SECURITY RESEARCH PROJECTS
under the 7th Framework Programme for Research

Investing into security research for the benefits of European citizens

September 2011
INTRODUCTION

Under its wider R&D budget for 2007-2013 – known as the Seventh Framework Programme for Research (FP7) – the EU is investing EUR 1.4 billion for security research. This catalogue presents an exhaustive overview of all projects currently supported by FP7’s Security Research budget as of July 2011.

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 equipments, systems and knowledge – the EU can better understand and prepare itself to face risks and disruptive events in a constantly changing world.

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

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

Further information is available at:


Prepared by the European Commission, Directorate-general Enterprise and Industry, Unit H4 Security Research and Development,

E-mail: entr-security-research@ec.europa.eu
TABLE OF CONTENTS

Introduction .................................................. 1
Table of contents ........................................... 3

Security of the citizens ........................................ 4
  BIO-PROTECT ........................................... 4
  CAPER ................................................... 6
  CBRNemap ............................................... 8
  COCAE .................................................. 10
  CommonSense ............................................ 12
  CONPHRMER ............................................ 14
  CUSTOM .................................................. 16
  DIRAC ..................................................... 18
  HEMOLIA ............................................... 20
  INDECT .................................................. 22
  LOTUS ..................................................... 24
  MIDAS ..................................................... 26
  ODYSSEY ............................................... 28
  OPTIX ..................................................... 30
  PREVAL ................................................... 32
  RAPTOR .................................................... 34
  SALIANT .................................................. 36
  SaveMed .................................................. 38
  SCIMS ..................................................... 40
  TOBIAS ................................................... 42
  UNCOSS .................................................... 44

Security of infrastructures and utilities ..................... 46
  ADABTS ................................................. 46
  ARENA .................................................... 48
  BASYLIS .................................................. 50
  COPRA ..................................................... 52
  DEMASST ............................................... 54
  DESURBS ............................................... 56
  EMILI ..................................................... 58
  EURACOM ............................................... 60
  iDetect-4All ............................................ 62
  INFRA ..................................................... 64
  ISTIMEI ................................................... 66
  MOSAIC .................................................... 68
  Ni253 ..................................................... 70
  PROTECTRAIL ........................................... 72
  RIBS ....................................................... 74
  SAMURAI .................................................. 76
  SECTRONIC .............................................. 78
  SECUR-ED ................................................ 80
  SeRoN ..................................................... 82
  SESAMIE ................................................... 84
  STAR-TRANS ........................................... 86
  SUBITO ..................................................... 88
  TASS ....................................................... 90
  VITRUV .................................................... 92

Intelligent surveillance and border security .................. 94
  AMASS ..................................................... 94
  ARGUS 3D .................................................. 96
  CASSANDRA ............................................. 98
  EFFSEC .................................................... 100
  GLOBE ..................................................... 102
  I2C ......................................................... 104
  IMOSSEC .................................................... 106
  LOGSEC .................................................... 108
  OPARUS .................................................... 110
  PERSEUS ................................................... 112
  SEABILLA .................................................. 114
  SUPPORT ................................................... 116
  TALOS ....................................................... 118
  VIRTUOSO ................................................ 120
  WIMA’S ..................................................... 122

Restoring security and safety in case of crisis ............... 124
  A4A ......................................................... 124
  ACRIMAS ................................................... 126
  AntiBotABE .............................................. 128
  BOOSTER ................................................. 130
  BRIDGE .................................................... 132
  COPE ....................................................... 134
  CRISIS ..................................................... 136
  CRISYS ..................................................... 138
  DISCOTESSCI ............................................ 140
  E-SPONDER .............................................. 142
  ESS ......................................................... 144
  FASTID ..................................................... 146
  FRESP ....................................................... 148
  IDIRA ....................................................... 150
  IMSK ......................................................... 152
  INDIGO ..................................................... 154
  L4S ......................................................... 156
  MULTIBIOODOSE .......................................... 158
  Multisense Chip .......................................... 160
  Opti-Alert ............................................... 162
  PANDORA .................................................. 164
  PLANTFOODSEC ......................................... 166
  PRACTICE ................................................ 168
  SecureEau ............................................... 170
  SecureNV ............................................... 172
  SGL for USaR ............................................ 174
  SICMA ..................................................... 176
  SPIRIT ..................................................... 178

Security systems integration, interconnectivity and interoperability ........................................... 180
  CREATIF ................................................... 180
  DITSEF ..................................................... 182
  EULER ...................................................... 184
  HELP ........................................................ 186
  SECRICOM ............................................... 188
  VIDEOSENSE .............................................. 190

Security and society ........................................... 192
  ADDPRW ................................................... 192
  BeSecu ..................................................... 194
  CAST ......................................................... 196
  COMPOSITE .............................................. 198
  CPSI ........................................................ 200
  CrisComScore ........................................... 202
  DRESS ....................................................... 204
  DETECTOR .................................................. 206
  EUSECON .................................................. 208
  FESTOIS .................................................... 210
  FOCUS ...................................................... 212
  FORESEC ................................................... 214
  INEX ......................................................... 216
  SAFE-COMMS ............................................. 218
  SAFIRE ..................................................... 220
  SAPIENT ..................................................... 222
  SIAM ......................................................... 224
  SMART ....................................................... 226
  ValueSec ................................................... 228

Security Research coordination and structuring .............. 230
  CRESCENDO .............................................. 230
  ESC ........................................................ 232
  ESCoRTS .................................................. 234
  EU-SEC II .................................................. 236
  NMFRDisaster ............................................ 238
  OPERAMAR ............................................... 240
  OSMOSIS ................................................... 242
  SecureCHAINS ............................................ 244
  SEREN ...................................................... 246
  SEREN2 .................................................... 248
  STRAW ....................................................... 250
**Project objectives**

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

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

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

The concept of BIO-PROTECT is the development of a fast-alert, easy-to-use device for detection and identification of airborne bacteria, spores, viruses and toxins. It is based on bioaerosol detection by fluorescence, scattering and background aerosol properties to detect presence of potentially harmful biological agents in ambient air and to trigger further identification.

**Description of the work**

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

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

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

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

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

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

**Expected results**

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

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

Acronym: BIO-PROTECT

Grant Agreement N°: 242306

Total Cost: € 3,954,812

EU Contribution: € 3,125,577

Starting Date: 01/06/2010

Duration: 36 months

Coordinator:

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

Contact:

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

Partners

NAME
LGI Consulting
AVSISTA
C-Tech Innovation Ltd
Environics Oy
CEA
Institut für Umwelt Technologien GmbH
Robert-Koch Institut
University of Aalborg

COUNTRY
France
Lithuania
United Kingdom
Finland
France
Germany
Germany
Denmark
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 Open, and optionally, Closed 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 (ETL), application workflow and Semantic Modelling of processes, legal and privacy limitations, will permit participating LEAs to share information, investigative and experiential knowledge. The CAPER platform will be built in close collaboration with the LEA users in order to fulfil their current and forthcoming needs. The project is clearly focused on the fusion and real validation of the existing state of the art, coupled with innovative new technologies, to solve current bottlenecks faced by LEAs.

Description of the work

The CAPER platform will consist of six core elements:

Open and Closed Data Sources: Multi-format, Multimedia and multimodal information from Open Sources, TV and Radio capture, and Information in closed legacy systems are the data sources to be mined and evaluated by CAPER.

Data Acquisition: Depending on the information source type, different acquisition patterns will be applied to ensure acquired information is the richest possible and 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. To be 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 interagency 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.
Information

Acronym: CAPER
Grant Agreement N°: 261712
Total Cost: € 7,157,120
EU Contribution: € 5,579,346
Starting Date: 1st of June 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/

Partners

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

Project objectives

The objectives of CBRNEmap are to:

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

Description of the work

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

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

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

Expected results

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

Acronym: CBRNEmap

Grant Agreement N°: 242338

Total Cost: € 1,662,022

EU Contribution: € 1,376,185

Starting Date: 01/06/2010

Duration: 16 months

Coordinator:
European CBRNE center at Umeå University
KBC Building
90187 UMEA
Sweden

Contact:
Agneta H. Plamboeck
E-mail: Agneta.Plamboeck@cbrnecenter.eu
Website: http://http://www.cbrnemap.org/

Partners

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

**Expected results**

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

**Acronym:**
COCAE

**Grant Agreement N°:**
218000

**Total Cost:**
€ 2,653,077

**EU Contribution:**
€ 2,037,610

**Starting Date:**
01/09/2008

**Duration:**
36 months

**Coordinator:**

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

**Contact:**

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

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological Educational Institute of Halkida (TEI)</td>
<td>Greece</td>
</tr>
<tr>
<td>Greek Atomic Energy Commission</td>
<td>Greece</td>
</tr>
<tr>
<td>Institute of Nuclear Physics, National Center for Scientific Research Demokritos</td>
<td>Greece</td>
</tr>
<tr>
<td>Oy Ajat Ltd</td>
<td>Finland</td>
</tr>
<tr>
<td>Freiburger Materialforschungszentrum, Albert Ludwigs Universität</td>
<td>Germany</td>
</tr>
<tr>
<td>Universidad Autonoma de Madrid, Departamento de Fisica de Materiales</td>
<td>Spain</td>
</tr>
<tr>
<td>Riga Technical University</td>
<td>Latvia</td>
</tr>
<tr>
<td>V.E. Lashkaryov Institute of Semiconductor Physics, National Academy of Sciences of Ukraine</td>
<td>Ukraine</td>
</tr>
<tr>
<td>Chernivtsi Yuri Fedkovych National University</td>
<td>Ukraine</td>
</tr>
</tbody>
</table>
CommonSense / Development of a Common Sensor Platform for the Detection of IED “Bomb Factories”

**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, 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 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.

**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.

- **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 radiation detection modules will also be developed.

- **Software Development and Networking**
  This WP focuses on the 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**
  The final WP focuses on the 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” proving ground.

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:
1. Development of modules for gas-phase detection of explosives with ppb sensitivity
2. Development of modules for water-phase detection of explosives with sub-ppm sensitivity.
3. Development of a small form factor low power gamma radiation sensor with <10% energy resolution and an energy range of 60keV to 2MeV.
4. Development of an intelligent learning network, using chemometric algorithm to teach itself to detect explosives and ignore interferents.
Information

**Acronym:**
CommonSense

**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, CORK
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@fp7projectcommonsense.eu
Website: www.fp7projectcommonsense.eu

---

**NAME**

University College Cork, National University of Ireland, Cork
Technion - Israel Institute Of Technology
The University Of Manchester
Alphasense Limited
Bundesanstalt Fuer Materialforschung und Pruefung
SensL Technologies Limited
Thales Communications S.A.
Police Service of Northern Ireland

**COUNTRY**

Ireland
Israel
United Kingdom
United Kingdom
Germany
Ireland
France
United Kingdom
CONPHIRMER / Counterfeit Pharmaceuticals Interception using Radiofrequency Methods in Realtime

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.

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.

© istockphoto.com
Information

**Acronym:**  
CONPHIRMER

**Grant Agreement N°:**  
261670

**Total Cost:**  
€ 3,794,807.80

**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

---

**NAME**

- 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)

**COUNTRY**

- United Kingdom  
- France/Germany  
- Slovenia  
- Sweden  
- United Kingdom  
- Poland
CUSTOM / Drugs and precursor sensing by complementing low cost multiple techniques

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

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

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

Description of the work
A drug precursor sensor demonstrator, implementing two main techniques will be developed:

» a low cost, high data throughput sensing technique, based on UV-Vis-NIR fluorescence which incorporates an array of different properly engineered chemical proteins able to bind the target analytes as happen in an ‘immuno-type’ reaction; and

» a highly sensitive and selective, compact and low weight, spectroscopic sensing technique in Mid-IR optical range, based on Laser Photo-Acoustic Spectroscopy (LPAS).

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

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

Acronym: CUSTOM

Grant Agreement N°: 242387

Total Cost: € 5,295,523

EU Contribution: € 3,486,406

Starting Date: 01/06/2010

Duration: 36 months

Coordinator:
SELEX SISTEMI INTEGRATI

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

Acronym: CUSTOM

Grant Agreement N°: 242387

Total Cost: € 5,295,523

EU Contribution: € 3,486,406

Starting Date: 01/06/2010

Duration: 36 months

Coordinator:
SELEX SISTEMI INTEGRATI

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

Name

SELEX Sistemi Integrati
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

**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 micro-machined GC columns, solid state lasers, and hollow fibres IR, will allow to develop a sensor that features hand-portability and prompt response –for field operation– and is capable to perform both bulk and trace analysis. The DIRAC sensor will further feature a) an advanced sampling device, that separates the analyte from larger amounts of materials by electrostatic charging; and, b), an advanced micro-machined pre-concentrator that treats sequentially both volatile ATS substances and non volatile ammonium salts.

**Description of the work**

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

- **Phase 1 (6 months), where requirements are reviewed;**
- **Phase 2 (24 months), where the sensor is developed together with its sensing modules, techniques and procedures;**
- **Phase 3 (12 months), where the sensor is tested, optimized and validated.**

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

**WPs active in phase 2 are:**

- **WP2**, where the sensing prototype is developed, with its strategies, procedures, and process controls
- **WP3**, that develops the sampling module, with its methods and procedures
- **WP4**, that develops the pre-concentration module, with its methods and procedures
- **WP5**, that develops the HF-IRAS module, with its methods and procedures
- **WP6**, that develops the GC separation and detection module, with its methods and procedures
- **WP7**, that develops the Expert System as a pattern recognition and learning machine.

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

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

**Expected results**

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

- Reliability (ability to reject interferents);
- Hand portability;
- Fast response (few minutes);
- Good sensitivity (tens of nano-grams or better);
- Broad chemical spread (sensitivity towards different drugs and precursors);
- Identification capacity, (ability to distinguish one target compound from another at least on a family base).
Information

Acronym: DIRAC

Grant Agreement N°: 242309

Total Cost: € 4,256,753.33

EU Contribution: € 2,987,717

Starting Date: 01/06/2010

Duration: 42 months

Coordinator:

CONSORZIO CREO
Centro Ricerche Elettro-Ottiche
SS 17 Localita Boschetto
L’Aquila 67100
Italy

Contact:

Sandro Mengali
Tel: +39-0862346210
Fax: +39-0862346201
Website: www.consortziocreo.it

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consorzio CREO- Centro Ricerche Elettro-Ottiche</td>
<td>Italy</td>
</tr>
<tr>
<td>Fraunhofer-Gesellschaft zur Foerderung der Angewandten Forschung E.V</td>
<td>Germany</td>
</tr>
<tr>
<td>Consiglio Nazionale delle Ricerche</td>
<td>Italy</td>
</tr>
<tr>
<td>EADS Deutschland GMBH</td>
<td>Germany</td>
</tr>
<tr>
<td>ELSAG DATAMAT S.p.A.</td>
<td>Italy</td>
</tr>
<tr>
<td>Universite de Lausanne</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Universitatea Dunarea de Jos Din Galati</td>
<td>Romania</td>
</tr>
<tr>
<td>Institut National de Criminalistiek en Criminologie</td>
<td>Belgium</td>
</tr>
<tr>
<td>National Bureau of Investigation</td>
<td>Finland</td>
</tr>
<tr>
<td>Consorzio Interuniversitario Nazionale per la Scienza e la Tecnologia dei Materiali</td>
<td>Italy</td>
</tr>
</tbody>
</table>
HEMOLIA / Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts

Project objectives

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

Description of the work

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

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

Expected results

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

Acronym: HEMOLIA

Grant Agreement N°: 261710

Total Cost: € 4,361,945

EU Contribution: € 2,979,390

Starting Date: 01/05/2011

Duration: 36 months

Coordinator:

VERINT SYSTEMS LTD.
—
33 Maskit St Herzliya,
46733 Israel
—

Contact: Gideon Hazzani
Tel.: +972 9 9622596
Phone: +972 9 9622596
Fax: +972 9 962 4747
E-mail: Gideon.Hazzani@verint.com
Website: http://verint.com/corporate/

---

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verint Systems Ltd.</td>
<td>Israel</td>
</tr>
<tr>
<td>MINISTRY OF JUSTICE</td>
<td>Denmark</td>
</tr>
<tr>
<td>OFICIUL NATIONAL DE PREVENIRE SI COMBATERE A SPALARII BANILOR</td>
<td>Romania</td>
</tr>
<tr>
<td>APLICACIONES EN INFORMATICA AVANZADA SA</td>
<td>Spain</td>
</tr>
<tr>
<td>CAPGEMINI NEDERLAND BV</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>ZWIAZEK BANKOW POLSKICH IZBA GOSPODARCZA</td>
<td>Poland</td>
</tr>
<tr>
<td>UNIWERSYTET WROCŁAWSKI</td>
<td>Poland</td>
</tr>
<tr>
<td>VERENIGING VOOR CHRISTELIJK HOGER ONDERWIJS WETENSCHAPPELIJK ONDERZOEK EN PATIENZORZ</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>SWITCHLEGAL ADVOCATEN</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>TELEKOMUNIKACJA POLSKA S.A.</td>
<td>Poland</td>
</tr>
<tr>
<td>Industrial Research Institute for Automation and Measurements PIAP</td>
<td>Poland</td>
</tr>
<tr>
<td>Ernst &amp; Young</td>
<td>Israel</td>
</tr>
</tbody>
</table>
Project objectives

The main objectives of the INDECT project are:

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

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

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

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

Description of the work

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

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

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

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

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

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

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

Expected results

The main expected results of the INDECT project are:

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

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

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

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

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

Acronym: INDECT

Grant Agreement N°: 218086

Total Cost: € 14,863,988

EU Contribution: € 10,906,984

Starting Date: 01/01/2009

Duration: 60 months

Coordinator:

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

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGH – University of Science and Technology</td>
<td>Poland</td>
</tr>
<tr>
<td>Apertus</td>
<td>Hungary</td>
</tr>
<tr>
<td>Gdansk University of Technology</td>
<td>Poland</td>
</tr>
<tr>
<td>InnoTec DATA GmbH &amp; Co. KG</td>
<td>Germany</td>
</tr>
<tr>
<td>IP Grenoble (Ensimag)</td>
<td>France</td>
</tr>
<tr>
<td>MSWiA – General Headquarters of Police (Polish Police)</td>
<td>Poland</td>
</tr>
<tr>
<td>Moviquity</td>
<td>Spain</td>
</tr>
<tr>
<td>Products and Systems of Information Technology</td>
<td>Germany</td>
</tr>
<tr>
<td>Police Service of Northern Ireland</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Poznan University of Technology</td>
<td>Poland</td>
</tr>
<tr>
<td>Universidad Carlos III de Madrid</td>
<td>Spain</td>
</tr>
<tr>
<td>Technical University of Sofia</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>University of Wuppertal</td>
<td>Germany</td>
</tr>
<tr>
<td>University of York</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Technical University of Ostrava</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Technical University of Kosice</td>
<td>Slovakia</td>
</tr>
<tr>
<td>X-Art Pro Division G.m.b.H.</td>
<td>Austria</td>
</tr>
<tr>
<td>Fachhochschule Technikum Wien</td>
<td>Austria</td>
</tr>
</tbody>
</table>
LOTUS / Localisation of Threat Substances in Urban Society

Project objectives

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

The LOTUS project aims to create a system by which illicit production of explosives and drugs can be detected during the production stage rather than preventing terrorist attacks while they are already in motion, which is extremely difficult. The LOTUS concept is aimed at detecting chemical signatures over a wide urban area. The detectors may be placed at fixed positions although most detectors should be mobile. These distributed detectors continuously sample air while its carrier performs its daily work. When a suspicious substance is detected in elevated amounts, information about the type, location, amount and time is registered and sent to a data collection and evaluation centre for analysis. Several indications in the same area will trigger an alert, enabling law enforcement agencies to further investigate and respond on.

Description of the work

The goal of LOTUS is to use an innovative approach to monitor illicit production of explosives and drugs, thus stopping terrorist attacks at an early stage and preventing produced drugs to get as far as the street. A number of key components necessary to achieve the goal have been identified:

- knowledge of the threat and dispersion of threat
- substances, sensors for their detection, system
- communication, information management,
- testing & verification and a field demonstration.

Continuous communication with end users is planned as well as a field demonstration at the end of the project. The project aims at demonstrating system capability by the modification of existing sensors and sensors in development in order to detect selected precursors and integrating the sensors in a network system using existing technology. By using existing global infrastructures for positioning (GPS) and networking (GSM, GPRS or 3G) the LOTUS system can be used more or less anywhere in the world at relatively small cost for supporting installations and extra personnel. Special attention will be given to secure communication. In order to interpret and present the results it is also necessary to learn how chemicals around an illicit production site are dispersed by full-scale measurements and modelling.

Expected results

Detection of explosives has traditionally been focused on detection when an explosive charge is already ready for use, being transported to or already at the scene of an attack. Preventing terrorist attacks while they are already in motion is extremely difficult. Not only is it difficult to find an explosive on a person or in a bag but one must also face the need to do this in a very short time and then immediately implement measures for countering the attack once a possible suspect or suspicious object has been found. The capability to intervene at an earlier stage is therefore of very high importance and testing whether the LOTUS system is a viable concept for finding the bomb/drug factory is the expected result for the LOTUS research.

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 can be expanded as and when needed to detect selected precursors and to respond to an attack at an early stage, is currently the best way to achieve a significant benefit in counter-terrorism. The LOTUS system is planned as well as a field demonstration at the end of the project. The project aims at demonstrating system capability by the modification of existing sensors and sensors in development in order to detect selected precursors and integrating the sensors in a network system using existing technology. By using existing global infrastructures for positioning (GPS) and networking (GSM, GPRS or 3G) the LOTUS system can be used more or less anywhere in the world at relatively small cost for supporting installations and extra personnel. Special attention will be given to secure communication. In order to interpret and present the results it is also necessary to learn how chemicals around an illicit production site are dispersed by full-scale measurements and modelling.
Information

Acronym: LOTUS

Grant Agreement N°: 217925

Total Cost: € 4,298,593

EU Contribution: € 3,189,146

Starting Date: 01/01/2009

Duration: 36 months

Coordinator:

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

Contact:

Dr. Sara Wallin
Tel: +46 8 5550 4097
Mobile: +46 709 277008
Fax: +46 8 5550 3949
E-mail: sara.wallin@foi.se
Website: www.lotusfp7.eu

Partners

NAME
FOI
Portendo AB
Saab AB
Bruker Daltonik GMBH
Ramem S.A.
Bruhn NewTech A/S
Research and Education Laboratory in Information Technologies
TNO
Universidad de Barcelona
Secrab Security Research

COUNTRY
Sweden
Sweden
Sweden
Germany
Spain
Denmark
Greece
The Netherlands
Spain
Sweden
MiDAS / The development and validation of a rapid millifluidic DNA analysis system for forensic casework samples

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 process. 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 on 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.
Information

Acronym: MiDAS

Grant Agreement N°: 242345

Total Cost: € 4,688,674.80

EU Contribution: € 3,231,404.60

Starting Date: 01/09/2010

Duration: 36 months

Coordinator:

FORENSIC SCIENCE SERVICE LTD
Research and Development
Birmingham Business Park, Solihull Parkway
B37 7YN
United Kingdom

Contact:
Cecilia Buffery
Tel.: +441256771521
Mobile: +447824 434158
Fax: +441256771521
E-mail: Cecilia.buffery@fss.pnn.police.uk
Website: www.forensic.gov.uk

Partners

NAME

Grid Xitek Limited (GXD) United Kingdom
Medizinische Universität Innsbruck (IMU) Austria
Bundeskriminalamt (BKA) Germany
Netherlands Forensic Institute (NFI) Netherlands
Arizona Board of Regents (University of Arizona- UoA) United States

COUNTRY

United Kingdom
Austria
Germany
Netherlands
United States
Project objectives

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

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

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

» Secure interoperable platform for ballistic information management.

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

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

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

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

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

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

Description of the work

The project was divided into seven work packages.

This included work packages for management and dissemination.

The project technical work packages consisted of the following:

» Intelligence Ballistic data capture and knowledge extraction.

» Ballistic risk management process support.

» Extended interoperability layer for semantically managing the Odyssey platform. The realisation of the above will result in:

» Acquiring integrated data including future multimedia sources and enriching data through a semantically enhanced metadatabase.

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

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

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

» Creating a policy driven data exchange platform.

Results

The results of the project are available on the website of the project www.odyssey-project.eu and the CORDIS website http://cordis.europa.eu/fp7/security. The exploitation of legacy systems.
**Information**

**Acronym:**
ODYSSEY

**Grant Agreement N°:**
218237

**Total Cost:**
€ 3,821,599

**EU Contribution:**
€ 2,400,000

**Starting Date:**
01/11/2008

**End Date:**
31/04/2011

**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

---

**Name**

- SHEFFIELD HALLAM UNIVERSITY (SHU)
- AN GARDA SIÓCHANA (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 PROGRAMSKOE OPREME IN SVETOVAJE D.O.O. (XLAB)

**Country**

- United Kingdom
- Ireland
- Spain
- Belgium
- The Netherlands
- United Kingdom
- Italy
- United Kingdom
- Austria
- United Kingdom
- Slovenia
Project objectives

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

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

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

Description of the work

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

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

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

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

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

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

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

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

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

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

Expected results

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

» Enhanced spectrometrics for an Integrated OPTIX system.

» Advanced data fusion and chemometrics algorithms.

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

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

Acronym: OPTIX
Grant Agreement N°: 218037
Total Cost: € 3,289,855
EU Contribution: € 2,487,556
Starting Date: 01/11/2008
Duration: 42 months

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

Contact:
Carlos de Miguel
Tel: +(34) 91 257 95 73
Mobile: + (34) 650 505 091
Fax: +(34) 91 257 70 18
E-mail: cdemiguel@indra.es
Website: www.fp7-optix.eu

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indra Sistemas S.A</td>
<td>Spain</td>
</tr>
<tr>
<td>University of Malaga</td>
<td>Spain</td>
</tr>
<tr>
<td>FOI</td>
<td>Spain</td>
</tr>
<tr>
<td>EKSPLA UAB</td>
<td>Sweden</td>
</tr>
<tr>
<td>AVANTES BV</td>
<td>Lithuania</td>
</tr>
<tr>
<td>Technical University of Clausthal</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Vienna University of Technology</td>
<td>Germany</td>
</tr>
<tr>
<td>University of Dortmund</td>
<td>Austria</td>
</tr>
<tr>
<td>Guardia Civil</td>
<td>Germany</td>
</tr>
<tr>
<td></td>
<td>Spain</td>
</tr>
</tbody>
</table>
Project objectives

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

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

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

Description of the work

The PREVAIL project focus on finding inhibitors to add to some precursors to prevent them from being used to produce homemade explosives or to prevent them from being concentrated by boiling of 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 found markers must be environmentally friendly, non-toxic and bio-degradable. Honeybees, microcrystals 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 is 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. Close collaboration with the Standing Committee on Explosives Precursors is necessary since PREVAIL does not want to duplicate work already done by that committee.

Expected results

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

<table>
<thead>
<tr>
<th>Acronym:</th>
<th>PREVAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Agreement N°:</td>
<td>241858</td>
</tr>
<tr>
<td>Total Cost:</td>
<td>€ 4,295,469</td>
</tr>
<tr>
<td>EU Contribution:</td>
<td>€ 3,343,162</td>
</tr>
<tr>
<td>Starting Date:</td>
<td>01/09/2010</td>
</tr>
<tr>
<td>Duration:</td>
<td>36 months</td>
</tr>
</tbody>
</table>

**Coordinator:**

Totalförsvarets forskningsinstitut  
Department of Energetic Materials  
Grindsjön Research Centre  
SE-147 25 Tumba  
Sweden  

---

**Contact:**

Malin Kölhed  
Tel.: +46 (0)8 5550 4197  
Mobile: +46 (0)70 9277010  
Fax: +46 (0)8 5550 3949  
E-mail: Malin.kolhed@foi.se  
Website: www.prevail-fp7.eu

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Totalförsvarets forskningsinstitut (FOI)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek (TNO)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Technion – Israel Institute of Technology (Technion)</td>
<td>Israel</td>
</tr>
<tr>
<td>Arkema France (Arkema)</td>
<td>France</td>
</tr>
<tr>
<td>KCEM AB (KCEM)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Yara International ASA (Yara)</td>
<td>Norway</td>
</tr>
<tr>
<td>Commissariat à l’Energie Atomique et aux Energies Alternatives (CEA)</td>
<td>France</td>
</tr>
<tr>
<td>Wojskowy Instytut Higieny i Epidemiologii (WIHiE)</td>
<td>Poland</td>
</tr>
<tr>
<td>SECRAB Security Research (SECRAB)</td>
<td>Sweden</td>
</tr>
</tbody>
</table>
RAPTOR / Rapid deployable, gas generator assisted inflatable mobile security kits for ballistic protection of European civilians against crime and terrorist attacks

**Project objectives**

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

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

» individuals,

» general security of events,

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

**Description of the work**

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

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

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

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

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

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

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

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

**Expected results**

» Compilation of threat scenarios,

» Performance requirements of protection kit,

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

» Development of textiles and coatings for inflatable structures,

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

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

» Adjusting of gas generator module to assure reliable inflation,

» Consolidation,

» Final testing of demonstrators, and

» Innovation plan, exploitation plan and feasibility study.
Information

Acronym: RAPTOR

Grant Agreement N°: 218259

Total Cost: € 2,849,867.76

EU Contribution: € 2,060,995.13

Starting Date: 01/01/2010

Duration: 48 months

Coordinator:

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

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

Dipl.-Ing. Johanna Schubert
Tel +49 (0)721 4640 249
Fax +49 (0)721 4640 111
Website: http://www.ict.fraunhofer.de

NAME

FRAUNHOFER (FHG-ICT)
Bundeskriminalamt (BKA)
Explosia
Fraunhofer (FhG-ICT) (Coordinator)
Lanco
P-D Interglas

COUNTRY

Germany
Germany
Czech Republic
Germany
Germany
United Kingdom
Project objectives

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

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

Description of the work

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

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

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

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

Expected results

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

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

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

Acronym: SALIANT

Grant Agreement N°: 242377

Total Cost: € 4,498,088.80

EU Contribution: € 3,362,598.60

Starting Date: 01/09/2010

Duration: 36 months

Coordinator:
UNIVERSITY OF NEWCASTLE UPON TYNE
Institute of Cellular medicine
Kensington Terrace 6
NE1 7RU, Newcastle Upon Tyne
United Kingdom

Contact:
Colin Self
Tel.: +44 191 223 5604
Fax: +44 191 223 5601
E-mail: c.h.self@ncl.ac.uk
Website: http://www.saliant.eu/

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selective Antibodies Limited (SAL)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>OY REAGENA Ltd (REAG)</td>
<td>Finland</td>
</tr>
<tr>
<td>Indicia Biotechnology (IND)</td>
<td>France</td>
</tr>
<tr>
<td>Department of Justice, Equality &amp; Law reform (FSL)</td>
<td>Ireland</td>
</tr>
<tr>
<td>Zilinska univerzita v ziline (UNIZA)</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Netherlands Forensic Institute (NFI)</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Applikon Analyzers (APP)</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Stichting Dienst Landbouwkundig Onderzoek (DLO-FBR)</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Centre of Excellence for Life Sciences Ltd (CELS)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Kite Innovation (Europe) Limited (KITE)</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
SAVEMed / Microstructure secured and self-verifying medicines

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.

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.

Expected results

A) Fabrication of novel overt and covered self-verifying security features in medical product.

B) Experimental proof of cost effective manufacturing route of tools equipped with durable micro- and nanostructures.

C) Fast measurement devices developed capable of identifying the secure microstructures in a variety of – coated and uncoated – medical products.

D) 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.
Information

Acronym: SAVEMed

Grant Agreement N°: 261715

Total Cost: € 4,248,115

EU Contribution: € 3,144,724

Starting Date: 01/04/2011

Duration: 36 months

Coordinator: NANO-4-U GMBH
N/A Mozartstrasse 7 N/A 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

NAME

Heliotis AG Switzerland
Centre Suisse d’Electronique et Microtechnique SA (CSEM) Switzerland
SteriPack Ltd. Ireland
Klocke Holding Germany
Mauer Sp. z o. o, Poland
United Nations Interregional Crime and Justice Research Institute (UNCRI) Italy
NANO4U GmbH Germany
SCIIMS / Strategic Crime and Immigration Information Management System

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 baseline in order to speed introduction of new innovative techniques, technologies and systems.

Description of the work

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

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

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

Expected results

Research of Information Management and Information Exploitation techniques in aid of the combating of organised crime. SCIIMS will research and develop ‘beyond state of the art’ technologies and techniques to search, mine, and fuse information from large heterogeneous data sets. Improving visualisation techniques of information for sense-making in order to conduct analysis, detect trends and improve the understanding and detection of People Trafficking and Smuggling.
Information

Acronym: SCIIMS
Grant Agreement N°: 218223
Total Cost: € 3,503,000
EU Contribution: € 2,318,996.45
Starting Date: 01/11/2009
Duration: 36 months

Coordinator:
BAE SYSTEMS INTEGRATED SYSTEM TECHNOLOGIES LIMITED
Commercial Department
Lyon Way, Frimley, Camberley
GU16 7EX, Surrey
United Kingdom

Contact:
Claire Dance
Tel: 01276 603226
Mobile: +44 (0)7793 423771
Fax: +44 (0)1276 603111
E-mail: claire.dance@baesystems.com
Website: http://www.sciims.co.uk/index.html

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAE SYSTEMS INTEGRATED SYSTEM TECHNOLOGIES LTD</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>INDRA SISTEMAS S.A. (INDRA)</td>
<td>Spain</td>
</tr>
<tr>
<td>DENODO TECHNOLOGIES SL (DENODO)</td>
<td>Spain</td>
</tr>
<tr>
<td>MAGYAR TUDOMANYOS AKADEMIA SZAMITASTECHNIKAI ES AUTOMATIZALASI KUTATO INTEZET (SZTAKI)</td>
<td>Hungary</td>
</tr>
<tr>
<td>UNIVERSIDADE DA CORUNA (UDC)</td>
<td>Spain</td>
</tr>
<tr>
<td>SELEX SISTEMI INTEGRATI SPA (SSI)</td>
<td>Italy</td>
</tr>
<tr>
<td>GREEN FUSION LIMITED (DATA FUSION)</td>
<td>Ireland</td>
</tr>
</tbody>
</table>
Project objectives

The project aim is to develop a demonstrable, modular and “close-to-market” demonstrator of a stationary, reliable, vehicle-portable, low false alarm rate Two Stage Rapid Biological Surveillance and Alarm System for Airborne Threats (TWOBIAS) for use at indoor or outdoor public sites regarded as targets for bioterrorist attacks. The objectives are to:

1. Establish a command and control software system for TWOBIAS in order to reliably function at a real-life site.
2. Test and evaluate biodetectors in large-scale chamber tests, and analyse background interference detection signals at real-life conditions.
3. Enhance the performance of TWOBIAS using advanced data classification methods.
4. Provide a functional combined two stage alarm biological detection and identification system.

Description of the work

TWOBIAS includes both detection (BDU – biological detection unit) and identification (BIU – biological identification unit) schemes:

» StageONE: First alarm based on best-in-use optimized optical BDU (detect-to-warn).

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

The project, containing six workpackages, will enhance the progress of the state-of-art technology by developing a reliable biological surveillance system TWOBIAS in order to reduce the total time response for first responders by focusing on:

» assessing the requirements by users;
» reducing false alarm rates by improving current BDUs using complementary orthogonal detector techniques obtaining classification of biological threat agents during detection;
» developing improved alarm algorithms for existing mature and almost mature BDUs;
» combining the improved BDU with a semi-automatic microfluidic on-site molecular identification unit (BIU) for multiplex identification of biological threat agents in air;
» 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.
**Acronym:**
TWOBIAS

**Grant Agreement N°:**
FP7 - 242297

**Total Cost:**
€ 4,935,083.65

**EU Contribution:**
€ 3,577,834

**Starting Date:**
01/07/2010

**Duration:**
3 years

**Coordinator:**
NORWEGIAN DEFENCE RESEARCH ESTABLISHMENT
FFI
Norway

**Contact:**
Janet Martha Blatny
Tel.: +47 63807827
Fax: +47 63807509

**NAME**
FFI
Centre d’Etudes du Bouchet, DGA
Dycor Global Solutions Ltd, DGS
TNO
Q-Linea, QL
SUJCHBO, SCB
FOI
Thales, TRT og TSS
Uppsala University, UoU

**COUNTRY**
Norway (lead)
France
Cyprus
The Netherlands
Sweden
Czech Republic
Sweden
France
Sweden
**Project objectives**

The waterways are becoming more and crucial for coastal economy and paradoxically, such areas remain very vulnerable to terrorism attacks especially against underwater IED threats. Coastal regions such as in southern Europe and south-east Asia are contaminated by different ammunition left on the sea bottom after war activities from World War I, II and more recent conflicts. This represents a constant threat to the sea traffic, fishermen, tourists and local populations. The objects on the sea bottom are of different nature and include torpedoes, airplane bombs, anti-ship mines, grenades, gun fuses, ammunition and projectiles of different calibers. For example, it is estimated that there are at least 130 000 tons of explosive devices in the eastern coastal waters of the Adriatic Sea. This dramatic pollution weakens the economic development capacity of such regions.

A major challenge is to provide new tools for keeping naval infrastructure safe: harbours, ships, coastal areas, ferry terminals, oil and gas terminals, power/nuclear plants, etc. The main objective of UNCOSS project is to provide tools for the non-destructive inspection of underwater objects mainly based on neutron sensor. This technology used has already been experimented for Land Protection (especially in the frame of FP6/Euritrack project). The application of this technology for underwater protection will be a major achievement.

The classical approach for underwater IED detection is mainly based on sonar detection (derived from military development for mine clearance) which can not guarantee if unattended objects contain explosive. The identification/classification of underwater objects using classical sensors such as sonar and video cameras, becomes more and more difficult when facing asymmetrical attacks. The UNCOSS project is a cost-effective response to new terrorism threats and provides a fundamental technology for the global issue of maritime surveillance and port/naval infrastructure protection.

There is no specific device capable of identifying explosive contents of submerged UneXplode Ordnance (UXO) therefore Explosive Ordnance Disposal (EOD) teams at present have to remove the objects without knowledge of the explosive charge presence.

**Expected results**

The end product of this project will be a prototype of a complete coastal survey system that will make use of a specifically designed underwater neutron sensor capable of confirming the presence of explosives on the bottom of the sea, either visible or partially covered by sediments. Such a device will allow a safer and more efficient removal of explosive devices from the sea bottom of the ports and elsewhere.

The final demonstration campaign shall perform in Croatia under the supervision of the IRB which shall be responsible for the management of all licensing and authorization issues.
Information

Acronym: UNCOSS

Grant Agreement N°: 218148

Total Cost: € 4,520,000

EU Contribution: € 2,780,000

Starting Date: 01/12/2008

Duration: 36 months

Coordinator:
CEA
Le Ponant de Paris
25 Rue Leblanc
F-75015 Paris Cedex 15
France

Contact:
Guillaume Sannie
Tel: +33169085188

PARTNERS

NAME
CEA
ECA S.A.
Ruder Boskovic Institute
Laseroptronix
Jozef Stefan Institute
A.C.T.d.o.o.
Port Authority Dubrovnik
Port Authority Bar
Port Authority Vukovar

COUNTRY
France
France
Croatia
Sweden
Slovenia
Croatia
Croatia
Montenegro
Croatia
ADABTS / Automatic detection of abnormal behaviour and threats in crowded spaces

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

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

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

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

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

ADABTS will develop new and adapt existing sensor processing methods and algorithms for detecting and tracking people in complex environments, involving groups of people or crowds. Extracted sensor data features (e.g. tracks, voice pitches, body articulations) need to be related to the behaviour primitives, and, moreover, to be dynamic and 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 GPU’s (Graphical Processing Units). Such hardware, in rapid development driven by the game industry, represents a huge potential for high-performance surveillance systems.

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

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

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

- Understanding of the user needs for automatic detection of unusual behaviour in crowds and new definitions of and methods for describing such behaviour.
- Methods and algorithms for unusual behaviour detection based on video and acoustic sensors.
- Real time optimization for commercially available low-cost hardware, including an on-line demonstration of capabilities at a football stadium.
**Information**

**Acronym:**
ADABTS

**Grant Agreement N°:**
218197

**Total Cost:**
€ 4,478,990

**EU Contribution:**
€ 3,229,034

**Starting Date:**
01/06/2009

**Duration:**
48 months

---

**Coordinator:**

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

---

**Contact:**

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

---

**Partners**

**NAME**

FOI
BAE Systems
Detec A/S
Home Office Scientific Development Branch
Institute of Psychology – Ministry of the Interior
SINTEF
TNO
University of Amsterdam

---

**COUNTRY**

Sweden
United Kingdom
Norway
United Kingdom
Bulgaria
Norway
The Netherlands
The Netherlands
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 number and impact of false alarms 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 through 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 on 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 to the user requirements, to the generic architecture, to the different research areas related to the components and to 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.
Information

**Acronym:** ARENA

**Grant Agreement N°:** 261658

**Total Cost:** € 4,861,867.60

**EU Contribution:** € 3,178,761.00

**Starting Date:** -

**Duration:** 36 months

**Coordinator:**

TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)
Swedish Defence Research Agency
Gullfossgatan 6
STOCKHOLM, 164 90
Sweden

**Contact:**
Åsa Waern
Tel : +4613378084
E-mail : asa.waern@foi.se
Website : http://www.foi.se/FOI/templates/startpage__96.aspx

Partners

**NAME**

BMT GROUP LIMITED (BMT)

ITTI Sp.zo.o. (ITTI)

SAGEM DEFENSE SECURITE (Sagem DS)

MORPHO (MPH)

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK – TNO (TNO)

THE UNIVERSITY OF READING (UoR)

PRO DOMO SAS (PRODOMO)

**COUNTRY**

United Kingdom

Poland

France

France

The Netherlands

United Kingdom

France
Project objectives

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

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

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

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

- To integrate all the software and hardware developments in the selected demo scenario.
- To test and to improve of the whole system in the demo scenarios executing a thorough testing and evaluation program.
- To perform demonstrations of the developed system to the end users involved in the project and to additional stakeholders as needed.
- To elaborate a technological and application roadmap for further research needs and users involvement.

Description of the work

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

The BASYLIS system will consist of 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.

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

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

Expected results

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

Acronym: BASYLIS

Grant Agreement N°: 261786

Total Cost: € 2,989,194.80

EU Contribution: € 2,037,265.00

Starting Date: 01/05/2011

Duration: 24 months

Coordinator:

IP Sistemas
Calle Anabel Segura nº 7- Planta B
28108, Alcobendas, Madrid
Spain

Contact: Sonia Gracia Anadón
Tel: +34 91 203 87 09
Mobile: +34 610.201.908
Fax: +34 91 209 78 28
E-mail: sgracia@indra.es
Website: www.basylis.european-project.eu

Partners

NAME

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 COLLEGUE LONDON (UCL)
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS (CNPIC)

COUNTRY

Spain
Spain
Italy
Denmark
Netherlands
Finland
Spain
United Kingdom
Spain
COPRA / Comprehensive European Approach to the Protection of Civil Aviation

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). 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. Besides considering new developments to an all-hazard approach to provide 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 WP’s will be supported by expert groups in workshops (WS). WP1 and WP 2 through workshop WS1. WP 3 will be supported in WS2. WP 4 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 on future aviation security research

» recommendations for standardization, test and certification issues

All taking into account passenger privacy, mobility, public acceptability, stakeholder requirements and the legal context of the European Union.
**Information**

**Acronym:** COPRA

**Grant Agreement N°:** 261651

**Total Cost:** € 1,291,405.20

**EU Contribution:** € 983,949.90

**Starting Date:** not yet determined

**Duration:** 18 months

**Coordinator:**

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
Fraunhofer Ernst-Mach-Intitut (EMI)
Hansastr. 27c
80686 Munich
Germany

**Contact:**

Dr. Tobias Leismann
Tel.: +49 761 2714 402
Mobile: +49 170 769 5101
Fax: +49 761 2714 1402
E-mail: Tobias.Leismann@emi.fraunhofer.de
Website: www.emi.fraunhofer.de

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Business School (EBS)</td>
<td>Germany</td>
</tr>
<tr>
<td>Airbus S.A.S. (AIR)</td>
<td>France</td>
</tr>
<tr>
<td>European Organisation for Security (EOS)</td>
<td>Belgium</td>
</tr>
<tr>
<td>Fraport AG Frankfurt Airport Services Worldwide (FRA)</td>
<td>Germany</td>
</tr>
<tr>
<td>Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)</td>
<td>the Netherlands</td>
</tr>
<tr>
<td>Morpho (MPH)</td>
<td>France</td>
</tr>
<tr>
<td>Commissariat à l’énergie atomique et aux énergies alternatives (CEA)</td>
<td>France</td>
</tr>
<tr>
<td>Smith Heimann GmbH (SMI)</td>
<td>Germany</td>
</tr>
<tr>
<td>University of Ljubljana (UL)</td>
<td>Slovenia</td>
</tr>
<tr>
<td>KLM – Royal Dutch Airlines NV (KLM)</td>
<td>the Netherlands</td>
</tr>
</tbody>
</table>
DEMASST was the first phase of the FP7 demonstration programme for security in mass transportation with the task to provide a roadmap for the development and integration of system-of-system solutions. By virtue of the similarity of problems across big cities in Europe, such security solutions have a potentially very important EU-wide market.

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

Description of the work

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

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

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

DEMASST proposed the methodological infrastructure for this. But an optimal demo project design does not stop with finding scientific answers: the issue of turning demonstration into innovation was top on DEMASST’s agenda. And this approach will have utility also beyond transportation. The project was carried out between January 2009 and May 2010.

Results

DEMASST results included the following:

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

**Acronym:**
DEMASST

**Grant Agreement N°:**
218264

**Total Cost:**
€ 1,840,555

**EU Contribution:**
€ 956,650

**Starting Date:**
12/01/2009

**End Date:**
11/05/2010

**Coordinator:**

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

---

**Contact:**

**E. Anders Eriksson**
Tel: +46-8 5550 3747
Mobile: +46 709 277 281
Fax: +46-8 5550 3866
E-mail: e.anders.eriksson@foi.se
Website: http://www.demasst.eu

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOI</td>
<td>Sweden</td>
</tr>
<tr>
<td>Ansaldo STS</td>
<td>Italy</td>
</tr>
<tr>
<td>CEA</td>
<td>France</td>
</tr>
<tr>
<td>EADS Astrium</td>
<td>France</td>
</tr>
<tr>
<td>FFI</td>
<td>Norway</td>
</tr>
<tr>
<td>Fraunhofer-INT</td>
<td>Germany</td>
</tr>
<tr>
<td>INECO</td>
<td>Spain</td>
</tr>
<tr>
<td>SINTEF</td>
<td>Norway</td>
</tr>
<tr>
<td>TECNALIA-INASMET</td>
<td>Spain</td>
</tr>
<tr>
<td>THALES Security Systems</td>
<td>France</td>
</tr>
<tr>
<td>TIFSA</td>
<td>Spain</td>
</tr>
<tr>
<td>TNO</td>
<td>Spain</td>
</tr>
<tr>
<td>VTT</td>
<td>The Netherlands</td>
</tr>
<tr>
<td></td>
<td>Finland</td>
</tr>
</tbody>
</table>
**DESURBS / Designing safer urban spaces**

**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 DESURBS solutions result in urban spaces less prone for 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 for 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 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 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.
**Information**

**Acronym:**
DESURBS

**Grant Agreement N°:**
261652

**Total Cost:**
€4,161,929

**EU Contribution:**
€3,208,549

**Starting Date:**
01/01/2011

**Durations:**
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

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loughborough University (Loughborough)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>The University of Birmingham (Birmingham)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>The Hebrew University of Jerusalem (HUJI)</td>
<td>Israel</td>
</tr>
<tr>
<td>Technical University of Crete (TUC)</td>
<td>Greece</td>
</tr>
<tr>
<td>Centre Internacional de Metodes Numerics en Enginyeria (CIMNE)</td>
<td>Spain</td>
</tr>
<tr>
<td>University of Southampton (IT Innovation)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Bezalel, Academy of Arts and Design (Bezalel Academy)</td>
<td>Israel</td>
</tr>
</tbody>
</table>
EMILI / Emergency management in large infrastructures

**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.

**Expected results**

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

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

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

**Description of the work**

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

Acronym: EMILI

Grant Agreement N°: 242438

Total Cost: € 3,997,230.40

EU Contribution: € 3,139,228

Starting Date: 01/01/2010

Duration: 36 months

Coordinator:
FRAUNHOFER IAIS
Schloss Birlinghoven
D-53754 Sankt Augustin
Germany

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

Partners

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

COUNTRY
Germany
Switzerland
Spain
Germany
The Netherlands
Serbia
Germany
EURACOM / European risk assessment and contingency planning methodologies for interconnected networks

Project objectives

EURACOM addresses the issue of the protection and resilience of energy supply for European interconnected energy networks. Its objective is to identify, together with European critical energy infrastructures operators, a common and holistic approach (end-to-end energy supply chain) for risk assessment and risk management solutions.

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

Description of the work

EURACOM will pursue 4 main objectives:

» Promoting a dialogue between energy and security stakeholders.

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

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

» European Forum for Energy Infrastructures – Security and Resilience

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

A common European methodology for risk management and contingency planning

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

This Pan-European methodology will be derived from:

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

» Supporting European policies for the protection of critical energy infrastructures

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

Results

Information

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

Coordinator:
EOS – THE EUROPEAN ORGANISATION FOR SECURITY

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

Partners

NAME
EOS -The European Organisation for Security
ALTRAN
CEA
JRC
TNO
THALES
EDISOFT

COUNTRY
EU
France
The Netherlands
The Netherlands
United Kingdom
Portugal
iDetecT 4ALL / Novel intruder detection and authentication optical sensing technology

Project objectives

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

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

Description of the work

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

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

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

Results

The results of the project are available on the website of the project www.idetect4all.com and the CORDIS website http://cordis.europa.eu/fp7/security.
**Information**

**Acronym:**
IDOteC 4ALL

**Grant Agreement N°:**
217872

**Total Cost:**
€ 3,236,675

**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

---

**Partners**

**NAME**
Instro Precision Ltd.
ARTTIC
Motorola Israel Ltd.
EVERIS Consulting
Cargo Airlines
3D s.a.
ANA Aeroportos de Portugal
LACHS
Azimuth Tecnologies Ltd.
S.C. PRO OPTICA S.A.

**COUNTRY**
United Kingdom
Belgium
Israel
Spain
Greece
Portugal
Belgium
Israel
Romania
INFRA / Innovative & novel first responders applications

Project objectives

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

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

» Communications objectives, which involve the research and development of an integral and interoperable wireless communications system that will allow First Responders to have reliable means of communications as they enter subway tunnels and buildings with thick concrete walls.

» First Responders objectives, which entail the R&D of a robust indoor-site navigation system based on three location sensors (an inertial sensor, a wireless sensor and a video sensor), a video annotation system for First Responder PDAs, sensors for real time identification of radiation exposure and hazardous materials and applications for gas leakage and hidden fire detection.

» Standardization objectives, which includes R&D of a European level proposal for the standardization of the framework of communications and applications as proposed by INFRA.

» Demonstration objectives, which consist on the demonstration of the validity of INFRA’s standards, communications and First Responder applications being developed.

Description of the work

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

The Critical Infrastructure Broadband Communications Base area will cover advanced wireless broadband network technology that is specially adapted to the needs of First Responder teams in Critical Infrastructure sites. The network shall support video, data and voice communications and it will consist of multi-radio mesh topology with self-adaptive and self-healing functionality.

The Critical Infrastructure Open Interoperability Standard area will cover the development of a highly dynamic system of systems made up of elements that interact with each other in unplanned and spontaneous ways. It will also cover the development of a First Responder oriented network-programming platform that will implement the systems-of-systems nature of First Responder applications and communications.

In addition, the abstraction level provided by this communication layer will be able to support future applications that will conform to the INFRA specifications, aiming to lay the foundation for a European First Responder interoperability standard.

The Communications Space will provide an unprecedented level of interoperability for voice and data communications. All First Responder teams, First Responder command posts and the Critical Infrastructure control centre, regardless of their radio technology, will be able to communicate with each other. Furthermore, First Responders will be able to use their legacy equipment inside buildings with thick concrete walls and in underground tunnels, where typically radio RF propagation is impaired. The Application Space will provide novel technologies and applications for the use of First Responders in Critical Infrastructure sites. These shall be Site Indoor Navigation (based on inputs from three independent tracking sources for increased reliability and accuracy), Thermal imaging (including gas-leaks detection and hidden-fire detection), Advanced Sensors (robust and lightweight fibre optic based sensors for the detection of hazardous materials) and Video Annotation (annotated with symbols and graphical components through dedicated authoring tools and short textual descriptions that aim at focusing the attention of the First Responder on a specific part of the picture).

Results

The results of the project are available on the website of the project www.infra-fp7.eu and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: INFRA

Grant Agreement N°: 225272

Total Cost: € 3,820,811

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

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Athena GS3 Security Implementations Ltd.</td>
<td>Israel</td>
</tr>
<tr>
<td>Halevi Dweck &amp; Co. ARTTIC Israel Company Ltd.</td>
<td>Israel</td>
</tr>
<tr>
<td>University of Limerick</td>
<td>Ireland</td>
</tr>
<tr>
<td>ISDEFE Ingeniería de Sistemas S.A.</td>
<td>Spain</td>
</tr>
<tr>
<td>Democritus University of Thrace</td>
<td>Greece</td>
</tr>
<tr>
<td>Rinicom</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Everis Spain S.L.</td>
<td>Spain</td>
</tr>
<tr>
<td>Hopling Networks B.V.</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Opgal Optronic Industries Ltd.</td>
<td>Israel</td>
</tr>
<tr>
<td>Research and Education Laboratory in Information Technologies</td>
<td>Greece</td>
</tr>
</tbody>
</table>
Project objectives

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

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

Description of the work

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

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

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

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

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

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

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

Expected results

» A prototype of electromagnetic sensing (ES) monitoring and surveillance system based on an ad-hoc networking of in situ sensors and airborne/satellite data.

» 4D tomographic infrastructure monitoring thanks to the exploitation and integration of the ES techniques.

» Validation of ES techniques through experiments at two test sites.

» Demonstration of the effectiveness of the system at two challenging test beds.

» Dissemination of ISTIMES approach and outcomes to public institutions and private companies.
Information

Acronym: ISTIMES

Grant Agreement N°: 225663

Total Cost: € 4,342,283

EU Contribution: € 3,113,460

Starting Date: 01/06/2009

Duration: 36 months

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

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

Partners

NAME
Technologies for Earth Observations and Natural Hazards (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)

COUNTRY
Italy
Italy
Italy
Switzerland
France
Sweden
Israel
Romania
Norway
MOSAIC / Multi-Modal Situation Assessment & Analytics Platform

Project objectives

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 multimedia 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 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,

iv) Tools and techniques for the extraction of key information from video, uncontrolled 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.

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 multimedia 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.

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.
Acronym: MOSAIC

Grant Agreement N°: 261776

Total Cost: € 3,606,642.00

EU Contribution: € 2,664,559.00

Starting Date: 01/04/2011

Duration: 36 months

Coordinator:

THE UNIVERSITY OF READING
Intelligent Media Systems and Services Research Laboratory,
School of Systems Engineering
Whiteknights Campus
PO Box 217
RG66AH Reading,
United Kingdom

Contact:
Prof. Atta Badii
Tel: +44 (0) 118 378 7842
Fax: +44 (0) 118 975 1994
E-mail: atta.badii@reading.ac.uk
Website: www.imss.reading.ac.uk

NAME

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

COUNTRY

United Kingdom
United Kingdom
Italy
Germany
United Kingdom
Belgium
United Kingdom
Project objectives

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

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

More specifically, the NI2S3 Project aims:

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

Description of the work

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

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

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

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

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

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

Expected results

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

NI2SR cross-border project will give the chance to realize technology and reference methodology for developing critical infrastructure security systems that can be better accepted by the possible stakeholders, being designed based on the guidelines of each of the participant’s country needs.

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

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

Acronym: NI2S3

Grant Agreement N°: 225488

Total Cost: € 4,325,728

EU Contribution: € 2,711,640

Starting Date: 01/07/2009

Duration: 24 months

Coordinator:

VITROCISET S.P.A.

Contact:

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vitrociset S.p.A.(VCS)</td>
<td>Italy</td>
</tr>
<tr>
<td>Università degli Studi di Firenze (UNIFI)</td>
<td>Italy</td>
</tr>
<tr>
<td>HW Communications Limited (HWC)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>AALBORG Universitet (AAU)</td>
<td>Denmark</td>
</tr>
<tr>
<td>AGH University of Science and Technology (AGH)</td>
<td>Poland</td>
</tr>
<tr>
<td>Comarch S.A. (COMARCH)</td>
<td>Poland</td>
</tr>
</tbody>
</table>
PROTECTRAIL / The Railway-Industry Partnership for Integrated Security of Rail Transport

Project objectives

The objective to provide a viable integrated set of security solution, by considering the extent of the assets involved, the nature of the threats, the amount of requirements and 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 solution, and will represent a comprehensive and scalable answers to rail security.

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

Description of the work

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

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

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

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

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

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

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

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

Expected results

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

**Acronym:**
PROTECTRAIL

**Grant Agreement N°:**
242270

**Total Cost:**
€ 21,775,289.80

**EU Contribution:**
€ 13,115,064.00

**Starting Date:**
01.08.2010 (to be confirmed)

**Duration:**
42 months

**Coordinator:**

**ANSALDO STS S.P.A.**
VIA P. MANTOVANI 3-5
16151 GENOVA
ITALIA

**Contact:**
Mr. Vito Siciliano
Tel.: +39-010-6552976
Fax: +39-010-6552006
Mob.: +39-3489895875
e-mail: Vito.Siciliano.Prof110@ansaldo-sts.com
Website: not yet available

**NAME**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ansaldo STS S.p.A.</td>
<td>Italy</td>
</tr>
<tr>
<td>Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Union Internationale Des Chemins De Fer</td>
<td>France</td>
</tr>
<tr>
<td>Selex Sistemi Integrati S.p.A.</td>
<td>Italy</td>
</tr>
<tr>
<td>Bombardier Transportation GMBH</td>
<td>Germany</td>
</tr>
<tr>
<td>Alstom Transport SA</td>
<td>France</td>
</tr>
<tr>
<td>Thales Security Solutions &amp; Services SAS</td>
<td>France</td>
</tr>
<tr>
<td>Sarad GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>UNIFE – The European Rail Industry</td>
<td>Belgium</td>
</tr>
<tr>
<td>Sagem Sécurité SA</td>
<td>France</td>
</tr>
<tr>
<td>Ductis GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>Železničná spoločnosť Slovensko a.s.</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Joint Stock Company Lithuanian Railways</td>
<td>Lithuania</td>
</tr>
<tr>
<td>ItalCertifer S.c.p.a.</td>
<td>Italy</td>
</tr>
<tr>
<td>PKP Polskie Linie Kolejowe SA</td>
<td>Poland</td>
</tr>
<tr>
<td>D’Appolonia S.p.A.</td>
<td>Italy</td>
</tr>
<tr>
<td>Elbit Systems Ltd.</td>
<td>Israel</td>
</tr>
<tr>
<td>Facultés Universitaires Notre-Dame de la Paix</td>
<td>Belgium</td>
</tr>
<tr>
<td>EPPRA</td>
<td>France</td>
</tr>
<tr>
<td>Kingston University Higher Education Corporation</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>SODERN</td>
<td>France</td>
</tr>
<tr>
<td>Smiths Heimann S.A.S.</td>
<td>Austria</td>
</tr>
<tr>
<td>Rail Cargo Austria</td>
<td>France</td>
</tr>
<tr>
<td>CEA Commissariat à l’Énergie Atomique</td>
<td>France</td>
</tr>
<tr>
<td>Institut Franco-Allemand de Recherches de Saint-Louis</td>
<td>France</td>
</tr>
<tr>
<td>Turkish State Railways</td>
<td>Turkey</td>
</tr>
<tr>
<td>MER MEC S.p.A.</td>
<td>Italy</td>
</tr>
<tr>
<td>Société Nationale des Chemins de Fer</td>
<td>France</td>
</tr>
</tbody>
</table>
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, 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.

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.

The particular objectives of the project include: • a set of functional and non-functional requirements that will drive an effective security system design process.
**Information**

**Acronym:**
RIBS

**Grant Agreement N°:**
242497

**Total Cost:**
€ 4,406,966.80

**EU Contribution:**
€ 3,321,957.80

**Starting Date:**
1 November 2010

**Duration:**
36 months

**Coordinator:**

**UNIVERSITY COLLEGE LONDON**
Department of Security and Crime Science
2 - 16 Torrington Place
2 - 16 Torrington Place
WC1E 7HN, London,
UNITED KINGDOM

---

**Contact:**
**Dr Hervé Borrion**
Tel : +44(0)20 3108 3194
Mobile : n/a
Fax : +44(0)20 3108 3088
E-mail : h.borrion@ucl.ac.uk
Website : www.ribs-project.eu

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIVERSITY COLLEGE LONDON (UCL)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY (TECHNION)</td>
<td>Israel</td>
</tr>
<tr>
<td>H.PETROPOULEA&amp;CO (2E)</td>
<td>Greece</td>
</tr>
<tr>
<td>KUNGLIGA TEKNISKA HOEGSKOLAN (KTH)</td>
<td>Sweden</td>
</tr>
<tr>
<td>DANMARKS TEKNISKE UNIVERSITET (DTU)</td>
<td>Denmark</td>
</tr>
<tr>
<td>EFI (ANONYMISED NAME OF PARTNER)</td>
<td>Greece</td>
</tr>
<tr>
<td>AEDAS ARCHITECTS LIMITED (AEDAS ARCHITECTS)</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Project objectives

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

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

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

Description of the work

SAMURAI will develop robust moving object, segmentation, categorization and tagging in video captured by multiple cameras from medium-long range distance, e.g. identifying, monitoring and tracking people with luggage between different locations at an airport. Automated focus of attention and identification in a distributed sensor network includes fixed and mobile cameras, positioning sensors and wearable audio or video sensors.

Global situational awareness assessment involves image retrieval of objects by types and movement patterns with incidents across a distributed network of cameras. Online adaptive unusual behaviour monitoring will profile and check inference of unusual behaviours/events captured by multiple cameras. The project will also exploit methods for feeding back into the algorithm human operator’s evaluation on any abnormality detection output in order to guide and speed up the incremental and adaptive behaviour profiling algorithm. SAMURAI will allow prevention and rapid-response to events as they unfold.

Expected results

SAMURAI will develop groundbreaking technology that can be interfaced with existing CCTV systems already employed widely within the EU. By concentrating the technology developments onto multiple cameras and mobile cameras, many of the limitations of the existing state-of-the-art will be overcome by incorporating strong end-users with a widely deployed CCTV system in the Consortium.

Security in public places is required for the correct functioning of society. However, existing CCTV systems are not effective at prevention of many incidents. Consequently, by improving these current CCTV systems, the main social impact of SAMURAI should be increased public confidence in security systems in public places.

The use of CCTV as a security and management aid is widespread in the EU and offers a huge marketplace for European business.

SAMURAI should provide a higher ‘added-value’ to installed CCTV system and give European producers a substantial advantage in the marketplace.
Information

Acronym: SAMURAI

Grant Agreement N°: 217899

Total Cost: € 3,638,131

EU Contribution: € 2,478,052

Starting Date: 01/06/2008

Duration: 36 months

Coordinator:
QUEEN MARY, UNIVERSITY OF LONDON
Department of Computer Science
Mile End Road
E1 4NS London
United Kingdom

Contact:
Shaogang GONG
Tel: +44 20 7882 5249
Fax: +44 20 8980 6533
E-mail: sgg@dcs.qmul.ac.uk
Website: www.samurai-eu.org

Partners

NAME                        COUNTRY
Queen Mary, University of London    United Kingdom
Universita’ degli Studi di Verona    Italy
Elsag Datamat S.p.A.    Italy
Waterfall Solutions Ltd    United Kingdom
Borthwick-Pignon OÜ    Estonia
Esaprojekt SP. Z O.O.    Poland
Syndicat Mixte des Transports pour le Rhône et l’Agglomération Lyonnaise    France
BAA Limited    United Kingdom
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, 24h a day in all weather conditions by means of:
  • Near range equipment
  • Far range equipment

» Communicates security information of significance to the infrastructure authorities (sea masters, operation control managers, etc.) and to selected authorised third parties of importance for the overall security situation (port authorities, coast guards, etc.) in real time.

» Aggregates, reports and displays any security-related information of significance in an intuitively understandable way. Reliably raises alarms in identified situations.

» Enables response procedures and actions to be undertaken in situations that require effective use of protective measures.

» Demonstrates system effectiveness in real maritime infrastructures.
Information

Acronym: SECTRONIC

Grant Agreement N°: 218245

Total Cost: € 7,080,433

EU Contribution: € 4,496,414

Starting Date: 01/02/2008

Duration: 48 months

Coordinator:
MARINE & REMOTE SENSING SOLUTIONS LTD
Suite 100
Saint-James Place 11
UK – SW1A 1NP London
United Kingdom

Contact:
Dr. Sverre Dokken
Tel.: +44 20 7871 2800
E-mail: sdokken@marss.co.uk
Website: www.sectronic.eu

Partners

NAME
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
Project objectives

SECUR-ED 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 inter-modal environments (transport nodes), taking into account various legal, cultural and societal environment.

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

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

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

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

Expected results

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

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

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

**Acronym:**
SECUR-ED

**Grant Agreement N°:**
261605

**Total Cost:**
€ 40,187,354.70

**EU Contribution:**
€ 25,468,072.00

**Starting Date:**
01/04/2011

**Duration:**
42 months

**Coordinator:**

THALES SECURITY SOLUTIONS & SERVICES SAS
Domain CTS
20-22 Rue Grange Dame Rose
78141 Velizy-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@thalesgroup.com
Website: www.secur-ed.eu

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thales Security Solutions &amp; Services SAS (THA)</td>
<td>France</td>
</tr>
<tr>
<td>Alstom Transport S.A. (ALS)</td>
<td>France</td>
</tr>
<tr>
<td>Ansaldo STS S.p.A. (ANS)</td>
<td>Italy</td>
</tr>
<tr>
<td>Azienda Trasporti Milanesi (ATM)</td>
<td>Italy</td>
</tr>
<tr>
<td>Bombardier Transportation GMBH (BOM)</td>
<td>Germany</td>
</tr>
<tr>
<td>Commissariat à l’énergie atomique et aux énergies alternatives (CEA)</td>
<td>France</td>
</tr>
<tr>
<td>Consorcio Regional de Transportes de Madrid (CTM)</td>
<td>Spain</td>
</tr>
<tr>
<td>Deutsche Bahn AG (DBA)</td>
<td>Germany</td>
</tr>
<tr>
<td>European Organisation for Security SCRL (EOS)</td>
<td>Belgium</td>
</tr>
<tr>
<td>Edisoft - Empresa de servicios e desenvolvimento de software SA (EDI)</td>
<td>Portugal</td>
</tr>
<tr>
<td>Totalforsvaret Forskningsinstitut (FOI)</td>
<td>Norway</td>
</tr>
<tr>
<td>Fraunhofer-GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG E.V (FHG)</td>
<td>Germany</td>
</tr>
<tr>
<td>HAMBURG-CONSULT GESELLSCHAFT FUER VERKEHRSBERATUNG M.B.H (HCO)</td>
<td>Germany</td>
</tr>
<tr>
<td>Ingenieria y Consultoria para el Control Automatico, SL (ICC)</td>
<td>Spain</td>
</tr>
<tr>
<td>INOV, INESC INOVACAO, INSTITUTO DE NOVAS TECNOLOGIAS (INO)</td>
<td>Portugal</td>
</tr>
<tr>
<td>JRC - JOINT RESEARCH CENTRE- EUROPEAN COMMISSION (JRC)</td>
<td>Belgium</td>
</tr>
<tr>
<td>Regia Autonoma de Transport Bucuresti (RTB)</td>
<td>Romania</td>
</tr>
<tr>
<td>EMEF, SA - Empresa de Manutencao de Equipamento Ferroviario, SA (EME)</td>
<td>Portugal</td>
</tr>
<tr>
<td>MTR S3 Solutions and Services LTD (MTR)</td>
<td>Israel</td>
</tr>
<tr>
<td>NICE SYSTEMS LTD (NIC)</td>
<td>Israel</td>
</tr>
<tr>
<td>Universitaet Paderborn (UPB)</td>
<td>Germany</td>
</tr>
<tr>
<td>Régie Autonome des Transports Parisiens (RTP)</td>
<td>France</td>
</tr>
<tr>
<td>Morpho (MPH)</td>
<td>France</td>
</tr>
<tr>
<td>Empresa Municipal de Transportes de Madrid SA (EMT)</td>
<td>Spain</td>
</tr>
<tr>
<td>Ministère de l’Intérieur, de l’Outremer et des collectivités territoriales Direction de la défense et de la sécurité civile (STS)</td>
<td>France</td>
</tr>
<tr>
<td>Société Nationale des Chemins de Fer Français (SNF)</td>
<td>France</td>
</tr>
<tr>
<td>FNMA SPA (FNM)</td>
<td>Italy</td>
</tr>
<tr>
<td>Universitetet i Stavanger (STA)</td>
<td>Norway</td>
</tr>
<tr>
<td>Société des Transports Intercommunaux de Bruxelles SSF (STI)</td>
<td>Belgium</td>
</tr>
<tr>
<td>NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK - TNO (TNO)</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Technische Universitaet Dresden (TUD)</td>
<td>Germany</td>
</tr>
<tr>
<td>Union Internationale des Transports Publics - UITP (UIJ)</td>
<td>Belgium</td>
</tr>
<tr>
<td>Union des Industries Ferroviaires Européennes - UNIFE (UNI)</td>
<td>Belgium</td>
</tr>
<tr>
<td>TEKNOLOGIAN TUTKIMUSKESKUS VTT (VTT)</td>
<td>Finland</td>
</tr>
<tr>
<td>Julius-Maximilians Universitaet Wuerzburg (WUE)</td>
<td>Germany</td>
</tr>
<tr>
<td>Ingenieria y Economia del Transporte S.A. (INE)</td>
<td>Spain</td>
</tr>
<tr>
<td>G. Team Security Ltd (GTE)</td>
<td>Israel</td>
</tr>
<tr>
<td>AXIS Communications Aktiebolag (AXI)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Turkkiye Cumhuriyeti Devlet Demir Yollari Isletmesi Genel Mudurlugu (TCD)</td>
<td>Turkey</td>
</tr>
</tbody>
</table>
Project objectives

The SeRoN project undertakes a holistic approach both at infrastructure object and road network level. Its main objectives are to investigate the impacts of possible man-made attacks on the transport network, in particular the resulting regional and supraregional impacts on transport links and their economic impacts. SeRoN focuses on the development and validation of an innovative methodology which is to provide a common framework for the analysis of critical road infrastructure objects or road transport networks with regard to their importance within the European transport network and regard to possible attacks. This methodology is based on an interdisciplinary interaction of expertise and innovative simulation methods. Furthermore, possible protection measures for critical road transport infrastructures can suitably be chosen and evaluated regarding their impact on security and cost-effectiveness.

Description of the work

First a comprehensive threat analysis for transport infrastructures focusing on man-made attacks is carried out. Then data on relevant infrastructure types and classes of the Trans-European road network is gathered, with so-called “partner regions” being more comprehensively covered. Data provided will be evaluated to identify generic infrastructure types and classes which are critical in terms of vulnerability to man-made attacks, e.g. due to their type of construction, and to classify them based on the risk they are exposed to. The results provide the input data for a knowledge database intended to be a means to manage and maintain categorised critical infrastructures and associated protection measures. Such object information is needed for the calculations at network level analysing the importance of individual infrastructures. Their vulnerability will be determined in probable scenarios, studying the impacts of a failure of critical (parts of) infrastructures and the resulting traffic disturbances using scenario analysis and macroscopic traffic flow models. Network data will include information about location and importance of infrastructures in the road network, traffic loads, etc. Thus critical infrastructures of the road network can be identified and ranked according to priority. The risk assessment includes the impact assessment for the respective infrastructure based on different occurrence scenarios with related event sequences. Vulnerabilities are estimated using the local traffic conditions and simulations, e.g. escape simulations, explosives and smoke propagation simulations. Security improvements will be determined and monetary and economic impacts of different measures examined by means of cost-benefit analyses to identify the most effective security measures. Finally at few suitable examples the new developed methodology will be validated before recommendations for infrastructure owners will be formulated taking into account external expert knowledge gained in workshops.

Expected results

The SeRoN results include a knowledge database, an innovative methodology and recommendations covering macro-economic, institutional and organisational and technical issues. They will allow infrastructure owners and operators developing strategies to improve the security of transport structures and to select investments into countermeasures and risk mitigation strategies. The developed methodology may be transferred to transport networks used by other traffic modes and to natural disasters.
**Information**

**Acronym:**
SeRoN

**Grant Agreement N°:**
225354

**Total Cost:**
€ 2,942,113

**EU Contribution:**
€ 2,246,110

**Starting Date:**
01/11/2009

**Duration:**
36 months

**Coordinator:**
PLANUNG TRANSPORT VERKEHR AG
Dr. Georg Mayer

**Contact:**
Dr. Georg Mayer
Planung Transport Verkehr AG
Kriegerstr. 15
D-70191 Stuttgart
Germany
georg.mayer@ptv.de

Dr. Christoph Walther
Planung Transport Verkehr AG
Stumpfstr. 1
D-76131 Karlsruhe
Germany
christoph.walther@ptv.de
www.ptv.de
Website: www.seron-project.eu

**Partners**

**NAME**
PTV Planung Transport Verkehr AG
Bundesanstalt für Straßenwesen (BASt)
Parsons Brinckerhoff
Technische Universität Graz
Traficon n.v
Ernst Basler und Partner
NIRAS A/S

**COUNTRY**
Germany
Germany
United Kingdom
Austria
Belgium
Switzerland
Denmark
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 develops a Decision Support System for the protection of the European power transmission, distribution and generation system. This Decision Support System enables to:

- identify the vulnerabilities of the analyzed grid and production plants and to 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 and
- 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, designs 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 developed. This project does not only consider the physical network, with its control and communication structure, as 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 are 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 the 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
Information

**Acronym:**
SESAME

**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  
Website: —

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politecnico di Torino (PoliTo)</td>
<td>Italy</td>
</tr>
<tr>
<td>Energy Institute at the J. Kepler University Linz (EI-JKU)</td>
<td>Austria</td>
</tr>
<tr>
<td>INDRA Sistemas SA (INDRA)</td>
<td>Spain</td>
</tr>
<tr>
<td>Heriot Watt University (HWU)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>e- Control (Ectrl)</td>
<td>Austria</td>
</tr>
<tr>
<td>Deloitte (Delo)</td>
<td>Spain</td>
</tr>
<tr>
<td>TU Delft (TUD)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Transelectrica (TrEI)</td>
<td>Romania</td>
</tr>
<tr>
<td>Kudos Research (KUDOS)</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
STAR-TRANS / Strategic risk assessment and contingency planning in interconnected transport networks

Project objectives

The fundamental assumption within STAR-TRANS is that transportation assets, such as airplanes and tunnels, are integral part of larger systems. Taken together, individual transportation networks form a “network of networks”. This provides a basis for an integrated EU-wide approach to risk management in transportation networks that would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States.

STAR-TRANS contribution to the risk assessment process in transportation networks is the recognition of the importance that the impact of a risk incident might have on the assets of the whole ‘network of networks’.

The project outcome will offer important aids for decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences, (cost, timing, resources, etc) of proposed actions.

A specialised software system will be developed that will support the end users, and network operators needs.

The objectives of the STAR-TRANS project are:

To produce a security risk assessment framework for European interdependent and interconnected transport networks and to evaluate the proposed risk assessment framework in two cities.

Description of the work

The aim of proposed transportation security risk assessment framework is to formalise the linkage between risk incidents, transportation network assets and dependency types between assets in order to assess the impact of an incident on the affected interconnected and interdependent networks at the ‘network of networks’ level. In particular, STAR-TRANS intends to:

1. formalise the impact assessment process at the ‘network of networks’ level;
2. develop ICT tools that support the formalised impact assessment process; and
3. trial & evaluate the developed impact assessment process and tools.

The STAR-TRANS comprehensive risk assessment approach targets at the security operation of the European transport networks. STAR-TRANS will be guided by a holistic risk assessment methodology for critical infrastructure for the analysis and assessment of common issues for risks, threats and vulnerabilities.

Within the STAR-TRANS framework, security risk in the integrated transportation networks will be defined as the combination of:

1. Vulnerability, reflecting the possibility of a risk incident, e.g. terrorist attack, to the interdependent and interconnected European transport networks, compared to the possibility of protecting it through inherent or managed safeguards.
2. Consequences of a successful attack, which is defined using (i) the possible number of causalities / fatalities, (ii) disruption and recovery time and (iii) the economic impact.

The combined approach of various transport networks in one risk assessment tool will allow for easy information exchange between different networks and infrastructure elements / facilities.

Expected results

It aims to develop and apply system analysis methods to assess the risk, vulnerability, safety and security elements of complex systems and critical infrastructures supporting road, and inter-modal transport. Emphasis is given on the study and development of open service-oriented architecture and software standards to support risk management and contingency planning.

The proposed STAR-TRANS actions in the area of transportation security will provide the technology basis and relevant knowledge for security capabilities needed in this area, while achieving a significant improvement with respect to performance, reliability, speed and cost and will reinforce the European industry’s potential to create important market opportunities.
Information

Acronym:
STAR-TRANS

Grant Agreement N°:
225594

Total Cost:
€ 3,195,188.88

EU Contribution:
€ 2,105,588.94

Starting Date:
01/11/2010

Duration:
30 months

Coordinator:

INTRASOFT INTERNATIONAL S.A.
Rue Nicolas Bové
1253 Luxembourg
Luxembourg

Contact:
Dr. Antonios Ramfou
E-mail: antonis.ramfou@intrasoft-intl.com
Website: www.startrans-project.eu

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRASOFT International SA</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>National Centre for Scientific Research Demokritos - Environmental</td>
<td>Greece</td>
</tr>
<tr>
<td>Research Laboratory</td>
<td></td>
</tr>
<tr>
<td>Center for Security Studies</td>
<td>Greece</td>
</tr>
<tr>
<td>Confederation of Organisations in Road Transport Enforcement</td>
<td>Belgium</td>
</tr>
<tr>
<td>QinetiQ SA</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Fraunhofer Institute for Transportation and Infrastructure Systems</td>
<td>Germany</td>
</tr>
<tr>
<td>Centre for Research and Technology Hellas - Informatics &amp; Telematics</td>
<td>Greece</td>
</tr>
<tr>
<td>Institute</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Metropolitan Police Service</td>
<td>Cyprus</td>
</tr>
<tr>
<td>CTL Cyprus Transport Logistics Ltd</td>
<td>Belgium</td>
</tr>
<tr>
<td>SQUARIS Ltd</td>
<td></td>
</tr>
</tbody>
</table>
SUBITO / surveillance of unattended baggage and the identification and tracking of the owner

Project objectives

SUBITO will research and develop automated detection of abandoned luggage, fast identification of the individual responsible and the tracking of their subsequent path.

The consortium, a diverse group of technology and implementation experts from across the EU, will develop an integrated threat detection system that provides a robust, timely alert to security personnel. Working closely with the end users, the team will design a system that is capable of distinguishing between genuine threats and false alarms in order to alert the user to high priority situations.

Key objectives are:

» Find abandoned luggage and identify and track the owner.
» Reduce the number and impact of false alarms.
» Demonstrate automated detection of abandoned goods, fast identification of individual who left them and fast determination of the individual’s location or their path.
» Demonstrate a scalable route to implementation.
» Examine the wider user of technologies for explosive threat identification in this context.
» Examine the use of camera technologies to distinguish between threatening and non-threatening goods.
» Manage public perception of this technology and its implications.

Description of the work

In recent years, there has been a number of incidents where terror organisations have planted explosive devices in ordinary baggage to cause immense disruption in mass transportation networks and other areas of critical infrastructure.

The threat of unattended baggage has led to increased vigilance amongst security personnel and the general public to ensure that unattended baggage is reported and investigated with utmost urgency. In conjunction with the introduction of enhanced CCTV, this has enabled an increase in the breadth and scope of data that can be collected at key locations. Unfortunately, this has not been matched by a corresponding improvement in the capabilities of systems to interpret and filter the data. This has remained the duty of trained human operators who often do not have the capacity to process the breadth of data that is received.

Consequently, the increase in data availability has been met by an increase in the number of false alarms; situations where unattended baggage has been incorrectly considered a potential threat. Often, due to the pressure to act quickly, the situational data is only analysed once a major event has occurred. This has resulted in unnecessary disruption to business operations, with associated cost implications and a lack of confidence regarding security procedures and equipment.

Building upon existing surveillance technology, the SUBITO programme will deliver a demonstration of semi-automated data processing designed to provide real-time detection of goods that have been abandoned. At the same time, the system will identify the individual who left the goods and will utilise the surveillance network to determine the current location of that individual and track their followed path. SUBITO will improve the efficiency of security personnel by automatically filtering out the major false alarms and therefore focusing their attention only on credible threats.

Expected results

With the help of our end user partners, SUBITO will demonstrate that a solution to this problem is achievable using existing infrastructure and security technologies from real locations operating under standard procedures.

SUBITO aims to deliver a generic approach that can be also applied to solve similar problems in more diverse applications. In addition the programme will carry out supporting studies investigating the benefits of incorporating additional sensors and controllable cameras to the system.
Information

Acronym: SUBITO
Grant Agreement N°: 218004
Total Cost: € 3,895,730
EU Contribution: € 2,581,055
Starting Date: 01/01/2009
Duration: 31 months

Coordinator:
SELEX SENSORS AND AIRBORNE SYSTEMS LIMITED
2 Crewe Road North
Edinburgh - EH5 2XS
Scotland
United Kingdom

Contact:
Ms Georgette Murray
Mark Riddell
Tel: +44(0)131 343 5992
Fax: +44(0)131 343 8110
E-mail: mark.riddell@selexgalileo.com
Website: www.subito-project.eu

Partners

NAME
SELEX Sensors and Airborne Systems Limited
ELSAG DATAMAT S.p.A
Office National d’Etudes et de Recherches Aérospatiales
L-1 Identity Solutions AG
CEA
University of Leeds
University of Reading
VTT
Österreichisches Forschungs und Prufzentrum Arsenal Ges.m.bH
Fiera di Genova S.p.A

COUNTRY
United Kingdom
Italy
France
Germany
France
United Kingdom
United Kingdom
Finland
Austria
Italy
TASS / Total airport security system

Project objectives

TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on integrating different types of selected real time sensors & sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions. TASS divides the airport security into six security control segments (environmental, cargo, people, airplanes, vehicle-fleet & facilities) each of them being monitored by various technologies that are fused together, creating a multsource labyrinth fusion logic enabling situational and security awareness of the airport anytime and anywhere. These fused control segments will be accessed through the TASS WEB-based portal by running a suite of applications making the airport security control centralized to all airport authorities. The integration will include the use of in-place technologies that will result in a cost-effective solution.

Description of the work

The overall mission of the TASS consortium is to research, develop and illustrate the capabilities of the data collection tools (which are mainly based on sensing real time technologies), the data fusion mediation system and portal and web based applications. TASS aims to integrate all these elements into one consolidated system where all the collected information is analyzed, alerted and viewed by the airport C3.

Although the array of sensors used in the TASS project consists of sensors based on both new and existing technologies, their integration and the fusion of their data will form an innovative centralized system which will provide an efficient method for securing an airport without affecting the passengers and flow of commerce.

The aim of this multidisciplinary Integrated FP7 Project is to ensure that TASS provides the airports’ C3 systems with the actionable information that they seek, in order to allow an effective timely response.

The envisaged TASS system architecture and the research to be performed in TASS consists of 3 main parts: (i) Data collection, sensing and alert technologies which will cover the airport, (ii) Data fusion which will gather the information generated by these sensors and fuse it, to create a comprehensive, real time, security overview of the airport and (iii) a new TASS C2 portal and related Webbased applications which will analyze and display the collected data of each operational area.

During the development stage there will be a strong emphasis on the end-user (airports) insights, needs and remarks. Based on these requirements, TASS will provide the appropriate tools to enable C2 operators to respond in real-time to security situations in the airport.

The TASS consortium brings together European airports, innovative SME’s, industrial and academic partners. The TASS solutions will be tested at several European airports including the hub airport Heathrow and Athens airport, in order to cover a wide range of needs at different levels of airport protection. The main test at Heathrow airport will involve scenarios including 2 connected to the upcoming 2012 Olympic Games in London.

Expected results

The TASS project aims to create an entire airport security monitoring solution while increasing the reliability and efficiency of the security screening while respecting the airport passengers’ privacy.

TASS will provide real-time accurate situational awareness of all airport facilities and its surroundings (perimeters, terminal, access-points, sensitive areas etc.), as well as of its people (passengers, employees etc.), vehicles, cargo and airplanes.
Information

Acronym: TASS

Grant Agreement N°: 241905

Total Cost: € 15,544,276.60

EU Contribution: € 8,986,696.15

Starting Date: 01/04/2010

Duration: 48 months

Coordinator:

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

Contact:
Mr. Gideon Hazzani
Phone: +972 9 962 2596
Fax: +972 9 962 4747
E-mail: Gideon.Hazzani@verint.com

Partners

NAME
Verint Systems Ltd
BAA Limited
Grupo Mecanica del Vuelo Sistemas S.A.
Rapiscan Systems Limited
Consorzio per la Ricerca Nell’ Automatica e Nelle Telecomunicazioni C.R.A.T
National Center for Scientific Research «Demokritos»
GMVIS Skysoft SA
Mentum SA
Vitrociset Spa
Alcatel-Lucent Italia S.P.A
The Provost Fellows & Scholars of the College of the Holy and Undivided Trinity of Queen Elizabeth near Dublin
IMEGO AB
Elbit Security Systems Ltd
Athens International Airport SA
Real Fusio France
Immersion SAS
Red-M Wireless Ltd.
BAE Systems (Operations) Ltd
Ernst & Young (Israel) Ltd

COUNTRY
Israel
United Kingdom
Spain
United Kingdom
Italy
Greece
Portugal
France
Italy
Italy
Ireland
Sweden
Israel
Greece
France
France
United Kingdom
United Kingdom
Israel
**VITRUV / Vulnerability Identification Tools for Resilience Enhancements of Urban Environments**

**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 **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 **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 on 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.
Information

Acronym: VITRUV

Grant Agreement N°: 261741

Total Cost: € 4,520,921.80

EU Contribution: € 3,339,898.00

Starting Date: DD/MM/YYYY

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

Partners

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

At present, Blue Border Surveillance is carried out predominantly by coast guard ships, aeroplanes and helicopters. These expensive measures are only fragmentary. They are not suitable to locate small boats within a wider maritime area and they do not allow a continuous 24 h/7 surveillance as a countermeasure to illegal immigration.

Concept

The surveillance system developed under the AMASS project will form an array of autonomous, automated surveillance platforms with active and passive sensors. The key sensors being used are high-end technology-un-cooled thermal imagers and highly sophisticated Hydrophones linked together via a wideband radio network. Alarms from the sensors will be analysed and integrated with back ground details (location, speed, class, …) into a "Geographical Information System" situated within a blue border command centre.

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

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

Project objectives

Based on in depth research into the situational data a good understanding of the operational as well as technical requirements of such a highly sophisticated surveillance system is forming the basis of this project. With AFM and ICCM acting as end users, tests at the end of the project will be under realistic conditions in territorial waters of countries (Malta / Canary Islands) highly affected by illegal immigration.

System configuration

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

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

Aim

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

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

Acronym: AMASS
Grant Agreement N°: 218290
Total Cost: € 4,970,709
EU Contribution: € 3,580,550
Starting Date: 01/03/2008
Duration: 42 months

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

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carl Zeiss Optronics GmbH</td>
<td>Germany</td>
</tr>
<tr>
<td>Crabbe Consulting Ltd</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Armed Forces Malta</td>
<td>Malta</td>
</tr>
<tr>
<td>Instituto Canario de Ciencias Marinas</td>
<td>Spain</td>
</tr>
<tr>
<td>Fugro Oceanor</td>
<td>Norway</td>
</tr>
<tr>
<td>OBR Centrum Techniki Morskiej</td>
<td>Poland</td>
</tr>
<tr>
<td>Fraunhofer Institut Informations- und Datenverarbeitung</td>
<td>Germany</td>
</tr>
<tr>
<td>IQ-Wireless</td>
<td>Germany</td>
</tr>
<tr>
<td>HSF</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>University of Las Palmas de Gran Canaria</td>
<td>Spain</td>
</tr>
</tbody>
</table>
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, on 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 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 to obtain 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 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 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 capability to evaluate the altitude of non cooperative vehicles (using only PSR 3D);

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

Expected results

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

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

Coordinator:
Selex Sistemi Integrati SpA
Civil Systems Business Unit
Via Tiburtina, 1231
n.a.
00131 Rome
Italy

Contact:
Claudia Fusai
Tel: +39 06 4150 5370
Mobile: n.a.
Fax: + 39 06 4150 2043
E-mail: cfusai@selex-si.com
Website: http://www.argus3d.eu/

Partners

NAME COUNTRY
Selex Sistemi Integrati (SELEX-SI) Italy
SESM Scarl (SESM) Italy
Università “La Sapienza” di Roma Dip. di Scienza e Tecnica dell’Informazione e della Comunicazione (INFOCOM) Italy
Przemysłowy Instytut Telekomunikacji S.A. (PIT) Poland
University College of London (UCL) United Kingdom
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. (FRAUNHOFER) Germany
ENAV S.p.A (ENAV) Italy
ECONET S.L. (ECONET) Spain
Dependable Real Time Systems Ltd. (DRTS) United Kingdom
ISO Software Systeme GmbH (ISO) Germany
REDHADA S.L. (REDHADA) Spain
CiaoTech Srl (CTECH) Italy
**CASSANDRA / Common assessment and analysis of risk in global supply chains**

**Project objectives**

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 enabled to fully adopt a risk based approach to their operational activities, and in particular to combine two strategic customs approached: the Risk-based approach with the System-based audit approach. As such, it is a more balanced approach then the US driven approach towards 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, 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 defines 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, contains 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**

CASSANDRA will:

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

Acronym: CASSANDRA

Grant Agreement N°: —

Total Cost: €14,813,514

EU Contribution: €9,958,749

Starting Date: 01/05/2011

Duration: 36 months

Coordinator:
Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO
Mobiliteit & Logistiek
Van Mourik Broekmanweg 6
PO Box 49
2600 AA Delft
The Netherlands

Contact:
Heather Griffioen-Young
Tel: +31 (0)888665931
Mobile: +31 (0)622461065
Fax: +31-346 353 977
E-mail: heather.griffioen@tno.nl
Website: www.tno.nl

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

© CASSANDRA
EFFISEC / Efficient integrated security checkpoints

**Project objectives**

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

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

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

**Description of the work**

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

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

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

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

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

**Expected results**

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

» allowing systematic in depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles, through the use of automatic gates and portable identity check and scanning equipment,

» providing objective criteria for submitting some travellers/vehicles/luggage to an extensive check in specific lanes.

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

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

Acronym: EFFISEC

Grant Agreement N°: 217991

Total Cost: € 16,310,974

EU Contribution: € 10,034,837

Starting Date: 01/05/2009

Duration: 54 months

Coordinator:

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

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sagem Sécurité</td>
<td>France</td>
</tr>
<tr>
<td>Thales Security Solutions &amp; Services</td>
<td>France</td>
</tr>
<tr>
<td>MultiX</td>
<td>France</td>
</tr>
<tr>
<td>Selex Galileo</td>
<td>Italy</td>
</tr>
<tr>
<td>Elsag Datamat Spa</td>
<td>Italy</td>
</tr>
<tr>
<td>Smiths Heimann</td>
<td>Germany</td>
</tr>
<tr>
<td>Sociedad Europea de Analisis Diferencial de Movilidad</td>
<td>Spain</td>
</tr>
<tr>
<td>VTT</td>
<td>Finland</td>
</tr>
<tr>
<td>FOI</td>
<td>Sweden</td>
</tr>
<tr>
<td>University of Reading</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Ministry of Interior – Romanian Border Police</td>
<td>Romania</td>
</tr>
<tr>
<td>Secalliance</td>
<td>France</td>
</tr>
<tr>
<td>MC2</td>
<td>France</td>
</tr>
<tr>
<td>Port of Lisbon</td>
<td>Portugal</td>
</tr>
<tr>
<td>JRC</td>
<td>European Union</td>
</tr>
<tr>
<td>Thales Security Systems Portugal</td>
<td>Portugal</td>
</tr>
</tbody>
</table>
Project objectives

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

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

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

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

Description of the work

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

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

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

» Knowledge of the problems from the user’s perspective. Addressing border problems from their point of view is key in obtaining useful information for the roadmap.

» Consortium’s extensive hands-on experience in border management projects. All the companies in the consortium had vast experience in working with the end users on the day to day challenge of border management.

» Integration as the driving force. The challenge in this project was not how to improve individual technologies, but rather to understand what they provide and create a framework for their interaction.

» Move beyond technology. Threats such as illegal immigration and smuggling of illegal goods and materials must be considered.

» The Broad border framework. Country of origin, transit areas, regulated and unregulated border lines and internal territory.

Results

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

**Acronym:** GLOBE

**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/

---

**NAME**

- Telvent Interactiva S.A.  
- Amper Sistemas S.A.  
- GMV Aerospace and Defence, S.A  
- Fundación Robotiker  
- 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  

**COUNTRY**

- Spain  
- Spain  
- Spain  
- Spain  
- Spain  
- France  
- Slovenia  
- Poland  
- Belgium  
- Portugal  
- Hungary  
- Norway  
- Portugal  
- Austria
**Project objectives**

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 generate justified alarms.
- Understanding of suspicious events and early identification of threats from series of detected spatiotemporal abnormal vessel behaviours (alarms).
- Generate electronic and formatted interpretation reports on the suspicious event to keep periodically informed decisional authorities.

**Description of the work**

The tasks to perform in the I2C integration project are:

- To test the fusion of data from a bench of sensors and other available intelligent information sources in order to perform optimal maritime security awareness.
  
  To do so:
  
  - Two coastal sites are installed with a set of sensors. These shore based platforms provide measurements (AIS messages, radar vessel tracks and optical imageries) to elaborate a maritime situational picture for all vessel types. Platforms at sea will also be deployed (aircraft & vessel patrols, Zeppelin and USV) to provide local node surveillance.
  
  - Fusion of all sensors 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.), to provide an intelligent maritime situational picture.
  
  - Applying rules on verified vessel conditions, to detect the abnormal vessel behaviours, then, alarms are issued to operator for validation. Examples of rules are:
    
    - Vessels boarding during night and with low wave height will generate an alarm on suspect event which can be analysed as trans-boarding of goods such as drugs.
    
    - Vessel stopped in international water during less than thirty minutes and with low surface current speed will generate an alarm on suspect event which can be analysed as dropping smuggling goods at sea.
    
  - Validated alarms are transferred to experts for understanding and identification of threats. Experts use tool kit to analyse the history of the alarm and its evolution during time with the help of knowledge models about 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, to detect suspicious events and early identification of associated threats.
- Assess the added value of the various sensor types and the integrated data processing according to various threats and detection conditions.
- Demonstration, that the integrated system fulfil the operational needs with prototypes installed in a few operational centres.
Information

Acronym: I2C

Grant Agreement N°: 242340

Total Cost: € 15,962,707

EU Contribution: € 9,869,621

Starting Date: 01/10/2010

Duration: 48 months

Coordinator:
DCNS SA
Direction Systèmes d’Information et de Surveillance
Rond point des artilleurs de marine
B.P. 403
83055 Toulon
France

Contact:
Michel Morel
Tel: + 33 (0) 498 039 259
Mobile: + 33 (0) 699 812 771
Fax: + 33 (0) 498 039 257
E-mail: Michel.Morel@dcnsgroup.com
Website: www.i2c.eu

Partners

NAME
ROCKVELL COLLINS France
FURUNO FINLAND OY
SES ASTRA TechCom SA
KONGSBERG NORTCONTROL IT A/S
KONGSBERG SPACETEC A/S
CLEARPRIORITY SA
ZLT ZEPPELIN LUFTSCHIFFTECHNIK GMBH ET CO KG
METEOSIM SL
AJECO OY
AIRSHIPVISION INTERNATIONAL SA
ECOMER
INTUILAB
SOFRESUD
ERIC VAN HOODYNOK ADVOCATEN
ARMINES
UNIVERSITE PAUL SABATIER III
ONERA
JOINT RESEARCH CENTRE
DEUTSCHE ZEPPELIN REDEREI GMBH

COUNTRY
France
Finland
Luxembourg
Norway
Norway
Belgium
Germany
Spain
Finland
France
France
France
Belgium
France
France
Belgium
Germany
Project objectives

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

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

Description of the work

IMCOSEC was guided by the following approach:

» Identification of security gaps based on the current processes, e.g. using the resilience matrix approach.

» Elaboration of target processes for closing these gaps and ensuring product integrity is supported by technologies either already deployable or under development.

» Identification of existing technologies to support and improve the container transport chain and integrate security.

» Consideration of ongoing projects and their intended results as well as parallel actions.

» Identification of additional requirements for R&D actions where these gaps cannot be closed by existing measures or research.

» Provision of a roadmap for demonstration activities where target processes and supporting technologies can establish efficiency, effectiveness and acceptance.

» Development of a guideline to improve existing or develop new technologies in order to meet the requirement given by the developed research roadmap.

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

Results

The major result of IMCOSEC was to provide a basic concept and roadmap for a large scale demonstration where intermodal chains are supposed to be demonstrated as “secure” corridors with effective processes and state of the art information, security and component technologies.
Information

Acronym:
IMCOSEC

Grant Agreement N°:
242295

Total Cost:
€ 1,142,591

EU Contribution:
€ 930,718

Starting Date:
01/04/2010

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bureau International des Containers et du transport intermodal (BIC)</td>
<td>France</td>
</tr>
<tr>
<td>CBRNE Ltd (CBRNE)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>INSTITUT FUER SEEVERKEHRSWIRTSCHAFT UND LOGISTIK (ISL)</td>
<td>Germany</td>
</tr>
<tr>
<td>International Container Security Organisation (ICSO)</td>
<td>Belgium</td>
</tr>
<tr>
<td>POLITECNICO DI MILANO (POLIMI)</td>
<td>Italy</td>
</tr>
<tr>
<td>STUDIENGESELLSCHAFT FUR DEN KOMBINIERTEN VERKEHR EV (SGKV)</td>
<td>Germany</td>
</tr>
<tr>
<td>TECHNISCHE UNIVERSITAET HAMBURG-HARBURG (TUHH)</td>
<td>Germany</td>
</tr>
<tr>
<td>TSB Innovationsagentur Berlin GmbH (FAV)</td>
<td>Germany</td>
</tr>
<tr>
<td>Union Internationale des sociétés de transport combiné Rail Route (UIRR)</td>
<td>Belgium</td>
</tr>
</tbody>
</table>
LOGSEC / Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security

Project objectives

The LOGSEC project had the following three main objectives:

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

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

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

Description of the work

The LOGSEC project team 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.
Information

Acronym: LOGSEC

Grant Agreement N°: 241676

Total Cost: € 800,047

EU Contribution: € 753,373

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

Partners

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

COUNTRY  
Spain  
Switzerland  
Belgium  
Belgium  
United Kingdom  
United Kingdom  
Switzerland
OPARUS / Open architecture for UAV-based surveillance system

Project Objectives

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

Description of the work

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

» WP 1 (Concepts and Scenarios) is dedicated to compilation and analysis of the operational concepts and scenarios of UAS use in the context of maritime and land aerial surveillance of European borders. The border surveillance missions that could be performed by UAS will be identified, and then further refined into scenarios in order to provide an operational framework to the architecture design. This task will propose complete concepts of data / information exchange between scenarios participants, including operational protocols. In this phase the end-user needs will be taken into account through direct exchange (Workshop).

» WP 2 (Legislation Analysis) intends to describe the current and emerging regulation framework for insertion of UAS into controlled civil airspace in order to identify its limitations regarding UAS border surveillance operations, and to recommend some legislation evolutions favouring the UAS use in border surveillance.

» WP 3 (Technical Analysis) is a central task dedicated to the parallel analysis and synthesis of the technical capabilities available for four main UAS components: the surveillance sensors, the aerial platforms, the datalink and communication networks and the ground stations. Generic classes of UAS components will be defined and described in terms of performances and costs.

» WP 4 (Open Architecture Definition) is dedicated to the identification of open architecture solutions to perform border surveillance missions. This task particularly focuses on cost-efficient solutions enabling maximum efficiency of UAS operations for European border surveillance.

» WP 5 (Information Exchange and Dissemination) is a Work Package dedicated to maintain a close communication level with the end-users, grouped in a User Advisory Board, in order to acknowledge and to check project consistency with the end-users requirements.

Expected results

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

» Fostering non-proprietary solutions for equipments and sub-systems (sensors, platforms, data links, and ground stations).

» Allowing smaller companies and SME’s from many member countries to enter the market.

» Open-up the market for non-military companies.

» Develop the dialogue between European end-users and make international operations between different nations more feasible.

» Allow companies to share different parts of a more complex system which distributes development costs and risks to a broader basis. This will foster the development of industrial co-operation similar to the “Airbus model”.

» Provide an overall benefit to the end-users by optimisation of costs (through lower development costs) and mission efficiency. The customer is expected to get a system of different classes of sub-systems which can be selected for joint operations for more performance instead of having heavily competing single systems.

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

Acronym: OPARUS

Grant Agreement N°: 242491

Total Cost: € 1,188,313

EU Contribution: € 1,188,313

Starting Date: 01/09/2010

Duration: 18 months

Coordinator:

SAGEM DÉFENSE SÉCURITÉ
27 rue Leblanc,
75015 Paris
France

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

Partners

NAME
Sagem Défense Sécurité
AFIT (Air Force Institute of Technology)
BAE Systems
Dassault Aviation
DLR
EADS-CASA
IAI
INTA
ISDEFE
ONERA
Selex Galileo
Thales Communication
Thales Systèmes Aéroportés

COUNTRY
France
Poland
United Kingdom
France
Germany
Spain
Israel
Spain
Spain
France
Italy
France
France
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.

PERSEUS contributes to Europe’s efforts to monitor illegal migration and combat related crime and goods smuggling by proposing a large scale demonstration of a 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.

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, 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.
Information

Acronym: PERSEUS

Grant Agreement N°: 261748

Total Cost: € 43,644,979.60

EU Contribution: € 27,847,579.00

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/

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>EADS DEFENCE AND SECURITY SYSTEMS (EADS-DS)</td>
<td>France</td>
</tr>
<tr>
<td>DCNS SA (DCNS)</td>
<td>France</td>
</tr>
<tr>
<td>ENGINEERING INGEGNERIA INFORMATICA SPA (ENGINEERING)</td>
<td>Italy</td>
</tr>
<tr>
<td>INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA (ISDEFE)</td>
<td>Spain</td>
</tr>
<tr>
<td>EADS - CONSTRUCCIONES AERONAUTICAS S.A. (EADS-CASA)</td>
<td>Spain</td>
</tr>
<tr>
<td>NATIONAL CENTER FOR SCIENTIFIC RESEARCH «DEMOKRITOS» (NCSRD)</td>
<td>Greece</td>
</tr>
<tr>
<td>GUARDIA CIVIL ESPAÑOLA (GUARDIA CIVIL)</td>
<td>Spain</td>
</tr>
<tr>
<td>INSTITUTT FOR FREDSFORSKNING STIFTELSE (PRIO)</td>
<td>Norway</td>
</tr>
<tr>
<td>SAAB AKTIEBOLAG (SAAB)</td>
<td>Sweden</td>
</tr>
<tr>
<td>SES ASTRA TECHCOM SA (SES-ASTRA)</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>Ajeco Oy (AJECO)</td>
<td>Finland</td>
</tr>
<tr>
<td>INTUWFAB (INTUWFAB)</td>
<td>France</td>
</tr>
<tr>
<td>METEOSIM SL (METEOSIM)</td>
<td>Spain</td>
</tr>
<tr>
<td>LUXSPACE SARL (LUXSPACE)</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>SOFRESUD (SOFRESUD)</td>
<td>France</td>
</tr>
<tr>
<td>INOV, INESC INOVACAO, INSTITUTO DE NOVAS TECNOLOGIAS (INOV)</td>
<td>Portugal</td>
</tr>
<tr>
<td>SKYTEK LTD (SKYTEK)</td>
<td>Ireland</td>
</tr>
<tr>
<td>Laurea-ammattikorkeakoulut oy (LAUREA)</td>
<td>Finland</td>
</tr>
<tr>
<td>DFRC AG (DFRC)</td>
<td>Switzerland</td>
</tr>
<tr>
<td>BOEING RESEARCH &amp; TECHNOLOGY EUROPE S.L. (BR&amp;TE)</td>
<td>Spain</td>
</tr>
<tr>
<td>ECORYS NEDERLAND B.V. (ECORYS)</td>
<td>Netherlands</td>
</tr>
<tr>
<td>CORK INSTITUTE OF TECHNOLOGY (CIT)</td>
<td>Ireland</td>
</tr>
<tr>
<td>MINISTERE DE L’INTERIEUR, DE L’OUTREMER ET DES COLLECTIVITES TERRITORIALES DIRECTION DE LA DEFENSE ET DE LA SECURITE CIVILES (Mol France)</td>
<td>France</td>
</tr>
<tr>
<td>Força Aérea Portuguesa (FAP)</td>
<td>Portugal</td>
</tr>
<tr>
<td>SATWAYS - PROIONTA KAI YPIRESIES TILMATIKIS DIKTYAKON KAI TILEPIKINONIAKON</td>
<td>Greece</td>
</tr>
<tr>
<td>EFARMOGON ETAIRIA PERIORISMENIS EFTHINIS EPE (SATWAYS)</td>
<td>Greece</td>
</tr>
<tr>
<td>MINISTRY OF NATIONAL DEFENCE, GREECE (HMOD)</td>
<td>Italy</td>
</tr>
<tr>
<td>NATO Undersea Research Centre (NURC)</td>
<td>Greece</td>
</tr>
<tr>
<td>Ministry of Citizens Protection (MCP-HCG)</td>
<td>Greece</td>
</tr>
</tbody>
</table>
SECURITY RESEARCH

Intelligent surveillance and border security

SEABILLA / Sea border surveillance

**Project objectives**

» Define the architecture for cost-effective European sea border surveillance systems, integrating space, land, sea and air assets, including legacy systems.

» Apply advanced technological solutions to increase performances of surveillance functions.

» Develop and demonstrate on the field significant improvements in detection, tracking, identification and automated behaviour analysis of all vessels, including hard to detect vessels, in open waters as well as close to coast.

**Description of the work**

SEABILLA is based on requirements for sea border surveillance defined by experienced operational users. These requirements have been transformed into scenarios, representative of gaps and opportunities for fruitful cooperative information exchange between Member States:

» for fighting drug trafficking in the English Channel;

» for addressing illegal immigration in the South Mediterranean; and

» for fighting illicit activities in open-sea in the Atlantic waters from Canary Islands to the Azores in coherence with the EU Integrated Maritime Policy, with the EU Integrated Border Management Policy (ref. EUROSUR), and in compliance with Member States sovereign prerogatives.

**Expected results**

The project will provide a feasible, cost effective solution in terms of maritime surveillance, based on best combination of advanced technology in the context of legacy systems, that could be implemented at national and EU level to increase effectiveness, pool resources and address successfully Maritime Security and Safety challenges.
Information

Acronym: SEABILLA

Grant Agreement N°: 241598

Total Cost: € 15,549,679

EU Contribution: € 9,843,601

Starting Date: 01/06/2010

Duration: 45 months

Coordinator:
SELEX SISTEMI INTEGRATI SPA
Via Tiburtina km 12,400, 00131 Roma, Italy

Contact:
Salvatore RAMPINO
Tel: +39 06 4150 2407
Mobile: +39 3357389405
Fax: +39 06 41502694
E-mail: srampino@selex-si.com
Website: www.seabilla.eu

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELEX Sistemi Integrati SPA</td>
<td>Italy</td>
</tr>
<tr>
<td>ALENIA AERONAUTICA</td>
<td>Italy</td>
</tr>
<tr>
<td>BAE SYSTEMS</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>CNIT (CONSORZIO NAZIONALE INTERUNIVERSITARIO TELECOMUNICAZIONI)</td>
<td>Italy</td>
</tr>
<tr>
<td>CORRELATION SYSTEMS</td>
<td>Ireland</td>
</tr>
<tr>
<td>ADS Defence &amp; Security</td>
<td>France</td>
</tr>
<tr>
<td>EUROCOPTER ESPANA</td>
<td>Spain</td>
</tr>
<tr>
<td>EDISOFT</td>
<td>Portugal</td>
</tr>
<tr>
<td>FOI</td>
<td>Sweden</td>
</tr>
<tr>
<td>HITT</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>INDRA ESPACIO</td>
<td>Spain</td>
</tr>
<tr>
<td>INDRA SISTEMAS</td>
<td>Spain</td>
</tr>
<tr>
<td>JRC</td>
<td>Europe</td>
</tr>
<tr>
<td>MONDECA</td>
<td>France</td>
</tr>
<tr>
<td>SAGEM DEFENCE SECURITE</td>
<td>France</td>
</tr>
<tr>
<td>SPACE APPLICATION SERVICES</td>
<td>Belgium</td>
</tr>
<tr>
<td>TELESPAZIO (TPZ)</td>
<td>Italy</td>
</tr>
<tr>
<td>THALES ALENIA SPACE FRANCE</td>
<td>France</td>
</tr>
<tr>
<td>THALES ALENIA SPACE ITALIA</td>
<td>Italy</td>
</tr>
<tr>
<td>THALES DEFENCE DEUTSCHLAND</td>
<td>Germany</td>
</tr>
<tr>
<td>TNO</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>THALES SYSTEMES AEROPORTES</td>
<td>France</td>
</tr>
<tr>
<td>TTI Norte</td>
<td>Spain</td>
</tr>
<tr>
<td>UNIVERSITY COLLEGE LONDON</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UNIVERSIDAD DE MURCIA</td>
<td>Spain</td>
</tr>
<tr>
<td>UNIVERSITY OF PORTSMOUTH</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
**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; 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 both in terms of 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 SUPPORT 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.
Acronym: SUPPORT
Grant Agreement N°: 242112
Total Cost: € 14,629,279.69
EU Contribution: € 9,920,607
Starting Date: 01/07/2010
Duration: 48 months

Coordinator:
BMT GROUP 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/

NAME | COUNTRY
--- | ---
BMT Group (BMT) | United Kingdom
Swedish Defence Research Agency (FOI) | Sweden
Securitas (Securitas) | Sweden
Technical Research Centre of Finland (VTT) | Finland
MARLO (Marlo) | Norway
INLECOM Systems (ILS) | United Kingdom
MARINTEK (Marintek) | Norway
Nautical Enterprise (NECL) | Ireland
STENA (Stena) | Sweden
eBOS Technologies (eBOS) | Cyprus
University of Innsbruck (UIBK) | Austria
Cargotec Port Security (CA) | Finland
Maritime Administration of Latvia (MAL) | Latvia
INRIA (Inria) | France
MARAC Electronics (ME) | Greece
Port of Piraeus (PPA) | Greece
EUROPHAR-EEIG Port of Valencia - Marseille – Genoa (PV) | EU
ECO SLC (ECO SLC) | The Netherlands
TALOS is an innovative, Adaptable Land Border Large Area Surveillance System, based on transportable surveillance integrated with fast deployable mobile unmanned ground and air vehicles, which will address new challenges of external land borders of the enlarged European Union.

Project objectives

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 main objectives are as follows:

» To design the Integrated, Adaptable Land Border Large Area Surveillance System based on Unmanned Ground and Air Vehicles (TALOS system).

» To run research works in the main topics addressed by TALOS project, i.e.: Unmanned Ground Vehicles, Command and Control, Communication, Virtual prototyping.

» To implement the core components of the designed TALOS system as a proof-of-concept prototype in the Integrated Project (IP).

» To set-up and run the TALOS demonstrator (prototype) that will show the main benefits of the proposed approach.

» To promote the usage of TALOS system concept all over Europe, and to contribute to the on-going efforts of their standardization in Europe.

» To show the cost-effectiveness of the TALOS mobile/transportable concept as opposed to conventional stationary border surveillance solution.

The main TALOS innovation covers:

» Scalability – its ability to change easily system scale due to changes in the requirements and local conditions such as border size, topography, density of surveillance elements etc.;

» Autonomous capability based on sets of rules (artificial intelligence) - programmed to the computers of the Unmanned ground vehicles and the Command & Control system;

» Mobility/transportability – the whole system will be Mobile/Transportable installed in standard containers, transported on trailers for fast deployment in selected border zones (according to intelligence);

» Tactical learning/adaptation behaviour – during development process, system will be adapted to local operational requirements, operators will be interrogated, and their needs implemented in system mission planning module;

» No need for fix infrastructure or fences – TALOS system, owing to its mobility and transportability, does not require any fixed infrastructure as well as fences;

» Enables response to intrusion in minutes – system will respond to intrusion in the matter of minutes, not hours; and

» Usage of ‘green’ energy – in remote locations (where it is impossible to connect to standard power lines) the energy will be drawn from the natural sources e.g. by means of solar panels (sunny area), wind towers (windy area), water wheels (near to rivers).
**Information**

**Acronym:**
TALOS

**Grant Agreement No.:**
218081

**Total Cost:**
€ 19,906,815

**EU Contribution:**
€ 12,898,332

**Starting Date:**
01/06/2008

**Duration:**
48 months

**Coordinator:**

**PRZEMYSŁOWY INSTYTUT AUTOMATYKI I POMIARÓW**
Aleje Jerozolimskie 202
PL – 02486 Warsaw
Poland

—

**Contact:**

**Mariusz Andrzejczak**
Tel: (48 22) 874 01 99
Fax: (48 22) 874 01 13
E-mail: mandrzejczak@piap.pl
Website: www.talos-border.eu

---

**Partners**

**NAME**

- Przemyślowy Instytut Automatyki i Pomiarów
- ASELSAN Elektronik Sanayi ve Ticaret A.S.
- 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 Aérospatiale
- 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
- France
- Estonia
- Belgium
- Turkey
- Poland
- Spain
- Finland
- Poland
Project objectives

The VIRTUOSEO Project aims to provide an integrated open source information exploitation (OSINF) toolbox to European authorities working in border security. This toolbox will extend the “security distance” of Europe’s borders by allowing EU agencies and member states to anticipate, identify and respond to strategic risks and threats in a timely manner. In short, the project aims to:

1. Improve the situational awareness of those organisations and individuals charged with securing Europe’s borders.
2. Help anticipate risks such as terrorism, illegal migration and the trafficking of goods and people using OSINF.
3. Create the kernel of a pan-European technological platform for the collection, analysis and dissemination of open source information, thus ensuring greater interoperability among European actors involved in border security.
4. Provide the tools for crisis management response if anticipation fails or in the event of a rupture scenario.

Description of the work

The VIRTUOSEO 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 VIRTUOSEO toolkit.

Three versions of the VIRTUOSEO Toolkit will be delivered:

- **VIRTUOSEO-V0**: A very basic version of the framework, integrating basic functions and demonstrating its potential.
- **VIRTUOSEO-V1**: A first version of the framework integrating some operational functions.
- **VIRTUOSEO-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 VIRTUOSEO toolkit (one that integrates various information services and intelligence applications) and full documentation on the platform itself.

The core platform will be freely available as open source software at the end of the project.
Information

Acronym: VIRTUOSO

Grant Agreement N°: 242352

Total Cost: € 11,510,542.25

EU Contribution: € 7,999,182.55

Starting Date: 01/05/2010

Duration: 36 months

Coordinator:

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

Contact:
Géraud Canet
Tel: +33 1 46 54 82 59
Fax: +33 1 46 54 75 80
E-mail: geraud.canet@cea.fr

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEA</td>
<td>France</td>
</tr>
<tr>
<td>EADS Defence and Security Systems</td>
<td>France</td>
</tr>
<tr>
<td>ATOS Origin Sociedad Anonima Espanola</td>
<td>Spain</td>
</tr>
<tr>
<td>Mondeca</td>
<td>France</td>
</tr>
<tr>
<td>Newstin a.s</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>SAIL Technology AG</td>
<td>France</td>
</tr>
<tr>
<td>Aalborg University</td>
<td>Denmark</td>
</tr>
<tr>
<td>Thales CommunicationsBertin Technologies</td>
<td>France</td>
</tr>
<tr>
<td>Stichting Katholieke Universiteit / Brabant Universiteit Van Tilburg</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>TNO</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Ingeniería de Sistemas Para la Defensa de Espana SA – ISDEFE</td>
<td>Spain</td>
</tr>
<tr>
<td>Hawk Associates Limited</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Compagnie Européenne d’Intelligence Stratégique – CEIS</td>
<td>France</td>
</tr>
<tr>
<td>Universita Degli Studi di Modena e Reggio Emilia</td>
<td>Italy</td>
</tr>
<tr>
<td>Columba Global Systems Ltd.</td>
<td>Ireland</td>
</tr>
<tr>
<td>Thales Research and Technology</td>
<td>France</td>
</tr>
</tbody>
</table>
**Project objectives**

WiMA²S addresses primarily the urgent need to control illegal immigration and human trafficking by sea, in the context of the Integrated Border Management. In line with the EU Maritime Policy, it also contributes to other public service missions: shipping safety, search and rescue, protection of the marine environment, fisheries monitoring, interception of illegal trade and smuggling arriving by sea.

WiMA²S aims in particular at developing key technologies to prepare the future for the operational use of Unmanned Air Vehicles (UAVs) and innovative mission aircraft.

WiMA²S takes into account the operational end-user requirements and the need to develop strong European capabilities in maritime surveillance, in particular the following elements:

» To build a maritime picture, detection and identification phases are mandatory.

» Air assets are unique for wide area maritime surveillance: they are the only one which can provide situation awareness over extended areas because of their endurance, speed and their capacity of reliable long distance detection accuracy; they can be directed to areas of interest, as close as possible from the threat point of origin, and have the flexibility to react to the situation, performing close-up inspection when needed.

» Shortfalls of surveillance capacities of EU wide maritime areas concerning responsibilities in border security, illegal immigration, fisheries control, pollution, terrorism, …

» Lack of air assets for surveillance and their relatively high costs.

» UAVs can be a very attractive technical solution for maritime surveillance — however, one of the main obstacles is integration in the European Air Traffic.

**Description of the work**

WiMA²S proposes solutions to these issues by:

» Developing original and innovative technological solutions to increase airborne maritime surveillance efficiency while reducing costs.

» Filling the gap between Piloted Mission Aircraft and UAVs for maritime surveillance, and preparing concepts for using UAVs with remote control mission system operation and combining these with existing maritime surveillance systems.

» Partly simulating and partly demonstrating — including a flight demo of a UAV — the concept with End-Users feedback.

» Analysing the cost efficiency in support of the feasibility of the concept.

» Reporting a road map in the final report for further technological projects in the priority topic of maritime surveillance.
Information

Acronym: WIMA²S

Grant Agreement N°: 217931

Total Cost: € 3,997,523

EU Contribution: € 2,737,169

Starting Date: 01/12/2008

Duration: 36 months

Coordinator:

THALES AIRBORNE SYSTEMS S.A
25 Avenue Gustave Eiffel
FR-33608 Pessac
France

Contact:
Gilles JURQUET
Fax: +33(0)5 - 57 26 71 60
E-mail: gilles.jurquet@fr.thalesgroup.com
Website: www.wimaas.eu

Partners

NAME | COUNTRY
---|---
Thales Systemes Aeroportes S.A | France
SELEX GALILEO | Italy
Dassault Aviation | France
SENER Ingeneria y Sistemas | Spain
FOI | Sweden
Fraunhofer IITB | Germany
JRC | Belgium
Air Force Institute of Technology | Poland
EUROSENSE | Belgium
SATCOM1 Aps | Denmark
SETCCE | Slovenia
Aerovisión Vehículos Aéreos S.L | Spain
Thales Communications S.A. | France
Mediterranean Academy Of Diplomatic Studies | Malta
A4A / Alert for All

Project objectives

The overall objective of A4A is to improve the effectiveness of alert 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 level of alerts’ 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 regional to pan-European range.

A4A will provide solutions to align alert procedures and processes in contemporary crises (natural or man-made) to 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 front 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 defining recommendations for the improvement of operational concepts that make use and profit from the A4A tools. Furthermore, the development of training material for authorities and responders will contribute to the end user acceptance.

Investigation on organisational, institutional and funding aspects for the deployment of A4A and a final show case 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.
## Information

**Acronym:** A4A  
**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. (DLR)  
Institute of Communications and Navigation  
Linder Hoehe  
51147 Cologne  
Germany

**Contact:**  
Cristina Párraga Niebla  
Tel: +49 (0) 8153 282824  
Mobile: +49 (0) 1727134781  
Fax: +49 (0) 8153 282844  
E-mail: Cristina.Parraga@dlr.de  
Website: www.alert4all.eu

## Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>German Red Cross (DRK)</td>
<td>Germany</td>
</tr>
<tr>
<td>Avanti Communications Ltd. (AVA)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>BAPCO LBG (BAPCO)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>TECNOSYLVA S.L. (TSYL)</td>
<td>Spain</td>
</tr>
<tr>
<td>EDISOFT-Empresa de Servicos e Desenvolvimento de Software S.A. (EDI)</td>
<td>Portugal</td>
</tr>
<tr>
<td>Fundación Tecnalia Research &amp; Innovation (Tecnalia)</td>
<td>Spain</td>
</tr>
<tr>
<td>Universität Stuttgart (USTUTT)</td>
<td>Germany</td>
</tr>
<tr>
<td>Swedish Defence Research Agency</td>
<td>Sweden</td>
</tr>
<tr>
<td>Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)</td>
<td>Germany</td>
</tr>
<tr>
<td>Eutelsat S.A. (EUT)</td>
<td>France</td>
</tr>
<tr>
<td>Institut fuer Rundfunktechnik GmbH (IRT)</td>
<td>Germany</td>
</tr>
</tbody>
</table>
Project objectives

The Phase I project ACRIMAS, a 15 months 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.

Expected results

ACRIMAS will prepare a strategic roadmap setting out the main areas and relevant topics of CM to be addressed by concrete DE activities in Phase II. In addition, ACRIMAS will deliver a demonstration concept for Phase II, describing how and where the DE activities in Phase II should be conducted.

Besides these two main deliverables, an important result of ACRIMAS will be a raised awareness among the relevant stakeholders in Europe about the upcoming demonstration programme and its preparation.
Information

Acronym: ACRIMAS

Grant Agreement N°: 261669

Total Cost: € 1,665,123

EU Contribution: € 1,109,381

Starting Date: 01/02/2011

Duration: 15 months

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, 53864 Euskirchen, Germany
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.int.fraunhofer.de

Partners

NAME

FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V (Fraunhofer) Germany
CRISIS MANAGEMENT INITIATIVE (CMI) Finland
NATIONAL CENTER FOR SCIENTIFIC RESEARCH «DEMOKRITOS» (NCSRD) Greece
NEDERLANDS INSTITUUT FYSIEKE VEILIGHEID (NIFV) Netherlands
T-SOFT AS (TSOFT) Czech Republic
TOTALFORSVARETS FORSKNINGSINSTITUT (FOI) Sweden
JRC -JOINT RESEARCH CENTRE- EUROPEAN COMMISSION (JRC) Belgium
CENTER FOR SECURITY STUDIES (KEMEA) Greece
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (TNO) Netherlands
TURKIYE KIZILAY DERNEGI (TRCS) Turkey
TECHNOLOGIES SANS FRONTERES ASBL (TSF) Belgium
UNITED NATIONS UNIVERSITY INSTITUTE FOR ENVIRONMENT AND HUMAN SECURITY (UNU-EHS) Germany
EADS DEFENCE AND SECURITY SYSTEMS (EADS) France
SELEX SISTEMI INTEGRATI SPA (SSI) Italy
PUBLIC SAFETY COMMUNICATION EUROPE FORUM AISBL (PSCE) Belgium

COUNTRY

Germany
Finland
Greece
Netherlands
Czech Republic
Sweden
Belgium
Greece
Netherlands
Turkey
Belgium
Germany
France
Italy
Belgium
AntiBotABE / Isolation of recombinant antibodies neutralizing botulinum toxins A,B,E

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 to previously isolate 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 NHPs antibodies has been described as an approach that allowed 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 IgGs. We have shown that “super-humanization” (also called “germline humanization”) of NHP antibodies is possible, by reversing most of these mutations while respecting the affinity. This process will be applied to the neutralizing scFvs isolated in the course of the project.

In the third part of the project, neutralizing, super-humanized scFvs will be expressed as full-sized IgGs and tested in a standardized protection model to verify their efficacy against several strains for each targeted serotype. At various steps of the project, our results will be communicated to the first responders more particularly involved against biothreats.

Expected results

The ideal result is an oligoclonal cocktail of 6 recombinant, super-humanized IgGs, neutralizing the neurotoxins secreted by all strains of Clostridium botulinum A, B and E. These IgGs will then be developed as medicine registered by EMEA, on credits provided by EDA. 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.
Information

Acronym: AntiBotABE

Grant Agreement N°: 241832

Total Cost: € 3,900,000

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centre de Recherche du Service de Santé des Armées (CRSSA)</td>
<td>France</td>
</tr>
<tr>
<td>Ministere de la defense (MLD)</td>
<td>France</td>
</tr>
<tr>
<td>Technische Universitat Braunschweig (TUBS)</td>
<td>Germany</td>
</tr>
<tr>
<td>Institut Pasteur (Pasteur)</td>
<td>France</td>
</tr>
<tr>
<td>Health Protection Agency (HPA)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Centre National de la Recherche Scientifique (DNRS)</td>
<td>France</td>
</tr>
<tr>
<td>LFB Biotechnologies (LFB)</td>
<td>France</td>
</tr>
<tr>
<td>University of Helsinki (UoH)</td>
<td>Finland</td>
</tr>
<tr>
<td>VITAMIB (VITAMIB)</td>
<td>France</td>
</tr>
</tbody>
</table>
**Project objectives**

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

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

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

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

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

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

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

**Description of the work**

The project is divided into six workpackages:

» **Management**

» **Systems Requirements & Design Concept**

A general methodology will be developed to identify the needs of the different BOOSTER end user categories and to build the global design of the system.

» **Fast evaluation**

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

» **New bio-dosimetric tools**

The work is to develop new biodosimetry systems and to integrate them with other procedures to determine radiation exposure. Two techniques will be investigated:

- \( \gamma \)-H2AX quantification; and
- Centrosome quantification.

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

» **Software development and integration of components**

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

» **System Validation and Training**

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

**Expected results**

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

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

**Acronym:**
BOOSTER

**Grant Agreement N°:**
242361

**Total Cost:**
€ 4,536,559.24

**EU Contribution:**
€ 3,284,291

**Starting Date:**
01/07/2010

**Duration:**
36 months

**Coordinator:**

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

**Contact:**

Mehdi GMAR
Tel: (+33) (0) 1 69 08 39 45
Fax: (+33) (0) 1 69 08 60 30
E-mail: mehdi.gmar@cea.fr
Website: http://www.booster-project.org/

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEA</td>
<td>France</td>
</tr>
<tr>
<td>National University of Ireland, Galway (NUIG)</td>
<td>Ireland</td>
</tr>
<tr>
<td>Karlsruher Institut fuer technologie (KIT)</td>
<td>Germany</td>
</tr>
<tr>
<td>Izotopkutato Intezet - Magyar Tudomanyos Akademia (IKI)</td>
<td>Hungary</td>
</tr>
<tr>
<td>Canberra France (CANBERRA)</td>
<td>France</td>
</tr>
<tr>
<td>Universidad politecnica de Valencia (UPVLC)</td>
<td>Spain</td>
</tr>
<tr>
<td>Orszagos Atomenergia Hivatal (HAEA)</td>
<td>Hungary</td>
</tr>
</tbody>
</table>
Project objectives

The goal of BRIDGE is to increase 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, 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, 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 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. 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
» 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
**Information**

**Acronym:**
BRIDGE

**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:**
STIFTELEN SINTEF
ICT
Forskningsveien 1
P.O. Box 124 Blindern
0314 Oslo
Norway

**Contact:**
Geir Horn
Tel: +47 22067561
Mobile: +47 93059335
Fax: +47 22067350
E-mail: geir.horn@sintef.no
Website: www.sintef.no

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almende B.V.</td>
<td>Netherlands</td>
</tr>
<tr>
<td>CNet Svenska AB</td>
<td>Sweden</td>
</tr>
<tr>
<td>Fraunhofer Institut für angewandte Informationstechnology FIT</td>
<td>Germany</td>
</tr>
<tr>
<td>Lancaster University</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Crisis Training AS</td>
<td>Norway</td>
</tr>
<tr>
<td>SAAB Training Systems</td>
<td>Sweden</td>
</tr>
<tr>
<td>THALES Nederland BV</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Universität Klagenfurt</td>
<td>Austria</td>
</tr>
<tr>
<td>Paris-Lodron-Universität Salzburg</td>
<td>Austria</td>
</tr>
<tr>
<td>VSH Hagerbach Test Gallery LTD</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Technische Universität Delft</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Stockholms Universitet</td>
<td>Sweden</td>
</tr>
<tr>
<td>Helse Stavanger</td>
<td>Norway</td>
</tr>
</tbody>
</table>
COPE / Common operational picture exploitation

Project objectives

The objective of the Common Operation Picture Exploitation (COPE) project was to achieve a significant improvement in civil crisis management command and control performance, reliability, and cost. New solutions were created by combing a user oriented human factors approach with the technology development. The aim was a step improvement in information flow both from and to the first responder in order to increase situational awareness across agencies and at all levels of the command chain in emergency management situations. A user-driven approach was taken to develop new technologies for supporting user information requirements at the scene of the event. First responders belong to a heterogeneous group in terms of crisis environments as well as roles, command structure, organisational and national differences. The project applied a wide range of human factors methods from functional task modelling to end user simulations to better understand the processes of individual agencies and to ensure that new systems both match requirements and can be integrated with legacy processes and technologies.

Description of the work

The project team has much experience from crisis management projects and it uses the skills and competences of research scientists both from industry and academia, of technology providers and systems integrators supported by end users. The COPE project developed use cases and scenarios with end users building a rich picture of the requirements and the differences in requirements across agencies, organisations and nations. The requirements were mapped against the technologies developed to offer tailored solutions. Commercial off-the-shelf products and novel technologies were integrated to a prototype system allowing operational evaluation with the selected realistic scenarios. The key objective was to develop novel technical support tools and mechanisms for collecting, gathering and disseminating information for the development of a Common Operational Picture (COP) in crisis circumstances. The research and development work focused on the following objectives:

» To understand and specify the information requirements of the first responder.

» To enable effective and appropriate communication links between teams at the first responder level and to enable them to feed information back to support the COP.

» To develop a user-driven methodology to understand working processes in order to map technologies on the user requirements and to take into account the similarities and differences between agencies, their differing levels of technological sophistication and to enhance capability in conjunction with legacy systems.

» To define how the first responder can feed the COP to give ground truth and to reduce the cultural power distance between the command centre and the ground.

» To trial and evaluate the technological feasibility of the solution.

» To develop and evaluate tailored computer-based decision support systems.

» To enhance the cognitive situational awareness of the first responder.

Results

The results of the project are available on the website of the project http://cope.vtt.fi and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: COPE

Grant Agreement N°: 217854

Total Cost: € 3,886,574.00

EU Contribution: € 2,535,049

Starting Date: 01/02/2008

End Date: 31/01/2011

Coordinator:

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

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHNICAL RESEARCH CENTRE OF FINLAND (VTT)</td>
<td>Finland</td>
</tr>
<tr>
<td>UTI SYSTEMS S.A. (UTI)</td>
<td>Romania</td>
</tr>
<tr>
<td>CESS GMBH CENTRE FOR EUROPEAN SECURITY STRATEGIES (CESS)</td>
<td>Germany</td>
</tr>
<tr>
<td>Pelastusopisto, Emergency Services College (ESC)</td>
<td>Finland</td>
</tr>
<tr>
<td>Ministry of Interior and Administration Reform (IGSU)</td>
<td>Romania</td>
</tr>
<tr>
<td>BAE Systems C-ITS (BAE Systems C-ITS)</td>
<td>Sweden</td>
</tr>
<tr>
<td>THE PROVOST FELLOWS AND SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY OF QUEEN ELISABETH NEAR DUBLIN (TCD)</td>
<td>Ireland</td>
</tr>
<tr>
<td>BAE SYSTEMS (OPERATIONS) LIMITED (BAE Systems UK)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>SKYSOFT PORTUGAL - SOFTWARE E TECNOLOGIAS DE INFORMACAO SA (Skysoft)</td>
<td>Portugal</td>
</tr>
</tbody>
</table>
CRISIS / Critical incident management training system using an interactive simulation environment

Project objectives

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

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

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

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

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

Description of the work

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

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

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

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

Expected results

The expected impacts are:

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

**Acronym:**
CRISIS

**Grant Agreement N°:**
FP7-242474

**Total Cost:**
€ 4,591,760.99

**EU Contribution:**
€ 3,495,611.99

**Starting Date:**
01/05/2010

**Duration:**
39 months

**Coordinator:**

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

---

**Contact:**

Prof. William Wong, BCom (Hons.) PhD FNZCS – Head,
Interaction Design Centre.
Tel: +44 20 8411 2684
E-mail: w.wong@mdx.ac.uk
Website:
http://idc.mdx.ac.uk/projects/crisis/
http://www.eis.mdx.ac.uk/research/idc/

---

**Partners**

**NAME**

- Middlesex University
- 3D Connections
- National Aerospace Laboratory
- ObjectSecurity Ltd
- Space Applications Services
- VSL Systems AB
- Linkoping University
- Haskoli Island (University of Iceland)
- AE Solutions
- ANA
- British Transport Police
- Flugstodir (ISAVIA)

**COUNTRY**

- United Kingdom
- Denmark
- Netherlands
- United Kingdom
- Belgium
- Sweden
- Iceland
- United Kingdom
- Portugal
- United Kingdom
- Iceland
CRISYS / Critical Response in Security and Safety Emergencies

**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, 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 a public-private dialogue with local, national, 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 step from a preliminary roadmap to a final roadmap which will be presented at a final conference.

**Expected results**

» Comprehensively Review the Current State of completed ongoing and planned work in the CMS field;

» Lay out any Further Research work required;

» Assess Relevant Trends factual, political and situational trends;

» Identify User Needs and classify requirements to address issues to enhance joint working including equipment interoperability;

» Create Network of users and suppliers with public and private engagement;

» Indicate Opportunities to involve participation in non EU countries;

» Disseminate Findings across European civil protection sector.
Information

Acronym: CRISYS
Grant Agreement N°: 261682
Total Cost: € 803,304
EU Contribution: € 740,945
Starting Date: 01/02/2011
Duration: 15 months

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUROPEAN ORGANISATION FOR SECURITY (EOS)</td>
<td>Belgium</td>
</tr>
<tr>
<td>EDISOFT SA (EDI)</td>
<td>Portugal</td>
</tr>
<tr>
<td>Center for Security Studies (KEMEA)</td>
<td>Greece</td>
</tr>
<tr>
<td>National Center for Scientific Research, “Demokritos” (NSCRD)</td>
<td>Greece</td>
</tr>
<tr>
<td>ALTRAN BV (ALTRAN)</td>
<td>Netherland</td>
</tr>
<tr>
<td>International Association of Fire and Rescue Services (CTIF)</td>
<td>France</td>
</tr>
<tr>
<td>Teletron Euroricerche SRL (TLT)</td>
<td>Italy</td>
</tr>
<tr>
<td>Compania nationala de transport al energiei eletrice Transelectrica SA (TRA)</td>
<td>Romania</td>
</tr>
<tr>
<td>Société Francoise de Medicine de Catastrophe (SFMC)</td>
<td>France</td>
</tr>
<tr>
<td>THALES Security Solution &amp; Service SAS (T3S)</td>
<td>France</td>
</tr>
<tr>
<td>INDRA SISTEMAS SA (IND)</td>
<td>Spain</td>
</tr>
<tr>
<td>Istituto Affari Internazionali (IAI)</td>
<td>Italy</td>
</tr>
<tr>
<td>University of Central Lancashire (UCLAN)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Ministry of the Interior, Department for Rescue Services, SISAASIAINMINISTERIO (FMOI)</td>
<td>Finland</td>
</tr>
<tr>
<td>Zanasi Alessandro SLR (ZAN)</td>
<td>Italy</td>
</tr>
</tbody>
</table>
DECOTESSC1 / Demonstration of counterterrorism system-of-systems against CBRNE phase 1

Project objectives

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

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

Furthermore, a strategic roadmap will be proposed that should aim at filling the identified gaps. This includes linkages with related subject areas and with stakeholder communities and a study regarding proposals for real demonstrations in phase 2.

The strategic roadmap to be developed in DECOTESSC1 will address the full concept of an EU counterterrorism system-of-systems against CBRNE and outlines all the necessary missions, tasks, capabilities, systems, technologies, etc. to be considered.

Description of the work

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

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

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

Results

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

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

Recommendations have been made in order to define the Phase 2 CBRNE demonstration project, as well as proposals for suitable demonstrations. A concluding workshop was organized in Brussels on 7th June 2011.

More info on the workshop in the event section of DG ENTR: : http://ec.europa.eu/enterprise/newsroom/cf/newsbytheme.cfm
Information

**Acronym:**
DECOTESSC1

**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-natuurwetenschappelijk Onderzoek – TNO
Department of CBRN Protection
Schoemakerstraat 97
PO Box 6060
NL-2600 JA Delft
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
Website: www.decotessc1.eu

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nederlandse Organisatie voor toegepast-natuurwetenschappelijk Onderzoek – TNO (TNO)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>AIT Austrian Institute of Technology GmbH (AIT)</td>
<td>Austria</td>
</tr>
<tr>
<td>Commissariat a l’Energie Atomique (CEA)</td>
<td>France</td>
</tr>
<tr>
<td>Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (FHG)</td>
<td>Germany</td>
</tr>
<tr>
<td>Totalforsvarets Forskningsinstitut (FOI)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Joint Research Centre (JRC)</td>
<td>Europe</td>
</tr>
<tr>
<td>Valtion Teknillinen Tutkimuskeskus (VTT)</td>
<td>Finland</td>
</tr>
<tr>
<td>Fundación Tecnalia Research &amp; Innovation (TEC)</td>
<td>Spain</td>
</tr>
<tr>
<td>Seibersdorf Labor GmbH (SLG)</td>
<td>Austria</td>
</tr>
</tbody>
</table>
Description of the work

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

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

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

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

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

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

Expected results

<table>
<thead>
<tr>
<th>Measures</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparedness</td>
<td>&lt;br&gt;Pcent of responders trained to respond to anticipated emergencies (e.g. 15 planning scenarios)</td>
</tr>
<tr>
<td>Safety Officer(s) have the training and experience necessary to manage hazards associated with all potential planning scenarios</td>
<td>YES</td>
</tr>
<tr>
<td>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</td>
<td>100%</td>
</tr>
<tr>
<td>Activate Response Safety and Health</td>
<td>&lt;br&gt;Pcent of responders injured or falling ill in response to the incident</td>
</tr>
<tr>
<td>Time in which Safety Officer is designated within the First Response structure (separate from MEOC, who may hold this role for a period of time)</td>
<td>Within 30 minutes from arrival of responders</td>
</tr>
<tr>
<td>Time in which deployment actions are initiated for Assistant Safety Officers or Safety Officers to provide technical assistance to incident safety official</td>
<td>Within 1 hour from arrival of responders</td>
</tr>
<tr>
<td>Identify safety needs</td>
<td>&lt;br&gt;Pcent of hazards detected/identified and characterized</td>
</tr>
<tr>
<td>Time in which an initial incident safety analysis is completed</td>
<td>Within 1 hour from responder arrival</td>
</tr>
<tr>
<td>Site/Incident Specific Safety and Health Training</td>
<td>&lt;br&gt;Pcent of emergency workers responding to an incident who are provided on-site training prior to assignment to work at incident</td>
</tr>
<tr>
<td>Ongoing Monitoring of Responder Safety and Health</td>
<td>&lt;br&gt;Time in which the medical unit is opened and operating within a MEOC structure</td>
</tr>
<tr>
<td>Percent of personnel wearing the required E-SPONDER equipment for site entry and work</td>
<td>100%</td>
</tr>
<tr>
<td>Percent of workers who have their representative exposure to hazardous substances quantified and recorded</td>
<td>100%</td>
</tr>
</tbody>
</table>
**Information**

**Acronym:**
E-SPONDER

**Grant Agreement N°:**
FP7-242411

**Total Cost:**
€ 12,922,363.40

**EU Contribution:**
€ 8,790,044

**Starting Date:**
01/07/2010

**Duration:**
48 months

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

**Contact:**
Dr. Dimitris Vassiliadis
Tel: +30.210.7450321
Fax: +30.210.7450399
E-mail: dvas@exodussa.com
Website: www.e-sponder.eu

---

**NAME**

Exodus S.A.
University of Modena and Reggio Emilia
CrisisPlan B.V.
Prosys Software GmbH
Immersion S.A.
Rose Vision
Telcordia Poland Sp. z.o.o.
Centre Suisse d’Electronique et de Microtechnique S.A.
Smartex Srl
Technische Universität Dresden
YellowMAP AG
PANOU S.A.
Telcordia Taiwan
Institute for Information Industry
Entente pour la forêt Méditerranée

**COUNTRY**

Greece
Italy
The Netherlands
Germany
France
Spain
Poland
Switzerland
Italy
Germany
Germany
Greece
Taiwan
Taiwan
France
Project objectives

The purpose of ESS is to enable improved control and management of major crisis events such as natural disasters, industrial accidents, terror attacks etc. The idea guiding the development of ESS is a portable, modular and autonomous system which fuse in real-time various forms of field-derived data including video, audio, weather measurements, location tracking, radioactivity, biochemical, telecom derived data, affected population reports and other information.

The data is collected and communicated via both portable and fixed platforms including wireless communication devices, Unmanned Aerial Vehicle (UAV), Unmanned Ground System (UGS), air-balloon and field vehicles. The fusion of the data is handled within a central system which performs information analysis and provides decision support applications for web based command and control systems. This provides flexible, yet comprehensive coverage of the affected area.

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

Description of the work

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

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

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

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

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

Expected results

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

Acronym: ESS

Grant Agreement N°: 217951

Total Cost: € 14 M

EU Contribution: € 9,1 M

Starting Date: 01/06/2009

Duration: 48 months

Coordinator:

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

Contact:
Mr. Gideon Hazzani
Email: Gideon.Hazzani@verint.com,
Website: www.ess-project.eu

Partners

NAME

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

COUNTRY

Israel
Italy
Germany
Czech Republic
Spain
France
Germany
United Kingdom
Greece
Italy
United Kingdom
France
Greece
Italy
Greece
Sweden
Israel
Israel
Israel
Project objectives

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

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

3. To test and evaluate the system.

4. To develop exploitation strategies.

Description of the work

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

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

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

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

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

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

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

Expected results

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

**Acronym:** FASTID  
**Grant Agreement N°:** 242339  
**Total Cost:** € 2,990,190  
**EU Contribution:** € 2,270,476  
**Starting Date:** 01/04/2010  
**Duration:** 36 months

### Coordinator:

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

---

### Contact:

**Peter Ambs, Operational Police Support Directorate**  
Tel: +33 (0)4.72.44.72.92  
Fax: +33 (0)4.72.44.73.80  
E-mail: p.ambs@interpol.int  
Website: [http://www.interpol.int/FASTID.asp](http://www.interpol.int/FASTID.asp)

### Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERPOL</td>
<td>France</td>
</tr>
<tr>
<td>Bundeskriminalamt</td>
<td>Germany</td>
</tr>
<tr>
<td>Plass Data Software A/S</td>
<td>Denmark</td>
</tr>
<tr>
<td>UNIVERSITY OF DUNDEE</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V</td>
<td>Germany</td>
</tr>
<tr>
<td>Crabbe Consulting Ltd</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Project objectives

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

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

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

Description of the work

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

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

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

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

4. System evaluation and optimisation of the performance
   » Determination of the optimum characteristics for the advanced respiratory protection systems.
   » Optimisation of the filter and hood systems.

5. Economic feasibility and manufacturability, exploitation and dissemination, IPR policy
   Examination of viability of a full scale production of the nanoporous adsorbent, the filter canister and the hood.

Expected results

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

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

Acronym: FRESP
Grant Agreement N°: 218138
Total Cost: € 4,032,757
EU Contribution: € 3,029,967
Starting Date: 01/06/2008
Duration: 42 months

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

Contact:
Dr. Peter Lodewyckx
Royal Military Academy – DEAO
E-mail: Peter.Lodewyckx@rma.ac.be
Website: www.rma.ac.be/fp7-fresp

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Royal Military Academy</td>
<td>Belgium</td>
</tr>
<tr>
<td>Budapest University of Technology and Economics</td>
<td>Hungary</td>
</tr>
<tr>
<td>University of Brighton</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>University of Alicante</td>
<td>Spain</td>
</tr>
<tr>
<td>TNO</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>High Technology Filters s.a.</td>
<td>Greece</td>
</tr>
<tr>
<td>MAST Carbon</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>NORIT Nederland B.V</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Laser Optical Engineering Ltd.</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
IDIRA / Interoperability of data and procedures in large-scale multinational disaster response actions

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, 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 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 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 trainings 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 coordinated large-scale disaster management. The IDIRA solutions are building on and are being integrated with existing infrastructure & response procedures.
Information

Acronym: IDIRA

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
Hansastraasse 37C
80686 - Muenchen
Germany

Contact:
Andreas Kuester
Tel : +49 (0) 351 4640 667
Mobile : +49 (0) 172 4117655
Fax : +49 (0) 351 4640 803
E-mail : Andreas.Kuester@ivi.fraunhofer.de
Website : http://www.ivi.fraunhofer.de

---

NAME

Fraunhofer Institute for Transportation and Infrastructure Systems (Fraunhofer)
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
Project objectives

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

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

Description of the work

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

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

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

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

Expected results

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

Acronym: IMSK

Grant Agreement N°: 218038

Total Cost: € 23,468,530

EU Contribution: € 14,864,308

Starting Date: 01/03/2009

Duration: 48 months

Coordinator:

SAAB AB
Saab Microwave Systems
SE-412 89 Göteborg
Sweden

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

Partners

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

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

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

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

Description of the work

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

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

Expected results

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

1. The INDIGO distributed framework enabling:
   - The involvement of multiple users in crisis exercises;
   - The intuitive authoring and control of crisis scenarios;
   - The visualization of a 2D/3D interactive Common Operational Picture;
   - The visual command and control of field units;
   - The development of additional modules with the INDIGO SDK.

2. The mobile INDIGO system that enables first responders and other field units to participate in INDIGO crisis exercises.

3. The Environment Service that hosts and delivers, in interactive time, all the information related to the situation, including massive geographic, cartographic and architectural data about the environment.

4. The Real-time Simulation Services that can stimulate the scenario or be used to support decision during real crisis.

5. The portable map table that will offer an extremely innovative and intuitive mean to interact with the Common Operational Picture in mobile crisis centers.

6. The standard proposition for a European 2D/3D emergency symbology.
Information

**Acronym:**
INDIGO

**Grant Agreement N°:**
242341

**Total Cost:**
€ 3,830,000

**EU Contribution:**
€ 2,790,000

**Starting date:**
01/05/2010

**Duration:**
36 months

**Coordinator:**
DIGINEXT SARL
Impasse de la Draille
Parc d’Activités La Duranne
13100 Aix en Provence
France

**Contact:**
Jerome Duchon
Tel : +33 (0)5 61 17 66 66
Fax : +33 (0)5 61 17 65 78
E-mail : Duchon@diginext.no-spam.fr
Website: http://indigo.c.s.fr

---

**NAME**
Diginext
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
France
Belgium
The Netherlands
Sweden
France
Project objectives

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

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

These challenges include:

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

Description of the work

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

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

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

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

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

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

Expected results

In terms of outputs, the project delivers the significant contributions:

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

**Acronym:** L4S

**Grant Agreement N°:** 225634

**Total Cost:** € 3,503,621

**EU Contribution:** € 2,415,768

**Starting Date:** 01/07/2009

**Duration:** 24 months

**Coordinator:**

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

**Contact:**

**Christos Konstantinou**
E-mail: ckonstantinou@deloitte.gr
Website: www.L4S-project.info

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deloitte Business Solutions Anonymi Etairia Symvoulon Epicheiriseon</td>
<td>Greece</td>
</tr>
<tr>
<td>Oesterreichische Studiengesellschaft Fuer Kybernetik</td>
<td>Austria</td>
</tr>
<tr>
<td>Alphalabs SARL</td>
<td>France</td>
</tr>
<tr>
<td>Universitaet Der Bundeswehr Muenchen</td>
<td>Germany</td>
</tr>
<tr>
<td>Athens Laboratory of Business Administration</td>
<td>Greece</td>
</tr>
<tr>
<td>Universita Cattolica Del Sacro Cuore</td>
<td>Italy</td>
</tr>
<tr>
<td>FVA SAS</td>
<td>Italy</td>
</tr>
<tr>
<td>Athens International airport S.A.</td>
<td>Greece</td>
</tr>
<tr>
<td>Creurers del port de Barcelona SA</td>
<td>Spain</td>
</tr>
<tr>
<td>Frequentis AG</td>
<td>Austria</td>
</tr>
<tr>
<td>Akad Wissenschaftliche Hochschule Lahr GmbH</td>
<td>Germany</td>
</tr>
</tbody>
</table>
MULTIBIODOSE / Multi-disciplinary biodosimetric tools to manage high scale radiological casualties

Project objectives

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

Description of the work

One work package (WP) will be devoted to each tool. Starting with the state of the art, each tool will be validated and adapted to the conditions of a mass casualty situation. A training programme will be carried out where appropriate and 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.

Expected results

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

Acronym: MULTIBIODOSE

Grant Agreement N°: 241536

Total Cost: € 4,661,432

EU Contribution: € 3,493,199

Starting Date: 01/05/2010

Duration: 36 months

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

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

Partners

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

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 itself. 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 in order to ensure 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 for 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:

1. **Sample enrichment**: Novel air sampling technologies and sampling procedures easily combinable with a chip.
2. **Micro-nanotechnological devices** combined with advanced biochemistry.
3. **Microfluidics** allows for fast and efficient hybridization of the PCR products on the capture microarray, implementing 3D-nanotechnology.
4. **Electrochemiluminescence-based detection** or electrochemical sensors ensure ultrasensitive detection.

Expected results

The aim is 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 it will carry out the detection reaction via innovative sensor technologies.
Information

Acronym: Multisense Chip
Grant Agreement N°: 261810
Total Cost: € 8,986,775.00
EU Contribution: € 6,619,399.50
Starting Date: 01.06.2011
Duration: 48 months

Coordinator:
microfluidic ChipShop GmbH
Geschäftsführung
Carl-Zeiss-Promenade 10 (until 30.04.2011)
New: Stockholmer Str. 20 (from 01.05.2011)
07745 Jena (until 30.04.2011)
New: 07747 Jena,
Germany (from 01.05.2011)

Contact:
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

Partners

NAME
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
BT
FLI
iMicroQ
IMM
URV
IFB
CED
Opti-Alert / Enhancing the efficiency of alerting systems through personalized, culturally sensitive multi-channel communication

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
(a) allows for a rapid simulation of the impact of different alerting strategies (depending on the selected media-mix and current availability of communication media),
(b) supports the composition of the optimal mix of communication channels (individualized alerting channels and mass media),
(c) improves alert compliance through social and cultural adaptation and personalization of alert messages and communication channels
(d) supports the rapid and automated implementation of a selected alert strategy,
(e) can simultaneously address a large variety of communication channels to facilitate efficient high-throughput alerting, and
(f) 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:
(a) an in-depth analysis of the impact which the observed socio-cultural differences have on regional alerting strategies,
(b) an analysis of the influence which the observed socio-cultural differences have on regional alerting strategies,
(c) an analysis of the impact of individualized alerting (via SMS, E-Mail, etc.) and alerting via the mass media,
(d) the identification of best-practices in alerting via mass media,
(e) 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 both to 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 tool suite. 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.
### Information

**Acronym:**
Opti-Alert

**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 FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
Institute for Software and Systems Engineering ISST,
Department 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

### Partners

#### NAME
- e*Message Wireless Information Services Deutschland GmbH
- UBIMET GmbH
- Proteo S. p. A.
- UNIQA Versicherungen AG
- Göteborgs Universitet
- Süddeutsches Institut für empirische Sozialforschung e.V.
- Regione Sicilia
- Nederlands Instituut Fysieke Veiligheid
- Università degli Studi di Perugia
- THALES Services SAS

#### COUNTRY
- Germany
- Austria
- Italy
- Austria
- Sweden
- Germany
- Italy
- Netherlands
- Italy
- France
PANDORA / Advanced training environment for crisis scenarios

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 affordable cost.

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

» A realistic and complete scenario with near real-time action, coherent with that expected in a real-world situation;

» Realistic emotional status, through affective inputs and stress factors;

» The potential to include different crises managers belonging to different sectors.

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

Description of the work

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

» WP1: User Requirements Analysis and design of PANDORA functional specifications – will provide a definition of both data and workflows needed to specify the proposed system and to clearly identify the processes that are the basis of the system services.

» WP2: Behaviour simulation and modelling - split into 5 tasks: the first two consolidate the basic preconditions for the behavioural planner, the third designs the general architecture of the planner, the remaining two provide proactive reasoning services to the planner.

» WP3: Crisis simulation and modelling - focused on three main modules: (1) the crisis knowledge base, (2) the crisis planner that generates the conceptual high level network of events that constitutes the plot for the scenario, and (3) the crisis modeller that tracks the evolution in real time of the scenario.

» WP4: Environment and Emotion Simulation Engine – seeks to integrate emotional human factors within training programs for crisis managers, taking into account several research topics:

  • Relevant human factors in crisis decision-making;
  • Neuro-physiological testing and measures;
  • Personalised and flexible training strategies.

» WP5: Environment design and building – seeks to authentically recreate the dynamic elements of the entire disaster environment, i.e. emulating a complete crisis room with realistic visuals and audio to create an immersive, chaotic and stressful environment.

» WP6: Development, integration and testing – will deliver the PANDORA software product that can be considered as a system composed of software subsystems/components implemented on different environments.

» WP7: Training testing, evaluation and assessment – will support the development of a robust evaluation methodology that complements the work done to build the PANDORA advanced training environment.

» WP8: Dissemination and exploitation.

» WP9: Project management.

Expected results

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

PANDORA will develop 3 key components:

» The crisis engine, which provides a scenario-based, interactive structure for the crisis management event;

» The emotion engine, which tags and manages information for training scenarios on the basis of emotional affect;

» The training environment, which integrates multimedia components dynamically to reflect a developing narrative-based crisis scenario.
Information

Acronym: PANDORA

Grant Agreement N°: 225387

Total Cost: € 3,995,071

EU Contribution: € 2,930,000

Starting Date: 01/01/2010

Duration: 2 years

Coordinator:

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

Contact:

Reginald DALY
Tel: +44 02083319685
Fax: +44 02083318665
Website: http://PANDORAproject.eu/

Partners

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

COUNTRY
United Kingdom
United Kingdom
United Kingdom
Italy
Italy
Italy
Slovenia
France
France
**PLANTFOODSEC** / Plant and food biosecurity

### 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 in stakeholders and general public on biosecurity issues;
- overcoming the fragmentation of partner’s 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 system, 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 partner’s 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 anticipates better 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 European agriculture, farming and agrifood industry.
Information

**Acronym:**
PLANTFOODSEC

**Grant Agreement N°:**
261752

**Total Cost:**
€ 5,609,529.69

**EU Contribution:**
€ 4,624,499.00

**Starting Date:**
01/02/2011

**Duration:**
60 months

**Coordinator:**

Università 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

---

**NAME**
Centre of Competence for the innovation in the agro-environmental field, University of Torino
National Institute of Agricultural Botany
The Secretary of State for Environment, Food and Rural Affairs
Rheinische Friedrich-Wilhelms-Universitaet 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
### Project objectives

The objective of PRACTICE project is to improve the preparedness and resilience of the EU member states and associated 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 1) identification, organization and establishment of knowledge of critical elements in the event structure thorough studies of a wide selection of scenarios, real incidents and exercises, 2) 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; 3) 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.
**Information**

**Acronym:**
PRACTICE

**Grant Agreement N°:**
261728

**Total Cost:**
€ 11,695,072

**EU Contribution:**
€ 8,424,029

**Starting Date:**
01/05/2011

**Duration:**
42 months

---

**Coordinator:**

**Umea University**
European CBRNE Centre
Linnaeus väg 6
90187 Umea

**Contact:**

**Dzenan Sahovic**
Tel : +46 (0) 90 786 5774
Mobile : +46 (0) 73 073 5303
Fax : +46 (0) 90 786 6681
E-mail : dzenan.sahovic@cbrne.umu.se
Website : www.umu.se/cbrne

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Umea University (UmU)</td>
<td>Sweden</td>
</tr>
<tr>
<td>FORSVARETS FORSKNINGINSTITUTT (FFI)</td>
<td>Norway</td>
</tr>
<tr>
<td>ASTRIAM S.A.S. (AST)</td>
<td>France</td>
</tr>
<tr>
<td>Cassidian SAS (EADS)</td>
<td>France</td>
</tr>
<tr>
<td>NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK – TNO (TNO)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>KING’S COLLEGE LONDON (KCL)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>IB Consultancy BV (IBC)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>CBRNE Ltd (CBRNEltd)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>NATIONAL CENTER FOR SCIENTIFIC RESEARCH «DEMOKRITOS» (NCSR)</td>
<td>Greece</td>
</tr>
<tr>
<td>TOTALFORSVARETS FORSKNINGSINSTITUT (FOI)</td>
<td>Sweden</td>
</tr>
<tr>
<td>UNIVERSITE CATHOLIQUE DE LOUVAIN (UCL)</td>
<td>Belgium</td>
</tr>
<tr>
<td>Netherlands Forensic Institute (NFI)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>STATNI USTAV JADERNE, CHEMICKE A BIOLOGICKE OCHRANY vvi (SUJCHBO)</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>SELEX SISTEMI INTEGRATI SPA (SSI)</td>
<td>Italy</td>
</tr>
<tr>
<td>SELEX GALILEO LTD (SELEX)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>ASTRI POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA (AstriPL)</td>
<td>Poland</td>
</tr>
<tr>
<td>COMITE EUROPEEN DE NORMALISATION (CEN)</td>
<td>Belgium</td>
</tr>
<tr>
<td>Szkoła Główna Służby Pozarnej (SGSP)</td>
<td>Poland</td>
</tr>
<tr>
<td>MITTUNIVERSITETET (MIUN)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Prometech BV i.o. (PRO)</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>BRUHN NEWTECH A/S (BNT)</td>
<td>Denmark</td>
</tr>
<tr>
<td>HEALTH PROTECTION AGENCY HPA (HPA)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>SODERSJUKHUSET AB (SPC)</td>
<td>Sweden</td>
</tr>
</tbody>
</table>
**SecurEau / Security and decontamination of drinking water distribution systems following a deliberate contamination**

**Project objectives**

The main objective of this proposal is to launch an appropriate response for rapidly restoring the use of the drinking water network after a deliberate contamination and by way of consequence to limit the impact on the population of safe water privation because of contaminated networks. Five main topics will be addressed:

- Detection of unexpected changes in water quality.
- Adaptation of analytical methods to rapidly detect specific CBRN contaminants.
- Localization of the point source(s) of contamination.
- Decontamination procedures of the distribution system.
- Controlling the efficacy of the corrective actions.

**Description of the work**

SecurEau will implement an effective and timely response on CBRN attack. Questions that will be addressed for successful coordinated response of water utilities and regulatory agencies to contamination include:

- Detection of unexpected changes in water quality which could be in relation with a deliberate contamination event, by applying commercially available or recently developed generic sensors placed throughout the distribution systems.
- Adaptation of known analytical methods to rapidly detect specific CBRN contaminants in water and especially in biofilms and on pipes walls.
- Localization of the point source(s) of contamination and subsequently the contaminated area (via modelling reactive transport) allowing delimitation of the corrective actions.
- Decontamination procedures (efficient and realistic) of the distribution system, i.e. adapted to size, age, architecture of the network, including the treatment of water extracted from the system and used for washing the pipe wall.
- Controlling the efficacy of the corrective actions by analysing the water bulk and especially the pipe walls surface and the deposits.
- The cases studies will give the chance for the practitioners to apply on site in realistic conditions the selected sensors, softwares and remediation technologies. It is a unique occasion to test an emergency procedure on a complicated, quasi directly inaccessible, and relatively fragile system, to evaluate its feasibility at field scale, and to evaluate the difficulty to apply corrective treatments to the huge water bulk generated by the neutralisation/extraction of contaminants.

**Expected results**

As a result of this research and methodological effort the consortium plans to develop and validate adapted technologies, analytical tools, sensors and new software, which should reinforce the competitiveness of European Union. These tools and technologies are planned to give results quickly at affordable costs. Cases studies will give the chance for the practitioners to apply on site in realistic conditions the selected sensors, software and remediation technologies.
Information

Acronym: SecurEau

Grant Agreement N°: 217976

Total Cost: € 7,470,489

EU Contribution: € 5,269,578

Starting Date: 01/02/2009

Duration: 48 months

Coordinator:

Université 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/

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Université Henri Poincaré – Nancy 1 (UHP)</td>
<td>France</td>
</tr>
<tr>
<td>Centre National de la Recherche Scientifique (CNRS)</td>
<td>France</td>
</tr>
<tr>
<td>Veolia Environnement Recherche et Innovation (VERI)</td>
<td>France</td>
</tr>
<tr>
<td>Rheinisch-Westfälisches Institut für Wasserforschung gemeinnützige GmbH (IWW)</td>
<td>Germany</td>
</tr>
<tr>
<td>University of Southampton (SOTON)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Faculdade de Engenharia da Universidade do Porto (FEUP)</td>
<td>Portugal</td>
</tr>
<tr>
<td>Riga Technical University (RTU)</td>
<td>Latvia</td>
</tr>
<tr>
<td>Centre national du Machinisme Agricole, du Génie Rural, des Eaux et des Forêts (CEMAGREF)</td>
<td>France</td>
</tr>
<tr>
<td>Commissariat à l’Energie Atomique (CEA)</td>
<td>France</td>
</tr>
<tr>
<td>Veolia Water Central (VWC)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Radiation and Nuclear Safety Authority (STUK)</td>
<td>Finland</td>
</tr>
<tr>
<td>National Institute for Health and Welfare (THL)</td>
<td>Finland</td>
</tr>
</tbody>
</table>
SECURENV / Assessment of environmental accidents from a security perspective

Project objectives

Environmental security is becoming an important issue for the future development of the European Union. Despite all efforts and advances in security and civil protection our natural habitat remains most vulnerable to natural or intentional environmental damage. New and emerging threats to the environment and the potential consequences of these are also becoming more and more difficult to anticipate.

The overall objective of the project has been to increase the knowledge-base needed to ensure the security of citizens from emerging new threats to the environment. The project has analysed major industrial and environmental accidents together with past examples of deliberate environmental destruction (warfare, terrorism, blackmail, etc.) from a security perspective. Foresight methods and scenario building techniques were developed and used to assess potential future risks with the objective to provide end-users and policy makers with recommendations for improving preparedness.

Description of the work

The project started by establishing a database with incidents and then analysing past environmental accidents, catastrophes and cases of deliberate attacks on the environment, such as examples of environmental warfare or the role of organised crime in environmental degradation. These background investigations confirmed that despite all efforts and advances in security and civil protection, the human habitat – our natural environment – remains most vulnerable. Parallel to the assessment work, a foresight methodology tailored to the specific needs of SECURENV was designed. The aim of the foresight exercise was to identify possible novel and emerging threats based on the background analysis already conducted. For this purpose, existing foresight approaches in the area of environment and security were reviewed, synthesised and tailored to support project objectives. Key milestones of the foresight were a two-round Delphi survey with over 120 European and other experts (April – September 2010), a two-day scenario workshop in Stockholm (November 2010) with European environmental and security experts and a final end-user workshop with European policy makers in Brussels (April 2011).

Special attention was given to the rapid developments in science and technology like biotechnology and nanotechnology, natural disasters and industrial accidents including Natech incidents, the risks involved with development of geoengineering methods as well as incidents related to invasive alien species, as investigations by the project and foresight exercise revealed the scale of the potential economic and environmental damage some of these incidents can cause.

Results

The foresight exercise identified potential vulnerabilities and emerging trends that could pose a threat to the security of European citizens. Results were converted into specific recommendations for

• Adjusting the European research agenda to address emerging threats to the environment.
• Awareness raising and increasing the knowledge-base of those professionals, who are involved in law enforcement, environmental protection and related areas.
Information

Acronym: SECURENV

Grant Agreement N°: 218152

Total Cost: € 851,245

EU Contribution: € 851,245

Starting Date: 01/05/2009

End Date: 30/05/2011

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

Partners

NAME
Geonardo Environmental Technologies Ltd.
Adelphi Research
The Swedish Defence Research Agency, FOI

COUNTRY
Hungary
Germany
Sweden
SGL for USaR / Second generation locator for urban search and rescue operations

**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. Employ the same kind of devices for monitoring and identifying hazardous conditions in voids of collapsed buildings due to construction’s physical damage, flaming or smoldering fires and gases released.

- To integrate early location and monitoring systems with communication and information management applications that can provide with multi-level processing and data fusion and will support relevant USaR services and logistics (medical support, mobilization, tools, transportations, communications). SGL for USaR project will use multidisciplinary approaches, optimize existing cutting-edge technologies and make the best use of available resources.

The project is targeted on delivering next generation systems for USaR operations. For that purpose, relevant technical, scientific and operational issues will be addressed.

The project focuses on rapid location of entrapped or buried victims (alive or deceased) and the continuous monitoring of the air conditions in the voids of damaged and partially collapsed structures. Entrapped people and voids are associated with characteristic visual, sound and chemical profiles, due to specific images or spectral emissions, to acoustic signatures and chemical markers.

The adaptation of crisis management USaR services (logistics) with the early location and monitoring systems in a mobile command and control operational center is employed.

The project is formed by eight sub-projects (work packages) running in parallel. These WPs address the development of simulation environments; the development and validation of portable devices for location operations; the development and validation of smart sensors environment for monitoring the situation under the ruins; the management of medical information, including privacy and bioethics; and finally the development of an ICT platform that will integrate all the previous data, ensure interoperability and control the flow of the information from the field to the operational center.

**Expected results**

SGL for USaR will deliver methods and guidelines, as well as, tangible prototypes: a stand-alone first responder device that integrates five different location methods; a networked rapid casualty location system (REDS) equipped with wireless sensor probes; an advanced environmental simulator for training and testing search and rescue units, including canine teams; and a prototype mobile operational command and control platform.
Information

Acronym: SGL for USaR

Grant Agreement N°: 217967

Total Cost: € 6,217,478

EU Contribution: € 4,859,026

Starting Date: 01/10/2008

Duration: 48 months

Coordinator:
NATIONAL TECHNICAL UNIVERSITY OF ATHENS
Heroon Polytechneiou
15780 Zographou
Greece

Contact:
Milt Statheropoulos
Tel.: + 30 210 7723109
Fax: + 30 210 7723188
E-mail: stathero@chemeng.ntua.gr
Website: www.sgl-eu.org

Partners

NAME
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
Envionics Oy
Austrian Academy of Sciences
Entente Interd épartementale 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
Spain
Germany
Spain
Finland
Germany
Spain
Greece
United Kingdom
Hungary
Portugal
United Kingdom
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 pre conceived scenario.

The combined effects of the above points allowed a documentation of both the unexpected bad and good things in the organization(s) thus leading to better responses, fewer unintended consequences and greater consensus on important decisions.

Application scenarios

The following scenarios were selected:

»Conventional weapons terrorist attack: being the most common and hence the most likely threat in the future. This scenario was used to evaluate the decision support achievable with the SICMA prototype in the management of casualties. The focus was on the management of the most likely category of casualties that 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 website of the project www.sicmaproject.eu and the CORDIS website http://cordis.europa.eu/fp7/security.
**Information**

**Acronym:**  
SICMA

**Grant Agreement N°:**  
217855

**Total Cost:**  
€ 3,902,630

**EC Contribution:**  
€ 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.sicmaproject.eu/SicmaProjectSite2008/index.html

---

**NAME**

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

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 threat 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:

1. tools to quantify the vulnerability of built infrastructure;
2. a portfolio of protective products;
3. a guidance tool for safety based engineering to realize a required built infrastructure protection and resilience level;
4. a proposal on how to take CBRE-threat into account in the building guidelines.

Description of the work

Terrorist attacks with explosives (E) or chemical, biological or radiological (CBR) agents are threats with a low probability but with disastrous consequences. People, critical infrastructures and utilities have to be protected. The societal community should not be disrupted by acts of terrorism.

SPIRIT works on solutions to realize sufficient resilience of the urban infrastructure for rare occasions with minimum effect on normality. Hitherto, normal regulations and building guidelines do not take into account the CBRE threat.

The required specialist knowledge on explosion dynamics, response of structures, dispersions of toxic agents and injuries is available within the SPIRIT Consortium. Making this knowledge available and finding solutions that can be integrated into normal planning and building procedures is part of the work to be carried out.

Expected results

The project will contribute to people safety and increase the resilience of built infrastructure against a terrorist threat by providing an integrated approach to counter CBRE-threats, including proposed guidelines for a EU Regulatory Framework. With this approach, government, end users of buildings and designers can define and achieve a desired level of protection.
**Information**

**Acronym:** SPIRIT

**Grant Agreement N°:** 242319

**Total Cost:** € 4,885,951.00

**EU Contribution:** € 3,497,684.50

**Starting Date:** 01/08/2010

**Duration:** 36 months

**Coordinator:**

NEDERLANDSE ORGANISATIE VOOR TOEGEPAST-NATUURWETENSCHAPPELIJK ONDERZOEK - TNO

Physical Protection and Survivability

Lange Kleiweg 137

PO Box 45

2280 AA Rijswijk

The Netherlands

—

**Contact:**

Ms Jolanda van Deursen

Tel : +31 (0) 888 66 1289

Mobile : +31 (0) 630 72 7331

Fax : +31 (0) 888 66 6932

E-mail : Jolanda.vandeursen@tno.nl

Website : http://www.infrastructure-protection.org

---

**Partners**

**NAME**

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

Commissariat à l’énergie atomique et aux energies alternatives (CEA) France

Schüßler-Plan Engineers Ltd (SP) Poland

Arup Group Ltd (ARUP) United Kingdom

Hamilton Erskine Ltd (HE) NI, United Kingdom

Artemis control AG (ART) Switzerland

Ducon GmbH (DUC) Germany

Ionicon Analytik GmbH (ION) Austria

Corsmit Raadgevend Ingenieurs BV (CORS) The Netherlands

Joint Research Centre (JRC) Italy
CREATIF / CBRNE related testing and certification facilities -
A networking strategy to strengthen cooperation and knowledge exchange within Europe

Project objectives

The CREATIF network focuses on information exchange and collaboration between existing test facilities throughout the EU targeted to CBRNE detection – to support best practice for providing quality test results which fulfil end-user demands of tested products and potentially supporting the interoperability of devices. Moreover, all stakeholders are invited to contribute to the discussion and introduce their needs and views on the topic.

The main objectives of CREATIF are defined as:
» collect and provide information on test facilities and their portfolio of expertise
» support user decisions and product / service development
» offer a forum to discuss security related testing for all stakeholders (decision makers, end-users, industry, EU-bodies)
» define roadmap for the future development of testing incl. standardization & certification
» amend testing protocols to cover human factors and operational issues of CBRNE detection

Description of the work

The CREATIF network is dedicated to provide a communication platform for technology users and decision makers, manufacturers and testers to discuss the future development of testing and to support user decisions and industry product / service development. All these stakeholders have been invited to become members of the network and exchange their views and knowledge: testing facilities can publish information about their expertise and testing capabilities in a database on testing facilities within EU-27, a stakeholder group of end-users and industrial experts has been established to integrate their point of view into project deliverables and topical workshops.

In these workshops specific themes in the field of certification and testing of CBRNE detection equipment are discussed. Proceedings have been compiled to distribute the outcome of discussions and present information to a wide audience. CREATIF has performed an examination of existing testing protocols and relevant standards to suggest harmonization of testing in the field of CBRNE detection. This will allow quality assurance and comparability of testing results. Possibilities to amend testing protocols by covering human factors and operational / scenario based testing are outlined. Additional deliverables of the network include a roadmap for a European certification system for CBRNE detection products & services and a concept on the continuation of the CREATIF network as an autonomous body after the end of the funded project.

The certification system for CBRNE detectors, as suggested by CREATIF, can be carried by the testing facilities already in the network, all other necessary structures like an overarching certification body assuring quality of testing and managing a kind of labelling system could be developed out of the network as well. The implementation will depend on the political willingness and financial support by national/European authorities.

Results

The most important deliverables produced by CREATIF include:
» Glossary of terms to find common language for CBRNE detection testing
» Database on test facilities for CBRNE detection equipment
» Report on available standards and protocols for testing CBRNE detection systems
» Outline for joint testing exercises for C / B / RN / E detection systems
» Workshop proceedings on end-user needs and stakeholder views to the topic of testing CBRNE detectors and standardization of testing
» Operational testing framework
» Road map for an European certification system for CBRNE sensor systems and devices
» Business plan for an independent CREATIF Network of test facilities
Information

Acronym: CREATIF

Grant Agreement N°: 217922

Total Cost: € 831,300

EU Contribution: € 831,300

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

Partners

NAME COUNTRY
Seibersdorf Labor GmbH (SL) Austria
DGA Techniques Terrestres (DGA LS) France
DGA Maîtrise NRBC – Site du Bouchet (DGA CBRN) France
Cotecna Inspection S.A. (COT) Switzerland
Federal Institute for Materials Research and Testing (BAM) Germany
The Swedish Defence Research Agency (FOI) Sweden
Netherlands Organisation for Applied Scientific Research (TNO) The Netherlands
SECURITY RESEARCH

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

Project objectives

One of the main problems of First Responders (FR) (fire fighters, police, etc.) in 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 headquarter.

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 FR according to their defined missions).
End-user inputs: Presentation of some typical infrastructures (arrangement of the buildings, legal constraints, emergency measures) and of typical intervention of FR

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

» Third Workshop: Presentation by the consortium of the selected technologies (innovated and/or improved).
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: Analyse and comments with the R&D team of the proposed solutions and first view on the integration in a systemic approach.

» Fifth Workshop: Demonstration 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.
### Information

<table>
<thead>
<tr>
<th>Acronym</th>
<th>DITSEF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Agreement N°:</td>
<td>225404</td>
</tr>
<tr>
<td>Total Cost:</td>
<td>€ 4,245,436</td>
</tr>
<tr>
<td>EU Contribution:</td>
<td>€ 2,800,000</td>
</tr>
<tr>
<td>Starting Date:</td>
<td>01/01/2010</td>
</tr>
<tr>
<td>Duration:</td>
<td>36 months</td>
</tr>
</tbody>
</table>

**Coordinator:**

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

**Contact:**

Philippe Clément
Tel: +33 1 69 19 94 85
E-mail: Philippe.clement@sagem.com
Website: http://www.ditsef.eu/

### Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sagem Defense Securite (SDS)</td>
<td>France</td>
</tr>
<tr>
<td>TNO</td>
<td>Netherland</td>
</tr>
<tr>
<td>EADS</td>
<td>France</td>
</tr>
<tr>
<td>Center for Security Studies (KEMEA)</td>
<td>Grece</td>
</tr>
<tr>
<td>CEA</td>
<td>France</td>
</tr>
<tr>
<td>Elsag Datamat spa (ED)</td>
<td>Italie</td>
</tr>
<tr>
<td>National Centre for Scientific Research ‘Demokritos’</td>
<td>Grece</td>
</tr>
<tr>
<td>INFITHEON Technologies Ltd (INFI)</td>
<td>Grece</td>
</tr>
<tr>
<td>T - SOFT spol. s r.o. Praha</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Ministry of Emergency Situations Territory Department “Civil Protection” – Montana Region</td>
<td>Bulgaria</td>
</tr>
</tbody>
</table>
EULER / European software defined radio for wireless joint security operations

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.

Expected Results

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

**Acronym:**
EULER

**Grant Agreement N°:**
218133

**Total Cost:**
€ 15,468,483

**EU Contribution:**
€ 8,720,692

**Starting Date:**
01/03/2009

**Duration:**
36 months

**Coordinator:**

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

---

**Contact:**

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

---

**NAME**

- Thales Communications S.A
- Eads Secure Networks
- Astrium Limited
- Budapest University of Technology and Economics
- Elsag Datamat s.p.a.
- Selex Communications S.P.A.
- Telespazio S.P.A.
- Universita di Pisa.
- Saab Communications
- TNO
- Indra Sistemas S.A.
- Rohde & Schwarz gmbh.
- Center for Wireless Communications, University of Oulu
- Prismtech Limited
- IMEC
- JRC
- Ecole Superieure d’Electricite
- Elektrobit Wireless Communications

**COUNTRY**

- France
- Hungary
- Italy
- Italy
- Italy
- Italy
- Sweden
- Spain
- Germany
- Finland
- United Kingdom
- Belgium
- Belgium
- France
- Finland
HELP / Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems

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. Project 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 to create and exploit synergies of composite radio systems encompassing commercial and professional mobile radio networking technologies can address the complex requirements of modern emergency communications. Project HELP will define and establish the foundations for the development of network and spectrum sharing concepts between networks. Project 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

Project 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, Project HELP will define a solution framework (system concept) for the provision of public safety communications over diverse wireless infrastructures. This will include, e.g., (1) determining internetworking solutions, (2) determining the required features and functionalities that will enable the use of commercial systems for public safety communications in emergency and disaster relief operations, (3) 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 Project HELP may have on the involved stakeholders will be investigated. Project HELP will eventually establish a consolidated basis and roadmap for the realisation of the envisioned solution framework.

Expected results

The tangible results include the provision of documentation describing: (1) key operational scenarios and system requirements, (2) feasibility studies to determine potential design choices for network and spectrum sharing solutions, (3) system concept, high level system design and associated management framework, (4) techno-economic assessment of the envisioned system concept and (5) a roadmap for the realisation of the envisioned solution framework. Furthermore, two Workshops will be organised and dissemination of the outcomes will be pursued.
Information

**Acronym:**
HELP

**Grant Agreement N°:**
261659

**Total Cost:**
€ 1,352,219

**EU Contribution:**
€ 991,255

**Starting Date:**
01/02/2011

**Duration:**
15 months

**Coordinator:**

UNIVERSITAT POLITÉCNICA DE CATALUNYA
Signal Theory and Communications
Jordi Girona 31
08034- Barcelona-
Spain

---

**Contact:**

Oriol Sallent
Tel.: +34 93 401 7197
Mobile: +34 619 35 16 54
Fax: +34 93 401 7200
E-mail: sallent@tsc.upc.edu
Website: www.fp7-sec-help.eu

---

**NAME**

- DATAX SP. Z O.O.
- CASSIDIAN S.A.S.
- BAPCO LBG
- JRC -JOINT RESEARCH CENTRE- EUROPEAN COMMISSION

---

**COUNTRY**

- Poland
- France
- United Kindom
- Belgium
In September 2006 the European Security Research Advisory Board (ESRAB) published a report setting the European security research agenda and the requirements on new communication infrastructures.

These requirements included security, dependability, enhanced connectivity, transmission of multiple formats and advanced search functions.

In response to these ESRAB requirements, the collaborative research project SECRICOM will create and demonstrate a secure communication platform for crisis management in Europe.

**Project objectives**

Solve problems of contemporary crisis communication infrastructures:
- Seamless and secure interoperability of existing many hundred thousand mobile devices already deployed;
- Smooth, simple, converging interface from systems currently deployed to systems of the new SDR generation;
- Creation of pervasive and trusted communication infrastructure, bring interconnectivity between different networks;
- Provide true collaboration and inter-working of emergency responders; and
- Seamlessly support different user traffic over different communication bearers.

Add new smart functions using distributed IT systems based on an SDR secure agents’ infrastructure:
- Easier instant information gathering and processing focusing on emergency responders main task – saving lives.

**Description of the work**

The project work is divided into nine RTD work-packages supported by two work-packages for management and dissemination. Top innovations deal with:
- Creation of secure wireless fault tolerant communication system for mobile devices based on push-to-talk system;
- Secure distributed system; and
- Secure docking module – system on chip design.

These innovations will be extended by:
- IPV6 based secure communication;
- Internetwork interfaces, interoperable, recoverable and extendable network;
- Communication infrastructure monitoring and control centre equipped with localization of actors.

**Expected results**

The SECRICOM will develop and demonstrate a secure communications infrastructure for public safety organisations and their users.

Achievements will include:
- The exploitation of existing publicly available communication network infrastructure with interface towards emerging SDR systems.
- Interoperability between heterogeneous secure communication systems.
- A parallel distributed mobile agent-based transaction system for effective procurement.
- Infrastructure based on custom chip-level security.
**Information**

**Acronym:**
SECRICOM

**Grant Agreement N°:**
218123

**Total Cost:**
€ 12,468,847

**EU Contribution:**
€ 8,606,791

**Starting Date:**
01/09/2008

**Duration:**
44 months

**Coordinator:**

QINETIQ LTD
Buckingham Gate 85
UK-SW1E 6PD London
United Kingdom

**Contact:**

David Traynor
Tel: +44 (0) 2392 31 2750
Fax: +44 (0) 2392 31 2768
Mobile: +44 (0) 7881846076 / (0) 7590551967
E-mail: dtraynor@qinetiq.com
Website: http://www.secricom.eu

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>QinetiQ Ltd</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Ardaco, as.</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Bumar Ltd.</td>
<td>Poland</td>
</tr>
<tr>
<td>NEXTEL S.A.</td>
<td>Spain</td>
</tr>
<tr>
<td>Infineon Technologies AG</td>
<td>Germany</td>
</tr>
<tr>
<td>Université du Luxembourg</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>Institute of Informatics, Slovak Academy of Sciences</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Graz University of Technology</td>
<td>Austria</td>
</tr>
<tr>
<td>Smartrends, s.r.o.</td>
<td>Slovakia</td>
</tr>
<tr>
<td>ITTI Sp. z o.o.</td>
<td>Poland</td>
</tr>
<tr>
<td>British Association of Public Safety Communication Officers</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>CEA</td>
<td>France</td>
</tr>
<tr>
<td>Hitachi Europe SAS</td>
<td>France</td>
</tr>
</tbody>
</table>
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:

1. Implement Ethical and Privacy Safeguards
2. Minimise False Alerts
3. Minimise Network (data) traffic bandwidth demand arising from VA deployment
4. Minimise the required human attention bandwidth in using VA surveillance
5. Ensure easy, cost-effective, efficient and effective deployment of VA systems
6. Establish a sustainable business case and revenue model for VA technology uptake
7. Minimise the storage requirements for VA deployment
8. Integrate with identification technologies
9. Trust interoperability between VA systems
10. Conduct benchmarking and comparative evaluation of alternative products

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’s 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 the European society, citizen 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, sense-ful, 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 inter-connected 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 the European citizen, 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.
### Information

- **Acronym:** VIDEOSENSE
- **Grant Agreement N°:** 261743
- **Total Cost:** € 6,412,895.00
- **EU Contribution:** € 5,282,366.00
- **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

---

### Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON (QMUL)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>EURECOM (EURECOM)</td>
<td>France</td>
</tr>
<tr>
<td>THALES SECURITY SOLUTIONS &amp; SERVICES SAS (THALES)</td>
<td>France</td>
</tr>
<tr>
<td>INGENIERA DE SISTEMAS PARA LA DEFENSA DE ESPANA SA-ISDEFE (ISDEFE)</td>
<td>Spain</td>
</tr>
<tr>
<td>TECHNISCHE UNIVERSITAET BERLIN (TUB)</td>
<td>Germany</td>
</tr>
<tr>
<td>ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE (EPFL)</td>
<td>Switzerland</td>
</tr>
<tr>
<td>INTERNATIONAL FORUM FOR BIOPHILOSOPHY (IFB)</td>
<td>Belgium</td>
</tr>
</tbody>
</table>
ADDPRIV / Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance

Project objectives

The ADDPRIV project proposes novel knowledge and developments to better comply with citizen’s 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 on 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 with; preliminary definition of the system compliance with citizens’ privacy evaluating criteria.

» Definition of technical specifications: detailed definition of the ADDPRIV solution 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 difference 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 leads 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 in redundancy with the already existing video surveillance systems.

» Analysis of the impact of the proposed solutions on human rights and organizational processes: analysis of ADDPRIV 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 of 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.
Information

**Acronym:** ADDPRIV

**Grant Agreement N°:** 261653

**Total Cost:** € 4,077,720.40

**EU Contribution:** € 2,818,338.00

**Starting Date:** 01/02/2011

**Duration:** 36 months

**Coordinator:**

Anova IT Consulting, SL

Avda. Punto Mobi, 4 - Parque Científico Tecnológico de la Universidad de Alcalá

28805 – Alcalá de Henares

Spain

**Contact:**

Paolo D’Arminio

Tel : +34 918 305 977

Mobile : +34 634 933 543

Fax : +34 918 305 928

E-mail : paolo.darminio@anovagroup.es

Website : www.addpriv.eu

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>KINGSTON UNIVERSITY HIGHER EDUCATION CORPORATION</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>POLITECHNIKA GDANSKA</td>
<td>Poland</td>
</tr>
<tr>
<td>LANCASTER UNIVERSITY</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>AVANZIT TECNOLOGIA, S.L.</td>
<td>Spain</td>
</tr>
<tr>
<td>HEWLETT PACKARD ITALIANA SRL</td>
<td>Italy</td>
</tr>
<tr>
<td>SOCIETA PER AZIONI ESERCIZI AEROPORTUALI SEA SPA</td>
<td>Italy</td>
</tr>
<tr>
<td>Renfe Operadora</td>
<td>Spain</td>
</tr>
<tr>
<td>THE PROVOST FELLOWS &amp; SCHOLARS OF THE COLLEGE OF THE HOLY</td>
<td></td>
</tr>
<tr>
<td>AND UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN</td>
<td>Ireland</td>
</tr>
</tbody>
</table>
Project objectives

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

Description of the work

The BeSeCu project will carry out the following research studies:

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

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

» Experimental trials will be carried out simulating real time evacuation scenarios in standardized settings including objective measures (e.g. response time) as outcomes as well as video-tape analysis. Results will be analysed to identify similarities and differences between cultures and ethnic groups as well as a range of socioeconomic factors. The analysis will triangulate findings obtained with objective measures, subjective experiences and behavioural observations. The research will be carried out by a consortium of 8 European partners including end-users (e.g. fire service colleges).

Expected results

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

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

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

Acronym: BeSeCu

Grant Agreement N°: 218324

Total Cost: € 2,446,144

EU Contribution: € 2,093,808

Starting Date: 01/05/2008

Duration: 36 months

Coordinator:

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

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

Partners

NAME                      COUNTRY            
Ernst-Moritz-Arndt-Universitat Greifswald  Germany
University Medical Centre Hamburg  Germany
University of Greenwich, School of Computing and Mathematical Sciences  United Kingdom
Institute of Public Security of Catalunya  Spain
Hamburg Fire and Emergency Service Academy  Germany
Man-Technology-Organisation (MTO)-Psychology  Sweden
Faculty of Fire Safety Engineering (SGSP)  Poland
Prague Psychiatric Centre University of Prague  Czech Republic
Association of Emergency Ambulance Physicians  Turkey
CAST / Comparative assessment of security-centered training curricula for first responders on disaster management in the EU

Project objectives

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

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

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

Description of the work

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

The comparative assessment covered:

- Didactic areas (electronic and hardcopy teaching materials used, computer modelling, field exercises);

- Subject areas (terror threats to FR; risk assessment and management; catastrophic terrorism; weapons of mass destruction, mass killing, mass disturbance; synchronization of response staff);

- Comparative evaluation of training course curricula by virtual reality safety training with biofeedback.

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

The results of the assessment were used to:

1. Establish an EU-security curricula database;

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

3. Recommend an Action Plan for eliminating training deficiencies;

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

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

Results

The results of the project are available on the website of the project http://cast.sbg.ac.at/ and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: CAST

Grant Agreement N°: 218070

Total Cost: € 2,858,318

EU Contribution: € 1,974,620

Starting Date: 01/07/2009

End Date: 30/06/2011

Coordinator:

UNIVERSITAT SALZBURG
Office of the Rectorate
Research Support Unit
Kapitelgasse 4-6
A-5020 Salzburg
Austria

Contact:

Prof. Friedrich Steinhäusler
Tel.: +43 (0) 662 8044 5700
Mobile: +43-680-123 7158
Fax.: +43-662-8040 150
E-mail: Friedrich.steinhaeusler@sbg.ac.at
Website: www.research.sbg.ac.at/cast

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universität Salzburg (PLUS)</td>
<td>Austria</td>
</tr>
<tr>
<td>Austrian Technologies (AT (AT)</td>
<td>Austria</td>
</tr>
<tr>
<td>DSTS-Advisers to Executives (DSTS)</td>
<td>Austria</td>
</tr>
<tr>
<td>– Fire Service Academy Hamburg (FSAH)</td>
<td>Germany</td>
</tr>
<tr>
<td>Research Institute of Red Cross (FRK)</td>
<td>Austria</td>
</tr>
<tr>
<td>Fraunhofer Institut (Chem. Technologie) (Fraunhofer ICT)</td>
<td>Germany</td>
</tr>
<tr>
<td>BMLVS / Heereslogistikschule (HLogS)</td>
<td>Austria</td>
</tr>
<tr>
<td>International Security Competence Center (ISCC)</td>
<td>Austria</td>
</tr>
<tr>
<td>University of Defense Brno (UDB)</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Corvinus University Budapest (VGT)</td>
<td>Hungary</td>
</tr>
<tr>
<td>SAAB Training Systems AB (SAAB)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Swedish Counter Terrorist Police (SCTU)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Diamond Aircraft Industries (DAI)</td>
<td>Austria</td>
</tr>
<tr>
<td>Tecnatom (TEC)</td>
<td>Spain</td>
</tr>
<tr>
<td>Sigmund Freud Privatuniversität Wien (SFU)</td>
<td>Austria</td>
</tr>
<tr>
<td>Police Service of Northern Ireland (PSNI)</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
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 organizational and cultural factors can facilitate or hinder successful change implementation in European policing.

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.

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:

1. A comparative strategic analysis of strengths, weaknesses, opportunities and threats for police organizations in 10 European countries
2. Analysis of the planning and execution of change processes and best practices to meet current and future challenges.
3. An annual European Police Monitor tracking how police forces across Europe are developing and improving.
Acronym: COMPOSITE

Grant Agreement N°: 241918

Total Cost: € 8,904,352.73

EU Contribution: € 6,623,303.00

Starting Date: 01/08/2010

Duration: 48 months

---

NAME

University of Utrecht
Police Academy, Apeldoorn
Fraunhofer Institute, Sankt Augustin
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
Germany
Germany
United Kingdom
United Kingdom
Belgium
France
France
Republic of Macedonia
Czech Republic
Italy
Romania
Spain

Coordinator:

Erasmus University Rotterdam
Rotterdam School of Management
Postbus 1738
3000 DR, Rotterdam
The Netherlands

Contact:

Gabriele Jacobs
Tel: +31(0) 10 4082061
Mobile: +31(0) 6 57559341
Fax: +31(0) 10 4089015
E-mail: gjacobs@rsm.nl
Website: www.composite-project.eu
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.

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 website of the project www.cpsi-fp7.eu and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

**Acronym:**
CPSI

**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 NATUURWETENSCHAPPELIJK ONDERZOEK – TNO**

Defence, Security and Safety
Kampweg 5
P.O. Box 23
3769 ZG Soesterberg
The Netherlands

---

**Contact:**

**Dr. Heather J. Griffioen-Young**

Tel.: +31-346-356-378
Mobile: +31-6-2246-1065
Fax: +31-346-353-977
E-mail: heather.griffioen@tno.nl
Website: www.cpsi-fp7.eu

---

**Partners**

**NAME**

TNO
FOI
University of Kent
Sogeti
Temis
JRC
Centre for European Security Studies
Social Cultural Planning Office
VLC

**COUNTRY**

The Netherlands
Sweden
United Kingdom
France
Italy
Austria
The Netherlands
Project objectives

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

To meet this goal the project has four key objectives:

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

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

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

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

Description of the work

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

We will study communication strategies in various recent cases and analyse the reception of information in stressful situations. By identifying critical factors the challenges of crisis communication are addressed.

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

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

Results

The results of the project are available on the website of the project http://www.crisiscommunication.fi and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: CrisComScore

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.crisiscommunication.fi

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Jyväskylä Yliopisto</td>
<td>Finland</td>
</tr>
<tr>
<td>Ben Gurion University of the Negev</td>
<td>Israel</td>
</tr>
<tr>
<td>University of Tartu</td>
<td>Estonia</td>
</tr>
<tr>
<td>Norwegian University of Science and Technology</td>
<td>Norway</td>
</tr>
<tr>
<td>Emergency Services College Finland</td>
<td>Finland</td>
</tr>
</tbody>
</table>
Project objectives

The DESSI project will develop a tool that will support decision-makers in situations, where different possible solutions for a perceived security-problem are available. It will enable a comparison and evaluation of different security investments and serve as a way to achieve transparency of the security decisions.

Description of the work

The post-9-11 era is still upon us. Investments in safeguarding the security of European citizens have increased dramatically. Often the security dimension overshadows other critical aspects of decisions, i.e. political, ethical, and social. This has led to a securitization of several areas of society, such as transport, public space, health care, etc. Decisions are seemingly immediate responses to specific security issues. They tend to be technology driven. There is an urgent need for a political framework that directs all processes that lead to decisions on security investment to be transparent and participatory, and that accounts for context and multi-dimensionality of society.

Security investments are made to avoid known or perceived threats. Threats could be conventional crime, cyber-crime, inner security, international conflicts, environmental hazards, and mixed forms of these. It is important to first understand the nature of the threat, consequences, probability and impact of the threat and who is affected by it.

Security investment includes a choice between different approaches to increasing security, and DESSI makes this choice explicit by describing and evaluating the security investment alongside its alternatives. In almost any security related decision-making, implicitly or explicitly a range of alternatives is considered. The DESSI tool will ensure this aspect to be explicit. The alternatives are identified or developed in a participatory process, including experts and stakeholders, which are informed by the threat description.

Security investments are often highly controversial and disputed decisions. This is not only because of political differences between actors but mostly because the societal phenomena involved (threat perception, technology insight, belief in alternative investments, etc.) are differently distributed and valued among the actors. Accordingly, a rigorous investment assessment method needs to make use of a participatory approach, which ensures that a range of relevant actors is taken on board in the assessment procedure.

Expected results

The DESSI project will provide a decision support system to decision makers and users of security investments. The system will give insight into the pros and cons of specific security investments. It will contribute to a transparent and participatory decision making that accounts for context and multi-dimensionality of society. It will be useful for public authorities, developers of security solutions, commercial enterprises and for social organizations that can use the DESSI tool to make their own comprehensive assessment as an input to strategic discussions or public debate.
## Information

**Acronym:** DESSI  
**Grant Agreement N°:** 261718  
**Total Cost:** € 1,902,303  
**EU Contribution:** € 1,561,095  
**Starting Date:** 01/01/2011  
**Duration:** 30 months  

**Coordinator:**  
**DANISH BOARD OF TECHNOLOGY**  
Danish Board of Technology  
Toldbodgade 12  
DK-1253 Copenhagen  
Denmark  

—  

**Contact:**  
**Ida Leisner**  
Tel : +45 3345 5355  
Mobile : +45 3345 5355  
Fax : +45 3391 0509  
E-mail : il@tekno.dk  
Website : www.securitydecisions.org, www.tekno.dk

## Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teknologiraadet - Danish Board of Technology (DBT)</td>
<td>Denmark</td>
</tr>
<tr>
<td>Peace Research Institute, Oslo (PRIO)</td>
<td>Norway</td>
</tr>
<tr>
<td>Teknologiraadet – Norwegian Board of Technology (NBT)</td>
<td>Norway</td>
</tr>
<tr>
<td>Verein für sozialwissenschaftliche Forschung und Beratung e.V. (SWFB)</td>
<td>Germany</td>
</tr>
<tr>
<td>Austrian Academy of Sciences, Institute of Technology Assessment (ITA)</td>
<td>Austria</td>
</tr>
</tbody>
</table>
Project objectives

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

Description of the work

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

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

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

Expected results

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

<table>
<thead>
<tr>
<th>Acronym:</th>
<th>DETECTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Agreement N°:</td>
<td>217862</td>
</tr>
<tr>
<td>Total Cost:</td>
<td>€ 2,424,416</td>
</tr>
<tr>
<td>EU Contribution:</td>
<td>€ 1,869,684</td>
</tr>
<tr>
<td>Starting Date:</td>
<td>01/12/2008</td>
</tr>
<tr>
<td>Duration:</td>
<td>36 months</td>
</tr>
</tbody>
</table>

**Coordinator:**

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

**Contact:**

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

## Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Birmingham</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Åbo Akademi University</td>
<td>Finland</td>
</tr>
<tr>
<td>University of Nottingham</td>
<td>United Kingdom, until 31.01.09</td>
</tr>
<tr>
<td>University of Zurich</td>
<td>Switzerland, from 01.02.09</td>
</tr>
<tr>
<td>University of Oslo, Centre for Human Rights</td>
<td>Norway</td>
</tr>
<tr>
<td>Raoul Wallenberg Institute of Human Rights and Humanitarian Law</td>
<td>Sweden</td>
</tr>
<tr>
<td>Danish Institute for Human Rights</td>
<td>Denmark</td>
</tr>
<tr>
<td>European University Institute</td>
<td>Italy</td>
</tr>
</tbody>
</table>
EUSECON / A new agenda for European security economics

Project objectives

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

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

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

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

Description of the work

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

It will employ the following methods:

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

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

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

Expected results

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

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

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

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

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

Acronym: EUSECON

Grant Agreement N°: 218105

Total Cost: € 3,000,736

EU Contribution: € 2,357,188

Starting Date: 01/03/2008

Duration: 48 months

Coordinator:

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

Contact:
Prof. Dr. Tilman Brück
Tel: +49-30-89789-591
Fax: +49-30-89789-108
E-mail: tbrueck@diw.de
Website: www.economics-of-security.eu/eusecon

Name

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
Queen Elisabeth House, University of Oxford
Centre for Criminology, 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

Country

Germany
Germany
Czech Republic
Czech Republic
Greece
United Kingdom
United Kingdom
United Kingdom
Spain
Spain
United Kingdom
Israel
Greece
Austria
Norway
The Netherlands
Project objectives

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

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

Looking ahead to the year 2030, this foresight study will scan the horizon of fields such as nanotechnologies, biotechnologies and information technologies, as well as capabilities that may emerge from converging fields. Emerging and evolving threats will then be evaluated by using various methods:

» Expert surveys to forecast likely onset of threat realization, assign prioritization and project the nature and extent of potential damage and social issues.

» Brainstorming to identify, discuss, classify and assess the potential threats.

» Listing and classifying interesting "weak signals" in order to identify "wild cards": unlikely but highly affecting events.

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

Critical early-warning indicators that hint at the growing likelihood of unforeseen scenarios will be identified.

Expected results

» Awareness of potential threats of specific new technologies.

» Initiation of a foresight process in Europe that continuously scans the unfolding technology landscape in anticipation of evolving threats.

» Alternative scenarios that outline future impacts of security threats with special attention to low likelihood but high-impact events.

» Identification of "early warning signals" that might hint at the growing likelihood of unforeseen scenarios.

» Policy guidelines aiming at novel means of preparedness for future threats.

Description of the work

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

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

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

Expected results

» Awareness of potential threats of specific new technologies.

» Initiation of a foresight process in Europe that continuously scans the unfolding technology landscape in anticipation of evolving threats.

» Alternative scenarios that outline future impacts of security threats with special attention to low likelihood but high-impact events.

» Identification of ‘early warning signals’ that might hint at the growing likelihood of unforeseen scenarios.

» Policy guidelines aiming at novel means of preparedness for future threats.
**Information**

**Acronym:** FESTOS

**Grant Agreement N°:** 217993

**Total Cost:** € 1,232,976

**EU Contribution:** € 824,552

**Starting Date:** 01/03/2009

**Duration:** 30 months

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

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

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interdisciplinary Center for Technology Analysis and Forecasting (ICTAF)</td>
<td>Israel</td>
</tr>
<tr>
<td>Turku School of Economics, Finland Futures Research Centre</td>
<td>Finland</td>
</tr>
<tr>
<td>Foundation for European Scientific Cooperation</td>
<td>Poland</td>
</tr>
<tr>
<td>EFP Consulting</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Technical University of Berlin</td>
<td>Germany</td>
</tr>
</tbody>
</table>
FOCUS / Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles

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:

1. 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;
2. natural disasters and environment-related hazards, with an emphasis on comprehensive risk reduction, civil protection and reconstruction;
3. critical infrastructure and supply chain protection, centred on preventing, mitigating and responding to exogenous threats that could have a significant impact on EU citizens;
4. the EU as a global actor regarding the so-called “wider Petersberg Tasks”, and building on EU and member states instruments and capability processes;
5. the evolution of the EU’s internal framework and prerequisites for delivering a comprehensive approach, including Lisbon treaty provisions and relevant strategies (e.g., for engagement with other international actors) as well as ethical acceptability and public acceptance.

The “embedded scenario” method and IT-based tools will be adjusted and sharpened as applied to these five thematic scenarios. Interrelations among themes and scenarios will be particularly addressed: FOCUS will investigate cross-cutting issues that constitute transversal key drivers/constraints. The project will explore interfaces and translation mechanisms by which exogenous threats – such as those stemming from global change – directly confront EU citizens, their perception and their actual state of security. It will also take into account the differential impact of external threats on national and European research programmes designed to enhance capabilities.

Expected results

FOCUS will deliver (a) an IT Platform with tools and infrastructure for designing, applying, evaluating and managing scenarios for research planning, all of which is (b) populated with scenarios and analyses; and, finally, (c) a roadmap with new tracks for security research.

In particular, FOCUS will identify and assess alternative sets of future tracks for security research in FP7 and subsequent programmes that will support the EU to adopt new roles in dealing with external threats, risks and vulnerabilities.
Information

Acronym: FOCUS

Grant Agreement N°: 261633

Total Cost: € 4,372,012

EU Contribution: € 3,407,075

Starting Date: 01/04/2011

Duration: 24 months

Coordinate:

SIGMUND FREUD PRIVATUNIVERSITAT WIEN GMBH
CEUSS | Center for European Security Studies
Schnirchgasse 9a
1030 Vienna
Austria

Contact:

Alexander Siedschlag
Tel: +43 (0) 1 798 62 90 50
Mobile: +43 (0) 699 113 69 717
Fax: +43 (0) 1 798 62 90 52
E-mail: siedschlag@european-security.info
Website: http://www.focusproject.eu

Partners

NAME

SIGMUND FREUD PRIVATUNIVERSITAT WIEN, CEUSS | CENTER FOR EUROPEAN SECURITY STUDIES (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)
INGENIERIA DE SISTEMAS PARA LA DEFENSA DE ESPAÑA SA (ISDEFE)
CESKE VYSOKE UCENI TECHNICKE V PRAZE (CVUT)
SECEUR SPRL (SECEUR)
UNIVERSITAET FUER WEITERBILDUNG KREMS (DUK)
UNIVERSITY OF HAIFA (U HAIFA)
UNIVERSITAET 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
Project objectives

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

Description of the work

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

» Desk study: A state-of-the-art scan of security and security research in 12 selected EU Member States and an analysis of the global context of European security are conducted to provide a common basis for the participatory foresight process.

» Participatory foresight methods: A kick-off workshop initiated public debate on European security and provided commentary and validation of state-of-the-art findings regarding threats and drivers. The workshop also produced statements on security and the security technologies that were used in the Delphi survey.

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

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

Results

The results of the project are available on the website of the project http://www.foresec.eu and the CORDIS website http://cordis.europa.eu/fp7/security.
**Information**

**Acronym:** FORESEC

**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

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis Management Initiative</td>
<td>Finland</td>
</tr>
<tr>
<td>Austrian Research Centres System Research</td>
<td>Austria</td>
</tr>
<tr>
<td>International Institute for Strategic Studies</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>FOI</td>
<td>Sweden</td>
</tr>
<tr>
<td>Centre for Liberal Studies</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>JRC</td>
<td>Italy</td>
</tr>
</tbody>
</table>
Project objectives

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

This security continuum results from the blurring of the demarcation between external and internal security questions, as external security authorities seek to locate threats in the internal security sphere and traditional internal authorities pursue security threats externally. While this continuum is studied in ongoing research, it contains essential value assumptions and ethical consequences that remain largely under-theorised, with significant consequences for both European policy and law-making.

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

INEX advances and tests the hypothesis that:

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

Description of the work

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

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

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

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

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

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

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

Results

The results of the project are available on the website of the project http://www.inex-project.eu and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: INEX

Grant Agreement N°: 218265

Total Cost: € 2,422,082

EU Contribution: € 1,890,248

Starting Date: 01/08/2008

End Date: 31/03/2011

Coordinator:

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

Contact:

J. Peter Burgess
Tel: +47 22 54 77 00
Fax: +47 22 54 77 01
E-mail: peter@prio.no
Website: http://www.inexproject.eu

Partners

NAME
International Peace Research Institute, Oslo
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
Project objectives

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

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

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

Description of the work

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

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

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

Results

The results of the project are available on the website of the project http://faculty.biu.ac.il/~sshpiro and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: SAFE-COMMS

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

Partners

NAME
Bar-Ilan University
A&B One GmbH
Research Institute for European and American Studies
University of Ulster
Universidad de Burgos
University of Rousse Angel Kunchev

COUNTRY
Israel
Germany
Greece
United Kingdom
Spain
Bulgaria
SAFIRE / Scientific approach to finding indicators and responses to radicalisation

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

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

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

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

**Acronym:** SAFIRE

**Grant Agreement N°:** 241744

**Total Cost:** € 3,681,260.00

**EU Contribution:** € 2,906,600.95

**Starting Date:** 01/06/2010

**Duration:** 42 months

**Coordinator:**

**Coordinators:**

**Coordinator:**

**Contact:**

**Dr. Heather Griffioen-Young**

Tel : +31-346356378

Fax : +31-346353977

E-mail : heather.griffioen@tno.nl

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

---

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNO</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Stichting Forum, Instituut voor Multiculturele Ontwikkeling</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>International Security and Counter-Terrorism Academy</td>
<td>Israel</td>
</tr>
<tr>
<td>Rand Europe Cambridge Ltd</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Stichting Hogeschool Utrech</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Bridge 129 Spa Safety and Security</td>
<td>Italy</td>
</tr>
<tr>
<td>Compagnie europeenne d’intelligence stratégique SA</td>
<td>France</td>
</tr>
<tr>
<td>Universidade de Coimbra</td>
<td>Portugal</td>
</tr>
<tr>
<td>Fondation pour la recherche stratégique</td>
<td>France</td>
</tr>
<tr>
<td>Universiteit van Amsterdam</td>
<td>The Netherlands</td>
</tr>
</tbody>
</table>
SAPIENT / Supporting fundamental rights, Privacy and Ethics in surveillance Technologies

Project objectives
SAPIENT aims to specify how and when smart surveillance should be used (or not) and its characteristics to be effective and scalable to rapidly adapt to changing situations. It will provide stakeholders with a set of criteria for data protection and integrity that can be used to verify that surveillance systems and the sharing of information respect the privacy of citizens. The project will develop and provide a privacy impact assessment methodology, which is tailor-made for surveillance projects and technology developments and, in so doing, the use of the methodology will provide means for limiting the collection and storage of unnecessary data. It will focus on the necessity and proportionality of data collection needs, in order to avoid undue threats to data protection and privacy. SAPIENT will pave the way towards an approach of surveillance where the respect for the privacy of the citizen will be central.

Description of the work
The SAPIENT project will define and characterize smart surveillance within technological, social, political, legal, and ethical contexts, bridging from current studies of state-of-the-art of surveillance to emerging technologies and related applications expected over the next decade.

The second step will begin the process of active stakeholder engagement within SAPIENT, through convening focus groups with participants representing various views and interests on different applications of smart surveillance.

Then the SAPIENT team will examine existing privacy impact assessment (PIA) methodologies and propose a methodology that is suitable for the assessment of state-of-the-art and emerging surveillance technologies and related applications.

The validation of the suggested PIA is done by three distinct field studies. These cases may focus upon technologies such as RFID, biometrics, or smart CCTV. A “lessons learned” evaluation will be completed at the conclusion of the case study test, and these will be used to revise the PIA methodology, resulting in the Surveillance Privacy Impact Assessment Manual.

Moreover a series of policy meetings will be held over the course of the project to present results of research. At the conclusion of the project, a final conference will be held to present the main findings and recommendations. It is expected to pave the way towards an approach of surveillance where the respect for privacy will be central.

Expected results
The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizen.
Information

Acronym: SAPIENT

Grant Agreement N°: 261698

Total Cost: € 1,539,687

EU Contribution: € 1,248,577

Starting Date: 01/02/2011

Duration: 36 months

Coordinator:

FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN WISSENSCHAFTEN E.V.
Fraunhofer Institute for Systems and Innovation Research
Breslauer Straße 48
76139 Karlsruhe, Germany

Contact:

Michael Friedewald
Tel: +49 (0) 721 6809 146
Fax: +49 (0) 721 6809 315
E-mail: michael.friedewald@isi.fraunhofer.de
Website: www.sapientproject.eu

Partners

NAME
Trilateral Research & Consulting LLP
Centre for Science, Society and Citizenship (CSSC)
University of Lugano, Faculty of Informatics
King’s College London, Department of War Studies
Centre for European Policy Studies (CEPS)

COUNTRY
United Kingdom
Italy
Belgium
Switzerland
United Kingdom
Belgium
SIAM / Security Impact Assessment Measures

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 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 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. Supplemental SIAM will 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 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.

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 for new SMTs is a complex task that demands from 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.
Information

Acronym: SIAM

Grant Agreement N°: 261826

Total Cost: €2,777,309,02

EU Contribution: €2,168,640,00

Starting Date: 01.02.2011

Duration: 36 months

Coordinator:
CENTRE FOR TECHNOLOGY AND SOCIETY, TECHNICAL UNIVERSITY BERLIN
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

Partners

NAME
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
SMART / Scalable Measures for Automated Recognition Technologies

Project objectives

The project’s objectives are to:

- Determine the state of the art and likely future trends of smart surveillance, its proportionality and impact on privacy;
- Identify 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, data exchange, 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 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 risks analysis inherent in 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 a 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 to surveillance in modern European society;
- A toolkit for policy makers based on the findings of this project.
Information

Acronym: SMART

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Central Lancashire, Centre of Law, Information &amp; Converging Technologies (CLICT)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>University of Malta (UoM)</td>
<td>Malta</td>
</tr>
<tr>
<td>University of Ljubljana (UL)</td>
<td>Slovenia</td>
</tr>
<tr>
<td>Laboratorio di Scienze della Cittadinanza (LSC)</td>
<td>Italy</td>
</tr>
<tr>
<td>Babeş-Bolyai University of Cluj-Napoca (BBU)</td>
<td>Romania</td>
</tr>
<tr>
<td>Universitetet i Oslo (UIO)</td>
<td>Norway</td>
</tr>
<tr>
<td>Universidad de Leon (ULE)</td>
<td>Spain</td>
</tr>
<tr>
<td>Law and Internet Foundation (LIF)</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>Masarykova univerzita (MU)</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Edith Cowan University (ECU)</td>
<td>Australia</td>
</tr>
<tr>
<td>Georg-August-Universitaet Goettingen Stiftung Oeffentlichen Rechts (UGOE)</td>
<td>Germany</td>
</tr>
<tr>
<td>Sheffield University (SHEFU)</td>
<td>Germany</td>
</tr>
<tr>
<td>Gottfried Wilhelm Leibniz Universitat Hannover (LUH)</td>
<td>Italy</td>
</tr>
<tr>
<td>CNR National Research Council (CNR)</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Universzita Komenskeho v Bratislave (FMUNIBA)</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Rijksuniversiteit Groningen (RuG)</td>
<td>Austria</td>
</tr>
<tr>
<td>University of Vienna (UNIVIE)</td>
<td>France</td>
</tr>
<tr>
<td>MORPHO (MPH)</td>
<td>International/France</td>
</tr>
<tr>
<td>INTERPOL</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Metropolitan Police Service (MET)</td>
<td></td>
</tr>
</tbody>
</table>
ValueSec / Mastering the Value Function of Security Measures

Project objectives

The objective of the ValueSec project is which would 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 in a security more transparent. The objectives of the projects are:

Objective 1: To survey the field of security economics, 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 recommendation 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 economical 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.

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.
**Information**

<table>
<thead>
<tr>
<th><strong>Acronym:</strong></th>
<th>ValueSec</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Grant Agreement N°:</strong></td>
<td>261742</td>
</tr>
<tr>
<td><strong>Total Cost:</strong></td>
<td>€ 4,473,885.00</td>
</tr>
<tr>
<td><strong>EU Contribution:</strong></td>
<td>€ 3,443,210.10</td>
</tr>
<tr>
<td><strong>Starting Date:</strong></td>
<td>February 1, 2011</td>
</tr>
<tr>
<td><strong>Duration:</strong></td>
<td>36 months</td>
</tr>
</tbody>
</table>

**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/

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTT Technical Research Centre of Finland (VTT)</td>
<td>Finland</td>
</tr>
<tr>
<td>Centre for European Security Strategies (CESS)</td>
<td>Germany</td>
</tr>
<tr>
<td>International Peace Research Institute (PRIIO)</td>
<td>Norway</td>
</tr>
<tr>
<td>University of Stavanger (UIS)</td>
<td>Norway</td>
</tr>
<tr>
<td>ATOS Origin S.A. (Atos)</td>
<td>Spain</td>
</tr>
<tr>
<td>Institute of Innovative Technologies (EMAG)</td>
<td>Poland</td>
</tr>
<tr>
<td>White Cyber Knight (WCK)</td>
<td>Israel</td>
</tr>
<tr>
<td>Policía Local de Valencia (VPD)</td>
<td>Spain</td>
</tr>
</tbody>
</table>
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.

Expected results

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

**Acronym:** CRESCENDO  
**Grant Agreement N°:** 218026  
**Total Cost:** € 499,523  
**EU Contribution:** € 499,523  
**Starting Date:** 07/07/2009  
**Duration:** 24 months

**Coordinator:**  
**CEA LIST**  
Commissariat à l’énergie atomique  
Centre de Saclay- Bât 476  
F91191 Gif-Sur-Yvette Cedex  
France  

---

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

---

## Partners

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

The Project delivers report on usefulness of competitions and also designs competition proposals in the security field for consideration by the EC to choose from and run under the FP7-SEC programme.

With these deliverables the main objectives of the project:

- To help EC to start using competitions as drivers of innovation;
- To open the opportunity to incentivise further technological progress in security field;
- To provide visibility for EU Security Research.

**Description of the work**

The “European Security Challenge” project aims to prepare all necessary background information for the European Commission to be able to make decision about and to start to run competitions in order to encourage disruptive research (unfunded research with a high risk of failure) as these kinds of projects are rarely pursued via normal grants and business processes in universities or enterprises. This approach can help to strengthen the idea of working with European governments to test innovative solutions and to further promote the EC Security Research programme as driver in European security innovation.

The core concept of the project is to research how competitions can stimulate innovation and compare them to other methods, such as grants, venture capital and patents. The project designs complex competition packages including scenarios, rules and marketing plans that, if implemented, will incentivize European innovators to work on high-impact projects order to push existing technical boundaries. These proposed competitions could impact Europe’s security industry by creating new technology knowledge, raising awareness and encouraging new networks that address issues within the EU’s four security missions.

To achieve these aimed results with the competition packages it is vital that the proposals have to include the most interesting and challenging scenarios, right technical and media goals and appropriate incentives.

The consortium consists of complementary experts in media communications (3D Communications – France), technology development (Institute Jozef Stefan – Slovenia) and competition management (Global Security Challenge – UK), necessary for such a highly complex competition design. The participating companies operate in England, Slovenia and France, which gives the team European-wide oversight and capabilities.

**Expected results**

The project aims to collect comprehensive data including expert opinions about incentives of prizes in order to deliver scientific argument on usefulness of competitions. The project also provides complex, executable plans for running security-themed competitions; the submitted competition packages will become property of the European Commission and any future use will be determined by the EC.
Information

Acronym: ESC

Grant Agreement N°: 261566

Total Cost: € 468,279

EU Contribution: € 468,279

Starting Date: 01 March 2011

Duration: 12 months

Coordinator:
Global Security Challenge LLP (GSC)
57 Gloucester Place,
London W1U 8JJ
UK

Contact:
Mr Simon Schneider
Tel: +44 (0) 207 224 0110
Email: schneider@globalsecuritychallenge.com
Website: www.omnicompete.com

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Security Challenge LLP (GSC)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>3D Communications</td>
<td>France</td>
</tr>
<tr>
<td>Institute Jozef Stefan (JSI)</td>
<td>Slovenia</td>
</tr>
</tbody>
</table>
ESCorts / European network for the security of control and real-time systems

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

See: www.escortsproject.eu/
Information

**Acronym:**
ESCoRTS

**Grant Agreement N°:**
218245

**Total Cost:**
€ 1,076,091

**EU Contribution:**
€ 673,603

**Starting Date:**
16/06/2008

**End Date:**
15/12/2010

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

**Contact:**
Luc Van den Berghe
Tel : +32 2 550 09 57
E-mail : luc.vandenberghe@cen.eu
Website : www.escortsproject.eu/

---

**NAME**

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)
COMITÉ EUROPEEN DE NORMALISATION (CEN)
SIEMENS AG (Siemens)
COMMISSION OF THE EUROPEAN COMMUNITIES - DIRECTORATE GENERAL
JOINT RESEARCH CENTRE - JRC (EC-DG JRC)
ABB SCHWEIZ AG (ABB)
Enel Ingegneria e Innovazione SpA (ENEL spa)

**COUNTRY**

France
Italy
Italy
United States
Romania
Italy
Italy
Belgium
Germany
Belgium
Switzerland
Italy
EU-SEC II / Coordinating national research programmes and policies on security at major events in Europe

Project objectives

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

Description of the work

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

Information exchange

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

Strategic activities

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

Joint activities

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

Transnational activities

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

EU-SEC II Manual

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

Expected results

» Harmonization of national research policies.

» Synchronization of national end-users into a coordinated platform to effectively address other stakeholders’ requirements involved in the provision of security at Major Events.

» Elaboration of a common understanding, identification and ways to respond to research needs and priorities among EU-SEC II Partners and EU national authorities thorough the creation of a durable structuring effect of the demand side of the European technology market.

» Elaboration of a strategic research roadmap for relevant EU and national institutions.
Information

**Acronym:** EU-SEC II

**Grant Agreement N°:** 218037

**Total Cost:** € 2,527,000

**EU Contribution:** € 2,527,000

**Starting Date:** 01/07/2008

**Duration:** 36 months

**Coordinator:**

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

**Contact:**
Alberto Pietro Contaretti
Tel: +39 011 6537 111
Fax: +39 011 6313 368
E-mail: contaretti@unicri.it
Website: www.eu-seci.org

Partners

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

Project objectives

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

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

The 5 Areas are:

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

Description of the work

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

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

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

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

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

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

Results

The results of the project are available on the website of the project http://www.mdais.org and the CORDIS website http://cordis.europa.eu/fp7/security.
**Information**

**Acronym:** NMFRDisaster

**Grant Agreement N°:** 218057

**Total Cost:** € 815,079

**EU Contribution:** € 815,079

**Starting Date:** 01/05/2008

**End Date:** 30/06/2009

**Coordinator:**

MAGEN DAVID ADOM
Yigal Alon 60
67062 Tel-Aviv
Israel

**Contact:**

Chaim Rafalowski
Tel: +972-36300292
Fax: +972-3-7396541
E-mail: chaimr@mdais.co.il
Website: http://www.mdais.org

**Partners**

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magen David Adom in Israel</td>
<td>Israel</td>
</tr>
<tr>
<td>SAMUR Proteccion Civil, Ayuntamiento de Madrid</td>
<td>Spain</td>
</tr>
<tr>
<td>AmbulanceZorg Nederland</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Danish Red Cross</td>
<td>Denmark</td>
</tr>
<tr>
<td>Sinergie S.r.l</td>
<td>Italy</td>
</tr>
<tr>
<td>Fundacion Rioja Salud</td>
<td>Spain</td>
</tr>
<tr>
<td>Center for Science, Society and Citizenship</td>
<td>Italy</td>
</tr>
<tr>
<td>Shield Group Inc.</td>
<td>Aruba</td>
</tr>
<tr>
<td>Charles University</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Al-Quds Nutrition and Health Research Institute</td>
<td>Palestinian territory</td>
</tr>
</tbody>
</table>
OPERAMAR / An interoperable approach to European Union maritime security management

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

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

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

- Grasp a better knowledge of Maritime Security users needs and their organizations and define interoperability models and analyse the associated issues, taking into consideration the challenging characteristics of the organizational environment in which they will be implemented,
- Develop common interoperability requirements and translate them into technical requirements, and
- Study the consequences and recommend a relevant strategic research roadmap.

Description of the project
OPERAMAR consisted in the establishment of an EU and Associated Countries network of maritime stakeholders, that identified interoperability challenges, for improving operational coordination.

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

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

OPERAMAR partners presented the project in several workshops, congresses and Maritime Events.

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

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

From the analysis of the present situation, the stakeholders network identified interoperability challenges, for significant improvements on the operational performances. The effectiveness of the methodological results was tested in three scenarios, Mediterranean, Black Sea and Atlantic Ocean (Canary Islands).

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

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

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

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

Results
The results of the project are available on the website of the project www.operamar.eu and the CORDIS website http://cordis.europa.eu/fp7/security.
Information

Acronym: OPERAMAR

Grant Agreement N°: 218045

Total Cost: € 669,132

EU Contribution: € 669,132

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

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMISSION OF THE EUROPEAN COMMUNITIES - DIRECTORATE GENERAL JOINT RESEARCH CENTRE (JRC)</td>
<td>Belgium</td>
</tr>
<tr>
<td>EDISOFT-EMPRESA DE SERVICOS E DESENVELVIMENTO DE SOFTWARE SA* (Edisoft)</td>
<td>Portugal</td>
</tr>
<tr>
<td>INDRA SISTEMAS (INDRA)</td>
<td>Spain</td>
</tr>
<tr>
<td>ISTITUTO AFFARI INTERNAZIONALI. (IAI)</td>
<td>Italy</td>
</tr>
<tr>
<td>Quintec Associates Ltd (QUINTEC)</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>SELEX SISTEMI INTEGRATI SPA (SELEX)</td>
<td>Italy</td>
</tr>
<tr>
<td>STM Savunma Teknolojileri Muhendislik ve Ticaret A.S. (STM)</td>
<td>Turkey</td>
</tr>
<tr>
<td>THALES SYSTEMES AEROPORTES SA (TAS)</td>
<td>France</td>
</tr>
<tr>
<td>THALES UNDERWATER SYSTEMS SAS (THALES)</td>
<td>France</td>
</tr>
<tr>
<td>THE ALLIANCE OF MARITIME REGIONAL INTERESTS IN EUROPE (AMRIE)</td>
<td>Belgium</td>
</tr>
</tbody>
</table>
OSMOSIS / Overcoming security market obstacles for SMEs’ involvement in the technological supply chain

Project objectives

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

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

» Identification of untapped market potentials in the technology security market supply chain;

» Liaison with large organisations to foster the involvement of SMEs in the security technology supply chain, including the involvement in joint R&D activities;

» The creation of a database of qualified SMEs that will create “meta-clusters” where Large Enterprises could identify partners for their engineering and/or R&D projects;

» Full support to SMEs to favour their involvement in the security supply chain;

» Dissemination and networking events to create a collaborative environment among key stakeholders.

Description of the work

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

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

1. Actions towards Key Stakeholders operating in the Security Technology supply chain, to stimulate and support such organisations in involving SMEs in engineering projects as well as in research projects, and to gather relevant information about untapped market potentials;

2. Actions towards SMEs, to create awareness on technology supply chain opportunities and provide specific services that help SMEs to enter the overall market supply chain;

3. Actions aimed at setting up means to facilitate communication and networking among key stakeholders and organizations.

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

» the competitiveness improvement of the ecosystem of the large organization,

» the capability of benefit from innovations and technological expertise offered by SMEs, and

» achievement of corporate social responsibility objectives.

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

» Access to a database of SMEs, classified following a specific taxonomy and including only relevant SMEs operating in security related engineering and/or research activities;

» A list of security research opportunities that could be exploited by SMEs to collaborate with large organizations;

» Information on security-related grants;

» Interactive communication tools to allow the communication of the identified opportunities and the transfer of specific knowledge to SMEs of the different meta-clusters.

Expected results

» More than 50 key stakeholders involved in the action;

» More than 250 pre-qualified SMEs will be included in the database, and their scientific, technology and engineering skills assessed, as well as technology development plans;

» Information campaign reaching more than 5,000 SMEs and other organisations;

» Support the start up of 20 collaborations among organisations not previously involved in the security technology supply chain with key stakeholders.
Information

**Acronym:**
OSMOSIS

**Grant Agreement N°:**
242416

**Total Cost:**
€ 725,432.60

**EU Contribution:**
€ 580,889

**Starting Date:**
01/04/2010

**Duration:**
24 months

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

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

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIAOTECH S.r.l.</td>
<td>Italy</td>
</tr>
<tr>
<td>SESM Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l.</td>
<td>Italy</td>
</tr>
<tr>
<td>GMVIS Skysoft, S.A.</td>
<td>Portugal</td>
</tr>
<tr>
<td>Consorzio Interuniversitario Nazionale per l’Informatica</td>
<td>Italy</td>
</tr>
<tr>
<td>Technische Universitat Munchen (TUM)</td>
<td>Germany</td>
</tr>
<tr>
<td>INNOSTART Nemzeti Uzleti es Innovacios Kozpont Alapitvany</td>
<td>Hungary</td>
</tr>
<tr>
<td>Honeywell, spol. s r.o.</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Instituto Nacional de Tecnica Aeroespacial</td>
<td>Spain</td>
</tr>
<tr>
<td>Fundación madrimasd para el Conocimiento</td>
<td>Spain</td>
</tr>
<tr>
<td>ELSAG Datamat S.p.a.</td>
<td>Italy</td>
</tr>
<tr>
<td>PNO Consultants S.A.S.</td>
<td>France</td>
</tr>
</tbody>
</table>
SecureCHAINS / Integration of security technology supply chains and identification of weaknesses and untapped potential

Project objectives

The SecureCHAINS project has as a main mission to contribute to a more competitive Security Technology Supply Chains (STSC). The project will cooperate with the industry to gain a better understanding of the nature and structure of the STSC from prime contractors to subcontractors coming from the various tiers of the supply chains.

The SecureCHAINS project will have the following six main objectives to:

» identify supply chains and stakeholders;

» detect untapped potential that can be integrated in the European STSC;

» engage innovative low tier suppliers in the STSC;

» contribute to the building of R&D competences in STSC;

» develop awareness building activities in Security related RTD topics; and

» promote and facilitate a communication platform/website and open dialogue in the fields related to Security Technology management, regulation, policy and forecasting.

Description of the work

The SecureCHAINS project will be carried out along the following four main axes of activities:

» To identify opportunities and weak spots in the supply chains. The technology tree drawn up for a research project will involve areas of technology of different degrees of maturity. We will apply the concept of ‘technology readiness levels’ to determine technical maturity. Immature technology so identified would be considered as a weak spot and the SecureCHAINS project would advise on how this might be strengthened;

» To involve the best intellectual and technological capabilities available throughout Europe in the security technology supply chains;

» To help organisations (SMEs, RTOs, Large Firms, etc.) to understand security related targets, mechanisms and opportunities;

» To facilitate the organisations access to the main stakeholders and integrators, while protecting their intellectual property.

The SecureCHAINS project is structured into 5 workpackages (WP):

» WP1 Security Technology Supply Chains framework setting;

» WP2 Analyses of the Supply Chains;

» WP3 Increasing SME engagement in the STSC;

» WP4 Technology Search & Transfer;

» WP5 Dissemination and Future exploitation results and activities.

Expected results

The main results are to:

» raise awareness about EU RTD funding programmes and promoting co-operation, exchange of information and networking among them;

» identify weak spots in the security supply chains;

» develop 5 technology trees;

» identify the problems that inhibit the participation of SMEs in RTD activities;

» interview and perform on-site visits to a minimum of 100 SMEs and RTOs;

» organise a minimum of 4 communication exchange fora at European Security related events; and

» produce 10 new RTD project proposals, involving a minimum 20 SMEs.
Information

- **Acronym:** SecureCHAINS
- **Grant Agreement N°:** 242417
- **Total Cost:** €1,014,344.37
- **EU Contribution:** €820,032
- **Starting Date:** 01/05/2010
- **Duration:** 24 months

Coordinator: INOVAMAIS SA

Contact: Alexandre Almeida
E-mail: alexandre.almeida@inovamais.pt
Website: www.securechains.eu

Partners

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td>INOVAMAIS - SERVICOS DE CONSULTADORIA EM INOVACAO TECNOLOGICA S.A.</td>
<td>Portugal</td>
</tr>
<tr>
<td>FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V</td>
<td>Germany</td>
</tr>
<tr>
<td>Deutsche Post World Net Market Research and Innovation GmbH (DHL Innovation Center)</td>
<td>Germany</td>
</tr>
<tr>
<td>INNOVA SPA</td>
<td>Italy</td>
</tr>
<tr>
<td>SOLLERTA Ltd</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>FUNDACION ROBOTIKER</td>
<td>Spain</td>
</tr>
<tr>
<td>Mr. Juergen K. von der Lippe and Dr. Jean Cornier</td>
<td>Germany</td>
</tr>
<tr>
<td>UNIVERSITATEA DIN CRAIOVA</td>
<td>Roumania</td>
</tr>
<tr>
<td>ALMA CONSULTING GROUP SAS</td>
<td>France</td>
</tr>
<tr>
<td>TECHNICAL SUPPORT FOR EUROPEAN ORGANISATIONS SPRL</td>
<td>Belgium</td>
</tr>
<tr>
<td>SOUTHEASTERN EUROPE TELECOMMUNICATIONS &amp; INFORMATICS RESEARCH INSTITUTE</td>
<td>Greece</td>
</tr>
</tbody>
</table>
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 fulfill in order to deliver a high level of service.

Also, coordination will be initiated in order to raise the level of knowledge of NCPs. This will be obtained by making common guides and setting up a website where all the deliverables will be made available.

Increase NCP knowledge and awareness of the European Security landscape. In order to deliver advices in their respective country, NCPs must have a minimum understanding of the European security landscape. Therefore, a mapping of the Security research programmes launched in Member States will be made. In addition, a mapping of competencies will be initiated. This latter task will aim at the identification of support structures such as government agencies, professional associations, end-users associations, SMEs associations, clusters involved in Security Research across Europe.

Coordination to ease transnational cooperation and training. The EU community potentially interested in Security Research faces a high level of fragmentation. Therefore, participants are confronted with difficulties finding other potential partners with whom they might collaborate. Hence, it is extremely important that the NCPs network delivers a high level service for the partner searches.

SEREN will initiate coordination in this field by agreeing on standardised partner search templates. In addition one training session focussed on the evaluation will be organised.

This shall enable an increase of the average advice quality delivered by the network and further optimize its services to the Security Research community.

Security research policies. SEREN will produce synthesis papers on key policies issues related to Security research in order to raise awareness on the contextual framework surrounding ESRP.

Results

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

© Andres Rodriguez - Fotolia.com
Information

Acronym:
SEREN

Grant Agreement N°:
217937

Total Cost:
€ 743,597

EU Contribution:
€ 557,692

Starting Date:
01/02/2008

End Date:
31/07/2009

Coordinator:

COMMISSARIAT À L’ENERGIE ATOMIQUE
European Affairs Directorate
91191 Gif-sur-Yvette
France

Contact:
Frédéric Laurent
Tel: +33 1 64 50 25 22
Fax: +33 1 64 50 11 57
E-mail: pcn_securite@cea.fr
Website: www.seren-project.eu/

Partners

NAME
CEA
Tarptautiniu mokslo ir technologijų pletros programų agentūra
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
Norwegian Information Council
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
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 výskumu a vývoja

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
Project objectives

The main objective of this project is to continue promoting and enhancing trans-national cooperation among Security National Contact Points (both at the level of 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 an intensive trans-national cooperation.

WP 2 – Joint Brokerage Events aims at improving the quality of the cooperation between security research stakeholders (researchers, large companies, SMEs, end-users) by providing the necessary support to ease the process of finding appropriate partners for building successful consortia. Trans-national events shall be organised to the benefit of cross-border audiences.

WP 3 – Mapping of security research competencies focus on the identification of Security Research Competencies in Europe, to increase the visibility of security related research in Europe and to optimize the networking between research facilities, universities, public authorities, end users and suppliers of security solutions and operators of critical infrastructures.

WP 4 – Partner Search is dedicated to promote transnational cooperation by facilitating the access of potential participants to future Security calls.

WP 5 - Monitoring of Security research area aims at providing to both NCPs and stakeholders an improved flow of security research area information. An in-depth mapping of security research systems and programmes is foreseen.

WP 6 – Communication and dissemination has as the objective to oversee and organize all aspects which are related to communication and dissemination of the project results and activities. A scientific approach of communication and dissemination will be applied for this project by stimulating and strengthening the relationship between persons and problems. Making project achievements and activities widely accessible and easily exploitable by project customers will be a challenge for this WP.

Expected results

Results from Security 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 effectiveness of third countries organization participation alongside European organizations.

• Strengthen the competitiveness of the European R&D in the Security theme.
Acronym: SEREN2

Grant Agreement N°: 261814

Total Cost: € 1,801,696.23

EU Contribution: € 1,499,546.21

Starting Date: —

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

NAME

Romanian Space Agency (ROSA) Romania
Foundation for Research & Technology – HELLAS (FORTH) Greece
Agenzia per la Promozione della Ricerca Europea (APRE) Italy
Österreichische Forschungsförderungsgesellschaft mbH (FFG) Austria
Euresearch Head Office Berne (EURESEARCH) Switzerland
Commissariat à l’Energie Atomique (CEA) France
Mokslo Inovacijų ir Technologijų Agentūraa (MITA) Lithuania
SIHTASUTUS ARCHIMEDES (Archimedes) Estonia
Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk (IPPT PAN) Poland
MATIMOP - Israel Industry Center for Research & Development (MATIMOP-IPERD) Israel
Norges forskningsråd – Research Council of Norway (RCN) Norway
The Scientific and Technological Research Council of Turkey (Tubitak) Turkey
Dienst voor Wetenschappelijke en Technische Informatie / Service d’Information scientifique et technique (STIS) Belgium
Centro para el Desarrollo Tecnológico Industrial (CDTI) Spain
Technologické centrum Akademie věd České republiky (The Technology Centre of the Academy of Science - TC AS CR) Czech Republic
Research Promotion Foundation (RPF) Cyprus
Totalförsvarets Forskningsinstitut – Swedish Defence Research Agency (FOI) Sweden
Council for Scientific and Industrial Research (CSIR) South Africa
Riga Technical University (RTU) Latvia
Centre for National Security and Defense Research (CNSDR) Bulgaria
Malta Council for Science and Technology (MCST) Malta
Zilinska Univerzita v Ziline (UNIZA) Slovakia
Finnish Funding Agency for Technology and Innovation (TEKES) Finland
Hrvatski institut za tehnologiju/ Croatian Institute of Technology / Odjel za međunarodnu suradnju/ International Cooperation Unit (HIT) Croatia
Fundacao para a Ciencia e Tecnologia (FCT) Portugal
National Institute of Aerospace Technology of Spain (INTA) Spain

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
STRAW / Security technology active watch

Project objectives

Europe is confronted with extremely diverse threats backed by unseen command structures and business-like financing mechanisms. Various security agencies concur that information is the key to defeating the enemy. This new environment has not only created a greater need for information but also a greater need to share and effectively control access to that information. This is the single greatest challenge European Security is facing today. STRAW is a Coordination and Support Action under the Security Research Theme that aims at providing a European Service of Technology Watch (TW) on Security Technologies.

The mission of STRAW is not only advising potential end-users (public authorities, EU security research community and public at large) about the fundamental technologies but also bring together the defense and security research industry for developing new civil applications.

A main output will be a web-based IT system with a TW list and interface for entering data on user requirements.

Description of the work

Several key milestones are specified to achieve this objective:

- Network and panel of experts constitution: The Consortium will identify the foremost representatives of the Security Sector mainly in Europe. Some of them will be invited to participate in a panel of experts to validate the results of the project. The STRAW network will be growing during the whole project.
- Information Collection: A main task will be the collection of relevant information related to security technologies, stakeholders and initiatives. Members of the network are requested to insert in STRAW any documentation that they consider to be interesting for analysis in STRAW website.
- Information Analysis: In collaboration with the panel of experts, partners will analyze the collected information by means of TW tools in order to present clear snapshot of the relevant security threats and opportunities existing on security.
- Wikibook construction: A wikibook will be developed to present the results of STRAW. The interactive element of the Wikibook will ensure the relevance of the project’s results beyond its duration.
- Delivery of information: The project’s main results will be delivered to the potential users of the information primarily through the STRAW web page and workshops.

Results

For more information on results, please visit the project’s website: www.straw-project.eu and the CORDIS website: http://cordis.europa.eu/fp7/security.
Information

**Acronym:** STRAW

**Grant Agreement N°:** 218132

**Total Cost:** € 1,341,933

**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
Website : www.straw-project.eu

Partners

**NAME**
Atos Origin SAE
Aerospace and Defence Industries Association
Thales Services
Siftelsen SINTEF
Fraunhofer FHG
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
Belgium
Acknowledgement
Investing into security research for the benefits of European citizens