks related to IEMI attacks to Critical Infrastructures

Further, viable (e.g. not only technically but also economically sustainable) solutions to estimate and reduce the risk will be made available to be provided to policy makers and Critical Infrastructure managers.

PARTNERS

Ingegneria Dei Sistemi S.p.A (IDS)
 Ecole Polytechnique Fédérale de Lausanne (EPFL)
 Haute Ecole Spécialisée de Suisse Occidentale (HES-SO)
 The University of York (UoY)
 MONTENA technology sa (Montena)
 Helmut-Schmidt- Universität (HSU)
 Leibniz Universität Hannover (LUH)
 Bergische Universität Wuppertal (BUW)
 Bergische Universität Wuppertal (RWM)
 University of Twente (UT)
 Istituto Superiore Mario Boella (ISMB)
 Navigate Consortium (NAVI)

COUNTRY

Italy
 Switzerland
 Switzerland
 United Kingdom
 Switzerland
 Germany
 Germany
 Germany
 Germany
 The Netherlands
 Italy
 Italy

TASS / Total airport security system

© josh webb - istockphoto.com


**RESEARCH
COMPLETED**
Information
Grant Agreement N°

241905

Total Cost

€14,966,370.60

EU Contribution

€8,986,696.15

Starting Date

01/04/2010

End Date

31/03/2014

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

Airports, airplanes and air travellers are often the targets of terrorists, a reality that poses many security challenges and requires a variety of security systems. The EU-funded project TASS – “Total airport security system” – is addressing these threats through the development of a sophisticated surveillance system that represents a security monitoring solution for an entire airport. The system is being designed to enhance the efficiency and reliability of security screening while protecting the privacy and rights of airport passengers.

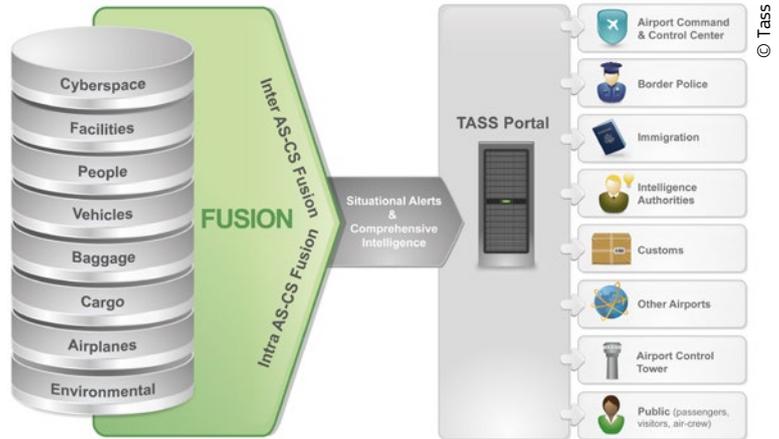
Description of the work

Offering real-time situational awareness of all airport facilities and surroundings – including people, vehicles, cargo and airplanes – the system collects and analyses data from different sources and technologies. It features three main components: the front end, the data fusion and mediation system, and portal/back-end applications. The portal displays all security and transport information, and notified authorities to execute decisions rapidly. It also minimises errors and false alarms.

So far, the project team has progressed well towards developing the system. After having mapped and classified potential threats to airports, it outlined the required technologies, designed the system’s architecture and adapted its front-end systems to airport environments. This has yielded a full ready-to-use TASS prototype. Testing took place at Heathrow International Airport in the United Kingdom in a complex system that combined many different components and systems. These ranged from various kinds of sensors and global position system tracking technologies to radio-frequency identification systems and an unmanned ground vehicle.

Results

With its integrated approach to airport security, TASS has effectively created a comprehensive airport security intelligence solution that offers accurate real-time situational awareness to airport authorities. Once finalised and commercialised, the solution promises to become an important alternative to current airport security systems. It will help thwart terrorist attacks, minimise injuries and save lives wherever it is implemented, making the world's airports safer than ever.



PARTNERS

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

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

XP-DITE / Accelerated Checkpoint Design Integration Test and Evaluation

© Thinkstock



Information

Grant Agreement N°

285311

Total Cost

€14,613,264.82

EU Contribution

€9,992,634.87

Starting Date

01/09/2012

Duration

55 months

Coordinator

NETHERLANDS ORGANISATION FOR APPLIED SCIENTIFIC RESEARCH (TNO)

Safety and Security Research
LANGE KLEIWEG 137

PO BOX 45

2280 AA RIJSWIJK,
THE NETHERLANDS

Contact

Mark van den Brink

Tel: +31 8886 63898

Mobile: +31 6 3015 8707

Fax: +31 8886 66938

E-mail:

mark.vandenbrink@tno.nl

Project objectives

The aim of the XP-DITE project is to develop, demonstrate and validate a comprehensive, passenger-centred approach to the design and evaluation of integrated security checkpoints at airports.

A key element of the project is the development of a design tool that allows the design of innovative new checkpoints and modification of existing checkpoints to meet combinations of overall system level requirements. Another major deliverable comprises a validated set of protocols and tools for evaluating the performance of the checkpoint, again at the system level.

Description of the work

Airport Checkpoint (ACP) requirements at overall checkpoint system-level are determined for security, operational, passenger perception and ethical aspects. A conceptual model is developed to enable development of the design process and evaluation platform. All requirements are assessed by the XP-DITE advisory board, expert groups and ethical advisory group.

A design process and supporting software (Design Tool) based on the conceptual model and overall system requirements will be developed. The design process is foreseen to be used for the creation or adaptation of an airport checkpoint and for the assessment of new technologies.

Computational evaluation methods at system or checkpoint level will build on the conceptual model. The aim is to quantify the overall performance from the properties of all the components involved. An experimental evaluation method for checkpoints will be developed with the aim of proposing a standard on-site test prescription for checkpoints applicable to any EU airport. Both compu-

tational and experimental methods will be combined into a single interface, the Shared Evaluation Platform (SEP), allowing for easy facilitation and evaluation of checkpoints at system level.

Proofs-of-concept airport checkpoint will be integrated and installed at Schiphol Airport and Manchester Airport. To fully demonstrate and exploit the capabilities of the XP-DITE results, not only commercial off-the-shelf components but also mature, close-to-market-introduction technologies will be developed. The results of the tests at airport and laboratory scale are given as feedback to the Design Tool and the SEP.

The results of the project will be disseminated widely and actively into the European security community by different means, such as websites, brochures, publications, conferences and workshops.

Expected results

The XP-DITE approach will allow airports, checkpoint designers and regulators to incorporate a wide range of requirements and to evaluate checkpoint performance against security performance, cost, throughput, passenger satisfaction and ethical factors. This will help ensure robust and controllable aviation checkpoint security performance, whilst providing freedom for airport operators to design checkpoints with innovative technologies and procedures.

All extra time spent at the airport has a cost. It means less time to spend at work, with children and for leisure. There are also secondary effects from the delays that create new costs. For example, longer delays at the airport encourage passengers to seek new modes of transportation for their trips, such as driving, that are less safe.

XP-DITE will have a positive impact in this respect by showing the way and handing the tools to reduce airport checkpoint delays, even with improved security.

adopting a unified approach on design and evaluation of airport checkpoints, introducing new system-level performance requirements.

Now security operations at European airports account for about 35 per cent of operating costs. These costs are either born by the passenger or else by the taxpayer. In many Member States, airports pay for their own security measures; in others the government picks up the tab. The total societal costs of security measures are even higher when factors such as delays, time needed to screen passengers at airports, and non-monetary costs such as privacy concerns or ethics balancing are considered.

XP-DITE will show that advanced, customer friendly and cost-effective security checkpoints can be achieved by

PARTNERS

Netherlands Organisation for Applied Scientific Research (TNO)
 Fraunhofer-gesellschaft zur Foerderung der angewandten Forschung (Fraunhofer)
 Swedish Defence Research Agency (FOI)
 Ingeniera de Sistemas para la Defensa de Espana (ISD)
 Schiphol Nederland (AAS)
 Morpho (MPH)
 Smiths Heimann (SMI)
 Eurofast SARL (IDP)
 Iconal Technology (ICO)
 Cascade Technologies (CAS)
 Alfa Imaging (ALF)
 Albert-Ludwigs-Universitaet Freiburg (UNF)
 The Manchester Airport Group (MAN)

COUNTRY

The Netherlands
 Germany
 Sweden
 Spain
 The Netherlands
 France
 Germany
 France
 United Kingdom
 United Kingdom
 Spain
 Germany
 United Kingdom

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

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

COUNTRY

Germany
 Belgium
 Belgium
 France
 United Kingdom
 Germany
 Italy
 Germany
 Germany

IPATCH / Intelligent Piracy Avoidance using Threat detection and Countermeasure Heuristics



Information

Grant Agreement N°

607567

Total Cost

€4,181,126

EU Contribution

€2,976,845

Starting Date

01/04/2014

Duration

36 months

Coordinator

BMT GROUP LTD (BMT)

Research Directorate

Goodrich House

1 Waldegrave Road

Teddington

TW11 8LZ

United Kingdom

Contact

Tom Cane

Tel: +44 (0) 20 8943 5544

Mobile:

+44 (0) 7500 871 748

E-mail:

tcane@bmtmail.com

Website: www.bmt.org

Project objectives

IPATCH addresses the issue of modern piracy and the challenges faced by merchant shipping in keeping crews safe whilst minimising costs. IPATCH will provide ships with new technology for enhanced early detection of piracy threats and real-time decision support for utilising countermeasures appropriately, effectively and safely if they come under attack.

The end of the 20th century has seen an unprecedented resurgence in piracy. In particular, the breakdown of governments and the ensuing lack of "law and order" in African nations have transformed the Gulf of Aden and, more recently, the Gulf of Guinea into some of the world's most dangerous places for commercial and private vessels. Piracy is also on the rise in other regions of the world, including South East Asia and South America. The international community has reacted to these threats with an increased military presence, but the immense costs of these operations demand that further non-military options need to be explored.

Recent years have seen an increase in the use of private maritime security companies on board ships. Whilst effective, these companies often act in a legal "grey area", and the high cost and risk of escalation of violence means they are not a viable solution for all shipping companies. More generally, a comprehensive analysis of available countermeasures is lacking, and inappropriate use can result in unnecessary extra cost for shipping companies and can actually place the ship and its crew at further risk.

Description of the work

IPATCH seeks to address these challenges by first performing an in-depth analysis of the effectiveness and costs – including the legal, ethical and societal implications – of piracy countermeasures. This analysis will be

based on historical data, expert knowledge and consultation with shipping companies and other stakeholders.

The results from this analysis will be compiled in a manual to provide well-founded and quantified recommendations to the industry, extending and complementing the IMO's Best Management Practices.

Finally, IPATCH will develop an onboard system for the early detection and classification of piracy threats with a decision support tool to assist the crew in making critical decisions on what actions to take for a given scenario. The IPATCH onboard system will consist of three elements:

- » A sensor suite, incorporating existing surveillance capabilities of the vessel (e.g. radar, AIS), and extending and complementing them with the use of advanced visual, thermal and infrared cameras.
- » A threat recognition system which fuses data from various sensors and employs new detection, tracking and situational awareness algorithms to give early warning of piracy threats to the captain and crew.
- » A decision support tool, which provides real-time situation information to the captain and crew and helps them select the most appropriate countermeasures and best course of action to take to protect the ship and crew from piracy threats as they develop, based on the knowledge captured at the beginning of the project.

The development of the system will take as its starting point the architecture developed in the FP7 project ARENA, which focused on the detection and classification of threats to mobile assets, specifically land-based trucks. In IPATCH, the ARENA platform will be refined and adapted for specific use in the maritime domain.

Towards the end of the project, a demonstration of

automated detection and decision support for piracy threats will be carried out on board a real vessel and threat scenarios will be simulated in order to evaluate the performance of different aspects of the system.

Expected results

IPATCH will provide:

- » A knowledge base that consolidates historical data on piracy incidents from heterogeneous sources, covering details on the attack, the defensive actions of the vessel, and the ensuing costs and impacts. The information will be augmented with evaluations of the legal, ethical, societal and economic implications of different countermeasures.
- » A manual on the use and implementation of countermeasures against piracy based on results from the historical analysis and stakeholder consultations.
- » An onboard system for the early detection and classification of piracy threats, building on the architecture from the ARENA project.
- » A maritime data set, comprising a collection of fully annotated and documented sensor data from realistic simulated piracy environments, to enable the development and performance evaluation of maritime threat detection algorithms. The dataset will be published for the benefit of both the maritime and research communities.

PARTNERS

BMT Group Ltd (BMT)
 Totalforsvarets Forskningsinstitut (FOI)
 University of Reading (UoR)
 ITTI Sp. z o.o. (ITTI)
 Università Cattolica del Sacro Cuore (UCSC)
 Sagem Défense Sécurité (SAG)
 Termisk Systemteknik i Sverige AB (TST)
 Université de Namur ASBL (UoN)
 Foinikas Shipping Company NE (FNK)

COUNTRY

United Kingdom
 Sweden
 United Kingdom
 Poland
 Italy
 France
 Sweden
 Belgium
 Greece

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.

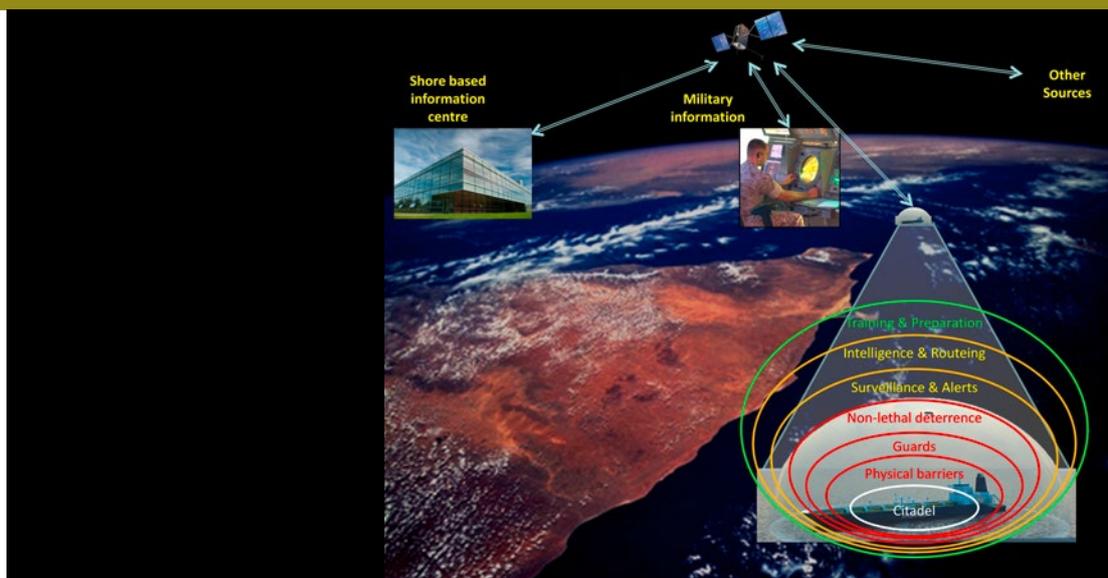
PARTNERS

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

COUNTRY

United Kingdom
 Spain
 Switzerland
 Belgium
 Poland
 Belgium
 United Kingdom
 Switzerland

PROMERC / Protection Measures for Merchant Ships



Information

Grant Agreement N°

607685

Total Cost

€3,131,452.00

EU Contribution

€2,224,958.00

Starting Date

01/03/2014

Duration

24 months

Coordinator

FLIR SYSTEMS LTD

(FLIR)

MARSS

2 Kings Hill Avenue
ME19 4AQ - West Malling -
United Kingdom

Contact

Craig Cooper

Tel: +44 1732 220011

E-mail:

Craig.Cooper@flir.uk.com

Website: www.flir.com

Project objectives

PROMERC aims to reduce the vulnerability of EU merchant fleets and maritime supply lines to criminal abduction and extortion and thereby reduce risk to mariners, shipping, and the environment, while also reducing costs. This will be delivered through the provision of:

- » Independent review and recommendations about non-lethal technologies for pirate avoidance and opposing the boarding of vessels by pirates;
- » An automated voyage planning support tool to aid shore based authorities, which will balance route management to mitigate risk against incurring additional fuel costs due to re-routeing and increased speed;
- » An automated decision support tool to provide seafarers with real time threat assessment, evaluation of possible courses of action and a recommended course of action. A manual to aid in the selection and use of appropriate counter piracy measures in a layered holistic defence;
- » Recommendations on the further development of counter piracy measures.

Description of the work

The PROMERC consortium brings together end-users, commercial, political, academic, and military entities along with leading research companies and agencies. The consortium's broad commercial and military security experience will be supported by active stakeholder engagement throughout.

The work falls into the following sections:

- » Current and Future Non-Military Counter Measures

The first part of PROMERC will identify and catalogue the different existing and potential non military protection measures against piracy available to the shipping industry. In addition to identifying current and emerging measures, the catalogue will also differentiate between active versus passive measures. Within the active measures, differentiation will be made between lethal vs. non-lethal measures. An assessment of the operational effectiveness of the Counter-measures will be made.

- » PEESLE constraints

An analysis of the Political-Economic-Ethical – Societal – Legal – Environmental (PEESLE) constraints on the use of existing and potential non-military protection measures will be performed.

- » Evaluation of Options

The operational effectiveness and findings from the previous two work packages will be developed to conduct a total cost benefit analysis, to develop a manual to aid in the selection and use of appropriate counter piracy measures in layered holistic defence and a user configurable counter measures Knowledge base which will provide recommendations on counter measures based on user entered constraints, cost and effectiveness thresholds.

- » Development of Tools

The heart of PROMERC will be the development and demonstration of decision aids for commercial shipping. One will provide an automated voyage planning support tool which will create seven day forecasts of piracy risks with real skill combining factors such as the day of the

week, the moon phase and visibility, location, season, environmental conditions (e.g. wind speed), with ship and voyage specific factors to produce routes optimised to minimise cost and risk.

The other will be a Counter-Measures Decision Aid to provide dynamic situation sensitive advice and guidance to the bridge team incorporating near real time updates and underpinned by the Counter Measure Knowledge Base to produce accurate up-to-date assessments.

Expected results

The PROMERC project will apply advanced geospatial analysis and intelligence techniques to provide the shipping industry with a layered approach to planning, routing and threat reduction that goes beyond current solutions. PROMERC will organize and consolidate the many dimensions of risk reduction by delivering a knowledge base, manuals and tools to assess the available counter-measures, the current and future threat situations, to identify and quantify the risks and to aid decisions before and during voyages. The system will provide situation and ship specific counter-measures and best practice guidance prior to and during the voyage, as well as interactive route planning tools to develop the counter-measures and sail plan to an acceptable level of risk and cost.

PARTNERS

FLIR Systems Ltd (FLIR)
 NATO Science and Technology Organization (CMRE)
 IMO World Maritime University (WMU)
 University of the Aegean – research Unit (UoA)
 Security Association for the Maritime Industry Ltd (SAMI)
 Uniresearch B.V. (UNR)
 Netherlands Organisation for Applied Scientific Research (TNO)
 Engineering Ingegneria Informatica Spa (EII)
 OLDENDORFF Carriers GmbH & Co KG (OLD)

COUNTRY

United Kingdom
 Italy
 Sweden
 Greece
 United Kingdom
 The Netherlands
 The Netherlands
 Italy
 Germany

SAFEPOST / Reuse and development of Security Knowledge assets for International Postal supply chains

© BMT GROUP LIMITED



Information

Grant Agreement N°

285104

Total Cost

€14,986,407.66

EU Contribution

€9,523,423

Starting Date

01/04/2012

Duration

48 months

Coordinator

Association of European**Public Postal Operators****AISBL (PostEurop)**

PostEurop Projects

Department

114 Boulevard Brand

Whitlock

1200 Brussels,

Belgium

Contact**Antonino Scribellito**

Phone: +32 2 773 11 93

Mobile: +32 491 08 57 25

Fax: +32 2 771 48 58

E-mail:

antonino.scribellito@

posteurop.org

Website:

www.posteurop.org

www.safepostproject.eu

Project objectives

SAFEPOST aims to raise the current level of postal security by integrating innovative screening solutions that: 1) do not disrupt the flow of enormous volumes of parcels and letters associated with operational postal processes and 2) support customs and counter-crime intelligence work within a European-wide cooperative distributed model.

Description of the work

Starting from the perspective of the partner postal operations, the project will first identify the main security threats and threat actors and the main security gaps in postal operations. Secondly, it will describe security measures and process improvements to maintain or augment the efficient and secure operation of postal services to address the identified threats.

After completing an inventory of security gaps, these will be developed into generic postal security models which will be integrated into a Postal Security Target Operating Model. This will enable postal operators, customs and other relevant actors to understand how to securely exchange information related not only to security but also to the optimization of postal flows.

To support the Postal Security Target Operating Model, a Postal security platform will be developed to help extend the current MEDICI effort. It will exploit previous FP7 project developments regarding e-freight and secure supply chains. SAFEPOST will extend the concept of its Postal Security Target Operating Model to propose a 'Common Postal Security Space' with a view to creating a future European/World Postal Security information sharing system.

Expected results

SAFEPOST will provide and showcase a novel solution for postal security that combines: supply chain and security performance and to monitor supply chain vulnerabilities.

- » security performance-enhancing solutions for postal operators;
- » postal operations efficiency improvements to compensate for time lost in screening;
- » EU coverage to raise level of postal security across all member states;
- » a postal security platform that facilitates interoperability and the integration of solutions across all domains

The results of the SAFEPOST will have a strategic impact in the following areas:

- » improving the EU's awareness and coordination of activities within and between EU Member States in the field of postal security and developments in supply chain security
- » linking EU projects from (DG MOVE, DG TAXUD, DG JLS, DG ENTR, DG JRC11) and national efforts to exploit synergies and create a coordinated approach to security throughout the entire supply chain;
- » encouraging all European post offices and related authorities to assume responsibility in securing their own processes within a European-wide cooperative distributed model;
- » creating transparency in the way postal security measures are enforced, and providing benchmarks;

- » establishing a Europe-wide forum to discuss and agree a Postal Security Target Operating Model which could provide the basis for standardization.

PARTNERS

Association of European Public Postal Operators AISBL (PostEurop)
 BMT Group Limited (BMT)
 Geopost – La Poste Group (GEO)
 Totalförsvarets forskningsinstitut (FOI)
 Tellusecure AB (TLS)
 MJC2 Limited (MJC2)
 INLECOM Systems Ltd. (ILS)
 Correos y Telégrafos S.A. (COR)
 Atos Spain S.A. (ATOS)
 Stichting Nederlands Normalisatie-instituut (NEN)
 Confederation of Organisations in Road Transport Enforcement AISBL (CORTE)
 Hellenic Post S.A (ELTA)
 K-NET S.A. (KNET)
 MARLO AS (MARLO)
 Fundación Zaragoza Logistics Center (ZLC)
 CONCEPTIVITY (CPT)
 Íslandspóstur hf (IP)
 Università degli Studi di Genova (UNIGE)
 Cross-border Research Association (CBRA)
 European Organisation for Security S.C.R.L. (EOS)

COUNTRY

Belgium
 United Kingdom
 France
 Sweden
 Sweden
 United Kingdom
 United Kingdom
 Spain
 Spain
 The Netherlands
 Belgium
 Greece
 Greece
 Norway
 Spain
 Switzerland
 Iceland
 Italy
 Switzerland
 Belgium

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

© Lv Design - Fotolia.com


**RESEARCH
COMPLETED**
Information
Grant Agreement N°

218197

Total Cost

€4,483,794

EU Contribution

€3,229,034

Starting Date

01/08/2009

End Date

31/07/2013

Coordinator
TOTALFORSVARETS
FORSKNINGSINSTITUT

 Division of Information
Systems

Postal Box: 1165

SE-58111 Linköping

Sweden

Contact
Jörgen Ahlberg

Tel: +46 13378068

Mobile: +46 706757384

Fax: +46 13378287

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.

Results

Current automatic detection systems struggle to make inferences about the intent of human behaviour. ADABTS has addressed the problem of identifying threatening or anomalous behaviour by extracting characterizations in realistic security settings based on expert classifications and the analysis of operator behaviour. Furthermore ADABTS has developed models for certain threats (e.g., violence) and for the typical behaviour in specific contexts, as well as methods for detecting these threats and deviations from the typical behaviour in surveillance data. A prototype system has been developed, creating a proactive system that focuses on detecting the presence of threatening or anomalous behaviour. The system allowed for the operator to focus purely on suspicious situations, as opposed to trying to follow all situations

at all times in public spaces.

ADABTS links different sensor techniques that allow for the system to cope with sensor uncertainties and thus enhancing the system performance. This allows for new system functionality that will disregard the vast amount of imagery that contains nothing unusual and will present events in the footage where something interesting might be going on. Improved events detection would benefit CCTV operators' effectiveness, leading to shorter reaction time concerning violent events. Furthermore, automated offline abilities, like searching databases, would also facilitate subsequent content-based retrieval in images after an incident. This creates new possibilities for increased security against threats like terror, crime and riots by enhanced warning systems. capabilities at a football stadium.

PARTNERS

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

COUNTRY

Sweden
 Norway
 The Netherlands
 The Netherlands
 Bulgaria
 United Kingdom
 United Kingdom
 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

Starting Date

16/05/2011

Duration

36 months

Coordinator

TOTALFORSVARETS**FORSKNINGSINSTITUT**

Swedish Defence

Research Agency

Gullfosgatan 6

STOCKHOLM, 164 90

Sweden

Contact**Åsa Waern**

Tel: +46 13378084

E-mail: asa.waern@foi.se

Website:

<http://www.foi.se>**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

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

COUNTRY

Sweden
United Kingdom
Poland
France
France
The Netherlands
United Kingdom
France

ARGOS / Advanced pProtection of critical buildinGs by Overall anticipating System

Smart Engine



Multisensory data fusion and data mining



Discrimination of false alarms and processing alerts by a Rules Based Engine (RUBE)

Gateway



Self-powered communications network



Pre-processing data functions in gateway

Multimodal Sensors network



Audio/Video sensors



Infrared sensors and laser scanners



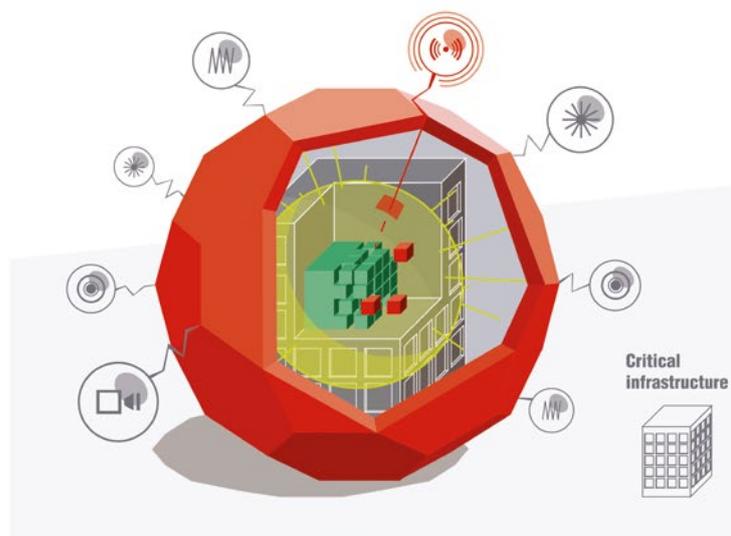
Wake-up cameras



Vibration sensors



Infrasound sensors



Information

Grant Agreement N°

313217

Total Cost

€4,645,416.00

EU Contribution

€3,464,258.50

Starting Date

01/01/2014

Duration

36 months

Coordinator

EVERIS SPAIN SL

Security & Defence
Avenida Manoteras 52
Madrid 28050 SPAIN

Contact

Mario Carabaño Marí

Tel: +34 91 749 00 00

E-mail: mario.carabano.mari@everis.com

Website: www.argos-project.eu

Project objectives

Socioeconomic activities such as supply and distribution of gas or electricity and the infrastructures that generate it or transport it are vital to the day-to-day functioning of any country. Due to several factors, the social and financial European situation, or supply constraints, energy and utilities have become a prominent issue in Europe.

Any uncontrolled disruption in those types of infrastructures may result in an unacceptable loss of human lives and a huge impact on the economic and social well-being of any country. It is critical to protect these infrastructures from threats to avoid potential disruption.

ARGOS [Advanced pProtection of critical buildinGs by Overall anticipating System] is a multimodal early warning security solution for Critical Infrastructures focused on low consumption technologies and detection algorithms based on data fusion and data mining smart techniques.

Description of the work

It is a 4.5 million euro project co-funded by the European Commission under the 7th Framework Programme that started in January 2014 and will end in December 2015. The ARGOS Consortium covers the entire value chain and includes all the expertise required for the successful execution of the project. The 13 partners are from seven different countries with a wide range of capabilities.

ARGOS will allow end-users to deploy the solution beyond the actual perimeter of the infrastructure, extending the "security zone" beyond the critical perimeter by defining wide early-warning areas that will enhance the Critical Infrastructures capacity to monitor, deter and respond to potential threats.

It is well-suited for remote semi-urban or non-urban environments where energy is not always available, since the solution will be based on an energy efficient algorithm for data processing, low-energy communications, self-powered networks of sensors, sleeping mode for video sensors and energy-efficient microelectronics. ARGOS will also focus on the development of non-privacy-invasive technologies such as vibration sensors and embedded video and audio analytics so capturing devices will transfer metadata instead of recorded images or sounds.

Some of the subsystems that encompass the ARGOS solution are, for example, vibration sensors, Infrared Cameras and Laser Telemeters, infrasound sensors, a module for data fusion and another one for data mining, audio and video analytics.

Expected Results

ARGOS will simultaneously evaluate and cross-check the inputs coming from the multimodal network of sensors in order to minimise false alarms, using data mining to account for correlations and interdependencies. Also the system will implement a “guided learning” methodology letting the operator teach the engine whether an alarm is true or false, in an iterative cycle of continuous and progressive improvement.

During the duration of the project, field trials will be done where the solution will be tested as means of validation. The first of the two trials will be done in Transgaz’s facilities (Bucharest) and will test the protection of a long cross Critical Infrastructure, such as a gas pipeline. The second trial will take place in the nuclear

facilities from the National Centre for Scientific Research Demokritos (Athens) and will test the protection of an energy producer critical infrastructure.

PARTNERS

Everis (EVR)
 S.C. Mira Telecom S.R.L. (MIT)
 Aratos Technologies S.A. (ARA)
 INFITHEON Technologies (INF)
 Centre For Security Studies (KEMEA) (KEM)
 HI-iberia Ingeniería y Proyectos (SL HIB)
 Athens Information Technology
 VTT Technical Research Centre of Finland
 Thales Services SAS (THA)
 Charles University in Prague (CUNI)
 Athena GS3 Security Implementations Ltd (ATH)
 National Centre for Scientific Research Demokritos (NCSRD)
 Port Authority of Gijon (PAG)

COUNTRY

Spain
 Romania
 Greece
 Greece
 Greece
 Spain
 AIT Greece
 VTT Finland
 France
 Czech Republic
 Israel
 Greece
 Spain

BASYLIS / moBile, Autonomous and affordable SYstem to increase security in Large unpredictable environments



© bluefern - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°

261786

Total Cost

€2,989,194.80

EU Contribution

€2,037,265

Starting Date

01/05/2011

End Date

31/05/2013

Project objectives

The BASYLIS system aims to create a transportable security platform capable of detecting a wide range of pre-determined 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.

Results

A system that ensures the complete protection of a Refugee camp on different levels thanks to long range systems like radar and lidar, to low range systems like underground seismic and metal sensor, and personal protection systems like bracelets and button alarm system, all with the aid of a system of video classification and an Acoustic Vector Sensors system and a multi-tracker and behaviour analysis system.

Coordinator

IP SISTEMAS

Calle Anabel Segura
n° 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

Description of the work

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.

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

The BASYLIS system integrates all the sensors in a unified system, incorporating three intelligence levels and merges alarms coming from different sensor for the same object before sending the data to a Behavioural Analysis module.

PARTNERS

IP SISTEMAS (IP)
NEW TECHNOLOGIES GLOBAL SYSTEMS (NTGS)
UNIVERSITA DEGLI STUDI DI FIRENZE (UFL)
TERMA A/S (TERMA)
MICROFLOWN (MICROFLOWN)
MIRASYS OY (MIRASYS)
UNIVERSIDAD POLITECNICA DE MADRID (UPM)
UNIVERSITY COLLEGE LONDON (UCL)
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS (CNPIC)

COUNTRY

Spain
Spain
Italy
Denmark
Netherlands
Finland
Spain
United Kingdom
Spain

IDETECT 4ALL / Novel Intruder Detection & Authentication

Optical Sensing Technology



© Antonis Papanthoniou - Fotolia.com

**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

Instro Precision Ltd.
 Motorola Israel Ltd.
 EVERIS Consulting
 Cargo Airlines
 3D s.a.
 ANA Aeroportos de Portugal
 LACHS
 Azimuth Technologies Ltd.
 S.C. PRO OPTICA S.A.
 Halevi Dweck & Co. Arttic Israel Company Ltd. (ARTTIC)
 Arttic Israel International Management Services 2009 Ltd (AIL)

COUNTRY

United Kingdom
 Israel
 Spain
 Israel
 Greece
 Portugal
 Belgium
 Israel
 Romania
 Israel
 Israel

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



© Auke 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

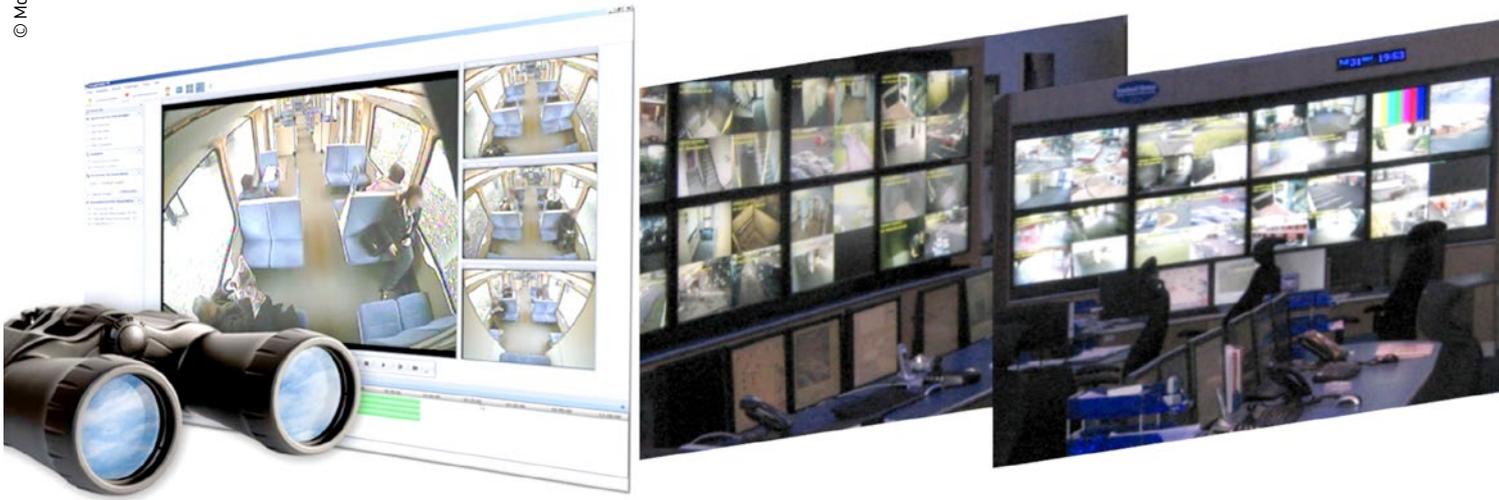
AGH University of Science and Technology (AGH)
 APERTUS Távoktatás-fejlesztési Módszertani Központ Tanácsadó és Szolgáltató Közhasznú Társaság (APERTUS)
 Gdansk University of Technology (GUT)
 InnoTec DATA G.m.b.H. & Co. KG (INNOTECH)
 Grenoble INP (INP)
 General Headquarters of Police (GHP)
 INDESOL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

COUNTRY

Poland
 Hungary
 Poland
 Germany
 France
 Poland
 Spain
 Germany
 United Kingdom
 Poland
 Spain
 Bulgaria
 Germany
 United Kingdom
 Czech Republic
 Slovakia
 Austria
 Austria

MOSAIC / Multi-Modal Situation Assessment & Analytics Platform

© Mosaic



Information

Grant Agreement N°

261776

Total Cost

€3,606,642

EU Contribution

€2,664,559

Starting Date

01/04/2011

Duration

36 months

Coordinator

THE UNIVERSITY OF READING

Intelligent Media Systems
and Services Research La-
boratory, 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@reading.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

The University of Reading (UoR)
 BAE Systems (Operations) Ltd (BAE)
 A E Solutions (BI) (AES)
 SYNTHEMA S.R.L. (SY)
 TECHNISCHE UNIVERSITÄT BERLIN (TUB)
 DRResearch Digital Media Systems GmbH (DR)
 WEST MIDLANDS POLICE AUTHORITY (WMP)
 INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)
 WARWICKSHIRE POLICE (WP)

COUNTRY

United Kingdom
 United Kingdom
 United Kingdom
 Italy
 Germany
 Germany
 United Kingdom
 Belgium
 United Kingdom

P5 / Privacy Preserving Perimeter Protection Project



Information

Grant Agreement N°
312784

Total Cost
€4,823,592.80

EU Contribution
€3,499,169.00

Starting Date
01/08/2014

Duration
36 months

Coordinator

**FOI – TOTALFORSVARETS
FORSKNINGSINSTITUT**

Division of Sensor
and EW Systems
Olaus Magnus väg 42
Linköping 581 11
SWEDEN

Contact

Dr. Ola Friman

E-mail: ola.friman@foi.se

Project objectives

The goal of P5 is the development of an intelligent, proactive perimeter surveillance system that works robustly under a wide range of weather and lighting conditions and that has strong privacy preserving features. The system will monitor the region outside the security area of critical buildings and infrastructure, and give early warning if terrestrial or airborne threats are detected. The work is carried out by nine partners and is coordinated by FOI, the Swedish Defence Research Agency. The research and development activities within P5 are financed by the participating organisations themselves and by the European Commission through the Framework 7 Grant 312 784.

Description of the work

The system will support, rather than replace, a human operator. A low false alarm rate due to animals or other innocuous events, combined with high threat detection sensitivity and privacy standards, are central ambitions of the project. To achieve these goals, a multispectral sensor suite comprising both passive and active sensors is envisaged, i.e., a system based on radar, visual and thermal sensors. The sensor suite will be complemented with advanced algorithms for information fusion, object detection and classification, privacy preservation, and high level modelling of intent and behaviour analysis.

Expected results

The P5 project is strongly user-driven and demonstration of the developed surveillance system will be conducted at two different critical infrastructure sites. Finally, the P5 project will make contributions to evolving standards in detection systems.

PARTNERS

TOTALFORSVARETS FORSKNINGINSTITUT (FOI)
 THE UNIVERSITY OF READING (UOR)
 TERMISK SYSTEMTEKNIK I SVERIGE AB (TST)
 SAGEM DEFENSE SECURITE (SAG)
 FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX DE NAMUR (FUNDP)
 VISUAL TOOLS SA (VT)
 IMST GMBH (IMST)
 OKG AKTIEBOLAG (OKG)
 HOME OFFICE CAST

COUNTRY

Sweden
 United Kingdom
 Sweden
 France
 Belgium
 Spain
 Germany
 Sweden
 United Kingdom

SAMURAI / Suspicious and Abnormal behaviour Monitoring Using a network of cAmeras for situation awareness enhancement

© diego cervo - Fotolia.com

RESEARCH
COMPLETED

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.

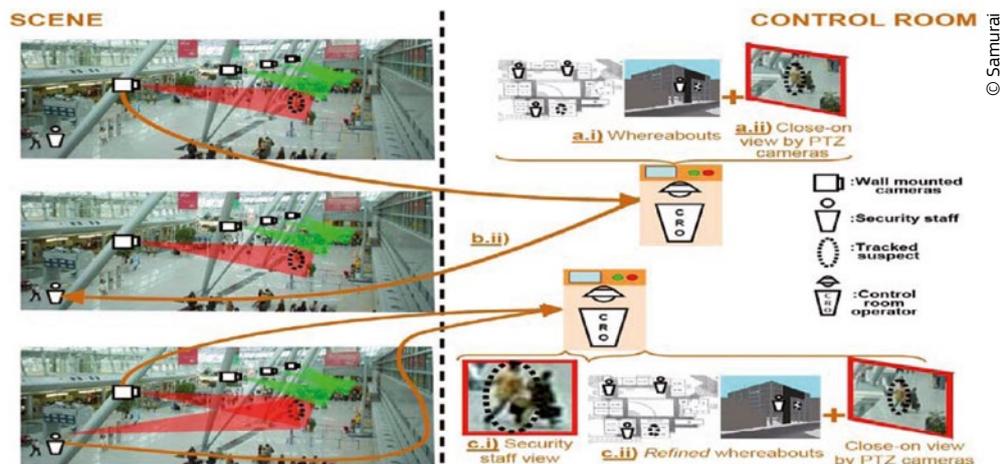
For combining sensor data, SAMURAI produced new visualisation software, the SUMURAI GUI, to display data from different inputs in one window. As well as active 3D image mapping, this includes a background algorithm that automatically filters out “useless” motion from sensor images to leave only relevant,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

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



© Artsem Martysjuk - Fotolia.com

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

SELEX Sensors and Airborne Systems Limited
ELSAG DATAMAT S.p.A
Office National d'Etudes et de Recherches Aérospatiales
L-1 Identity Solutions AG
Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
University of Leeds
University of Reading
Valtion Teknillinen Tutkimuskeskus (VTT)
Österreichisches Forschungs und Prufzentrum Arsenal Ges.m.bH
Fiera di Genova S.p.A
The Chancellor, Masters and Scholars of the University of Oxford

COUNTRY

United Kingdom
Italy
France
Germany
France
United Kingdom
United Kingdom
Finland
Austria
Italy
United Kingdom

ARGUS 3D / AiR GUIDANCE and Surveillance 3D

© Argus - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°

218041

Total Cost

€4,943,520

EU Contribution

€3,262,050

Starting Date

01/12/2009

End date

30/11/2012

Coordinator

SELEX SISTEMI**INTEGRATI SPA****Civil Systems Business****Unit**

Via Tiburtina, 1231

00131 Rome

Italy

Contact**Claudia Fusai**

Tel: +39 06 4150 5370

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.

Results

ARGUS 3D developed two types of non-conventional radar systems that can detect, recognize and track NCT

(non-cooperative targets). The first system, "3D PSR", uses a monopulse estimation capability in the vertical plane, enabling it to identify the altitude of any detected target. The second system – composed of passive and bi-static radar sensors – detects and tracks objects by processing reflections from sources of illumination already available in the environment such as commercial broadcasts or communication signals.

The two systems were successfully tested in seven different scenarios:

1. small civil airport
2. transponder out of service or switched off
3. tracking of ultra-light motorized
4. small touristic aircraft
5. commercial flights
6. PSR (primary surveillance radar) out of service
7. quasi-real simulated scenario (Rome region)

In each test, ARGUS 3D systems were tested alongside conventional ATC systems. All the results obtained confirmed that ARGUS 3D could improve current ATC systems via :

- » extending the coverage for specific zones where conventional systems typically have difficulty
- » greater provision of estimated altitude of targets where this was previously impossible
- » passive radar networks to fuse information and alarm systems
- » provision of surveillance information without interruption
- » control of the flight in case of data provided by conventional surveillance
- » updating of the final user about the dangerous situation detected by the passive radar network
- » establishing a suitable security level and reaction time upon detection of a target

PARTNERS

Selex Sistemi Integrati (SELEX-SI)

SESM Scarl (SESM)

Università "La Sapienza" di Roma Dip. di Scienza e Tecnica dell'Informazione e della Comunicazione (INFOCOM)

Przemysłowy Instytut Telekomunikacji S.A. (PIT)

University College of London (UCL)

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)

ENAV S.p.A (ENAV)

ECONET S.L. (ECONET)

Dependable Real Time Systems Ltd. (DRTS)

ISO Software Systeme GmbH (ISO)

REDHADA S.L. (REDHADA)

CiaoTech Srl (CTECH)

COUNTRY

Italy

Italy

Italy

Poland

United Kingdom

Germany

Italy

Spain

United Kingdom

Germany

Spain

Italy

ABC4EU / Automated Border Gates For Europe



Information

Grant Agreement N°
312797

Total Cost
€16,817,103.60

EU Contribution
€12,015,246.04

Starting Date
01/01/2014

Duration
42 months

Coordinator

INDRA SISTEMAS S.A.
(INDRA)
SECURITY SYSTEMS /
ELECTRONIC IDENTITY
ANABEL SEGURA 7
28108 – Alcobendas-
Madrid - Spain

Contact
Daniel Cuesta
Tel: +34 91 480 7993
Fax: +34 628 23 82 50
Fax: +34 91 480 6031
E-mail: dcuesta@indra.es
Website: www.abc4eu.com/
www.abc4eu.eu

Project objectives

The Main Goals of the ABC4EU Project are:

- » Analyse the ABC concept vs EU legislation, in particular the Schengen Border Code, to identify which processes can / cannot be automated and the impact that different levels of automation could have in the SBC procedures.
- » Optimize and harmonize the ABC processes related to the increasing flow of people crossing borders.
- » Assess the feasibility of a future Registered Travel Programme (RTP) in the EU which could be integrated into the ABC gates that would allow third country nationals to benefit from an automated BCP process in terms of flow efficiency, while maintaining the security requirements of the border crossing.
- » Assess the feasibility of a future Entry / Exit System (EES) in the EU which could be integrated into the ABC gates.
- » Evaluate, optimize and harmonize the use of 2nd generation passports biometrics for passengers' identification.
- » Identification and design of a basic set of features to achieve a common user experience.
- » Identification and removal of obstacles which are preventing today the certification distribution throughout Europe both for ePassport verification (CSCA – DS certificates) and for Extended Access Control (TA certificates) to access the fingerprint information in 2nd generation ePassports.
- » Assess and evaluate the compliances of the proposed processes with the legal requirements to protect fundamental rights, in particular the protection of personal data and with ethical principles.

Description of the work

The main objective of the ABC4EU project is to update and integrate the current ABC gates systems already deployed in many member states extending its use to second generation passports and citizens of countries outside the EU. In ABC4EU, the upgrade and testing of the ABC gates will be done in the pilots deployed in Spain and Portugal (in airports, harbours and land borders).

In ABC4EU, RTP and EES concepts will be developed and tested in order to assess their feasibility.

In ABC4EU, special attention will be paid to legal, social and ethical issues and for dissemination and exploitation. ABC4EU consortium considers that all the research carried out in the project has to be compliance to the laws related to border controls in the European Union and respectful to the rights of the European and third country citizens, from the social and ethical point of view.

Expected results

- » The need for harmonization in the design and operational features of an ABC System across the E.U. Border Crossing Points (BCPs) is the main goal of the project. The harmonisation and standardisation proposals to be produced by ABC4EU will include requirements and guidelines for all affected parties in the border policy division.
- » Development of concepts for the expansion of ABC systems for Third-Country Nationals (RTP, EES and Integration with other Back-Office systems).
- » Definition of the concept for the inclusion of BCPs into an Integrated Border Management System (both national and EU level).
- » Contribute towards extending the usage of fingerprint verification, not only as a complement to facial biometrics, but as a fundamental part of border control.

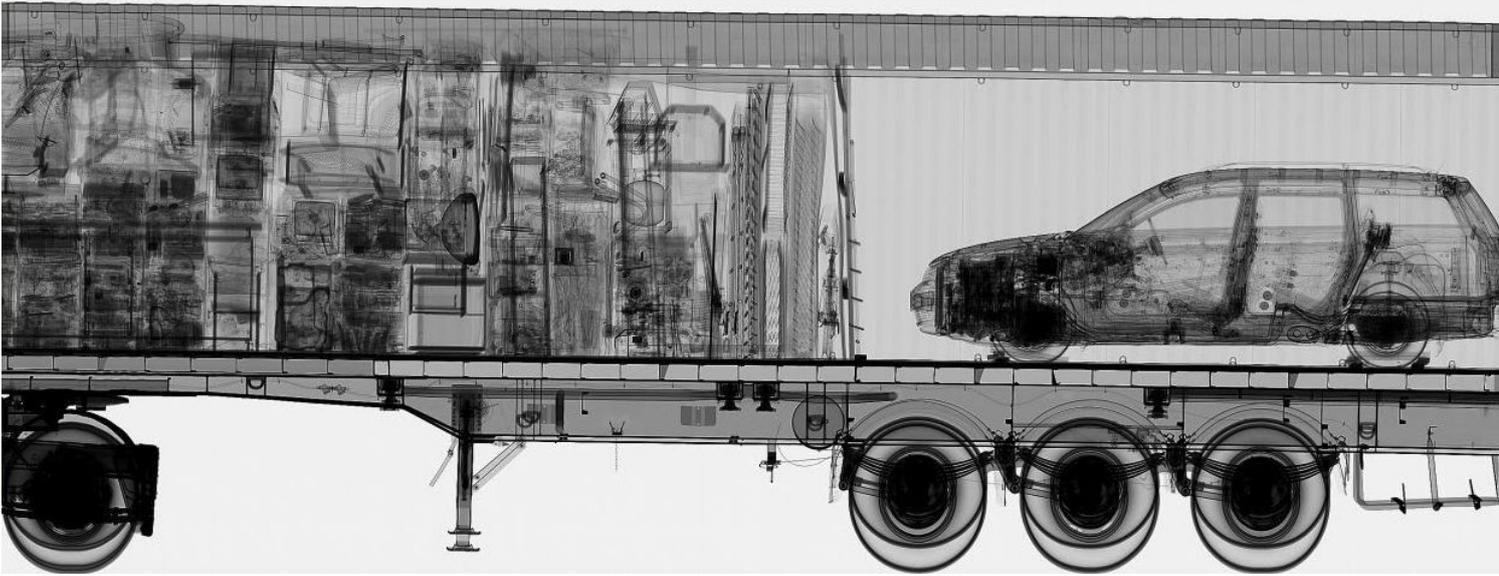
PARTNERS

Indra Sistemas, S.A. (INDRA)
 PricewaterhouseCoopers Auditores, S.L. (PWC)
 Vision-Box, Soluções de Visão por Computador, S.A. (VISIONBOX)
 Laurea-ammattikorkeakoulu Oy. (LAUREA)
 Eticas Research and Consulting, S.L. (ETICAS)
 Centre for Irish and European Security, Ltd. (CIES)
 Dermalog Identification Systems, GMBH. (DERMALOG)
 Cognitec Systems GmbH. (COGNITEC)
 Universidad Rey Juan Carlos. (URJC)
 Università degli Studi di Milano. (UMIL)
 SAFE ID Solutions GmbH. (SAFE ID)
 Ministerio del Interior – Spanish National Police. (MIR-DGP)
 Ministério da Administração Interna – Serviço de Estrangeiros e Fronteiras. (SEF)
 Politsei- ja Piirivalveamet. (EPBGB)
 Ministerul Afacerilor Interne. (GDCIT)

COUNTRY

Spain
 Spain
 Portugal
 Finland
 Spain
 Ireland
 Germany
 Germany
 Spain
 Italy
 Germany
 Spain
 Portugal
 Estonia
 Romania

ACXIS / Automated Comparison of X-ray Images for cargo Scanning



Information

Grant Agreement N°
312998

Total Cost
€4,771,721

EU Contribution
€3,394,004

Starting Date
01/09/2013

Duration
42 months

Coordinator

**EIDGENOESSISCHE
MATERIALPRUEFUNGS-
UND FORSCHUNGSANS-
TALT (EMPA)**

Center for X-ray Analytics
Ueberlandstrasse 129
CH-8600 Duebendorf

Contact
FLISCH ALEXANDER
Tel: +41 58 765 45 67
Mobile : +41 79 109 26 81
Fax: +41 58 765 11 22
E-mail:
alexander.flisch@empa.ch
Website: www.empa.ch

Project objectives

The main objectives of the project ACXIS are to develop a manufacturer independent reference data base for X-ray images of illegal and legitimate cargo, procedures and algorithms to uniform X-ray images of different cargo scanners and measurement parameters, and an automated identification of potentially illegal cargo.

Historic images of real detections and images of illegal cargo mock-ups as well as images of legitimate cargo will be integrated into the reference data base. This database will automatically analyse the image and will independently inspect uncritical cargo. The new system will be analysed in collaboration with end-users, scientists, and security experts in order to define different threats in cargo screening scenarios.

Current training consists in the identification of a small set of critical cargo elements superimposed on historic images of the inspection system. A draw-back of this system is the adaption of the inspection officer to the small set of training images that are usually limited due to factors like confidentiality of the image data. The set of training images is significantly enhanced if artificial cargo image can be generated with arbitrary positioning of objects in the image data base.

The highly innovative system will be implemented using a simulator to be used in the field by end users in order to ensure optimal results.

Description of the work

The ACXIS project work programme consists of six work packages. The first work package comprises the financial, technical and organisational management of the project. In the second work package, cargo mock-ups will be built and scanned with different X-ray systems. The X-ray images will be integrated in the manufacturer independent reference data base.

Work package three is the development of a data base system to store images of historic detections as well as mock-up images of illegal and legitimate cargo (recorded in work package two) in the standard representation of cargo images to be developed in work package four. In the same work package, methods to streamline the images from different X-ray scanner manufacturers, to reduce background from the containment and to correct artefacts from scattering and imperfect detection systems will be developed to guarantee comparability of the images.

Work package five will develop new concepts for the inspection and automated detection of illegal cargo based on the newly developed data base of reference images. In work package six, the results of all other work packages will be compiled into a working demonstrator that can be employed for on-site presentation of the newly enabled detection capabilities. State-of-the-art computer-based training will be further developed in order to achieve the maximum possible detection by the new cargo inspection system. In work package six, the system will be validated and both exploitation and dissemination activities will be coordinated.

Expected results

ACXIS is expected to:

- » A system consisting of three components: a way to transform X-ray images into a standard cargo image, a database filled with images of legal and illegal cargo, and software to determine illegal cargo.
- » A database with image analysis that will utilise cargo X-rays for inspection officer training.
- » Optimisation of detection system for the maximum benefit of Customs officers and independency on scanner's manufacturer based on end user collaboration and testing.

Implementation of detection software as an add-on to existing scanners independent of scanner's manufacturer.

As both data base and detection procedures are developed based on the reference data type, the resulting procedures can be applied Europe-wide as soon as all manufacturers will provide the corresponding interface.

In the ACXIS project, the tutor system of CASRA for luggage screening shall be expanded for the application on high-energy cargo inspection systems combining the data base, the frame work to generate artificial images and the tutor software system.

PARTNERS

Eidgenössische Materialprüfungs- und Forschungsanstalt (EMPA)
 APSS Software & Services AG (CASRA)
 Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)
 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (EZRT)
 Smiths Heimann S.A.S. (SH)
 Eidgenössische Zollverwaltung (FCA)
 Ministere van Financien Directoraat Generaal Belastingdienst (DTCA)

COUNTRY

Switzerland
 Switzerland
 France
 Germany
 France
 Switzerland
 The Netherlands

CONSORTIS / Concealed Object Stand-Off Real-Time Imaging for Security



Information

Grant Agreement N°

312745

Total Cost

€5,132,839

EU Contribution

€3,953,449

Starting Date

01/01/2014

Duration

38 months

Coordinator

TEKNOLOGIAN
TUTKIMUSKESKUS VTT
(VTT)

Intelligent Sensor Systems

Tietotie 3

P.O. Box 1000

FI-02044 VTT, Espoo,

Finland

Contact
M. Sipilä

Tel: +358 20 722 7007

Fax: +358 20 722 7001

E-mail:

consortiscoordinator@vtt.fi

Website: www.consortis.eu

Project objectives

The project will develop a demonstrator for detection of stand-off real-time concealed objects to support high throughput security screening for European mass-transit markets and infrastructure security.

Description of the work

The technological approach will build on and extend current millimetre-wave imaging technology. The system will undergo an end-user demonstration at a European transport hub.

The ethical issues surrounding the use of stand-off body scanners will be evaluated to ensure that the technology is properly deployed.

The consortium includes end-users as project partners who will ensure maximum relevance and impact to the user community.

The consortium will also address the exploitation of the technology developed in the project, especially the commercialisation and manufacture of the technology through the small and medium sized enterprises involved in the project.

Expected results

A main concrete output of the project will be a live demonstration of the working system at an airport. This demonstration is intended to give end users the opportunity to see the system in operation in a realistic environment.

The results will also include their experience and comments about the system's performance and limitations. From the general public's point of view, the main result will be a better traveller experience with less intrusion into privacy, less encroachment, shorter waiting times and fewer restrictions – all with ethical considerations fully taken into account.

PARTNERS

Teknologian tutkimuskeskus VTT (VTT)
 Asqella Oy (AQA)
 The University Court of the University of St Andrews (USTAN)
 InnovaSec Ltd (ISEC)
 Totalförsvarets forskningsinstitut (FOI)
 Eberhard Karls Universität Tübingen (EKUT)
 Wasa Millimetre Wave Ab (WMW)
 Gotmic Ab (GOTMIC)
 Finavia Oyj (FNA)
 Rapiscan Systems Ltd. (RSN)
 Technische Universiteit Delft (TU Delft)

COUNTRY

Finland
 Finland
 United Kingdom
 United Kingdom
 Sweden
 Germany
 Sweden
 Sweden
 Finland
 United Kingdom
 The Netherlands

DOGGIES /

Detection of Olfactory traces by orthoGonal Gas identification technologies



Information

Grant Agreement N°
285446

Total Cost
€4,940,117.60

EU Contribution
€3,499,966.00

Starting Date
01/06/2012

Duration
36 months

Coordinator

III V LAB GIE (III-V LAB)
Optronics Devices Research
Group
1, avenue Augustin Fresnel
F-91767 Palaiseau Cedex,
FRANCE

Contact
Dr. GERARD Bruno
Tel: +33 (0)1 69 41 57 91
Mobile:
+33 (0)6 82 76 47 76
Fax: +33 (0)1 69 41 57 38
E-mail:
bruno.gerard@3-5lab.fr
Website: www.3-5lab.fr

Project objectives

The key objective of DOGGIES is to develop an integrated sensor system for the detection of illegal substances and hidden persons. This would complement trained dogs currently used in border checks and custom points by police units.

The project aims to demonstrate:

1. an operational movable stand-alone sensor for efficient detection of hidden persons, drugs & explosives;
2. the potential adaptation of this solution to the detection of a much wider range of illegal substances.

One of the main operational challenges is to provide reliable detection in real environments, in particular with the presence of "interferents".

It is expected that the use of specific pre-concentrators on one hand, and the combination of the signal emerging from advanced software on the other hand will improve the detection reliability.

Description of the work

The initial phase of project starts with the definition of the operational system requirements and the end-users requirements.

Local environmental conditions which could affect the capability of the sensor to detect hidden persons and volatile traces from drugs and explosives are also investigated.

Our project studies only living persons and we first identify the protocols used by canine border teams to collect and store odour samples, and the training process followed by the dogs.

The next phase of the project is devoted to the development of independent building blocks for the realization of

the DOGGIES sensors:

- » Miniaturised Mid Infra-Red Photo Acoustic Spectrometer (MIRPAS) module for the detection of the target analytes.

The main objective of this task is to build miniaturised photo-acoustic spectrometer (PAS) modules for the measurement of human scent.

- » Ion mobility spectrometry

Additionally a mobile prototype of a non-radioactive ion mobility spectrometer with gas-chromatographic pre-separation (GC-IMS) for the identification and quantification of gas-phase trace substances relevant for the overall objectives of the project is developed.

- » Data acquisition and fusion

In parallel the appropriate computational methods and techniques are developed in order to acquire the data generated from the measuring units in a reliable way, to process them and to extract the required information using advanced mathematical tools.

The final phase is the operational testing and validation of DOGGIES system.

Expected results

DOGGIES is expected to improve security and safety in Europe and worldwide, and reduce traffics and illegal immigration; taking into account the high financial and psychological costs that result from an act of terrorism, the deployment of DOGGIES would substantially benefit to the entire society.

An expected result of DOGGIES is to produce a final demonstrator efficiently assessed in different relevant operating scenarios.

For the accomplishment of this demonstrator, the following main technical objectives must be achieved:

- » Identify the operational specifications and the end-users requirements
- » Identify the most relevant VOCs related to human, drugs and explosives or their precursors
- » Demonstrate a widely tuneable MIR source, based on quantum cascade lasers arrays multiplexed thanks to silicon-based arrayed waveguide gratings
- » Demonstrate a miniature MIR photo-acoustic spectrometer (MIRPAS) module
- » Demonstrate a portable Gas Chromatography-Ion Mobility Spectrometer (GC-IMS) module using a non-radioactive ionising source
- » Demonstrate selective pre-concentration of the selected relevant VOCs

- » Integrate finally in a single portable instrument MIRPAS, GC-IMS, pre-concentrator and gas sampling with data acquisition and fusion software.

As a conclusion, after 28 months, the main building blocks required for the development of an operational movable stand-alone sensor detecting efficiently hidden persons, drugs & explosives, are nearly in place. It is expected that this instrument will be able to complement, if not replace, the dogs currently used by the canine units of the police force, in operations in urban or remote areas such as border and custom points.

PARTNERS

III V Lab GIE (III-V LAB)
 Center for Security Studies (KEMEA)
 National and Kapodistrian University of Athens (U.o.A.)
 Gasera OY (GASERA)
 Leibniz-Institut für Analytische Wissenschaften – ISAS – e.V. (ISAS)
 G.A.S. Gesellschaft für analytische Sensorsysteme m.b.H. (GAS)
 Consorzio Interuniversitario Nazionale Per La Scienza E Tecnologia Dei Materiali (INSTM)
 Consiglio Nazionale delle Ricerche (CNR-IMM)
 AEA s.r.l. (AEA)
 Institut National De Police Scientifique (INPS)
 Université de Nice – Sophia Antipolis (UNS)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LETI)
 Thales Hellas Anonymi Etaireia Paragogis Emporias kai Ypiresion Ilektronikou Exoplismou (THA)

COUNTRY

France
 Greece
 Greece
 Finland
 Germany
 Germany
 Italy
 Italy
 Italy
 France
 France
 France
 Greece

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

End Date
31/01/2014

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

EFFISEC will provide border officers with up-to-date technologies to

- » allow systematic in-depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles, though the use of automatic gates and portable identity checking and scanning equipment;
- » provide objective criteria for subjecting some travellers/vehicles/luggage to an extensive check in specific lanes.

Description of the work

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 communication.

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

Results

EFFISEC developed, delivered and demonstrated several ways of improving the in-depth controls of travellers in the land and maritime checkpoints in Europe:

- » Integrated approach to border security based on the use of several technological solutions have been proposed: identity checks of travellers, explosives and illicit materials detection, vehicle plate, colour and type recognition, secure communication, hidden objects detection.
- » New and unique biometrics-based portable identity checks technology for travellers staying in their vehicles have been proposed and demonstrated.
- » Automatic border check gate has been proposed for pedestrians. This gate was combined with the development of a unique X-ray based luggage scanning technology.
- » Innovative technologies for very low quantity trace detection of illicit materials have been developed and demonstrated in both land and maritime border conditions.
- » Stolen vehicles plate, colour and type recognition system has been proposed.
- » Innovative X-ray machine for objects hidden in cars has been developed and demonstrated.
- » In depth privacy protection studies in relation to the above mentioned technologies were proposed.
- » The project proposed ideas about future standardisation work in these areas.

**RESEARCH
COMPLETED**

PARTNERS

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

COUNTRY

France
 France
 France
 Italy
 Italy
 Germany
 Spain
 Finland
 Sweden
 United Kingdom
 Romania
 France
 Portugal
 Portugal
 France
 Belgium
 France

FASTPASS / A harmonized, modular reference system for all European automatic border crossing points



© Thinkstock

Information

Grant Agreement N°
312583

Total Cost
€15,485,790.40

EU Contribution
€11,287,715.05

Starting Date
01/01/2013

Duration
48 months

Coordinator

**AIT Austrian Institute of
Technology GmbH – (AIT)**
Safety & Security
Department

Donau-City-Straße 1
1220 Wien - Austria

Contact

Markus Clabian

Tel: +43 50550 4294

Mobile: +43 50550 4294

Fax: +43 50550 4150

E-mail:

markus.clabian@ait.ac.at

www.ait.ac.at

Project objectives

FastPass will establish and demonstrate a harmonised, modular approach for Automated Border Control (ABC) for different border control points (land-, sea- and air-) across Europe. The project specific objectives are:

- › a harmonised ABC solution that is able to integrate an entry/exit system (EES) and a registered traveller programme (RTP),
- › a harmonised ABC usability, based on travellers' feedback, which also helps border guards to focus on potential risks,
- › an ABC solution supporting an innovative border crossing concept with interfaces to existing security and infrastructure processes demonstrated at air-, land- and sea borders,
- › a European solution and a new European ABC suppliers network.

Description of the work

FastPass brings together key players from the entire ABC value chain - system and component producers, research institutions, government authorities and end-users. The development of a harmonized ABC gate will be accomplished with continuous end-user involvement. The entire innovation process, from components development to the final design of the user interface, will be continuously evaluated by the two end user groups, travellers and border guards. Border control is a major challenge for security and mobility within the EU. Travellers request a minimum delay and a speedy border crossing, while border guards must fulfil their obligation to secure the EU's borders against illegal immigration and other threats. Fastpass will serve both demands at the same time: to keep security at the highest level while also increasing the speed and the comfort for all legitimate travellers at all border control points.

The FastPass ABC process will be designed to address both requirements with equal emphasis. One aspect of aiding a speedy border crossing by legitimate travellers is a harmonised user interface. This will allow frequent travellers from Europe and third country states to pass through an ABC with minimum delay, using the full potential of ID documents. Improved traveller identification technologies, such as new biometric modules, will increase the security of the ABC process and minimise spoofing.

A demonstration and evaluation at all types of borders (air, land and sea) will be implemented in at least three different member states. Compliance with European societal values and citizens' rights is central to the acceptance of the developed technologies, and will accompany the development and end-user interaction throughout the project.

Expected results

FastPass will design a modern border control process, taking full account of privacy, social, ethical and legal issues. This will result in smooth and fast border crossing for legitimate travellers, while ensuring a high level of security. The FastPass solution will provide travellers a seamless, fast border transit harmonized for different (land-, sea- and air-) border control points across Europe and will enable border guards to maintain strict and absolute control which is both unobtrusive and convenient to use.

FastPass will be based on innovative modules that can be standardized across Europe using the experiences of several test installations. The technical design and standards will be open for (European) manufacturers to promote an open standard. The FastPass design will provide border control authorities with a standard, proven design with module options to reduce design, specification and procurement time. This will also provide manufacturers and integrators with a standard design which is simpler, faster and cheaper to build – and easier for customers to understand when comparing designs from different suppliers.

PARTNERS

AIT Austrian Institute of Technology GmbH (AIT)
 Teknologian tutkimuskeskus VTT (VTT)
 Bundesministerium für Inneres (BMI)
 Österreichische Staatsdruckerei GmbH (OeSD)
 Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung E.V (FhG)
 Katholieke Universiteit Leuven (KU Leuven)
 Rajavartiolaitos (RAJA)
 secunet Security Networks AG (secunet)
 Mirasys Ltd (Mirasys)
 Regula Baltija SIA (Regula)
 The University of Reading (UREADSSE)
 International Centre for Migration Policy Development (ICMPD)
 Tampereen Yliopisto (UTA)
 Gunnebo Entrance Control Ltd (Gunnebo)
 Giesecke & Devrient GmbH (G&D)
 Modi Modular Digits GmbH (Modi)
 Magnetic Autocontrol GmbH (Magnetic)
 JRC –Joint Research Center – European Commission (JRC)
 ITTI Sp.zo.o.(ITTI)
 Deltabit Oy (deltabit)
 The Chancellor, masters and scholars of the University of Oxford (UOXF)
 Ministerstwo Spraw Wewnętrznych (PBG)
 Finavia Oyj (Finavia)
 Dimotiko Limeniko Tameio Mykonou (PoM)
 Fraport AG Frankfurt Airport Services Worldwide (Fraport)
 Flughafen Wien AG (VIE)
 Intrepid Minds Ltd (IRM)

COUNTRY

Austria
 Finland
 Austria
 Austria
 Germany
 Belgium
 Finland
 Germany
 Finland
 Latvia
 United Kingdom
 Austria
 Finland
 United Kingdom
 Germany
 Germany
 Germany
 Belgium
 Poland
 Finland
 United Kingdom
 Poland
 Finland
 Greece
 Germany
 Austria
 United Kingdom

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



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

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: sebastienbrangoulo@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 require-

ments 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

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

COUNTRY

France
 Norway
 Germany
 France
 Germany
 Germany
 Italy
 France
 Italy
 Italy
 Belgium
 Germany
 Sweden
 Italy
 France
 Estonia
 Sweden
 France

HANDHOLD / HANDHold - HANDHeld OLfactory Detector

© Handhold



Information

Grant Agreement N°
284456

Total Cost
€4,580,959.97

EU Contribution
€3,495,805.59

Starting Date
01/04/2012

Duration
42 Months

Coordinator

THE QUEEN'S UNIVERSITY OF BELFAST (QUB)
Institute of Electronics,
Communications and Information Technology (ECIT)
Queen's Road, Queen's
Island
BT3 9DT, Belfast,
United Kingdom

Contact
DAVID LINTON
Tel: +44 28 9097 1761
Mobile: +44 7837 716 589
Fax: +44 28 9097 1702
E-mail: d.linton@ee.qub.ac.uk
www.handhold.eu

Project objectives

The main objective is to develop a CBRNE modular sensor platform which is reconfigurable and can be deployed for stand-off detection for periods of up to eight hours, operating on battery power alone. This platform will be capable of stand-alone use, mimicking the operational characteristics of sniffer dogs used to detect drugs and explosives. The project will also develop state of the art sensors for:

- » chemical and explosives
- » biohazard detection
- » RN detection.

While the sensor developments are part of HANDHOLD, the project is more than just a sensor development project. The end user interface and networked supervision of multiple units give Handhold a strategic advantage in tackling border security and enhancing public safety.

Description of the work

Conceptually, the architecture of the HANDHOLD system can be broken down into three distinct layers. Aside from complying with scalability requirements, the system can be used for offline data analysis regarding correlations of spatio-temporal data or to support decision makers such as enabling a controller to remotely coordinate field operations directly from the headquarters.

The proposal is to build a three-layer architecture:

- » Sensors Systems Layer – this layer is focused on the requirements specification for mobile sensors. It includes any commercial sensor that might be acquired in addition to the detailed specifications of the three HANDHOLD family devices that will be developed within the scope of the project.

- » Communication Network Layer – this layer will specify all the requirements for the communication server that will operate as a gateway for the data flow between the devices at the Sensors Systems Layer and the HANDHOLD central system installed within the Application Server at the Control Centre system Layer. Field measurements (i.e., sniffed data) are only transmitted to the Application Server if the corresponding sensors are registered within the Communication server. It will support both modes of sensor operation real-time or collect data and send it off-line.

- » Control Centre System Layer – this layer contains the HANDHOLD central system (application server) and manages all Client Dashboards which are directly or remotely connected to the application server.

A HANDHOLD platform can be equipped with a single or multiple sensors and can be re-equipped by unplugging one or more sensors and inserting new sensors in their place. In this way the HANDHOLD platform goes beyond the capability of most sniffer dogs as the latter are normally trained to target just one substance. Moreover, the HANDHOLD platform can embrace new sensor technologies as they become available.

The hardware platform and its embedded software will be developed using the latest results from research in hardware and software design methodologies, and will be independent of the target molecules being detected. Individual sensors inserted into the platform will define the operational detection capability of any particular instance of the HANDHOLD platform.

In this way the HANDHOLD device will be capable of being deployed in a range of operational contexts associated with border security and customs controls. This includes but is not limited to:

- » Postal inspection and sorting offices

- » Maritime container transport
- » Baggage inspection at airports
- » Inspection of vehicles, ships and aircraft

Expected results

To deliver a prototype at month 24 to test the integration of early stage CBRNE sensors and supervisory systems. This prototype will be evaluated in a controlled but realistic environment. By month 42 a prototype will be delivered for field testing by users that incorporates feedback with smaller size, lighter, longer battery life and integrated supervision.

PARTNERS

The Queen's University of Belfast (QUB)
 CapnaDSP LTD (CAPNA)
 The Office of the Revenue Commissioners (ORC)
 Scorpion Networks LTD (SBN)
 Karlsruher Institut fuer Technologie (KIT)
 DEFENDEC OU (DEFD)
 INOV, INESC INOVACAO, INSTITUTO DE NOVAS TECNOLOGIAS (INOV)
 UNIVERSITY COLLEGE CORK, NATIONAL UNIVERSITY OF IRELAND, CORK (Tyndall-UCC)
 NATIONAL UNIVERSITY OF IRELAND, GALWAY (NUIG)

COUNTRY

United Kingdom
 United Kingdom
 Ireland
 Ireland
 Germany
 Estonia
 Portugal
 Ireland
 Ireland

INGRESS / Innovative Technology for Fingerprint Live Scanners



Information

Grant Agreement N°

312792

Total Cost

€4,252,658

EU Contribution

€3,233,782

Starting Date

01/11/2013

Duration

36 Months

Coordinator

MORPHO (MPH)

Direction of Products and
Innovation - DPI

11 boulevard Gallieni

92130 Issy Les Moulineaux
France

Contact
Stéphane Revelin

Tel: +33 (0) 1 58 11 32 15

Mobile: +33 (0) 6 75 89 51 09

Fax: + 33 (0) 1 58 11 87 01

E-mail: [stephane.revelin@](mailto:stephane.revelin@morpho.com)morpho.comWebsite: www.morpho.com

Project objectives

For over ten years, the use of fingerprints has been a key technology to help address both identification and security issues around the world. Unfortunately, the overall success of fingerprints for identification and verification purposes greatly depends on the quality of the fingerprints initially enrolled and acquired.

INGRESS aims to research, develop and validate innovative technologies to take fingerprint images. It will pave the way to the manufacture of novel fingerprint scanners capable of properly sensing fingerprints of intrinsic very-low quality and/or featuring superficial skin disorders.

The project focuses on capturing a sub-surface fingerprint and delivering a high-quality image through medical imaging techniques, such as ultrasound, and Full Field Optical Coherence Tomography. Printed Organic Electronics technologies (such as OLED) will also be studied in order to create a new generation of high resolution and mobile fingerprint sensors.

Therefore, the new scanners will be immune to voluntary or involuntary finger alteration, enabling equal access to the biometric technology for all citizens.

INGRESS will evaluate the currently developed technologies and propose a technology development roadmap for the purpose of using fingerprints from identity documents in border control and law enforcement applications.

Description of the work

INGRESS is developing innovative technologies for fingerprint live scanners that support the examination of additional biometrics associated with the finger in order to address the issue of sub par fingerprint images obtained from fingers with superficial skin disorders.

The OCT and ultrasound technologies will make it possible to take fingerprint information under the skin. The patterns that will be revealed thanks to these new techniques will come from the dermis "matrix". This sub-layer is responsible for the formation of the outer layer. Some biometric elements lying in this deeper layer will then become visible and will enrich traditional fingerprint images, allowing for the creation of a high-quality image. The project also focuses on high definition fingerprint imaging by improving upon some promising new technologies, such as Organic Light Emitting Diodes (OLEDs) and Organic Photo Diodes (OPDs).

Having gathered stakeholders' requirements, the project will develop several mock-ups (OCT, ultrasound and OLED) at different levels of maturity, in a privacy-by-design approach, which will be evaluated through technology readiness levels. A technological roadmap and a cost study allowing for these mock-ups to reach the product stage will also be defined.

The evaluation will be done via different steps: a laboratory test will verify their performance, and cross compatibility with legacy data and traditional sensors, their ergonomics and the feasibility of a large scale test; then a test on the field with a large set of users will be implemented to validate the relevance of such technologies and prove their feasibility in the context of border control and law enforcement.

Expected results

INGRESS' innovative technologies will look and acquire additional biometrics linked to the finger that will complement existing techniques. The solutions proposed in the project offer major improvements to biometrics acquisition. They mainly address the issue of superficial skin disorders by developing hardware and software solutions, while also supporting anti-spoofing detection. The developed technology will greatly enhance image quality and preserve privacy.

The current very low quality fingerprint images of damaged fingers will be overcome by the use of sub-surfacing techniques, which will be the main asset for image quality improvement. This complementarity will deliver high-quality fingerprint images that are still compliant with programs and applications currently using digital fingerprints as a mean of authentication or identification (e.g. EU-Passport, EURODAC, VIS, Entry/Exit, Registered Traveller Program or other European and national applications).

PARTNERS

Morpho (MPH)
 Przedsiębiorstwo Badawczo-Produkcyjne Optel Sp Zoo (OPT)
 Alma Mater Studiorum-Università di Bologna (UBO)
 Centre National de la Recherche Scientifique (CNRS)
 Université de Lausanne (UNIL)
 Hogskolen I Gjøvik (GUC)
 CSEM Centre Suisse d'Electronique et de Microtechnique
 SA - Recherche et développement (CSEM)
 Türkiye Bilimsel Ve Teknolojik Arastirma Kurumu (TUB)
 Rijksuniversiteit Groningen (RUG)
 Ministère de l'Intérieur (ST(SI)²)

COUNTRY

France
 Poland
 Italy
 France
 Switzerland
 Norway

 Switzerland
 Turkey
 The Netherlands
 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

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)
 Association pour la Recherche et le Développement des Méthodes et Processus industriels (ARMINES)
 EADS Deutschland GmbH - Innovation Works (EADS)
 Ecole Polytechnique Fédérale de Lausanne (EPFL)
 Centre for Science, Society and Citizenship (CSSC)
 The University of Padua (UNIPD)
 Chambre de Commerce et d'Industrie de Paris (ESIEE)
 GTP Technology (GTP)
 TraceTech Security (TTS)
 3D General Aviation Applications SA (3DSA)
 Israel National Police (INP)
 ARTTIC Belgium (ART)

COUNTRY

France
 United Kingdom
 France
 France
 Germany
 Switzerland
 Italy
 Italy
 France
 France
 Israel
 Greece
 Israel
 France

SNIFFLES / Artificial sniffer using ion trap technology



© WAGTAIL

Information

Grant Agreement N°
285045

Total Cost
€5,226,007.41

EU Contribution
€3,493,625

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.

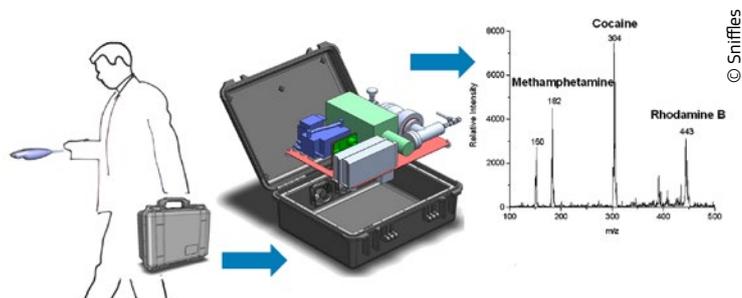
The end stage of phase 2 is the system integration to ensure that each sub system is working in synchronicity with its partners;

» 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.



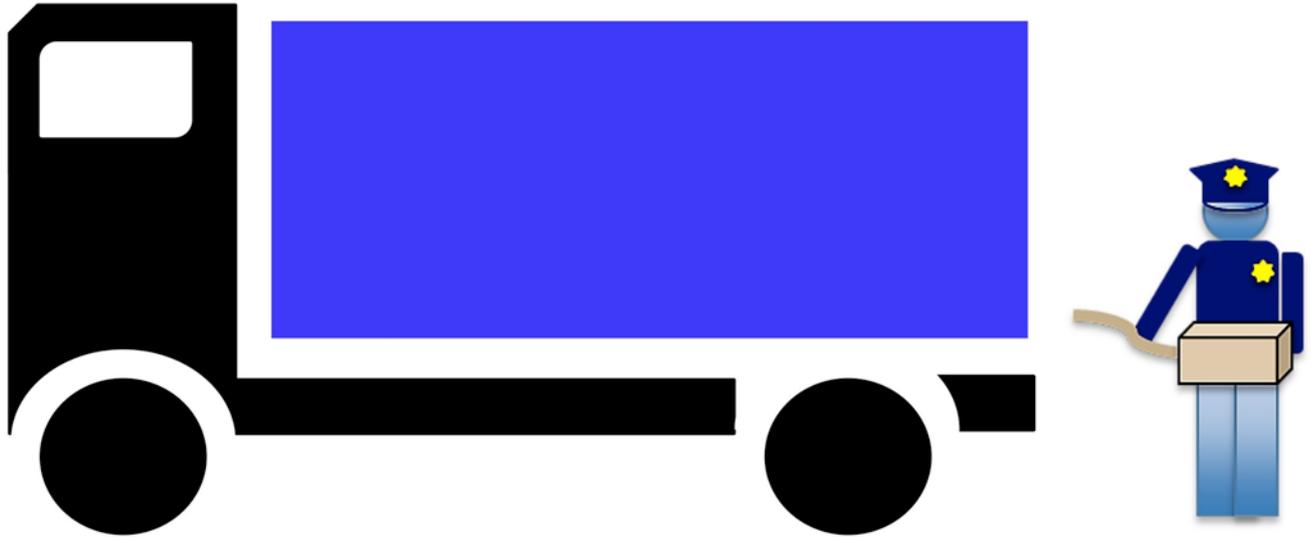
PARTNERS

- TWI Ltd (TWI)
- The University of Liverpool (UOL)
- Université Aix-Marseille 1 Provence (UdP)
- DSM R&D Solutions BV (DSM)
- Q Technologies Ltd (Qttec)
- 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

SNOOPY / Sniffer for concealed people discovery



Information

Grant Agreement N°
313110

Total Cost
€2,605,284.96

EU Contribution
€1,835,891.00

Starting Date
01/01/2014

Duration
36 months

Coordinator

UNIVERSITÀ DEGLI STUDI DI BRESCIA (UNIBS)

Dipartimento Ingegneria dell'Informazione
Via Branze, 38
25133 - Brescia - Italy

Contact
Giorgio Sberveglieri
Tel: +390303715771
Fax: +390302091271
E-mail:
giorgio.sberveglieri@unibs.it
Website: www.unibs.it

Project objectives

The SNOOPY project aims to:

- » develop an artificial instrument (the SNOOPY sniffer) that identifies the presence of hidden people through the identification of gaseous compounds peculiar of the presence of human beings, arising from, for example, sweat odour;
- » defining a metric to calibrate and assess the SNOOPY sniffer performances;
- » develop a protocol to integrate the use of already used tools, such as trained dogs and/or ion mobility spectrometry (IMS).

In this regard the SNOOPY sniffer will improve the capability of border authorities with respect to illicit traffic of people.

Description of the work

The SNOOPY consortium will address the project objectives through:

- » Development of a pre-concentration unit;
- » Development of gas sensors based on different sensing and transduction mechanisms;
- » development of a pattern recognition software aimed to identify the presence of hidden people in containers based on the sensor array response;
- » Creation of a compact prototype based on above technologies;
- » Benchmarking of the SNOOPY sniffer with already adopted approaches, namely IMS and trained dogs.

Expected results

The main expected result from the SNOOPY project is a sniffer prototype with the following features:

- » portable, thanks to the use of low-weight, small size and low-power consumption technologies;
- » suited to work in a 24/7 way;
- » able to recognize – once trained and calibrated – the sniffed atmospheres on its own, providing the information directly to the user through a display or a set of LEDs, without the need of data transmission and elaboration to remote stations;
- » Equipped with a small pipe to collect odours in proximity of small apertures, which are present, for example, at lorry/container doors, even if locked, and from which inner odours can be smelled;
- » User-friendly: the SNOOPY sniffer will provide a three-fold output: hidden person present - no hidden person – doubt (in case of doubt the vehicle/cargo will be subject to a more accurate analysis)

PARTNERS

Università degli Studi di Brescia (UNIBS)
 Consiglio Nazionale delle Ricerche (CNR)
 Università degli Studi di Roma Tor Vergata (UTOV)
 EADS Deutschland GMBH (EADS)
 C-TECH Innovation Limited (CTECH)
 Center for Security Studies (KEMEA)

COUNTRY

Italy
 Italy
 Italy
 Germany
 United Kingdom
 Greece

TERASCREEN / Multi-frequency multi-mode Terahertz screening for border checks



© Aleksei Potov's

Information

Grant Agreement N°
312496

Total Cost
€4,782,686.32

EU Contribution
€3,489,932

Starting Date
01/05/2013

Duration
42 Months

Coordinator

ALFA IMAGING S.A.
(ALFA IMAGING)
C/Rumania 8 Nave 24
28802 – Alcalá de Henares
Spain

Contact
Naomi Alexander
Tel: +34 91 515 94 16
Mobile: +34 691 221799
Fax: +34 918 827892
E-mail: nalexander@
alfaimaging.com
Website:
www.fp7-terascreen.eu

Project objectives

The overall objective of the project is to develop and demonstrate in a live border control environment a safe, privacy respecting, high throughput security screening system which automatically detects and classifies potential threat objects concealed on a person.

This will advance state of the art, providing an innovative security screening solution for border and security checks that is effective in terms of both security and operation.

The TeraSCREEN Prototype System will integrate a passive and active subsystem, including the sensor data fusion, image processing and the Automatic Object Detection and Classification, and the Privacy Enhancing algorithms complying with EC Regulation No 1147/2011, respecting fundamental rights and observing the principles recognised by the Charter of Fundamental Rights of the European Union;

Description of the work

Two real-time stand-off imaging subsystems will be developed: a multi-frequency (360GHz, 220GHz and 94GH) Passive subsystem and a 360GHz Active subsystem

Innovative (advancing state of the art) components necessary for the subsystems will be developed, although using commercial-off-the-shelf (COTS) components when available and sharing the components that are common to both subsystems.

Some of these components developed in TeraSCREEN can be exploited in other systems. The performance of the developed components will be summarised after testing in a datasheet-like summary, which will enable exploitation and dissemination of the results. Component packaging, interconnection and transitions will be investigated as part of the component development.

The resulting passive and active subsystems will be integrated. The sensor data fusion and image processing will be developed, along with the user interface. This software will be incorporated into the TeraSCREEN Prototype System, which will then be tested and characterised.

The tests of the integrated system will be carried out at ICTS's VeriSys test facilities where explosive materials can be made available and ICTS's operational knowledge will be used to input into staff training procedures for the Pilot Test. The System will be demonstrated in a Pilot Test at a live control point and passengers will be screened on an opt-in basis.

The ethical requirements and implications for the operation of the TeraSCREEN Prototype System at border checkpoints will be managed throughout the project. The (possibly negative) ethical impact will be compared to the perceived and real benefit created by the TeraSCREEN System.

Expected results

The main project result will be an innovative prototype security screening system. This system will operate at multiple mm-wave and THz frequencies and in both passive and active mode in order to automatically detect and classify objects concealed under clothing. It will screen subjects non-intrusively and in real-time. The concealed object detection and classification will be presented automatically to the operator on a generic computerised silhouette.

The innovative prototype security screening system developed will therefore provide a safe, non-intrusive, privacy respecting, high throughput and high security level solution. The automatic threat detection feature also reduces the level of attention required from the

operator, which implies a reduction in the personnel necessary for continuous operation.

This Prototype System will be demonstrated at a live operational control point and its performance there will be evaluated. The results of this evaluation will be another very important project result, proving that this solution can produce consistent and secure results in operational settings, in addition to increasing throughput and respecting privacy.

The components that will be developed to achieve this main project result are also worth including as project results in their own right. Several components will be developed in this project beyond current state of the art.

PARTNERS

Alfa Imaging S.A. (Alfa Imaging)
 Universidad Pública de Navarra (UPNA)
 Anteral S.L. (Anteral)
 Science and Technology Facilities Council (STFC-RAL)
 Teratech Components Ltd. (Teratech)
 Acreo Swedish ICT AB (Acreo)
 OMMIC SAS (Ommic)
 Università degli Studi di Roma "Tor Vergata"
 Goethe-Universität Frankfurt am Main
 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (FHR, FKIE)
 ICTS UK Ltd (ICTS UK)
 Albert-Ludwigs-Universität Freiburg (Uni Freiburg)

COUNTRY

Spain
 Spain
 Spain
 United Kingdom
 United Kingdom
 Sweden
 France
 Italy
 Germany
 Germany
 United Kingdom
 Germany

OPARUS / Open Architecture for UAV-based Surveillance System



© Netfalls - Fotolia.com

**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

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

COUNTRY

France
 Poland
 United Kingdom
 France
 Germany
 Spain
 Israel
 Spain
 Spain
 France
 Italy
 France
 France
 United Kingdom

SUNNY / Smart UNattended airborne sensor Network for detection of vessels used for cross border crime and irregular entry



Information

Grant Agreement N°
313243

Total Cost
€14,439,544.88

EU Contribution
€9,569,977.68

Starting Date
01/01/2014

Duration
42 months

Coordinator

BMT GROUP LIMITED
Research
Waldegrave road 1
Teddington TW11 8LZ –
United Kingdom

Contact
Mary Vayou
Phone:
+44 (0)20 8943 5544
Fax: +44 (0)20 8943 5347
E-mail:
m.vayou@bmtmail.com
Website: www.bmt.org

Project objectives

The SUNNY project aims to develop system solutions to improve the effectiveness of EU border monitoring compared to legacy systems whilst keeping the affordability and interoperability as key enabling factors.

Description of the work

SUNNY's objectives are the following:

- » Novel sensors and on-board processing generation. The focus will be on developing and integrating sensors of low weight, low cost and high resolution, which can operate under variable conditions such as darkness, snow, and rain. In particular, SUNNY will develop sensors that can generate both Visible, Near Infrared (NIR-SWIR) and LWIR images and hyper-spectral data. It also aims to couple sensor processing and preliminary detection results (on-board) with local aerial platform control, leading to innovative active sensing techniques, replacing low level sensor data communication by a higher abstraction level of information communication.
- » The exploitation and adaptation of emerging standard wireless technologies and architectures to the SUNNY scenarios towards the EUROSUR's goal of defining European-wide standards. Existing wireless standard technologies, such as IEEE 802.11a/g/n, IEEE 802.11p, DVB-T2, Mobile WiMAX, LTE, and Wi-Fi@700MHz will be considered due to their low cost and features such as radio resource management, provisioning of high bitrates, and mobility management.
- » A two-tier intelligent heterogeneous airborne sensor network will be integrated in order to provide both large field and focused surveillance capabilities. In this

network, the first-tier sensors, carried by medium altitude, long-endurance aerial platforms are used to patrol large border areas to detect suspicious targets and provide global situation awareness. Fed with the information collected by the first-tier sensors, the second-tier sensors will be deployed to provide more focused surveillance capability by tracking the targets and collecting further evidence for more accurate target recognition and threat evaluation. Novel algorithms will be developed to analyse the data collected by the sensors for robust and accurate target identification and event detection.

Expected Results

It is recognised that the legacy sensors and communications system developed for military applications are not optimised for border monitoring and their interoperability with civil standards is limited. Moreover, it is acknowledged that the diffusion of the information is tailored in service systems to highly skilled personnel and the number of operators to conduct the activity is high. Via the integration of technologies developed across different initiatives, the SUNNY approach will deliver pre-processed information with meaningful decision support tools enabling the reduction of number and required

level of expertise of border surveillance personnel. The SUNNY project aims to contribute to the objectives of EUROSUR by improving sensor and data transmission capacities and real time data processing capabilities.

PARTNERS

BMT Group Ltd
 Metasensing B.V.
 Xenics
 Queen Mary and Westfield College, University of London
 Tecnia
 INESC PORTO
 Technical University of Crete
 Ministério da Defesa Nacional (CINAV)
 SPECIM, Spectral Imaging Ltd
 ALENIA AERMACCHI SPA
 TTI NORTE, S.L.
 CENTER FOR SECURITY STUDIES (KEMEA)
 MARLO a.s.
 Vitrociset S.p.A.
 NCSR 'Demokritos'
 CNIT RASS
 SAAB AKTIEBOLAG
 ALTUS LSA COMMERCIAL AND MANUFACTURING SA

COUNTRY

United Kingdom
 The Netherlands
 Belgium
 United Kingdom
 Spain
 Portugal
 Greece
 Portugal
 Finland
 Italy
 Spain
 Greece
 Norway
 Italy
 Greece
 Italy
 Sweden
 Greece

CONTAIN / CONTAINER securiTY Advanced Information Networking



Information

Grant Agreement N°

261679

Total Cost

€15,525,218.11

EU Contribution

€10,044,904.00

Starting Date

01/10/2011

Duration

42 months

Coordinator

TOTALFÖRSVARETS FORSKNINGSINSTITUT (FOI)

Division of Information and
Aeronautical Systems
Gullfossvägen 6, Stockholm
164 90 Sweden

Contact

Pontus Svenson

Tel: +46 8 5550 3732

Mobile: +46 734 44 77 32

Fax: +46 8 5550 3700

E-mail: ponsve@foi.se

Website: www.foi.se

Project objectives

CONTAIN is aimed at specifying and demonstrating a European Shipping Containers Surveillance system which will encompass regulatory, policy and standardisation recommendations, new business models and advanced container security management capabilities. The CONTAIN system will:

1. Support transport security stakeholders in managing container security threats within logistic chains as part of an integrated approach to the efficient management of Door to Door (D2D) transportation networks;
2. Provide a coherent set of cost effective and efficient technology options for container-integrated sensor, communication and security hardware and software technologies to monitor container movements and security and business related parameters in real time, whilst addressing the technology, implication of and links to screening and detection technologies;
3. Enable ports and transport networks to establish cost effective container security processes and to optimise operational processes, both in terms of security performance and efficiency and quality of container transport services;
4. Provide added value to key investments made by EU customs organisations to achieve higher levels of protection of markets and society and to offer favorable conditions for business development focusing on improved real time risk evaluation and control;
5. Provide appropriate information gathering, validation, fusion and situational awareness services to establish dependable near real time 'corridor container traffic maps' and their integration into a EU Container Traffic

Map for use by organisations and systems established to promote and implement an integrated EU surveillance policy;

6. Enable the establishment of secure trade lanes between the EU and selected trading partners;
7. Assist policy makers at national and EU level to promote container security based on sound economic and technological evidence and to benchmark container security performance in order to formulate improvement policies;
8. Facilitate the further development of European standards to address and improve container and supply chain security and progress towards a single international shipping containers security standard.

Description of the work

CONTAIN has produced innovative solutions for the risk-based approach to container targeting and scanning, optimization of container transport, and information interoperability and exchange, including information security aspects. A CONTAIN platform has been established that is used to connect information sources and users. Improved positioning, e-seal and container security device equipment has been developed, as well as procedures and technology solutions for finding containers mis-declared as empty. The results of CONTAIN are demonstrated in two small-scale and one large scale demonstration: Genoa in December 2014, Valenia in January 2015, and Bologna in February 2015. The results of CONTAIN will be recorded in the European Container Surveillance Framework (ECSF) and in the Contin Manual, which will contain a guide for how to implement the results of the project.

Expected results

CONTAIN is expected to lead to increased visibility of the supply chain using new and improved sensory and positioning devices and increased situational awareness of logistics operators as well as authorities (including customs) by using new information sharing and decision support systems.

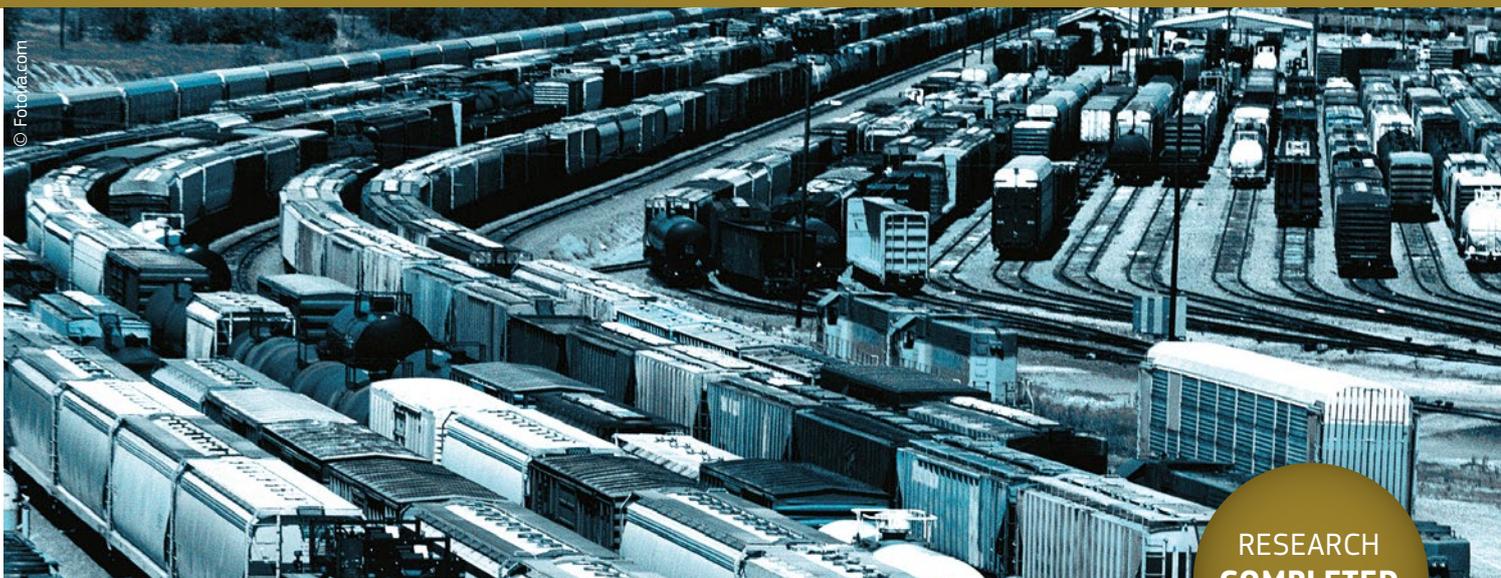
PARTNERS

BMT Group Limited (BMT)
 Conceptivity Sarl (CTY)
 Inlecom Systems Ltd (ILS)
 Consorzio IB Innovation (IBI)
 JRC – Joint Research Centre – European Commission
 Selex ES SPA (SE)
 Thales Research & Technology (UK) Limited (TLUK)
 Telespazio Spa (TPZ)
 Marlo AS(Marlo)
 Novacom Services SA (Novacom)
 Teknologian Tutkimuskeskus VTT (VTT)
 MJC2 Limited (MJC2)
 eBOS Technologies Ltd (eBOS)
 European Organization for Security SCRL (EOS)
 Fundacion de la Comunidad Valenciana Para La Investigacion, Promocion Y Estudios Comerciales de Valenciaport (VAL)
 Agenzia Delle Dogane (AD)
 Thales Italia Spa (TLIT)
 SO.GE.MAR. Societa Generale Magazzine Raccordati Interporto SPA (SOG)

COUNTRY

United Kingdom
 Switzerland
 United Kingdom
 Italy
 Belgium
 Italy
 United Kingdom
 Italy
 Norway
 France
 Finland
 United Kingdom
 Cyprus
 Belgium
 Spain

 Italy
 Italy
 Italy

GLOBE / Global Border Environment

© Fotovra.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

Telvent Interactiva S.A.
 Amper Sistemas S.A.
 GMV Aerospace and Defence, S.A
 Instituto Nacional de Técnica Aeroespacial
 Altran Technologies
 SETTCE
 Econet Polska sp. z.o.o.
 Eurosense Belfotop N.V.
 Skysoft Portugal, Software e Tecnologias de Informação, S.A.
 CES vision Ltd.
 PRIO
 Empresa de Serviços e Desenvolvimento de Software, S.A.
 Cogent Systems GMBH
 CIAOTECH Srl (CIAOTECH)
 Fundación Tecnalía Research & Innovation (TECNALIA)

COUNTRY

Spain
 Spain
 Spain
 Spain
 France
 Slovenia
 Poland
 Belgium
 Portugal
 Hungary
 Norway
 Portugal
 Austria
 Italy
 Spain

TALOS /

Transportable autonomous patrol for land border surveillance system



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 in-

terrogated 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

Przemysłowy Instytut Automatyki i Pomiarów
 ASELSAN Elektronik Sanayi ve Ticaret A.Ş.
 European Business Innovation & Research Center S.A.
 Hellenic Aerospace Industry S.A.
 Israeli Aerospace Industries
 ITTI Sp. z o.o.
 Office National d'Etudes et de Recherches Aéropatiales
 Smartdust Solutions Ltd.
 Société Nationale de Construction Aéropatiale
 STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.
 Telekomunikacja Polska SA
 TTI Norte S.L.
 Technical Research Center of Finland
 Politechnika Warszawska

COUNTRY

Poland
 Turkey
 Romania
 Greece
 Israel
 Poland
 France
 Estonia
 Belgium
 Turkey
 Poland
 Spain
 Finland
 Poland

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

Carl Zeiss Optronics GmbH
 Crabbe Consulting Ltd
 Armed Forces Malta
 Instituto Canario de Ciencias Marinas
 Fugro Oceanor
 OBR Centrum Techniki Morskiej
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)
 IQ-Wireless
 HSF
 University of Las Palmas de Gran Canaria

COUNTRY

Germany
 United Kingdom
 Malta
 Spain
 Norway
 Poland
 Germany
 Germany
 Czech Republic
 Spain

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



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- NATUURWE- TENSCHAPPELIJK ONDERZOEK

Mobiliteit & Logistiek

Van Mourik Broekmanweg 6

PO Box 49

2600 AA Delft

The Netherlands

Contact

Heather Griffioen-Young

Tel: +31 888 665 931

Mobile: +31 622 461 065

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

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

COUNTRY

The Netherlands
 The Netherlands
 The Netherlands
 Germany
 Spain
 Switzerland
 Belgium
 The Netherlands
 Portugal
 Luxembourg
 Spain
 Belgium
 Germany
 The Netherlands
 United Kingdom
 The Netherlands
 Spain
 The Netherlands
 Germany
 The Netherlands
 United Kingdom
 Austria
 Switzerland
 Egypt
 Portugal
 The Netherlands
 Egypt

CLOSEYE / Collaborative evaluation Of border Surveillance technologies in maritime Environment bY pre-operational validation of innovativE solutions

© Thinkstock



Information

Grant Agreement N°
313184

Total Cost
€12,230,221.51

EU Contribution
€9,218,256.37

Starting Date
27/03/2013

Duration
38 months

Coordinator

Guardia Civil (GUCI)
Mr. JOSÉ MANUEL
SANTIAGO MARÍN
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
C/ Guzmán el Bueno 110
28003 - Madrid
Spain

Contact
José Manuel Santiago Marín
Tel: +34 915146775
Mobile: +34 915146254
Fax: +34 915146264
E-mail: jmsantiago@guardiacivil.es
Website: www.closeye.eu

Project objectives

The main objectives of the CLOSEYE project are the following:

- » To provide the EU with an operational and technical framework that would increase situational awareness and improve the reaction capability of authorities surveying the external borders of the EU by following a decentralized approach;
- » To validate new security solutions taking into account any aspect of border security that could threaten human rights or break international law;
- » To enable public authorities in charge of border surveillance to innovate faster in the provision of their institutional services, making them more efficient and effective;
- » To increase the research capacity and innovation performance of European companies and research institutions, creating new opportunities to take international leadership in new markets;
- » To conduct pre-operational validation of common application of surveillance tools at EU level via the competitive testing and assessment of several potential solutions;
- » To achieve a competitive testing framework

Description of the work

The proposed implementation roadmap for CLOSEYE consists on the implementation of three consecutive phases which include the set of activities necessary to achieve the goals of the Project:

Phase 1: Definition

The definition phase should be based on the latest relevant requirements for European Border Surveillance. CLOSEYE:

- » Identification of the needs and the available solutions that could be tested and validated in cooperation.
- » Definition of a validation strategy (including a practical exercise plan), setting scenarios and issues for concrete implementation of activities.
- » Establishment of good practice procedures and criteria for evaluation and monitoring (common evaluation criteria and implementation methods).

Phase 2: Execution

This phase will implement the validation strategy as prescribed by the CLOSEYE Consortium in Phase 1 (in particular the Call for Tenders for the implementation of testing). During this phase, the providers of solutions to be tested, are to be selected via the competitive call as defined in Phase 1. These providers will execute the testing in real operational scenarios, with their solutions integrated with other existing systems, and working under the supervision of the CLOSEYE Consortium.

Phase 3: Evaluation

In this phase, which will conclude the overall validation, CLOSEYE Consortium will conduct a thorough assessment of the solution performances and cost-benefit ratio of the alternatives tested in Phase 2, against the set of jointly defined performance criteria. This phase includes a set of recommendations that could be extended to other relevant EU organizations.

Expected results

Pre-operational validation guided by end-users, will allow a tangible assessment of the performance levels offered by innovative technologies in a realistic user-defined operational scenario, where a trade off between efficiency, effectiveness and cost can be aligned with actual needs. Moreover, pre-operational validation will allow, not only the assessment of a stand-alone technology, but also the assessment of the integration of the new capabilities provided into current surveillance infrastructure at all levels in the systems' lifecycle (from technical to logistics, training, maintenance, operation and disengagement).

The close link between end-users and industry, especially in those cases where there is a fuzzy perception of the

real needs of the user in daily practice for a particular technology, will extend the benefits of pre-operational validation beyond technical development. The identification of innovative applications, business models and procurement strategies will reverberate in the integration of innovative solutions as fully operational tool. By acting as technologically knowledgeable validator of new R&D, the public demand side can drive innovation.

PARTNERS

Guardia Civil (GUCI)
 Guardia Nacional Republicana, (GNR)
 Ingeniería de Sistemas para la Defensa de España (ISDEFE)
 Agenzia Spaziale Italiana (ASI)
 European Union Satellite Center (EUSC)
 Marina Militare Italiana (MARINA)

COUNTRY

Spain
 Portugal
 Spain
 Italy
 EU
 Italy

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

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 images) 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

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

COUNTRY

France
 France
 Finland
 Luxembourg
 Norway
 Norway
 Belgium
 Germany
 Spain
 Finland
 France
 France
 France
 France
 Belgium
 France
 France
 France
 Belgium
 Germany

OPERAMAR /

An interoperable approach to European Union maritime security management

© Bruno Delacotte - Fotolia.com

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 road-map 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

Thales Underwater Systems SAS (THALES)
 SELEX Sistemi Integrati S.p.A. (SELEX)
 Indra Sistemas S.A. (INDRA)
 Quintec Associates Ltd. (QUINTEC)
 The Alliance of Maritime Regional Interests in Europe (AMRIE)
 European Commission - Joint Research Centre (JRC)
 Istituto Affari Internazionali (IAI)
 Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)
 STM Savunma Teknolojileri Muhendislik ve Ticaret A.S. (STM)
 Thales Systemes Aeroportes S.A. (TAS)

COUNTRY

France
 Italy
 Spain
 United Kingdom
 Belgium
 Belgium
 Italy
 Portugal
 Turkey
 France

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



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

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

COUNTRY

Spain
 France
 France
 Italy
 Spain
 Spain
 Greece
 Spain
 Norway
 Sweden
 Luxembourg
 Finland
 France
 Spain
 Luxembourg
 France
 Portugal
 Ireland
 Finland
 Switzerland
 Spain
 Netherlands
 Ireland
 France
 Portugal
 Greece
 Greece
 Italy
 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

End Date
28/02/2014

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

SeaBILLA aims to develop sea border surveillance capabilities to address a number of perceived surveillance challenges in current critical EU regional theatres. The project seeks to:

- » reduce the number of illegal immigrants attempting to enter the EU undetected;
- » increase internal security by contributing to the prevention of cross-border crime;
- » enhance search and rescue capabilities, especially to save more lives of migrants who attempt risky ways to cross the border.

SeaBILLA contributed to these objectives by studying, developing and demonstrating cost-effective solutions for extending, in general, the areas covered by surveillance, with special emphasis on:

- » open sea, where surveillance is currently limited to areas with ongoing operations;
- » improving the capability to detect small and/or non-reporting vessels typically used by immigrants and illegal traffickers;
- » improving the capability to track, classify and identify non-reporting vessels.

Description of the work

SeaBILLA is a user-driven project and the user defined scenarios dictated the project work-plan in four project areas:

Project Area 1 (SP1) - Capabilities Roadmap: for each of the above mentioned scenarios, very realistic "vignettes" describing illegal actions have been outlined with the authorities in charge; this baseline of operational requirement has been used to identify the required operational surveillance capabilities, surveillance systems solution, for each scenario, and fill the gaps in legacy systems.

Project Area 2 (SP2) - Surveillance segments improvements: to increase the detection and tracking of small and non-reporting boats focusing airborne, space borne, land and sea based surveillance means available in the near term or new application of existing solutions.

Project area 3 (SP3) - Sensors networking and information fusion: it addresses sensors networking, data fusion and high level processing techniques and solutions which boost the operational capabilities through more effective exchanges of information, correlation tools, data mining engines, abnormal behavior detection etc. from both currently available but not fully exploited information, and from the improved sensor chains.

Project Area 4 (SP4) - Trials, demonstrations and validation. SeaBILLA partners, and in particular the associated end-users, will evaluate the effectiveness of the SeaBILLA results of Project Area 2 and 3, through their integration and extensive simulation in laboratories to compare the achieved capabilities in the context of the various operational "vignettes" to measure the improvements respect to the current situation and selected demos on sites for single surveillance sensor or for a sub-set integrated solution.

**RESEARCH
COMPLETED**

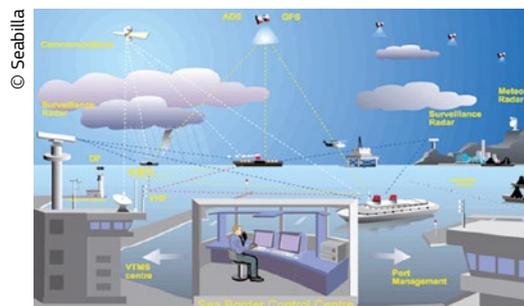
Results

In agreement with the end user community, Seabilla has focused three main European sea areas (Atlantic, English Channel, Med) where to develop solution to counter specific threats.

The following seven scenarios have been detailed:

1. Atlantic Drug Trafficking
2. Atlantic Illegal Immigration
3. Mediterranean Drug Trafficking

4. Mediterranean Illegal Immigration
5. English Channel Anti-terrorism
6. English Channel Illegal immigration
7. English Channel Drug trafficking



PARTNERS

SELEX Sistemi Integrati SPA (SSI)
 Alenia Aeronautica
 Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)
 BAE Systems (Operations) Ltd (BAES)
 Correlation Systems (CorrSys)
 Cassidian S.A.S. (EADS DS)
 Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)
 Eurocopter España (ECE) (ECE)
 Totalförsvarets Forskningsinstitut (FOI)
 Holland Institute of Traffic Technology BV (HITT Traffic)
 Indra Espacio S.A. (IE)
 Indra Sistemas S.A. (INDRA)
 European Commission - Joint Research Centre (JRC)
 Mondeca S.A. (Mondeca)
 Sagem Défense Sécurité (SAGEM)
 Space Applications Services N.V./S.A (SpaceApps)
 Thales Alenia Space Italia S.p.A. (TASI)
 Thales Defence Deutschland GmbH (TMSS)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Telespazio S.p.A. (TPZ)
 Thales Systèmes Aéroportés S.A. (TSA)
 TTI Norte (TTI)
 University College London (UCL)
 Universidad de Murcia (UMU)
 University of Portsmouth Higher Education Corporation (UoP)
 Thales Alénia Space France (TASF)
 Thales Communications & Security S.A. (TCF)

COUNTRY

Italy
 Italy
 Italy
 United Kingdom
 Israel
 France
 Portugal
 Spain
 Sweden
 The Netherlands
 Spain
 Spain
 Belgium
 France
 France
 Belgium
 Italy
 Germany
 The Netherlands
 Italy
 France
 Spain
 United Kingdom
 Spain
 United Kingdom
 France
 France

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.

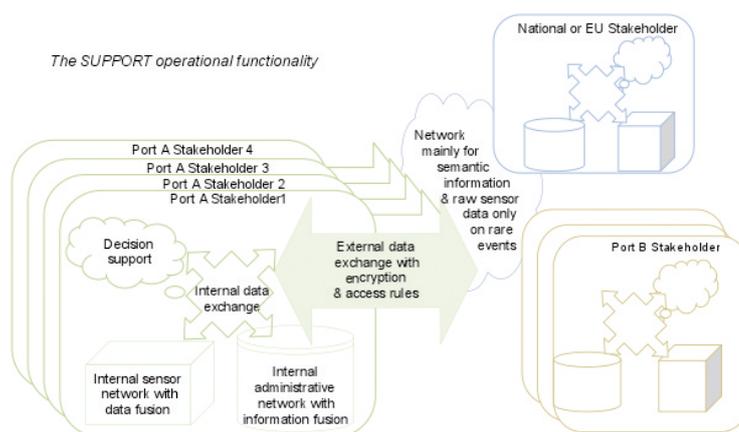
These demonstrators will simulate a full scale installation of the SUPORT Platform with integration with existing systems facilitating measurements of the impact on both the security and efficient operation of the port.

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.



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

TRITON / Trusted Vessel Information from Trusted On-board Instrumentation



© Triton_ISMB_A

Information

Grant Agreement N°
312687

Total Cost
€2,151,993.60

EU Contribution
€1,533,099.00

Starting Date
01/12/2013

Duration
24 months

Coordinator

**ISTITUTO SUPERIORE
MARIO BOELLA (ISMB)**

Navigation Technologies
Research Area
Via P.C. Boggio 61
10138 – Torino – Italy

Contact

Marco PINI

Tel: +39 011 2276436

Mobile: +39 335 6443351

Fax: +39 011 2276299

E-mail: pini@ismb.it

Website:

www.tritonproject.eu

Project objectives

The TRITON project mainly focuses on two objectives. The first is to develop a GPS/Galileo receiver impervious to intentional jamming and spoofing attacks; and the second is to enhance the robustness of the vessel-to-vessel and vessel-to-shore base station communication links. More specifically, the project aims at:

1. Hardening on-board GNSS receivers against spoofing and jamming. Acknowledging the primary role of Global Navigation Satellite System (GNSS) to support ship reporting systems, the project will focus on the GNSS-based positioning system which interfaces with the on-board unit. The goal is to provide a "trusted" GNSS-based source of positioning and timing information, robust against intentional jamming and spoofing attacks, while strengthening a vessel's ship reporting system.
2. Enhancing ship-to-ship and ship-to-shore communications. TRITON proposes to enforce AIS (automatic identification system) reliability and safety, by adding a new communication channel in the ultra high frequency band. This will be based on layering a secure communication module on top of the standard AIS transceiver. This module will exploit the "white spaces" freed by analog TV, offering a broadband channel that allows several services and enhancements to the current system.

Description of the work

A new awareness has grown across civilian and commercial maritime control stakeholders: that surveillance and safety systems may be under the attack of unintentional or malevolent players, whose aim is to bypass or manipulate control systems to obtain economic gain. The advances of mass-priced technology easily sold over the Internet make this a serious threat that maritime authorities must have cope with.

The TRITON project will research possible solutions to such threats by focusing on enhanced trustworthiness of on-board instrumentation used to report vessel information to the control organisms.

The project starts with the analysis of the state of the art of ship reporting systems, identifying current risks of intentional interference. Such an analysis includes the definition of user requirements based on interviews of stakeholders, end users and experts in the maritime domain. The user requirements and the identified set of risks will be critically analyzed to derive a set of specifications which, in turn, will guide the design and development of the GNSS and communication modules.

The GNSS module will be built on top of a software receiver, able to detect jamming signals and mitigate GNSS spoofing attacks. The countermeasures implemented in the GNSS module are complementary to those provided by GNSS Signal In Space (SIS) authentication. The GNSS module is connected to the robust communication module, which includes a commercial AIS. The frequency diversity provided by the use of white spaces allows for secure mechanisms and a more robust communication in the very high frequency (VHF) segment. The analysis and design of the communication module takes into account the VHF Data Exchange System (VDES) introduced within the e-maritime framework.

In the last phase of the project, the team will have the chance to test and demonstrate the developed technical solutions at the European Commission's Joint Research Centre (JRC).

In addition to its technical work packages, the project foresees a deep analysis from a policy and regulation perspective. This will provide guidelines to future maritime applications as based on the benefits created by TRITON's technologies and methods. TRITON also dedicates a specific task to define a detailed action plan for commercialisation of its research results.

Expected results

At the end of the project, a proof of concept of its proposed technological solutions will be folded into a prototype and appropriate test suites. These will encompass both the robust GNSS receiver and the enhanced communications transceiver. The prototype will be tested at JRC.

Ultimately, the project will boost the understanding of current threats in maritime navigation via its comprehensive analysis of the sector's technological, market-based (cost-benefit) and regulatory aspects.

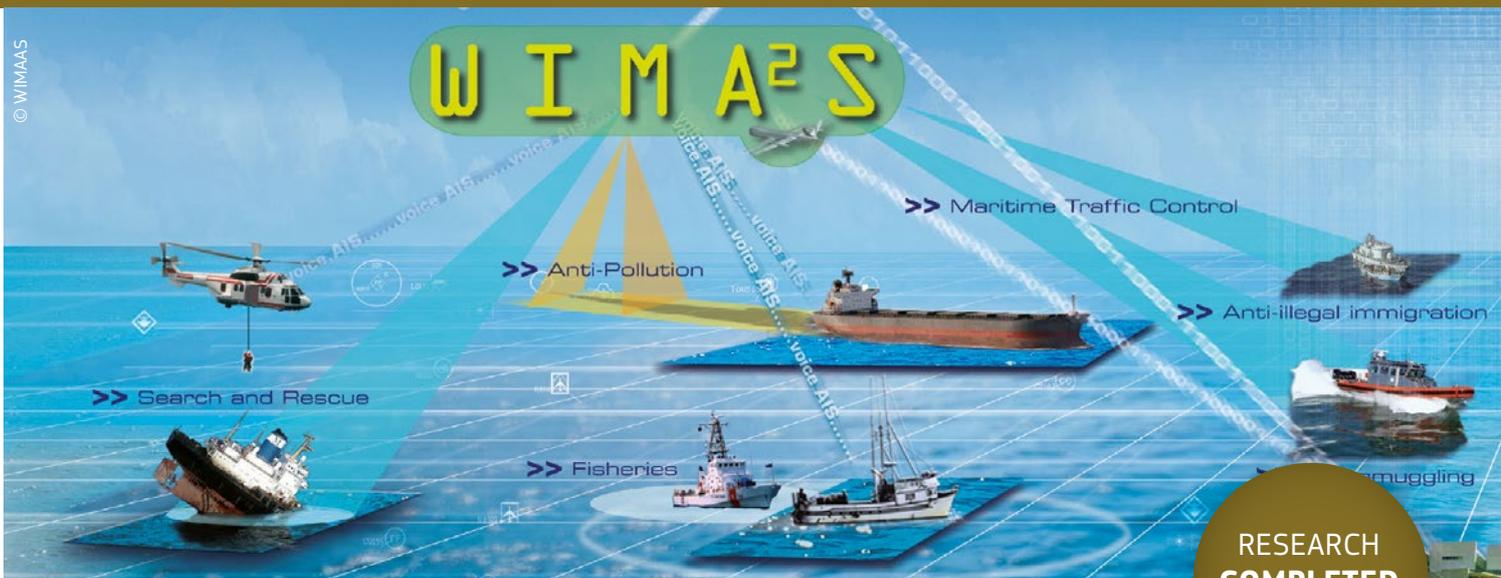
PARTNERS

Istituto Superiore Mario Boella (ISMB)
Kongsberg Norcontrol IT (KNC)
Acorde Technologies (ACORDE)
7i Group (7iG)
Alpha Consult (ALPHA)
Granturco and Partners (G&P)

COUNTRY

Italy
Norway
Spain
Sweden
Italy
Belgium

WIMAAS / Wide maritime area airborne surveillance



**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

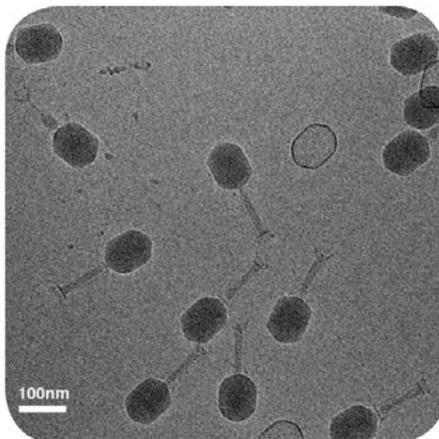
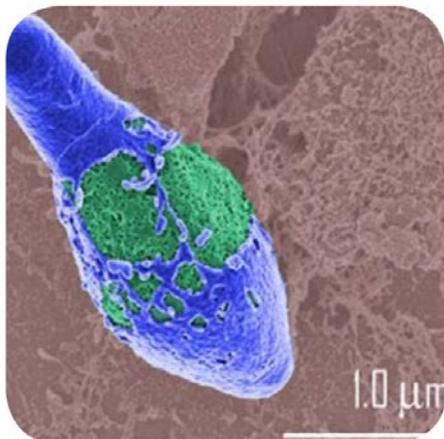
Thales Systemes Aeroportes S.A
 SELEX GALILEO
 Dassault Aviation
 SENER Ingenieria y Sistemas
 Totalförsvarets Forskningsinstitut (FOI)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)
 European Commission - Joint Research Centre (JRC)
 Air Force Institute of Technology
 EUROSENSE
 SATCOM1 Aps
 SETCCE
 Aerovisión Vehículos Aéreos S.L
 Thales Communications S.A.
 Mediterranean Academy of Diplomatic Studies

COUNTRY

France
 Italy
 France
 Spain
 Sweden
 Germany
 Belgium
 Poland
 Belgium
 Denmark
 Slovenia
 Spain
 France
 Malta

ANTIBOTABE / Isolation of recombinant antibodies neutralizing botulinum toxins A, B and E

© AntiBotABE



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 biotreatments.

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 (EMA). 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

Centre de Recherche du Service de Santé des Armées (CRSSA)
 Ministère de la défense (MLD)
 Technische Universität Braunschweig (TUBS)
 Institut Pasteur (Pasteur)
 Health Protection Agency (HPA)
 Centre National de la Recherche Scientifique (CNRS)
 LFB Biotechnologies (LFB)
 University of Helsinki (UoH)
 VITAMIB (VITAMIB)

COUNTRY

France
 France
 Germany
 France
 United Kingdom
 France
 France
 Finland
 France

BOOSTER / Bio-dosimetric tools for triage to responders



© Tommy Windecker - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°

242361

Total Cost

€4,583,559.24

EU Contribution

€3,284,291

Starting Date

01/07/2010

End Date

30/06/2013

Coordinator

**COMMISSARIAT
A L'ENERGIE ATOMIQUE
ET AUX ENERGIES
ALTERNATIVES**

 CEA LIST – Digiteo Labs
91 191 Gif-sur-Yvette
FRANCE
Contact**Marie-France ROBBE**

Tel: +33 (0) 1 69 08 87 49

Fax: +33 (0) 1 69 08 60 30

E-mail:

marie-france.robbe@cea.fr

Website:

<http://www.booster-project.org/>**Project objectives**

The effective management of an event involving the exposure of numerous people to radioactive material, whether accidental or following a malevolent act, requires a mechanism for the rapid triage of exposed individuals.

BOOSTER aims to develop new bio-dosimetric tools and to integrate them into a toolbox to quickly evaluate the level of potential casualties after a radiological event, and allow for an efficient triage of exposed people.

The project's objectives were: rapid evaluation of radiological incidents by sensors and retrospective dosimetry, development of new fast-acting biodosimetric sensors and adaptation of existing methods and devices, and the integration of all sensors in a portable toolbox usable by first responders, and for the training of first responders.

Description of the work

The BOOSTER System architecture was conceived to fit current procedures for radiological crisis management, based on the definition of different areas. The exclusion and controlled areas are defined from the radioactivity levels measured. The equipment used in the controlled area allows the cartography of the radiological situation: dose-rate-meters (Colibri & GPS-COM) for real time radiological measurements, rugged PDA for live information from first responders, gamma camera (Gampix) for hot spot location, and portable detector (FALCON 5000) for identification of radionuclides.

Results

The BOOSTER project developed a global and unique toolbox for:

- » quickly assessing the radiological situation in the field,
- » evaluating the radiological dose received by each victim and the toxicity of products used during the attack,
- » speeding up the categorization and triage of exposed individuals.

It also allows for potential follow-up material for medical staff in the medium/long term after an event.

PARTNERS

Commissariat à l'énergie atomique et aux énergies alternatives
AREVA CANBERRA
Hungarian Atomic Energy Authority
Center for Energy Research of the Hungarian Academy of Sciences
Karlsruher Institut für Technologie (KIT)
National University of Ireland, Galway (NUI Galway)
Universidad Politécnica de Valencia (UPV)

COUNTRY

France
France
Hungary
Hungary
Germany
Ireland
Spain

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

Ness A.T. Ltd. (Ness TSG)
 VectorCommand Ltd (VCL)
 Police National CBRN Centre (PNCBRNC)
 Prolog Development Center (PDC)
 Technical University of Denmark (DTU)
 Danish Emergency Management Agency (DEMA)
 Studiecentrum voor Kernenergie/Centre d'Etude de l'Energie Nucléaire (SCK-CEN)
 ARTTIC (ART)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Service de Santé des Armées (SSA)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Centre for European Security Studies (CESS)
 Robert Koch Institute (RKI)
 Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)
 Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH) (HMGU)
 Hospital University of Bonn (UKB)
 University of Jyväskylä (JyU)
 Technical Research Centre of Finland (VTT)
 University of Salzburg (PLUS)
 National Radiation Protection Institute (SURO)
 VÚJE Trnava (VUJE)
 Inconnect (INCONNECT)
 Magen David Adom (MDA)
 Center for Science Society and Citizenship (CSSC)
 Peace Research Institute Oslo (PRIO)

COUNTRY

Israel
 United Kingdom
 United Kingdom
 Denmark
 Denmark
 Denmark
 Belgium
 France
 France
 France
 Germany
 Germany
 Germany
 Germany
 Germany
 Germany
 Finland
 Finland
 Austria
 Czech Republic
 Slovakia
 The Netherlands
 Israel
 Italy
 Norway

COUNTERFOG / Device for large scale fog decontamination



Information

Grant Agreement N°
312804

Total Cost
€4,417,089.40

EU Contribution
€3,471,992.70

Starting Date
01/11/2013

Duration
48 months

Coordinator

UNIVERSIDAD DE ALCALA (UAH)
Departamento de Teoría de la Señal y Telecomunicaciones
Escuela Politécnica Superior. Campus externo
N-II km 33,600
28805 - Alcalá de Henares
Spain

Contact
JOSÉ LUIS PÉREZ-DÍAZ
Tel: +34 918856746
Fax: +34 616689298
E-mail: JI.perezd@uah.es
Website: www.counterfog.eu

Project objectives

COUNTERFOG will design, build and test a rapid response system for combating dispersed CBRN agents by using a fog made of a solution that could eventually contain any kind of neutralizing component. It should not only be suitable to be "incorporated" into a fog fire protection system in buildings, but also be able to be used in open air conditions. It is intended to provide a very fast and early response, greatly reducing the number of potential fatalities.

It is intrinsically an environmental-friendly and electric-compatible system. It would have three benefits: First, neutralizing and collapsing the CBRN cloud, second, rapidly decontaminating all the affected people in that area, and finally, rapidly decontaminating any equipment and the facility itself. It will be possible to counteract a CBRN cloud in large, open areas.

A Fog Dynamic Laboratory will be designed, built and used in the project to test the ability such a system has to condense different kinds of smokes, clouds or fogs and its ability to simultaneously neutralize different kinds of CBRN agents and combined incidents. A portable prototype will also be developed for full scale tests.

This project will also determine the best neutralizing agents and will characterize the effects and performance of the system. Eventually, the real applicability, side effects and compatibility with conventional fire protection facilities will also be investigated.

Description of the work

Computer aided engineering tools, the most recent manufacturing techniques and new materials are combined to design and build a "COUNTERFOG" generator able to produce an efficient neutralizing/decontaminating fog.

A laboratory for testing the fog dynamics will be designed and built as well. This will be used for experiments to determine the fog dynamics, fog dynamic interaction, condensation and neutralization with fogged decontaminants. It includes testing the harmfulness of the best decontaminants using small laboratory animals.

Other auxiliary technologies will be also developed as a simple sensor for monitoring the progress of the decontamination or new agents particularly useful for this kind of system.

A system prototype will be installed onboard a truck and a second one will be installed in a large building. Finally, full scale tests both in a large building and at open-air sites will be completed.

Expected results

COUNTERFOG will result in the development and characterization of the system with a guide for use, efficiency assessment and other parameters.

It will lead to the development, test and demonstration of a practical, fast, harmless and efficient system for neutralization of CBRN attacks and decontamination of large areas, including a way to track the progress of decontamination.

It will produce a set of demonstrated decontamination agents suitable for use in COUNTERFOG and an assessment of their expected efficiency. Particular attention will be focused on test the effectiveness of the system to counteract against combined risks that can arise as a consequence of terrorist attacks or accidents.

As a result of the tests, practical guides and know-how about the best way to install and use the COUNTERFOG will be provided.

PARTNERS

Universidad de Alcalá (UAH)
 University of Strathclyde (STR)
 Institute of Solid State Physics, Bulgarian Academy of Sciences (BAS)
 Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT)
 Institute of Inorganic Chemistry, Academy of Sciences of Czech Republic (IIC)
 Consilium Marine & Safety AB (CONSILIUM)
 BPE e.K. (BPE)
 Sección Española de la Asociación Europea de Ferroviarios (AEC-ES)
 Universidad Carlos III de Madrid (UC3M)
 Vojensky Vyzumny Ustav SP (VVU)

COUNTRY

Spain
 United Kingdom
 Bulgaria
 Spain
 Czech Republic
 Sweden
 Germany
 Spain
 Spain
 Czech Republic

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

Ecole Royale Militaire - Koninklijke Militaire School (RMA)
 Budapest University of Technology and Economics (BME)
 University of Brighton (UoB)
 University of Alicante (UALI)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 High Technology Filters s.a. (HTF)
 MAST Carbon (MAST)
 NORIT Nederland B.V (NORIT)
 Laser Optical Engineering Ltd. (LOE)
 ProQares BV (ProQares)

COUNTRY

Belgium
 Hungary
 United Kingdom
 Spain
 The Netherlands
 Greece
 United Kingdom
 The Netherlands
 United Kingdom
 The Netherlands

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

Universite Paris XII- Val de Marne (SAMU)
 IB Consultancy BV (IBC)
 NBC-SYS SAS (NBC Sys)
 Blücher GmbH (Blücher)
 Astrium SAS (Astrium)
 Falcon Communications Limited (CBRNe World)
 Bertin Technologies SAS (Bertin)
 Statni Ustav Jaderne, Chemicke a Biologicke Ochrany vvi (SUJCHBO)
 Drzavna Uprava za Zastitu i Spasavanje (DUZS)
 Prometech BV (Prometech)
 Hotzone Solutions Benelux (Hotzone Solutions)

COUNTRY

France
 The Netherlands
 France
 Germany
 France
 United Kingdom
 France
 Czech Republic
 Croatia
 The Netherlands
 The Netherlands

MIRACLE / Mobile Laboratory for the Rapid Assessment of CBRN Threats Located within and outside the EU



Information

Grant Agreement N°

312885

Total Cost

€1,420,617.05

EU Contribution

€1,130,605.00

Starting Date

01/12/2013

Duration

18 months

Coordinator

UNIVERSITÉ

CATHOLIQUE DE LOUVAIN (UCL)

Centre de Technologies Moléculaires Appliquées (CTMA)

Clos Chapelle-Aux-Champs

UCL- B1.30.24

1200 – Brussels – Belgium

Contact

GALA JEAN-LUC

Tel: +32 2 764 33 32

+32 2 764 33 65

Mobile: +32 495 59 78 13

Fax: +32 2 764 31 66

E-mail:

Jean-luc.gala@uclouvain.be

Website:

<http://www.uclouvain.be/ctma.html>

Project objectives

In the event of a major intentional, accidental or natural CBRN incident, fast detection and identification of agents on scene are crucial to ensure adequate risk assessment, optimal risk management, and proper counter measures. Consequently, a determining factor in effective incident response is to bring a rapidly deployable CBRN diagnostic and forensic device as close as possible to the crisis area.

However, there are many different ways to understand what a mobile response unit should be and develop it as a efficient counter-measure in case of CBRN-events. In that respect, the C, B, or RN specificity of the threat is of paramount importance, as is the possibility to have scalable capabilities and the possibility for joint multi-national intervention.

The objective of MIRACLE is to harmonize the definition of a mobile CBRN laboratory, to define its needs, and subsequently to provide solutions for deployment of this device in- and outside the EU.

Description of the work

A set of scenarios will be developed in which mobile laboratory capabilities could be added value. The scenarios will be divided by agent (C, B or RN) or location (within or outside the EU). For each scenario the criteria used to elaborate on the development of a mobile device will examine the potential cross-border impact of the CBRN incident and potential added value of the mobile laboratory facility in this context (no matter in what form). We will define and analyze the type of missions of a mobile device according to a set of 8 different scenarios of Chemical, Biological, Radiological and Nuclear cross-border incidents within and outside Europe.

A state of the art analysis of existing capabilities within the EU and gap analysis will identify areas for improvement and will assess the best possible organizational and operational structures to enable sustainability at optimal costs for society. The role of national or international regulatory authorities and agencies will be reviewed to assess which should be stakeholders of CBRN mobile abilities and how to coordinate the activities that are responsible for EU CBRN crisis management. A straightforward interface with existing EU capabilities and expertise will be delineated. A strong emphasis will also be put on other synergistic EU and non-EU projects.

Practicalities (i.e., structures, equipments and functions including operational procedures, communication, logistics, forensics and related legal issues) will be assessed with technological suppliers and end-users. Building partnerships and cooperation with interested stakeholders (e.g., EU key actors, nations within and outside the EU in strong demand for this type of capacity) will be a specific task dedicated to the dissemination of the MIRACLE project.

Expected results

The project outcome will be a set of deliverables describing the needs and solutions for a mobile CBRN laboratory ability. This will facilitate the plan for an evidence-based mobile CBRN laboratory capacity based on flexibility, scalability, modularity, and interoperability. This project is deemed of essential added value for EU policy as it is also in line with European Security Research and Innovation Forum and the EU-CBRN Action Plan.

PARTNERS

Université catholique de Louvain (UCL)
 Astrium SAS (AST)
 Bundeswehr Institute of Microbiology (IMB)
 Forsvarets forskningsinstitutt (FFI)
 Totalforsvarets forskningsinstitut (FOI)
 Nederlands Forensisch Instituut (NFI)
 Health Canada (PHAC)
 Police Service of Northern Ireland (PSNI)
 National Institute of Public Health & the Environment / Rijksinstituut voor Volksgezondheid en Milieu (RIVM)

COUNTRY

Belgium
 France
 Germany
 Norway
 Sweden
 The Netherlands
 Canada
 United Kingdom
 The Netherlands

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



© rolffimages - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°
241536

Total Cost
€4,580,243.01

EU Contribution
€3,493,199

Starting Date
01/05/2010

End Date
30/04/2013

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.

Results

The MULTIBIODOSE project analysed and adapted a variety of biodosimetric tools for assessing radiation exposure to the general population and enabling the identification of those exposed who should receive medical treatment.

The following biodosimetric tools were tested: dicentric assay, micronucleus assay, gamma-H2AX assay, blood serum protein expression assay and electron paramagnetic resonance (EPR)/optically stimulated luminescence (OSL) dosimetry in components of pocket electronic devices.

The project also established a biodosimetric network called "Realizing the European Network of Biodosimetry" (RENEB), which kicked off January 2012. The goal of

RENEB is to establish a sustainable European network in biological dosimetry involving laboratories and organisations from 16 countries that can support a coordinated response in case of major nuclear or radiological emergency in Europe. All MULTIBIODOSE partners are members of RENEB, and all biodosimetric tools developed and validated in MULTIBIODOSE are also included in the network. Within RENEB an exercise and training program was developed that will be pursued in the future.

The project also produced a software package for integrated statistical analysis of data from each of the assays described. Full details of the software functions are given in the manual which is available for download, using the software from the web page of MULTIBIODOSE. The software and manual were finalised and tested with the assistance of all project participants.

PARTNERS

Stockholm University Centre For Radiation Protection Research (SU)
 Bundesamt für Strahlenschutz (BfS)
 Universiteit Gent (UGent)
 Health Protection Agency (HPA)
 Institut de Radioprotection et de Sûreté Nucléaire (IRSN)
 Istituto Superiore di Sanità (ISS)
 Norwegian Radiation Protection Authority (NRPA)
 Radiation and Nuclear Safety Authority (STUK)
 Westlakes Scientific Consulting (WSC)
 Universitat Autònoma de Barcelona (UAB)
 Institute of Nuclear Chemistry and Technology (INCT)
 Helmholtz Zentrum München (HMGU)
 Bundeswehr Institut für Radiobiologie in Verbindung mit der Universität Ulm (UULM)
 University of Oxford (UOXF)
 EURADOS (EURADOS)

COUNTRY

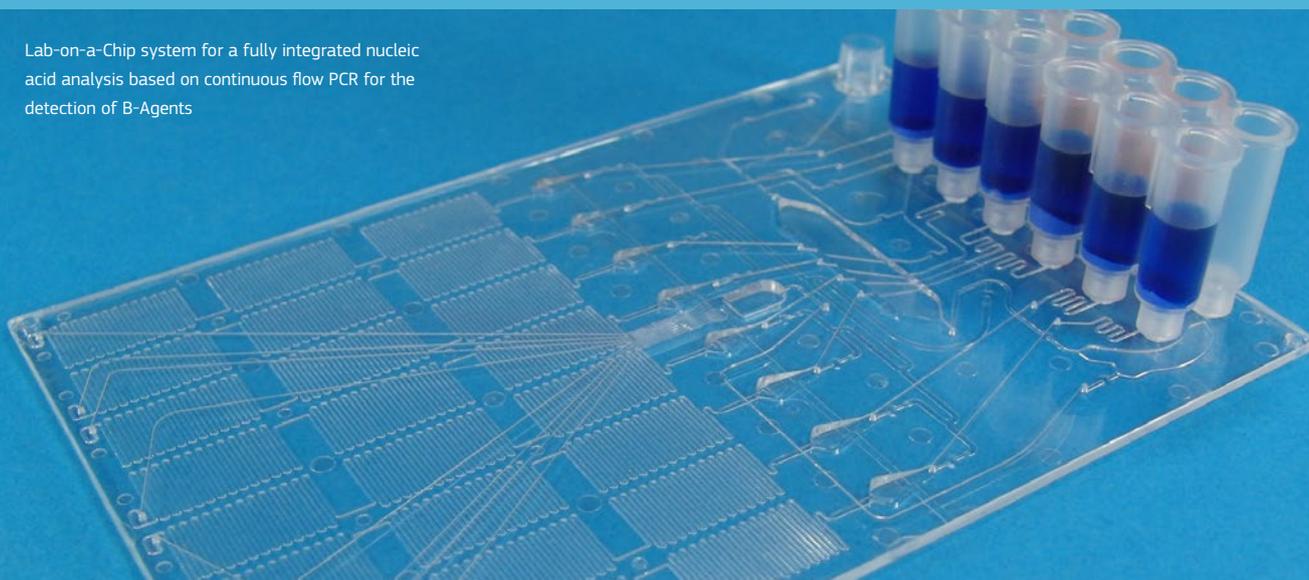
Sweden
 Germany
 Belgium
 United Kingdom
 France
 Italy
 Norway
 Finland
 United Kingdom
 Spain
 Poland
 Germany
 Germany
 United Kingdom
 Germany

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

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

Microfluidic ChipShop GmbH (MFCS)
Bertin Technology (BT)
Friedrich Loeffler Institut (FLI)
Integrated Microsystems for quality of Life SL (iMicroQ)
Institut für Mikrotechnik Mainz (IMM)
Universitat Rovira i Virgili (URV)
Institute of Physical Biology (IFB)
Cedralis (CED)

COUNTRY

Germany
France
Germany
Spain
Germany
Spain
Slovenia
France

PRACTICE / Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment 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

UMEÅ UNIVERSITY

European CBRNE Centre

Linneaus väg 6

90187 Umeå, Sweden

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

www.umu.se/cbrne

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

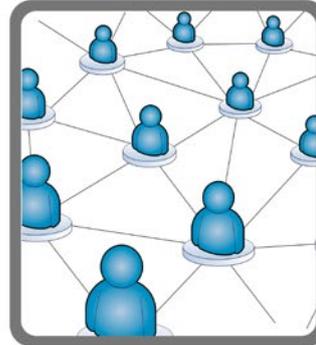
Umea University (UmU)
 Forsvarets forskningsinstitut (FFI)
 ASTRIUM S.A.S. (AST)
 Cassidian S.A.S. (EADS)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 KING'S COLLEGE LONDON (KCL)
 IB Consultancy BV (IBC)
 CBRNE Ltd (CBRNEItd)
 NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSR)
 Totalförsvarets Forskningsinstitut (FOI)
 UNIVERSITE CATHOLIQUE DE LOUVAIN (UCL)
 Netherlands Forensic Institute (NFI)
 STATNI USTAV JADERNE, CHEMICKÉ A BIOLOGICKÉ OCHRANY vvi (SUJCHBO)
 SELEX SISTEMI INTEGRATI SPA (SSI)
 SELEX GALILEO LTD (SELEX)
 ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (AstriPL)
 COMITE EUROPEEN DE NORMALISATION (CEN)
 Szkoła Główna Służby Pożarniczej (SGSP)
 MITTUNIVERSITETET (MIUN)
 Prometech BV i.o. (PRO)
 BRUHN NEWTECH A/S (BNT)
 HEALTH PROTECTION AGENCY (HPA)
 SODERSJUKHUSET AB (SPC)

COUNTRY

Sweden
 Norway
 France
 France
 The Netherlands
 United Kingdom
 The Netherlands
 United Kingdom
 Greece
 Sweden
 Belgium
 The Netherlands
 Czech Republic
 Italy
 United Kingdom
 Poland
 Belgium
 Poland
 Sweden
 The Netherlands
 Denmark
 United Kingdom
 Sweden

A4A / Alert for All

© DLR



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 Communica-
tions 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

Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)
 German Red Cross (DRK)
 Avanti Communications Ltd. (AVA)
 BAPCO LBG (BAPCO)
 TECNOSYLVA S.L. (TSYL)
 Empresa de Serviços e Desenvolvimento de Software, S.A. (EDISOFT)
 Fundación Tecnia Research & Innovation (Tecnia)
 Universität Stuttgart (USTUTT)
 Totalförsvarets Forskningsinstitut (FOI)
 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
 Eutelsat S.A. (EUT)
 Institut fuer Rundfunktechnik GmbH (IRT)

COUNTRY

Germany
 Germany
 United Kingdom
 United Kingdom
 Spain
 Portugal
 Spain
 Germany
 Sweden
 Germany
 France
 Germany

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-

UNIVERSITÄT

GREIFSWALD

Lehrstuhl Gesundheit

und Prävention

Institut für 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 respond 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.



PARTNERS

Ernst-Moritz-Arndt-Universität Greifswald
 University Medical Centre Hamburg
 University of Greenwich, School of Computing and Mathematical Sciences
 Institute of Public Security of Catalunya
 Hamburg Fire and Emergency Service Academy
 Man-Technology-Organisation (MTO)-Psychology
 Faculty of Fire Safety Engineering (SGSP)
 Prague Psychiatric Centre University of Prague
 Association of Emergency Ambulance Physicians
 Alma Mater Studiorum - Università di Bologna (UNIBO)

COUNTRY

Germany
 Germany
 United Kingdom
 Spain
 Germany
 Sweden
 Poland
 Czech Republic
 Turkey
 Italy

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
Forskingsveien 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

Stiftelsen SINTEF (SINTEF)
 Almende B.V. (Almende)
 CNet Svenska AB (CNET)
 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FIT)
 Lancaster University (ULANC)
 Crisis Training AS (CTAS)
 SAAB Training Systems (SAAB)
 THALES Nederland BV (THALES NL)
 Universität Klagenfurt (UNIKLU)
 Paris-Lodron-Universität Salzburg (PLUS)
 VSH Hagerbach Test Gallery LTD (VSH)
 Technische Universiteit Delft (TUDelft)
 Stockholms Universitet (US)
 Helse Stavanger (RAKOS)

COUNTRY

Norway
 The Netherlands
 Sweden
 Germany
 United Kingdom
 Norway
 Sweden
 The Netherlands
 Austria
 Austria
 Switzerland
 The Netherlands
 Sweden
 Norway

CascEff / Modelling of dependencies and cascading effects for emergency management in crisis situations



Information

Grant Agreement N°

607665

Total Cost

€4,626,904.00

EU Contribution

€3,594,937.80

Starting Date

01/04/2014

Duration

36 months

Coordinator

SP SVERIGES TEKNISKA FORSKNINGSINSTITUT (SP)

Fire Research

Brinellgatan 4

Box 857

SE-50115 Borås, Sweden

Contact

Prof. Anders Lönnemark

Tel: +46 10 516 5691

Mobile: +46 722 255691

Fax: +46 33 416012

E-mail:

anders.lonnermark@sp.se

Website: www.sp.se

Project objectives

Modern socio-technical systems are increasingly characterised by high degrees of interdependencies. Whereas these interdependencies generally make systems more efficient under normal operations, they contribute to cascading effects in times of crises.

CascEff will improve our understanding of cascading effects in crisis situations through the identification of initiators, dependencies and key decision points. The main objectives of the CascEff project are to:

1. gain a better understanding of the cascading effect in crisis situations.
2. develop an "incident evolution tool" for predicting present and future crisis evolution leading to cascading effects.
3. identify human activities in the crisis.
4. improve incident management for present and future threats.

Description of the work

The experiences from past incidents and findings on initiators, dependencies and key decision points will be further developed in the methodological framework of the incident evolution tool. This will enable improved decision support, contributing to the reduction of collateral damages and other unfortunate consequences associated with large crises. Use of the tool will be validated through its integration into different incident management and training platforms representing different end users in the project (e.g. NoKeos, iCrisis, RIB, WIS and XVR).

The work with CascEff is divided into five research work packages:

WP1: Incident management. A methodology will be developed for incident management which integrates predictions of an incident's evolution as based on an improved understanding of cascading effects. The methodology will be developed on the basis of identified and elaborated scenarios, taking into account cascading effects and their effect on the evolution of scenarios.

WP2: Originators and dependencies. The WP aims to identify essential characteristics that are required for development of an incident evolution tool with the aim to manage cascading effects. This includes the development of a methodology for analysing previous incidents regarding their originators, dependencies, and consequences.

WP3: First responders tactics, human activities, interaction and behaviour. The aim is to identify which human activities need to be taken into account during key points in an incident's evolution where decisions need to be made. This work package will also develop a methodology for communication and coordination during crisis situations that reflects the respective roles of members of the public, media organisations, first responders and intervention commanders at different levels.

WP4: Incident Evolution Tool development and implementation in existing systems. The incident evolution methodology that will incorporate cascading effects will be implemented into incident management frameworks used by end users in Europe today. The tools will be developed in close cooperation with end users (first responders, emergency managers, decision makers, etc.).

WP5: Scenario development and simulated exercises.

Scenarios will be developed for testing the incident command methodology and tools. In addition there is one work package for dissemination of the results (WP6) and one for project management (WP7).

Expected results

The project will produce models of dependencies and effects in crisis situations (of both physical and human components) causing a cascading effect. It will also provide a methodology to create this model for future threats, and tools to foresee the evolution of an incident. These tools will be available on a real time basis as well as for planning and training purposes, in particular in cross border crisis situations.

This will lead to reduced direct and indirect consequences by:

- » Reducing the extent of crisis scenarios subject to cascading effects and the risk for cross border scenarios
Highlight the need for cross border collaboration in response to specific originators
- » Promote new response strategies and structures and methodologies
- » Include development of a cloud monitoring system for multi-hazard events
- » Improve both the evacuation of large areas in crisis situations and the use and role of the media in crisis situations

PARTNERS

SP Sveriges Tekniska Forskningsinstitut (SP)
 Lunds Universitet (ULUND)
 Myndigheten för Samhällsskydd och Beredskap (MSB)
 Universiteit Gent (UGent)
 Institut National de L'environnement et des risques (INERIS)
 Service Public Federal Interieur (KCCE)
 Safety Centre Europe BVBA (SCA)
 Université de Lorraine (UL)
 University of Leicester (ULEIC)
 Northamptonshire County Council (NFRS)
 E-Semble BV (ESM)

COUNTRY

Sweden
 Sweden
 Sweden
 Belgium
 France
 Belgium
 Belgium
 France
 United Kingdom
 United Kingdom
 The Netherlands

CAST / Comparative Assessment of Security-Centered Training Curricula for First Responders on Disaster Management in the EU



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

UNIVERSITÄT SALZBURG

Office of the Rectorate

Research Support Unit

Kapitelgasse 4-6

A-5020 Salzburg

Austria

Contact

Prof. Friedrich

Steinhäusler

Tel: +43 662 8044 5700

Mobile: +43 680 123 7158

Fax: +43 662 8040 150

E-mail: Friedrich.steinhaeus-

ler@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 States 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 DERM – the Database on Emergency Response Major Incidents. Containing 110 real-life incidents from across Europe, Russia and the US, DERM 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.

RESEARCH
COMPLETED

The recommendations and new procedural priorities suggested include:

- » making the DERM 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.

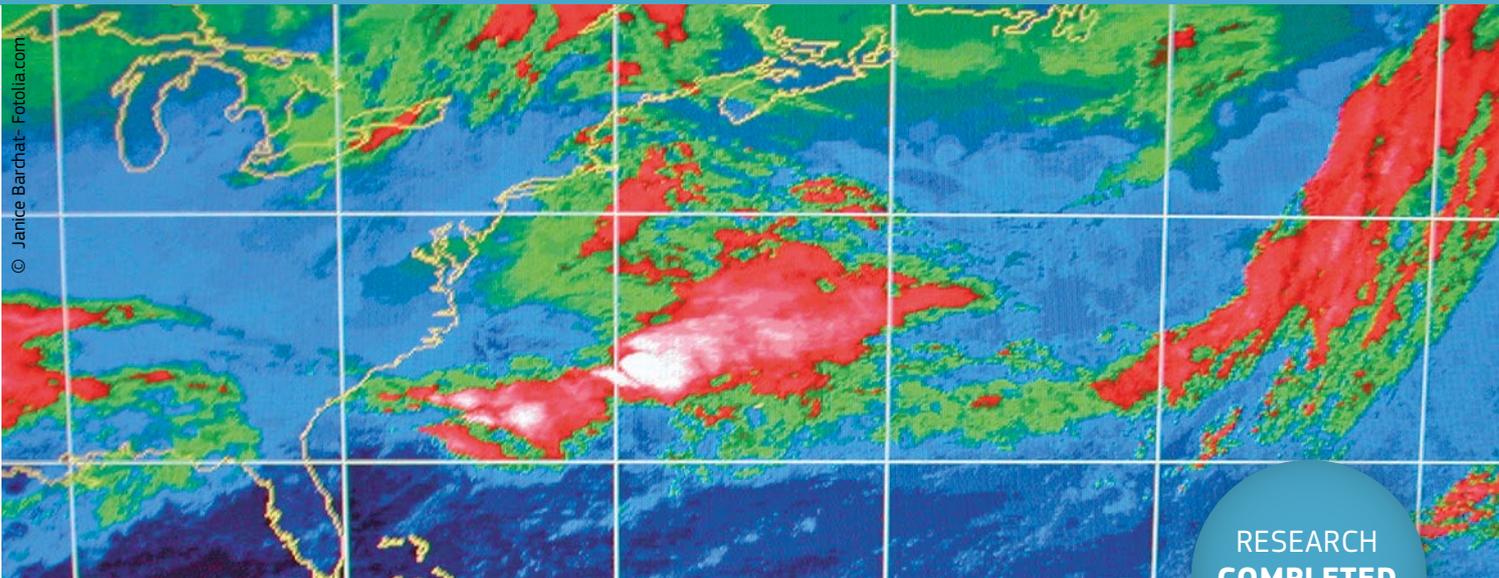
PARTNERS

Universität Salzburg (PLUS)
 DSTS-Advisers to Executives (DSTS)
 Fire Service Academy Hamburg (FSAH)
 Research Institute of Red Cross (FRK)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ICT)
 BMLVS / Heereslogistikschule (HLogS)
 International Security Competence Center (ISCC)
 University of Defense Brno (UDB)
 Corvinus University Budapest (VGT)
 SAAB Training Systems AB (SAAB)
 Swedish Counter Terrorist Police (SCTU)
 Diamond Aircraft Industries (DAI)
 Tecnom (TEC)
 Sigmund Freud Privatuniversität Wien (SFU)
 Police Service of Northern Ireland (PSNI)

COUNTRY

Austria
 Austria
 Germany
 Austria
 Germany
 Austria
 Austria
 Czech Republic
 Hungary
 Sweden
 Sweden
 Austria
 Spain
 Austria
 United Kingdom

COPE / Common Operational Picture Exploitation



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 Hämmäläinen

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

TECHNICAL RESEARCH CENTRE OF FINLAND (VTT)
 UTI SYSTEMS S.A. (UTI)
 CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)
 Pelastusopisto, Emergency Services College (ESC)
 Ministry of Interior and Administration Reform (IGSU)
 BAE Systems C-ITS (BAE Systems C-ITS)
 THE PROVOST, FELLOWS AND SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED
 TRINITY COLLEGE DUBLIN (TCD)
 BAE SYSTEMS (OPERATIONS) LIMITED (BAE Systems UK)
 SKYSOFT PORTUGAL - SOFTWARE E TECNOLOGIAS DE INFORMAÇÃO SA (Skysoft)

COUNTRY

Finland
 Romania
 Germany
 Finland
 Romania
 Sweden

 Ireland
 United Kingdom
 Portugal

CRISCOMSCORE / Developing a crisis communication scorecard



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 cooperation 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.

RESEARCH
COMPLETED

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

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

© Francois Doismel - 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
United Kingdom

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://idc.mdx.ac.uk/projects/crisis/)
[http://www.eis.mdx.ac.uk/
research/idc/](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

Middlesex University Higher Education Corporation (MU)
 SHELTERLAND ApS - 3D CONNECTION (CRI)
 National Aerospace Laboratory (NLR)
 ObjectSecurity Ltd (OS)
 Space Applications Services (SAS)
 VSL Systems AB (VSL)
 Linköping University (LiU)
 Haskoli Island - University of Iceland (HI)
 A E Solutions (BI) Ltd (AES)
 Aeroportos de Portugal, SA (ANA)
 British Transport Police Authority (BTP)
 Flugstodir (ISAVIA)

COUNTRY

United Kingdom
 Denmark
 The Netherlands
 United Kingdom
 Belgium
 Sweden
 Sweden
 Iceland
 United Kingdom
 Portugal
 United Kingdom
 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 TEKILLINEN

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

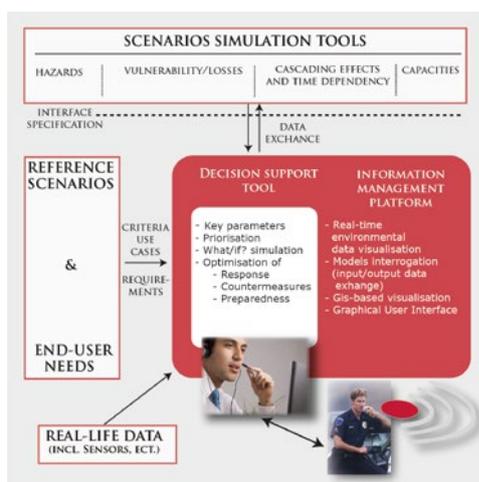
CRISMA IP focuses on large scale crisis scenarios with immediate and extended human, societal, structural and economic, often irreversible, consequences and impacts. These crisis scenarios cannot be managed alone with regular emergency and first responder resources, but require multi-organisational and 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.

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.



© Crisma

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

Valtion Teknillinen Tutkimuskeskus (VTT)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Analisi e Monitoraggio del Rischio Ambientale (AMRA)
 AIT Austrian Institute of Technology GmbH. (AIT)
 Association for the Development of Industrial Aerodynamics (ADAI)
 Tallinna Tehnikaulikool - Tallinn University of Technology (TTU)
 NICE Systems Ltd (NICE)
 European Aeronautics Defence and Space Company – CASSIDIAN Division (EADS)
 Insta DefSec (INS)
 Spacebel S.A (SpB)
 Cismet GmbH (CIS)
 Pelastusopisto - The Emergency Services College (ESC)
 Magen David Adom (MDA)
 Public Safety Communication Europe Forum (PSCE)
 Ilmatieteen laitos - Finnish Meteorological Institute (FMI)
 Deutsches Rotes Kreuz (DRK)
 ARTELIA Eau & Environnement (AEE)

COUNTRY

Finland
 Germany
 Italy
 Austria
 Portugal
 Estonia
 Israel
 Germany
 Finland
 Belgium
 Germany
 Finland
 Israel
 Belgium
 Finland
 Germany
 France

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

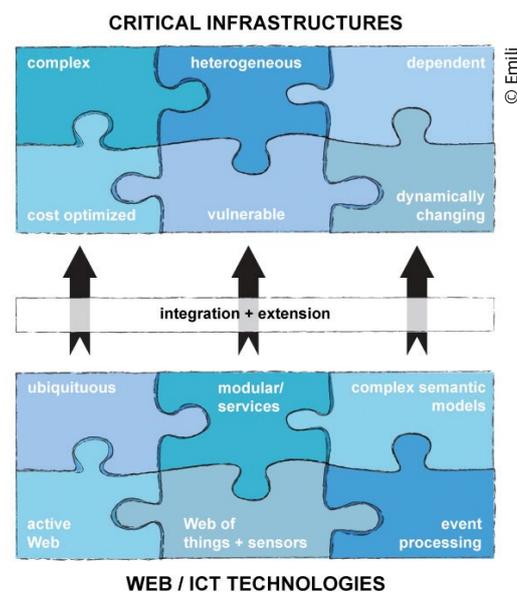
Dr. Rüdiger Klein
Tel.: +49 2241 14 2608
Fax: +49 2241 14 2342
E-mail: Ruediger.Klein@IAIS.
Fraunhofer.de
Website: www.emili-project.eu

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.



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

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
<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

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IVI)
 Salzburg Research (SRFG)
 Frequentis (FRQ)
 Brimatech Services GmbH (BRI)
 National and Kapodistrian University of Athens (NKUA)
 Earthquake Planning and Protection Organization (EPPO)
 German Red Cross (branch of the state of Saxony) (DRK-SN)
 University of Greenwich (UOG)
 IES Solutions (IES)
 Flexit Systems (FLEXIT)
 Austrian Red Cross Headquarters (ORK-HQ)
 Hellenic Ministry of Defence (HMOD)
 Department of Fire Brigade, Public Rescue and Civil Defence – Ministry of Interior (CNVVF)
 Satways Ltd. (STWS)
 TLP, spol. s r.o. (TLP)
 World Agency of Planetary Monitoring & Earthquake Risk Reduction (WAPMERR)
 Local Government of Achaia Prefecture (NEA)
 Center for Security Studies (KEMEA)

COUNTRY

Germany
 Austria
 Austria
 Austria
 Greece
 Greece
 Germany
 United Kingdom
 Italy
 Austria
 Austria
 Greece
 Italy
 Greece
 Czech Republic
 Switzerland
 Greece
 Greece

INDIGO / Crisis management solutions

© Galina Pankratova - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°

242341

Total Cost

€3,835,727

EU Contribution

€2,787,672

Starting date

01/05/2010

End Date

30/04/2013

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.

Results

The project developed a system to improve crisis management and crisis training, while improving cooperation across organisations and nations. The system integrates the latest advances in virtual reality and simulation in order to homogenize and enhance both operational preparedness and management of an actual complex crisis.

INDIGO's technology provides for inter-organisation preparation and response to trans-boundary crises and disasters in any environment. It also allows for inter-organisation exercises and information sharing and analysis to improve horizontal and vertical relations. Its features include:

- » 3D interactive and realistic visualization of the complete crisis environment, including data coming from the field, simulation results, and building interiors;
- » creation and simulation of different evolving scenarios for planning, training, and anticipating future states

and impending developments during operations, and the analysis of events after the crisis;

- » simultaneous training of decision makers, crisis managers and first responders influenced by simulated scenario and who would reciprocally influence its evolution;

INDIGO also drew up a European emergency symbology for 2D/3D maps. This will fill an important gap by offering a common visual reference that can be used across Europe for an immediate understanding of a situation, thus improving decision-making across organizational boundaries.

PARTNERS

Diginext SARL
 Consiglio Nazionale delle Ricerche
 Centre for Advanced Studies, Research and Development in Sardinia
 Immersion SAS
 European Committee for Standardization
 Crisisplan
 Swedish National Defence College
 Entente pour la forêt méditerranéenne

COUNTRY

France
 Italy
 Italy
 France
 Belgium
 The Netherlands
 Sweden
 France

OPSIC / Operationalising Psychosocial Support in Crisis



Information

Grant Agreement N°

312783

Total Cost

€4,371,594.28

EU Contribution

€3,333,918

Starting Date

01/02/2013

Duration

36 months

Coordinator

Danish Red Cross (DRC)

IFRC Reference Centre for
Psychosocial Support
Blegdamsvej 27
2100 Copenhagen OE
Denmark

Contact

Martha Margrethe Bird

Tel: +45 3525 9341
Mobile: +45 31 69 65 40
Fax: +45 35 25 92 92
E-mail: mabir@rodekors.dk
Website: www.opsic.eu

Project objectives

Over the past 20 years, psychosocial support (PSS) has played an increasingly important role in responses to crises and a number of high-quality European PSS guidelines and best practice studies have been made. However, none of the existing guidelines are fully comprehensive in terms of psychosocial support for all target groups, in different phases and different types of crisis.

The objective of the project is to design and develop an IT/web-based comprehensive operational guidance system (OGS) based on new research and analysis of existing PSS guidelines and best practices. The OGS will operate as a common shared platform and single point of reference for PSS in crisis management, serving multiple target groups with multiple functions.

A static part of the OGS will include a comprehensive guideline and a clear overview of existing guidelines, providing crisis managers and other professionals with an IT-based best practice go-to-point for all methods and tools needed to plan, as well as conduct and evaluate PSS interventions throughout all stages and all kinds of crises.

An interactive part of the OGS will give staff, volunteers, victims and affected communities direct access to relevant PSS information and guidance on self-help tools and methods. As PSS crisis managers can access statistical information based on hits and completed questionnaires, this platform can also be used to monitor the resilience and psychosocial well-being of helpers and survivors so that timely support may be provided.

Description of the work

Existing PSS guidelines will be identified and analysed in order to assess their practical relevance. Their tools and methods will be matched to various target groups,

types and phases of crisis (natural or man-made) and gaps will be filled-in from literature. Where this is not possible, recommendations for future research will be made. Finally, a clear overview of existing guidelines will be made.

Focusing on crises which took place in Europe during the past 10-15 years, existing best practice studies will be identified and criteria for best practices in PSS assessment, intervention and established, will be listed. This will result in an overview of best practices.

A review of studies on long-term impact of crises will be made, including long-term psychological, societal and cultural impact of crises as well as resilience factors at the individual, family, group, community and societal levels in affected populations.

Incorporating all of the above, a comprehensive guidelines will be made based on recommendations for best practice PSS interventions for all relevant types and phases of crises as well as target groups. Ethical, cultural and gender considerations will be taken into account.

An IT/web-based operational guidance system (OGS) will be designed and developed. It will be validated through workshops, demonstrations and simulation tests in three countries with crisis managers, first responders and volunteers. Lessons learned will be incorporated into the comprehensive guidelines as well as the OGS. Subsequently, the OGS will be demonstrated for a governmental end-user and a road map for implementation of the OGS into EU end-users' protocols will be prepared.

Throughout the process, the advisory board and the ethical board as well as project partners will participate in consultations and give recommendations.

Expected results

Improved planning and coordination of crisis response PSS interventions in full compliance with existing European guidelines and agreed international standards.

In synthesizing all existing PSS guidelines and best practice studies into a generally accessible, coherent, information and guidance system for crisis managers and other stakeholders, this project will contribute to more secure societies as it provides important technical support to crisis managers and other professionals for their timely and optimal delivery of psychosocial support.

Victims and affected populations will have a more active participation in strengthening their own resilience and psychosocial well-being through self-help and peer-

support mechanisms. This will reduce short-term as well as long-term consequences of crisis both in the individual as well as on group and society level.

PARTNERS

Danish Red Cross (DRC)
 University of Innsbruck, Dept. of Psychology (UIBK)
 Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
 IMPACT (IMPACT)
 Academic Medical Centre (AMC)
 University of Zagreb, Faculty of Humanities and Social Sciences (UNIZ)
 Magen David Adom (MDA)
 General Directorate of Emergency and Civil Protection -Samur (SAMUR)
 Centre for Science, Society and Security (CSSC)
 Crossing Channels (CC)
 The National Centre for Crisis Management Research and Training (CRiSMART)

COUNTRY

Denmark
 Austria
 The Netherlands
 The Netherlands
 The Netherlands
 Croatia
 Israel
 Spain
 Italy
 The Netherlands
 Sweden

OPTI-ALERT / Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication

© S. Hofschlaeger / pixelto.de

OPTI-ALERT

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

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-FHSS)
 e*Message Wireless Information Services Deutschland GmbH (EMESS)
 UBIMET GmbH (UBIMET)
 Proteo S. p. A. (PROTEO)
 UNIQA Versicherungen AG (UNI)
 Göteborgs Universitet (UGOT)
 Süddeutsches Institut für empirische Sozialforschung e.V. (SINE)
 Regione Sicilia (SIC)
 Nederlands Instituut Fysieke Veiligheid (NIFV)
 Università degli Studi di Perugia (UNIPG)
 THALES Services SAS (THALES)

COUNTRY

Germany
 Germany
 Austria
 Italy
 Austria
 Sweden
 Germany
 Italy
 The Netherlands
 Italy
 France

POP-ALERT / Population Alerting: Linking Emergencies, Resilience and Training



Information

Grant Agreement N°

608030

Total Cost

€1,134,770.80

EU Contribution

€998,848.38

Starting Date

01/04/2014

Duration

24 months

Coordinator

UNIVERSITY OF GREENWICH

School of Computing and Mathematical Sciences
Old Royal Naval College,
Park Row, Greenwich
SE10 9LS, LONDON,
UNITED KINGDOM

Contact

Elisabeth Bacon

Tel: +44 2083318544

Fax: +44 2083318824

E-mail: e.bacon@gre.ac.uk

Website: www.gre.ac.uk

Project objectives

The main objective of POP-ALERT is to prepare societies and populations for crises and disasters in a rapid, effective and efficient way by blending traditional Crisis Preparedness and First-Reaction strategies with the use of innovative tools. POPALERT's conceptual approach focuses on how best to alert and support action by citizens under crisis conditions, in familiar and unfamiliar surroundings using mechanisms that will follow intuitive human behaviour.

POP-ALERT's objectives recognise that in most circumstances the number of personal response options are limited and the correct responses may have to be initiated without any prior knowledge of the surroundings or threats.

The project will aim to achieve the following:

- » Gain insight into society's understanding of large scale disaster events, their willingness to accept risk probabilities and engage in preparedness, and their behavioural responses to diverse situations by measuring expectations in both domestic and foreign situations;
- » Identify success stories within existing and past community preparedness programmes – both at the local and EU level – and compile a portfolio of case studies on social networking and community initiatives which could potentially be replicated in crisis;
- » Undertake evidence-based research on the most effective existing delivery routes for informing European citizens in a situation of crisis and to assess the overarching authority strategies of local and national administrations to contribute to the preparedness of citizens;

- » Study the best ways to blend contemporary tools with the existing practices in order to create flexible and easily deployable toolkits for preparing and alarming the European population in case of a crisis, taking into account social and cultural differences;
- » Propose a pilot project by designing criteria for selection of the area and population to be involved in the pilot, developing scenarios and objectives;
- » Provide a generic methodology to assess the effectiveness in raising an improved level of preparedness of the community.

Description of the work

POP-ALERT proposes to undertake thorough behavioural research and Crisis Management research in order to create a framework to facilitate the assessment of the population's capacity to make use of different Crisis Management strategies and technologies developed at the EU level.

The project will seek to study the best ways to blend contemporary tools with the existing practices identified in order to create flexible and easily deployable toolkits for preparing and alarming the European population in case of a crisis. The approach this project proposes for improving the current practices revolves around the use of messaging and cultural sharing technologies to create awareness.

POP-ALERT will propose a pilot project in order to test the generic methodologies and to assess their effectiveness in raising an improved level of preparedness of the community.

Expected results

1. A classification of the drivers, constraints and complexities of population preparedness in domestic and foreign situations and the creation of a framework for assessing and understanding community preparedness at the EU level.
2. A model for presenting, blending and disseminating community preparedness practices in order to promote transfer of knowledge and replicability to a larger scale.
3. A collection of sample training curriculums and tools to be used by authorities, organisations and first responders for preparing the community to cope with large scale crisis situations.
4. A set of methodologies for effectively communicating with populations using contemporary messaging and social networking tools to notify modern societies of risks and strategies related to large scale crisis situations.
5. A toolkit for preparing and alerting populations, including the best forms of accessibility to different communities, reaching through to citizens, strategies for achieving acceptance and indicators for evaluating the success of the strategies proposed.
6. A project demonstrating the efficiency and effectiveness of the tools developed, including an evaluation and recommendations for future actions to ensure these practices reach the market.

PARTNERS

University of Greenwich
 European Organisation For Security SCRL (EOS)
 Association Comité National Français du Comité Technique International de Prévention et d'Extinction du Feu (CTIF)
 Altran BV (ALTRAN)
 Camara Municipal de Lisboa (CML)
 Training 4 Resilience (T4R)
 Siemens Schweiz AG (SIEMENS)
 Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)
 Center for Security Studies (KEMEA)
 University of Chester
 Service Départemental d'Incendie et de Secours de la Haute-Corse (SDIS 2B)

COUNTRY

United Kingdom
 Belgium
 France
 The Netherlands
 Portugal
 United Kingdom
 Switzerland
 Portugal
 Greece
 United Kingdom
 France

PREDICT / Preparing for the Domino Effect in Crisis Situations



Information

Grant Agreement N°

607697

Total Cost

€4,635,020.99

EU Contribution

€3,460,192.99

Starting Date

01/04/2014

Duration

36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA)

CEA Centre Gramat
46 500 Gramat - FRANCE

Contact

Dominique Sérafin

Tel: +33 (0) 5 65 10 54 46

Mobile:

+33 (0) 6 76 73 54 22

E-mail:

Dominique.serafin@cea.fr

Website:

www.predict-project.eu

Project objectives

The general goal of the PREDICT project is to deliver a comprehensive solution for dealing with cascading effects in multi-sector crisis situations. Its objectives are:

- » gather and analyse available domain knowledge;
- » develop a common framework;
- » create conceptual and executable models of cascading effects and interdependencies;
- » develop a suite of software tools;
- » validate the solution through running simulations;
- » disseminate project results and build appropriate liaisons among stakeholders.

Description of the work

The PREDICT solution comprises three pillars: methodologies to consider cascading effects, creation of models and, finally, development of tools.

PREDICT's work consists of:

- » WP1 provides organisational basis and on-going overall management for all project activities;
- » WP2 delivers basis for modelling in a form of taxonomy and scenario and inputs for system design as a technical specification;
- » WP3 uses the basis from WP2 in order to provide understanding of cascading effects by defining models and methodologies;
- » WP4 delivers overall system design (system architecture) and manages iterative system realisation and integration;
- » WP5 and WP6 develop together crucial elements of the PREDICT Incident Evolution Tool i.e. Foresight and Prediction Tool (WP5), Decision Support Tool (WP6) and Expert Integration Network Module (WP6);
- » WP7 provides the Training Module for Incident Evolution Tool and manages end-users involvement in a form of continuous evaluation;
- » WP8 End-user network will organise a series of 5 workshops throughout the project, involving external end-users;
- » WP9 Dissemination & Exploitation provides the necessary website and workshop to liaise with other projects and organise the final conference. It will also look at ways to exploit the results of the project after it ends.

Expected results

The PREDICT solution is:

- » expected to increase the awareness and understanding of cascading effects in crisis situations;
- » expected to enhance the preparedness for cascading effects;
- » expected to improve the capability to respond of various levels decision makers (local, regional, national or international).

PARTNERS

Commissariat à l'Energie Atomique (CEA)
 ITTI Sp. Zo.o. (ITTI)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V. (Fraunhofer)
 THALES SA (Thales)
 Compagnie Européenne d'Intelligence Stratégique (CEIS)
 Netherlands Organisation for Applied Scientific Research (TNO)
 Technical Research Centre of Finland (VTT)
 Veiligheids regio Zuid-Holland Zuid (Safety region South-Holland South) (VRZHZ)
 Suomenympäristökeskus (Finnish Environment Institute) (SYKE)
 Union Internationale des Chemins de Fers (UIC)
 Thales Netherlands (TRT-NL)

COUNTRY

France
 Poland
 Germany
 France
 Belgium
 The Netherlands
 Finland
 The Netherlands
 Finland
 France
 The Netherlands

PSYCRIS / PSYcho-Social Support in CRISIS Management



Information

Grant Agreement N°

312395

Total Cost

€4,774,842.99

EU Contribution

€3,827,525.79

Starting Date

01/07/2013

Duration

36 months

Coordinator

Ludwig-Maximilians- Universitaet Muenchen – (LMU)

Department Psychologie
Geschwister-Scholl-Platz 1
80539 – MÜNCHEN
GERMANY

Contact

Dr. Christine Adler

Tel: +49 89 2180 5175

Fax: +49 89 2180 5224

E-mail:

Christine.adler@psy.lmu.de

Website:

www.uni-muenchen.de

Project objectives

The aim of PsyCris is to develop and provide a roadmap as a bottom-up strategy to improve the psycho-social support infrastructure and the transnational cooperation of psycho-social emergency response services after a major incident in Europe. Within this overall objective, the proposed project PsyCris (36-months) has the following goals: (1) status quo analysis of psychological and medical support in crises in European countries, (2) improvement of support strategies for victims and crisis managers, (3) enhancement of psycho-medical preparedness for major incidents (contingency planning), (4) development of interventions to deal with stress and reduce stress related disorders of crisis management personnel and authorities, (4) providing efficient self-help strategies to communities affected by crises and (5) investigation of long-term psychosocial, societal and cultural impact of crises.

Description of the work

The PsyCris project will be executed over a 36-month period in three stages. The first stage is characterised by the concept development of three reference disaster scenarios. The opinion and comments of end-users will be included in this process. The actual needs of end-users will be carefully identified. This will ensure high quality user requirements specification and a realistic operational concept accepted by the end-users. An evaluation of effective psycho-medical interventions and of longer term societal, psychological and cultural impact of a crisis will be carried out. In the second stage, the development and design of the components of the PsyCris tool kits will take place. In the third stage, the various components (e.g. stress assessment, stress management, contingency planning, help the people help themselves) will be integrated in an overall PsyCris tool kit demonstrator, which will be based on a comprehensive knowledge

system (PsyCris Preparedness-Planning-Prevention (PPP) Platform).

The PsyCris PPP Platform will be developed on the grounds of our understanding of prevention, which is based on three stages: primary, secondary and tertiary prevention. Finally, the effectiveness of PsyCris PPP Platform will be evaluated, once again involving end-users in this process.

Research and development are based on a multi-disciplinary approach including methods from psychology (e.g. stress management, human resources management, psycho-trauma intervention), education sciences (e.g. knowledge management), informatics (e.g. decision making heuristics), engineering, sociology and health sciences. Current and possible changes in society, health systems and climate as well as cross-cultural and gender aspects are carefully considered. The 11 partners of the consortium comprise research centres, public bodies, small / medium enterprises and stakeholder / end-user organisations from Germany, Spain, Israel, Lithuania, Luxembourg and Austria.

Expected results

As its main product, the project will provide a set of tool kits enabling (1) efficient handling of relevant data, (2) transfer of knowledge and practical competences relevant for crisis management, stress control and social support and (3) rapid decision-making in crises. The tool kits are integrated within a computerised knowledge system combining e-learning and face-to-face teaching. PsyCris will propose guidelines for preparedness, prevention and intervention for crises: it is expected that the results will have a significant impact on public health, community resilience, international cooperation and cost containment.

PARTNERS

Ludwig-Maximilians-Universitaet Muenchen (LMU)
 Universidad de Granada (UGR)
 UMIT-Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT)
 Viesoji Istaiga Kitokie projektai (KKP)
 Blended Solutions GmbH (BSO)
 Bayerische Forschungsallianz (Bavarian Research Alliance) GmbH (BayFOR)
 Amuta LeYeladim beSikun - Cohen-Harris Resilience Center for Trauma and Disaster Intervention (CHC)
 Unfallkasse Thüringen (UKT)
 Insight Instruments (ISI)
 Protection Civile Luxembourg Groupe de Support Psychologique ASBL (GSP)
 Colegio Oficial de Psicólogos de Andalucía Oriental (COPAO)

COUNTRY

Germany
 Spain
 Austria
 Lithuania
 Germany
 Germany
 Israel
 Germany
 Austria
 Luxembourg
 Spain

SECURENV / Assessment of environmental accidents from a security perspective



© 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.

**RESEARCH
COMPLETED**



© SECURENV



PARTNERS

Geonardo Environmental Technologies Ltd.
Adelphi Research
Totalförsvarets Forskningsinstitut (FOI)

COUNTRY

Hungary
Germany
Sweden

S-HELP / Securing Health.Emergency.Learning.Planning



Information

Grant Agreement N°

607865

Total Cost

€4,436,136.72

EU Contribution

€3,496,836.15

Starting Date

01/02/2014

Duration

36 months

Coordinator

UNIVERSITY COLLEGE

CORK + (UCC)

Business Information

Systems

O'Rahilly Building

Cork – Ireland

Contact

Karen Neville

Tel: 353 + 21 + 4903668

Mobile: 353 + 863952582

Fax: 353 + 21 4271566

E-mail: KarenNeville@UCC.ie

Website:

<http://www.fp7-shelp.eu/>

Project objectives

Securing Health.Emergency.Learning.Planning

Main Goal: development of decision support tools for improving preparedness and response of health services involved in emergency situations.

The central aim of the S-HELP project is to develop and deliver a holistic approach to healthcare preparedness, response and recovery. More precisely, it aims to:

- » define an interoperability standard to enable communication and coordination across different geographical areas and cultural settings;
- » facilitate a collaborative solution driven by end-users and supporting partners to meet the needs of different users in Europe and beyond;
- » define and apply an interoperability standard for multiple agencies that jointly respond to a disaster;
- » advance the design and application of currently available solutions to improve preparedness, response and recovery in emergency situations;
- » deliver decision supporting tools for emergency preparedness, response and recovery that are tested, evaluated and enhanced through quality, end user designed emergency scenarios.

Description of the work

The S-HELP decision support system will promote evidence-based decisions at all stages of emergency management (EM) – before, during and immediately following an incident, and including post-incident stages of evaluation and communication of information to the public.

S-HELP DSS will use a seven-stage methodological framework. This consists of one coordination and project management work package (WP1) and six targeted work packages (WP2-7). Seamless inter-linkages with all work packages will guarantee the effective transfer, sharing and exchange of information during the whole project.

Expected results

The S-HELP DSS will bring significant benefits to the management of emergencies, from learning and preparing for emergency incidents and analysing threats, to post evaluation, reporting and logistics management.

The tools delivered through S-HELP will result in improved preparedness and response of health services involved in large scale and/or cross border emergency situations.

An interoperable knowledge base for responder and decision-makers will be developed, thereby supporting the EU regulation CEN BT/WG 161, 'Protection and Security of the Citizen'.

PARTNERS

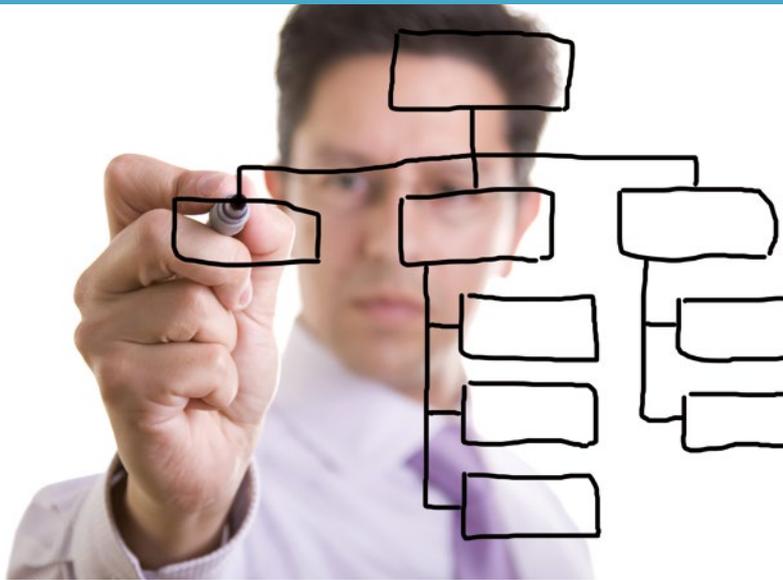
Future Analytics Consulting Limited (FAC)
 accelopment AG(ACCEL)
 Magen David Adom in Israel (MDA)
 Health Service Executive (HSE)
 Public Health Agency (PHA)
 Lunds Universitet (LU)
 Technische Universität Graz (TUGraz)
 Vectorcommand LTD.(VCL)
 Universität Wien (UVIE)

COUNTRY

Ireland
 Switzerland
 Israel
 Ireland
 United Kingdom
 Sweden
 Austria
 United Kingdom
 Austria

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).

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.



© Sicma

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

ELSAG DATAMAT S.P.A. (ED)
 SKYTEK LTD (SKYTEK Ltd)
 Centre for European Security Strategies GMBH (CESS)
 IFAD TS A/S (IFAD)
 ELBIT SYSTEMS LTD (ESL)
 ITTI Ltd (ITTI)
 INDUSTRIEANLAGEN BETRIEBSGESELLSCHAFT MBH (IABG)
 UNIVERSITA CATTOLICA DEL SACRO CUORE (UCSC)
 CONSIGLIO NAZIONALE DELLE RICERCHE (CNR-IASI)
 SELEX SISTEMI INTEGRATI SPA (SSI)

COUNTRY

Italy
 Ireland
 Germany
 Denmark
 Israel
 Poland
 Germany
 Italy
 Italy
 Italy

SNOWBALL / Lower the impact of aggravating factors in crisis situations thanks to adaptative foresight and decision-support tools



Information

Grant Agreement N°

606742

Total Cost

€5,205,926.70

EU Contribution

€3,882,462.70

Starting Date

01/03/2014

Duration

36 months

Coordinator

STE GENERALE DE DISTRIBUTION ET DE COMMUNICATION - GE DI COM (GEDICOM)

Avenue Maurice Bertaux 91
94420 - Le Plessis Trevisé
France

Contact

Jean Bruma

Tel: +33 (0)1 45 93 23 28

Mobile:

+33 (0)6 70 61 05 40

Fax: +33 (0)1 45 76 01 07

E-mail: jbruma@gedicom.fr

Website: www.gedicom.fr

Project objectives

The project's first objective is to help decision-making bodies make the most efficient decisions in times of crisis to minimize the effects of a crisis and its casualties. Snowball's main innovation is to integrate the cascading effects of a crisis in simulations, including post-communication to the public, therefore providing more accurate simulations and decision support.

To better predict cascading effects, the project will focus on three areas: the study and deeper understanding of cascading effects; the collection and storage of data and its availability; and the simulation of probable events occurring in the cascading chain.

Predicting cascading effects implies a better understanding of previous large-scale crisis and how these effects occurred. The project will study a wide history of crises to gain this understanding. One objective will be to study how population behaviour may become a cascading effect and an aggravating factor within a crisis.

Data availability is also crucial to the project. This is a real problem for crisis analyzing tools because data for studying a crisis, whether public or private, is not always reliable or consistent. Since cascading effects involve a variety of events across various fields (climate, networks, and human), this problem of data availability will be central to Snowball's work.

Thus, a key objective will be to provide access to all the data needed by the consortium. This will imply checking the reliability of data and unifying data formats so that all be integrated in the same tool.

The project will not only gather information while analyzing the mechanisms of cascading effects, it will also forecast via simulation the evolution of a crisis and its cascading effects. To do this, a methodology to integrate cascading effects will be developed by the project partners.

This methodology will break down the crisis into elementary "bricks". This approach relies on the fact that, whatever the crisis - earthquake, volcano, storm, etc. - the resulting sequence of events is often similar (damages to networks, changes in population behaviour, etc.). In other words, a large portion of events from each type of crisis is the same. Thus globally, from one crisis to another, the originators may be different, but the events cascading from it are more or less similar.

One of the project's central ideas is to insert into one structural database all the possible events, broken down into their elementary bricks, and to make it possible for any crisis to be modelled in the database.

The advantage of such approach is that two different crisis can be modelled at the same time, with their consequences gathered into one. More importantly, the tool will be generic to allow monitoring of all types of crisis. Another advantage is that the tool could subsequently be extended to integrate more and more crisis events/bricks, thus refining the accuracy of its simulations.

The project's global solution will be tested via a demonstration that will serve two goals. First, the project will validate the functioning of the solution. Second, the partners will use the solution in different case scenarios to assess the preparedness of public bodies and first responders to manage and contain a crisis, including its cascading effects.

Description of the work

To develop a platform dedicated to monitoring a crisis and predicting its cascading effects, Snowball will analyse the needs and practices of potential end-users (decision makers, governments). An extensive study of previous crises and events whose effects and thus impact were amplified will be conducted to define a road map for forecasting cascading effects.

On the basis of these two studies, Snowball will determine the necessary data to be fed into the tool to establish the links between crises and how they can be predicted.

Expected results

A methodology for containing cascading effects which is adaptable to different levels of data availability.

A platform for assessing a crisis, predicting cascading effects, simulating its evolution, displaying the events and providing support to decision-makers.

PARTNERS

Ste Générale de Distribution et de Communication (GEDICOM)
 Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (Fraunhofer)
 Istituto Superiore Mario Boella sulle Tecnologie dell'Informazione e delle Telecomunicazioni (ISMB)
 Universita degli Studi di Napoli Federico II (LUPT-PLIVINS)
 Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)
 Université Catholique de Louvain (UCL)
 Inéo Engineering & Systems SNC (INEO)
 Szkoła Główna Sluzby Pozarniczej (SGSP)
 Pelastusopisto, Emergency Services College (ESC)
 Evroproject ood (EP)
 Magyar Voroskereszt Tarsadalmi Szerverzet (HRC)

COUNTRY

France
 Germany
 Italy
 Italy
 Germany
 Belgium
 France
 Poland
 Finland
 Bulgaria
 Hungary

ACRIMAS / Aftermath Crisis Management System-of-systems Demonstration - Phase I



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

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-INT)
 CRISIS MANAGEMENT INITIATIVE (CMI)
 NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSR)
 NEDERLANDS INSTITUUT FYSIEKE VEILIGHEID (NIFV)
 T-SOFT AS (TSOFT)
 TOTALFORSVARETS FORSKNINGINSTITUT (FOI)
 EUROPEAN COMMISSION - JOINT RESEARCH CENTRE (JRC)
 CENTER FOR SECURITY STUDIES (KEMEA)
 NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (TNO)
 TURKIYE KIZILAY DERNEGI (TRCS)
 TECHNOLOGIES SANS FRONTIERES ASBL (TSF)
 UNITED NATIONS UNIVERSITY (UNU-EHS)
 Cassidian S.A.S. (EADS)
 SELEX SISTEMI INTEGRATI SPA (SSI)
 PUBLIC SAFETY COMMUNICATION EUROPE FORUM AISBL (PSCE)

COUNTRY

Germany
 Finland
 Greece
 The Netherlands
 Czech Republic
 Sweden
 Belgium
 Greece
 The Netherlands
 Turkey
 Belgium
 Germany
 France
 Italy
 Belgium

CAERUS / Evidence based policy for post-crisis stability: bridging the gap



Information

Grant Agreement N°

607960

Total Cost

€4,080,027

EU Contribution

€3,249,999

Starting Date

01/03/2014

Duration

36 months

Coordinator

UNIVERSITÉ CATHOLIQUE DE LOUVAIN (UCL)

Centre for Research on the Epidemiology of Disasters, Institute of Health and Society

Clos-Chapelle-aux-Champs, 30

B1.30.15

1200 Woluwe Saint Lambert, Brussels, Belgium

Contact

Debarati Guha Sapir

Tel: +32 2764 3327

Mobile: +32 475 617 019

Fax: +32 2 764 3441

E-mail:

debarati.guha@uclouvain.be

Website: www.uclouvain.be

www.cred.be

http://caerus-info.net

Project objectives

The CAERUS consortium aims to identify humanitarian relief actions that pave the way for human development and stability in post-crisis societies. In particular, we aim to:

- 1) improve policies for transitional situations at global and regional level as well as strengthen operational policies in the field;
- 2) better understand the role of health and education as a drivers of stability in post-crisis settings;
- 3) adapt and apply existing European technologies to improve the efficiency of relief to development action.

Description of the work

Our research focuses on health and education in post-conflict and post-disaster settings. We will investigate how improved sectoral policies and delivery channels can help shape overall policies addressing the transition from fragility to resilience and development.

We will also implement population-based studies in key crisis-affected areas to obtain field evidence regarding the effects of such policies on populations. We will combine quantitative and qualitative data to investigate health equity, provision of health services by non-state armed actors, and the role of education in post-conflict. We will map vulnerabilities through geocoded information.

We will also seek to detect barriers to the provision of basic services in post-crisis settings. The CAERUS project will assess how European technologies, especially field telecommunications and mobile laboratory capacities, can be used to increase the timeliness and effectiveness of service provision in remote areas. At the same time these activities will increase European capacities to respond to outbreaks of rare and emerging diseases with pandemic potential.

Expected results

- » Policy and operational recommendations for transition to development phases;
- » Evidence from field studies on health equity, provision of health services by non-state armed actors, and the role of education in post-conflict areas;
- » Guidelines on the use of technologies, such as mobile laboratories and rapid diagnostic tests, in fragile settings to improve service delivery.

PARTNERS

Université Catholique de Louvain (UCL)
Forskningstiftelsen FAFO (FAFO)
European Center for Development Policy Management (ECDPM)
Norsk Institutt for Luftforskning (NILU)
Paris-Lodron-Universität Salzburg (PLUS)
The Royal Institute of International Affairs (RIIA)
Jadavpur University (JU)

COUNTRY

Belgium
Norway
The Netherlands
Norway
Austria
United Kingdom
India

COBACORE / Community Based Comprehensive Recovery



© Thinkstock

Information

Grant Agreement N°

313308

Total Cost

€4,378,908.70

EU Contribution

€3,497,636.07

Starting Date

01/04/213

Duration

36 months

Coordinator

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK – (TNO)

TNO Defense, Safety and Security

Oude Waalsdorperweg 63

2597 AK The Hague

THE NETHERLANDS

Contact

Paul A.J. Tilanus

Tel: +31 88 866 72 92

Fax: +31 88 866 73 75

E-mail: paul.tilanus@tno.nl

Website: www.tno.nl

Project objectives

The Community Based Comprehensive Recovery (COBACORE) project aims to support common needs assessment and recovery planning efforts in complex multi-sectorial, multi-stakeholder crisis environments by building upon the community as an important source of information and capabilities. COBACORE aims to help bridge the so-called collaboration gap: failure of collaboration through insufficient information sharing among partners, incompatible work practices and misaligned decision making processes. In the field of humanitarian needs assessment, this collaboration gap is ubiquitous and detrimental to the efficiency of many recent relief efforts. Closing this gap is the key to reduce the time needed for needs assessment, better needs monitoring, and planning.

The COBACORE project has four specific objectives: 1) Understand the domain of common needs assessments, 2) Develop a supporting environment for common needs assessment processes, 3) Evaluate the COBACORE workspace in a realistic setting and 4) Achieve transfer of concepts and tools to stakeholder communities.

Description of the work

COBACORE is a set of interconnected modules and mechanisms that maintain three state models: the community model, the context model, and the needs model. The information contained in these models is accessible for users through a collaborative workspace, customized to suit their needs and preferences. The models are built up post-crisis through collected data from the affected area, through collaborative manual completion and maintenance, and through use of existing information sources, and based upon generic frames that are developed in advance for different scenarios. Various supporting functions monitor and manage the models, and respond to demands from users.

The project has three major phases: the preparatory phase, the concept development phase and the evaluation and dissemination phase. In the preparatory phase, activities are mainly aimed at understanding the domain, preparing the case studies and setting the boundaries of work. In the concept development phase, project activities are geared at knowledge acquisition and user requirements analysis, whereas the evaluation and dissemination phase is mostly focused on concept evaluation and dissemination activities. Concept development and evaluation with end-users take places during every phase of the project.

Expected results

The COBACORE project will develop a platform through which greater cross-jurisdictional and joined-up delivery mechanisms can enhance the preparedness and response model to disasters (both natural and man-made) at different geographic scales (national, regional and community). The COBACORE platform is a web-based, information-driven workspace that is readily accessible from mobile devices, operational centers and remote locations. The platform will have different interfaces for the different stakeholders in the damage and post-crisis needs assessment community, tailored to suit user-specific demands and capabilities.

The COBACORE suite of tools will support common needs assessments efforts – damage recovery needs, economic needs, health and social needs, and other critical humanitarian needs. The COBACORE assets will stimulate community-wide involvement in information gathering, sensemaking, and needs assessment practices. The COBACORE will not replace but complement existing practices and tools, and will stimulate a community-based approach to needs assessment processes.

PARTNERS

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 University of Ulster (UU)
 Het Nederlandse Rode Kruis (NLRC)
 Deutsches Rotes Kreuz EV (GRC)
 Stichting Katholieke Universiteit Brabant Universiteit van Tilburg (TU)
 Downey Hynes Limited (DHP)
 Integrasys SA (INT)
 Causeway Data Communications LTD (GEOP)
 Žilinska Univerzita v Žiline (UZ)

COUNTRY

The Netherlands
 United Kingdom
 The Netherlands
 Germany
 The Netherlands
 Ireland
 Spain
 United Kingdom
 Slovakia

DESTRIERO / A DEcision Support Tool for Reconstruction and recovery and for IntEroperability of international Relief units in situations, including CBRN contamination Risks



Information

Grant Agreement N°

312721

Total Cost

€4,171,403.71

EU Contribution

€2,933,015.58

Starting Date

01/09/2013

Duration

36 months

Coordinator

E-GEOS (EG)

Product Development and

Programs -

Defence and Security

Via Stanislao Cannizzaro 71

00156-Rome-Italy

Contact

Maria Michela Corvino

Tel: +39 06 4079 6363

E-mail:

michela.corvino@e-geos.it

Website:

www.destriero-fp7.eu

www.egeos.it

Project objectives

DESTRIERO's objective is to develop a next generation post-crisis needs assessment tool for reconstruction and recovery planning. This will include: structural damage assessment and related data integration and analysis based on international standards; and novel (automated) data and information interoperability across organisations and systems in combination with an advanced multi-criteria decision analysis tool and methodology for multi-stakeholder information analyses, priority setting, decision making and recovery planning.

DESTRIERO aims to develop an advanced net-centric information management tool to support damage and needs assessment and the reconstruction and recovery phases in post-crisis situations.

- » DESTRIERO envisions an integrated framework with the following innovative functionalities: support continuous damage and contamination assessment, monitoring and updating through a combination of satellite data and aerial photos enriched with data from the field
- » Boost information sharing by "automated" data and information interoperability between relief organisations and their information systems for coordinated PDNA (post-crisis damage and needs assessment) and RRP (reconstruction and recovery plan) processes
- » Visualisation of these data in a common operational picture with links to needs assessments and recovery planning information within a multilayer GIS type user interface
- » Support prioritisation and joint decision making with a novel tool, based on a recently developed decision support methodology and prototype software

- » Centralise management information in a single location, including PDNA and RRP frameworks

Description of the work

Today more people than ever are threatened by disasters, with no regards if natural or man-made. DESTRIERO aims at developing a next generation post-crisis needs assessment tool for reconstruction and recovery planning.

Earth observation images will contribute to fast damage assessment and monitoring of the areas, together with data acquired by relief units on the field using novel smart-phone apps.

Identified needs will be recorded, stored and made available to all organisations involved.

Coordination and collaborative work at all levels of the organisations and among different ones will be possible through a network centric approach for the interoperability of information and service and the decision support tool. Critical infrastructure recovery will be considered a priority, as it's essential for the recovery of social and economic aspects (roads, bridges, schools, hospitals, plants, etc.), CBRN contamination and humanitarian aspects will also be taken into consideration, as aggravating circumstances, while support to accountability of humanitarian aid contributions will be facilitated.

Expected results

The DESTIERO Project expected results are the following:

- » Faster and better damage assessment for planning and monitoring of progress of recovery;

- » Improved damage assessment by integrating satellite data, aerial photos and data from the field (e.g. from mobile devices) into a coherent information management tool.
- » Fast and intuitive access for distributed users to visualise the dynamic “common operational picture”, during the planning and reconstruction period.
- » Integrate state of the art visualisation techniques based on I-NAV (Integrated NAVigation Services) developed in the FP6 LIMES project (FP6 Programme – Aeronautics&Space/ GMES Security).
- » Tagging of geographical areas (e.g. on contamination) and damaged buildings (e.g. on state of reconstruction) on satellite images will enable distributed users in control rooms or on the field to drill down to different layers of damage reports, pictures, remote control data, needs assessment and priority reports as well as progress information on-going the recovery phase.
- » Enable better collaborative decision making during the planning and reconstruction phase.
- » Support standardisation of assessment data, interoperability between different information systems from stakeholders and capabilities to compare damage and recovery requirements towards prioritisation and joint decision making.
- » DESTRIERO tool will offer standard damage assessment templates, built on internationally agreed procedures and standards (e.g. DaLa), to collect data in homogeneous formats.

PARTNERS

e-GEOS (EG)
 Consorzio Interuniversitario Nazionale per L'Informatica (CINI)
 Thales (TRT)
 Amper Programas de Electronica y Comunicaciones (AMPER)
 Universitat Politecnica de Valencia (UPVLC)
 Fraunhofer Institute for Industrial Engineering IAO (FHG)
 Asociacion de Empresas Tecnologicas Innovalia (INNO)
 Sesm Soluzioni Evolute per la Sistemistica e i Modelli S.C.A.R.L. (SESM)
 ITTI Sp Zoo (ITTI)
 Saadian Technologies Limited (SAADIAN)
 Fundação Assistência Médica Internacional (AMI)
 Police Service of Northern Ireland (PSNI)
 Słozkola Głowna Sluzby Pozarniczej (SGSP)

COUNTRY

Italy
 Italy
 France
 Spain
 Spain
 Germany
 Spain
 Italy
 Poland
 Ireland
 Portugal
 United Kingdom
 Poland

HELP / Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems

© Rafał Olechowski - Fotofia.com

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
POLITÈCNICA
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.

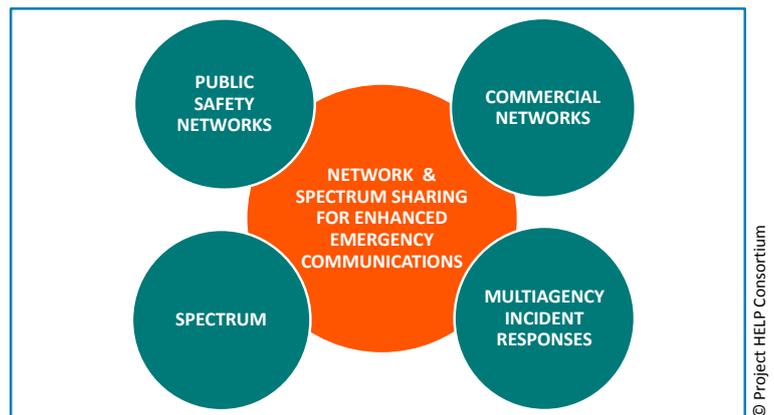
This will include, e.g.:

- » 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>.



© Project HELP Consortium

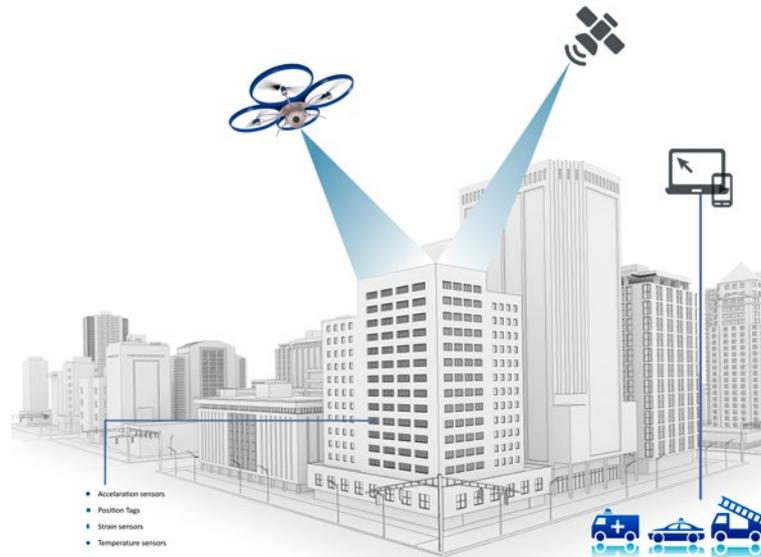
PARTNERS

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

RECONASS / Reconstruction and REcovery Planning: Rapid and Continuously Updated CONstruction Damage, and Related Needs ASSessment



Information

Grant Agreement N°
312718

Total Cost
€5,479,160.80

EU Contribution
€4,260,240.00

Starting Date
01/12/2013

Duration
42 months

Coordinator

INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS, (ICCS)

I-SENSE Group
9, Iroon Politechniou Str.
Zografou
Building of Electrical Engineers, Office 2131
GR-15773, Athens GREECE

Contact

Angelos Amditis
Tel: +30 210 772 2398
Fax: +30 210 772 2291
E-mail:
A.Amditis@iccs.gr
Website:
<http://www.iccs.gr/eng/>
<http://i-sense.iccs.ntua.gr/>

Project objectives

This work aims to develop a monitoring system for constructed facilities to provide a reliable, near real-time assessment of the structural condition and damage of both the structural components and the structural system of the monitored facility as a whole, after a disaster.

The scientific and technological objectives include:

1. SotA analysis for post-crisis damage and needs assessment tools;
2. Development of an indoor, automated, real-time, wireless, local positioning system by using 3D localization of tags for information gathering;
3. Development of method and software for assessment of economic loss, building functionality, volume of debris, duration of repairs and needs in manpower and materials;
4. Use of sensor-based damage assessment of the monitored buildings for calibrating and validating the remote sensing methods;
5. Demonstration of the RECONASS system in a 1:2 scale 3-storey reinforced concrete building;
6. Deployment of UAV for data analysis and evaluation;
7. Conceptualize the use of sensor-equipped buildings for additional threat detection (e.g. chemical or biological contamination).

Description of the work

RECONASS' main work packages include:

- » User Requirements and System Architecture;
- » RECONASS Monitoring System-Accurate Positioning-Secure Communication;
- » Damage, Loss and Needs Assessment;
- » Synergistic Damage Assessment with Air- and Space-borne Remote Sensing- Synoptic and Building-Specific Integration;
- » The PCCDN Tool;
- » System Integration;
- » System Evaluation.

Expected results

RECONASS is expected to deliver:

- » A combination of FMCW radar techniques with RF beam-steering and/or a multi band RF front end;
- » A stable/portable gateway will be developed having extended capabilities to offer ubiquitous connectivity and seamless services;
- » Photogrammetric processing of oblique airborne imagery taken from an UAV or satellite.

Its social and economic consequences include speeding up restoration and reconstruction efforts, providing updated information to response crews, reducing disaster costs and promoting safety.

PARTNERS

Institute of Communication and Computer Systems (ICCS)
 Technische Universität Dresden (TUD)
 Swedish Defense Research Agency (FOI)
 RISA Sicherheitsanalysen GMBH (RISA)
 Technice e Consulenze Nell' Ingegneria Civile SPA (TECNIC)
 D. Bairaktaris & Associates Structural Design Office (DBA)
 GEOSIG AG (GS)
 University of Twente, Faculty of Geo-Information Science and Earth Observation (ITC)
 Bundesanstalt Technisches Hilfswerk (THW)

COUNTRY

Greece
 Germany
 Sweden
 Germany
 Italy
 Greece
 Switzerland
 The Netherlands
 Germany

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.

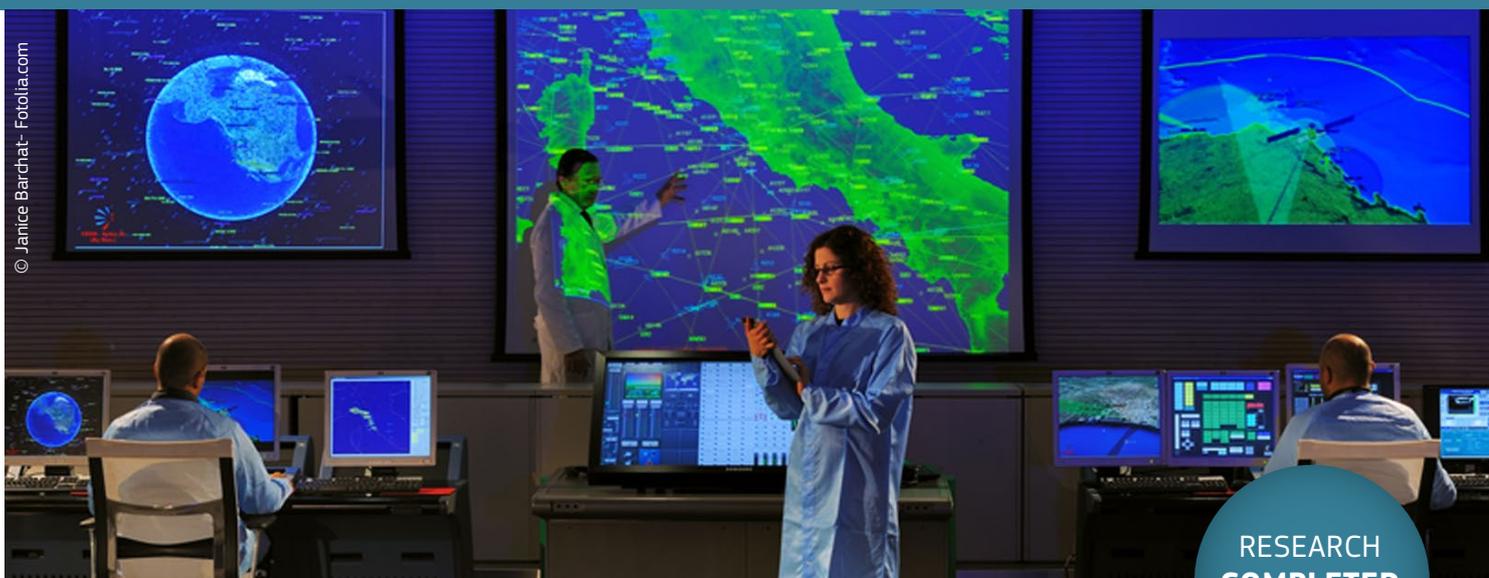
PARTNERS

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

CRISYS / Critical Response in Security and Safety Emergencies



© Janice Barchat - Fotolia.com

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

European Organization for Security (EOS)
 EDISOFT SA (EDI)
 Center for Security Studies (KEMEA)
 National Center for Scientific Research, "Demokritos" (NSCRD)
 ALTRAN BV (ALTRAN)
 International Association of Fire and Rescue Services (CTIF)
 Teletron Euroricerche SRL (TLT)
 Compania nationala de transport al energiei electrice Transelectrica SA (TRA)
 Société Française de Médecine de Catastrophe (SFMC)
 THALES Security Solution & Service SAS (T3S)
 Indra Sistemas S.A (INDRA)
 Istituto Affari Internazionali (IAI)
 University of Central Lancashire (UCLAN)
 Ministry of the Interior, Department for Rescue Services, SISAASIAINMINISTERIO (FMOI)
 Zanasi Alessandro SLR (ZAN)

COUNTRY

Belgium
 Portugal
 Greece
 Greece
 The Netherlands
 France
 Italy
 Romania
 France
 France
 Spain
 Italy
 United Kingdom
 Finland
 Italy

DARIUS / Deployable SAR Integrated Chain with Unmanned Systems

(SAR = Search and Rescue)

© alxpain - 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.euWebsite: 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

BAE Systems (Operations) Ltd (BAES)
 Cassidian S.A.S. (CASS)
 DFRC AG (DFRC)
 SKYTEK LTD (SKY)
 TELINT RTD Consultancy Services LTD (TEL)
 FUTURE INTELLIGENCE EREVNA TILEPIKINONIAKON KE PLIROFORIAKON SYSTIMATON EPE (FINT)
 OFFICE NATIONAL D'ETUDES ET DE RECHERCHES AEROSPATIALES (ONE)
 STIFTELSEN SINTEF (SIN)
 ECA SA (ECA)
 NATIONAL TECHNICAL UNIVERSITY OF ATHENS (NTUA)
 CENTER FOR SECURITY STUDIES (KEM)
 ECOMED bvba (ECO)
 CORK INSTITUTE OF TECHNOLOGY (NMCI)

COUNTRY

United Kingdom
 France
 Switzerland
 Ireland
 United Kingdom
 Greece
 France
 Norway
 France
 Greece
 Greece
 Belgium
 Ireland

ELITE / Elicit To Learn Crucial Post –Crisis Lessons



Information

Grant Agreement N°

312497

Total Cost

€1,185,911.40

EU Contribution

€940,418

Starting Date

01/01/2013

Duration

18 months

Coordinator

UNIVERSIDAD DE NAVARRA (TECNUN)

Paseo Manuel de Lardizabal 13

20018 Donostia-San Sebastian

Spain

Contact

José María Sarriegi

Tel: +34 943 21 98 77

Fax: +34 943 31 14 42

E-mail: coordinator@elite-eu.org

elite-eu.org

Website:

<http://www.elite-eu.org/>

Project objectives

The overall objective of the ELITE project is to improve European emergency preparedness, response and recovery from natural disasters such as floods, large scale forest fires and earthquakes. For this purpose several sub objectives are defined:

- » To establish a Community of Practice (CoP) in Crisis Management to improve the sharing of lessons learned and disaster knowledge among different organizations involved in the crisis management process such as responders, civil protection agencies, NGOs, critical infrastructures, private firms and industries etc.
- » Create a tested and validated ELITE living document of crisis management. The ELITE living document is a publicly available web solution comprised of:
 - + A “living” repository of best practices
 - + A “living” repository of guidelines
 - + Social media features where authorised agents can freely operate and interact
- » Implement the ELITE living document gathering information from experts through three scenario based workshops, a table-top exercise and interviews.
- » Analyse the learning process from lessons learned to lessons implemented to identify the existing difficulties
- » Deliver recommendations for future research. The project will deliver recommendations for future research in these topics:
 - + Knowledge gathering, categorisation and analysis processes
 - + Best practices and guidelines for each individual analysed disaster type: floods, earthquakes and fires.
 - + Integration of common aspects of different disaster types.
 - + Use of social media for learning and cooperation purposes.

Description of the work

The project is divided into six workpackages:

WP1: Management

WP2: ELITE Community of Practise –Workshops

Four scenario based workshops will be arranged for each disaster scenario (Fires, Earthquakes, Floods and Holistic). The ELITE CoP will contribute to the founding of the lessons learned database, to required validations and to dissemination and continuous update of the living document.

WP3: ELITE living document of crisis management

WP3 builds upon information from WP2 and comprises all the tasks needed to develop the living document, including requirement specification, design and programming.

WP4: Knowledge gathering, categorisation and analysis

WP4 includes knowledge gathering, categorisation and analysis in order to develop a holistic analysis of lessons learned.

WP5: Learning process analysis

Through WP5 a framework for knowledge and experience transfer, and learning process improvement across organizations and countries within the EU will be developed

WP6: Dissemination of lessons learned

It includes the dissemination activities carried out by all partners at workshops, meetings, etc. and by building relations with major actors involved in natural disasters.

Expected results

- » The establishment of the ELITE CoP that enables the involvement of end-users in the project as well as a broad dissemination and continuous update of the living document.
- » A tested and validated living document, which integrates the lessons learned in previous disasters, for improved preparedness, management and recovery from crises.
- » Holistic analyses of gathered lessons learned revealing common problems, best practises and solutions to transfer knowledge between disaster areas.
- » Inventory of relevant learning processes and training regimes in crisis management and an analysis of their benefits and weaknesses. The advantage of ELITE is that it will extract the underlying knowledge and experience transfer process in crisis management. Learning processes are important means to prepare for crisis management and training aims at preparing personnel on being effective and making decisions under high pressure and consequence contexts. The goal is continuous improvement.
- » Deliver recommendations for future research based on the research carried out in the ELITE project in journals, conferences and media, and ensure that funds is available for continuously updating the living document.

PARTNERS

Universidad de Navarra (TECNUN)
 Forsvarets Forskninginstitut (FFI)
 Hogskolen I Gjovik (GUC)
 Forschungsinstitut des Rotten Kreuzes (FRK)
 I.S.A.R. Germany Stiftung Gemeinnutzige Ug (Haftungsbeschrant) Gmbh
 Thales S. A. (TRT)
 Szkola Glowna Sluzby Pozarniczej (SGSP)
 Consiglio Nazionale delle Ricerche (IMAA-CNR)
 Associazione dei Comuni Dell'Umbria

COUNTRY

Spain
 Norway
 Norway
 Austria
 Germany
 France
 Poland
 Italy
 Italy

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 eLearn 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%

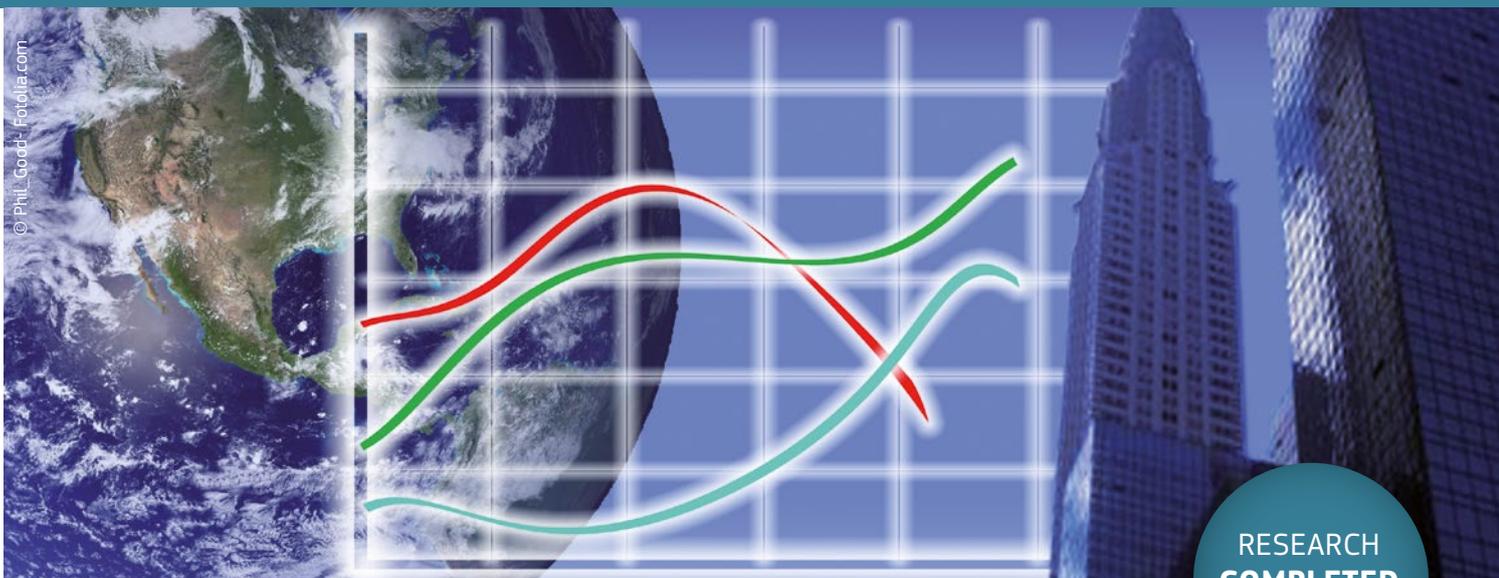
PARTNERS

Exodus S.A.(EXO)
 University of Modena and Reggio Emilia (UNIMORE)
 CrisisPlan B.V. (CPLAN)
 Prosyst Software GmbH (PROS)
 Immersion S.A. (IMM)
 Rose Vision (ROSE)
 Telcordia Poland Sp. z.o.o. (TARC-PL)
 Centre Suisse d'Electronique et de Microtechnique S.A. (CSEM)
 Smartex Srl (SMTX)
 Technische Universität Dresden (TUD)
 YellowMAP AG (YA)
 PANOU S.A. (PANOU)
 Telcordia Taiwan (TARC-TW)
 Institute for Information Industry (III)
 Entente pour la forêt Méditerranée (EPLFM)

COUNTRY

Greece
 Italy
 The Netherlands
 Germany
 France
 Spain
 Poland
 Switzerland
 Italy
 Germany
 Germany
 Greece
 Taiwan
 Taiwan
 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

End Date

31/05/2013

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.

Results

The aim of the ESS project was to provide crisis managers with information needed to inform their decisions, and to mount an

RESEARCH
COMPLETED

effective response. ESS' specific objectives included improving on-scene data collection, expanding the dissemination of accurate data and minimising the uncertainty inherent to crises.

The ESS project achieved the following:

- » The development and improvement of front-end data collection tools
- » The creation of a centralised data fusion system that connects to all front-end sensors activated in the system.
- » The synchronised dissemination of relevant data

Sensors are often hard to put in place in crisis situations, which leads to insufficient or broken data. To counter this problem, ESS worked on the integration of current technologies to generate portable sensor platforms (UAVs, air balloons, blimps, tripods, etc.), which are especially hardy and reliable in the face of extreme conditions.

To connect and harmonise all the information flowing from the sensors, ESS developed the "Data Fusion Mediation System" (DFMS) as a centralised database connected to all front-end sensors activated in the system. ESS improved communication between sensors and database, data fusion of data from different types of sensors and spatial data localisation.

To improve dissemination the project developed a web-based portal. The idea behind the ESS portal was to create an efficient synchronisation framework to manage data and information flows between different public authorities involved in emergency management operations and the crisis managers (rescue forces, police, fire-department, homeland-security, municipality, etc.). The ESS portal provided the involved actors with a common, uniform and ubiquitous platform for collecting, analysing and sharing real time data for supporting management decisions.

PARTNERS

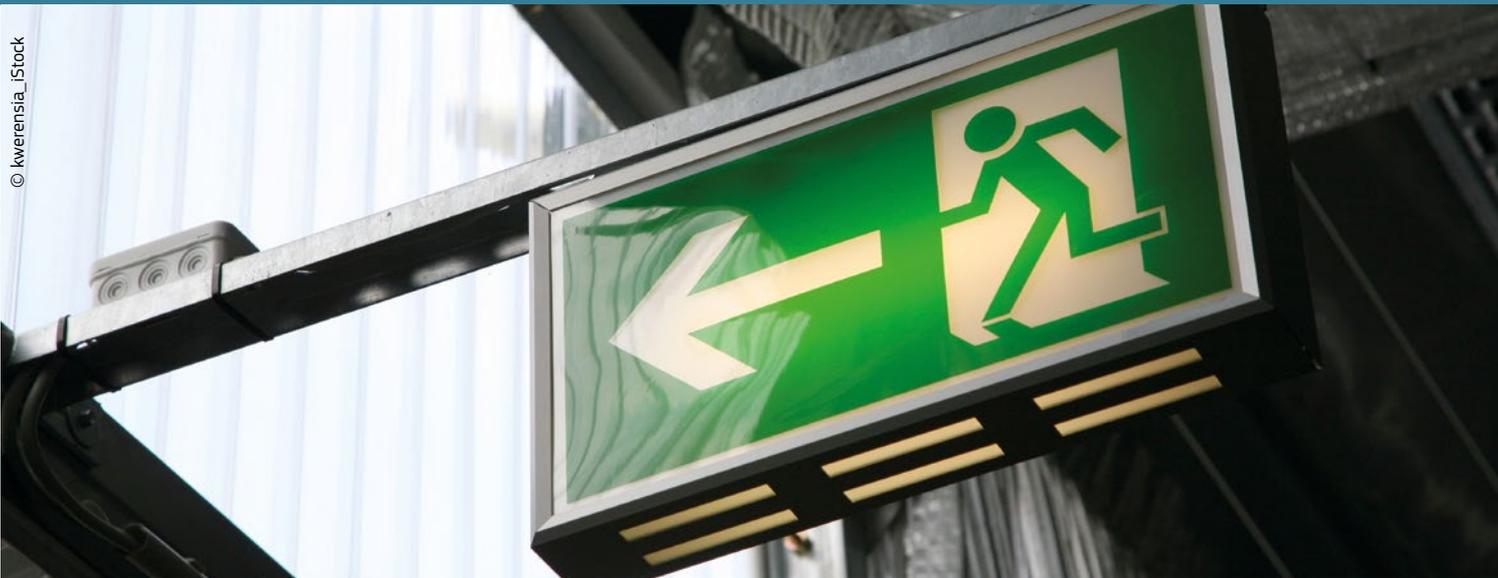
VERINT SYSTEMS LTD (VRNT)
 Wind Telecomunicazioni SpA (WIND)
 International Geospatial Services Institute GMBH (IGSI)
 Intergraph CS (ING)
 GMV Sistemas S.A. (GMV)
 CS Systèmes d'Information (CS)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IAIS)
 ITIS Holdings plc. (ITIS)
 Algosystems SA (ALGO)
 Alcatel-Lucent Italia (ALI)
 APD Communications Ltd. (APD)
 Anonymos Etaireia Antiprosopeion Emporiou Kai Viomichanias (ANCO)
 FAENZI srl. (FNZI)
 CENTER FOR SECURITY STUDIES (KEMEA)
 The Imego Institute (IMEGO)
 Magen David Adom (MDA)
 Ernst & Young (EY)
 Aeronautics Defense Systems (AERO)
 DIGINEXT SARL (DXT)
 Entente pour la forêt méditerranéenne (CEREN)

COUNTRY

Israel
 Italy
 Germany
 Czech Republic
 Spain
 France
 Germany
 United Kingdom
 Greece
 Italy
 United Kingdom
 Greece
 Italy
 Greece
 Sweden
 Israel
 Israel
 Israel
 France
 France

eVACUATE / A holistic, scenario-independent, situation-awareness and guidance system for sustaining the Active Evacuation Route for large crowds

© kwerensia_istock



Information

Grant Agreement N°
313161

Total Cost
€13,135,530.71

EU Contribution
€8,583,311.91

Starting Date
01/04/2013

Duration
48 months

Coordinator

EXODUS S.A (EXO)
Department of Business
Development and Delivery
73-75 Mesogeion Av &
Estias Str 1
115 26 Athens,
Greece

Contact
Dimitrios Vassiliadis
Tel: +30 2107450300
Mobile: +30 6947566676
Fax: +30 2107450399
E-mail: dvas@exus.co.uk
Website: www.exus.co.uk

Project objectives

The dynamic capture of situational awareness concerning crowds in specific mass gathering venues and its intelligent enablement into emergency management information systems, using smart communication devices and spaces is critical for achieving rapid, timely guidance and safe evacuation of people out of dangerous areas. Humans could be overwhelmed by fast changes of potentially dangerous incidents occurring at confined environments with mass-gathering. They could fail to make objective decisions to find their way to safety. This condition may lead to mass panic and make emergency management more challenging. To cope with these incidents, eVACUATE yields a holistic system:

- » To provide a valuable tool to guarantee enhanced Situational Awareness both to the crowds involved during a crisis but also to the crews operating in situ as well as in remote locations (security crews, first responders, crisis managers)
- » To adapt dynamically evacuation plans according to current conditions
- » To provide an easy to use (visual, multi-lingual) set of safe evacuation instructions available over a multitude of alternative and complementary presentation channels under a resilient, reliable and robust way, regardless of the functionality of the "global network"
- » To support civil protection authorities in the formation and validation of proper safety procedures for crowd management (Reconstruction of Experiences)
- » To set a cornerstone for the standardization of equipment, processes and methodologies for evacuation purposes on an EU level, addressing the cross-cultural issues emerging from diversity imposed by citizens

Description of the work

The overall mission of the eVACUATE consortium is to research, develop and demonstrate the capabilities of a framework that will enhance the effectiveness of complex crowd evacuation operations by:

1. Defining a full architecture and developing underlying necessary technological backbone, designed to provide improved data fusion, interconnection and interoperability between the different system elements and layers, reducing data ambiguity to a minimum.
2. Providing a full-set of systems and services built in accordance to innovative, integrated standards and peer-to-peer architecture, supporting a variety of complex crowd evacuation operations. This will be achieved with:
 - » Monitoring crowd behavior, surveying current environmental conditions, controlling the evacuation flow and predicting incidents that could cause problems to the overall operations
 - » Dynamically simulating an evacuation in a faster than real-time way so as to predict potential (future) incidents evolving as a consequence of other current events, through a game awareness framework
 - » Developing a centralized Data Fusion Mediation System (DFMS) to provide together with the command and control modules, the web portal and the back-end applications, an accurate and intelligent coordination of activities during evacuation operations and decision making
3. Integrating different innovative and existing modules such as:
 - » Multiple types of sensors ranging from visual cameras and hyper-spectral imaging to RFIDs and pervasive technologies,
 - » Sophisticated early location devices, based on Wireless Sensors Networks consisting of low-power sensors nodes
 - » Communication between first responders, command

centers and the crowd itself with integrated networking platforms and ad-hoc mechanisms to guarantee resilient communications

and performing the necessary hardware and software enhancements, so that all involved system elements can be seamlessly integrated to the main platform while interoperability is ensured.

4. Studying and developing the underlying socio-economic environment by addressing ethics, legal issues, regulation societal context, standardization and National and International operating procedures

5. Demonstrating the developed system and validating its operational characteristics in full-scale field trials that

will simulate realistic emergencies and crises. The whole system will be tested involving four different evacuation scenarios: a Football Stadium Scenario, an Airport scenario, a Cruise ship scenario and an Underground (Metro) scenario.

Expected results

eVACUATE foresees to develop an evacuation platform and strategy which through enhanced situational awareness will guide people away from the dangerous situations. In addition, eVACUATE is anticipating to increase effectiveness of forces responding to crisis in view of leading crowd to safer zones while reducing collateral damage, human errors and achieving faster restoration of security at the events venue and its affected proximities.

PARTNERS

EXODUS S.A (EXO)
 University of Southampton IT Innovation Centre (ITINNOV)
 Institute of Communications and Computer Systems (ICCS)
 HKV LIJN in Water BV (HKV)
 Telesto Technologies (TEL)
 Tekniker-Ik4 (TEK)
 Athens International Airport S.A (AIA)
 Vitrociset s.p.a (VITRO)
 Crowd Dynamics International Limited (CDI)
 INDRA SISTEMAS S.A. (INDRA)
 Katholieke Universiteit Leuven (KUL)
 Diginext SARL (DXT)
 Politecnico Di Torino – Dipartimento di Matematico (POLITO)
 STX France S.A (STX-FR)
 Technische Universität Dresden (TUD)
 Technische Universität Chemnitz (TUC)
 Real Sociedad De Futbol S.A.D (ASRS)
 Metro Bilbao S.A (METB)
 Telecom Italia S.p.A (TIM)

COUNTRY

Greece
 United Kingdom
 Greece
 The Netherlands
 Greece
 Spain
 Greece
 Italy
 United Kingdom
 Spain
 Belgium
 France
 Italy
 France
 Germany
 Germany
 Spain
 Spain
 Italy

FASTID / Fast and efficient international disaster victim identification



Information

Grant Agreement N°
242339

Total Cost
€2,990,190

EU Contribution
€2,270,476

Starting Date
01/04/2010

End Date
31/03/2013

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.

RESEARCH
COMPLETED

Results

FASTID focused on developing a prototype database to support Interpol's "Disaster Victim Identification" (DVI) forms since the latter represent massive amounts of paperwork that are hard to navigate. To improve Interpol's database's search function several matching techniques were developed as part of the project whose research included DNA matching techniques and "image" matching techniques.

FASTID created methods to search image databases by content-based image retrieval methods, using tattoo images as a secondary means of identification, for example. It also explored identification of human skeletal remains using face recognition software (FRS) and craniofacial reconstruction (CFR) and superimposition (CFS).

The team developed face recognition methods to aid the identification of persons based on images through biometric algorithms. The project also created training material in support of global common operational methodologies regarding data recording in INTERPOL member countries.

The prototype system has been implemented on Interpol's hosted platform in Lyon. Its conversion into actual production would aid international police cooperation for both disaster victim identification and for daily police work. The database has decentralized access for use in conjunction with mass fatality events and everyday policing requirements, for example.

PARTNERS

International Criminal Police Organization - I.C.P.O. (INTERPOL)
 Bundeskriminalamt (BKA)
 Plass Data Software A/S (Plass Data)
 University of Dundee (UNIVDUN)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Crabbe Consulting Ltd (CCLD)

COUNTRY

France
 Germany
 Denmark
 United Kingdom
 Germany
 United Kingdom

ICARUS / Integrated Components for Assisted Rescue and Unmanned Search operations



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

ECOLE ROYALE MILITAIRE - KONINKLIJKE MILITAIRE SCHOOL (RMA)	Belgium
SPACE APPLICATIONS SERVICES NV (SPACE)	Belgium
ESTUDIOS GIS S.L. (E-GIS)	Spain
Centre de Tecnologia aeroespacial (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

COUNTRY

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 3 6300292

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

Magen David Adom
 SAMUR Protección Civil, Ayuntamiento de Madrid
 AmbulanceZorg Nederland
 Danish Red Cross
 Sinergie S.r.l
 Fundación Rioja Salud
 Center for Science, Society and Citizenship
 Shield Group Inc.
 Charles University
 Al-Quds Nutrition and Health Research Institute

COUNTRY

Israel
 Spain
 The Netherlands
 Denmark
 Italy
 Spain
 Italy
 Aruba
 Czech Republic
 Palestinian-administered areas

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

SGL FOR USAR / Second generation locator for urban search and rescue operations



© puck - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°
217967

Total Cost
€6,218,278

EU Contribution
€4,859,026

Starting Date
01/10/2008

End Date
31/10/2012

Coordinator

**NATIONAL TECHNICAL
UNIVERSITY OF ATHENS**

Heroon Polytechniou
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.

Results

The project developed two tangible product prototypes: FIRST and REDS.

FIRST is a portable rescue device to monitor hazardous conditions or locate entrapped victims/dead bodies within collapsed buildings. It can be used for:

- » locating trapped victims
- » detecting unconscious victims using human scent
- » surveillance and monitoring of confined spaces
- » environmental monitoring of hazardous conditions

The second prototype, REDS, is a network of remotely controlled sensors that can be installed in a collapsed building for unattended monitoring and to detect life signs or hazardous conditions. It consists of eleven nodes: four fixed anchors and seven mobile probes. The latter comprise a gas sensor system, video camera, audio sensor, vibration sensor, medical locator, telemedicine probe and field portable GC/IMS instruments. REDS was designed to:

- » monitor confined spaces
- » check for life signs or hazardous conditions
- » remotely monitor a victim's vital signs
- » monitoring safety conditions during search and rescue
- » augment the capabilities of rescue teams

The project also developed a centralized command-and-control system to integrate the two prototypes and an environmental test chamber to simulate collapsed buildings, an alarm module and a digital library to identify image and sound signatures.

Finally, SGL for USAR investigated bioethics in rescue operations and created an online technology forum for discussion and collaboration between interested parties.

PARTNERS

National Technical University of Athens
 Service Départemental d'Incendie et de Secours du Vaucluse
 Direccio General De Prevencio I Extincio D'incendis I Salvaments
 FAENZI s.r.l.
 Valtion Teknillinen Tutkimuskeskus
 Gesellschaft zur Förderung der Analytischen Wissenschaften e.V.
 ECOMED bvba
 Environics Oy
 Austrian Academy of Sciences
 Entente Interdépartementale en vue de la Protection de l'Environnement et de la Foret contre l'Incendie
 ANCO S.A. Agencies, Commerce & Industry
 University of Dortmund
 TEMAI Ingenieros S.L.
 G.A.S. Gesellschaft für analytische Sensorsysteme mbH
 Universidad Politecnica de Madrid
 Savox Communications Ltd
 University of Athens
 Markes International ltd
 Bay Zoltan Foundation for Applied Research
 Critical Links SA
 The University of Loughborough

COUNTRY

Greece
 France
 Spain
 Italy
 Finland
 Germany
 Belgium
 Finland
 Austria
 France
 Greece
 Germany
 Spain
 Germany
 Spain
 Finland
 Greece
 United Kingdom
 Hungary
 Portugal
 United Kingdom

SPARTACUS / Satellite Based Asset Tracking for Supporting Emergency Management in Crisis Operations



Information

Grant Agreement N°
313002

Total Cost
€4,497,612

EU Contribution
€3,175,396

Starting Date
01/11/2013

Duration
36 months

Coordinator

D'APPOLONIA S.P.A. (DAPP)
Innovation Consulting
Division
Via San Nazaro 19
16145, Genova, ITALY

Contact
Clemente Fuggini
Tel: +39 02 51800562
Mobile: +39 3332090873
Fax: +39 02 51800563
E-mail: clemente.fuggini@dappolonia.it
Website: www.dappolonia.it

Project objectives

Motivated by the opportunity to develop industrial "pull" applications and services for the European EGNOS and GALILEO satellite systems, SPARTACUS will design, develop, test and validate in simulated and real world scenarios GALILEO-ready tracking/positioning solutions for critical asset tracking and crisis management. At a general level, SPARTACUS will implement solutions for location awareness for crisis management based on existing (GPS, EGNOS, EDAS) and incoming (GALILEO) satellite services and technologies. This will provide precise tracking/positioning by ensuring no gaps in communication or coordination information. This will be done in three application areas, namely to:

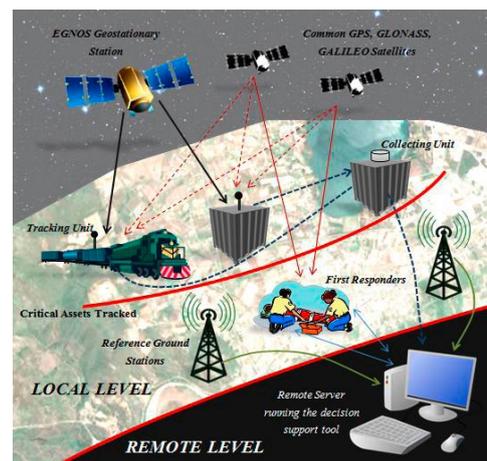
- » track, trace, and localise critical transport assets especially in times of crisis and in case of major failure of existing networks;
- » track the flow of relief support goods from the sending side to the receiving/end place;
- » support and ensure the safety of first responders in crisis management operations.

SPARTACUS end-users are rail and infrastructure managers, companies involved in logistic operations during crisis context, and first responders involved in emergency coordination and management.

Description of the work

The project's methodology will progress through identification, development, implementation and exploitation. Based on identification of end-user requirements, the functional and technical specifications of components and those at system level will be defined, followed by development of positioning, timing and communication technologies. The components will be integrated to achieve the system's full functionalities for demonstration in test beds, trials and practical exercises. Exploitation of the project results as well as training activities constitute the final actions SPARTACUS will carry out to ensure the solutions' deployment and to raise end-users' awareness and market acceptance.

SPARTACUS will work toward innovative hardware and software. This will include hardware adaptations, algorithms to improve the accuracy in tracking assets and persons, integration of the receivers with inertial platforms to provide dead-reckoning functionalities, and the availability of communication networks during emergencies via satellite backhauling.



Expected results

The main expected results are:

- » a GNSS-based unit for tracking critical assets and tracing first responders in disaster areas;
- » a communication networks that integrates terrestrial (4G-LTE) and satellite communications which will be made available during emergencies to provide a local communication network for first responders operating in disaster areas;
- » a set of decision support tools to be used for fleet management regarding the tracking of critical assets and for coordination in the case of first-responder operations;
- » a set of smartphone applications to improve location awareness and decision support as fed with operationally relevant information;
- » a fully integrated platform for critical assets tracking and coordination of first responders.

PARTNERS

D'Appolonia S.p.A. (DAPP)
 University of Pavia (UNIPV)
 University of Bologna (UNIBO)
 Newcastle University (UNEW)
 Romanian Railway Authority (AFER)
 Institut Mihajlo Pupin (IMP)
 Disaster Management Advice and Training (DMAT)
 AnsuR Technologies (ANSUR)
 TriaGnoSys GmbH (TGS)
 GlobalGPS (GLOB)
 Akkon University (AKKON)

COUNTRY

Italy
 Italy
 Italy
 United Kingdom
 Romania
 Serbia
 Austria
 Norway
 Germany
 Bosnia
 Germany

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. *SPEEDKITS*. Following best practice guidelines from humanitarian organisations, these solutions will also be *SEEDKITS*, 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

CENTRE SCIENTIFIQUE & TECHNIQUE DE L'INDUSTRIE TEXTILE BELGE (CTB)
 AIDE INTERNATIONALE DE LA CROIX-ROUGE LUXEMBOURGEOISE ASBL (SRU)
 HET NEDERLANDSE RODE KRUIS (NLRC)
 SIOEN INDUSTRIES NV (SIOEN)
 VRIJE UNIVERSITEIT BRUSSEL (VUB)
 TECHNISCHE UNIVERSITEIT EINDHOVEN (TU/e)
 POLITECNICO DI MILANO (POLIMI)
 De Mobiele Fabriek B.V (DMF)
 STICHTING WASTE (WASTE)
 STICHTING PRACTICA (PRACTICA)
 D'APPOLONIA SPA (DAPP)
 IBBK FACHGRUPPE BIOGAS GMBH (IBBK)
 MILLSON BV (MIL)
 ARTSEN ZONDER GRENZEN (MEDECINS SANS FRONTIERES NEDERLAND) VERENIGING (MSF)
 STIFTELSEN FLYKTNINGERADET (NRC)

COUNTRY

Belgium
 Luxembourg
 The Netherlands
 Belgium
 Belgium
 The Netherlands
 Italy
 The Netherlands
 The Netherlands
 The Netherlands
 Italy
 Germany
 The Netherlands
 The Netherlands
 Norway

BEAT / Biometrics Evaluation and Testing



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

Idiap Research Institute (IDIAP)
 Universidad Autonoma de Madrid (UAM)
 University of Surrey - CVSSP (UNIS)
 Ecole Polytechnique Federale de Lausanne - LASEC (EPFL)
 TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARASTIRMA KURUMU (TUBITAK)
 Commissariat à l'énergie atomique et aux énergies alternatives - LETI (CEA)
 Morpho (MPH)
 TÜVİT (TUVIT)
 Katholieke Universiteit Leuven (KULeuven)

COUNTRY

Switzerland
 Spain
 United Kingdom
 Switzerland
 Turkey
 France
 France
 Germany
 Belgium

FORTRESS / Foresight Tools for Responding to cascading effects in a crisis

© Image courtesy of A.Savin



Information

Grant Agreement N°

607579

Total Cost

€4,716,286.60

EU Contribution

€3,400,665.70

Starting Date

01/04/2014

Duration

36 months

Coordinator

TECHNISCHE UNIVERSITÄT BERLIN (TUB)

Center for Technology and
Society

Hardenbergstrasse 16-18
10623 – Berlin – Germany

Contact

Dr. Leon Hempel

Tel: +49-30-314 25373

Mobile:

+49-0176 111 20400

Fax: +49-30-314 26917

E-mail:

hempel@ztg.tu-berlin.de

Website: fortress-project.eu

Project objectives

Given the increasing interdependencies between different infrastructural sectors and countries, FORTRESS aims to improve crisis management practices by identifying the diversity of cascading effects that flow from the inter-relations of systems. Here, crisis management refers to a process of actions, decisions, and communications that are launched and implemented when an organisation has to cope with a major event with its consequences. Given the diversity of such organisations involved, a common understanding of the current situation, unfolding events, structures and processes is essential in order to achieve coordinated action and to avoid misunderstandings during crises.

The empirical results will be consolidated to create the FORTRESS Incident Evolution Tool (FIET). This will help forecast potential cascading effects. The tool integrates system and spatial data as well as sociological, human decision-making data.

Description of the work

FORTRESS is divided into three phases.

Phase 1 of the project will begin with a knowledge review around crisis situations. This includes the current understanding of cascading and cross-border effects of vulnerability and resilience as well as existing tools for crisis management.

In phase 2, an empirical database for the FIET will be developed. FORTRESS will combine case studies of historical crisis (from both Europe and International cases) with real-time scenario case studies of crisis management. The real-time scenario case studies consist of four crisis exercises.

1. A dam disruption in the border region of France and Italy
2. multiple infrastructure breakdowns due to a pan-European blackout in Berlin
3. cross-border flooding scenario in the Netherlands
4. a massive flooding in the Paris area with international impacts

Finally, in phase 3, a scenario builder tool for cascading and cross-border effects and further elements of the FIET will be developed.

Expected results

FORTRESS will develop a collaborative and accessible modelling platform for cascading and cross-border effects as well as a demonstrator of the FORTRESS Incident Evolution Tool (FIET) that can be used as a foresight tool to assist decision-makers in understanding the potential effects of their decisions in training environments.

PARTNERS

Technische Universität Berlin (TUB)
 Trilateral Research & Consulting LLP (TRI)
 Treelogic, Telemática y Lógica Racional para la Empresa Europea S.L. (TREE)
 Electricité de France S.A. (EDF)
 Dialogik gemeinnützige Gesellschaft für Kommunikations- und Kooperationsforschung mbH (DIA)
 IRKS Research GmbH (IRKS)
 Ritchey Consulting AB (RCAB)
 University College London (UCL)
 Istituto Superiore sui Sistemi Territoriali per l'Innovazione (SITI)
 GMV Sistemas S.A.U. (GMV)
 Veiligheidsregio Kennemerland (VRK)
 Service Départemental d'Incendie et de Secours des Alpes de Haute-Provence (SDIS 04)
 Berliner Wasserbetriebe (BWB)

COUNTRY

Germany
 United Kingdom
 Spain
 France
 Germany
 Austria
 Sweden
 United Kingdom
 Italy
 Spain
 The Netherlands
 France
 Germany

REDIRNET / Emergency Responder Data Interoperability Network



Information

Grant Agreement N°

607768

Total Cost

€4,327,171.80

EU Contribution

€3,498,968.00

Starting Date

01/03/2014

Duration

30 months

Coordinator

ARDACO, A.S.

EU department

Polianky 5

841 01 – Bratislava –

Slovakia

Contact

Peter Dohanyos

Tel: +421 (2) 3221 2311

E-mail: peter.dohanyos@

ardaco.com

Website: www.redirnet.eu

Project objectives

Over the recent years the majority of the REDIRNET consortia have participated in Projects SECRIKOM and FREEESIC, involving partners engaging significantly with a wide range of public safety officers across the EU. A benefit of this engagement has been the recognition that in addition to agency interoperability of communications a pressing need exists for agency interoperability of additional IT systems such as databases, sensor systems and cameras.

REDIRNET provides a framework for addressing this need with detailed mapping of user preferences and related legal requirements using innovative technologies. The consortium is aware that frequently it is non-technical issues that hinder agency interoperability, regardless of the quality of technical solutions. Consequently, user engagement across a range of agencies EU-wide will be ongoing throughout the duration of REDIRNET.

Description of the work

In recent years, first responder organizations across Europe have considerably improved their communications and IT systems with the deployment of new technologies. These include such innovations as unmanned surveillance and sensor systems that assist preventative actions and enhance responses to major crisis events.

Nevertheless, a number of recent major incidents have highlighted the challenges first responders face, most notably concerning interoperability barriers. These challenges are all the more difficult against the current economic and financial situation, where agencies are under considerable budgetary pressures and cannot invest

significant sums of money to enhance their interoperability. Even if inter-agency cooperation is not required on a frequent basis, enhancing agency interoperability has to be done through cost-effective solutions.

The project's work is divided into 7 work packages:

- » WP 1 – Project management;
- » WP 2 – Issues and Requirements;
- » WP 3 – Definition of pan-European interoperability framework;
- » WP 4 – Implementation of interoperability platform;
- » WP 5 – Integration of end users systems;
- » WP 6 – Acceptance and scenario testing by users;
- » WP 7 – Dissemination and exploitation.

The REDIRNET interoperability platform will be built as an extension of the FREEESIC platform which aimed to resolve interoperability issues between first responder communication systems in the same manner. REDIRNET will inherit the security features of the FREEESIC platform (i.e., ability to interconnect systems with certain levels of classification) and develop new features and modules enabling the interoperability of access to data fields and streams.

Furthermore the previous collection of interoperability issues undertaken by FREEESIC will be used as the baseline of inventory of issues that will be added during the REDIRNET project.

Expected results

REDIRNET introduces an interoperability system that provides seamless interoperability for participating agencies at a minor investment, but with great flexibility (in term of settings which data are visible for which partner agency) via a REDIRNET socio-professional web.

Agencies will be able link up to partner agencies of their choice and operational need, while being able at the same time to manage the scope of such interoperability.

To help set up these link-up arrangements REDIRNET will be enhanced with semantic web methods by relying on the vocabulary and processes of the user commu-

nity. Inter-operating agencies will need only to develop one gateway (to REDIRNET) leading to a cost effective solution; agency technologies will also be developed to facilitate the integration of user systems into REDIRNET. A content management system is software will allow the easy creation and management of webpages by separating the creation of content from the mechanics required to present it on the web.

PARTNERS

Ardaco, a.s. (ADO)
 British Association of Public-Safety Communications Officials (BAPCO)
 Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC)
 Institut Jožef Stefan (JSI)
 Nextel S.A. (NEXTEL)
 Pramacom Prague spol. s r.o. (PMC)
 Ústav Informatiky, Slovenská akadémia vied (UISAV)
 Université du Luxembourg (UL)
 Verde, s.r.o. (VERDE)

COUNTRY

Slovak republic
 United Kingdom
 Belgium
 Slovenia
 Spain
 Czech Republic
 Slovak Republic
 Luxembourg
 Slovak Republic

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:

- » 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).
- » Legal and ethical exchange of data to offer secure and legally/ethically compliant inter-organisation communication;

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.

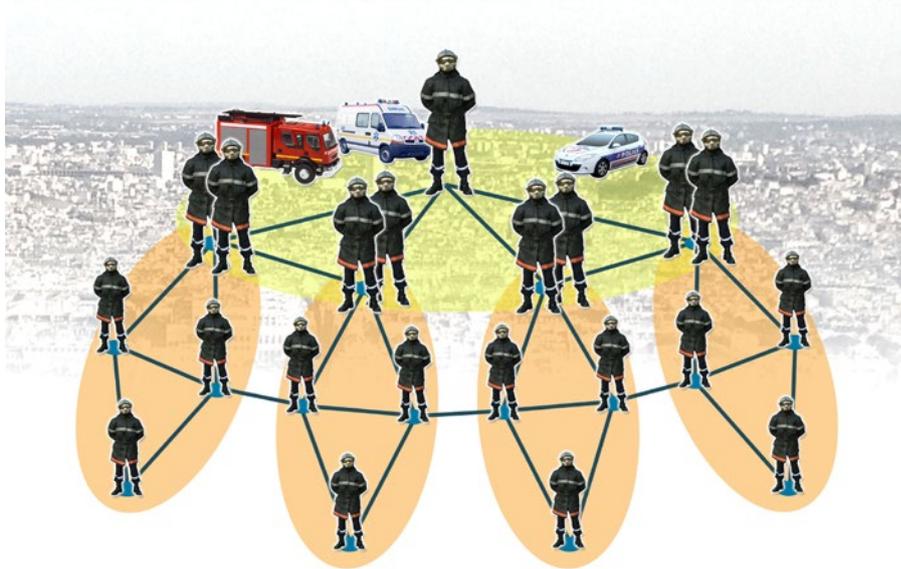
PARTNERS

ENGINEERING - INGEGNERIA INFORMATICA SPA (ENG)
 SEMANTIX TECHNOLOGIES PLIROFORIKIS TILEPIKOINONION ANONYMOS ETAIREIA (SEM)
 CENTRE FOR RESEARCH AND TECHNOLOGY HELLAS/INFORMATICS & TELEMATICS INSTITUTE (CERTH/ITI)
 QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)
 SINGULARLOGIC ANONYMOS ETAIRIA PLIROFORIAKON SYSTIMATON & EFARMOGON PLIROFORIKIS (SL)
 VRIJE UNIVERSITEIT BRUSSEL (IES/VUB)
 INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA-ISDEFE (ISDEFE)
 ALMAVIVA - THE ITALIAN INNOVATION COMPANY SPA (Almaviva)
 INNOVATION ENGINEERING SRL (INNEN)
 AYUNTAMIENTO DE MADRID (ADM)

COUNTRY

Italy
 Greece
 Greece
 United Kingdom
 Greece
 Belgium
 Spain
 Italy
 Italy
 Spain

C2-SENSE / Interoperability Profiles for Command/Control Systems and Sensor Systems in Emergency Management



Information

Grant Agreement N°

607729

Total Cost

€4,363,641

EU Contribution

€2,885,416

Starting Date

31/03/2017

Duration

36 months

Coordinator

SAGEM DEFENSE SECURITE (SAGEM)

Direction R&T

Arcs de Seine, 18/20 Quai

du Point du Jour

92100

Boulogne-Billancourt,

France

Contact

Banu Maria

Tel: +33 1 58 11 67 78

Mobile: +33 6 18 12 93 94

E-mail:

maria.banu@sagem.com

Website: www.c2-sense.eu

Project objectives

Effective management of emergencies depends on timely information availability, reliability and intelligibility. To achieve this, different Command and Control (C2) Systems and Sensor Systems have to cooperate, which is only possible through interoperability. However, unless standards and well-defined specifications are used, interoperability can be very complex.

C2-SENSE uses a "profiling" approach to achieve seamless interoperability by addressing all the layers of the communication stack in the security field.

The project's main objective is to develop a profile based Emergency Interoperability Framework by using existing standards and semantically enriched Web services to expose the functionalities of C2 systems, sensor systems and other emergency/crisis management systems.

C2-SENSE will develop a testing and a certification methodology allowing for the assessment of networked C2 and sensors systems for compliance with the profiles. The methodologies and framework will be made publicly available.

Description of the work

The work towards the definition and implementation of the profiles is organized in three steps:

- » First, an "emergency domain inventory" will be created by surveying existing standards, real life use cases of sensors, devices, C2 systems and emergency management architectures for different scenarios in the security field.
- » Then, based on this inventory, a common emergency domain ontology will be developed to gather all stakeholders' knowledge in a unique and flexible data model.
- » Finally, by using the concepts in this ontology, and by taking into account both the functional and operational requirements, as well as different countries' cultural, linguistic and legal issues, "emergency interoperability profiles" that will constitute the framework will be developed.

In parallel with the framework definition work stream, the pilot mapped on the requirements of the Apulia Civil Protection Service will be designed and implemented to serve as a validation model and demonstration of the concepts.

The necessary standardization activities will be initiated to evolve the C2-SENSE "Emergency Interoperability Framework" into a standard specification for interoperability between sensor systems and C2 systems.

Expected results

- » Increased robustness for sensors network management (sensors discovery mechanism, sensors allocation and life-cycle management).
- » A trusted communication infrastructure model creating interconnectivity between different networks including TETRA, WiMAX, GSM and WiFi.
- » Re-usable Web services for the emergency domain (assets and resources management, situation awareness, operations planning) based on standard data models.
- » Semantic mediation mechanisms able to: harmonize information conforming to different but overlapping emergency standards; and automate many implementation processes.
- » A service level agreements framework to be adopted for deployed procedures and operations.
- » A definition of overall interoperability requirements and a methodology to certify compliance.

PARTNERS

SAGEM DEFENSE SECURITE (SAGEM)
 LUTECH SPA (LUTECH)
 Austrian Institute of Technology GmbH (AIT)
 Software Research, Development and Consultancy Limited (SRDC)
 REGIONE PUGLIA (REGIONE PUGLIA)
 INNOVA PUGLIA SPA (IP)
 PRZEMYSLOWY INSTYTUT AUTOMATYKI I POMIAROW (PIAP)
 Regola srl (Regola)

COUNTRY

France
 Italy
 Austria
 Turkey
 Italy
 Italy
 Poland
 Italy

DISASTER / Data Interoperability Solution At Stakeholders Emergency Reaction

© PHOTOPOUR - 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

ing 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

Treelogic Telemática y Lógica Racional para la Empresa Europea S.L. (TREE)
 Fachhochschule Köln (CUAS)
 Fundación CTIC Centro Tecnológico para el desarrollo en Asturias de las Tecnologías de la Información (CTIC)
 Dansk Brand-Og Sikringsteknisk Institut Forening (DBI)
 Aimtech Consulting Limited (AIM)
 Veiligheidsregio Kennemerland (VRK)
 Antworning Ingenieurburo Weber Schutte Kaser partnerschaft (ANT)

COUNTRY

Spain
 Germany
 Spain
 Denmark
 United Kingdom
 The Netherlands
 Germany

ESENet / Emergency Services Europe Network

© Shutterstock



Information

Grant Agreement N°
313013

Total Cost
€704,845.20

EU Contribution
€629,266.98

Starting Date
01/01/2013

Duration
24 months

Coordinator

**INTELLIGENCE FOR
ENVIRONMENT AND
SECURITY – IES SOLU-
TIONS (IES)**

Via Monte Senario, 98
00141 Roma,
Italy

Contact
Uberto DELPRATO
Tel: +39 06 8184832
Mobile: +31 346 6367499
Fax: +39 06 87459009
E-mail: u.delprato@
iessolutions.eu
Website:
www.iessolutions.eu

Project objectives

The ESENet initiative aims at establishing a network of stakeholders in the Emergency Management domain that will identify, discuss and agree on communication needs, requirements, new technologies and best practices in responding to everyday, as well as, major emergencies.

The project aims to achieve the following via public reports:

- » The identification of gaps in the emergency service provision chain and the collection of user requirements; the results of such activity will be a living document that will be made available to all stakeholders;
- » The selection of available and/or promising technologies for tackling the identified challenges and also identifying areas where further research is needed;
- » The analysis of organisational gaps, with suggestions and best practices at EU level about procedures, framework agreements and reorganising suggested tasks; the results of such work will be reported in a public deliverable in the form of a roadmap to improve the Emergency Services throughout Europe;
- » The identification of available standards, gaps in existing standards or areas where standards will be needed in the future.

Description of the work

The project plans to organise a total of 8 web-meetings and 4 workshops during the term of the project. Experts from emergency service authorities, public safety representatives and commercial organisations are invited to attend and contribute to working documents prepared by the project partners on several topics, including interoperability at all levels (from the technical level to the organisational level) and in all types of safety and security missions (daily/ordinary and/or large scale missions as well as local or cross-border missions).

The communication requirements covered by ESENet range from "Citizens to authorities", "Authorities to authorities" and "Authorities to citizens".

Expected results

The main expected results of the coordination activities of ESENet are:

- » An agreed list of user requirements and lesson learnt on all levels of interoperability;
- » A consolidated network of end users, practitioners and industries willing to leverage the quality of Emergency services by identifying area for improvements;
- » A roadmap for a common EU approach to a new set of standards and legal framework accommodating the needs of emergency services.

PARTNERS

Intelligence for Environment and Security – IES Solutions (IES)
European Emergency Number Association (EENA)
Erupsi (ERUPSI)

COUNTRY

Italy
Belgium
Slovakia

ISITEP / Inter System Interoperability for Tetra-TetraPol Networks



Achieving a full Interoperability through the integration of all TETRA and TETRAPOL networks, with new mission procedures and enhanced terminals.

Information

Grant Agreement N°
312484

Total Cost
€15,985,650.87

EU Contribution
€10,292,495.07

Starting Date
01/09/2013

Duration
36 months

Coordinator

SELEX ES (SES)
Institutional Financing EU,
NATO and United Nations
Via Tiburtina km 12,400
00131 - Roma - Italy

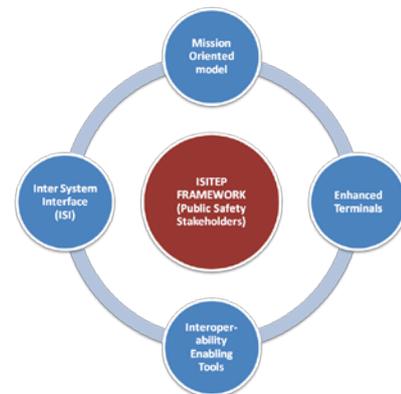
Contact
Paolo DI MICHELE
Tel: +39 06 4150 4850
Mobile: +39 335 7570 556
Fax: +39 06 4458 3088
E-mail: paolo.dimichele@selex-es.com
Website: www.selex-es.com

Project objectives

- » Develop a future-proof pan-European framework for the integration of different Public Protection & Disaster Relief (PPDR) national organizations, merging communications technology, operational procedures and the legal framework
- » Test the provided framework using a number of multi-agency cooperation scenarios, such as cross-border Police hot pursuit, Joint police patrol surveillance operation, joint forces airplane disaster management, and VIP protection through cooperation of national police forces

Description of the work

ISITEP will develop procedures, technology and legal agreements to achieve a cost effective solution for PPDR interoperability.



ISITEP will demonstrate full radio interface capabilities for PPDR resources. ISITEP end users will drive requirements to guarantee legal, operational and technical coherence. In addition, a legal agreement template will be proposed for approval between Norway and Sweden within the project timeframe. Through ISITEP, European end users will utilize enhanced terminals in operations abroad within an agreed framework of procedures. This will improve cooperation among European PPDR resources for the benefit of all citizens. European stakeholders will have an economically sustainable solution for sharing national PPDR services. ISITEP's results will be disseminated by a proper plan utilizing the resources of the Consortium, which includes all the manufacturers of national European networks and the main PPDR stakeholders. Furthermore, through ISITEP technology, the European security industry will have new market opportunities.

Expected results

The project goals will be obtained through the delivery of the ISITEP framework, which will be based on:

» Mission oriented procedures, functional models and legal agreements

» An European network solution integrating all types of European national PPDR networks through a novel InterSystem Interface (ISI) over IP protocol, encompassing:

- ETSI standardized ISI among TETRA national networks
- ISI over IP Gateways among national TETRAPOL networks

- ISI over IP gateways among TETRAPOL - TETRA networks

» Bi-technology terminals based on smartphones/tablets with PPDR applications

» Supporting tools to assess business sustainability, technology needs and improve training

Thanks to increased cooperation achieved through the proposed framework, a better management of migration at European national borders is expected with a reduction of cross border crime activities and a more effective protection of EU citizens. Similar significant improvements are expected in joint disaster relief operations.

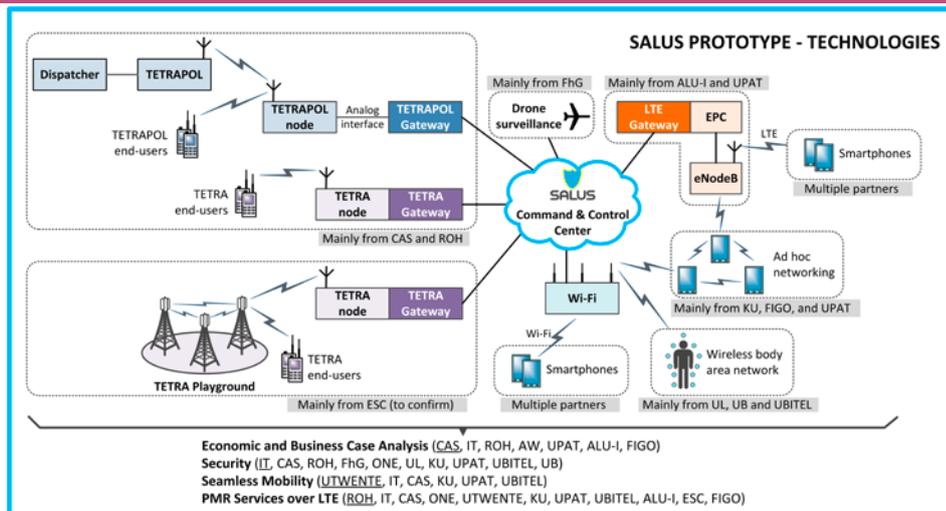
PARTNERS

Selex ES (SES)
 Service Public Federal Interieur (BFP)
 Norwegian Ministry of Justice and Public Safety (DNK)
 Myndigheten for Samhallsskydd och Beredskap (MSB)
 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (V&J)
 Amper Sistemas S.A. (AMP)
 Cassidian Finland OY (CAS FI)
 Cassidian SAS (CAS FR)
 Motorola Solutions Danmark AS
 Istituto Superiore delle Telecomunicazioni e delle Tecnologie dell'Informazione (ISCOM)
 Net Technologies Etaireia Periorismenis Efthynis (NETTECH)
 Università degli Studi Roma Tre (RM3)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Universitat Politecnica de Catalunya (UPC)
 Devoteam Fringes (DVT)

COUNTRY

Italy
 Belgium
 Norway
 Sweden
 Netherlands
 Spain
 Finland
 France
 Denmark
 Italy
 Greece
 Italy
 The Netherlands
 Spain
 Spain

SALUS / Security And Interoperability in Next Generation PPDR CommUnication Infrastructures



IT-Instituto de Telecomunicacoes (PT) | CAS – Cassidian (FR) | ROH – Rohill (NL) | AW – Airwave (UK) | FhG – Fraunhofer IOSB (DE) | ONE – OneSource (PT) | UL – Univ. Ljubljana (SI) | UTWENTE – Univ. Twente (NL) | KU – Kingston University London (UK) | UPAT – Uni Patras (GR) | UBITEL – Ubitel (RUS) | UB – Univ. Belgrade (SRB) | PSCE – Public Safety Communications Europe (BE) | ALU-I – Alcatel Lucent International (FR) | FIGO – FIGO BV (NL)

Information

Grant Agreement N°
313296

Total Cost
€4,768,125.28

EU Contribution
€3,499,829.00

Starting Date
01/09/2013

Duration
36 months

Coordinator

**INSTITUTO DE
TELECOMUNICAÇÕES
(IT)**

Aveiro
Campus Universitário de
Santiago
3810-193
Portugal

Contact
Hugo Marques
Tel: +351 234 377 900
Mobile: +351 917 866 391
Fax: +351 234 377 901
E-mail:
hugo.marques@av.it.pt
Website: www.sec-salus.eu

Project objectives

- » Design, develop and validate the next generation PPDR network concept;
- » Support TETRA and TETRAPOL functionalities on the next generation PPDR network;
- » Provide guidelines towards the medium/long term evolution of the PPDR network;
- » Set out economic implications and possible migration paths for the PPDR network and service evolution;
- » Collect statistical data related to police forces and first responders across Europe;
- » Foresee business cases associated with the evolution of the PPDR network;
- » Contribute towards the standardisation efforts on the next generation PPDR network (including architectural design and spectrum requirements).

Description of the work

SALUS Project aims to develop and prototype the next generation PPDR network and services for public protection and disaster relief. The network will be backward compatible with legacy communication technologies, fully converged with the 4G evolutionary wireless paradigm and supporting robust and reliable transmission of broadband data. This task is supported by network operators and industry, which will provide security, privacy, seamless mobility, Quality of Service (QoS) and reliability support for mission-critical PMR voice and broadband data services.

Expected results

To enable robust, reliable, and secure mobile broadband communication for a wide variety of PPDR applications, including the ability of inter-system, inter-agency and cross-border interoperability.

PARTNERS

European Commission (EC)
 Instituto de Telecomunicacoes (IT)
 Cassidian SAS (CAS)
 Rohill Technologies BV (ROH)
 Airwave Solutions Ltd (AW)
 Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V (FhG)
 One Source Consultoria Informatica Lda (ONE)
 Univerza v Ljubljani (UL)
 Universiteit Twente (UTWENTE)
 Kingston University Higher Education Corporation (KU)
 University of Patras (UPAT)
 Ubitel CO Ltd (UBITEL)
 Elektrotehnicki Fakultet Univerzitet u Beogradu (UB)
 Public Safety Communication Europe Forum AISBL (PSCE)
 Alcatel-Lucent International SAS (ALU-I)
 Pelastusopisto, Emergency Services College (ESC)

COUNTRY

Belgium
 Portugal
 France
 Netherlands
 United Kingdom
 Germany
 Portugal
 Slovenia
 The Netherlands
 United Kingdom
 Greece
 Russian Federation
 Serbia
 Belgium
 France
 Finland

SAVASA / Standards Based Approach to Video Archive Search and Analysis

© Mike Zakharov - Fotolia.com

RESEARCH
COMPLETED

Information

Grant Agreement N°

285621

Total Cost

€4,061,085

EU Contribution

€3,166,266.58

Starting Date

01/12/2011

End Date

31/12/2014

Coordinator

ANGEL IGLESIAS S.A. -**IKUSI**

R&D

Paseo Miramon

20009, San Sebastian

Contact**Gorka Pérez**

Tel: +34 943 44 88 00

Mobile: +34 650 15 69 56

Fax: +34 943 44 88 20

E-mail:

gorka.perez@ikus.com

Website: <http://www.ikus.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 technolo-

gies 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.

Results

At the end of the project, the SAVASA platform has been implemented and has provided a step forward for video surveillance archive exploitation comprising a unified archive integration layer that is capable of making multiple remote or local video archiving systems available to end-users as a logically unified archive. It also provides a common video search and indexing application that builds upon the integration layer which supports multi-modal video search over multiple archives in a distributed manner.

The application of open standards has been a design requirement for moving from a legacy set of proprietary compression, encoding and container formats into an integrated set of open source and open standards tools. A set of enhanced video analytics applications have been deployed that can leverage the common archive integration and search applications to provide operators with tools that are lacking in current systems.

The whole framework provides an absolute guarantee that neither legal nor ethical norms are compromised. The integration of video semantic analysis and annotation permits operators to perform searches across multiple archives based on a generalised hypothesis rather than concrete syntactic concepts. In a few words, the SAVASA project has reached its S&T objectives by focusing on interoperability, open standards, ethical and privacy protection, semantic video analytics and multiple archive integration.

PARTNERS

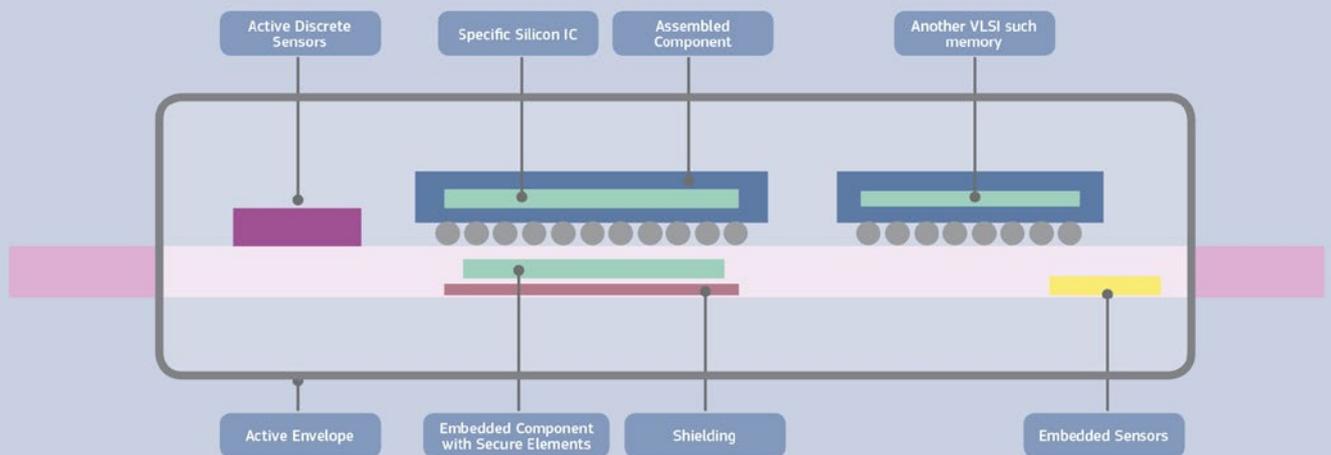
Angel Iglesias S.A.- IKUSI (IKUSI)
 Asociación Centro de Tecnologías de Interacción Visual y Comunicaciones Vicomtech (VICOM)
 Studio Professionale Associato a Baker & McKenzie (BAK)
 HI-Iberia Ingeniería y Proyectos S.L. (HIB)
 Dublin City University (DCU)
 University of Ulster (UU)
 INECO (INECO)
 Demokritos (NCSR)
 Sintel Italia (SINTEL)
 Dirección General de Tráfico – Ministerio del Interior (DGT)
 RENFE Operadora (RENFE)

COUNTRY

Spain
 Spain
 Italy
 Spain
 Ireland
 United Kingdom
 Spain
 Greece
 Italy
 Spain
 Spain

UNSETH / Embedded protection of security systems and anti-tampering technologies

Physical Architecture for Secure Electronic Module



Information

Grant Agreement N°
312701

Total Cost
€6,615,904

EU Contribution
€3,874,033

Starting Date
01/01/2014

Duration
36 months

Coordinator

THALES COMMUNICATIONS & SECURITY SAS (TCS)
HTE - Hardware Technology
Tools & Engineering
4 Avenue des Louvresses
92230 GENNEVILLIERS
FRANCE

Contact
Bernard Candaele
Tel: +33 1 46 13 27 66
Mobile: +33 6 08 65 07 96
Fax: +33 1 46 13 25 55
E-mail: bernard.candaele@thalesgroup.com
thalesgroup.com
Website:
www.thalesgroup.com

Project objectives

Security has become a vital part of European electronic products and equipment as they handle sensitive data in uncontrolled environments and face increasing IPR protection, counterfeiting and cloning issues. New applications combine a challenging set of requirements including low-cost, security and tamper-resistance.

UNSETH aims to complement the available solutions at chip level, by adding new technologies (like tamper detection features and higher tamper resistance) for electronic assembly and packaging and to propose a generic protection profile up to the highest possible assurance level, while meeting the need to protect against high conceivable level of attack.

UNSETH explores and derives the advantages which can be obtained by introducing new nanomaterials printed envelope, embedded 3D devices into electronic printed circuit board assembly and a novel system-in-package with active anti-tamper sensors. These processes will be combined, focusing on both the electronic modules themselves as well as the manufacturing process.

The aim is to set up and qualify European technologies capabilities and to maintain Europe as a worldwide player in the field of secure and safe electronic architectures. Major achievements expected are protection against tampering and counterfeiting, higher security compatible with mass production cost and robust secure protection needed for high end products.

Description of the work

The project seeks to couple case constraints with requirements and combine these with the intrinsic nanomaterial active envelope, embedded die security and tamper resistant SiP. This will serve to obtain cost-effective hardware architectural building blocks that will serve as a basis for prototyping but also as reference when analyzing potential attacks and developing countermeasures to protect against these.

The project proposes to develop state of the art and advanced technologies, i.e. nanoparticle inks by aerosol-jet from Fraunhofer ENAS, embedded components packaging in PCB from AT&S and eWLP and SiP system-in-package assembly from Nanium. Thales brings applications for security with its entity TCS and checks manufacturability of the technologies with TGS. Epoche & Espri is the Security evaluation center and proposes a related Protection Profile.

UNSETH work integrates results from ongoing embedded die technology work in the FP7 HERMES scheme. PCB module containing embedded dies is used and integrated to build UNSETH technology prototype to be assessed with security evaluation.

The project realizes several test vehicles to validate the building blocks for the different technologies, to perform security evaluation of the integrated solution, as well functional verifications and solution manufacturing within the timeframe.

Expected results

The project will validate two complementary technologies:

- » an embedded component in the printed circuit board to form a highly integrated part of the electronic system which can be protected to form a first level of anti-tamper protection;
- » secure active sensor printed on a casing above the electronic module to form a second level of anti-tamper envelope.

The project will perform tests and evaluate the reliability of the assembled boards equipped with the smart envelope.

The project will draw on conclusions from the security testing & evaluation to provide guidance to users and integrators of the UNSETH technology. Finally, the security testing and evaluation protocol will be formatted in a standard form to be shared with the European community.

PARTNERS

Austria Technologie & SystemTechnik Aktiengesellschaft (AT&S)
 Nanium S.A (NAN)
 Fraunhofer-Gesellschaft for Foerderung der Angewandten Forschung E.V. (FhG ENAS)
 Thales Global Services SAS (EPM)
 Epoche and Espri S.L. (EPO)

COUNTRY

Austria
 Portugal
 Germany
 France
 Spain

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

Thales Communications S.A
 Cassidian S.A.S. (EADS DS)
 Astrium Ltd. (EADS-Astrium)
 Budapest University of Technology and Economics
 Eltag Datamat s.p.a.
 Selex Communications S.P.A.
 Telespazio S.P.A.
 Università di Pisa.
 Saab Communications
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Indra Sistemas S.A.
 Rohde & Schwarz gmbh.
 Center for Wireless Communications, University of Oulu
 Prismtech Limited
 Interuniversitair Micro-Electronica Centrum VZW (IMEC)
 European Commission - Joint Research Centre (JRC)
 Ecole Supérieure d'Electricité
 Elektrobit Wireless Communications
 SELEX Sistemi Integrati S.p.A. (SELEX)

COUNTRY

France
 France
 United Kingdom
 Hungary
 Italy
 Italy
 Italy
 Italy
 Sweden
 The Netherlands
 Spain
 Germany
 Finland
 United Kingdom
 Belgium
 Belgium
 France
 Finland
 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.freestic.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

Ardaco, a.s. (ADO)
 National Security Authority of the Slovak Republic (NSA)
 Université du Luxembourg (UL)
 British Association of Public Safety Communication Officers (BAPCO)
 ITTI Ltd. (ITTI)
 NEXTEL S.A. (NEX)
 Centre de Communications du Gouvernement (CCG)
 World Consult, a.s. (WCT)
 Pramacom Prague (PCM)

COUNTRY

Slovak Republic
 Slovak Republic
 Luxembourg
 United Kingdom
 Poland
 Spain
 Luxembourg
 Slovak Republic
 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 inter-networking 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

Universidad del Pais Vasco EHU UPV (UPV/EHU)
 Itelazpi SA (ITEL)
 Grupo Comunicaciones y Sonido SL (CYS)
 University of Plymouth (UoP)
 Viotech Communications SARL (VIO)
 National Center for Scientific Research "DEMOKRITOS" (NCSR-D)
 Cosmote Kinites Tilepikoinonies AE (COS)

COUNTRY

Spain
 Spain
 Spain
 United Kingdom
 France
 Greece
 Greece

HIT-GATE / Heterogeneous Interoperable Transportable GATEway for First-Responders



Information

Grant Agreement N°
284940

Total Cost
€5,052,636.30

EU Contribution
€3,451,257.72

Starting Date
01/02/2012

Duration
30 months

Coordinator

THALES COMMUNICATIONS & SECURITY
Direction Technique
4 avenue des Louvresses
92230 Gennevilliers,
France

Contact
Vania Conan
Tel: +33 1 46 13 35 30
Fax: +33 1 46 13 26 86
E-mail:
Vania.conan@thalesgroup.com

Project objectives

The goal of HIT-GATE is to develop a generic gateway that allows communications across networks currently used by first responders in Europe. Present networks use a large number of different and incompatible technologies therefore compromising efficient coordination of combined operations (such as cross-border or crisis management). Addressing specifically this issue to answer First Responder needs, HIT-GATE will support a mix of technologies used today by organizations involved in Public-Safety, ranging from legacy-PMR, TETRA to next-generation networks. In this way, organizations may keep their existing systems and/or adopt novel technologies, since the proposed HIT-GATE solution is future proof and ensures communications interoperability between the networks (limited, of course, to the limitations in capabilities of each network). HIT-GATE will also enable communications across heterogeneous networks between first responders during operations. By connecting HIT-GATE to their networks, first responders may continue to use their current receiver equipment, communications base-stations and communications infrastructures.

Description of the work

The overall strategy adopted to successfully achieve HIT-GATE objectives and goals is as follows:

1. Implement a coherent management group capable to provide continuous oversight over several of the project areas, including, project coordination (e.g., budget, calendar, scope and risk), quality, scientific accomplishments, end-users participation and exploitation activities. Project Management activities will be aligned with principles and best practices from PMBOK and CMMI.

2. Actively involve of end-users throughout the project phases, with a strong participation in initial phases (definition of user requirements and operational scenarios) and demonstration activities. Active participation of end-users will ensure that HIT-GATE is a valid product and that meets their needs.
3. Adopt known and proven development processes and sub-disciplines (ISO 12207) with enough flexibility to incorporate new know-how and corrections as a result of new discoveries and/or verification activities.
4. Achieve capabilities at early stages of the project. For that, a two-iteration process will be implemented:
 - » a. Iteration 1: stand-alone HIT-GATE capabilities and subset of IP-adaptors (covering TETRA, TETRAPOL and analog-PMR).
 - » b. Iteration 2: networking HIT-GATE capabilities and complete set of IP-adaptors (covering GSM/Cellular and Broadband).
5. Demonstrate actual HIT-GATE capabilities to end-users in a field-simulated scenario. A demonstration, involving FRs and their technology, will be conducted close to the end of the project.

Expected results

HIT-GATE will deliver:

- » The design of a modular architecture of an inter-network Gateway allowing incorporation of both legacy first responder network and future networks
 - » Specifications of open-interfaces and recommendations for standards
 - » A mature prototype of a transportable, rapidly deployable and autonomous Gateway that will be demonstrated to end-users and become a foundation for commercial exploitation
- » The demonstration of cross-network services, including voice and data, required by first responders across heterogeneous networks used at European Level.

PARTNERS

Thales Communications & Security SAS (TCS)
 National Center for Scientific Research "Demokritos" (DEM)
 Center For Security Studies (KEMEA)
 Teletel S.A. – Telecommunications and Information Technology (TELETEL)
 Amper Sistemas, S.A. (AMPER)
 Cluster de Seguridad y Confianza de la Comunidad de Madrid (Cluster Seguridad)
 Edisoft Empresa de serviços e desenvolvimento de software (EDISOFT)
 Rohill Technologies BV (ROHILL)
 ITTI Sp.zo.o. (ITTI)
 Thyia Tehnologije d.o.o (THYIA)
 Rinicom Limited (RINICOM)

COUNTRY

France
 Greece
 Greece
 Greece
 Spain
 Spain
 Portugal
 The Netherlands
 Poland
 Slovenia
 The United Kingdom

PPDR-TC / Public Protection Disaster Relief – Transformation Center



© PPDR-TC

Information

Grant Agreement N°

313015

Total Cost

€3,962,239.68

EU Contribution

€2,890,684.20

Starting Date

01/04/2013

Duration

30 months

Coordinator

EXODUS S.A. (EXO)

Business Development and

Delivery

73-75 Mesogeion Av &

Estias Str 1

115 26 – Athens

Greece

Contact

Dimitris Vassiliadis

Tel: +30 210 7450321

Mobile: +30 6 947566676

Fax: +30 210 7450399

E-mail: dvas@exus.co.ukWebsite : www.exus.co.uk

Project objectives

In order to satisfy the increasing demands of future PPDR communications systems there are certain technical and economic barriers that need to be overcome. There is a need to develop the architecture of future PPDR systems to include solutions that effectively tackle emergency situations at hand, while also coordinating first responders at operational, strategic and tactical levels increase.

One of the basic aims of these systems will be to pave the way for establishing rapidly deployable broadband infrastructure in the field. PPDR systems should include capabilities such as voice, real-time video and localisation of responders, as well as high speed data transfer for dealing with natural and man-provoked disasters. The basic challenge is providing services to the end-user independently of the underlying telecommunication infrastructure.

The major objective of PPDR-TC is to provide the strategic roadmap toward the full migration path of future PPDR system's evolution, which will satisfy the mid and long-term requirements for the next 10-15 years.

In order to cope with this goal PPDR-TC established a modular study approach with the following building blocks:

- » Extensive data gathering from European PPDR organisations to define reference usage scenarios, classify current and future services, while identifying candidate PPDR technologies and architectures.
- » Derive technical recommendation based on validation of the candidate technologies and architectures so as to achieve uniform communication for public safety agencies (broadband, TETRA, TETRAPOL networks, etc.), offering ubiquitous secure communication over dedicated and commercial networks, while establishing seamless connection to other networks (LTE, 3G, WiMAX, etc.).

- » Provide economic recommendations based on validation of the candidate PPDR technologies, according to specific economic factors (NPV, IRR, ROI, etc.) and presenting a cost/benefit analysis to the decision makers.

Description of the work

The overall mission of PPDR-TC consortium is to research, design, validate and recommend a complementary architecture capable of enhancing future PPDR community operations. To accomplish that, PPDR-TC consortium has adopted a specific incremental approach:

1. To build on PPDR-TC foundations that will constitute the elementary information and assumptions for the elaboration of the operational, technical and business analysis framework by:
 - » Defining future PPDR reference usage scenarios
 - » Depicting future requirements in dealing with day to day as well as major event incidents
 - » Identifying services and applications that will meet the PPDR specific requirements
2. To organise and structure the PPDR roadmap guidelines based on the selection of key parameters impacting PPDR market/technologies and on elaboration of plausible scenarios for their future evolutions by:
 - » Classifying future reference services and applications
 - » Providing PPDR market scenarios evolution and prioritise technological selections
3. To technically validate and economically assess the viability of the proposed options for future PPDR systems, architecture and services through:
 - » Simulations according to specific parameters associated with the key technical enablers of the selections (traffic

growth, spectrum requirements, end-to-end delay, jitter, etc)

- » Development of suitable financial tools and provision of cost/benefit analysis based on economic factors and metrics for the financial viability checking of the proposed solution.
- 4. To elaborate a 10-15 years roadmap developing options for evolution path towards full compliance to PPDR requirements in Europe based on the analysis of the technical and economical/costs reports and recommendations by:
 - » Verifying the resulted recommendations with PPDR communities and relevant stakeholders
 - » Promoting the implemented roadmap to the standardization bodies in order to build compliant business models in accordance with the existing standards.

Expected results

PPDR-TC aims at creating a holistic approach which will recommend future systems applied in critical events as well as normal work depending on end-users' requirements. The proposed solution will have few dimensions so it can be tuned by decision-makers to the size of each critical incident taking technical, financial, organisational and business constraints into account. The future PPDR systems will be designed in order to handle sensitive information and increase the level of citizen's security by strengthening cooperation among first responders in emergency situations.

PARTNERS

EXODUS S.A. (EXO)
 Institute of Communication and Computer Systems (ICCS)
 Thales Communications & Security SAS (TCS)
 Rinicom Limited (RINI)
 TELETEL S.A. – Telecommunications and Information Technology (TELE)
 AEGIS Systems Limited (AEGI)
 ITTI Sp.zo.o. (ITTI)
 TEKEVER – Tecnologias De Informacao, S.A. (TEK)
 Universita Degli Studi Di Modena e Reggio Emilia (UNIMORE)
 SC Lithuanian radio & TV centre (LRTC)

COUNTRY

Greece
 Greece
 France
 United Kingdom
 Greece
 United Kingdom
 Poland
 Portugal
 Italy
 Lithuania

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 project developed its "Silentel" client application that communicate only with the server and was designed to support the operation of public safety agencies and other responders on a daily basis and in crisis situations. The system enables flexible management of groups by facilitating phone calls and instant messaging between actors using different devices and located in different countries.

SECRICOM's results manifested themselves in the system's security, quality and ability to work across multiple platforms. The system allows for resilient connectivity through a multi-bearer-router and an extendable, on-site deployable network.

In terms of security, it exploited:

- » state-of-the-art encryption and user authentication software
- » trusted docking station concepts
- » chip-level security and a secure docking module
- » threat and intrusion detectors and monitors

SECRICOM's technology is capable of functioning across multiple platforms through communication servers and gateways that are applicable for a range of modern devices and interoperable with legacy systems. The research team also worked to improve the quality of service by developing

a user-friendly system with a monitoring and control system that was ready for Internet Protocol Version 6.

Three core agent types were identified and implemented:

1. information delivery agents (IDA) to send information from/to data sources
2. user communication agents (UCA) to communicate information with to human users through guided dialog, with most of these done via Silentel's "push-to-talk" devices
3. IP agents (IPA) to monitor and configure network routing devices

The project provided a proof-of-concept solution for crisis management communications and was effectively demonstrated via four live demonstrations.

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

CRISP / Evaluation and certification schemes for security products - Capability Project



Information

Grant Agreement N°
607941

Total Cost
€2,634,214.38

EU Contribution
€2,213,041.26

Starting Date
01/04/2014

Duration
36 months

Coordinator

**STICHTING NEDERLANDS
NORMALISATIE-
INSTITUUT (NEN)**

NEN Environment and
Society

Vlinderweg 6
PO Box 5059
2600 GB - Delft - The
Netherlands

Contact

Ronald Boon
Tel: + 31 15 269 04 12
E-mail: crisp@nen.nl
Website:
<http://crispproject.eu>

Project objectives

The objective of CRISP is to enhance existing security evaluation and certification schemes by offering an innovative evaluation methodology that integrates security, trust, efficiency and freedom infringement assessment dimensions.

The proposed scheme is based on a taxonomy encompassing a variety of security products and services across applications. It will take into account the varying roles of a diverse stakeholder community and engage with each group to gather insights to help avoid acceptance problems that challenge current schemes.

In relation to this overall objective CRISP will:

- » Create a taxonomy of security products and systems, concepts of operations, application areas, performance and set out criteria for comparing security products and systems.
- » Provide a historical perspective on security standards and certification in Europe and analyse the state of the art in security standards, certification and accreditation at the Member State, regional and international level.
- » Identify and determine the role of different stakeholders, gauge their views on the challenges affecting security certification and determine requirements for a harmonised EU-wide approach.
- » Examine the core dimensions (such as security, trust, efficiency, freedom infringement) of security product certification and present the requirements for enhancing existing evaluation and certification schemes.
- » Present a certification methodology, policy and procedures for security products, test-drive, evaluate and refine it.

- » Present a roadmap for adopting the proposed certification scheme and work towards enhancing acceptance of the new certification measures.

Description of the work

In order to assess how existing evaluation and certification schemes could be used and further developed for the certification of security products and services, CRISP follows a tailored strategy.

CRISP will define and classify the EU security products and services market, identify and analyse relevant stakeholders and find best practice models by investigating the state of the art in security certification in across a range of European countries and international countries.

After analysing existing practices, CRISP will develop a multi-dimensional certification scheme to address the gaps in the current certification scenario and the recommendations of the European Commission, particularly the need to include human factors in the evaluation of security products and services. CRISP's basis for a holistic evaluation of security products and services is a model that encompasses as many perspectives as possible in a well-structured and easily comprehensible manner.

At the highest aggregation level, there are four dimensions: Security, Trust, Efficiency and Freedom Infringement (S-T-E-Fi). Within the CRISP concept, each security product type incorporates a specific S-T-E-Fi evaluation scheme that considers the interrelations between the four dimensions. Depending on the product type, each of the infringement dimensions has a different impact on the evaluation result. Depending on the S-T-E-Fi result, the security product or service is approved or rejected.

CRISP incorporates a high level of stakeholder engagement strategy throughout the project.

Expected results

CRISP's key output will be an EU Security Certification Manual, which will leverage the information gleaned from the analysis of existing certification schemes. This certification manual will specify standards and requirements for certification and accreditation of security products. The manual will be targeted at certification and accreditation bodies and inter alia, set out their roles and responsibilities.

Overall, CRISP will help the European security industry maintain its status as a leader in the global security industry. The project will also help Europe progress towards harmonised security certification by determining the requirements for successful evaluation and certification of security products/systems in Europe, developing a methodology and presenting a roadmap to achieve this impact.

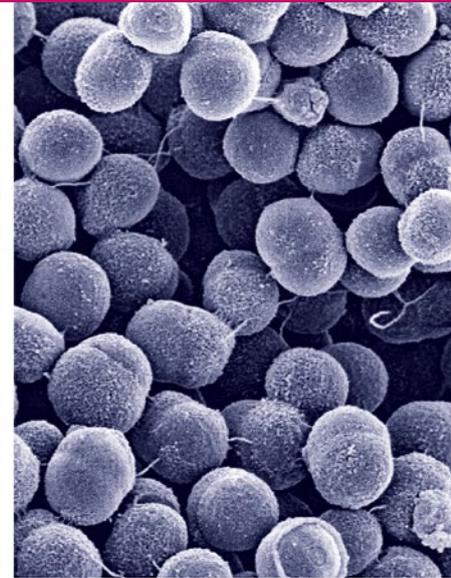
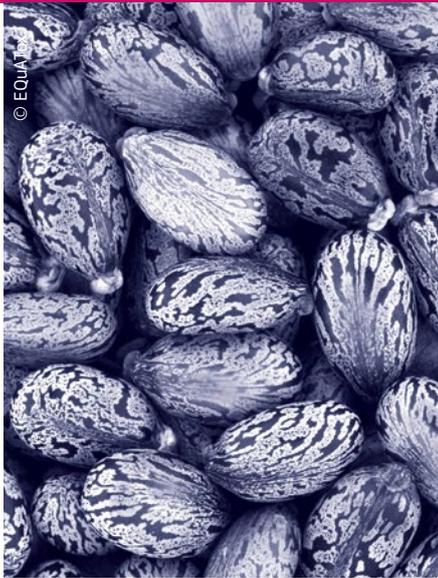
PARTNERS

Stichting Nederlands Normalisatie-Instituut (NEN)
 Trilateral Research & Consulting LLP (TRI)
 Technische Universität Berlin (TUB)
 IRKS Research GmbH (IRKS)
 Vrije Universiteit Brussel (VUB)
 Universitat Jaume I de Castellon (UJI)
 Informacijski Pooblaščenec – Information Commissioner (IP-RS)

COUNTRY

The Netherlands
 United Kingdom
 Germany
 Austria
 Belgium
 Spain
 Slovenia

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

Robert Koch-Institut (RKI)
 European Commission - Joint Research Centre (JRC)
 Institut Scientifique de Santé Publique (WIV-ISP)
 University of Helsinki, Finnish Institute for Verification of the Chemical Weapons Convention, VERIFIN (UH/VERIFIN)
 French agency for food, environmental and occupational health safety (Anses)
 Toxogen GmbH (Toxo)
 Totalförsvarets Forskningsinstitut (FOI)
 Federal Department of Defence, Civil Protection and Sport - SPIEZ LABORATORY (VBS-LS)
 ChemStat (CHS)

COUNTRY

Germany
 Belgium
 Belgium
 Finland
 France
 Germany
 Sweden
 Switzerland
 Switzerland

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@](mailto:Agneta.plamboeck@cbrne.umu.se)[cbrne.umu.se](mailto: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

ANVIL / Analysis of Civil Security Systems in Europe

© Larissa Belova - iStock


**RESEARCH
COMPLETED**
Information
Grant Agreement N°

284678

Total Cost

€2,202,702.60

EU Contribution

€2,009,228

Starting Date

01/03/2012

End Date

28/02/2014

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*

Results

Current European civil security systems are heavily localised, with complex institutional arrangements and varying degrees of centralization. There is a strong use of voluntary organizations in most countries, however, the role of the private sector is limited, with outsourcing of core tasks in crisis management not a major trend. Civil security systems are generally perceived as effective. In terms of efficiency, costs are often dispersed and therefore total national civil security budgets are largely unknown. Despite this uncertainty, a majority of citizens appear to have a positive attitude towards civil security and feel generally safe, though levels of support differ somewhat geographically. There is a well-developed framework for external and cross-border assistance, but it is used only reluctantly by

countries needing help during domestic crises. Looking at national civil security in the EU context, there is a basic acceptance, but low visibility of the EU as a coordinator and facilitator of joint responses to disasters occurring inside or outside Europe. Finally, there is a limited role for regional organizations, which are seen to be weakly institutionalised, have limited competences in crisis and emergency management and depend on often reluctant member states for financial resources and operational capacities. Results from the ANVIL project are appearing in international peer reviewed publications such as the Journal of Risk Research, as well as in a forthcoming book title 'EU civil security governance: Diversity and cooperation in crisis and disaster management' to be published by Palgrave Macmillan.

PARTNERS

Research Management AS (Resman)
 Universiteit Utrecht (Utrecht)
 Ideella Foreningar Utrikespolitiskainstitutet, Informationsavd (UI)
 University of Essex (UEssex)
 Institut za Medunarodne Odnose (IMO)
 Hellenberg Oy (HI)
 Istituto Affari Internazionali (I.A.I.)
 Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)
 Försvarshögskolan, Swedish National Defence College (SNDC)
 Univeristet u Beogradu, Fakultet Bezbednosti (FB)
 Fondation pour la Recherche Strategique (FRS)
 Uniwersytet im. Adama Mickiewicza w Poznaniu (AMU)

COUNTRY

Norway
 Netherlands
 Sweden
 United Kingdom
 Croatia
 Finland
 Italy
 Germany
 Sweden
 Serbia
 France
 Poland

ATHENA



Information

Grant Agreement N°

613220

Total Cost

€5,436,445.04

EU Contribution

€2,631,592.00

Starting Date

01/12/2013

Duration

36 months

Coordinator

POLICE AND CRIME

COMMISSIONER FOR WEST YORKSHIRE (WYP)

West Yorkshire for

Innovation (WyFi)

Laburnum Road

PO Box 9

WF1 3QP – Wakefield

United Kingdom

Contact

Jessica Gibson

Tel: +44 (0) 1924 292207

Mobile:

+44 (0) 7515 573789

E-mail: [jessica.gibson@](mailto:jessica.gibson@westyorkshire.pnn.police.uk)

westyorkshire.pnn.police.uk

Website:

<http://www.westyorkshire.>

[police.uk/athena](http://www.westyorkshire.police.uk/athena)

Project objectives

The public are under-utilised as crisis responders; often first on the scene, and vastly outnumbering emergency responders, they are creative and resourceful.

In a crisis, the public self-organise into groups, adapt quickly, emerge as leaders and experts, and perform countless life-saving actions. Though to do this they are increasingly reliant upon the use of new media. Therefore ATHENA will:

- » help by joining their conversations and adding an enabling voice.
- » give them the information they need, in a way they can understand.
- » assist them in targeting their actions; directing them to the places they need to be and away from danger.
- » identify emergent behaviour that is beneficial, and then provide support with law enforcement agency (LEA) resources to develop that behaviour.

Description of the work

The goal of the ATHENA project is to deliver two major outputs that will enable and encourage users of new media to contribute to the safety of citizens in crisis situations, and in search and rescue actions.

The ATHENA project places considerable importance on the involvement of end-users, and the project will be developed through an iterative process involving close working between technical and end-user partners.

Expected results

» A set of best practice guidelines for LEAs, first responders and citizens for the use of new media, supporting tools and technologies in crisis situations

» A suite of prototype software tools to enhance the ability of LEAs, first responders and citizens in their use of new media in crisis situations

ATHENA will provide the emergency services with new real-time intelligence from crowd-sourced information, assisting in decision making and making search and rescue more efficient.

ATHENA will create a fundamental and permanent shift in the way crisis situations are managed; helping the public become a part of the crisis team.

It will use social media and smart mobile devices as part of a shared and interoperable two-way communication platform. By developing an orchestrated cycle of data, information and knowledge, ATHENA will empower both the public and emergency services with the intelligence they need in dealing with a crisis.

PARTNERS

Police and Crime Commissioner for West Yorkshire (WYP)
 International Organization for Migration (IOM)
 Sheffield Hallam University (SHU)
 Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (FKIE)
 SAS Software Limited (SAS)
 Municipality of Ljubljana (MOL)
 Thales Nederland BV (Thales-NL)
 University Of Virginia (UVA)
 Försvarshögskolan, Swedish National Defence College (SNDC)
 EPAM Systems (Nordic) AB (EPAM)
 Izmir Buyuksehir Belediyesi (IBB)
 Research In Motion Limited (RIM)
 Epidemico Ltd (EMCO)

COUNTRY

United Kingdom
 Belgium
 United Kingdom
 Germany
 United Kingdom
 Slovenia
 Netherlands
 United States
 Sweden
 Sweden
 Turkey
 Canada
 Ireland

COSMIC / The Contribution of Social Media in Crisis Management



Information

Grant Agreement N°

312737

Total Cost

€1,228,896

EU Contribution

€997,040.20

Starting Date

01/04/2013

Duration

24 months

Coordinator

EUROPEAN DYNAMICS ADVANCED SYSTEMS OF TELECOMMUNICATIONS INFORMATICS AND TELEMATICS SA (ED)

Department of Research
and Development
Kifissias 209
15124, Marousi, Greece

Contact

Ioannis Kotsiopoulos

Tel: +30 210 8094500

Fax: +30 210 8094508

E-mail: ioannis.kotsiopoulos@

eurodyn.com

Website:

www.eurodyn.com

Project objectives

The major premise of the COSMIC project is that the experience from recent emergency situations is indicative of a need to instigate collaboration efforts and exchange of ideas and know-how across national borders and among different stakeholders. Extant research on information technology design for emergency purposes indicates that the conventional command and control approach to emergency response, which favours a hierarchical approach to communication structures, should be replaced by one which relies on decentralised structures and prioritises social interactions among different stakeholders. A suitable information technology design should be able to enhance informal interactions in dispersed networks (and localities), while being flexible enough to accommodate situational and locational variation (and make sense of such variation) so as to enhance information sharing. This can result in adding visibility, permanence and sensibility to ephemeral information shared over those dispersed networks.

The project will bridge the gap between different stakeholders with various and sometimes conflicting needs, and will complement existing EC and other international projects by integrating the know-how derived from them and disseminating it to a wide network of interested parties. In particular, the project aspires to:

- » explore new and emerging communication technologies and applications and provide insight into the most effective ways to utilise this media for the safety and security of citizens in crisis situations
- » assist better communication and better information gathering for authorities and first responders
- » examine the potential roles and ethics for citizen participation in emergency response

» produce guidelines to assist authorities and first responders in deploying new and emerging communication technologies and applications for protecting citizens in crisis situations

Description of the work

COSMIC will achieve its objectives via these lines of action:

- » Studies on crises, the main stakeholders (including the public) and the communication technologies they currently use. Emerging technologies will be investigated and stakeholders informed about available innovative forms of communication.
- » Strategic support: COSMIC will analyse the stakeholders in crises and offer ways to achieve sustainable collaboration.
- » Awareness raising and dissemination: COSMIC will communicate progress made and promote its vision for crisis management.

Expected results

COSMIC will highlight the use of citizen-generated data as an indicator of where specific emergency resources or search and rescue operations are necessary. This will assist decision makers, and law enforcement and first responders in using new technology for communication and information gathering. It will also positively influence citizens' preparedness by showing how trusted information can be communicated to the public and, in reverse, how citizens can assist the authorities and one another via own-produced relevant supplementary information.

To this end, the project will offer expert-validated advice and guidelines on how new media technologies and applications can best be used for rapid response to crises. A series of workshops and a final conference will help validate those guidelines and will verify their usefulness and relevance for the various stakeholders.

On a wider perspective, it is expected that the findings of COSMIC will be used to formulate recommendations for other EU projects, governments, and researchers regarding possible new areas of study and research.

PARTNERS

European Dynamics, Advanced Systems of Telecommunications Informatics and Telematics SA (ED)
 Trilateral Research & Consulting LLP (TRI)
 Radboud University Nijmegen – Crisislab (RUN)
 KOC University (KU)
 Elliniki Omada Diasosis Somateio (HRT)
 Public Safety Communication Europe Forum AISBL (PSCE)
 Veiligheidsregio Zuid-Holland Zuid (VZHZ)

COUNTRY

Greece
 United Kingdom
 The Netherlands
 Turkey
 Greece
 Belgium
 The Netherlands

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>.

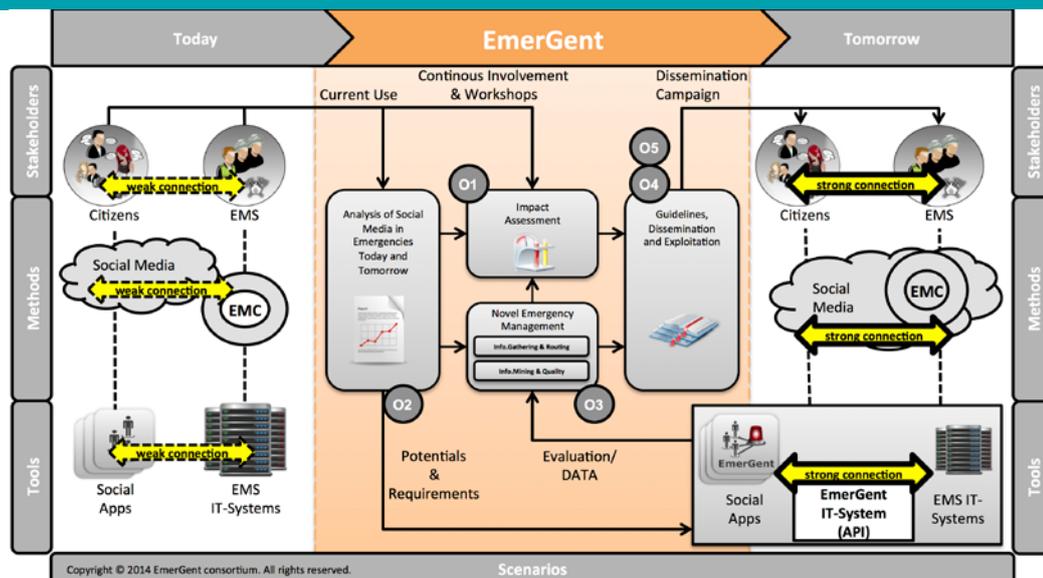
PARTNERS

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Totalförsvarets Forskningsinstitut (FOI)
 University of Kent (UniKent)
 Sogeti Nederland B.V. (Sogeti)
 Temis S.A. (Temis)
 European Commission - Joint Research Centre (JRC)
 WWEDU World Wide Education GmbH (CESS)
 Ministerie van Volksgezondheid, Welzijn en Sport (SCP)
 VLC Projects B.V. (VLC)
 Sigmund Freud Privatuniversitat Wien GmbH (SFP UW)

COUNTRY

The Netherlands
 Sweden
 United Kingdom
 The Netherlands
 France
 Belgium
 Austria
 The Netherlands
 The Netherlands
 Austria

EmerGent / Emergency Management in Social Media Generation



Information

Grant Agreement N°

608352

Total Cost

€4,153,322

EU Contribution

€3,331,184

Starting Date

01/04/2014

Duration

36 months

Coordinator

UNIVERSITY OF PADERBORN (UPB)

COMPUTER APPLICATION
AND INTEGRATION IN
DESIGN AND PLANNING
(C.I.K.)

Pohlweg 47-49

33098 Paderborn, Germany

Contact

Therese Friberg

Tel: +49 (0)5251 60 5474

Mobile:

+49 (0)174 3427984

Fax: +49 (0)5251 60 3206

E-mail: friberg@cikupb.de

Website:

<http://www.fp7-emergent.eu>

Project objectives

Social media is a serious and fast growing phenomenon for creating and maintaining social links. The convergence of social networking and mobile media technology is changing the way people communicate, and access or share information, especially during emergency or crisis situations. Wherever emergencies or crises occur, ad-hoc communities are built through existing social media channels. But these communities are often unconnected or weakly connected to the emergency management services (EMS) and the corresponding emergency management processes.

The overall objective of EmerGent is to understand the positive and negative impacts of social media in emergencies to:

1. enhance objective and perceived safety and security of citizens before, during and after emergencies,
2. strengthen the role of European companies that supply services and products related to EmerGent's results.

Description of the work

Today the "emergency management cycle" (EMC) with its phases does not capture social media with its highly valuable information. Although existing social apps (e. g. for mobile devices) are sometimes used by citizens to share their observations and feelings, these are only weakly connected to existing EMS systems. To achieve the goal of EmerGent the consortium has developed a strong research oriented methodology.

Within the "Analysis of Social Media in Emergencies Today and Tomorrow", EmerGent investigates the current use of

social media during emergencies, and the future potential for citizens and EMS involvement within all phases when using social media. It also performs an analysis of the methods and tools for citizens and EMS to integrate on a technical level.

The results of the analysis are used to assess the impact of social media in emergencies for citizens and EMS through continuous citizen and EMS involvement via social media and workshops. This includes users who will participate over the long-term as well as development of basic infrastructures to maintain and support relationship via social media. The methodology of the impact assessment consists of case studies, analyses of past emergencies where social media played a crucial role, workshops with experts and deep-content analysis of feelings and reactions on both sides.

To handle the vast amount of valuable and distributed information, methods for information mining and information quality are developed to classify and rate the available and provided data from users. Information gathering and information routing, including the development of new social apps, will be done as part of the "Novel Emergency Management". The development of new social apps will obtain and provide visualisations of the most relevant information (as assessed by EmerGent) integrated with several social network providers.

Expected results

All analysis and impact assessment results lead to the creation of guidelines. These guidelines enable EMS and all other involved stakeholders to understand

- » the benefits of social media and
- » its integration into their process on different levels (conceptual & technical).

The insights and results from the studies are incorporated into these guidelines via

- » the collection and presentation of Information,
- » the analysis of social media in emergencies and
- » the development of Information Mining and Information Quality methods,

An IT-system for the “Novel Emergency Management in Social Media Generation” will be developed.

PARTNERS

University of Paderborn (UPB)
 Intelligence for Environment and Security - IES Solutions (IES)
 Oxford Computer Consultants (OCC)
 University of Siegen (USI)
 The Tavistock Institute of Human Relations (TIHR)
 Western Norway Research Institute (WNRI)
 Federation of the European Union Fire Officer Associations (FEU)
 European Emergency Number Association (EENA)
 City of Dortmund, Fire Department, Institute of Fire Service and Rescue Technology (FDDO)
 Centrum Naukowo-Badawcze Ochrony Przeciwpozarowej im. Jozefa Tuliszkowskiego Panstwowy Instytut Badawczy (CNBOP-PIB)

COUNTRY

Germany
 Italy
 United Kingdom
 Germany
 United Kingdom
 Norway
 Luxembourg
 Belgium
 Germany
 Poland

IMPACT Europe / Innovative Method and Procedure to Assess Counter-violent-radicalisation Techniques in Europe



Information

Grant Agreement N°
312235

Total Cost
€3,534,308.74

EU Contribution
€2,801,537.10

Starting Date
01/2014

Duration
42 months

Coordinator

RAND EUROPE (RAND)
Westbrook Centre, Milton
Road
Cambridge, UK CB4 1YG

Contact
Ines von Behr
Tel: +32 2669 2408
E-mail: ivonbehr@rand.org
Website:
<http://impacteurope.eu/>

Project objectives

The key motivation behind IMPACT Europe is to develop an evaluation toolkit to enable evaluators, policy-makers, frontline workers and academics working in the field of violent radicalisation to answer the three questions that limit the effectiveness of their work:

- » How effective are various programmes at tackling violent radicalisation?
- » What are the best practices in tackling violent radicalisation?
- » How does this inform our knowledge and understanding of violent radicalisation?

Description of the work

IMPACT Europe will develop a toolkit to help professionals in the public and voluntary sectors design, implement and evaluate how their programmes (whether policies and interventions) tackle violent radicalisation. The toolkit will also help professionals go beyond the evaluation of a single project by integrating best practices into the design and implementation of future programmes.

Expected results

The IMPACT Europe evaluation toolkit will be composed of four elements:

1. A standardised methodology to provide professionals with a tool to conduct robust evaluations;
2. An evaluation results database to allow professionals to analyse these results over time, identify best practices and develop a more informed understanding of violent radicalisation;
3. A training course (including a train-the-trainer component), to build professionals' capacity to design, carry out and learn from appropriate evaluations;
4. A training manual to provide easy reference for professionals using the toolkit.

PARTNERS

RAND Europe (RAND)
 Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek (TNO)
 Fondation pour la Recherche Stratégique (FRS)
 Studio CEVAS (CEVAS)
 ITTI (ITTI)
 University of Milan Bicocca (UNIMIB)
 Hogeschool Utrecht (HU)
 Verwey-Jonker Instituut (VJI)
 Intelligence in Science (ISC)
 International Security and Counter-terrorism Academy (ISCA)
 Nationale Politie (DNP)
 Radical Middle Way (RMW)

COUNTRY

United Kingdom
 The Netherlands
 France
 Italy
 Poland
 Italy
 The Netherlands
 The Netherlands
 Belgium
 Israel
 The Netherlands
 United Kingdom

iSAR+ / Online and Mobile Communications for Crisis Response and Search and Rescue



Information

Grant Agreement N°

312850

Total Cost

€5,225,062

EU Contribution

€3,987,991.65

Starting Date

01/01/2013

Duration

30 months

Coordinator

TEKEVER - TECNOLOGIAS DE INFORMACAO, S.A. (TEKEVER)

Rua das Musas 3.30

1990-113 Lisboa

Portugal

Contact

Pedro Sinogas

Tel: +351 213 304 300

Mobile: +351 213 304 300

Fax: +351 213 304 301

E-mail: pedro.sinogas@tekever.com

Website: isar.i112.eu

Project objectives

Citizens can function as the “in-situ first sensors” now that they are empowered by new communication media such as mobile phones with cameras and internet-based applications that connect to social media platforms. However their added-value involvement in crisis response efforts is often disregarded by PPDRs when they are developing situational awareness during emergencies.

The iSAR+ project aims to research and develop guidelines and an associated platform that, in emergencies or crises, enables citizens using new mobile and online technologies to actively participate in the response effort. This could be done through bi-directional provision, dissemination, or sharing and retrieval of information essential for critical PPDR intervention, in disaster relief scenarios.

In particular, iSAR+ aims to achieve the following objectives:

- » Develop effective guidelines to enable the new media users to contribute to crisis response efforts and search and rescue actions;
- » Recommend the most effective and efficient ways for citizens to contribute to crisis response and search and rescue actions;
- » Design iSAR+ to suit PPDR organisations;
- » Design iSAR+ to suit citizens;
- » Design iSAR+ accordingly to the EU ethical and legal framework;
- » Design an innovative iSAR+ technological platform for experimentation and validation purposes, which gets the most out of mobile technology and social media;

» Define a stepwise process for the adoption of online social media and mobile technologies in PPDR organisations;

» Integrate iSAR+ in the existing PPDR toolkit for crises;

» Establish a wide European community of end-users, interested in researching the challenges of using social media for supporting disaster relief operations.

Description of the work

In order to address the project objectives iSAR+ reached the conclusion that the answer is not solely technological. Useful technology is already available; the real problem is mostly related to the question of how to use existing technology so that PPDRs and citizens may mutually trust the channels of bi-directional social media communication.

Therefore the iSAR+ approach, code named the THEO approach, is based on a multi-dimensional analysis that encompasses the technological, human, ethical, legal, and the organisational perspectives of the problem. In iSAR+ each THEO dimension is assigned a work package to thoroughly study the project's challenges under its respective perspective.

The THEO work packages are executed concurrently and the results are merged to form one unified vision. This process is repeated through several iterations. At the end of each iteration, the iSAR+ end user community meets at showcases and workshops, to review the achieved results. The end-user feedback will then be incorporated into the next iteration of the project, thus promoting the establishment of an end-user driven solution by the time the final project iteration is achieved.

Expected results

The iSAR+ project will aim for three major results, as follows:

1. A set of guidelines that incorporate findings and recommendations from the organisational (e.g., governance, structure, processes and roles), the human (e.g., human behaviour and cognitive performance during crises), the ethical and legal (e.g., consideration of EU privacy rights concerns and legal framework, often disregarded by popular social media) and the technological (e.g., ICT for crisis) dimensions.
2. A technological platform that integrates the best technology available in order to deliver a set of services that, by design, are compliant with the iSAR+ guidelines;
3. A roadmap to assist PPDRs and citizens on the adoption process of the guidelines established in this project.

PARTNERS

Tekever - Tecnologias de Informação, S.A. (TEKEVER)
 Bridge 129 Spa - Safety and Security (BRIDGE129)
 Centre for Science, Society and Citizenship (CSSC)
 Deveryware (DEV)
 Pelastusopisto, Emergency Services College (ESC)
 Ernst-Moritz-Arndt-Universität Greifswald (EMAUG)
 ITTI Sp.zo.o. (ITTI)
 Helse Bergen Hf*Haukeland University Hospital (HUS)
 Kuopion Kaupunki (PSPELA)
 Police and Crime Commissioner for North Yorkshire (PCCNY)
 Pole Pilote De Securite Locale (PSSL)
 Poliisiammattikorkeakoulu (POLAMK)
 The Provost, Fellows, Foundation Scholars & The Other Members Of Board
 Of The College Of The Holy & Undivided Trinity Of Queen Elizabeth Near Dublin (TCD)
 Thales Communications & Security SAS (THALES)
 Itä-Suomen Yliopisto (UEF)
 Zanasi Alessandro Srl (ZANASI)

COUNTRY

Portugal
 Italy
 Italy
 France
 Finland
 Germany
 Poland
 Norway
 Finland
 Unit Kingdom
 France
 Finland

 Ireland
 France
 Finland
 Italy

PARIS / PrivAcY pReserving Infrastructure for Surveillance



Information

Grant Agreement N°

312504

Total Cost

€4,771,052

EU Contribution

€3,490,491

Starting Date

01/01/2013

Duration

36 months

Project objectives

PARIS will define and demonstrate a methodological approach for the development of surveillance infrastructure which enforces the right of citizens to privacy, justice, and freedom. It will take into account the evolving nature of such rights such as aspects that are acceptable today but might not be in the future, as well as the social and ethical nature of those rights, e.g. the variation of the perception of rights in different countries.

Description of the work

The methodological approach will be based on two pillars: 1) a theoretical framework for balancing surveillance with the protection of privacy and data which fully integrates the concept of accountability, and 2) an associated process for the design of surveillance systems which takes into account privacy and accountability from the start, i.e. privacy-by-design and accountability-by-design.

Coordinator

TRIALOG

25 rue du Général Foy

75008 Paris, France

Contact
Antonio Kung

Tel: +33 1 44 70 61 00

Fax: +33 1 44 70 05 91

E-mail:

antonio.kung@trialog.com

Website:

<http://www.paris-project.org>

Expected results

First a generic framework will be defined for SALT: Socio-ethical/Legal/Technological aspects. Based on the SALT framework, guidelines will be provided to define specialized conceptual frameworks, e.g. for a given country. Examples of SALT frameworks will be provided. The interplay of SALT frameworks and the exchange of surveillance data will be analysed.

A framework management tool will be developed in order to 1) allow for the creation and editing of a conceptual framework, and 2) subsequently act as a reference for surveillance system designers. A SALT compliant design process will be defined so that the balance of surveillance and privacy according to the specialised framework will be ensured throughout the process.

Two use cases will be demonstrated, one based on video search technology which focuses on archived data, and the other based on biometrics technology which focuses on embedded systems sensor data. The two use cases will use different SALT frameworks. The resulting methodology will be promoted through associations and standardisation bodies.

PARTNERS

Trialog
 Austrian Institute of Technology GmbH (AIT)
 Institut National de Recherche en Informatique et en Automatique (INRIA)
 Katholieke Universiteit Leuven (KUL)
 Universidad de Malaga (UMA)
 Université de Namur
 Thales Communications & Security SA
 Visual Tools SA

COUNTRY

France
 Austria
 France
 Belgium
 Spain
 Belgium
 France
 Spain

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

Compagnie Européenne d'Intelligence Stratégique (CEIS)
 Hawk Associates Limited (HAWK)
 Thales SA (THALES)
 Atos Spain SA (ATOS)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 ISEA Psy (ISEA)
 EUROSINT Forum (EUROSINT)
 Zanasi Alessandro (ZANASI)
 University Konstanz (UKON)
 Technische Universität Graz (TUG)

COUNTRY

France
 United Kingdom
 France
 Spain
 France
 France
 Belgium
 Italy
 Germany
 Austria

SAFIRE / Scientific Approach to Finding Indicators for & Responses to Radicalisation

© SAFIRE

RESEARCH
COMPLETED

Information

Grant Agreement N°

241744

Total Cost

€3,681,260

EU Contribution

€2,906,600.95

Starting Date

01/06/2010

End Date

30/11/2013

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.nlWebsite: [http://www.safire-
project.eu](http://www.safire-project.eu)**Project objectives**

The key in democratic societies is to ensure citizens' rights to free thought – even radical thought – while protecting society from the fallout of illegal actions from violent radicalised groups and individuals. Successfully achieving this goal depends on understanding the phenomenon of radicalisation, from its roots in thought and discourse to the stage where individuals go beyond it and engage in violent and illegal behaviour in the name of their cause.

SAFIRE is an EU project started in June 2010 to explore this interesting and sensitive topic. The scope of SAFIRE primarily involves groups and individuals on the extreme and violent end of the radicalisation spectrum. However, in order to understand them and their motives, we also need to step back and understand what happened before they turned to a more violent version of their philosophy.

Description of the work

In this project, we focus on two innovations in this field of research:

- » Developing a non-linear model of the radicalisation process based on typologies of radical groups, cultural aspects of radicalisation, observable indicators of radicalisation, interventions designed to reverse, halt or prevent the radicalisation process.
- » The collection of qualitative and quantitative empirical data to test hypotheses about radicalisation and principles of effective interventions.

Results

We developed and carried out the SAFIRE research with the explicit application to policy and field in mind. Some relevant practical results are:

- » Intervening in the pre-violent stage of radicalisation is not supported by all EU Member States
- » Various cultural factors seem to make a society more or less susceptible to radicalisation
- » Part of the challenge of dealing with violent radicalisation is separating the wheat from the chaff
- » Different types of radicalised groups have different characteristics and, as such, require a different approach to deal effectively with the threat of violence they pose to society
- » The Internet is an increasingly important environment for individuals on the way towards radicalisation
- » Indicators of radicalisation cannot be sought in unchanging behaviour or in any one individual behaviour
- » Most successful interventions designed to prevent violent radicalisation tend to focus on psychological factors, such as self-esteem, dealing with negative emotions, and reducing feelings of injustice

PARTNERS

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Stichting Forum, Instituut voor Multiculturele Ontwikkeling (FORUM)
International Security and Counter-Terrorism Academy (ISCA)
Rand Europe Cambridge Ltd (RAND)
Stichting Hogeschool Utrecht (Hogeschool Utrecht)
Bridge 129 Spa Safety and Security (Bridge)
Compagnie européenne d'intelligence stratégique SA (CEIS)
Universidade de Coimbra (UC)
Fondation pour la recherche stratégique (FRS)
Universiteit van Amsterdam (UvA)

COUNTRY

The Netherlands
The Netherlands
Israel
United Kingdom
The Netherlands
Italy
France
Portugal
France
The Netherlands

SLANDAIL / Security System for language and image analysis



Information

Grant Agreement N°

607691

Total Cost

€3,844,488.80

EU Contribution

€2,942,445.00

Starting Date

01/04/2014

Duration

36 months

Coordinator

THE PROVOST, FELLOWS, FOUNDATION SCHOLARS & THE OTHER MEMBERS OF BOARD OF THE COLLEGE OF THE HOLY & UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN (TCD)

Department of Computer
Science

O'Reilly Institute, Trinity

College

Dublin 2- Ireland

Contact

Prof. Khurshid Ahmad

Tel: +353 (0)1 896 8429

Mobile:

+353 (0)87 9757669

Fax: +353 (0)1 677 2204

E-mail: kahmad@scss.tcd.ie

Website: www.cs.tcd.ie/

khurshid.ahmad

Project objectives

SLANDAIL has three key objectives:

- » Collate and review the sharing and dissemination of disaster zone information amongst experts tasked with improving the security of citizens and property;
- » Create protocols to protect the rights of the citizens and to manage the confidentiality of the collected data and processed information relating to individual citizens;
- » Build and test a prototype system for collecting, processing, aggregating and disseminating information for disaster emergency management.

Description of the work

The project will begin with a comprehensive specification and analysis of end-user needs. Relevant disaster case studies will be identified, the existing use of social media in disaster management will be evaluated, the technology systems used by civil protection agencies will be reviewed and the compliance protocols for data protection used by such agencies will be examined.

The ethical and factual provenance of data and information will be ensured through examining the societal impact of social media in security contexts.

The project will then develop methods and ontologies for extraction and analysis of multilingual textual and speech data and images from social media. Software systems for text and image analytics will subsequently be evaluated and integrated to produce a final demonstrator. The performance and communicability of this system will be tested and evaluated.

Expected results

The main research output of SLANDAIL will be the specification and a prototype of an emergency management system that takes its feeds from emergency operatives, social media feeds and formal media feeds. The system will be multi-modal (encompassing text, speech and image analytics), multi-lingual and capable of aggregation. It will moreover have a novel self-learning component that will update the emergency management systems knowledge base through the life cycle of a disaster.

PARTNERS

The Provost, Fellow, Foundation Scholars and the Other Members of Board of the College of the Holy & Undivided Trinity of Queen Elizabeth near Dublin (TCD)
 Institut for Angewandte Informatik e.V. (INFAI)
 University of Ulster (Ulster)
 Universita Degli Studi di Padova (UNIPD)
 CID GmbH (CID)
 Stillwater Communications Limited(Stillwater)
 Centre for Irish and European Security Limited (CIES)
 Police Service of Northern Ireland (PSNI)
 Datapiano SRL (DataPiano)
 Bundesministerium der Verteidigung (BLS)
 Pintail Ltd (PT)
 An Garda Siochana

COUNTRY

Ireland
 Germany
 United Kingdom
 Italy
 Germany
 Ireland
 Ireland
 United Kingdom
 Italy
 Germany
 Ireland
 Ireland

SUPER / Social sensors for security Assessments and Proactive Emergencies management



Information

Grant Agreement N°
606853

Total Cost
€4,252,770.40

EU Contribution
€3,117,318.00

Starting Date
01/04/2014

Duration
36 months

Coordinator

VITROCISSET S.P.A.
(VITRO)
Business Unit Homeland
Security
Via Tiburtina
1020
00156 – Rome - Italy

Contact
Marco Cosentino
Tel: +39 06 8820 4316
Fax: +39 06 8820 6189
E-mail:
m.cosentino@vitrociset.it
Website: www.vitrociset.it

Project objectives

The main goal of the SUPER project is to research and implement a holistic integrated approach to using social media in emergencies and security incidents. This will operate at multiple time-scales while providing several security and emergency management functionalities. The SUPER approach will exploit social media information to assess citizens' behaviours and attitude before, during and after security or emergency incidents. This information will be integrated into tools serving both the strategic and the tactical level of security/emergency management, thus facilitating security operators and civil protection officers in a variety of tasks. These include: intelligence gathering and strategic planning, real-time management of security operations, generation of a common operational picture (COP) and other tasks. SUPER's technologies will be validated in two distinct scenarios, one dealing with emergency management during (natural or man-made) disasters and the other with police services.

Description of the work

The SUPER consortium has devised a 36-month work plan for its objectives. This is organized into nine major work areas. The work areas can be clustered into three categories:

1. Horizontal work packages spanning the whole duration of the project which are pertinent to all activities of SUPER.
2. Technological development work packages, dealing with the project's core of research and technology development (RTD) areas such as algorithms and techniques for social media analysis and development of a modular plug-n'-play architecture for SUPER's framework.
3. Integration, validation, testing and evaluation activities whose main goal is to enable an early launch of the project's integration and applications developments by remedying potential problems.

Expected results

The main outcome of the SUPER research (i.e. behavioural analysis algorithms) will be integrated into security and emergency management applications. Its research will be used to drive implementation of the next-generation emergency management and crisis management tools.

PARTNERS

Vitrociset S.p.A. (VITRO)
 University of Glasgow (GLA)
 Institute of Communication and Computer Systems/National Technical University of Athens (ICCS/NTUA)
 Sensing & Control Systems S.L. (S&C)
 Civil Protection Service of Campania Region (Regione Campania)
 Fundació Barcelona Media -Yahoo! Research (BM-Yahoo!)
 SENSAP Swiss AG (SENSAP)
 IN2 Search interfaces development ltd (IN2)
 Inspectoratul General al Politiei Romane (IGPR)

COUNTRY

Italy
 United Kingdom
 Greece
 Spain
 Italy
 Spain
 Switzerland
 United Kingdom
 Romania

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 SURVEILLE 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 DETECTOR – 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

EUROPEAN UNIVERSITY INSTITUTE (EUI)
 UNIVERSITY OF BIRMINGHAM (UOB)
 RAOUL WALLENBERG INSTITUTE OF HUMAN RIGHTS AND HUMANITARIAN LAW (RWI)
 TECHNISCHE UNIVERSITEIT DELFT (TU DELFT)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IOSB)
 UNIVERSITE LIBRE DE BRUXELLES (ULB)
 FORUM EUROPEEN POUR LA SECURITE URBAINE (EFUS)
 MERSEYSIDE POLICE AUTHORITY (MERPOL)
 ALBERT-LUDWIGS-UNIVERSITAET FREIBURG (ALU-FR)

COUNTRY

Italy
 United Kingdom
 Sweden
 The Netherlands
 Germany
 Belgium
 France
 United Kingdom
 Germany

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

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

ANOVA IT CONSULTING, SL
 KINGSTON UNIVERSITY HIGHER EDUCATION CORPORATION
 POLITECHNIKA GDANSKA
 LANCASTER UNIVERSITY
 AVANZIT TECNOLOGIA, S.L.
 HEWLETT PACKARD ITALIANA SRL
 SOCIETA PER AZIONI ESERCIZI AEROPORTUALI SEA SPA
 Renfe Operadora
 THE PROVOST FELLOWS & SCHOLARS OF THE COLLEGE OF THE HOLY
 AND UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN

COUNTRY

Spain
 United Kingdom
 Poland
 United Kingdom
 Spain
 Italy
 Italy
 Spain
 Ireland

ALTERNATIVE /

Developing alternative understandings of security and justice through restorative justice approaches in intercultural settings within democratic societies

© eva serrabusa - istockphoto.com



Information

Grant Agreement N°

285368

Total Cost

€4,354,777.60

EU Contribution

€3,423,262

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

www.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

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)
Rendőrtisztví Főiskola (RTF)
Bundesministerium für Inneres (SIK)
Verein für Rechts- und Kriminalsoziologie (IRKS)
European Research Services GmbH (ERS)

COUNTRY

Germany
Hungary
Austria
Austria
Germany

DETECTOR /

Detection technologies, ethics, human rights and terrorism

© V. Yakobchuk - Fotofia.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.detector.bham.ac.uk**Project objectives**

The overall objective of DETECTOR 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.

DETECTOR 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

DETECTOR 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 DETECTOR'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

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

International Peace Research Institute
Ericsson Security Systems
Centre d'études sur les conflits
Vrije Universiteit Brussel
Vrije Universiteit Amsterdam
Centre for Security Studies, Collegium Civitas
Centro de Investigación de Relaciones Internacionales y Desarrollo
Bilkent University
Centre for European Policy Studies

COUNTRY

Norway
Norway
France
Belgium
The Netherlands
Poland
Spain
Turkey
Belgium

PACT / Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action



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

VITAMIB SAS (VITAMIB)
 ATOS SPAIN SA (ATOS)
 CENTRE FOR IRISH AND EUROPEAN SECURITY LIMITED (CIES)
 MARKET & OPINION RESEARCH INTERNATIONAL LIMITED (IPSOS MORI)
 CENTER FOR SECURITY STUDIES (KEMEA)
 MINISTRY OF PUBLIC SECURITY (MOPSI/IP)
 NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" (NCSR Demokritos)
 RAND EUROPE CAMBRIDGE LTD (RAND)
 INSTITUTT FOR FREDSFORSKNING STIFTELSE (PRIO)
 UPPSALA UNIVERSITET (UU)
 CENTRE FOR SCIENCE, SOCIETY AND CITIZENSHIP (CSSC)

COUNTRY

France
 Spain
 Ireland
 United Kingdom
 Greece
 Israel
 Greece
 United Kingdom
 Norway
 Sweden
 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

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ISI)
 Trilateral Research and Consulting LLP (Trilateral)
 Vrije Universiteit Brussel, Research Group on Law, Science, Technology and Society (VUB-LSTS)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 The University of Edinburgh (UEdin)
 Eötvös Károly Public Policy Institute (EKINT)
 Zuyd University of Applied Sciences (Zuyd)
 Market & Opinion Research International Ltd. (Ipsos MORI)

COUNTRY

Germany
 United Kingdom
 Belgium
 The Netherlands
 United Kingdom
 Hungary
 The Netherlands
 United Kingdom

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

SMART / Scalable Measures for Automated Recognition Technologies



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

University of Central Lancashire (CLICT)
 University of Malta (UoM)
 University of Ljubljana (UL)
 Laboratorio di Scienze della Cittadinanza (LSC)
 Babeş-Bolyai University of Cluj-Napoca (BBU)
 Universitetet i Oslo (UiO)
 Universidad de Leon (ULE)
 Law and Internet Foundation (LIF)
 Masarykova univerzita (MU)
 Edith Cowan University (ECU)
 Georg-August-Universitaet Goettingen Stiftung Oeffentlichen Rechts (UGOE)
 Sheffield University (SHEFU)
 Gottfried Wilhelm Leibniz Universität Hannover (LUH)
 CNR National Research Council (CNR)
 Univerzita Komenskeho v Bratislave (FMUNIBA)
 Rijksuniversiteit Groningen (RuG)
 University of Vienna (UNIVIE)
 Morpho (MPH)
 International Criminal Police Organization - I.C.P.O. (INTERPOL)
 Metropolitan Police Service (MET)

COUNTRY

United Kingdom
 Malta
 Slovenia
 Italy
 Romania
 Norway
 Spain
 Bulgaria
 Czech Republic
 Australia
 Germany
 United Kingdom
 Germany
 Italy
 Slovakia
 The Netherlands
 Austria
 France
 France
 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



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

Oesterreichische Akademie der Wissenschaften (OEAW)
 Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)
 Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC)
 Teknologiradet - The Danish Board of Technology (DBT)
 European University Institute (EUI)
 VEREIN FÜR RECHTS-UND KRIMINALSOZIOLOGIE (IRKS)
 Medián Opinion and Market Research Ltd. (Median)
 Teknologiradet - Norwegian Board of Technology (NBT)
 The Open University (OU)
 Akademien der Wissenschaften Schweiz Verein (TA-Swiss)
 Unabhaengiges Landeszentrum fuer Datenschutz (ULD)

COUNTRY

Austria
 Spain
 Spain
 Denmark
 Italy
 Austria
 Hungary
 Norway
 United Kingdom
 Switzerland
 Germany

ASSERT / Assessing Security Research: Tools and Methodologies to measure societal impact

© istockphoto.com



Information

Grant Agreement N°

313062

Total Cost

€553,420.40

EU Contribution

€498,600.74

Starting Date

01/05/2013

Duration

15 months

Coordinator

INSTITUTE FOR THE SOCIOLOGY OF LAW AND CRIMINOLOGY / INSTITUT FÜR RECHTS UND KRIMINALSOZIOLOGIE (IRKS)

Scientific Director: PD Dr.

Reinhard Kreissl

Museumstraße 5/12

1070 – Vienna - Austria

Contact

PD Dr. Reinhard Kreissl

Tel: +43 1 526 15 16

Fax: +43 1 526 15 16 10

E-mail: office@irks.atWebsite: <http://www.irks.at>

Project objectives

The need to consider the societal impact of EU security research has been acknowledged on many occasions by different actors. However, in traditional thinking, societal impacts are reduced to side effects of instrumental (technological and legal) security measures. This binary thinking has to be overcome.

ASSERT will demonstrate that societal dimensions of security research can increase the variety pool of feasible solutions if taken into account from the very beginning of the “design process”.

Identifying and building on the state of the art in societal security research we will identify best practice cases, exploring and assessing societal impacts of science and technology in the security domain and beyond. This will be done in a multidisciplinary fashion from different perspectives, including end-users, stakeholders, researchers, evaluators, policy-makers, civil society and NGOs. Bringing together these different perspectives in a series of workshops will create the basis for the development of a tool and a strategy for the sustainable implementation of societal impacts in future EU security research activities.

Description of the work

- » Build a typology of the different ways that societal impact of security research is being assessed in security research programmes across the globe
- » Analyse good practices of the exploration and assessment of the societal impact of broader areas of science and technology
- » Assess the extent to which these good practices are feasible and useful to security technology research
- » Provide a user friendly knowledge base (online tool and database) to assist the European Commission in implementing the recommendations of ASSERT and other relevant research on assessing the societal impacts of security research
- » Develop an online assessment tool for determining societal impact
- » Organise a series of thematic workshops to engage with experts and stakeholders
- » Organise a “Master Class” for security research evaluators to discuss ASSERT results
- » Broad engagement with experts and stakeholders along clearly identified intervention points through tailored dissemination strategies

Expected results

- » Overview of good practices of the exploration and assessment of societal impact of broader areas of science and technology
- » A database of experts and evaluators (full data protection compliance)
- » Clear recommendations for mainstreaming security impact assessment tools and methodologies in security research
- » A ready-for-use security research online impact assessment tool (SERIA)

PARTNERS

Institut für Rechts- und Kriminalsoziologie / Institute for the Sociology of Law and Criminology (IRKS)
 Technical University Berlin (TUB)
 Trilateral Research & Consulting LLP (TRI)
 King's College London (KCL)
 The University of Stirling (STIR)
 Hamburg-Consult Gesellschaft fuer Verkehrsberatung m.b.H. (HC)

COUNTRY

Austria
 Germany
 United Kingdom
 United Kingdom
 United Kingdom
 Germany

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: [gjacob@rsm.nl](mailto: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

Erasmus Universiteit Rotterdam
 University of Utrecht
 Police Academy, Apeldoorn
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Police Academy, Brandenburg
 University of Durham
 Sheffield University
 University of Antwerp
 CNRS, Paris
 Capgemini Telecom Media defence
 University St. Kliment Ohridski, Skopje

Masaryk University, Brno
 Formit, Rome
 Babes-Bolyai University, Cluj
 Esade Business School, Barcelona

COUNTRY

The Netherlands
 The Netherlands
 The Netherlands
 Germany
 Germany
 United Kingdom
 United Kingdom
 Belgium
 France
 France
 Republic
 of Macedonia
 Czech Republic
 Italy
 Romania
 Spain

DESSI / Decision Support on Security Investments

© Jesus Conde - istockphoto.com


**RESEARCH
COMPLETED**
Information
Grant Agreement N°

261718

Total Cost

€1,902,303

EU Contribution

€1,561,095

Starting Date

01/01/2011

End Date

30/06/2013

Coordinator
**DANISH BOARD
OF TECHNOLOGY**

Toldbodgade 12

DK-1253 Copenhagen

Denmark

Contact
Ida Leisner

Tel: +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 to support decision-makers in situations where different possible solutions for a perceived security-problem are available. It will enable comparison and evaluation of different security investments and serve as a way to achieve transparency of the security decisions.

Description of the work

There is an urgent need for a political framework whose underlying decisions on security investment are transparent and participatory, and which 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 threats and their consequences, probability and impact (i.e., who is affected). Security investment implies choosing between different approaches to increasing security, and DESSI makes this choice explicit by describing and evaluating each security investment alongside its alternatives.

The DESSI tool will ensure decision-making process is explicit. The alternatives are identified or developed in a participatory process, including experts and stakeholders, who are informed by the threat description. Security investments can be highly controversial and disputed. This is not only because of political differences between actors but also due to societal phenomena (threat perceptions, technology insights, belief in alternative investments, etc.) which differently distributed and valued across all the actors. Accordingly, a rigorous investment assessment method needs to make use of a participatory approach which ensures this range of actors is taken on board.

Expected results

The DESSI project has created a novel procedure and a web-based decision support system to decision makers and users of security investments. The procedure and the decision support system (DSS) have been tested within the project and on several occasions afterwards. The consortium continues to develop the (DSS) and collaborate to further its use and development.

The DSS give stakeholders and decision makers insight into the pros and cons of specific security problems and investments. It contributes to a transparent and participatory decision making that accounts for the context and multi-dimensionality of society. As an

additional feature not envisioned in the beginning of the project the DESSI procedure also prove to be an good method for user driven, open innovation, as participants are assisted in creating alternative strategies to address the security problems. It continues to be a useful procedure for public authorities, developers of security solutions, commercial enterprises and social organizations that have used the DESSI tool to make their own comprehensive assessment as an input to internal, strategic discussions and public debate.

PARTNERS

Teknologiraadet - Danish Board of Technology (DBT)
 Peace Research Institute, Oslo (PRIO)
 Teknologiraadet – Norwegian Board of Technology (NBT)
 Verein für sozialwissenschaftliche Forschung und Beratung e.V. (SWFB)
 Austrian Academy of Sciences, Institute of Technology Assessment (ITA)

COUNTRY

Denmark
 Norway
 Norway
 Germany
 Austria

ePOOLICE / early Pursuit against Organized crime using enviroNmental scanning, the Law and IntelligenCE systems

© Thinkstock



Information

Grant Agreement N°

312651

Total Cost

€5,295,925.74

EU Contribution

€3,493,810

Starting Date

01/01/2013

Duration

36 months

Project objectives

The project aims at developing an efficient and effective environmental scanning system as part of an early warning system for the detection of emerging organised crime (OC) threats. The purpose is to improve LEA's situation in fighting OC by dealing with early signs of a emerging threats through a combination of technological resources and human actors.

Description of the work

ePOOLICE has been organized in different Work Packages: **WP1**, Project Management and Coordination.

WP2 aims to ensure the commitment and involvement of End-users and other stakeholders in order to successfully achieve the project's goals; it will push the development of the methodological part of the project.

WP3 deals with the technical and legal/ethical constraints and the design of the system framework considering the user requirements (from WP2) and the relevant ethical and legal issues. **WP4** will develop and define a data model for the Environmental Knowledge Repository (EKR) as a common, uniform representation of extracted information for **WP5** Environmental radar, as well as for the derived fused information, inferred knowledge, hypothesis, etc. in **WP6**. **WP7** comprises development of end-user tools for alert visualization and situation assessment, based on the signals and data captured by the radar. **WP8** is responsible for the integration of the tools developed, considering the framework design in WP3. Finally dissemination and exploitation tasks are covered in **WP9**.

Coordinator

INGENIERÍA DE SISTEMAS

PARA LA DEFENSA DE ESPAÑA SA (ISDEFE)

Defence and Security

Division

Beatriz de Bobadilla, 3

E-28040 - Madrid - Spain

Contact

Raquel Pastor Pastor

Tel: +34 91 411 50 11

Mobile: +34 639 839 158

Fax: +34 91 411 47 03

E-mail: rpastor@isdefe.es

Website: www.epoolice.eu

Expected results

ePOOLICE will support LEAs:

- » to scan the environment to feed new and emerging threats into the serious and organised crime threat assessment processes
- » to map changes within the OC situations that impact the security of the European Union Member States
- » to enable the strategic decision makers to counter-balance detected upcoming threats before they materialize

by:

- » using feedback from analysts to distillate and propose new indicators/signals and adjust its warning/alert levels;
- » discovering and proposing new sources to be scanned;
- » evaluating and estimating the importance of sources;
- » providing more effective information into foresight to fight all sorts of organised crime.
- » providing a better understanding of the new and upcoming technologies and trends, leading to the strategic planning into security issues of all stakeholders

PARTNERS

Ingeniería de Sistemas para la Defensa de España SA (ISDEFE)
 Aalborg Universitet (AAU)
 Commissariat a l'Energie Atomique et aux Energies Alternatives (CEA)
 Thales Communications & Security SAS (TCS)
 Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V. (FKIE)
 Universidad de Granada (UGR)
 Sheffield Hallam University (SHU)
 Inthemis (INTHE)
 Legind Technologies AS (LTA)
 SAS Software Limited (SAS)
 Ministerio del Interior (MIR-GUCI)
 West Yorkshire Police Authority (WYP)
 United Nations Interregional Crime and Justice Research Institute (UNICRI)
 Fachhochschule fur Offentliche Verwaltung und Rechtspflege in Bayern (FHVRP)
 European Police Office (EUROPOL)
 Institutet for Fremtidforskning Forening (CIFS)
 Thales Nederland BV (TRT-NL)

COUNTRY

Spain
 Denmark
 France
 France
 Germany
 Spain
 United Kingdom
 France
 Denmark
 United Kingdom
 Spain
 United Kingdom
 Italy
 Germany
 The Netherlands
 Denmark
 The Netherlands

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

Peace Research Institute Oslo (PRIO)
 Totalförsvarets Forskningsinstitut (FOI)
 DEN HAAG CENTRUM VOOR STRATEGISCHE STUDIES (HCSS)
 TRILATERAL RESEARCH & CONSULTING LLP (TRI)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-ISI-INT)
 CENTRE FOR IRISH AND EUROPEAN SECURITY (CIES)
 AUSTRIAN INSTITUTE OF TECHNOLOGY GmbH (AIT)
 Morpho (MPH)
 MAGEN DAVID ADOM (MDA)
 Police Service of Northern Ireland (PSNI)

COUNTRY

Norway
 Sweden
 Netherlands
 United Kingdom
 Germany
 Ireland
 Austria
 France
 Israel
 United Kingdom

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: +972 36407574

Mobile: +972 544381600

Fax: +972 36410193

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

© ESRI Final Report, Part 2, Working Group 10

FOCUS

FP7 - SEC - 2010 - 1



Information

Grant Agreement N°
261633

Total Cost
€4,372,012

EU Contribution
€3,407,075

Starting Date
01/04/2011

End Date
31/03/2013

Coordinator

**SIGMUND FREUD
PRIVATUNIVERSITÄT
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.

Results

FOCUS elaborated five indicative scenarios to frame the alternative future security roles the EU could play by the year 2035. The aim was to use these scenarios to derive the future security research needed to support those EU roles. The 2035 scenarios were:

- » The EU evolves into a common "securitisation model". It rests on a much closer integration of national security research

programmes with that of the EU to help Europe deal with security incidents.

- » By 2035, competing national and regional policies beyond their borders are producing an increasingly fragmented world, split into tiny privileged elites versus the teeming masses of “have-nots.” The rapidly evolving risk for everyone is a disastrous collapse of society and civilisation.
- » Security management is a risk-driven process. Collaboration between international organisations, member states, EU bodies, civil society organisations and the private sector via security data compilation, crowd sourcing and information sharing has led to the establishment of a harmonised risk management approach.
- » The EU’s policy to counter cyber-attacks is paramount since

this form of societal defence has become all-encompassing for Europe’s economic, industrial, and scientific development. Continuous cooperative vulnerability assessments involving as many countries as possible have become a priority.

- » The EU is the governing authority of scientific and technological innovations related to security of the citizen. Capability development leads to a convergence of research in the fields of civil security, policing needs, emergency response, and disaster management. This links the EU’s internal decision-making structures to its external strategic environment.

FOCUS’s foresight work led to its ultimate result: an IT-based interactive roadmap for security research. Based on the project’s five indicative scenarios, it allows users to modulate its parameters to determine their most appropriate future research options.

PARTNERS

SIGMUND FREUD PRIVATUNIVERSITÄT WIEN GMBH (SFU-CEUSS)
 ATOS ORIGIN SOCIEDAD ANONIMA ESPAÑOLA (ATOS)
 BOC ASSET MANAGEMENT GMBH (BOC)
 INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (CSDM)
 CROSS-BORDER RESEARCH ASSOCIATION (CBRA)
 INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPAÑA SA (ISDEFE)
 CESKE VYSOKE UCENI TECHNICKE V PRAZE (CVUT)
 SECEUR SPRL (SECEUR)
 UNIVERSITÄT FUER WEITERBILDUNG KREMS (DUK)
 UNIVERSITY OF HAIFA (U HAIFA)
 UNIVERSITÄT FUER BODENKULTUR WIEN (BOKU)
 INSTITUTO NACIONAL DE TECNICA AEROESPACIAL (INTA)
 CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)

COUNTRY

Austria
 Spain
 Austria
 Bulgaria
 Switzerland
 Spain
 Czech Republic
 Belgium
 Austria
 Israel
 Austria
 Spain
 Germany

FORCE / FOResight Coordination for Europe



Information

Grant Agreement N°

607858

Total Cost

€1,056,513.40

EU Contribution

€930,510.74

Starting Date

01/04/2014

Duration

24 months

Coordinator

EFPC (UK) LTD

19 Broomburn Court, 14
Broomburn Drive
G77 5JG - Newton Mearns
Scotland

Contact

Michael Remes

Tel: +44 141 563 6853

Mobile: +972 544 801 255

Fax: +972 893 27362

E-mail:

michael@efpcgroup.com

Website: www.efpcgroup.com

Project objectives

- » To examine previous Security Research foresight studies and horizon-scanning activities in FP7 and elsewhere in Europe
- » To produce, based on this work, a foresight model and intelligent decision support system (IDSS), which is scalable with future foresight research activities conducted in Europe. These tools will help policy makers and stakeholders in the security domain do strategic planning with regard to relevant trends and threats by using methodologies and information from available studies.

Description of the work

FORCE activities will include:

- » Examining outputs from Security Research projects funded in FP7 and other sources related to foresight and horizon-scanning activities via: literature review, workshops; interviews; collaboration with national and international foresight networks
- » Assessing methods used in security foresight studies in the last five years regarding their strengths and weaknesses
- » Identifying possible gaps between potential future threats and methods used so far
- » Producing a foresight model that is scalable and sustainable beyond the project's life
- » Developing the IDSS as an end-user tool and producing and running test scenarios against which the system can be evaluated
- » Supporting the visibility and take up of security research results at stakeholder level, especially vis-a-vis end users through dissemination of the foresight model and corresponding IDSS

Expected results

A foresight model (including online mapping tool for interrogating available security related foresight studies, methodologies and tools) and an Intelligent Decision Support System (IDSS) to help identify emerging threats and other factors for policy makers and security stakeholders. These tools will be evolvable and sustainable beyond the end of the project.

PARTNERS

EFPC (UK) Ltd (EFPC)
Globaz, S.A. (GLOBAZ)
Technische Universität Berlin (TUB)
Inovamais – Servicos De Consultadoria Em Inovacao Tecnologica S.A. (INOVA+)
Tel Aviv University (TAU), the Unit for Technology and Society Foresight
Atos Spain S.A.

COUNTRY

United Kingdom
Portugal
Germany
Portugal
Israel
Spain

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



© Cornelius - Fotolia.com

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.

**RESEARCH
COMPLETED**

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

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

Technical University Berlin (TUB)
 University of Kassel (UNIKASSEL)
 University of Newcastle (UNEW)
 Kingston University London (KU)
 Higher Institute on Territorial System for Innovation Torino (SITI)
 Tel Aviv University (ICTAF)
 Vrije Universiteit Brussels (VUB)

COUNTRY

Germany
 Germany
 United Kingdom
 United Kingdom
 Italy
 Israel
 Belgium

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

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 60602600 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

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 University of Ulster (UU)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-EMI)
 Albert-Ludwigs-Universität Freiburg (ALU)
 ITTI Sp.zo.o. (ITTI)
 The Stephen Lawrence Charitable Trust (SLCT)
 Downey Hynes Limited (DHP)
 JVM Limited (JVM)
 Crabbe Consulting Ltd. (CCLD)
 Consiglio Nazionale delle Ricerche (CNR)
 Università degli Studi Mediterranea di Reggio Calabria (UMRC)
 Experian Nederland BV (EXP)
 Stichting Dr. Hilda Verwey-Jonker Instituut (VJI)
 Institute for Housing and Urban Development Studies B.V. (EUR)

COUNTRY

The Netherlands
 United Kingdom
 Germany
 Germany
 Poland
 United Kingdom
 Ireland
 United Kingdom
 United Kingdom
 Italy
 Italy
 The Netherlands
 The Netherlands
 The Netherlands

EUSECON / A new agenda for european security economics



RESEARCH
COMPLETED

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, geopolitical 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

German Institute for Economic Research
 Institute for Peace Research and Security Policy at the University of Hamburg
 Economics Institute of the Academy of Sciences of the Czech Republic
 Charles University Prague
 University of Patras
 The Chancellor, Masters and Scholars of the University of Oxford
 Ingeniería de Sistemas para la Defensa de España, S.A.
 Basque University
 RAND Europe
 Hebrew University Jerusalem
 University of Thessaly
 University of Linz
 International Peace Research Institute, Oslo
 Institute of Social Studies
 Athens University of Economics and Business - Research Center (AUEB-RC)

COUNTRY

Germany
 Germany
 Czech Republic
 Czech Republic
 Greece
 United Kingdom
 Spain
 Spain
 United Kingdom
 Israel
 Greece
 Austria
 Norway
 The Netherlands
 Greece

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 modeling 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.



PARTNERS

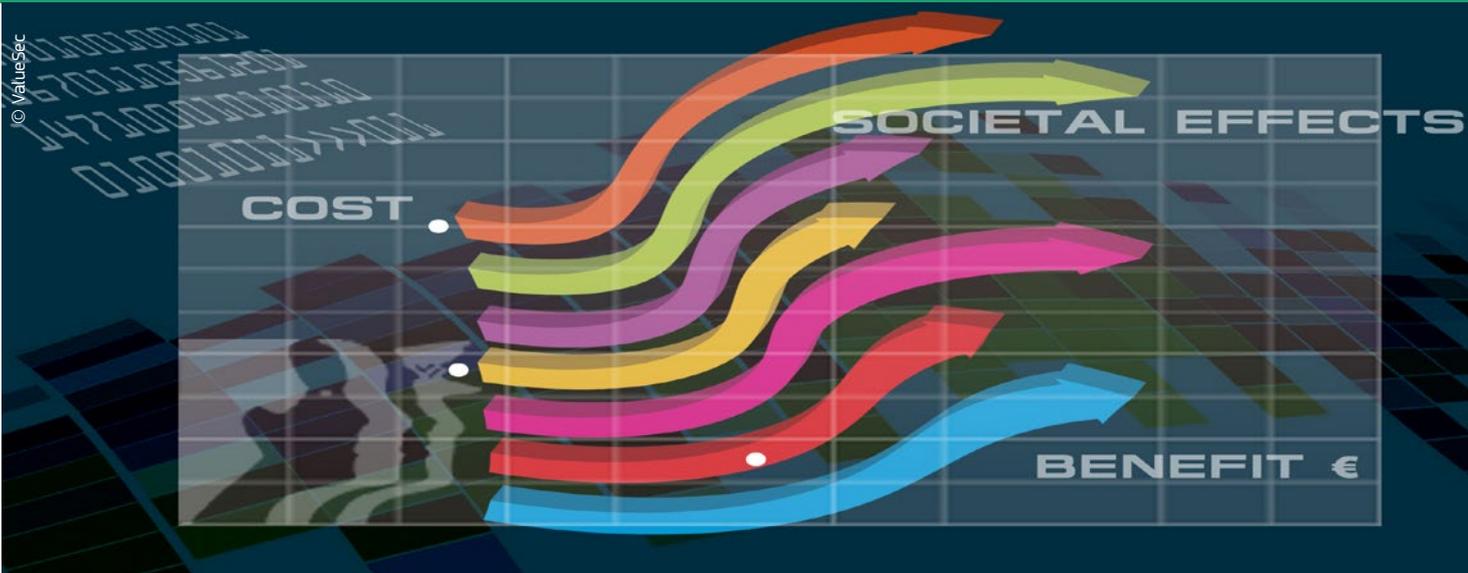
UNIVERSITA' DEGLI STUDI DI TRENTO (UNITN)
 DEEP BLUE SRL (DBL)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 UNIVERSIDAD REY JUAN CARLOS (URJC)
 THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN (UNIABDN)
 FERROCARRIL METROPOLITA DE BARCELONA SA (TMB)
 ATOS SPAIN 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

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

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IFF)
 VTT Technical Research Centre of Finland (VTT)
 Centre for European Security Strategies (CESS)
 International Peace Research Institute (PRIO)
 University of Stavanger (UIS)
 ATOS Origin S.A. (Atos)
 Institute of Innovative Technologies (EMAG)
 White Cyber Knight (WCK)
 Policía Local de Valencia (VPD)

COUNTRY

Germany
 Finland
 Germany
 Norway
 Norway
 Spain
 Poland
 Israel
 Spain

ARCHIMEDES / Support to security end users

© Cristian Baltg - 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

European Organisation for Security (EOS)
 Ministerio Del Interior (MIR-ES)
 Ingeniera De Sistemas Para La Defensa De España SA-ISDEFE (ISDEFE)
 Universite catholique De Louvain (UCL)
 Haut Comite Francais Defense Civile (HCFDC)
 German European Security Association EV (GESA)
 Przemyslowly Instytut Automatyki I Pomiarow (PIAP)
 @ Mediaservice.Net SRL (MEDIASERVICE)

COUNTRY

Belgium
 Spain
 Spain
 Belgium
 France
 Germany
 Poland
 Italy

EU-SEC II / Coordinating National Research Programmes and Policies on Security at Major Events in Europe



© Fotofa.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.itWebsite: 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.

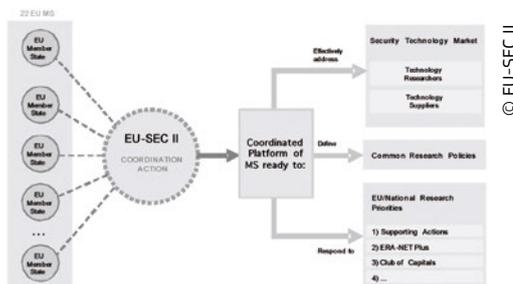
One of EU-SEC II's objectives was to investigate which services the House could offer, focusing in particular on public-private partnerships (PPPs), common research standards and media management. The final output was a pilot research strategic roadmap to direct future research priorities.

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.



PARTNERS

United Nations Interregional Crime and Justice Research Institute
 Europol
 Bundesministerium 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 Síochana
 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 Batig - 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

Fundación Tecnalia Research & Innovation (TECNALIA)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Valtion Teknillinen Tutkimuskeskus (VTT)
 Ministerio de Defensa de España (MDE)
 Totalförsvarets Forskningsinstitut (FOI)
 Austrian Institute of Technology GmbH (AIT)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 The University of Manchester (UNIMAN)
 Österreichisches Rotes Kreuz – Austrian Red Cross (ÖRK ARC)
 Prosegur Compañía de Seguridad SA (PROSEGUR)

COUNTRY

Spain
 Germany
 Finland
 Spain
 Sweden
 Austria
 The Netherlands
 United Kingdom
 Austria
 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 through 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

ALMA CONSULTING GROUP SAS (Alma)
 EFPC (UK) LTD (EFPC)
 FM MANAGEMENT CONSULTANCY SRL (FMMC)
 PROXIMA CENTAURI SAS (KAOS)
 ADVISIO OU (ADVISIO)
 GLOBAZ SA (GLOBAZ)
 EVERIS SPAIN SLU (EVR)
 INOGATE- CONSULTORIA EM INOVACAO EMPRESARIAL SA (INOGATE)
 SISEKAITSEAKADEEMIA (EASS)
 ACADEMIA DE POLITIE ALEXANDRU IOAN CUZA (AICPA)
 GRAD SKOPJE (CoS)

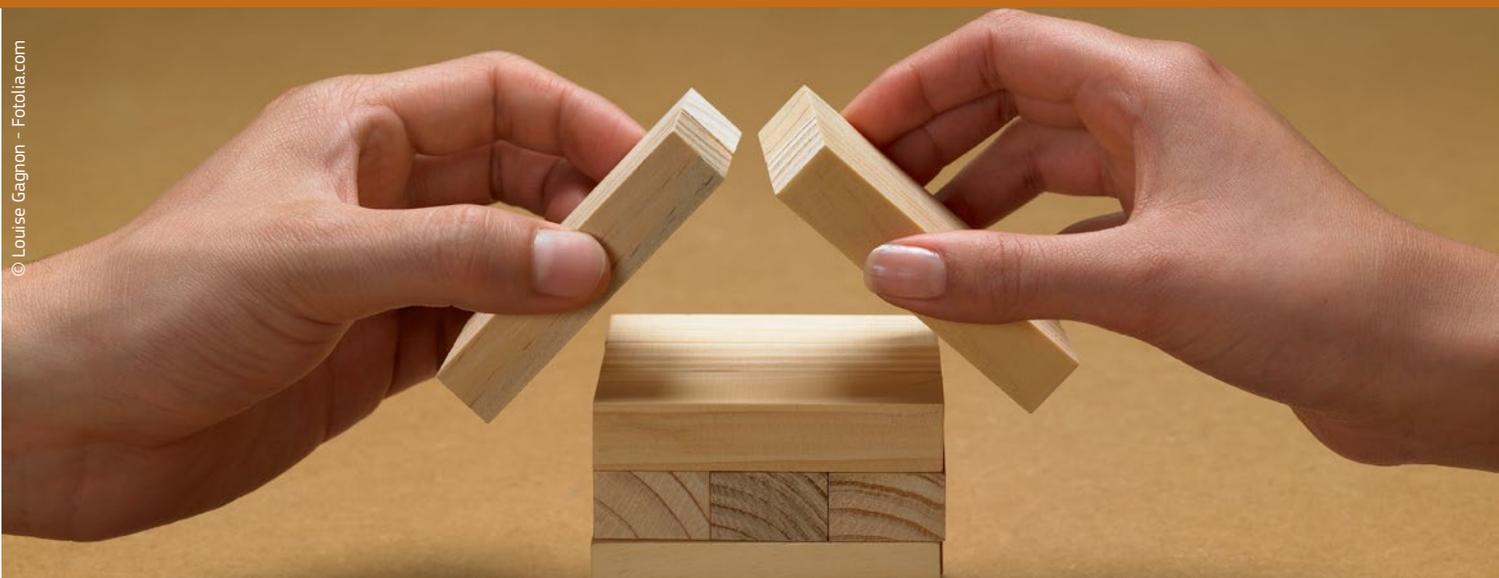
AUTORIDAD PORTUARIA DE GIJON (PAG)
 HUNGARIAN MINISTRY OF INTERIOR (ORFKV)
 OU BALTIC INNOVATION AGENCY B.I.A. (BIA)
 ROMANIAN MINISTRY OF ADMINISTRATION AND INTERIOR (MAI)

COUNTRY

France
 United Kingdom
 Romania
 France
 Estonia
 Portugal
 Spain
 Portugal
 Estonia
 Romania
 Former Yugoslav
 Republic of Macedonia
 Spain
 Hungary
 Estonia
 Romania

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,
10127 Turin, Italy

Contact

Barbara Maria Rohmann

Tel: +39 0116537111

Fax: +39 0116313368

E-mail: rohmann@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.

⁽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.

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.

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

United Nations Interregional Crime and Justice Research Institute (UNICRI)
 Bundesministerium für Inneres-Ministry of the Interior (BM.I)
 Deutsche Hochschule der Polizei (DHPol)
 Ministerio del Interior (MIR-CNP)
 Ministère de l'Intérieur (D.G.P.N.)
 Metropolitan Police Service (MetPol)
 An Garda Síochána (AGS)
 Ministero dell'Interno (MinInterno)
 Ministry of Security and Justice (MinJus)
 Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI/MAI)
 Center for Security Studies (KEMEA)
 State Police of Latvia (SP)
 Ministry of Administration and Interior-Inspectorate General of Romanian Police (MoAI-GIRP)
 Ministry of Interior of the Slovak Republic (MINV-APZ SK)
 Academy of the Ministry of the Interior (Academy of MOI)
 Ministry of the Interior of the Republic of Slovenia (MOI SI)
 Ministry of the Interior of the Republic of Estonia (MOI)
 Cyprus Police (Cyprus Police)
 Hungarian National Police (HNP)
 Malta Police Force (MPF)
 Swedish National Police Board (Polisen)
 The Danish National Police (DNP)
 Police department under the Ministry of the Interior of the Republic of Lithuania (PD)
 Police College of Finland (Polamk)
 Wyższa Szkoła Policji W Szczytnie (WSPol)

COUNTRY

Italy
 Austria
 Germany
 Spain
 France
 United Kingdom
 Ireland
 Italy
 The Netherlands
 Portugal
 Greece
 Latvia
 Romania
 Slovakia
 Bulgaria
 Slovenia
 Estonia
 Cyprus
 Hungary
 Malta
 Sweden
 Denmark
 Lithuania
 Finland
 Poland

CIPRNet / Critical Infrastructure Preparedness and Resilience Research Network



© CIPRNet

Information

Grant Agreement N°
312450

Total Cost
€7,663,168.20

EU Contribution
€6,569,842.50

Starting Date
01/03/2013

Duration
48 months

Coordinator

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER)

Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS Adaptive Reflective Teams Department (ART)
Schloss Birlinghoven
53757 – Sankt Augustin
Germany

Contact
Erich Rome

Tel: +49 2241 14 2683
Fax: +49 2241 14 4 2683
E-mail: erich.rome@iais.fraunhofer.de
Website: www.ciprnet.eu

Project objectives

CIPRNet has four general scientific and technological objectives:

- » To strengthen and structure the European Critical Infrastructure Protection (CIP) research area by establishing a network of shared CIP knowledge and expertise that offers and transfers knowledge to isolated CIP and adjacent research areas.
 - » To provide support from CIP research communities to emergency managers, governmental agencies and policy-makers, enhancing their all-hazard preparedness for, response to, and recovery of disrupted, failed or destroyed Critical Infrastructures (CI) and their cascading effects.
 - » To enhance the resilience of CI by improving the knowledge and understanding, preparation and mitigation of CI disruptions and their consequences.
 - » To lay the foundation for a long-lasting virtual centre of competence and expertise in CIP, the "European Infrastructures Simulation & Analysis Centre" (EISAC).
- CIPRNet will reach these objectives by:
- » Implementing new capabilities for supporting more effective responses to disasters that affect or originate from CI,
 - » Building the required capacities for creating these new capabilities, and
 - » Founding a long-lasting virtual centre of competence and expertise in CIP (VCCC).

Description of the work

CIPRNet's joint R&D activities towards implementing new capabilities include:

- » Creating added-value, decision-support capabilities with consequence analysis for national and multi-nation emergency management and CI owners based upon integrating technologies available at CIPRNet partners,
- » Supporting the secure design of Next Generation Infrastructures (such as Smart Grids),
- » Creating a 'what if' modelling, simulation and analysis capability for emergency managers for exploring different courses of action in crises.

CIPRNet has a dedicated agenda for further extending and integrating existing technology such as interoperability middleware and creating new simulator federations for the new capabilities.

The second cluster of joint activities addresses capacity building, for reaching the specific goal of creating a critical mass of expert knowledge and expertise in CIP. This includes

- » Cooperation and coordination with other CIP related networks
- » Staff exchange and training
- » Collaboration and exchange with and training of end users and other stakeholders
- » Dedicated dissemination, training and teaching activities

CIPRNet will conduct training exercises, bringing together tools and expertise to develop realistic, complex scenarios. To increase their impact and visibility, CIPRNet will demonstrate the new capabilities in a real crisis management exercise. For this, CIPRNet will investigate a real or realistic emergency scenario; produce consequence analysis of CI failures and cascading effects; perform a vulnerability analysis and hazard analysis within that scenario; and derive courses of actions with their consequences for decision-makers.

The distributed VCCC will allow the integration and coordination of research activities, the dissemination of results, and offer services to the CIP community and end-users. An electronic platform will support the VCCC, deploying new community services via Internet. This will include enquiries to experts, an online glossary on CIP, CIP bibliographies and project lists, and more.

Expected results

Expected tangible results of CIPRNet include:

- » A new Decision Support System capability with consequence analysis for single or multi-nation emergency management (for training and hot phase support)

- » A new 'what if ...' modelling, simulation and analysis capability for emergency managers (for training) and short term predictions (for hot phase support)
- » More and better trained researchers and experts as a result of the various dissemination and training activities of CIPRNet
- » The VCCC, providing support from the CIP research communities to stakeholders. Its services will be accessible through the CIPRNet web site
- » An association fostering the evolution of the VCCC to EISAC for sustaining support beyond the duration of CIPRNet

PARTNERS

Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V. (Fraunhofer)
 Agenzia Nazionale per le Nuove Tecnologie, L'Energia e lo Sviluppo Economico Sostenibile (ENEA)
 Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
 Union Internationale des Chemins de fer (UIC)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 The European Union represented by the European Commission represented by the Joint Research Centre (JRC)
 Stichting Deltares (Deltares)
 University of Cyprus (UCY)
 Uniwersytet Technologiczno-Przyrodniczy im. Jana i Jędrzeja Śniadeckich w Bydgoszczy (UTP)
 Università Campus Bio-Medico di Roma (UCBM)
 The University of British Columbia (UBC)
 ACRIS GmbH (ACRIS)

COUNTRY

Germany
 Italy
 The Netherlands
 France
 France
 European Union
 The Netherlands
 Cyprus
 Poland
 Italy
 Canada
 Switzerland

EUROFORGEN - NOE / European forensic genetics network of excellence

© Euroforigen

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.euroforigen.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

Universitätsklinikum Köln (UHC)
 Universidade de Santiago de Compostela (USC)
 Nasjonalt Folkehelseinstitutt (NIPH)
 Queen Mary and Westfield College, University of London (QMUL)
 Københavns Universitet (UCPH)
 Netherlands Forensic Institute (NFI)
 Medizinische Universitaet Innsbruck (IMU)
 Universitetet for Miljø og Biovitenskap (UMB)
 Uniwersytet Jagiellonski (JU)
 University of Northumbria at Newcastle (UNN)
 Epiontis GmbH (EPTS)
 GABO:mi Gesellschaft fuer Ablauforganisation:milliarium mbH & Co. KG (GABO:mi)

COUNTRY

Germany
 Spain
 Norway
 United Kingdom
 Denmark
 Netherlands
 Austria
 Norway
 Poland
 United Kingdom
 Germany
 Germany

PLANTFOODSEC / Plant and food biosecurity

© Monika Wisniewska - Fotolia.com



Information

Grant Agreement N°
261752

Total Cost
€5,609,529.69

EU Contribution
€4,624,499

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

Università degli Studi di Torino (UNITO-AGROINNOVA)
 National Institute of Agricultural Botany
 The Secretary of State for Environment, Food and Rural Affairs
 Rheinische Friedrich-Wilhelms-Universität Bonn
 Institut National de la Recherche Agronomique
 Regional Environmental Center for Central and Eastern Europe
 Imperial College of Science, Technology and Medicine
 Middle East Technical University
 SPIN-TO Srl
 United Nations Interregional Crime and Justice Research Institute
 The Agricultural Research Organisation of Israel – The Volcani Centre
 Oklahoma State University
 Kansas State University

COUNTRY

Italy
 United Kingdom
 United Kingdom
 Germany
 France
 Hungary
 United Kingdom
 Turkey
 Italy
 Italy
 Israel
 United States
 United States

SEREN / Security Research NCP network – Phase 1



© Andres Rodriguez - Fotolia.com

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.

**RESEARCH
COMPLETED**

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

Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Tarptautiniu mokslo ir technologiju pletros programu agentura
 Achimedes Foundation
 Foundation For Research & Technology – Hellas
 National Office for Research and Technology
 Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk
 Matimop, Israel Industry Center For Research & Development
 Agenzia per la Promozione della Ricerca Europea
 Romanian Space Agency
 Norges forskningsråd
 The Scientific and Technological Research Council of Turkey
 Service d'information scientifique et technique / SPP Politique scientifique –
 Dienst voor Wetenschappelijke en Technische Informatie / POD Wetenschapsbeleid
 Österreichische Forschungsförderungsgesellschaft mbH
 Agência de Inovação, Inovação Empresarial e Transferência de Tecnologia, S.A
 Centro para el Desarrollo Tecnológico Industrial
 SenterNovem
 Technologické centrum
 Research Promotion Foundation
 Totalförsvarets Forskningsinstitut (FOI)
 Euresearch
 Council for Scientific and Industrial Research
 Riga Technical University
 Centre for National Security and Defense Research
 Malta Council for Science and Technology
 Home Office
 Luxinnovation GIE
 Danish Agency for Science Technology and Innovation -Ministry of Science, Technology and Innovation
 Agentura na podporu vyskumu a vyvoja

COUNTRY

France
 Lithuania
 Estonia
 Greece
 Hungary
 Poland
 Israel
 Italy
 Romania
 Norway
 Turkey

 Belgium
 Austria
 Portugal
 Spain
 The Netherlands
 Czech Republic
 Cyprus
 Sweden
 Switzerland
 South Africa
 Latvia
 Bulgaria
 Malta
 United Kingdom
 Luxembourg
 Denmark
 Slovakia

SEREN2 / Security REsearch Ncp network – phase 2

© kablitzsch - Fotolia.com

**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.

WP2 – 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.

WP3 – 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.

WP4 – Partner Search is dedicated to *promote transnational cooperation by facilitating the access of potential participants to future Security calls*.

WP5 – 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.

WP6 – 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 SERENZ 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

Romanian Space Agency (ROSA)
 Foundation for Research & Technology – HELLAS (FORTH)
 Agenzia per la Promozione della Ricerca Europea (APRE)
 Österreichische Forschungsförderungsgesellschaft mbH (FFG)
 Euresearch Head Office Berne (EURESEARCH)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Mokslo Inovacijų Ir Technologijų Agentūra (MITA)
 SIHTASUTUS ARCHIMEDES (Archimedes)
 Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk (IPPT PAN)
 MATIMOP - Israel Industry Center for Research & Development (MATIMOP-ISERD)
 Norges forskningsråd – Research Council of Norway (RCN)
 The Scientific and Technological Research Council of Turkey (Tubitak)
 Dienst voor Wetenschappenlijke en Technische Informatie /
 Service d'Information scientifique et technique (STIS)
 Centro para el Desarrollo Tecnológico Industrial (CDTI)
 Technologické centrum Akademie věd České republiky
 (The Technology Centre of the Academy of Science - TC AS CR)
 Research Promotion Foundation (RPF)
 Totalförsvarets Forskningsinstitut (FOI)
 Council for Scientific and Industrial Research (CSIR)
 Riga Technical University (RTU)
 Centre for National Security and Defense Research (CNSDR)
 Malta Council for Science and Technology (MCST)
 Zilinska Univerzita v Ziline (UNIZA)
 Finnish Funding Agency for Technology and Innovation (TEKES)
 Hrvatski institut za tehnologiju/ Croatian Institute of Technology / Odjel za međunarodnu suradnju/
 International Cooperation Unit (HIT)
 Fundacao para a Ciencia e Tecnologia (FCT)
 National Institute of Aerospace Technology of Spain (INTA)

COUNTRY

Romania
 Greece
 Italy
 Austria
 Switzerland
 France
 Lithuania
 Estonia
 Poland
 Israel
 Norway
 Turkey
 Belgium
 Spain
 Czech Republic
 Cyprus
 Sweden
 South Africa
 Latvia
 Bulgaria
 Malta
 Slovakia
 Finland
 Croatia
 Portugal
 Spain

SOURCE / Virtual centre of excellence for research support and coordination on societal security



© Kim Eriksen, NRK P3

Information

Grant Agreement N°
313288

Total Cost
€5,576,210.00

EU Contribution
€4,997,588.00

Starting Date
01/01/2014

Duration
60 months

Coordinator

**INSTITUTT FOR
FREDSFORSKING
STIFELESE (PRIO)**
Dimensions of Security
Hausmanns gate 7
0186 – Oslo – Norway

Contact
J. Peter Burgess
Tel: +47 22547738
Mobile: +47 90923949
E-mail:
jpeterburgess@prio.org
Website: www.prio.org

Project objectives

The aim of the SOURCE project is to create a robust and sustainable virtual centre of excellence which explores and advances the societal issues of security research and development.

Description of the work

SOURCE is built upon five types of activities: networking activities, research, information gathering, education and training and, finally, knowledge-sharing. Together these address the ambitions and the expected impact of the EU's Work Programme specific to the Security call.

Via an integrated information-gathering hub, education programmes across security sectors, and a comprehensive programme of networking activities, SOURCE's virtual centre will gather experts and actors from all levels of the security chain (researchers, industry actors, policy-makers, civil society, end-users and the public at large). All will be linked by a common effort of documenting, analysing and understanding the links between security and society where the former is played out.

Expected results

The project will relay on an array of networking activities, meetings, scientific and popular publications, film, press and social media, a scholarly journal and the formation of an international association for the study and improvement of societal security. SOURCE's Network of Excellence will raise awareness among policy makers and end-users, increase the security industry's competitiveness by better responding to the social "layers of insecurity" across society and, as a consequence, contribute to the improved well-being and security of European citizens.

PARTNERS

Institutt for fredsforsking stifelese (PRIO)
 Totalforsvarets Forskningsinstitut (FOI)
 Centre for Irish and European Security Limited (CIES)
 Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung e.v (Fraunhofer)
 Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
 Centre for European Policy Studies (CEPS)
 Vrije Universiteit Brussel (VUB)
 IRKS-Research GesmbH
 King's College London (KCL)
 European Organisation for Security (EOS)
 Fundacion Tecnalia Research & Innovation (TECNALIA)
 Fondation Nationale des Sciences Politiques (Sciences Po)

COUNTRY

Norway
 Sweden
 Ireland
 Germany
 The Netherlands
 Belgium
 Belgium
 Austria
 United Kingdom
 Belgium
 Spain
 France

VIDEOSENSE / Virtual Centre of Excellence for Ethically-guided and Privacy-respecting Video Analytics in Security



© iofoto - Pavel Losensky - Huma - NZ:Photos - 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@reading.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

THE UNIVERSITY OF READING (UoR)
 QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)
 EURECOM (EURECOM)
 THALES SECURITY SOLUTIONS & SERVICES SAS (THALES)
 INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA ISDEFE (ISDEFE)
 TECHNISCHE UNIVERSITAET BERLIN (TUB)
 ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE (EPFL)
 INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)

COUNTRY

United Kingdom
 United Kingdom
 France
 France
 Spain
 Germany
 Switzerland
 Belgium

VOX-Pol / Virtual Centre of Excellence for Research in Violent Online Political Extremism



Information

Grant Agreement N°

312827

Total Cost

€5,554,326.28

EU Contribution

€5,129,681.00

Starting Date

01/01/2014

Duration

60 months

Coordinator

DUBLIN CITY UNIVERSITY (DCU)

School of Law
& Government
Glasnevin

Dublin 9, Ireland

Contact

Maura Conway

Tel: +353 (0)1 700 6472

Mobile:

+353 (0)87 295 1284

Fax: +353 (0)1 700 7374

E-mail:

info@voxpoleu

maura.conway@dcu.ie

Website: www.voxpoleu

Project objectives

- » Promote long-term relationships between established national research groups and new researchers/research groups;
- » Provide training via conferences, summer schools, and workshops to researchers, PhD students, early career researchers and those who monitor or respond to VOPE about the tools, methods and substantive issues of violent online political extremism;
- » Raise awareness about the interplay of e-research ethics, privacy, surveillance, freedom of speech, and responses to violent online political extremism;
- » Outreach to diverse publics via mass media, public lectures and other public events, free-to-access publications, etc., which describe our research and its purposes;
- » Influence European and international research agendas in key aspects of violent online political extremism.

Description of the work

- » Integration and networking of research activities within EU and globally of those working on violent online extremism and its effects, including the online strategies of: violent jihadists, the extreme right, violent nationalist-separatist and ethnic separatist movements;
- » Creation of a sustainable critical mass of innovative activity among today's fragmented group of researchers and research topics through joint research, networking events, and teaching and learning activities;
- » Create an archive of politically extreme Internet-based content as the basis for joint research activity; develop new analytical tools and methodologies, teaching and training, and dissemination activities;
- » Harness software tools used in other domains to collect and analyse violent online political extremist content;
- » Forge long-term relationships between established national research groups, new researchers, security practitioners, the Internet industry, civil society and policymakers to develop a multi-disciplinary Virtual Centre of Excellence for Research in Violent Online Political Extremism;
- » Ensure that EU and Member State strategies targeting violent online political extremism are based on concrete evidence, experience, and knowledge.

Expected results

- » Critical mass of research excellence in the relevant research areas within the EU together with VOX-Pol's international partners;
- » Synergy on approaches, methodologies, and technologies currently being developed independently by disciplinarily and/or geographically distinct research communities;
- » Better informed policy agendas on national, European, and international levels in key aspects of responses to violent online political extremism.

PARTNERS

Dublin City University (DCU)
 University of Oxford (UOXF)
 Indraprastha Institute of Technology Delhi (IIITD)
 King's College London (KCL)
 Universiteit van Amsterdam (UVA)
 Nederlandse Organisatie voor Toegepast Natuurwetenschap (TNO)
 Institut für Friedensforschung und Sicherheitspolitik an Der Universität Hamburg (IFSH)
 at the University of Hamburg
 Central European University (CEU)
 University College London (UCL)

COUNTRY

Ireland
 United Kingdom
 India
 United Kingdom
 The Netherlands
 The Netherlands
 Germany
 Hungary
 United Kingdom

3D-Forensics / Mobile high-resolution 3D-Scanner and 3D data analysis for forensic evidence

© IOF



Information

Grant Agreement N°
312307

Total Cost
€1,770,435

EU Contribution
€1,420,262

Starting Date
01/05/2013

Duration
24 months

Coordinator

**Fraunhofer-Gesellschaft
zur Foerderung der
angewandten Forschung
e.V. (FhG)**

Fraunhofer-Institut für
Angewandte Optik und
Feinmechanik IOF
Albert-Einstein-Straße 7
07745 Jena,

Germany

Contact

Peter Kühmstedt

Tel: +49 (0)3641 807 230

Fax: +49 (0)3641 807 602

E-mail: peter.kuehmstedt@

iof.fraunhofer.de

Website:

www.3D-Forensics.eu

Project objectives

- 1) Development of a mobile high-resolution 3D scanning system for forensic evidence recovery at crime scenes.
- 2) Development of 3D data analysis and processing software tools to provide results which may be used in the investigation and prosecution of crime.
- 3) Test and evaluation of the 3D scanning system with processing and analysis software by members of the forensic community.
- 4) To supplement the expertise of an SME-based consortium with further end-user and applied research knowledge for efficient and effective development of a new product.

Description of the work

In the first phase of the project the technical requirements placed on the design of the 3D scanning and analysing system will be confirmed and further detailed. This will be achieved by considering the present use of traces in the investigation and prosecution of crime and the potential offered by the application of the 3D scanning technology. An important result will be confirmation of the types of traces the scanning system should focus on, most probably footwear and vehicle tyre impressions.

In the second phase of the project the complete system will be designed, consisting of two parts. Firstly, a mobile hand-held 3D-sensor system based on high-resolution fringe projection, including embedded FPGA-based electronics for fast data processing, designed for direct use at crime scenes. Secondly, a set of software tools designed for collection of 3D-data, the easy extraction of 3D-features out of scanned traces and their forensic analysis. The design will need to ensure that the data provided by the system is of a type and quality that police can use it for investigations and, where necessary, be admissible as evidence in court.

The third phase of the project will be development and integration of the system's modules as determined by the previous design phase. The development of two prototypes is foreseen. They will be tested in the fourth phase of the project, which is focussed on the test and evaluation of the development results.

Dissemination, exploitation and management activities run throughout the course of the project.

The project responded to a topic in the FP7 Security Research work programme that was specifically targeted towards Small and Medium sized Enterprises (SMEs). Five of the seven partners are SMEs. The work in the project will be

focussed towards providing a solution which is sufficiently attractive to the police community to be commercially exploited by the SMEs.

Expected results

The system offers the potential to reduce the time required to match or rule out the presence of suspects at crime scenes. In addition, the application of advanced optical scanning and data analysis technology offers the possibility to increase the evidentially relevant detail obtained from traces at crime scenes.

PARTNERS

Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V. (FhG)
Regio Politie Zeland
DelftTech BV
Lucas Instruments GmbH
Enclustra GmbH
Gexcel srl
Crabbe Consulting Ltd

COUNTRY

Germany
The Netherlands
The Netherlands
Germany
Switzerland
Italy
United Kingdom

GRAFFOLUTION / Awareness and Prevention Solutions against Graffiti Vandalism in Public Areas and Transport



Information

Grant Agreement N°

608152

Total Cost

€1,921,748

EU Contribution

€1,497,040

Starting Date

01/03/2014

Duration

24 months

Coordinator

SYNYO GMBH (SYNYO)

Research & Development

Department

Otto-Bauer-Gasse 5/14

1060 – Vienna – Austria

Contact

Bernhard Jäger

Tel: +43 1 9962011 6

Mobile:

+43 699 18 940 006

Fax: +43 1 99 620 11 77

E-mail: bernhard.jaeger@synyo.com

synyo.com

Website:

www.graffolution.eu

www.synyo.com

Project objectives

The key objectives of Graffolution are to:

1. Enforce fundamental research studies on graffiti vandalism in public areas and transport, and identify relevant stakeholders, roles and processes.
2. Analyse initiatives, measures, technical methods and best practices against graffiti vandalism in Europe and survey requirements of all affected stakeholders.
3. Elaborate concepts and solutions against illegal graffiti, and design a web-based awareness and prevention framework for stakeholders and the public.
4. Develop a collaborative knowledge base for local experts and affected stakeholders to improve the exchange of know-how and support decision makers at European level.
5. Provide an open information hub that adopts social media technologies to increase awareness among sprayers and citizens through information and visualisations.

Description of the work

Graffolution seeks to counteract the increase of graffiti vandalism in public areas and transportation networks by focusing on smart awareness and positive prevention solutions for all affected stakeholder groups, including those who have used street art as part of city regeneration and placemaking strategies.

The project will work to deliver an extensive set of “collaborative tools and resources” that would include:

- (a) a secure space for duty holders, with case studies and other methods of evidencing successful practice, to empower city administrations, public transport services and law enforcement agencies, to share knowledge and more widely promote best practices.
- (b) an interactive “Open Information Hub” targeting local communities, citizens and sprayers to strengthen public awareness and enforce the prevention of illegal spraying activities, using effectual tools and visualisations. Social media features and channels will also be integrated to reach young people, graffiti writers and other connected parties.

Expected results

Graffolution will provide a new and comprehensive approach to discover unused potential for collaboration and knowledge exchange on a pan-European level that involves the public to significantly reduce illegal graffiti on the sustainable basis of a low cost, web-based platform.

Some expected results from Graffolution include:

- » Facilitate knowledge exchange between key stakeholders on a pan-European level
- » Increase awareness on graffiti vandalism
- » Improve security in public areas and transport
- » Improve living environments and minimise feelings of insecurity
- » Minimise costs on removal and prosecution

PARTNERS

SYNYO GmbH (SYNYO)
 Universitat de Barcelona (UB)
 The University of Arts London (UAL)
 Sine-Institute gGmbH (SINE)
 Ferrocarrils de la Generalitat de Catalunya (FGC)
 London Borough of Islington (LBI)
 Union Internationale des Chemis de Fer (UIC)
 Eticas Consulting (EC)

COUNTRY

Austria
 Spain
 United Kingdom
 Germany
 Spain
 United Kingdom
 France
 Spain

MISAFE / The Development and Validation of Microbial Soil Community Analyses for Forensics Purposes



Information

Grant Agreement N°

313149

Total Cost

€2,604,269.40

EU Contribution

€1,991,000.00

Starting Date

01/06/2013

Duration

24 months

Coordinator

THE HEBREW

UNIVERSITY OF JERUSALEM (HUJI)

Plant Pathology and Micro-
biology

Faculty of Agriculture, Food
and Environment 12
76100, Rehovot, Israel

Contact

Edouard Jurkevitch

Tel: 972-8-9489167

Fax: 972-8-9489062

E-mail: edouard.jurkevitch@
mail.huji.ac.il

Website:

[https://sites.google.com/
site/fp7misafe/](https://sites.google.com/site/fp7misafe/)

Project objectives

Soil is a complex and heterogeneous material. However, that complexity can make it a useful form of trace evidence in crime investigation. It is easily transferable - attaching, staining and smearing to inanimate objects, as well as to live and dead bodies - it is a potentially valuable asset for use in forensic analysis since its characteristics are affected by its origin, history, environment and management. However, largely due constraints of the current methodology of analysis, soil use as forensics tool is limited.

Soil provides an enormous phylogenetic and functional microbial diversity, with up to one billion cells and many thousands of bacterial species per gram. Soil bacterial communities also are affected by their environment, and have the ability to reflect the history of a given soil, thereby providing a unique and powerful tool for tracing soil origin. Soil evidence is often comparative; as soils differ in microbial content, a comparison of the communities inhabiting soils may reveal if samples from different scenes are derived from the same or from some other, unrelated, location.

Taking advantage of the advent of powerful molecular technologies, and associated big data handling approaches, soil bacterial DNA can be isolated and used to profile the bacterial communities associated with a soil sample. These DNA-based technologies are ripe for forensic analyses and their implementation, discriminating between sites, even between closely related sites.

The objectives of MiSAFE are to develop soil DNA tools for profiling soil bacterial communities in forensic samples, and setting up and implementing protocols and working procedures based on the most powerful DNA technologies. MiSAFE also will construct a framework for a pan-European database of soil microbial communities and soil proper-

ties for potentially comparing forensic soil samples. This project is a partnership between two SMEs, two police forces and three academic institutions.

Description of the work

The expertise of each partner is called upon for the development of specific aspects of the project, and for their integration. This includes:

- » Setting standard parameters of soil DNA extraction and selecting a best performing procedure;
- » Developing sampling and storage procedures;
- » Evaluating and comparing DNA technologies applied to soil forensics;
- » Delimiting spatial and temporal boundaries of soil microbial profiling, and set up a soil profile database;
- » Developing and implementing bioinformatics and statistical tools required for soil microbial profiling;
- » Evaluating and validating the protocols and the material, providing legal support to the approach.

Expected results

The methods developed are based on technologies and approaches already in use in forensic laboratories and are rapidly applicable. The project seeks to provide:

- » Protocols for field sampling and sample collection, so that soil samples can be used for a diversity of analyses, including DNA-based analyses;
- » Determination of DNA parameters, and DNA extraction methods;
- » Implementation of DNA technology for soil forensics;
- » A conceptual framework for the use of microbial DNA in soil forensics;
- » A framework for a prototype soil DNA geoforensics database;
- » Bioinformatics and statistics tools for data analysis, providing the significance of the results acquired;
- » Validation of the methods for use in forensic laboratories.

PARTNERS

The Hebrew University of Jerusalem (HUJI)
 Libragen (LIB)
 CLC Bio (CLCBio)
 Ecole Centrale de Lyon (ECL)
 James Hutton Institute (JHI)
 Ministry of Public Security (MOPS/INT)
 Ministerio del Interior (GC)

COUNTRY

Israel
 France
 Denmark
 France
 United Kingdom
 Israel
 Spain

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

© Beboy - Fotolia.com


**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

CiaoTech Srl (CTECH)
 SESM Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l.
 GMVIS Skysoft, S.A.
 Consorzio Interuniversitario Nazionale per l'Informatica
 Technische Universität München (TUM)
 INNOSTART Nemzeti Uzleti es Innovacios Kozpont Alapítvány
 Honeywell, spol. s r.o.
 Instituto Nacional de Tecnica Aeroespacial
 Fundación madrimasd para el Conocimiento
 ELSAG Datamat S.p.a.
 PNO Consultants S.A.S.

COUNTRY

Italy
 Italy
 Portugal
 Italy
 Germany
 Hungary
 Czech Republic
 Spain
 Spain
 Italy
 France

P-REACT / Petty cRiminality diminution through sEarch and Analysis in multi-source video Capturing and archiving plaTform



Information

Grant Agreement N°

607881

Total Cost

€1,893,606

EU Contribution

€1,489,396

Starting Date

01/04/2014

Duration

24 months

Coordinator

FUNDACIÓN CENTRO DE TECNOLOGÍAS DE INTERACCIÓN VISUAL Y COMUNICACIONES VICOMTECH (VICOM)

Security Projects

Paseo Mikeletegi 57

20009 – Donostia / San

Sebastián – Spain

Contact

Juan Arraiza

Tel: +34 943 30 92 30

Fax: +34 943 30 93 93

E-mail:

security@vicomtech.org

Website:

www.vicomtech.org

Project objectives

P-REACT aims to:

- » design and develop a cost-effective solution for petty crime detection, response, investigation and analysis;
- » deliver novel video and audio analytics to detect petty crime incidents and develop crime reporting and analysis solutions to strengthen decision-making and responses;
- » design and develop a novel, cloud-based Video Content Management System (VCMS) that is capable of being delivered as a service;
- » exploit the use of semantic technologies to aid crime analysis and mapping which will help forecast, prevent and detect future petty crimes;
- » analyse technical barriers in the standardisation and scalability of the technologies and to ensure that any societal, ethical and legal issues are properly balanced and addressed;
- » Organise the demonstration, validation and evaluation of the proposed system according to defined user scenarios.

Description of the work

The P-REACT project will design and develop a low cost surveillance platform that will ensure communication between key users with a focus on increasing the ability of on the ground police and security personnel to respond. The solution will encompass intelligent video and audio sensors to detect petty crime incidents and a cloud-based monitoring, alert detection and storage platform.

An incident detected by sensors will initiate a work flow including alerting relevant Security Personnel and/ or police with the relevant video and intelligence information, ensuring the appropriate response. The solution will encourage community participation in the reporting of petty crime and as such will be designed to receive information (images, video) captured by mobile smart devices or unconnected surveillance system.

Expected results

1. Intelligent management of multi-sources camera and sensors (IR, depth, etc.) through embedded systems.
2. Light visual and video analytics at the embedded system level.
3. The development of novel cloud service Video Surveillance as a Service (VSaaS) for the video archive integration.
4. The development of a video platform which small business can report incidents and upload relevant video footage from surveillance systems or mobile devices.
5. Assure the privacy and the security of the surveillance data.
6. Security framework ensuring the data privacy, data protection and access level control to the P-REACT system.
7. Present trials in real conditions based on pragmatic scenarios.

PARTNERS

Fundación centro de tecnologías de interacción visual y comunicaciones Vicomtech (VICOM)
 Kinesense Limited (KS)
 Aditess Advanced Integrated Technology Solutions & Services (ADI)
 Future Intelligence LTD (FINT)
 Center for Research and Technology Hellas (CERTH)
 Center for Security Studies (KEMEA)
 Società Reti e Mobilità SRL (SRM)

COUNTRY

Spain
 Ireland
 Cyprus
 United Kingdom
 Greece
 Greece
 Italy

ROSFEN / Rapid On-site Forensic Analysis of Explosives and Narcotics

© ROSFEN



Information

Grant Agreement N°

321829

Total Cost

€1,997,635

EU Contribution

€1,420,262

Starting Date

01/04/2013

Duration

24 months

Coordinator

University College Cork,
National University of
Ireland, Cork, Tyndall
National Institute (Tyndall-UCC)

Tyndall National Institute

Lee Maltings,

Dyke Parade, Cork,

Ireland

Contact
Aidan Quinn

Tel: +353 21 490 4424

E-mail: aidan.quinn@

tyndall.ie

Website: www.tyndall.ie

Project objectives

Forensic analysis is an essential resource in the battle against organised crime and terrorist attacks. A key challenge in forensics is the detection of trace explosive residues at a post-blast scene or on the hands or clothes of an alleged suspect. Detection of the high-explosive primer charge (e.g., Pentaerythritol tetranitrate, PETN) is often hampered by higher-concentration residues from the main charge, e.g., ammonium nitrate. Detection of the primer can be essential in order to secure a prosecution, especially if the materials that comprise the main charge are commonly available, e.g., ammonium nitrate is present in fertiliser.

ROSFEN's goal is to deliver an advanced forensic platform for rapid, on-site direct detection and lab-quality analysis of narcotics, explosives and their precursors. The ROSFEN platform is based on a novel chip-based triple quadrupole mass spectrometer with an advanced front-end ion filter and a sample introduction/pre-concentration module. The performance targets are detection limits down to 1 ng/mL for the ion-filtered mass spectrometer with 1 % false alarm rate. The response time target is < 10 seconds for a single scan with < 30 minutes set-up time.

The field-deployable ROSFEN platform will be a fraction of the size, power consumption and weight of 'state of the art' lab-based tandem mass spectrometer products, with a target weight of 40 kg; power consumption of 450 W and size of 35 cm (W) × 70 cm (L) × 35 cm (H).

Description of the work

ROSFEN will focus on design and development of

- » Field-deployable, chip-based tandem mass spectrometer (MS) system with in-line ion filter (FAIMS-AIMS2) for on-site direct analysis of narcotics, explosive compounds and precursor materials.
- » Macromolecules and high-surface area templates for molecular recognition-based "trapping" of explosive compounds.
- » Modules for sample introduction, vapour collection and multi-pass analyte recycling
- » The performance of the system will be assessed in a forensic analysis laboratory by forensics experts and also in a secure "real-world" proving ground by crime-scene officers.

Expected results

ROSFEN will enable reduction of total analysis time (samples, blanks, controls) for explosives and narcotics from more than 8 hours to just minutes, thus reducing the work load on forensic labs and enabling faster intelligence-led investigations.

ROSFEN will thus enable European industry to develop and deliver innovative technologies into key global markets: Analytical instruments for security applications (\$2 billion annually) and the \$3.3B market for mass spectrometry.

PARTNERS

University College Cork, National University of Ireland, Cork, Tyndall National Institute (Tyndall-UCC)
 Microsaic Systems (Microsaic)
 Environics OY (Environics OY)
 Universitaet Basel (UNIBAS)
 Department of Justice Northern Ireland, Forensic Science Northern Ireland (FSNI)
 Police Service of Northern Ireland (PSNI)

COUNTRY

Ireland
 United Kingdom
 Finland
 Switzerland
 United Kingdom
 United Kingdom

SMARTPREVENT / Smart Video-Surveillance System to Detect and Prevent Local Crimes in Urban Areas



Information

Grant Agreement N°

606952

Total Cost

€1,943,448.00

EU Contribution

€1,499,995.50

Starting Date

01/03/2014

Duration

24 months

Coordinator

TREELOGIC TELEMÁTICA Y LÓGICA RACIONAL PARA LA EMPRESA EUROPEA SL (TREELOGIC)

R&D Department

Parque Tecnológico de

Asturias, Parcela 30

33428- Llanera- Asturias

(Spain)

Contact

SERGIO GARCÍA ÁLVAREZ

Tel: +34 985 966 136

E-mail: [sergio.garcia.alvarez@](mailto:sergio.garcia.alvarez@treelogic.com)

treelogic.com

Website:

www.smartprevent.eu

Project objectives

The SmartPrevent project focuses on the detection and prevention of frequent petty crimes that are of high impact to local communities and citizens in urban scenarios, considered to be a low-cost video-surveillance system oriented to end-users.

The objectives of SmartPrevent project are:

- » Detection of crime on persons and local businesses in urban areas;
- » Crime prevention over persons and local businesses in urban areas;
- » Video-surveillance system oriented for end-users.
- » Video-surveillance system as an effective and efficient punitive tool that protects people's privacy;
- » Temporal and spatial adaptability;
- » Low-cost video-surveillance system.

Description of the work

The increase of criminal activity is manifested in an increased frequency of small crimes like graffiti, theft, robbery, and destruction of rubbish bins. This has had a big impact for local governments, citizens and businesses.

Current video-surveillance systems in urban scenarios are very limited and only consist of a presentation of visual information captured by the visual sensors network, not oriented to end-users, limiting their capacity to help and prevent the criminal activity. Furthermore, the visual-surveillance systems usually do not have any automatic process to store the most relevant evidence to be used in the legal punitive process of criminals.

SmartPrevent will address this challenge by:

- » Studying the characteristics of frequent criminal activities in real urban scenarios including typical variations and unanticipated criminal situations;
- » Developing a low-cost, adaptable video-surveillance system in order to detect and prevent criminal activities;
- » Building a video-surveillance system that functions as a punitive tool in order to store the most relevant evidence of the detected criminal activities.

Rather than providing new methodologies or tools, SmartPrevent will focus on: a) improving already-existing methodologies by means of a set of guidelines for the use of video-surveillance systems; and b) providing a set of tools capable to improve the existing crime detection systems. Our solution will be validated by deploying a realistic prototype scenario, which will actively involve the detection and prevention of crimes in urban areas and the management of these detections by final users.

Expected results

We will develop and provide four important benefits: i) Systematic characterization of usual petty crimes in an area under automatic surveillance; ii) automatic detection of the most usual and frequent criminal activities; iii) a set of automated tools capable of alerting the appropriate responders; and iv) early prevention of crimes by prediction and early detection of crimes.

PARTNERS

Treelogic Telemática Y Lógica Racional para la Empresa Europea SL (TREELOGIC)
Queen Mary and Westfield College, University of London (QMUL)
Vision Semantics Limited (VSL)
Emza Visual Sense Ltd (EVS)
Ayuntamiento de Las Rozas de Madrid (ALR)
Ankara Strateji Enstitüsü Derneği (ASED)

COUNTRY

Spain
United Kingdom
United Kingdom
Israel
Spain
Turkey

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

© Fotofia.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

Commissariat à l'énergie atomique (CEA-LIST)
 European Aeronautics Defence and Space Company EADS France SAS
 Astrium SAS
 Finmeccanica- Societa Per Azioni
 Morpho (SGM)
 Thales avionics SA
 Österreichisches Forschung- und Prüzzentrum Arsenal GesmbH
 Totalförsvarets Forskningsinstitut (FOI)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 Valtion Teknillinen Tutkimuskeskus (VTT)
 European Materials research society
 Tübitak Marmara research centre information technology institute
 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
 Stiftelsen SINTEF
 Fundación Robotiker
 Fondation pour la Recherche Stratégique
 Istituto Affari Internazionali
 European Commission - Joint Research Centre (JRC)
 European Biometrics forum limited
 Association française de normalisation
 Ministère de l'intérieur
 Center for Security Studies
 AIT Austrian Institute of Technology GmbH (AIT)

COUNTRY

France
 France
 France
 Italy
 France
 France
 Austria
 Sweden
 The Netherlands
 Finland
 France
 Turkey
 Germany
 Norway
 Spain
 France
 Italy
 Belgium
 Ireland
 France
 France
 Greece
 Austria

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.vandenbergh@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

COMITÉ EUROPÉEN DE NORMALISATION (CEN)
 AREVA T&D SA (Areva)
 Enginet srl (EngiNet)
 UNINFO - Associazione di Normazione Informatica (UNINFO)
 OPUS PUBLISHING GENERAL PARTNERSHIP (OPUS)
 COMPANIA NATIONALA DE TRANSPORT AL ENERGIEI ELECTRICE TRANSELECTRICA SA (Transelectrica)
 ENEL PRODUZIONE. S.P.A. (ENEL)
 MEDITERRANEA DELLE ACQUE S.p.A. (Med-d-Acque)
 SIEMENS AG (Siemens)
 European Commission - Joint Research Centre (JRC)
 ABB SCHWEIZ AG (ABB)
 Enel Ingegneria e Innovazione SpA (ENEL spa)

COUNTRY

Belgium
 France
 Italy
 Italy
 United States
 Romania
 Italy
 Italy
 Germany
 Belgium
 Switzerland
 Italy

ETCETERA / Evaluation of critical and emerging technologies for the elaboration of a security research agenda



Information

Grant Agreement N°

261512

Total Cost

€1,996,728

EU Contribution

€1,512,742

Starting Date

01/10/2011

End Date

30/09/2013

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 indispensable 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).

**RESEARCH
COMPLETED**

Results

Several new approaches for research planning have been developed and analysed. Among these is an enhanced and novel technology scanning method based on three established techniques. Other methods applied and compared were participatory processes and technical approaches utilising scientific metrics. Based on this broad methodological framework, tentative results concerning the development of research agendas to overcome critical dependencies and to harness opportunities of emerging technologies were developed. Ethical aspects have been taken into account at all levels of the project. The final report is available at www.etcetera-project.eu

PARTNERS

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Totalförsvarets Forskningsinstitut (FOI)
 Fundación Tecnalia Research & Innovation (Tecnalia)
 Ingeniería de Sistemas para la Defensa de España, S.A. (Isdefe)
 Universität Duisburg-Essen (UDE)
 AIT Austrian Institute of Technology GmbH (AIT)
 Commissariat à l'énergie atomique et aux énergies alternatives (CEA)
 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
 VDI Technologiezentrum GmbH (VDI-TZ)
 Morpho (MPH)
 Ansaldo STS S.p.A. (ASTS)
 COMSEC Unternehmensgruppe (COMSEC)
 Centre for Science, Society and Citizenship (CSSC)
 Storstockholms brandförsvär (SSBF)

COUNTRY

Germany
 Sweden
 Spain
 Spain
 Germany
 Austria
 France
 The Netherlands
 Germany
 France
 Italy
 Germany
 Italy
 Sweden

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 work-packages (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

Serviços de Consultadoria em Inovação Tecnológica, S.A. (INOVAMAS)
 Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)
 Deutsche Post World Net Market Research and Innovation GmbH (DHL Innovation Center)
 INNOVA SPA
 SOLLERTA Ltd
 FUNDACION ROBOTIKER
 Mr. Juergen K. von der Lippe and Dr. Jean Cornier
 UNIVERSITATEA DIN CRAIOVA
 ALMA CONSULTING GROUP SAS
 TECHNICAL SUPPORT FOR EUROPEAN ORGANISATIONS SPRL
 SOUTHEASTERN EUROPE TELECOMMUNICATIONS & INFORMATICS RESEARCH INSTITUTE

COUNTRY

Portugal
 Germany
 Germany
 Italy
 United Kingdom
 Spain
 Germany
 Romania
 France
 Belgium
 Greece

STRAW / Security Technology Active Watch



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@

atosresearch.eu

Project objectives

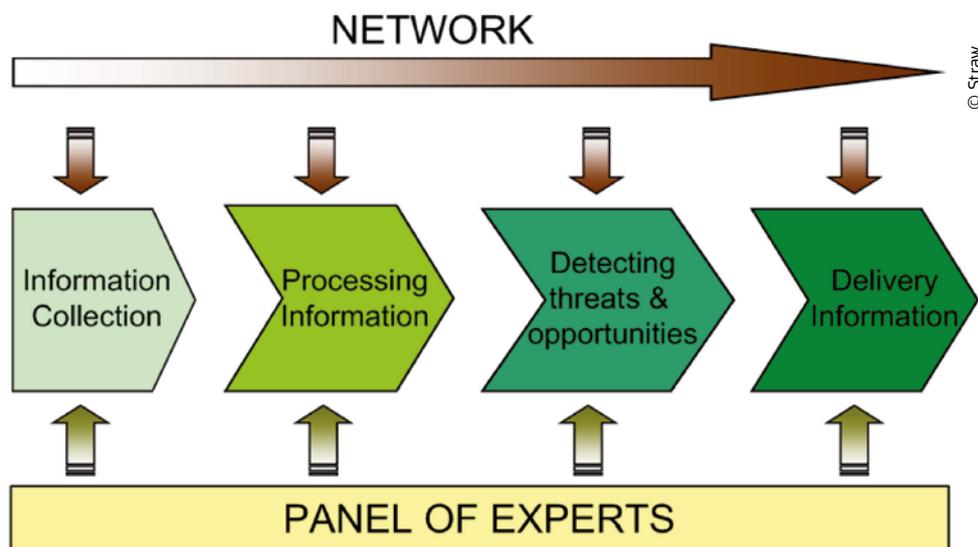
The STRAW project aimed to enhance European civil security by facilitating cooperation amongst various stakeholders, including researchers, technology providers and end-users.

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.



PARTNERS

Atos Origin SAE
Aerospace and Defence Industries Association
Thales Services
Stiftelsen 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

DITAC / Disaster Training Curriculum

© Arkadi Bojar-Ujrov - 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: +49 1607234539

Mobile: +49 1607234539

Fax: +49 1607234539

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

University Clinic Bonn Germany (UKB)
 Prehospital and Disaster Medicine Centre (PKMC)
 Hanover Associates (HA)
 Center for Research in Emergency and Disaster Medicine (CRIMEDIM)
 Clinical Emergency Hospital Bucharest (URGENTA)
 Nations Health Career School of Management gGmbH (NHSC)
 General and Teaching Hospital Celje (SBC)
 Istanbul Aydin University (AFAM)
 Croatian urgent medicine and surgery association (CROUMSA)
 German Aerospace Center (DLR)
 Bonn International Center for Conversion (BICC)
 GABO:mi Gesellschaft für Ablauforganisation:milliarium mbH & Co. KG (GABO)

COUNTRY

Germany
 Sweden
 England
 Italy
 Romania
 Germany
 Slovenia
 Turkey
 Croatia
 Germany
 Germany
 Germany

LEILA / Law Enforcement Intelligence Learning Applications



Information

Grant Agreement N°

608303

Total Cost

€1,978,327.45

EU Contribution

€1,499,837.00

Starting Date

01/04/2014

Duration

24 months

Coordinator

GLOBO TECHNOLOGIKI - PLIROFORIKI ANO- NYMI ETAIREIA, IDIOTIKI EPICHEIRISI PAROCHIS YPIRESION ASFALIAS

R&D

37 A Psaron str.

152 32 – Halandri – Greece

Contact

Manos Foufoudakis

Tel: +30 2121217216

Mobile: +30 6936660395

Fax: +30 2106466165

E-mail: mfoufoudakis@

globogr.com

Website:

www.leila-project.eu

Project objectives

Intelligence analysis (IA) professionals are faced with daily challenges to meet high demands for rapid, accurate assessments that require discovery and marshalling of evidence, integration and synthesis of data from disparate sources, interpreting and evaluating information that is constantly changing, and providing documentation and recommendations (intelligence products).

The definition of the new competences and skills needed by the next generation of intelligence analysts is crucial to the design of effective learning curricula that can better address the training needs of law enforcement agents.

The emerging learning model for intelligence analysis should integrate methodologies and tools designed to improve critical thinking, awareness of cognitive biases, improved capabilities in filtering and analyzing massive amount of data (even available online and in different languages), decision making under social and time pressure, collaboration skills, creative intelligence, reporting and communication skills.

The aim of the LEILA project is to provide law enforcement organizations with innovative learning methods to address the improvement of intelligence analysis in regards to the aforementioned capabilities and skills.

The radical innovation of the LEILA holistic approach is due to the combination of several fields which are normally explored and applied separately, such as:

- » psycho-sociological and cognitive factors in decision making (e.g. decision biases, critical thinking, multiple reasoning strategies, creativity);
- » decision making strategies under uncertainty (e.g. Bayesian approaches, game theory);

» group interaction dynamics in intelligence analysis.

A variety of learning experiences (e.g. games of deterrence, intelligence analysis under stress, emergence in highly collaborative situations) are simulated and computerized in different games that offer the possibility to actively acquire the new IA skills from different angles.

To reach these aims, the project evolves towards three research outcomes:

1. Analyze and describe the specific skills and competences of the intelligence analysts by exploring different characteristics and abilities and identifying learning needs and areas of improvement;
2. Design an innovative methodology and a set of learning experiences to address the specific needs of intelligence analysts;
3. Develop and validate a set of serious games that enable trainees to acquire the skills and competencies requested by their role.

Description of the work

The work plan is based on an iterative and action oriented user-centric approach that involves different actors and guarantees the substantive quality of the technological research. More specifically, the different participants include end-users, domain experts, cognition specialists, educational experts, and technological and learning game designers, allowing for each actor to bring its particular competence to the project. The LEILA project covers both the practical and theoretical perspectives in an interrelated manner.

Expected results

The expected results of LEILA project is to provide the trainee with a comprehensive and consistent set of tools enabling him/her to appropriately analyze available data, search for extra data, transform raw data into meaningful information with respect to the case under consideration, and draw conclusions about this case, as well as to support all enabling factors that help the trainee to accomplish the task efficiently.

PARTNERS

GLOBO TECHNOLOGIES SA
ORT France
Alphalabs Sarl
Zanasi & Partners
FVA New Media Research
National Defense University CAROL I
Center for Security Studies

COUNTRY

Greece
France
France
Italy
Italy
Romania
Greece

SAFECITI / Simulation Platform for the Analysis of Crowds Behaviour in Urban Environments with Training and Predictive Capabilities



Information

Grant Agreement N°

607626

Total Cost

€1,899,049.28

EU Contribution

€1,442,733.96

Starting Date

01/03/2014

Duration

24 months

Coordinator

NEXT LIMIT S.L (NL)

SAFECITI

Calle Angel Cavero 2

28043 Madrid (Spain)

Contact

Victor Gonzalez

Tel: +34 917 160 214

Fax: +34 917 219 464

E-mail:

safeciti@nextlimit.com

Website:

www.nextlimit.com

Project objectives

The SAFECITI project proposes the creation of a simulation system for police intelligence analysts to predict the behaviour of crowds in urban environments under specific threats or stresses (e.g. turmoil, violence, panic, catastrophes or terrorism) to train officers and develop better safety plans and tactic operations.

This platform will be designed both as a simulation platform for training purposes and as a predictive tool for operational use. The platform will include performance measurement tools based on safety goals (people and infrastructure damage) to measure the skills of the analyst. All the simulations will be stored in a database to work as a historic repository but also, more interestingly, as a large set of useful data to be re-analyzed by artificial intelligence algorithms to create predictive models. The main goal of this predictive model will be the creation of a virtual analyst that is able to recommend actions based on the enriched analysis of hundreds or thousands of simulations.

Description of the work

The development of the simulation platform involves several technological challenges that will be covered in the work plan:

- » Requirements and specifications: definition of the specifications mainly driven by end user requirements; serious game technology selection; requisite verification methodology;
- » Interactive graphical platform, interfaces and control system: development of the main control system, integration of all the modules in the interactive platform; user interfaces; scene setup; interactive workflow, control and network modules;
- » Graphics components: 3D models for human representation, static and dynamic versions, 3D vehicles and graphics optimization;
- » Generation of urban environment: development of urban generation module (as the project aims to simulate realistic environments);
- » Advanced crowd simulation: design and development of the crowd simulation engine that initializes and updates the entities, their behaviours and their actions on the environment;
- » Database module and predictive model: development of database components and predictive models, which provide a very powerful tool for expanding the framework of the project beyond classic e-learning;
- » System validation: validation of the system. Field expertise by the Spanish national police department will help to validate and test the system.

Expected results

SAFECITI will not only improve the training methodologies and performance measurement of the analysts, but will create an innovative profile for new-generation analysts who will be trained in a first stage and operate the system later during their whole operational life, thus helping to enrich the system with new simulations and validation cases. These new analysts will be able to project new operational plans in advance by simulating “what-if” cases in complex scenarios, and anticipating threats.

The main expected impacts of SAFECITI are:

- » improvements in the safety of citizens against different threats;
- » threat anticipation and adequate response through planning;
- » development of next-generation intelligence analysts;
- » technologies and services for new SMEs’ business development.

PARTNERS

Next Limit S.L. (NL)
 Griffin Software SRL (GR)
 Golaem S.A. (GO)
 ESRI R&D Center Zurich AG (ESRI)
 Politecnico di Torino (POLITO)
 Ministerio del Interior (MIR-DGP)

COUNTRY

Spain
 Romania
 France
 Switzerland
 Italy
 Spain

LIST OF PROJECTS

3D-FORENSICS	510	CREATIF	12
A4A	288	CRESCENDO	524
ABC4EU	212	CRIM-TRACK	108
ACRIMAS	330	CRISCOMSCORE	300
ACXIS	214	CRISIS	302
ADABTS	190	CRISMA	304
ADDPRIV	436	CRISP	404
ADVISE	376	CRISYS	344
AEROCEPTOR	78	CUSTOM	98
ALTERNATIVE	438	CWIT	140
AMASS	248	DARIUS	346
ANTIBOTABE	268	D-BOX	44
ANVIL	410	DECOTESSC1	14
ARCHIMEDES	484	DEMASST	142
ARENA	192	DESSI	460
ARGOS	194	DESTRIERO	336
ARGUS 3D	210	DESURBS	124
ASSERT	456	DETECTOR	442
ATHENA	412	DIRAC	100
AVERT	38	DISASTER	380
BASYLIS	196	DITAC	536
BEAT	370	DITSEF	144
BESECU	290	DOGGIES	218
BESECURE	476	E-CRIME	114
BIO-PROTECT	6	EDEN	16
BONAS	40	EFFISEC	220
BOOSTER	270	ELITE	348
BRIDGE	292	EMERGENT	418
C2-SENSE	378	EMILI	306
CAERUS	332	EMPHASIS	46
CAMINO	110	ENCOUNTER	48
CAPER	94	EPOOLICE	462
CASCEFF	294	EQUATOX	406
CASSANDRA	250	ESC	526
CAST	296	ESCORTS	528
CATO	272	ESENET	382
CBRNEMAP	8	E-SPONDER	350
CIPRNET	494	ESS	352
CLOSEYE	252	ETCETERA	530
COBACORE	334	ETTIS	464
COCAE	10	EULER	392
COCKPITCI	112	EURACOM	146
COMMONSENSE	42	EUROFORGEN - NOE	496
COMPOSITE	458	EUROSKY	148
CONPHIRMER	96	EU-SEC II	486
CONSORTIS	216	EUSECON	478
CONTAIN	242	EVACUATE	354
COPE	298	EVIDENCE	80
COPRA	138	FASTID	356
COREPOL	440	FASTPASS	222
COSMIC	414	FESTOS	466
COUNTERFOG	274	FIDELITY	224
CPSI	416	FOCUS	468

FORCE	470	ODYSSEY	88
FORESEC	472	OPARUS	238
FORLAB	50	OPERAMAR	256
FORTRESS	372	OPSIC	312
FREESIC	394	OPTI-ALERT	314
FRESP	276	OPTIX	58
GAMMA	150	OSMOSIS	516
GERYON	396	P5	204
GLOBE	244	PACT	446
GRAFFOLUTION	512	PANDORA	160
HANDHOLD	226	PARIS	424
HARMONISE	126	PEP	362
HELP	338	PERSEUS	258
HEMOLIA	102	PLANTFOODSEC	498
HIT-GATE	398	POP-ALERT	316
HOMER	52	PPDR-TC	400
HYPERION	54	PRACTICE	286
HYRIM	116	P-REACT	518
I2C	254	PREDICT	318
ICARUS	358	PREEMPTIVE	118
IDETECT 4ALL	198	PREVAIL	60
IDIRA	308	PRISMS	448
IFREACT	278	PROMERC	186
IMCOSEC	180	PROTECTRAIL	162
IMPACT EUROPE	420	PSYCRIS	320
IMSK	68	RAPTOR	70
INDECT	200	RECOBIA	426
INDIGO	310	RECONASS	340
INEX	444	REDIRNET	374
INFRA	152	REWARD	22
INGRESS	228	RIBS	128
INNOSEC	488	ROSFEN	520
INSEC	490	S(P)EEDKITS	368
IPATCH	182	SAFECITI	540
ISAR+	422	SAFE-COMMS	342
ISIS	18	SAFEPOST	188
ISITEP	384	SAFEWATER	24
ISTIMES	154	SAFIRE	428
L4S	156	SALIENT	62
LEILA	538	SALUS	386
LINKSCH	82	SAMURAI	206
LOGSEC	184	SAPIENT	450
LOTUS	56	SAVASA	388
MEPROCS	84	SAVELEC	90
MIDAS	86	SAVEMED	104
MIRACLE	280	SAWSOC	120
MISAFE	514	SCIIMS	106
MODES_SNM	20	SCINTILLA	26
MOSAIC	202	SEABILLA	260
MULTIBIDOSE	282	SECCRIT	122
MULTISENSE CHIP	284	SECONOMICS	480
NI2S3	158	SECRICOM	402
NMFRDISASTER	360	SECTRONIC	164

LIST OF PROJECTS

SECUREAU	28	VOX-POL	508
SECURECHAINS	532	WIMAAS	266
SECUR-ED	130	XP-DITE	178
SECURENV	322		
SEREN	500		
SEREN2	502		
SERON	166		
SESAME	168		
SGL FOR USAR	364		
S-HELP	324		
SIAM	474		
SICMA	326		
SLAM	408		
SLANDAIL	430		
SMART	452		
SMARTPREVENT	522		
SMARTPRO	92		
SNIFFER	30		
SNIFFER	230		
SNIFFLES	232		
SNOOPY	234		
SNOWBALL	328		
SOURCE	504		
SPARKS	170		
SPARTACUS	366		
SPICED	32		
SPIRIT	132		
STAR-TRANS	172		
STRAW	534		
STRUCTURES	174		
SUBCOP	64		
SUBITO	208		
SUNNY	240		
SUPER	432		
SUPPORT	262		
SURPRISE	454		
SURVEILLE	434		
TACTICS	72		
TALOS	246		
TASS	176		
TAWARA_RTM	34		
TERASCREEN	236		
THE HOUSE	492		
TIRAMISU	66		
TRITON	264		
TWOBIAS	36		
UNCOSS	74		
UNSETH	390		
VALUESEC	482		
VASCO	134		
VIDEOSENSE	506		
VIRTUOSO	76		
VITRUV	136		

European Commission

Luxembourg: Publications Office of the European Union, 2014

2014 — 548 pp. — 21 cm x 29.7 cm

ISBN 978-92-79-43792-2
doi:10.2769/52221

*Security Research Projects
under the 7th Framework Programme for Research*

EU Research for a Secure Society

Further information available at: <http://ec.europa.eu/dgs/home-affairs/innovation-and-industry/>

