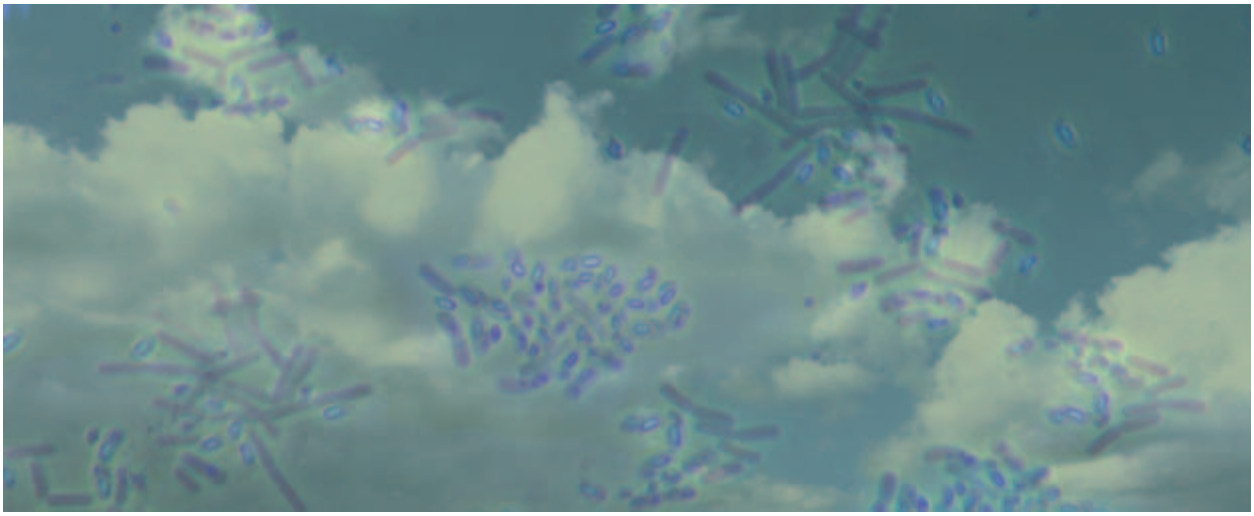
Preparatory Action for Security Research

(PASR 2006)

AEROBACTICS ASSESSMENT OF THE QUANTITY, IDENTITY, VIABILITY, ORIGIN AND DISPERSION OF AIRBORNE MICRO-ORGANISMS FOR APPLICATION IN CRISIS MANAGEMENT TOOLS



Sensor systems for bioterror detection require quantitative input about the natural background of micro-organisms and environmental pathogenic traits, in order to distinguish natural occurrences from real attacks. However, knowledge of numbers, species, viability and pathogenicity of airborne micro-organisms is extremely scarce, and models to predict background fluctuations are inadequate. The proposed project is designed to close these gaps of knowledge.

For biological crisis management, agencies rely on predictive microbial dispersion models. However, existing models are based on inadequate assumptions and parameters. Therefore, the proposed project is also designed to verify model assumptions and determine model parameters.

Two models will be developed and tested, one for background levels and long-range dispersion, and one for the aerial dispersion from an unwanted release.

Data will be gathered by sampling and analysing representative sections of the atmosphere, as well as soils and plants. Both natural events and intentional releases of micro-organisms will be utilised experimentally.

Improved modelling tools will be implemented for use in crisis management.

The **AEROBACTICS** project intends

- to quantify the natural background of micro-organisms in air using a combination of measurements performed from small aircrafts and towers and an atmospheric dispersion model developed to describe the spatial and temporal distribution of viable micro-organisms,
- to analyse the measured micro-organisms with respect to species composition, viability and origin,
- to communicate such results to consortia that are involved in sensor development,
- to develop a predictive model tool for short and regional range aerial dispersion of micro-organisms from single sources, including micrometeorological parameters relevant for the viability of micro-organisms, and
- to communicate all results within the EU terror prevention networks for fulfilling agencies' needs of knowledge and predictive tools as quickly as possible.

For further information please visit http://AeroBactics.dmu.dk

G.A. SEC6-PR-214400
Total Cost : € 1,564,276
EU Contribution : € 951,923
Starting Date : 1/1/2007
Duration : 24 months

Coordinator:
National Environmental Research Institute
Roskilde, DK

Contact:
Ulrich Karlson
Tel : + 45-46 30 13 87
Fax : + 45-46 30 11 14
E-mail : uka@dmu.dk
http://AeroBactics.dmu.dk

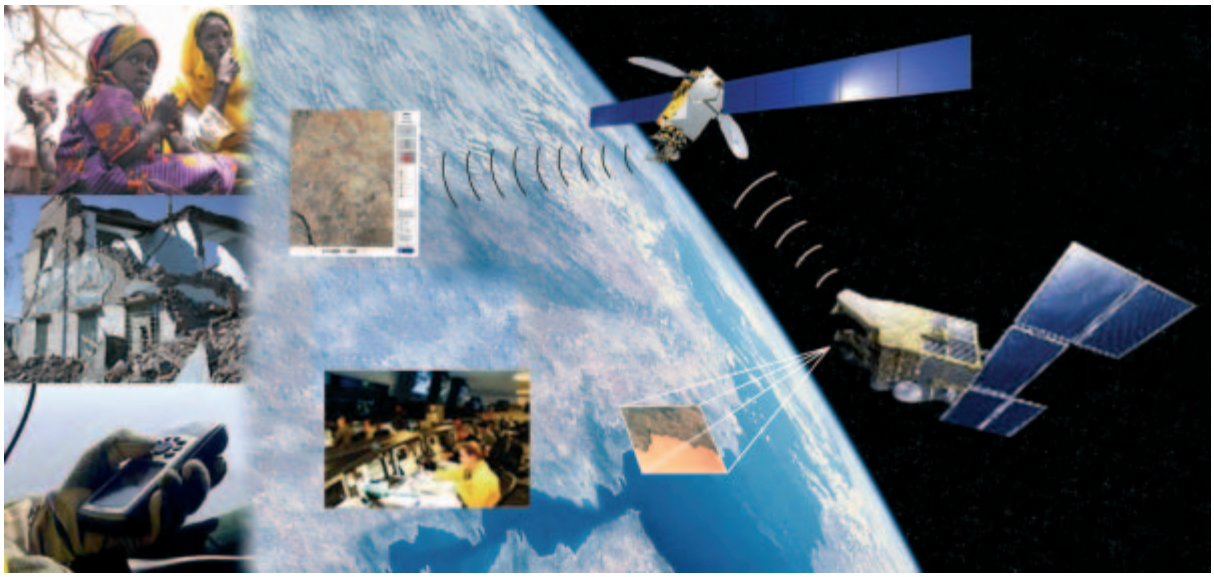
Partners:

University of Kalmar, Department of Biology and Environmental Science	**SE**
University of Bergen, Department of Biology	**NO**
Statens Serum Institut, National Centre for Biological Defence	**DK**

Preparatory Action for Security Research

(PASR 2004)

ASTRO+ ADVANCED SPACE TECHNOLOGIES TO SUPPORT SECURITY OPERATIONS



The objectives

of **ASTRO+** are to study and illustrate how space capabilities - Earth Observation and Reconnaissance, Navigation, Telecommunication and their integration and implementation into services and infrastructures:

- can contribute in the short and long term to the equipment of Europe in security facilities supporting in particular the improvement of foreign operations,
- can support the definition and elaboration of the European Research Security Programme by proposing an R&T innovation roadmap for space.

Main results

- Show the benefits of space technologies through the demonstration of precursor services for joint operations abroad
- Work with users of European security operations (peacekeeping forces, civil security forces, NGOs) in order to increase the value of space capabilities
- Answer to the implementation of a European security strategy by proposing new operational services available in short term using space and by proposing a medium-term R&T action plan to exploit emerging mission concepts
- Set up networking mechanisms between space sector, research, users and stakeholders to create a multidisciplinary approach to address space services for security and to create a European framework for a “Space and Security charter”.

Description of the work

The duration of **ASTRO+** was 15 months, the first 8 months dedicated to transverse analysis and definitions with the end users, the 7 last months dedicated to demonstration of missions, feedbacks analysis and R&T conclusion.

The activities of **ASTRO+** have been broken down into 7 work packages series, defined and validated in close cooperation with the users and space stakeholders.

State of the art assessment – Mission scenarios – Service architecture evolution

Refinement of needs evolution with the end user programme and characterisation of potential solutions at short to long term.

Performance of R&T analysis and developments

Analysis of space technologies per segment (EO, NAV, COMM and their integration, dual use) to develop and propose for user validation new space services and infrastructures to support the mission concepts elaborated.

Demonstration of improved space-based security applications

To achieve the evaluation of added value brought by integrating the three space technologies together an exercise was run in Poland begin February 2006 to represent operations abroad through a scenario showing:

- a situation centre installed in Toulouse integrating Imagery intelligence facilities, civil and secured communications, tracking services, and communication with a distant theatre.
- an operation centre in charge of regular rehearsals for crisis management operations abroad of European forces, integrating secured mobile communication and tracking for vehicles and forces, local imagery facilities.

G.A. SEC4-PR-009600
Total Cost : € 2,946,866
EU Contribution : € 2,200,000
Starting Date : 1/1/2005
Duration : 15 months

Coordinator:
EADS Astrium SAS Ground Systems,
Applications and Services
France

Contact:
Bruno Vatan
Tel : +33 (0)5 62 19 69 48
Fax : +33 (0)5 62 19 50 74
E-mail : bruno.vatan@astrium.eads.net

Partners:

EADS Astrium Limited	UK
EADS Astrium GmbH	DE
Alcatel Space	FR
Alenia Spazio	IT
Telespazio	IT
Centre National d'Etudes Spatiales	FR
Deutsches Zentrum für Luft- und Raumfahrt	DE
Alcatel ETCA	BE
Ecole Royale Militaire de Belgique	BE
Fondation pour la Recherche stratégique	FR
Istituto Affari Internazionali	IT
Indra Espacio	ES
Landmäteriet Metria	SE
Infoterra Limited	UK
Nottingham Scientific Limited	UK
Space Research Centre Polish Academy of Science	PL
QinetiQ	UK
Royal United Services Institute for Defence & Security Studies	UK
SkySoft Portugal	PT
European Union Satellite Centre	ES
Infoterra GmbH	DE

Preparatory Action for Security Research

(PASR 2006)

BIO3R BIOTERRORISM RESILIENCE, RESEARCH, REACTION – SUPPORTING ACTIVITY PROMOTING CO-OPERATION TO ASSESS THE BIO THREAT AND ORGANISE A COLLECTIVE AND COMPREHENSIVE RESPONSE FOR EU SOCIETY AND CITIZENS' BIOSECURITY

Since 2001, the EU has adopted various measures to strengthen the Member States "solidarity", which implies more assistance and collaboration. **BIO3R** seeks to contribute to the improvement of the European preparedness in the field of bioterrorism and to a better comprehension of citizens and professionals regarding this issue and the need to strengthen the prevention and response measures.

BIO3R aims at tackling three key words for a global and comprehensive policy:

- RESEARCH : an evaluation of the state of the art, in relation with the risk assessment and the identification of operational requirements, will help to select priorities for research;
- REACTION : one issue is the reinforcement of crisis-management policies, through an improvement of the networking and a better integration of public and law strategies at European, national and local levels;
- RESILIENCE: the objective is to make EU societies stronger and more resistant to aggression by reinforcing the awareness and the preparation of the EU citizens regarding the biothreat, through and reliable information, education and training, and thus by acting on their perception.

The involvement of policy users and operational actors from various professional backgrounds, at different levels, is deemed to be an indispensable requirement for its success.

1. Identification of operational requirements

BIO3R will rely on the analysis of a few realistic scenarios, leading to a threat assessment and the identification of operational requirements. It will be completed by an evaluation of the epidemiological modelling capacities in relation with the improvement of bioterrorism preparedness and response.

2. Countermeasures

Assessment of the available and promising means and countermeasures related to the mitigation of the effects of a biological attack, as well as, if relevant, identification of potential improvements.

This part of **BIO3R** will address the following issues:

- techniques and tecnologies in the fields of detection, identification, protection and decontamination ;
- available / existing prophylactic and curative therapeutic countermeasures.

3. Ethical and legal issues

Identification of the major ethical and legal issues which could arise from the development and the implementation of measures dedicated to the prevention or the response.

4. Resilience

Contribution to the improvement of the prevention, resilience and mitigation of threat

A study of crisis management issues and a cross evaluation of public health policies will be carried out, and the issue of communication and coordination between the actors will be looked into. **BIO3R** will also contribute to the education and training of hospital professionals and first responders through the development of a training kit, as well as to the improvement of the comprehension and awareness of the European citizens thanks to a web portal and a model of public handbook.

G.A. SEC6-SA-204300
Total Cost : € 642,067
EU Contribution : € 481,550
Starting Date : 01/02/2007
Duration : 18 months

Coordinator:
Fondation pour la Recherche Stratégique
France

Contact:
Jean-François Daguzan
Tel : + 33 1 43 13 77 98
Fax : + 33 1 43 13 77 52
E-mail : jf.daguzan@frstrategie.org

Partners:

Bertin	FR
Centre d'Études du Bouchet	FR
Centre National d'Études Spatiales	FR
Eau de Paris	FR
FOI, Defence Analysis	SE
Groupe Hospitalier Pitié Salpêtrière	FR
Industrieanlagen-Betriebsgesellschaft mbH	DE
Istituto Affari Internazionali	IT
Multitel	BE
Nomisma, Societa di Studi Economici, S.p.A.	IT
Robert Koch Institut	DE
Sagem Défense Sécurité	FR
The Netherlands Organisation for Applied Scientific Research	NL
Université Catholique de Louvain	BE
Université Henri Poincaré Nancy 1	FR
Universitätsklinikum Bonn	DE
Université Paris 7 Denis Diderot	FR
University of Reading	GB
Military Institute of Hygiene & Epidemiology	PL

Preparatory Action for Security Research

(PASR 2006)

BIOTESTING EUROPE

TOWARDS A NETWORK FOR TESTING AND CERTIFICATION OF BIOMETRIC COMPONENTS AND SYSTEMS

BioTesting Europe prepares the setting up of a European network for testing and certification of biometric components and systems. To understand the need for such a network the project takes the political and cultural developments of the last few years into consideration.

According to the EC policies, as has been stated in the The Hague program, a coherent approach and harmonised solutions on biometric identifiers and data are necessary in the fight against illegal migration and to improve the security of the European citizens.

In order to establish European interoperability within the large scale cross national identity management systems, more specific requirements for designing testing and evaluation schemes are needed. An integrated and European approach is the absolute success factor in achieving these goals. That means simultaneous actions are needed that facilitate alignment between all levels of stakeholders that are involved: end users, testing laboratories, accreditation organizations and industry.

Although much work has been done in the area of independent testing of biometric systems, there are still many open issues to be resolved due to a fragmentation of efforts and a lack of input by end users. To improve this situation, this project aims at setting up a framework for a European network of testing laboratories for performance and interoperability testing and security evaluation of biometric systems.

Objectives of the project

1. Outlining the need for testing and certification on the end user level and defining the 'business case'
2. Making an up-to-date inventory of:
   - What needs to be tested based on end user requirements
   - Most relevant existing testing schemes
   - Existing competencies at European independent testing laboratories in the area of biometric per¬form¬ance, interoperability, and security testing
   - Existing work on standardization and testing (within and outside EU)
3. Based on the outcome of the inventory:
   - Mapping of the user requirements on the existing competencies
   - Performing a gap analysis to determine what existing competencies can be used and what needs to be developed
4. The final outcome of the project will be:
   - A European Biometric Testing and Certification Roadmap, including research targets and a business model
   - Work plan and coordinated actions for the further development of the European biometrics testing and certification network: BioTesting Europe

G.A. SEC6-SA-214900
Total Cost : € 358,000
EU Contribution : € 268,000
Starting Date : early 2007
Duration : 9 months

Coordinator:
European Biometrics Forum

Contact:
Max Snijder
Tel : +31624 603809
Fax : +35314885810
E-mail : max.snijder@eubiometricsforum.com

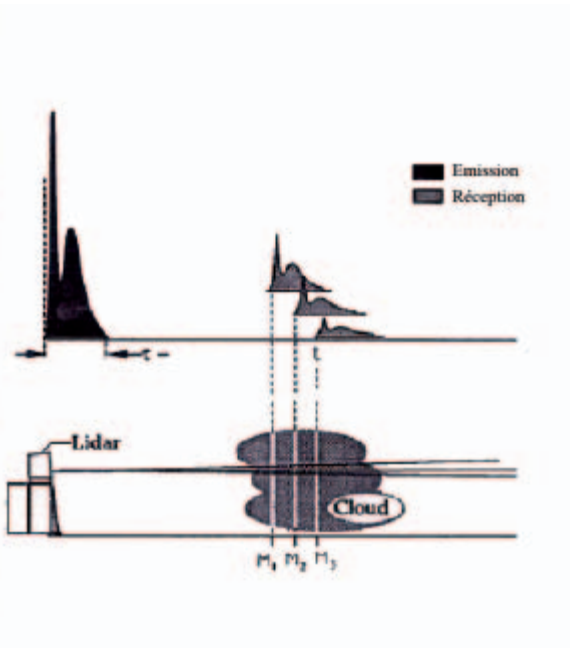
Partners:
National Physics Laboratory **UK**
Fraunhofer-Institut für Graphische Verarberaitung (IGD) **DE**
European Commission / Joint Research Centre – IPSC **BE**

Preparatory Action for Security Research

(PASR 2006)

BODE

BIOLOGICAL OPTICAL DETECTION EXPERIMENT



Biological weapons have been a threat for many years but recent advances in biotechnology make the problem potentially more serious. Hence the escalating dangers must be controlled and detection and alarm systems developed.

Biological detection technologies are in a much less mature stage of development than chemical detectors so the **BODE** project addresses the necessity of developing a reliable, accurate, stand off detection tool for biological particles.

The objectives of the **BODE** project are:

- to federate European participants in biological detection research,
- to identify the functional and operational requirements of a detection apparatus,
- to analyse the state of the art,
- to propose the specifications for a biological detection demonstrator device,
- to design, manufacture and integrate a demonstrator element,
- to proceed to specific experimental investigations and demonstration.

Biological warfare agents are increasingly viewed by potential aggressors as cost effective offensive weapons, particularly when their potential enemies have a superior conventional capability. Limited financing and training are needed to establish a biological weapons program and biological weapon production has low visibility. Biological weapons can be dispatched through relatively easy means of delivery. Small quantities of lethal biological agents can be easily obtained, concealed, transported, and released in susceptible populations. Minute amounts of some biological weapons can cause mass casualties. Distinguishing the biological agents from the myriad of similar naturally occurring micro organisms in the environment makes this task especially daunting.

Hence the **BODE** project addresses those issues and the understanding of the necessity of developing a reliable, accurate, detection tool for biological particles. The objectives of the project are to federate various European participants in stand-off biological detection. These include companies, industrials and governmental researchers, users and first responders. It will generate specific research, development and analysis, leading in a timely manner to a demonstration of an experimental biological detection device through:

- Identification of the functional and operational requirements
- An analysis of the state of the art and a proposed specification for a biological detection demonstrator device
- Demonstrator elements manufacturing and integration
- Specific experimental investigations and demonstrations

The **BODE** project focus will be on Dry Detection Technologies – optical stand-off using technologies LIDAR, with an intelligent warning algorithm. It will also focus on, improving methodologies for analyzing physical aerosol signatures, miniaturizing and ruggedizing detectors, and forecasting the exploitation power of these technologies when integrated in networked systems.

G.A. SEC6-PR-209400
Total Cost : € 2,494,355
EU Contribution : € 1,815,614
Starting Date : 01/01/2007
Duration : 27 months

Coordinator:
CILAS Compagnie Industrielle des Lasers
France

Contact:
Eneka IDIART BARSOUM
Tel : 33-2-38-64-40-49
Fax : 33-2-38-64-40-75
E-mail : Idiart@cilas.com

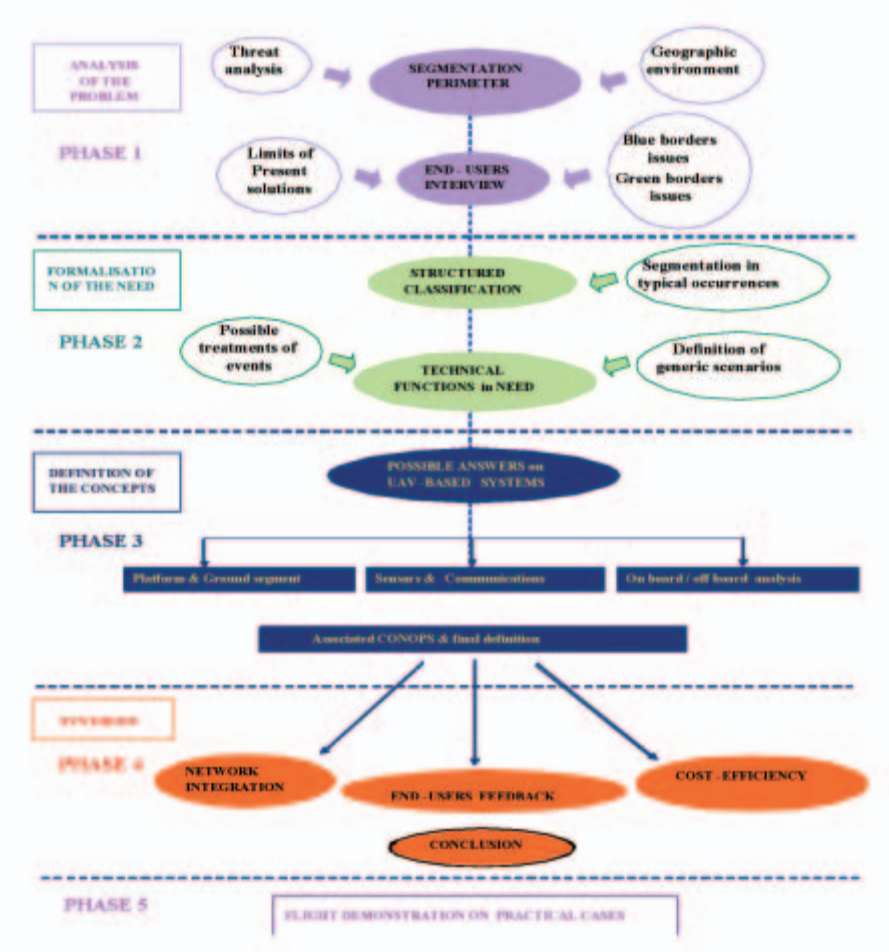
Partners:

Biral	**UK**
Deutsche Zentrum für Luft und Raumfahrt (DLR)	**DE**
Galileo Avionica	**IT**
Délégation Générale pour l'Armement (DGA/CEB)	**FR**
Swedish Defence Research Agency (FOI)	**SE**
EADS CRC	**FR**
AS Laser Diagnostic Instruments (LDI)	**EE**

Preparatory Action for Security Research

(PASR 2005)

BORDER SURVEILLANCE - UAV



The **BS-UAV** supporting activity is to present a structured analysis of the potential contribution of Unmanned Aerial Vehicles (UAV) to peacetime security on European borders.

The study will be conducted in five steps:

1. the understanding of problems posed to people in charge of security on the Continent's various types of borders;
2. the synthesis of these expressions of need under the form of generic situations;
3. the requirements on UAV systems able to handle these situations;
4. the definition of realistic UAV-based systems that would fulfil most of those requirements;
5. the presentation of those results to End-Users, coupled with a live demonstration of a small UAV conducting a typical surveillance mission, in order to illustrate the potential of those systems.

The general approach will be to answer different questions:

- What is the need in terms of Border Surveillance?
- What could be done to try to fulfil this need, using UAV based solutions?
- What technologies are involved in the systems composing those solutions?
- In what areas new technologies could be of help to build those systems?

In order to answer those questions, the work will be divided in five phases:

- **PHASE 1** will deal with an ANALYSIS of the PROBLEM, in terms of threats identification and classification, and environment modelling and characterisation.
- **PHASE 2** will address the FORMALISATION of the NEED, to form a structured classification of the situations, and of the technical need to address those situations.
- **PHASE 3** will be the DEFINITION of the CONCEPTS able to answer the identified need based on inputs from Phases 1 and 2. The concepts will be UAV-based systems.
- **PHASE 4** will address potential technical and economical constraints that would be linked to the proposed solutions. Propositions for security improvements on EU borders will be formalised in this phase.
- **PHASE 5** will propose a FLIGHT DEMONSTRATION on various cases defined during the study, in order to illustrate the practical gain that could be obtained, in terms of security, through use of UAVs.

The outcome of the study will be:

- a global synthesis of border control problems. Similarities and differences between regions, national specificities and local analysis of threats,
- development of original and innovative concepts of use for UAV based surveillance systems. The study will include :
  - an analysis of the required technologies involved in the proposed systems,
  - an analysis of the degree of data analysis and decision-taking functions and related processing technologies needed to conduct the required missions,
  - an overview of the challenge of integrating UAV based systems into the existing European network.
- feedback from End-Users on the use of UAVs, and an illustration of the validity of the concept through a practical example.

G.A. SEC5-SA-105800
Total Cost : € 578,601
EU Contribution : € 433,950
Starting Date : 1/9/2006
Duration : 15 months

Coordinator:
Dassault Aviation DGT/DPR
France

Contact:
Raymond FRISBY
Tel : +33 1 47 11 40 69
Fax : +33 1 47 11 32 19
E-mail : raymond.frisby@dassault-aviation.fr

Partners:

Alenia Aeronautica	IT
Eurosense	BE
Nationaal Lucht- en Ruimtevaartlaboratorium	NL
Rolls-Royce	UK
SAAB	SE
SENER Ingeniería y Sistemas, S.A	ES
Security Technology Competence Centre	SL
THALES Communications S.A.	FR
Flying Robots	FR

Preparatory Action for Security Research

(PASR 2006)

CITRINE

COMMON INTELLIGENCE AND TRACEABILITY FOR RESCUE AND IDENTIFICATION OPERATIONS

CITRINE aims at developing a first version of an integrated set of shared information management tools and models to facilitate the efficient integration of diverse emergency and management services for humanitarian operations and rescue tasks in support of the external policies of the EU with an emphasis on security aspects and attention to organisational structures, inter-organisational co-ordination and communication, distributed architectures and human factors.

CITRINE will support the crisis management process in mitigation, damage assessment and preliminary recovery phase, focusing on humanitarian activities provided by NGOs and Health Services.

CITRINE will encompass:

- At coordination level:
  - Tools for gathering and merging any type of available information coming from European and National agencies, organisations and citizens
  - Decision aid tools to support logistic operations and work planning.
  - Information sharing tools.
- At tactical level:
  - Relevant tools to produce a comprehensive humanitarian oriented, real time situation

Decision aid tools to dispatch casualties and evacuated populations and optimise the use of rescue means.

Nowadays, humanitarian action is impaired by delay due to poor situation assessment and by organisation problems due to lack of coordination between all involved agencies (NGO, Health Services, Civil Protection, Local Authorities…). New threats introduced by terrorist groups increase the complexity to anticipate appropriate response plans due to unpredictable modus operandi. When assessing the situation each agency addresses partially the situation with regards to its domain of expertise. No overall situation assessment is performed which often results in misinterpretation and inadequate engagement and action.

Expected results: While focusing on the humanitarian mission domain in the case of a major CBNRE disaster, **CITRINE** will integrate state of the art building blocks into a consistent system to develop a first version of both a coordination centre and a command post which will be demonstrated in the trials.

CITRINE project will focus on the following items:

1. Development of the first version of a scalable, modular information system for situation assessment. The tool will:
   a) Collect, analyse, store and display toxicity data for early warning,
   b) Provide a coherent composite picture of the current situation along with prediction of the situation (estimated further risk) to assist through a DSS the decision makers in situation understanding.
2. Reporting on specific points of coordinating operational emergency team to an incident involving toxic agents, both for humanitarian organisations and public health authorities, such as health facilities needed, stockpiling issues, detection instruments needed, strategic evacuation, rescue camps management, etc. In particular, **CITRINE** should allow to test and rank different response actions, including, as applicable, Quarantine/isolation, Movement restrictions, Preventive medication, Ring vaccination, Targeted vaccination, Mass vaccination and Prophylactic vaccination.

G.A. SEC6-PR-204100
Total Cost : € 1,883,475
EU Contribution : € 1,412,606
Starting Date : January 2007
Duration : 18 Months

Coordinator:
THALES SECURITY SYSTEMS
France

Contact:
Christian FEDORCZAK
Tel : +33 1 40 83 22 10
Fax : +33 1 40 83 21 21
e-mail: christian.fedorczak@thalesgroup.com

Partners:

EADS Defence and Security Systems	**FR**
Consorzio SESM	**IT**
ELSAG Spa	**IT**
Skysoft Portugal – Software e Technologias de Informação S.A.	**PT**
Thales Research and Technology	**FR**
Universidad Politecnica de Valencia	**ES**
Fundação Assistência Médica Internacional	**PT**
ITTI Sp. z o.o.	**PL**

Preparatory Action for Security Research

(PASR 2004)

CRIMSON: THE CRISIS SIMULATION SYSTEM

CRIMSON
Urban Crisis Simulation

The CRIMSON project aims to research, develop and validate an innovative system using the latest Virtual Reality technologies for the inter-organisational preparation, rehearsal and management of security missions in response to urban crisis (terror attacks, seizure of hostages, NBCR crisis, etc.).

The **CRIMSON** system will allow the 3D simulation and evaluation of complex urban crisis and contingency scenarios that would be difficult to simulate and validate in real conditions. This system will offer a unique tool for creating, communicating and sharing complex knowledge between users with very different educational or cultural background. It will dramatically enhance the planning and management of crisis, the preparation of crisis management tasks, and, at the same time, it will provide a captivating tool for the collaborative training of the security actors and the information of citizens.

By combining the latest cutting-edge technologies of videogames, military simulations, virtual reality and geographic information, the CRIMSON project represents a big step forward in meeting the challenge of effective crisis management preparation and rehearsal in complex urban environments. CRIMSON represents an important innovation compared to current systems that are based on a 2D top-down representation of the environment which is not adapted to fundamentally three-dimensional and interactive urban environments. It goes far beyond video-games and 3D simulations by enabling real users, with no specific computer expertise, to create and populate their own crisis environment and develop their own scenarios.

Therefore, the **CRIMSON** project develops a software application and a set of interaction devices that will enable the simulation of a virtual urban environment. It empowers multiple participants to interactively populate this environment and create crisis scenarios by animating citizens, actors of the crisis, vehicles as well as modifying the crisis parameters along the time (ex: the movement of a toxic cloud, panic movements, traffic jams, etc.). Thus, participants can visually and interactively rehearse, assess and validate crisis response scenarios. Scenarios such as rescue of hostages seized inside a building as well as NBCR accidents/attacks can be experienced.

The main features of the **CRIMSON** system include:

- Interactive visualisation of massive urban databases including threats, resources, population and vehicles.
- Behavioural simulation of the traffic and the actors of the crisis, as individuals or as groups;
- Intuitive crisis scenario editor allowing the definition of different crisis configurations and parameters as well as their evolution along the time (accidents, fires, explosions, behaviour of citizens, traffic, weather conditions, etc.);
- Innovative physical and games-like interfaces that make the man-machine interaction very intuitive for non computer experts;
- Integration of the different modules within the CRIMSON seamless, open and distributed architecture that will support collaborative sessions;
- The system runs on entry level PC, with the appropriate graphic board and hard drive, as well as on tailored workstations featuring innovative interfaces.

More information is available at http://crimson.c-s.fr

Ref : G.A. SEC4-PR-110500
Total Cost : € 2,933,610
EU Contribution : € 1,520,000
Starting Date : 1/12/2004
Duration: 28 months

Coordinator:
CS Systèmes d'Information -
Virtual Reality Dept.
ZAC de la Grande Plaine
Rue Brindejonc des Moulinais
31500 Toulouse – France

Contact:
Olivier Balet
Tel : +33 (0) 561 176 528
Fax : +33 (0) 561 176 578
E-mail : Olivier.Balet@c-s.fr

Partners:

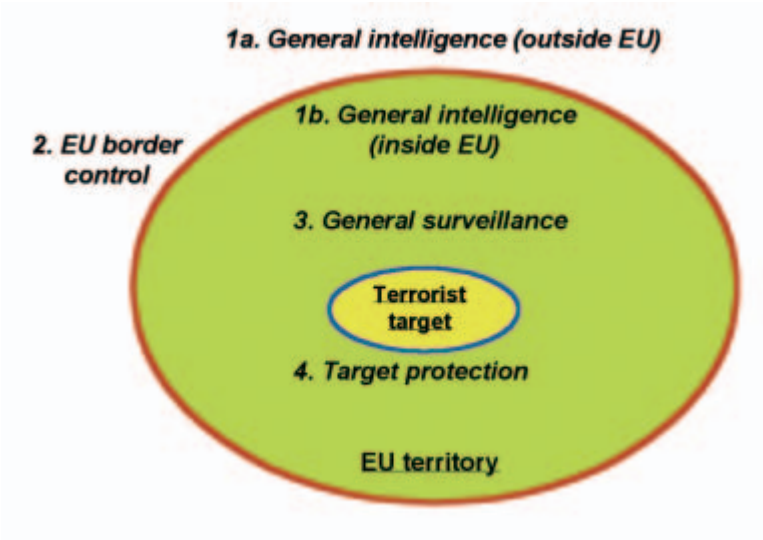
CS Systèmes d'Information	FR
Consiglio Nazionale delle Ricerche	IT
Crisis Research Center – University of Leiden	NL
Centre for Advanced Studies, Research and Development in Sardinia	IT
Mathématiques Appliquées SA	FR
Estonian Rescue Board	EE

Preparatory Action for Security Research

(PASR 2004)

ESSTRT:

EUROPEAN SECURITY: HIGH LEVEL STUDY ON THREATS RESPONSES AND RELEVANT TECHNOLOGIES



TO CARRY OUT AN ATTACK, TERRORISTS HAVE TO CROSS 4 FENCES.
THE EU RESPONSE IS TO MAKE EACH OF THE 4 FENCES AS EFFECTIVE AS POSSIBLE.

ESSTRT is a supporting activity that provides a comprehensive overview of necessary responses to security challenges. ESSTRT has analysed the terrorist and weapons threats to Europe, and unstable situations that ferment threats. Counters to these threats are to make « security fences » against terrorism (intelligence, border control, surveillance and target protection) as strong as possible. The characteristics of different targets have been analysed in order to understand any particular vulnerabilities. Also, the political, legal and ethical issues associated with the various security solutions have been analysed, e.g. privacy issues, potential danger to humans and social exclusion.

Scientific and technological aspects included are:

- Key security technologies that need to be developed
- How new technologies can improve security
- The potential for combining these with non-technological means to confront threats.
- Outline net cost and benefit estimates of using the technologies.

The Study recommends that:

- Member States conduct risk-based assessments of Critical National Infrastructure.
- Member States adopt a range of actions intended to prevent terrorist action, to pursue those responsible, to protect against attacks and to develop resilience against them.

- Member States should have a crisis management structure that regularly rehearses tackling contingencies.
- These national actions should be backed by a set of enabling capabilities including intelligence information, a strong policy of public communication, and robust relationships with international partners.
- The EU should develop a comprehensive strategy as well as a stronger operational and tactical structure, and a High Representative for internal security should be appointed.
- The EU should establish a Crisis Management Centre in Brussels supported by secure communications between the crisis management structures of Member States
- The EU should also work with important partner countries to develop links between terrorism analysis centres and share analysis of risks and counter-measures

Among technologies that, if advanced and improved, would considerably bolster security measures are:

- Scanners to detect weapons or hazardous substances. This would improve security at airports and other travel hubs, for example by better scanning of people and luggage for weapons.
- "Smart containers" for sea transport and large vehicles, because of the inadequacies of scanning technologies for large objects.
- Area surveillance and perimeter/border protection. This would include surveillance of public spaces to detect unusual behaviour, and of remote, unattended borders.
- Personal identification, including biometrics. Though biometrics have been introduced into some personal identification documents, rates of false rejection and false acceptance are too high and need to be reduced.
- Fast detection and identification of chemical, biological and radiological substances

Measures to increase security have raised concerns about erosion of civil liberties and democratic values and some new counter-terrorism legislation has promoted vigorous public debate. There has been concern over lack of judicial oversight and democratic control, and over some technologies. The challenge is to find an acceptable balance, which will vary from country to country and will depend on threat perceptions. Recommendations on further research on social and political issues have been made.

Further information available at http://www.thalesresearch.com/Default.aspx?tabid=465

G.A. : SEC4-SA-003200
Total Cost : € 811,320
EU Contribution : € 599,938
Starting Date : 01/12/2004
Duration : 16 months

Coordinator:
Thales Research and Technology Ltd
UK

Contact:
Peter Munday
Tel : +44 118 923 8239
Fax : +44 118 923 8399
E-mail : peter.munday@thalesgroup.com

Partners:
International Institute for Strategic Studies **UK**
Crisis Management Initiative **FI**
Thales e-Security **UK**

Preparatory Action for Security Research

(PASR 2006)

EUROCOP THE PEDESTRIAN POLICE OFFICER

Pedestrian police officers play a major role in policing and security. They have to enable lawful activities of all citizens, to protect human rights, and to be prepared for public disorder, major incidents, acts of terrorism.

Key to their mission is the ability to gather intelligence, record crime and incidents, retrieve information from police systems and input information into them, identify people encountered, be accessible to their communities. They need to spend as much time as possible engaged in active policing in the street visible to citizens and respectful of privacy.

Currently, their efficiency suffers from poor information capture and management, lack of connection with vehicles and central office; they have spent much time in office work and not enough time in the street.

The objective of the one-year Supporting Activity «**EuroCop**» is to define and evaluate technologies to improve the efficiency of a pedestrian police officer. It will provide pedestrian police officers with better information capture and management, improving the global efficiency of the system.

At each step to consider legal, ethical and privacy requirements. Particular attention will be paid to acceptability by citizens

Police forces make a major contribution to the security of a country. Protecting frontiers, protecting against terrorism, crisis management are the main missions which can be achieved through interoperability of integrated systems for information and communication, which becomes mandatory.

Police forces organisation differs from country to country but their **core missions** are similar: to protect Life and Property, to prevent Crime, to detect and arrest offenders… Pedestrian police officers will always be irreplaceable because they have access everywhere (gardens, stairs, cellar…) and they are the first final milestone to any action.

Key to their mission is the ability to gather intelligence, record crime and incidents, retrieve information from police systems and input information into them, identify people encountered, be accessible to their communities. They need to spend as much time as possible engaged in active policing visible to citizens and respectful of privacy.

Currently, pedestrian police officers have limited communication equipment and are not included in the police network (and eventually the Criminal Justice). They spend only a small part of their time (sometimes as low as 20%) policing on the street. **There is therefore a strong need to improve the efficiency of pedestrian police officers** to increase the time available for patrol.

The police officers equipment has usually not been designed in a systemic approach. Different soldiers equipment programmes (Soldato del futuro, IZF, F.IS.T, FELIN) explore the future with a systemic approach and could give some ideas of the different types of system and equipment However the needs and constraints of soldiers and police officers are very different and military equipment can inspire research but can not just be copied for police needs.

The aim of the Supporting Activity « EuroCop » is to define and evaluate technologies to improve the efficiency of pedestrian police officers. It will provide Pedestrian police officers better information capture and management, strengthening their efficiency and the global efficiency of the system.

G.A. SEC6-SA-211900
Total Cost : € 547,252
EU Contribution : € 410,439
Starting Date : 01/02/2007
Duration : 15 months

Coordinator:
SAGEM DEFENSE SECURITE
France

Contact:
Jean-Thierry AUDREN
Tel : +33 1 58 12 41 35
Fax : +33 1 58 11 70 84
E-mail : jean-thierry.audren@sagem.com

Partners:

Swedish Defence Research Agency	**SE**
University of Reading (IRC)	**UK**
Fondation pour la Recherche Stratégique	**FR**
Netherlands Organisation for Applied Scientific Research	**NL**
Ministère de l'Intérieur et de l'Aménagement du Territoire	**FR**

Preparatory Action for Security Research

(PASR 2006)

GATE NEXT GENERATION ANTI-TERRORISM FINANCING (ATF) METHODS

GATE aims to study **new adaptive multidisciplinary modelling techniques** to detect criminal behaviour by flagging suspicious human behaviours for Anti-Money Laundering (AML). As in this scenario behavioural modelling is informed by intelligence from within individual financial institutions, but is enriched by additional informational items and that we seek to encapsulate by the term '**expanded behavioural modelling**'.

The project will identify, design, develop, deploy and validate models in real conditions within banks to capture more complex behaviours including multidisciplinary aspects beyond utilising transaction data from financial institutions, such as demographics, lifestyle or cultural behaviour of the involved people. Collection of this peripheral yet crucial information for modelling the problem domain will be integrated with transaction data and hence modelling will acquire an enriched and more dynamic perspective.

The financing of criminal and terrorist activities is an international problem of massive proportions, which must be addressed with an international solution, exploiting where possible state-of-the-art technology solutions to identify suspicious transactions in a way that allows law enforcement intervention in a timely manner, armed with the best possible tools that facilitate capturing new AML/ATF methods and practices.

It is envisaged to implement wide research across the underlying areas of existing political, regulatory, technological, legal, and best practice as well as to study the effectiveness and impact from the perspective of both user groups and regulations. Furthermore, the project incorporates in depth research of ongoing legislative and regulatory initiatives taken at Community level in the areas of justice, civil protection by integrating organisation whose strategic activities are primary in the line of setting and advising respectively regulations and political decisions.

G.A. SEC6-PR-205800
Total Cost : € 1,133,078
EU Contribution : € 783,685
Starting Date : 01/01/2007
Duration : 24 months

Coordinator:
EXODUS SA.

Contact:
Anastasia Garbi
Tel : + 30-210-7470198(int.301)
Fax : + 30-210-7450399
E-mail : angarbi@exodus.gr

Partners:

Piraeus Bank SA.	**EL**
London School of Economics	**UK**
Joint Research Center	**EC**
Alliance & Leicester Plc.	**UK**

Preparatory Action for Security Research

(PASR 2004)

GEOCREW

STUDY ON GEODATA AND CRISIS EARLY WARNING SITUATION AWARENESS

The **GEOCREW** supporting activity is a study dedicated to the early detection of (man-made) crises with a potential international dimension and relevance to the security of European citizens. If detected early, a crisis can be handled and solved at lower engagement levels before it evolves to critical or military dimensions.

The study is composed of two parts which concentrate on different focuses and complement one another. The first part (**CREW**) comprises an overall architecture for integrating different information sources identified through user requirements of security related services, the second part (**GEODATA**) concentrates on the specific utilization of geospatial data for improving situation awareness, using a more detailed technical approach.

This architecture should enable collaboration schemes for continuous cooperation and workshare of organisations cooperating in the field of crisis early warning within EU and its Member States.

An essential part of the **GEOCREW** study was the collection of operational and functional requirements on geospatial and non-geospatial information from/together with the relevant users, as well as the proof of the concept in a case study and in demonstrators.

The **GEOCREW** study covers the following activities:

- Identification of EU / national organisations dealing with crisis management and geospatial data for security objectives
- Collection of user requirements related to information and functionality
- Gathering of available information on geospatial and non-geospatial data, information and processing (including from open sources)
- Analysis/definition of operational concepts and processes based on user requirements
- Assessment of available technologies and standards
- Definition of an outline architecture for a collaborative intelligence platform
- Assessment of a European earth observation ground segment infrastructure with respect to the proposed concept
- Design and system architecture of a GeoToolBox for easy handling of geospatial data
- Configuration of a demonstrator for the generation of a consistent environmental picture.
- Configuration of a demonstrator on RDF and Semantic Web Technology Assessment showing the effectiveness of the technical concept
- Evaluation of a past early warning case in a case study showing the added value of the **GEOCREW** architecture concept

Results and achievements

The main result of **GEOCREW** was the elaboration of an architecture concept for a collaborative secure virtual platform.

It could allow organisations like intelligence services, crisis and situation awareness centres, institutes within EU and its Member States to integrate different and comprising data sources like geospatial data, open sources, reports.

The realisation of the **GEOCREW** architecture concept could provide the means to fulfil their task of political crisis early warning in a more comprehensive, effective and timely way.

G.A. : SEC4-SA-5200
Total Cost : € 695,573
EU Contribution : € 532,900
Starting Date : Jan 1st, 2005
Duration : 13 months

Coordinator:
ESG Elektroniksystem - und Logistik GmbH
Germany

Contact:
Manfred Müller
Tel : +49-89-9216-2721
Fax : +48-89-9216-2732
E-mail : mamueller@esg.de

Partners:

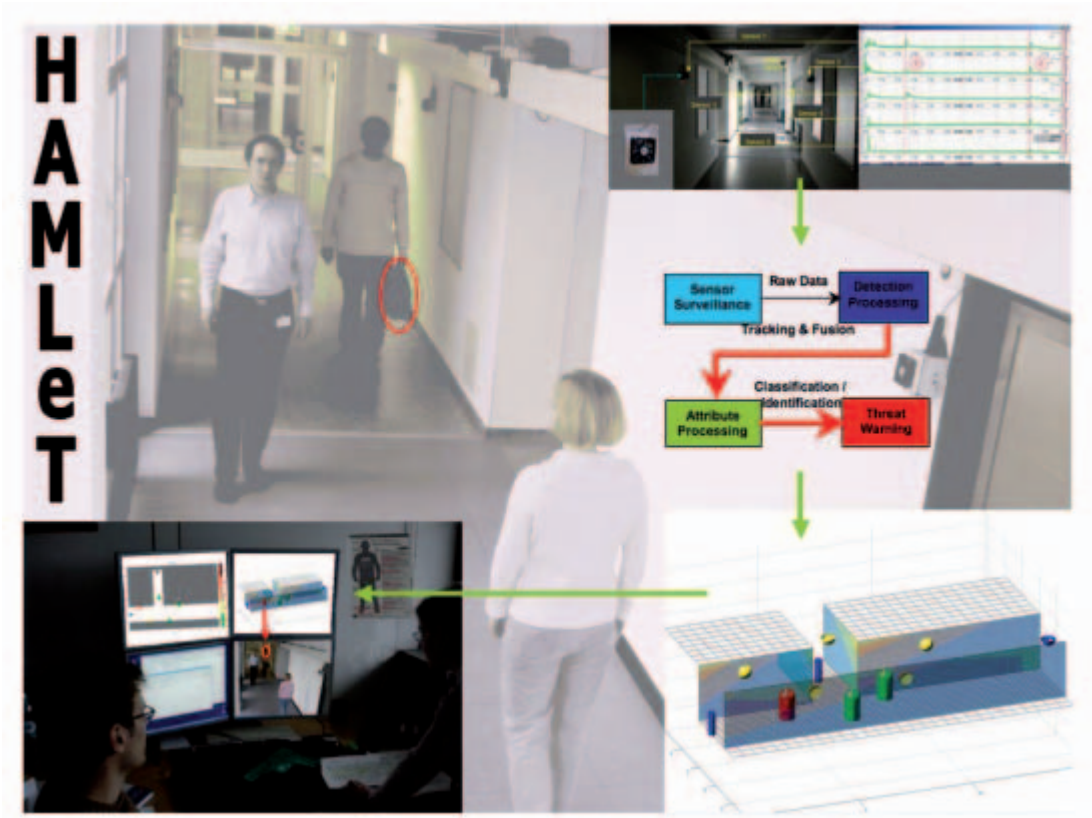
BAE Limited	**UK**
Asemantics S. R. L.	**IT**
Deutsches Zentrum für Luft- und Raumfahrt e. V	**DE**
Eurosense S. R. O.	**SK**
GMV S. A	**ES**
Joint Research Centre European Commission	**IT**
Open Geospatial Consortium Europe	**UK**
Planetek Italia	**IT**
Stichting National Lucht-en Ruimtevaartlaboratorium	**NL**

Preparatory Action for Security Research

(PASR 2006)

HAMLeT

HAZARDOUS MATERIAL LOCALISATION & PERSON TRACKING



One important aspect with respect to current threats is covered by security assistance systems comprising state-of-the-art surveillance technology. Such systems are indispensable for improving public domain security in the open European societies. In this context, the supporting activity **HAMLeT** (Hazardous Material Localization & Person Tracking) was successfully evaluated from the third call of the PASR.

HAMLeT will demonstrate core functions of an in-door security assistance system for real-time decision support by using advanced sensors and multiple sensor fusion techniques. The main goal of **HAMLeT** is to classify, track and localize potential threats in order to focus the attention of security personnel.

Basic input data for the classification are provided by chemical sensors detecting hazardous materials, such as explosives. However, due to the fact that chemo-sensors have limited spatio-temporal resolution, an individual chemical sensor is unable to localize hazardous material and to associate it with potential threats. Within the integrative approach of **HAMLeT**, this deficiency is compensated in dynamic scenarios by fusing the output of several chemical sensors with kinematical data from laser range-scanning and video sensors used for multiple persons tracking.

Among the expected results, recommendations will be given for characterization and standardization of the detection performance of related chemical sensors with respect to probes, e.g. explosives. Currently, common standards of that kind do not exist. **HAMLeT** demonstrates new capabilities for early detection, localization, and continuous tracking of individuals or groups carrying hazardous material within a multiple person flow. In particular, **HAMLeT** will show that only in an integrated multiple sensor system, the potential of chemical sensors for security applications can be fully exploited.

G.A. SEC6-SA-204400
Total Cost : € 318,267
EU Contribution : € 218,823
Starting Date : 01/11/2006
Duration : 15 months

Coordinator:
Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN) e.V.
53343 Wachtberg, Germany

Contact:
Dr. Wolfgang Koch
Tel : + 49 228 9435 373
Fax : + 49 228 9435 685
E-mail : HAMLeT@fgan.de

Partners:

Fachhochschule Bonn-Rhein-Sieg, 53757 Sankt Augustin	**DE**
Rheinische Friedrich Wilhelms-Universität, 53012 Bonn	**DE**
Università degli Studi di Udine, 33100 Udine	**IT**
Wehrwissenschaftliches Institut für Werk-, Explosiv- und Betriebsstoffe, 85435 Erding	**DE**

Preparatory Action for Security Research

(PASR 2005)

HITS/ISAC

HIGHWAY TO SECURITY: INTEROPERABILITY FOR SITUATION AWARENESS AND CRISIS MANAGEMENT

The vision of **HiTS/ISAC** is a more secure Europe through prevention of terrorism and organised crime. Superior situation awareness and cross-border interoperability are key enablers, leading to new technical and operational methods to work, train and co-operate across Europe.

Today, information in databases at law-enforcement authorities is distributed across Europe. The information is not easily available to other authorities in Europe, especially not “on-line”.

The objective of **HiTS/ISAC** is to enable information analysis and fusion from many different sources, through secure cross-border on-line group cooperation between authorities, in order to detect and provide early warnings for suspicious activities, be it communication between suspected criminals, or anomalous movement of persons, goods or money, etc.

HiTS/ISAC will develop a Problem Solving Environment and demonstrate it in a Virtual Operations Room which can be established anywhere, at any time. Tools and processes will be developed and implemented, and demonstrated using realistic scenarios.

HiTS/ISAC addresses three of the priority missions identified in the Preparatory Action in the field of Security Research.

- First, the project focus is on prevention and prediction as protection against terrorism and organized crime.
- Second, the proposed research will facilitate interoperability between authorities in role-based cooperation.
- Third, the project aims to provide mechanisms for information sharing with security and integrity.

G.A. SEC5-PR-113700
Total Cost : € 1,739,093
EU Contribution : € 1,132,895
Starting Date : 1/6/2006
Duration : 18 months

Coordinator:
Saab AB
Sweden

Contact:
Mr. Jan Larsson
Tel : +46(0)8 58084991
Fax : +46(0)8 58087252
E-mail: jan.larsson@saab.se

Partners:

EADS Defence and Security Systems SA	**FR**
TeliaSonera	**FI**
Swedish Defence Research Agency	**SE**
EADS Secure Networks	**FI**
TietoEnator ALISE	**LV**
Denodo Technologies S.L.	**ES**
Hugin Expert A/S	**DK**
Cybernetica AS	**EE**
UAB "ERP"	**LT**
Military University of Technology	**PL**

Preparatory Action for Security Research

(PASR 2004)

IMPACT

INNOVATIVE MEASURES FOR PROTECTION AGAINST CBRN TERRORISM

Project/SA Objectives

The objectives of **IMPACT** are to lay the foundations for an integrated European CBRN counter terrorism research and acquisition programme and to validate, assess and demonstrate innovative technological capabilities, operational concepts and procedures to assist in developing preventive and suppressive crisis management.

Current European capabilities to detect and respond to the types of CBRN threats are very modest. Responsibility in Europe for initially responding to terrorist incidents is spread among many organisations. The lack of co-ordination is obvious. There is an urgent need to unify much of the current response capability while at the same time setting standards and establishing guidelines for European nations to address coordination of their response to terrorism. To address the particular issues surrounding CBRN weapons, Europe must adopt a broad strategy to address the best ways to prevent a terrorist event.

Our approach is based on five pillars:

- Assessing the threat
- Preventing an event
- Protecting against an event
- Responding to an event
- Recovering from an event

Results and achievements

The scenario building and preliminary risk assessment, aiming at strengthening the understanding of the CBRN threat, are accomplished. In addition, a CBRN agent database was constructed. The analysis of the role of first responders throughout Europe has been performed and a proposal for a European doctrine for first responders was written. An in-depth list of system requirements for the immediate response team, as well as requirements on C, B R/N detection, physical protection, decontamination and sampling were formulated an embedded in a requirement database. An overview of current and emerging detection techniques for C and R/N was provided. Likewise, the current European capabilities for detection (and sampling) of B agents was assessed and reported. A CR/N demonstrator with common language output was evaluated. Existing B detection platforms were assessed and evaluated. A task-analysis of first responders in CBR-scenarios was performed and state-of-the-art equipment was tested against the requirements. Current mass decontamination facilities, as well as COTS decontaminants were evaluated in a preliminary study. Existing operating procedures for CBRN sampling and sampling operations, including protocols and work instructions from different European nations and instructions from NATO, OPCW and also from IAEA, EPA NIOSH, ISO-organisations, were reviewed. Techniques for analysis of samples containing a mixture of agents were reviewed and proposals for improvement were made.

The highlights of the project were presented at an **IMPACT** symposium to stakeholders from governments, industries, institutes and first responders (Brussels, 25 October 2006).

For more information http://www.impact-eu.com/

G.A. : SEC4-PR-008000
Total Cost : € 4,308,695
EU Contribution : € 2,717,640
Starting Date : 1/12/2004
Duration : 24 months

Coordinator:
TNO Defence, Security and Safety
Netherlands

Contact:
Peter Van Hooft
Tel : (+31) 15 284 3530
Fax : (+31) 15 284 3963
E-mail : hooft@pml.tno.nl

Partners:

ARC Seibersdorf research GmbH	AU
BAE SYSTEMS Advanced Technology Centre	UK
Bruker Daltonik GmbH	DE
Centre d'Etude le Bouchet	FR
Consejo superior de Investigaciones Cientificas	ES
Dekati Oy	FI
eBiochips Systems GmbH	DE
Environics Oy	FI
Swedish Defence Research Agency	SE
Fraunhofer Institute for Silicon Technology	DE
Fraunhofer Institute for Reliability and Microintegration	DE
Joint Research Centre Ispra	IT
Smiths Detection	UK
Thales	FR
Rijksinstituut voor Volksgezondheid en Milieu	NL
Veterinary and Agrochemical Research Centre	BE
Valtion Teknillinen Tutkimuskeskus	FI
National Inst. For NBC Protection	CZ
Safety Equipment Development AB	SE

Preparatory Action for Security Research

(PASR 2004)

ISCAPS

INTEGRATED SURVEILLANCE OF CROWDED AREAS FOR PUBLIC SECURITY

The general objective of **ISCAPS** is to reduce the risks of malicious events by providing efficient, real-time, user-friendly, highly automated surveillance of crowded areas. This goal is achieved through industrial research in complementary technologies, bringing some existing technologies to maturity and demonstrating them in a real world environment.

The general scenario for **ISCAPS** is a public area in which people are moving around, and where there is an opportunity for expected threats. The project examines different types of public areas and their surveillance requirements.

These types include:

- different crowd densities – ranging from isolated individuals to fairly crowded areas (using standard definitions of groups and crowds);
- different control levels for managing the public area – gated (restricted) areas, channelled areas and open areas.

ISCAPS is being implemented in several steps:

1. Scenarios & Requirements: Identification & analysis of potential threat scenarios. Several of these scenarios have been selected. They serve as the basis for the requirements of the application being developed.
2. Technology development: Development of the system solution (hardware, algorithms, application) for covering the requirements developed in step 1.
3. Integration & Demonstration: Integration of the technology developed by the partners, and demonstration based on selected scenarios.
4. Road map: Based on the results of the demonstration, determination of the areas where additional research efforts are needed.
5. In parallel: Analysis of the social, legal and ethical aspects associated to the project; dissemination of the results.

Results and achievements

The following categories of results have been defined and completed:

A. Understanding and description of the different types of threats. Definition of the corresponding suspicious behaviours.
B. Design of a system architecture suited to address these threats, using break through technologies.
C. Knowledge of the difficulties to address to develop operational solutions, and of the areas where research efforts have to be increased. Definition of a roadmap.
D. Development of a dialogue with the end-users facing these potential threats.
E. Integration of privacy concerns in the design of solutions.
F. Demonstration of a global multi-sensor integrated system for detection of abnormal behaviour in a crowd

G.A. : SEC4-PR-013800
Total Cost : € 2,312,892
EU Contribution : € 1,699,999
Starting Date : 1/2/2005
Duration : 24 months

Coordinator:
Sagem Défense Sécurité,
France

Contact:
Jean-Marc Suchier
Tel : +33 1 53 23 18 50
Fax : +33 1 40 70 68 60
E-mail : jean-marc.suchier@sagem.com

Partners:

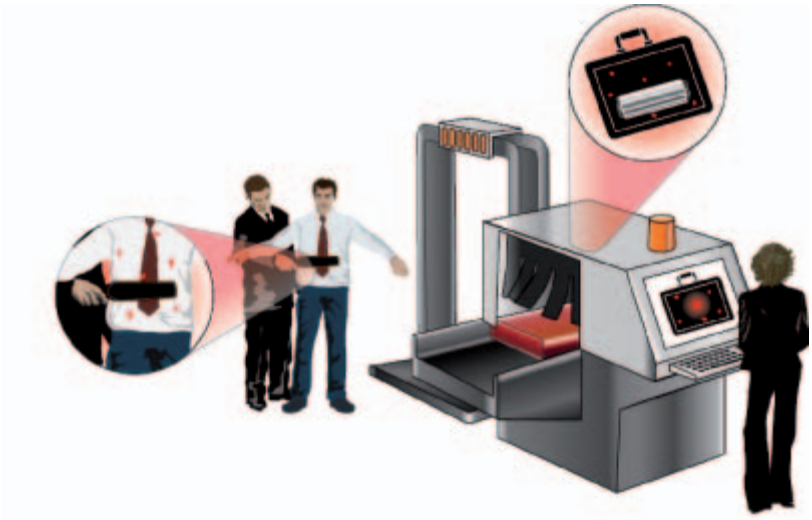
BAE Systems (Operations) Limited	**UK**
Commisariat à l'Energie Atomique	**FR**
DATAMAT S.P.A.	**IT**
ELSAG S.P.A.	**IT**
Fondation pour la Recherche Strategique	**FR**
GMV S.A.	**ES**
Societé Nationale des Chemins de Fer Français	**FR**
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	**NL**
University of Reading	**UK**

Preparatory Action for Security Research

(PASR 2006)

ISOTREX INTEGRATED SYSTEM FOR ON-LINE TRACE EXPLOSIVES DETECTION IN SOLID AND VAPOUR STATE

ISOTREX



The **ISOTREX** project has the main aim to contribute to trace explosive detection with instrument development able to detect trace high energized materials. The increasing frequency of terrorist attacks, in transit areas characterized by a flux of people and goods (airports, railways stations, central banks and main post offices) requires the increase of fast screening sensors suitable to detect hidden explosives from their traces released in the environment (gaseous emissions, dispersed particles on packing surfaces or cloths).

The **ISOTREX** project will investigate the development of instrument for particle/vapour detection as demonstrator of a portable system to be implemented in large check points (e.g. airports, customs, main post-offices) and for special police teams. The modular design of the system will allow its separation into two sub-systems and their displacement in different checking points according to different scenarios. The sub-system for explosives particle and liquid detection is based on LIBS (Laser Induced Breakdown Spectroscopy) technique and the other for explosive vapour detection on IR absorption methods (either cavity ring-down or laser photo-acoustic spectrometer). For each instrument a software for prompt explosive detection will be developed according to the generated data base, taking care to reduce false alarms. Following recent events in London, liquid explosive and main precursors will be investigated with the proposed techniques.

The project intends to exploit the capabilities offered by laser technologies in the application to explosives detection. Our target will be the detection of low levels of vapour and particles. To this aim the laser techniques considered for the specific exploitation are characterized by high selectivity and sensitivity (LIBS laser induced breakdown spectroscopy; CRDS cavity ring down spectroscopy; LPAS laser photo-acoustic spectroscopy) with concrete possibilities of miniaturization and consequently significant opportunities for development of commercial field instruments. In particular it is planned to design two laser based sub-systems, suitable both for independent or combined operation, which are capable of fast and real time monitoring of an explosive by detecting its molecular signature (high resolution IR absorption either in NIR by CRDS or in MIR by LPAS) and its elemental composition (plasma atomic/ionic emission by LIBS). The final instruments shall be easy to operate also by technically unskilled operators. Given a variety of the explosives and their matrices, the proposed instrument prototypes, are intended to recognize the presence of the energetic materials and to identify the most common explosive types and materials potentially dangerous. Materials identified as the energetic ones, but not fully recognizable by an initially developed database, shall be tagged as materials which require attention and further analyses.

The Advanced Technological Demonstrators (ATDs) will be implemented for use in environments subject to security restrictions (e.g. airport gates) to reveal the presence of hazardous species, either independently or after a preliminary warning from other sensors (different instrumentations, dogs, human suspicions).

G.A. SEC6-PR-203600
Total Cost : € 1,656,359
EU Contribution : € 1.242.265
Starting Date : 01/01/2007
Duration : 24 months

Coordinator:
ENEA
ENEA (Ente per le nuove tecnologie, j'energia e l'ambiente)
Italy

Contact:
Antonio Palucci
Tel : + 39 06 9400 5299
Fax : + 39 06 9400 5312
E-mail : palucci@frascati.enea.it

Partners:

Consiglio Nazionale delle Ricerche (CNR)	**IT**
Improve Process Analytic and Control (IPAC)	**AT**
Von Hoerner & Sulger GmbH (vH&S)	**DE**
TelCon S.r.L.	**IT**

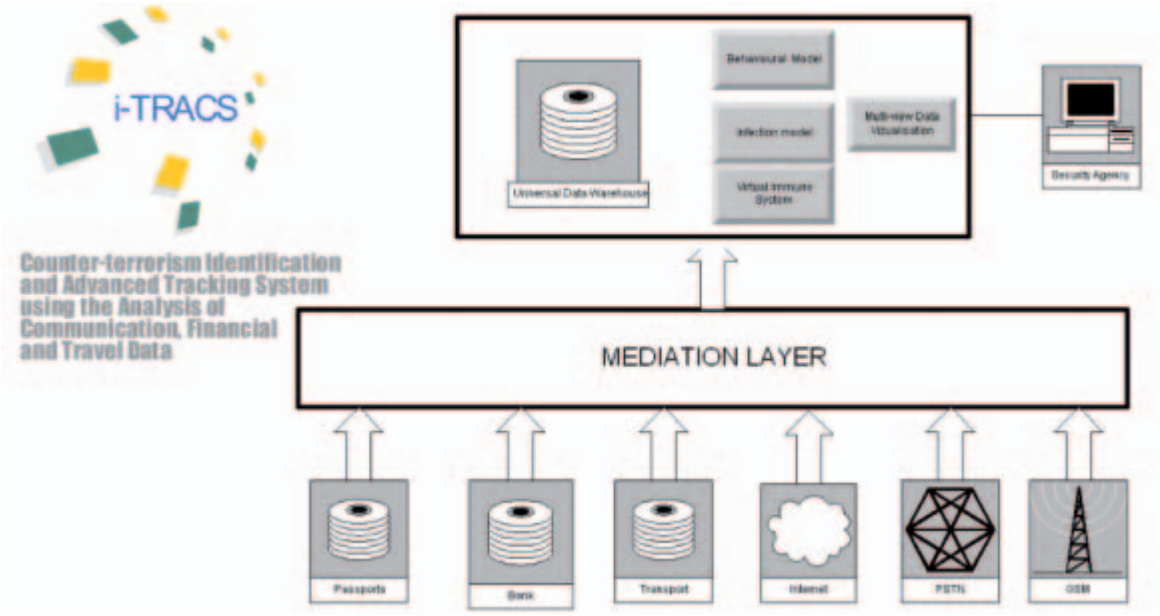
DIRECTORATE GENERAL ENTERPRISE AND INDUSTRY

SECURITY RESEARCH

Preparatory Action for Security Research

(PASR 2006)

I-TRACS COUNTER-TERRORISM IDENTIFICATION AND ADVANCED TRACKING SYSTEM USING THE ANALYSIS OF COMMUNICATION, FINANCIAL AND TRAVEL DATA



The **i-TRACS** project aims to improve the competitiveness of EU private & public organisations in the field of anti-terrorism and homeland security by the research and technological development of an innovative advanced tracking system consolidating and integrating multiple information data sources. The application of a wide spectrum of data sources offers a new level of efficiency.

i-TRACS will rely on a strong Consortium and User Advisory Group to provide technology, regulatory and market watches, to develop acceptable socially intelligent S&T innovations towards workable solutions.

The challenge lies in balancing the need for surveillance with the need for protecting civil liberties and the privacy of the ordinary citizen.

The **i-TRACS** Consortium has the confluence of expertise to fully expect to achieve unique and novel solutions (prototype) to empower the required and justifiable data intelligence gathering and linking of evidence in order to track and hopefully halt prima facie suspected criminal activities.

i-TRACS involves a wide range of users and stakeholders representing a broad spectrum of interests, cultural heritage and technical background such as public organisations, criminology, security and financial experts, as well as civil liberties groups to ensure the safeguarding of the Legal and Ethical standards in the design and development of i-TRACS innovative framework.

i-TRACS will lay the foundations for how data from multiple sources – but with a common thread – can be retrieved, selectively combined in a socio-ethically responsible way, analysed and such intelligence used to optimise the identification of prima facie suspect, or known, terrorists and the tracking of their activities.

i-TRACS will deliver a "shoe box" Demonstrator (prototype) comprising the tools and technologies for selected end-user scenarios to prove the need, feasibility, relevance and efficiency of the above approach. This will be done by a method called "war gaming", which derived from the field of military operations research. Some project members will elect to "play" the role of aggressors and attempt to realise their goals.

The awareness raising programme associated with the project will:

(a) Discuss aspects of this approach with interested stakeholders (users, security solution integration providers, other societal stakeholders).

(b) Contribute to relevant European Security Research Agenda workshops to share ideas on methods, best practice, tools and technologies (state-of-the-art) required for the tracking (pro-active, targeted investigations, surveillance) of critical suspected entities.

(c) Alert Member States to the need for harmonisation of laws to enable, but control, access to, and use of, transactional data.

(d) Highlight the need for innovation towards European tools and methodologies to support counter terrorism at both the European and national levels by developing, executing and analysing use cases at the level of European Directorates with national stakeholder participation.

G.A. SEC6-PR-210500
Total Cost : € 2,526,092
EU Contribution : € 1,883,826
Starting Date : 01/01/2007
Duration : 24 months

Coordinator:
CICOM (FR)

Contact:
Aurélien André
Tel : + 33 4 93 00 60 07
Fax : + 33 4 93 00 60 01
E-mail : aurelien@cicom.fr

Partners:

AQSACOM	FR
BAE Systems	UK
Thorpeglen	UK
IPIPAN (Institute of Computer Science, Polish Academy of Sciences)	PL
Northamptonshire Police Authority	UK
Privacy International	UK
Pride S.p.A	IT
Computer and Automation Research Institute, Hungarian Academy of Sciences	HU
University of Reading, School of Systems Engineering	UK

Preparatory Action for Security Research

(PASR 2005)

MARIUS

MOBILE **A**UTONOMOUS **R**EACTIVE **I**NFORMATION SYSTEM
FOR **U**RGENCY **S**ITUATIONS

MARIUS aims at developing a pre-operational autonomous Command Post which can be deployed very quickly to monitor every type of crisis management operations.

It will be equipped with its own sensors, information and communications systems and focuses on improving Crisis Management efficiency: deployment rapidity, inter-agency co-operation, situation assessment and decision-making.

The project will also address situation awareness and interoperability issues through the analysis of the operational scenarios and of the pre-normative aspects.

The **MARIUS** Demonstrator will be deployable by helicopter and will incorporate open scalable IT infrastructure, generic gateways, decision support and crisis communication support.

The **MARIUS** Consortium will provide a pre-operational version of the system integrating technological components necessary to evaluate innovative functions.

The consortium will be complemented by the User Group, comprising national end-users and European Stakeholders, who will warrant the operational pertinence of the project, from the present situation (NATO/Framework Nations dependency) to the 2010 Headline Goals.

The innovation in **MARIUS** lies in the integration of the following state-of-the-art elements, customised to fulfil the requirements of a generic crisis management system:

1. An airborne (helicopter) segment equipped with EO/IR sensor, GSM detection & location sensor, SMS broadcast capability, a data link to the ground station, radio systems (voice);
2. A mobile crisis management system, built around the following major blocks:

- UMS – a ground station with a modular approach that can be used for mobile command and control applications and can be expanded to control multiple unmanned air vehicles;
- ZODIACO – the Tactical Command an Control system, used to establish the situation, combining the data elaborated by UMS, the intelligence data bases and the various reports coming from the rescue teams;
- The decision support module, used to task the different rescue teams as a function of the situation analysis and of the various reports received,
- The Human-Machine Interface (HMI) part, consisting of ZODIACO HMI for tactical situation, UMS HMI for the sensors data and an additional HMI for decision support,
- The gateways to the infrastructure and deployable communication networks;

3. The ground sensors (cameras) and their specific data link;
4. A Micro-drone to demonstrate airborne surveillance functions in case of disaster;
5. The deployable wireless communications network.

Expected results

Due to its modularity and flexibility, **MARIUS** is to be used in any type of crisis and it is expected to bring an important added-value for disaster response activities.

The main **MARIUS** tangible result will consist in the demonstration that it is feasible to develop a joint crisis Command Post which can be deployed in a few hours in any part of the world. The system will be equipped with the relevant communications capabilities to manage the operations in the field. All agencies will potentially work on the same system, thus enhancing the interoperability between them. Trials will take place in Valencia (Spain) in June 2007 with the full support of the city firemen.

G.A. : SEC5-PR-107900
Total Cost : € 1,915,905
EU Contribution : € 1,431,988
Starting Date : 1/3/2006
Duration : 18 months

Coordinator:
EADS Defence and Security systems SA- Global Security
France

Contact:
Philippe Chrobocinski
Tel : +33 1 34 60 77 64
Fax : +33 1 30 47 61 19
E-mail : philippe.chrobocinski@eads.com

Partners:

THALES Communications SA	FR
SELEX Communications SpA	IT
SELEX Sistemi Integrati SpA	IT
THALES Research and Technology	FR
AMPER PROGRAMAS DE ELECTRONICA Y COMUNICACIONES SA	ES
EUROCOPTER SAS	FR
BAE Systems	UK
Immobiliser Central Europe Ltd	CZ
CRANFIELD University	UK
Universidad Politécnica de Valencia	ES
Commissariat à l'Energie Atomique	FR
SWAPCOM	FR

Preparatory Action for Security Research

(PASR 2005)

PALMA PROTECTION OF AIRLINERS AGAINST MANPADS ATTACKS

Project Objectives

PALMA's main objective is to evaluate, at European level, the efficiency and the impacts of on-board self-protection systems (certification, environment and population safety, air traffic, costs…).

Through the investigation of critical technologies for short, medium and long term solutions, future research needs will be identified and, if needed, requirements for a future operational system will be defined.

Description of the work

The project is divided in three main items:

- Identification of the functional and operational requirements,
- Technological analysis, including specific experimental investigations,
- Recommendation for future developments.

Expected results

The main expected outputs of the project are:

- Recommendations for future regulations,
- Definition of intermediate solutions with existing technologies and a research programme for a fully compliant system,
- Roadmap for European technology developments.

G.A. SEC5-PR-110800
Total Cost : € 1,984,538
EU Contribution : € 1,457,000
Starting Date : 01/02/2006
Duration : 18 months

Coordinator:
EADS CCR DCR/STI/T
France

Contact:
Gilles Fournier
Tel: +33 (0)1 46 97 36 71
Fax: +33 (0)1 46 97 30 08
E-mail: gilles.fournier@eads.net

Partners:

THALES AVIONICS SA	FR
AIRBUS France SAS	FR
MBDA France	FR
EADS Deutschland GmbH	DE
Deutsches Zentrum für Luft- und Raumfahrt e.V.	DE
DIEHL BGT Defence GmbH & Co. KG	DE
Aviation Défense Service	FR
ALENIA Aeronautica S.p.A.	IT
LACROIX Etienne tous artifices SA	FR
Dereham Designs and Packaging Ltd	UK
CILAS	FR

Preparatory Action for Security Research

(PASR 2005)

PATIN PROTECTION OF AIR TRANSPORTATION AND INFRASTRUCTURE

Description of the work

In a first step, the security measures of the existing Air Transportation system will be analysed. A threat assessment and risk analysis will be undertaken to detect where improvements are needed. The security requirements will be defined through a security assessment methodology and the setting of target levels of security. A security case methodology will be developed to assess to what extent the security requirements are met by proposed enhancements in operations, procedures, systems and technology. Compliance for operations, procedures, systems and technology will be laid down in draft regulations and recommended practices.

In the next step, the technologies for protection of air transport and infrastructure against different terrorist attacks will be identified and analysed. State of the art and upcoming technologies will be identified, analysed and specified based on potential threats and operational requirements. Technologies will be assessed with respect to threat analysis, technology availability and maturity, target levels of security and regulations. The complete air transport and infrastructure chain is considered, including information infrastructure, airport, aircraft on ground and aircraft in flight.

Then the system design, architecture and the operational concept for the protection of the air transportation chain will be considered. Based on the description of the current system and the available technologies, concepts will be developed for the protection of the critical infrastructure and the airport/aircraft protection system.

A final step will bring the project results from research to practice. Security and governmental authorities, standardisation and regulation bodies, will be continuously informed about the outcome of the project. A user conference inviting all air transportation stakeholders will be installed to test the practicability of the proposed security concept for aircraft self-protection.

Project Objectives

PATIN aims to ensure the security of EU citizens by protecting the whole air transportation system against terrorist attacks, including airport, aircraft, critical ground infrastructure and the information system. The project will assess aspects of crisis management, interoperability and optimisation of security networks.

PATIN will analyse all potentially relevant threats and technologies and will derive from these a set of viable future operational concepts.

A conference and joint exercises with the stakeholder community (users and security organisations) will be organised to assess the operational concepts and the improved security provided. **PATIN** adapts a layered protection mechanism which forms a system-of-system interconnected through networks. A top level network will provide information for the whole of European air transportation. Local networks will detect anomalies at airports followed by reactive and proactive measures against co-ordinated terrorist attacks.

PATIN will also address the issues of human factors, security implications of measures implemented, regulations as well as social and ethical values

G.A. : SEC5-PR-110400
Total Cost : € 3,538,298
EU Contribution : € 2,651,542
Starting Date : 1/7/2006
Duration : 15 months

Coordinator:
Diehl BGT Defence
Germany

Contact:
Dr.Klaus Scheerer
Tel : + 49 7551 89 6790
Fax : + 49 7551 89 4687
E-mail : klaus.scheerer@diehl-bgt-defence.de

Partners:

Flughafen München GmbH	**DE**
BAE Systems Advanced Technology Centre	**UK**
Belgian Advanced Technology Systems S.A.	**BE**
DT Media Limited	**UK**
Chemring Countermeasures	**UK**
Deutsches Zentrum für Luft- und Raumfahrt	**DE**
Dassault Aviation S.A.	**FR**
EADS Deutschland GmbH Defence Electronics	**DE**
European Organisation for the Safety of Air Navigation	**BE**
Galileo Avionica S.p.A.	**IT**
Hellenic Aerospace Industry S.A.	**EL**
Ericsson Microwave Systems A.B.	**SE**
Stichting Nationaal Lucht- en Ruimtevaartlaboratorium	**NL**
SAAB AB (Publ)	**SE**
SAGEM S.A.	**FR**
Thales Avionics. S.A.	**FR**
Netherlands Organisation for Applied Scientific Research	**NL**
42 Solutions B.V.	**NL**
Czech Airport Authority	**CZ**
Selex Sensors and Airborne Systems Limited	**UK**

Preparatory Action for Security Research

(PASR 2005)

PETRA.NET NETWORK FOR THE PROMOTION, ENHANCEMENT AND TAKE-UP OF SECURITY RESEARCH ACTIVITIES

PETRA.NET will establish a network linking the security research community with public authority users such as the police, fire brigade, ambulance service and civil defence. This network will promote the transfer of research results into the operational environment using trusted and secure dissemination mechanisms. It will also support the cross-fertilisation of emerging research results between PASR activities and the public authority user community.

PETRA.NET will meet these objectives through three thematic sub-actions:

- Establishing an interface between the PASR research community and the public authority user community in the form of an Observatory
- Brokering information exchange relationships between members of the research community and the user community
- Analysing, disseminating and exchanging information on how PASR research can have an impact in the operational environment.

PETRA.NET is led by members of the public authority user community with a wealth of experience in EU-funded research. They are therefore ideally placed to establish this network and to broker the necessary cross-fertilisation relationships.

PETRA.NET's primary objective is:

To build a Network linking the security research community with the public authority user community to promote the transfer of results from the security research domain to the operational environment and to provide a conduit for obtaining user requirements.

The project has three sub-objectives as follows:

1. To provide a secure interface though end-users can access emerging research results

A web-based Observatory will be established which will:

- Monitor and review emerging results from PASR projects
- Keep a watching brief on results from other relevant Commission-funded research
- Provide the public authority user community with access to information on these research activities

2. To provide networking opportunities for the public authority user community and the research community

PETRA.NET will support individuals, organisations and agencies seeking information on the PASR projects by putting them in contact with those having it. This will be achieved through a virtual helpdesk offering networking activities and information brokerage services and through access to experts involved in the PASR programme.

3. To analyse, disseminate and exchange information with the public authority user community

Emerging trends in EC-funded security research will be identified, assessed and made available to user communities. **PETRA.NET** will also run Thematic Workshops on specific aspects of security research. The project will also publish a quarterly electronic newsletter specifically to highlight PASR project progress and results and key developments specifically designed for public authority user community.

Total Cost : € 466,645
EU Contribution : € 364,000
Starting Date : 01/10/2006
Duration : 24 months

Coordinator:
Sussex Police Authority
UK

Contact:
Chief Superintendent Robert Hammond
Tel : + 44 1243 843654
Fax : + 44 +44 1243 843441
E-mail : Jim_hammond@btconnect.com

Partners:

IBI Group (UK) Limited	**UK**
Ministero dell'Interno – Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile	**IT**
Garda Síochána	**IE**
Korps Landelijke Politiediensten	**NL**
LISITT Universitat de Valencia	**ES**
Universita' Della Calabria	**IT**
IES Consulting	**IT**

DIRECTORATE GENERAL ENTERPRISE AND INDUSTRY

SECURITY RESEARCH

Preparatory Action for Security Research

(PASR 2005)

PRISE PRIVACY ENHANCING SHAPING OF SECURITY RESEARCH AND TECHNOLOGY – A PARTICIPATORY APPROACH TO DEVELOP ACCEPTABLE AND ACCEPTED PRINCIPLES FOR EUROPEAN SECURITY INDUSTRIES AND POLICIES

PRISE is a supporting activity that will promote a secure future for European citizens based on innovative security technologies and policies in line with privacy protection and human rights in general.

PRISE will provide guidelines and support for security solutions with a particular emphasis on human rights, human behaviour and perception of security and privacy.

It will assist the European Union in shaping its forthcoming security programme in order to achieve active contributions for maintaining security of its citizens with due regard for fundamental rights and democratic accountability at EU and national level.

The principal results will be sets of criteria for privacy enhancing security technologies. These sets of criteria will be applicable on different levels (research, development, implementation) and by different actors (research coordinators, industry, policy makers, public and private users).

The criteria will contribute directly to a tangible and demonstrable improvement in security as accepted and acceptable security technologies will be implemented more easily, more widely used and confronted with less disaffirmation from the general public and from users of these technologies.

Privacy enhancing or at least compliant security technologies will increase competitiveness of European security industries by providing guidance for the provision of widely acceptable security technologies; therefore they will contribute to security on a global level.

PRISE includes the following core tasks:

- developing and testing a set of criteria and guidelines for privacy enhancing security research and technology development,
- elaborating these criteria and guidelines with direct involvement of providers of security technologies, private and public users and implementers, institutions and bodies shaping policies and regulation as well as organisations representing potentially and actually conflicting interests,
- transforming the results into privacy-enhancing development and implementation scenarios of security technologies and measures,
- testing these scenarios in a set of participatory technology assessment procedures in different European states allowing for a substantiated indication of public perception and citizens' preferences,
- disseminating the results to actors relevant for the shaping of technologies and policies.

Further information is available at: http://prise.oeaw.ac.at.

G.A. SEC5-SA-108600
Total Cost : € 824,329
EU Contribution : € 617,900
Starting Date : 01/02/2006
Duration : 28 months

Coordinator:
Austrian Academy of Sciences
Austria

Contact:
Johann Čas
Tel : +43 1 51 581 6581
Fax : +43 1 710 98 83
E-mail : jcas@oeaw.ac.at

Partners:

Danish Board of Technology DBT	**DK**
Unabhängiges Landeszentum für Datenschutz ULD	**DE**
Norwegian Board of Technology NBT	**NO**

Preparatory Action for Security Research

(PASR 2005)

PROBANT PEOPLE REAL-TIME OBSERVATION IN BUILDINGS: ASSESSMENT OF NEW TECHNOLOGIES IN SUPPORT OF SURVEILLANCE AND INTERVENTION OPERATIONS

The **PROBANT** project will focus on the development, integration and validation of technologies enabling operators in crisis intervention and surveillance situations to observe individuals located inside buildings and trace them in real time.

The aim of the project is to improve the capability of security officers (in particular police officers) to visualize, locate, and identify human beings hidden behind walls and to follow their movements. In addition, measurements of biometric values will help determining if they are alive, nervous, sleeping, etc.

The system will allow for sophisticated data analysis techniques and for remote control.

In the field of protection against terrorism, the technologies validated by **PROBANT** will serve to prepare for solutions to threat detection and identification in cases where hostages are at stake, like kidnapping and hijacking.

They will allow officers to dispose of the information necessary to plan and execute a safe and adequate rescue operation. Moreover they may be used – according to national penal procedure law dispositions – in investigative operations related to terrorist networks.

PROBANT will trade-off the most innovative and promising technologies and will select them with respect to operational requirements.
Two demonstrators will be manufactured integrating the selected technologies. Both demonstrators will be evaluated under realistic conditions to be determined by the participating end-users, who will also provide a test environment simulating rooms and hostage crisis scenarios. Reproducible movements of bodies will be performed within this environment to objectively assert the performance of the demonstrators. Guidelines will be drawn with respect to performance and to the impact on the operational situations.

The following demonstrable novelties in security are expected as a result of **PROBANT**:

- Effective detection and real time observation of moving people in closed environments, with false alarm rate < 10 % and detection rate > 90 % (impossible with existing devices);
- Improvement of the quality of information in images derived from raw data;
- Improvement of the user-interface features, allowing operators to rapidly understand the images and to take decisions with a high level of confidence;
- Provision of more reliable techniques using biometric data to profile and label the moving people and to establish if a person hidden is still alive;
- Implementation of real time wireless transmission of data to remote control centers, allowing for advanced data processing and comparison with other information sources (merging information from other crisis cells).

G.A. SEC5-PR-104000
Total Cost : € 1,825,071
EU Contribution : € 1,176,799
Starting Date : 1/4/2006
Duration : 24 months

Coordinator:
Société d'Applications Technologiques de l'Imagerie Micro-Onde (SATIMO)
France

Contact:
Luc Duchesne
Tel : +33 1 69298156
Fax : +33 1 69290227
E-mail : lduchesne@satimo.fr

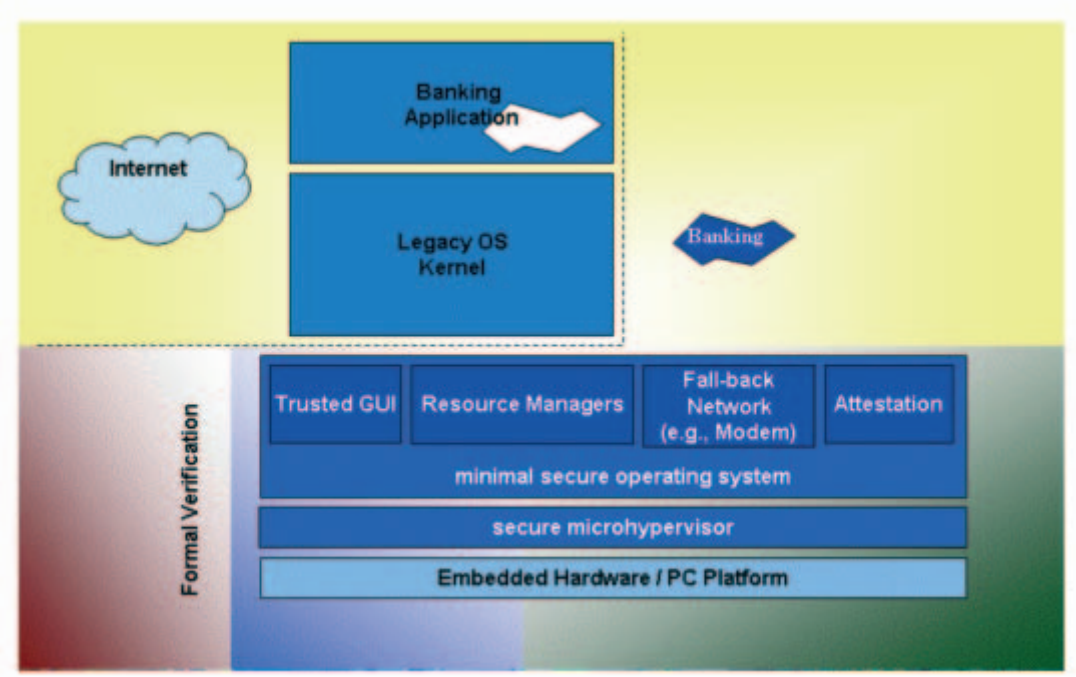
Partners:

Delft University of Technology	**NL**
DG Joint Research Centre of the European Commission	**IT**
Police Federale – Direction Générale de l'appui policier – Direction des Unités Spéciales	**BE**
Korps Landelijke Politiediensten – Dienst Specialistische Recherchetoepassingen	**NL**

Preparatory Action for Security Research

(PASR 2005)

ROBIN OPEN ROBUST INFRASTRUCTURES



The vulnerability of information and communication infrastructure is one of the key threats to modern society. Experience shows that this vulnerability is largely rooted in commonly used operating systems that have become incredibly complex and are thus very hard to harden against attacks. However, in practice the use of these legacy systems cannot be avoided. Even worse, stripped down versions increasingly find their way into embedded systems thus increasing the vulnerability of our infrastructure.

The objective of this Preparatory Action is to explore key technologies for a small, robust platform that can host legacy operating systems and their applications, but that is small enough to undergo formal analysis and construction techniques.

Preliminary studies have shown that in the order of a hundred thousand lines of code can be sufficient.

The platform will allow applications to be split into security-sensitive and other parts. It will also allow applications to fall back into an emergency mode. This platform will be open and originate from Europe, which will establish an alternative to proprietary US solutions that are expected to appear soon.

PARTNERS AND OBJECTIVES

TECHNISCHE **U**NIVERSITÄT **D**RESDEN

- **ROBIN Security Platform**
  consisting of a secure microhypervisor complemented with trusted servers that, together, allow running legacy operating systems next to security-sensitive applications.

STMICROELECTRONICS **S.A.**

- **ROBIN on Embedded Platform**
  and split of embedded applications into security-sensitive and security-insensitive parts.

RADBOUD **U**NIVERSITY **N**IJMEGEN

- **Formal Specification and Verification**
  of the microhypervisor interface and selected microhypervisor components.

SECUNET **S**ECURITY **N**ETWORKS **AG**

- **Application Scenarios**
  illustrating the applicability and use of the Robin Security Platform.

G.A. SEC5-PR-104600
Total Cost : € 1,885,061
EU Contribution : € 1,436,995
Starting Date : 1/2/2006
Duration : 24 months

Coordinator:
Technische Universität Dresden
Germany

Contact:
Prof. Hermann Härtig
Tel : +49-351-463 38 282
Fax : +49-351-463 38 284
E-mail: haertig@os.inf.tu-dresden.de

Partners:

Technische Universität Dresden	**DE**
STMicroelectronics S.A.	**FR**
Radboud University Nijmegen	**NL**
Secunet Security Networks AG	**DE**

Preparatory Action for Security Research

(PASR 2005)

SECCONDD SECURE CONTAINER DATA DEVICE STANDARDISATION

The aim of the **SECCONDD** Supporting Activity is to initiate the international standardisation of the technical interface between a secure container or vehicle and a data reader at a port or border crossing.

The interface should enable law enforcement and trade officials to read security data, including stored information from internal security and location sensors. It will thus be possible for them to determine where the container or vehicle has been, whether items (e.g. explosive devices) or people may have been inserted en route, and whether there may be hazardous items within it. Secondary purposes are to interface to a cargo tracking system and to provide data for automated cargo handling systems.

The interface will be specified in such a way that it:

- employs radio frequencies which can be used worldwide;
- can be read rapidly and at a range consistent with port operations;
- has authentication and data protection features;
- has optional data fields to support new sensors;
- can be implemented in a device with low cost, small size and low power consumption.

SECCONDD is expected to produce a set of unbiased, open, technical standards that can be utilised as inputs by the International Standards Organisation for future secure container standardisation activities.

The **SECCOND** work will consist of the following tasks:

Scenarios development to identify how effective a Goods Data Device (GDD) would be against terrorist or other threats, e.g. insertion of contraband:

- Study threat scenarios,
- Outline process and technology measures to overcome threats,
- Study constraints introduced by supply chain realities,
- Study additional possibilities with a long range communications link on the GDD.

GDD data: Identify the security data to be carried in the GDD to help counter the threats

- Identify the security data needed in the GDD,
- Identify the trade data needed in the GDD,
- Identify how the data is entered/initialised and deleted.

Protection and Authentication of the GDD data.

GDD Interrogation:

- Study port operations and how the GDD could be interrogated there,
- Study land border operations and how the GDD could be interrogated there,
- Identify other places where a GDD could be usefully interrogated,
- Study interfacing to a ship or lorry tracking system.

Interface Protocol: to identify possible suitable candidates.

- frequency bands for short and long range communications,
- physical and data link layer protocols,
- network and transport layer protocols,
- application layer protocols.

Interface Implications of the candidate interface protocols on the GDD size, cost and power supply.

G.A. SEC5-SA-105100
Total Cost : € 533,628
EU Contribution : € 399,851
Starting Date : 1/6/2006
Duration : 12 months

Coordinator:
Thales Research and Technology Ltd
UK

Contact:
Michael Naylor
Tel : +44 118 9238229
Fax : +44 118 923 8399
E-mail : mike.naylor@thalesgroup.com

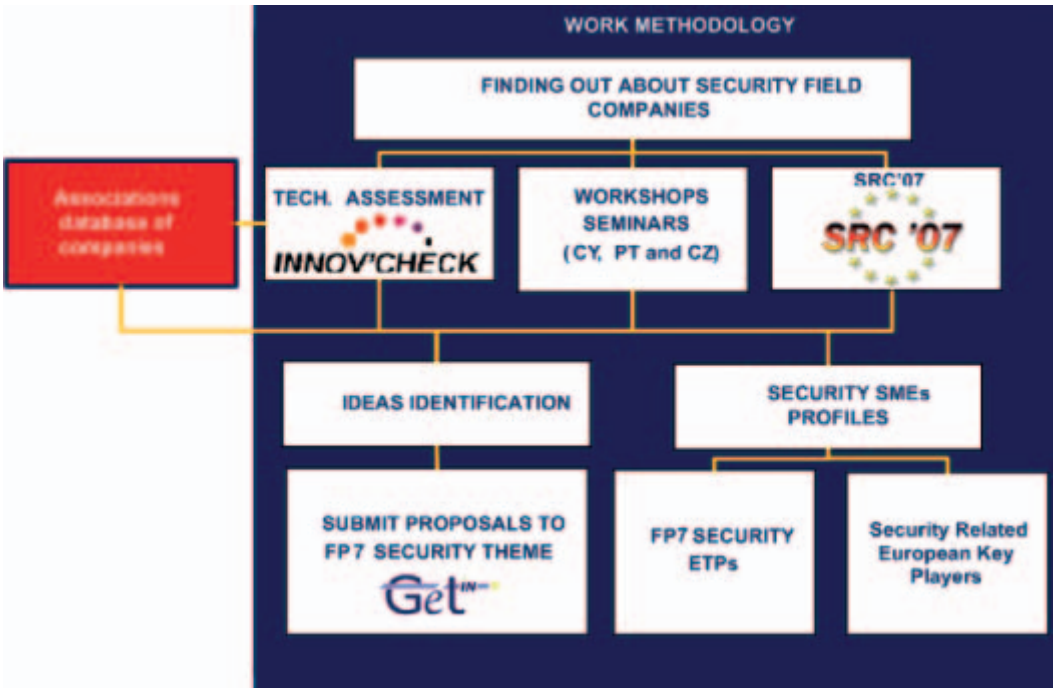
Partners:

SELEX Communications S.P.A	**IT**
Cotecna	**UK**
Her Majesty's Revenue & Customs	**UK**
Comité Européen de Normalisation	**BE**

Preparatory Action for Security Research

(PASR 2006)

SecureSME SUPPORTING SECURITY FIELD SMES IN PREPARING RTD PROJECTS



The main goal of **SecureSME** is to promote the integration of SMEs operating in the area of security to the European science and technology supply chains, and in particular to contribute to an increased participation of SMEs in FP7 Security research activities.

SecureSME will help to reinforce the competitiveness of industry and research in the security field and will also help to build effective partnerships among all the security technology actors (industry, research organisations, users…).

The consortium consists of 6 partners acting as multipliers and/or experts on security issues and European research projects.

SecureSME will be carried out along four main axes of activities:

- Awareness building and workshops/seminars
- Research and innovation strategy assessment
- Building R&D competences
- Preparation of future activities

SecureSME will address the following strategic objectives:

1. to identify research challenges that are relevant for the security domain and appropriate for SMEs, including the take up of research results from FP6 and other programmes, and to assist SMEs in developing their own proposal ideas as well as contributions to other proposals; this will be supported by using IT tools developed in earlier Framework Programme projects as well as other networks and platforms;
2. to establish contacts with proposal coordinators from industry and research organisations who wish to identify and integrate knowledgeable SMEs in their consortia, and to assist them to assemble successful integrated science and technology supply chains in the security area;
3. to provide SME targeted workshops related to the FP7 Security theme calls;
4. in all these activities to focus on the following research domains:
   - Optimising the security and protection of networked systems and critical infrastructures,
   - Protecting against terrorism and organised crime (including bio-terrorism and incidents with explosives biological, chemical and other substances),
   - Enhancing crisis management capabilities (including evacuation, search and rescue operations, control and remediation),
   - Enhancing border security and improving situation awareness,
   - Achieving interoperability and integration of systems.
5. to set-up a wide ranging service network that will share research and management information tools and models and will contribute to integrating science and technology supply chains, including SMEs, in the security domain.
6. to contribute to the elaboration of a strategic research agenda for the FP7 Security theme.

G.A. SEC6-PR-211900
Total Cost : € 330,289
EU Contribution : € 247,545
Starting Date : 15/01/2007
Duration : 24 months

Coordinator:
Inovamais – Serviços de Consultadoria em Inovação Tecnológica S.A.
Portugal

Contact:
Mr. Alexandre Almeida
Tel : + 35 1 229 39 63 50
Fax : + 35 1 229 39 63 51
E-mail : alexandre.almeida@inovamais.pt

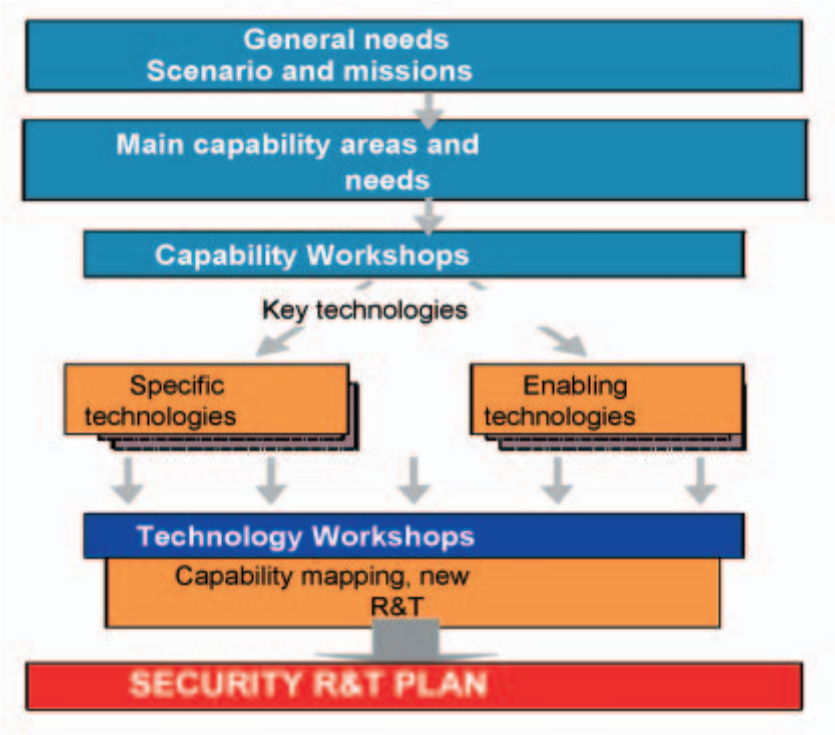
Partners:

AFCEA - Portugal	**PT**
Sollerta	**UK**
Innova Spa	**IT**
Robotiker	**ES**
Alcatel Alenia Space – Italia	**IT**

Preparatory Action for Security Research

(PASR 2004)

SENTRE SECURITY NETWORK FOR TECHNOLOGICAL RESEARCH IN EUROPE



Objectives

The **SeNTRE** support activity has delivered a strategic research plan for European security by establishing and consulting a network of users and technology experts at national and European levels, in direct link with the EC Advisory Board on Security (ESRAB) .The study, performed by a number of European organisations with relevant expertise, has provided the EU with a comprehensive input for planning its programme for security research (ESRP).

SeNTRE has brought together a network of users from Member States and European organisations and through this approach it has made a major contribution to the security of the citizen in Europe. Politically, it has helped to develop support for the action and to build visibility. Technically, it has helped to achieve wider commonality of the best possible security systems in Europe. Organisationally, it has paved the way for an improved exchange between national and European levels through a network of security and technical experts.

Description of the work

At the heart of the SenTRE methodology lays a double top/down / bottom-up approach to identify respectively the user/capability needs and the technology requirements.

- Definition of security missions

Identify what security and security-related activities should comprise

- Preparation and review of initial mission priorities

Several scenarios, grouped in themes, were elaborated using a theoretical methodology, adapted from military-security planning to the specific civil-security environment

- Validation through capabilities workshops & security taxonomy

Elementary capabilities were gathered via workshops and interviews of end-users at national and European level. A specific taxonomy for security was also developed and submitted to the Commission and ESRAB.

- Preparation of technology priorities

Technological requirements have been elaborated using a theoretical methodology, adapted from military capability-based research planning to the specific security environment and building on experience acquired in the civil domain.

- Validation through technology workshops

Technological requirements were gathered via workshops and interviews at national and European level. Existing ASD structures, including the SMIG network, were used to engage with a large industrial and research community base. Various end-users were also present to validate the expressed technological requirements. A taxonomy specific to security has been developed to structure the technology requirement database and linked to the capability database.

- Preparation of a strategic research plan (Final result)

The outputs of the capability analysis process and the technology requirement process formed the basis for the strategic research plan. This plan has been provided as an input to the European Commission security research planning for FP7. In particular SenTRE has proposed that the ESRP should be **security mission driven for the large projects**, validated and orientated by the users involved in the security research network. ESRP should support R&D of **specific security technologies** that are not covered in other FP7 themes as well as **large demonstration projects**. The strategic plan also has concluded that **Human/social factors should be embedded in all key projects**, especially in those with crisis management dimensions. Finally it has recommended that a specific section of ESRP should allow a bottom-up flexible approach.

G.A. SEC4-SA-013400
Total Cost : € 1,056,327
EU Contribution : € 792,245
Starting Date : 1/12/2004
Duration : 14 months

Coordinator:
ASD
Belgium

Contact:
Frederic Perlant
Tel : +32-2-7758130
Fax : +32-2-7758131
E-mail : frederic.perlant@asd-europe.org

Partners:

European Association of Aerospace Industries	Europe
Totalförsvarets forskningsinstitut	SE
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek	NL
Industrieanlagen-Betriebsgesellschaft mbH	DE
QinetiQ	UK
Joint Research Centre – Institute for Protection and Security of the Citizen	Europe
Istituto Affari Internazionale	IT
Foundation for Strategic Research	FR
Austrian Research Centers	AU
Délégation Générale de l'Armement (Centre d'Etude du Bouchet)	FR
Fraunhofer-Gesellschaft	DE
VTT Technical Research Centre of Finland	FI
EADS Astrium	UK
Finmeccanica	IT
Dassault	FR
Sagem	FR
Rheinmetall	DE
EADS	FR
Thales Avionique	FR
Herstal Group	BE
Saab Ericsson Space	SE
BAE Systems	UK

DIRECTORATE GENERAL ENTERPRISE AND INDUSTRY

SECURITY RESEARCH

Preparatory Action for Security Research

(PASR 2005)

SOBCAH SURVEILLANCE OF BORDER COASTLINES AND HARBOURS

The availability of sophisticated surveillance systems is instrumental in reducing the risk of terrorist attacks. The goal of **SOBCAH** is to reinforce the security of the European borders through a well defined process which plans to:

- identify the main threats relevant to "green" and "blue" borders,
- elaborate the most suitable architectural solutions based on the most advanced existing sensors and network technologies,
- execute a proper modelling of the established solution,
- carry out the technology validation of the selected solution, first in the laboratory and then in the port of Genoa (Italy),
- elaborate a consistent Road Map.

The **SOBCAH** demonstration will provide an efficient, real-time, user-friendly, highly automated surveillance system to be deployed in one of the larger European Ports, i.e. an area exposed to terrorist attacks, covering all kind of border security threat.

Current security systems are effective in isolation (i.e. customs, goods tracking, VTS, personnel identification) but are poorly integrated: **SOBCAH** will maximise their effectiveness through innovative application of fusion and high levels of integration.

SOBCAH aims to overcome complex systems engineering issues including:

- Integration of incumbent systems with new technologies,
- Real time situational awareness,
- Data fusion,
- Multiple users with multiple views,
- Multi-level security with segregated access to controlled information,
- Net centric and interoperability.

SOBCAH will be based on an open architecture and will provide decision-makers with an accurate and up to data picture of the surveyed borders/infrastructure. Large volumes of multi-sensor data will be converted into actionable information for tactical operations, introducing a high level of automation to assist operators to recognise threats and to initiate subsequent interventions.

Six scenarios will be analyzed:

1. Demonstration of enhanced container security,
2. Detection of vehicles exhibiting anomalous behaviours
3. Detection of small boats exhibiting anomalous behaviours
4. Underwater attack by drivers
5. Cargo stocking / segregation
6. Biometrics Identification

G.A. SEC5-PR-102100
Total Cost : € 3,007,109
EU Contribution : € 2,010,600
Starting Date : 1/2/2006
Duration : 18 months

Coordinator:
GALILEO AVIONICA S.p.A.
Italy

Contact:
Mario Audenino
Tel : +39 011 9967659
Fax : +39 011 9967604
E-mail : mario.audenino@galileoavionica.it

Partners:

SELEX Sensors and Airborne Systems Ltd.	**UK**
HELLENIC AEROSPACE INDUSTRY S.A.	**EL**
PATRIA Advanced Solutions Oy	**FI**
THALES RESEARCH & TECHNOLOGY LIMITED	**UK**
THALES UNDERWATER SYSTEMS SAS	**FR**
The Netherlands Org. for Applied Scientific Research	**NL**
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.	**DE**
OBR Centrum Techniki Morskiej	**PL**
SELEX Sistemi Integrati	**IT**
INDRA SISTEMAS S.A.	**ES**
RHEINMETALL Defence Electronics GmbH	**DE**
Sistemi e Telematica S.p.A.	**IT**
Software e Tecnologias de Informacao S.A.	**PT**
DELOITTE	**IT**
Autorità Portuale di Genova	**IT**

DIRECTORATE GENERAL ENTERPRISE AND INDUSTRY

SECURITY RESEARCH

Preparatory Action for Security Research

(PASR 2006)

STABORSEC STANDARDS FOR BORDER SECURITY ENHANCEMENT

The enhancement of the European border security level will require a better interoperability of the technologies deployed at borders. The **STABORSEC** supporting activity will identify the technical standards that will support such improvement.

This work will be based on the results produced by the border security group of the European Security Research Advisory Board, and by other European research projects. **STABORSEC** will identify the standards and their full assessments, including the conformity and the evaluation mechanisms, to guarantee an effective interoperability in the domain of borders security.

STABORSEC will produce a detailed prioritised inventory of the standardisation efforts to be deployed to cover appropriate interoperability needs. This output will be public, will guide the upcoming European standardisation activities, and will contribute to the enhancement of border security levels.

Objectives of STABORSEC

The goal of **STABORSEC** is to focus on the inventory of needed standards for stand-alone equipments used for Border Security. **STABORSEC** will not address the interoperability issues at the overall system level (National border security level).

The objectives of the supporting activity can be summarised as follows:

- To consolidate the list of technologies identified for border security, from the results of other European projects, as well as through the direct contribution of end-users participating to the supporting activity.
- To determine the interoperability needs associated to these technologies, and the areas where standards are required.
- To inventory the corresponding existing specification standards and the associated assessment standards when in place.
- To identify the missing assessment standards of the existing specification standards.
- To identify the standards, and their assessment, that must be developed, and provide for each of them a description of its scope and its business justification.
- To propose priorities and a time frame for the implementation of these standards.

These objectives will give a clear view to border authorities that technologies can offer trusted and interoperable services for border security enhancement.

As already mentioned, these objectives are targeting stand-alone equipment, considering that it is a necessary stage before addressing integrated border security. Future research for technology used for border security should use **STABORSEC** results as an integration framework of interoperable characteristics of stand-alone equipments.

G.A. SEC6-SA-210900
Total Cost : € 680,837
EU Contribution : € 452,286
Starting Date : 01/02/2007
Duration : 18 months

Coordinator:
Sagem Défense Sécurité

Contact:
Nicolas Delvaux
Tel : + 33 1 58 11 33 70
Fax : + 33 1 40 70 68 60
E-mail : nicolas.delvaux@sagem.com

Partners:

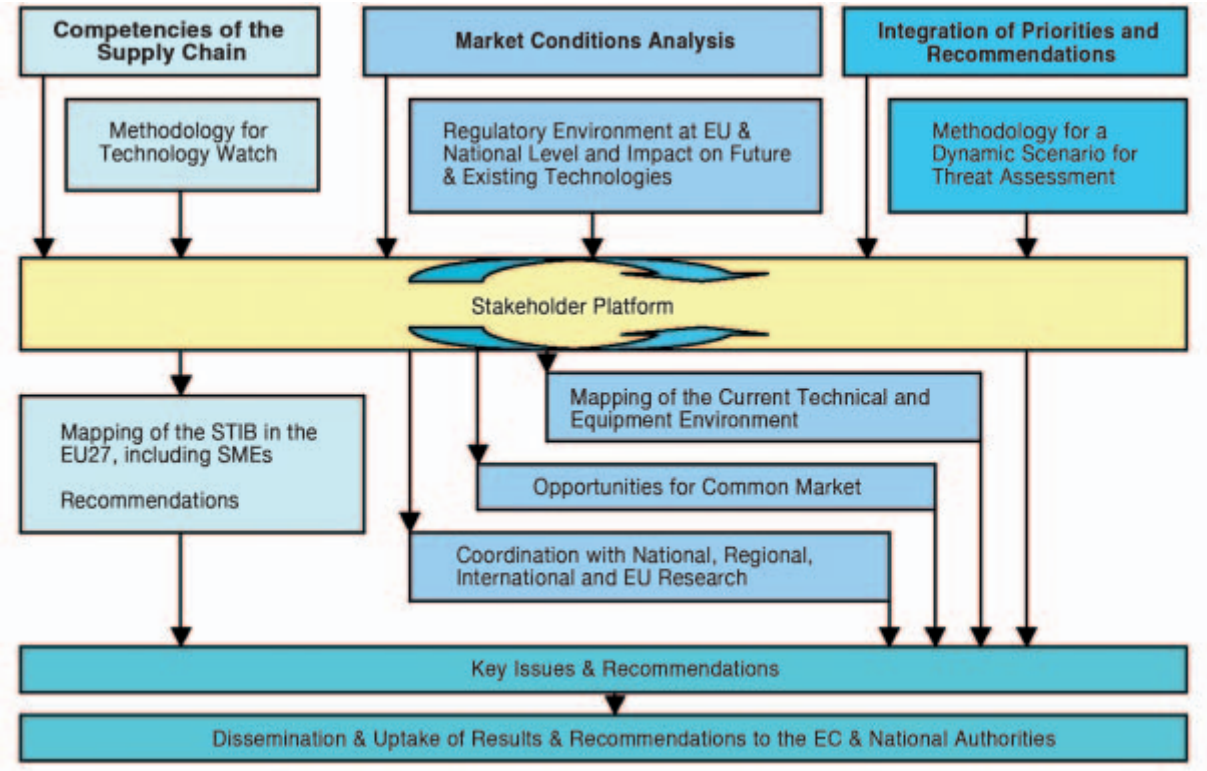
Diehl BGT Defence GmbH & Co. KG	**DE**
Industrial Research Institute for Automation and Measurements	**PL**
Comité Européen de Normalisation	**BE**
Joint Research Centre European Commission	**IT**
Her Majesty's Revenue and Customs	**UK**
MARTEC SA	**FR**
Malta Maritime Authority	**MT**

Preparatory Action for Security Research

(PASR 2006)

STACCATO

STAKEHOLDERS PLATFORM FOR SUPPLY CHAIN MAPPING, MARKET CONDITIONS ANALYSIS AND TECHNOLOGIES OPPORTUNITIES



STACCATO aims at proposing methods and solutions for the creation of a security market and a structured supply chain in Europe. In line with ESRAB recommendations, it will go beyond research needs and gap analysis already undertaken through efforts supported by PASR, by identifying implementation measures. To this end, **STACCATO** will:

- map existing competencies in the EU-27, highlighting particularly the role of the SMEs in order to integrate their innovation potential and examine ways to effectively undertake a coordination of the European Security and Technological Industrial Base (STIB),
- propose a methodology for a technological watch,
- analyse the conditions and propose recommendations to develop a common European Security Equipment Market (ESEM), by identifying common needs, taking into account regulatory issues and coordinating with regional, national, international and EU security research programmes.

These activities will be supported by an enlarged multi-sector stakeholders platform composed of users, industry, SMEs, academia and think tanks of the EU-27 based on the SeNTRE and ESRAB experience.

STACCATO's contributions are:

Supply Chain Involvement (including SMEs and new Member States)

STACCATO's objective is to address the whole supply chain, thus expanding the involvement of science and technology providers to the new Member States as well as to European SMEs.

Technology watch and STIB mapping in EU 27 (including SMEs)

STACCATO aims at assessing the competences of the supply chain in Europe through technology watch and mapping of the equipment and technology environment and the STIB. This analysis will take into account the existing capabilities in the EU 27 and worldwide in order to identify the starting point in Europe and the gaps that need to be filled in order to answer the European needs.

Establishment of stakeholder platforms/network

STACCATO's objective is to include representatives of SMEs and new Member States who have specific capabilities in the existing network of industry, research and technology organizations, think tanks, academia and users.

Coordination with existing or planned research programmes in Europe

STACCATO will identify common research projects or programmes at the national, regional, European and international level and will thus contribute to the synergy and complementarity of FP7 Security research activities.

Promote the creation of a European security equipment and system market

The above mentioned technology watch, STIB mapping and comparison of existing research programmes in Europe will allow for the necessary analysis for the future creation of a common market in the security field.

Priorities and recommendations identification, integration and dissemination

STACCATO will present a methodology for a dynamic scenario for threats and vulnerabilities assessment, technological challenges, priorities and recommendations for a common market for security solutions and support to the European STIB.

G.A. SEC6-SA-214200
Total Cost : € 695,141
EU Contribution : € 502,321
Starting Date : 15/01/2007
Duration : 16 months

Coordinator:
AeroSpace and Defence Industries Association of Europe - ASD

Contact:
Gloria Martini
Tel : +32-2-7770253
Fax : +32-2-7633565
E-mail : gloria.martini@asd-europe.org

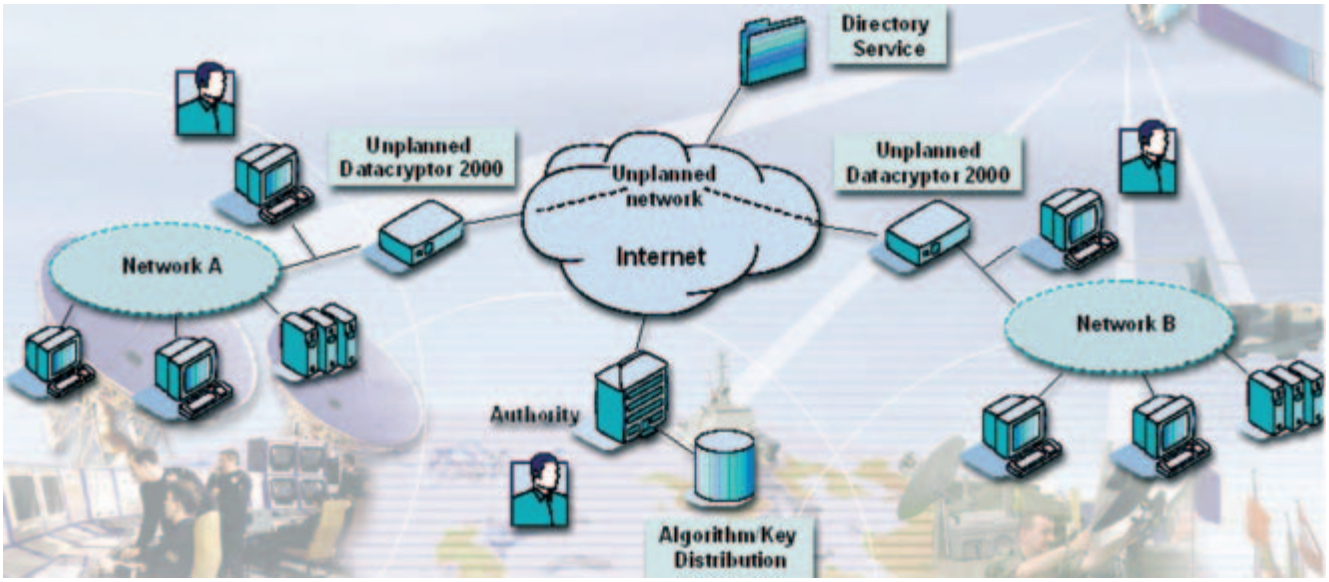
Partners:

Dassault Aviation	FR
Diehl BGT Defence GmBH & Co.	DE
European Aeronautic Defence and Space Company – EADS France	FR
Astrium SAS	FR
Electricité de France - EDF	FR
Finmeccanica SpA	IT
Indra Sistemas S.A.	ES
Sagem Défense Sécurité	FR
Thales Avionics SA	FR
Österreichisches Forschungs- und Prüfzenzentrum Arsenal G.m.b.H	AT
Commissariat à l'Energie Atomique	FR
Swedish Defence Research Agency (FOI)	SV
Industrianlagenbetriebsgesellschaft (IABG)	DE
Netherlands Organisation for Applied Scientific Research (TNO)	NL
Technical Research Centre of Finland (VTT)	FI
Fondation pour la Recherche Stratégique	FR
Istituto Affari Internazionali	IT
European Biometric Forum	IRL
European Association for Bio-Industries	BE
Commission of the European Communities, DG JRC	Europe

Preparatory Action for Security Research

(PASR 2004)

SUPHICE SECURE UNPLANNED PROVISIONING OF HIGH INTEGRITY COMMUNICATIONS



In the EU, national classifications including the design of crypto take precedence over other Member States and the Union itself and EU obligations to protect the rights of the citizen are enacted differently in each Member State.

SUPHICE will prove that;

- A common EU crypto with an unclassified design that is not owned by a member state is suitable for all grades in multiple nations
- The EU's requirements for 'dual certification' can be achieved
- A certified EU algorithm can be made available for requirements up to TOP SECRET

SUPHICE will develop and demonstrate the use of on-demand, secure communications service-provision to deliver unplanned, policy based, reconfiguration of soft-loaded cryptos. This will enable communications consistent with national and international policies for the range of European and National agencies involved (MoD, Coalition, Civil, Intelligence).

Using the above **SUPHICE** will create a working group of EU national IA authorities and propose ways forward.

OVERVIEW OF ACHIEVEMENTS

SUPHICE has advanced the state of the art, achieving progress in a number of key areas:

1. From a situation in which there is no generally accepted algorithm suitable for EU use in a SECRET environment **SUPHICE** has developed requirements, implemented and verified the implementation of the VEGAS algorithm, submitted and completed primary evaluation and certification at SECRET and submitted the implementation for secondary evaluation under the EU's CISPS process.
2. By placing the VEGAS algorithm in an equipment that is of EU origin but that is already certified for national and NATO use by a number of EU member states, **SUPHICE** has demonstrated that the same cryptographic product may be used without contravening EU, national or NATO Policy and Directives.
3. **SUPHICE** has sought to address one of the impediments to a European market for cryptos by delivering the primary and secondary certifications using a product, the overall design of which, with the exception of the EU algorithm, is unclassified and not the property of one nation. This has not been fully achieved due to various procedural issues although major advancements have been made towards mutual certification.
4. **SUPHICE** has demonstrated the on demand policy based deployment of High Integrity communications security using web based techniques including UDDI, WSDL and BPEL.
5. **SUPHICE** has set up and operated the basis of a forum for the National Technical Infosec Authorities of Member States to explore the practical applicability of the approaches to policy based deployment of dynamic systems together with the mechanisms by which these might achieve approval.
6. The concepts and techniques of **SUPHICE** have also been tested at presentations where many nations have confirmed that this approach is relevant and constitutes a significant European advantage over home grown and other overseas products.

For more information: http://www.suphice.com

G.A. SEC4-PR-017100
Total Cost : € 1,938,700
EU Contribution : € 1,350,000
Starting Date : 1/2/2005
Duration : 18 months

Coordinator:
Thales-eSecurity Ltd
UK

Contact:
Peter Davies
Tel : +44(0)1273 384600
Fax : +44(0)1273 384601
E-mail: Peter.Davies@thales-esecurity.com

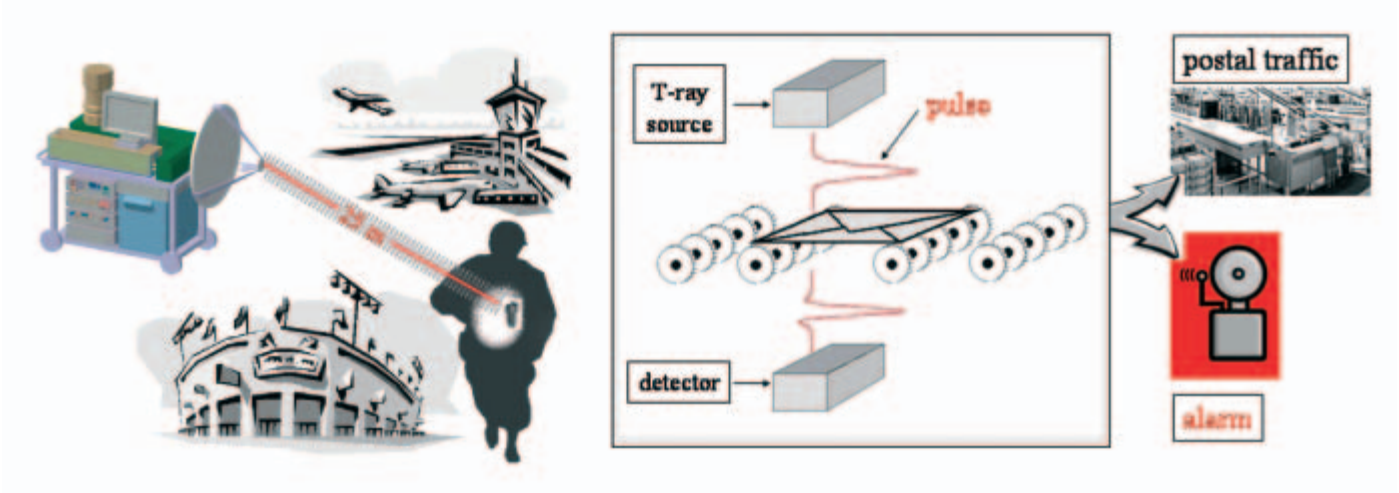
Partners:

Thales Research & Technology (UK) Ltd	**UK**
Ericsson Microwave Systems AB	**SE**
Avensus BV, formerly Evolve Datacom BV	**NL**
Tietoenator Financial Solutions SIA	**LV**
EFT Consultants Polska SP	**PL**
ESL Advanced Information Technology	**AT**
Thales Defence Deutschland	**DE**
L2K Spolencost S.R.O.	**CZ**
Intracom SA Hellenic Telecommunications & Electronics Industry	**GR**

Preparatory Action for Security Research

(PASR 2004)

TERASEC ACTIVE TERAHERTZ IMAGING FOR SECURITY



TERAHERTZ SCANNER FOR STAND-OFF DETECTION AND LETTER INSPECTION

OBJECTIVE

Suicide bombers and anonymous mail attacks have become serious threats world wide. Since X-ray is difficult to apply for personnel scans due to radiation safety regulations, new technologies for remote detection of threats are required. Also fast and reliable technologies are needed to detect threats hidden in mail or similar. Due to their unique properties terahertz (THz) rays offer an alternative inspection method, which can cope with these new challenges.

The goal of this project is to improve homeland security by developing a new technology, which will allow detecting threats, explosives, pathogens and chemicals hidden by a person or inside objects such as letters or luggage. This new technology is based on THz radiation and advanced sensor concepts. In combination with existing sensors this will lead to an increased level of security at public places for example airports.

This new class of sensors will support governments, agencies and public authorities in their effort to protect the public against terrorism.

RESULTS

- Two THz imaging systems were developed and evaluated. One system is for close-by inspection and the other is for stand-off imaging.
- Enabling technology for these systems has been developed.
- Recommendations how to handle ethical aspects have been worked out.
- A roadmap for further development and implementation in security applications has been worked out.
- The partnership between public users, industry, and research, and the competitiveness of European industry in the field of security research has been strengthened.
- Based on these results support for governments, agencies, and public authorities to protect the public against terrorism will be given.

G.A. SEC4-PR-004000
Total Cost : € 2,977,484
EU Contribution : € 2,149,679
Starting Date : 1/1/2005
Duration : 24months

Coordinator:
Deutsches Zentrum für Luft- und Raumfahrt e. V.
Germany

Contact:
Dr. Heinz-Wilhelm Hübers
Tel : +49-30-67055596
Fax : +49-30-67055507
E-mail: Heinz-Wilhelm.Huebers@dlr.de

Partners:

Bundesanstalt für Materialforschung und -prüfung	DE
Crystal Fibre A/S	DK
The Chancellor, Masters and Scholars of the University on Cambridge	UK
Chalmers Tekniska Högskola	SE
EADS Deutschland G. m. b. H.	DE
Jena Optronik G. m. b. H.	DE
Smiths Heimann G. m. b. H.	DE
Scuola Normale Superiore	IT
Technische Universität Carola Wilhelmina zu Braunschweig	DE
Teraview Ltd.	UK
University of Southampton	UK
Diehl BGT Defence GmbH & Co. KG	DE
Joint Research Centre – European Commission	BE

Preparatory Action for Security Research

(PASR 2004)

TIARA TREATMENT INITIATIVES AFTER RADIOLOGICAL ACCIDENTS

Objectives

The purpose of the **TIARA** supporting activity has been to create a European network which may participate in the management of a crisis after the accidental or malevolent dispersal of radionuclides in a public place.

A preview of the state of treatment of contamination by radionuclides in Europe highlighted the following points: a paucity of physicians with experience of treatment, operational issues not anticipated, a requirement for the rationalisation of treatment and research into new treatments.

We have proposed to: provide guidance on dose assessment and efficacy of treatment ; foresee the operational needs for treating persons in the case of mass casualties; monitor scientific and technological development on research into new treatments.

This supporting activity has included physicians involved in decorporation treatment or in other emergencies, experts involved in dose assessment and research studies. The participants, exercising informed discussion with other physicians and scientists, have intended to develop a European network which may disseminate information, contribute to the rationalisation of decorporation treatment and advise on European research programs where deficiencies are apparent.

Description of work

The first action has been to prepare the physicians, inexperienced in the management of radiological exposures and treatment by generating scientific and radiological information in guidance notes.

The second action has been to evaluate the need for stocks of pharmaceutical and the best means to organize distribution of supplies of pharmaceuticals for internal contamination treatment.

The third action has been to identify situations where, in the absence of effective treatment, it is important to describe

current research and prospects for research and development.

For expected effective treatments several factors must be addressed including: firstly, the availability of effective specific treatment for the radionuclides involved, their rapid transport to and distribution of the drugs at the place of the malevolent dispersal and the easy administration of the drug even if numerous people are contaminated.

Results and achievements

TIARA partners have discussed technological and operational issues on dose assessment (leading to effective) treatment decision making, stockpiling of suitable and safe treatments for large scale distribution, needs to develop more effective and further medical treatments and ease and simplicity of administration of drugs to large numbers of persons.

Meetings have been organised on scenario for potential number of persons injured, stockpiles of antidotes, medical centres of reference, cross-border cooperation and other related issues of indeterminable resolution.

A **first report** concerned the evaluation of current treatments for radionuclides. The review highlighted needs of harmonisation between organisations:

Scientific and technological initiatives for research and development in means of decorporation have been explored and described in **a second report**. With the view that it could be necessary to dispose of treatments adapted for large numbers of casualties contaminated.

The efficacy of some current pharmaceutical forms of treatments has to be re-evaluated or improved in human medicine. Important characteristics are to be searched for new forms of DTPA.

Moreover the **TIARA** consortium has established relationships with industrial manufacturers that prepare decorporating drugs and researchers involved in this field.

The **third report** concerned operational issues in relation with national authorities for crisis-specific "scenarios" and stockpiles. The divide between security protection and incident response can only be bridged at the higher levels of governmental planning. Cross-border co-operation is essential and vital.

An important purpose of TIARA has been to constitute a "primary core" embracing the expertise of the relevant organisations within an enlarged European operational network.

The **TIARA** consortium has organised a **Training Course** on Treatment Initiatives After Radiological Accidents aimed to prepare and inform physicians about the management options for radioactively contaminated persons. Answers to medical responders potentially present at the sites of incidents, reception areas and hospitals were given. Participants were issued from emergency organisations, radiation protection services and national authorities, principally from Europe but also from Canada, Israël, Japan and USA.

Finally, a **booklet** of practical guidance on dose assessment was achieved for and distributed during the Training Course. The guide has been intended to facilitate triage and treatment decisions by medical officers, based on radiological dose assessment after potential contamination by inhalation.

G.A. SEC4-SA-014100
Total Cost : € 324,752
EU Contribution : € 171,900
Starting Date : 1/3/2005
Duration : 24 months

Coordinator:
Commissariat à l'énergie atomique (CEA),
DSV/CARMIN
France

Contact:
Florence Menetrier
Tel : +33 1 46 54 98 29
Fax : +33 1 46 54 98 62
E-mail : florence.menetrier@cea.fr

Partners:

Centrum för strålningsmedicin/Karolinska Institutet	SE
Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas	ES
Forschungszentrum Karlsruhe GmbH	DE
Health Protection Agency	UK
Radiation and Nuclear Safety Authority	SF
Institute of Naval Medicine	UK
Statens Räddningsverk (Swedish Rescue Services Agency	SE

Preparatory Action for Security Research

(PASR 2005)

TRIPS TRANSPORT INFRASTRUCTURES PROTECTION SYSTEM

The **TRIPS** project addresses security in mainline, subway or metro railways systems. Enhancing security to improve the protection of railway systems poses many challenges in the mission of protection of the EU citizens against terrorism.

The project will investigate possibilities offered by technology and improved processes to deliver innovative solutions that improve reactions and increase the effectiveness of security measures for the protection of passengers and infrastructure. The recent events in London and in Madrid show how vulnerable public transport systems are to terrorist attacks.

The **TRIPS** project embraces the problem, taking a wide approach, and even though the PASR is limited to a period of 18 months it will include tangible verification of technologies, focused on some critical aspects of railway systems.

The project include railway tracks, railway infrastructure surveillance, detection of explosive inside carriage and coach or other non conventional threats, as well as a communication and protection system architecture design.

Expected Results

- To understand the capability of present technology to reduce the risk of terrorist threat, through analysis, simulation and proof of concept test in selected scenarios.
- To identify gaps from requirements, defining the future efforts in research and development of technology, organisation and standard, taking advantage of End User contribution and relationships with other projects.
- To define design criteria for future infrastructures in order to get a better early recognition of suspicious conditions.
- To show a demonstration of currently available technologies that may be used to improve the protection of railway systems.

G.A. SEC5-PR-101800
Total Cost : € 2,496,614
EU Contribution : € 1,722,270
Starting Date : 1/4/ 2006
Duration : 18 months

Coordinator:
ANSALDO TRASPORTI SISTEMI FERROVIARI SpA
OPE/RES
Italy

Contact:
Vito Siciliano
Tel: +39 010 655 2976
Fax: +39 010 655 2494
E-mail : vito.siciliano@atsf.it

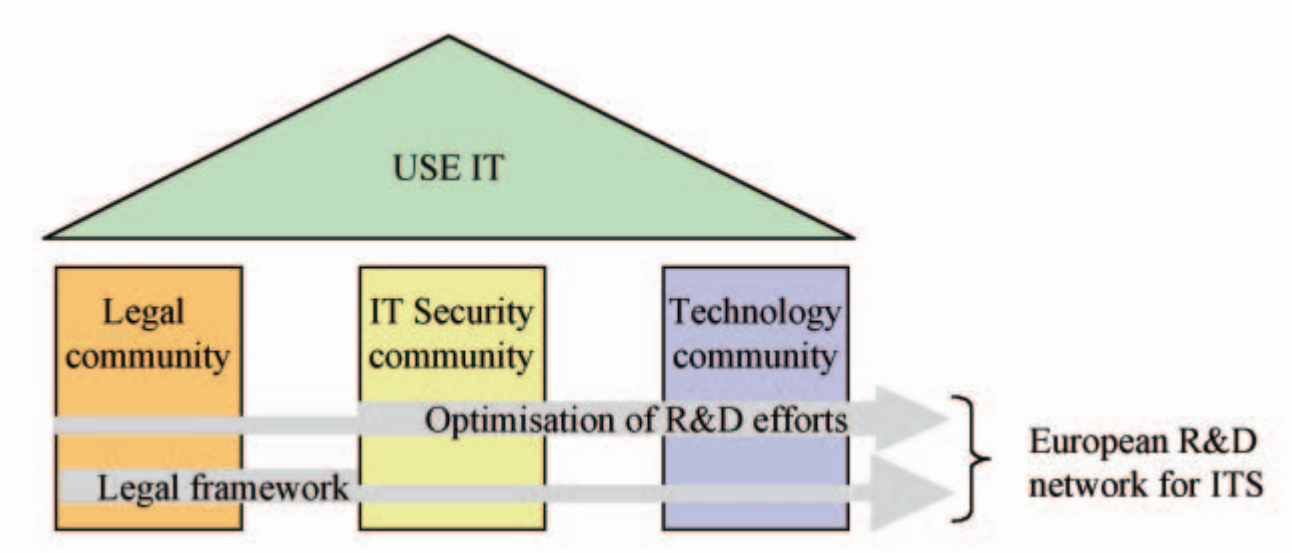
Partners:

BAE SYSTEMS (Operations) Ltd	UK
Diehl BGT Defence	DE
ERICSSON MICROWAVE SYSTEMS AB	SE
IDS INGEGNERIA DEI SISTEMI S.p.A.	IT
PIAP	PL
Rheinmetall Landsysteme GmbH	DE
Sagem Défence Sécurité	FR
SciSys Limited	UK
SENER INGENIERÍA Y SISTEMAS, S.A.	ES
SMITHS DETECTION WATFORD LIMITED	UK
SNCF	FR
THALES SECURITY SYSTEMS SAS	FR
TNO	NL
UNION INTERNATIONALE DES CHEMINS DE FER	FR
VZLU	CZ
ZootFly, LCC	SL

Preparatory Action for Security Research

(PASR 2005)

USE IT USER SUPPLIER EUROPEAN NETWORK FOR INFORMATION TECHNOLOGY SECURITY



The main objective of the **USE IT** supporting activity is to structure the European Research and Development (R&D) community in the Information Technology Security (ITS) domain in order to develop the sharing of heavy resources not dedicated to security issues today: information technology research laboratories, test and evaluation facilities.

This structuring should be done in an appropriated legal context in order to handle properly juridical issues. Or differently said: the supporting activity wants to mix the know-how of the failure analysis, the IT security and the legal communities in order to create a new European environment for information technology security R&D.

The described main objective can be divided into two sub-objectives:

- Optimise R&D efforts: develop shearing of heavy resources between security and non-security domain
- Create a legal framework: develop an appropriated legal context in order to handle properly juridical issues

Expected Results

The results of the supporting activity will be:

1. Report about state-of-the-art in the failure analysis domain
2. Report about state-of-the-art in the security domain
3. Bibliography about European Community and national laws
4. Analysis of European and national laws
5. Model of network charter
6. Synthesis about technical means for sensitive data exchange
7. Report describing network set-up
8. Website
9. Workshop

G.A. SEC5-SA-115200
Total Cost : € 538,756
EU Contribution : € 397,400
Starting Date : 1/2/2006
Duration : 18 months

Coordinator:
Centre National d'Etudes Spatiales DCT/AQ/LE
France

Contact:
Francis Pressecq
Tel : +33 5 61 27 46 69
Fax : +33 5 61 27 47 32
E-mail : francis.pressecq@cnes.fr

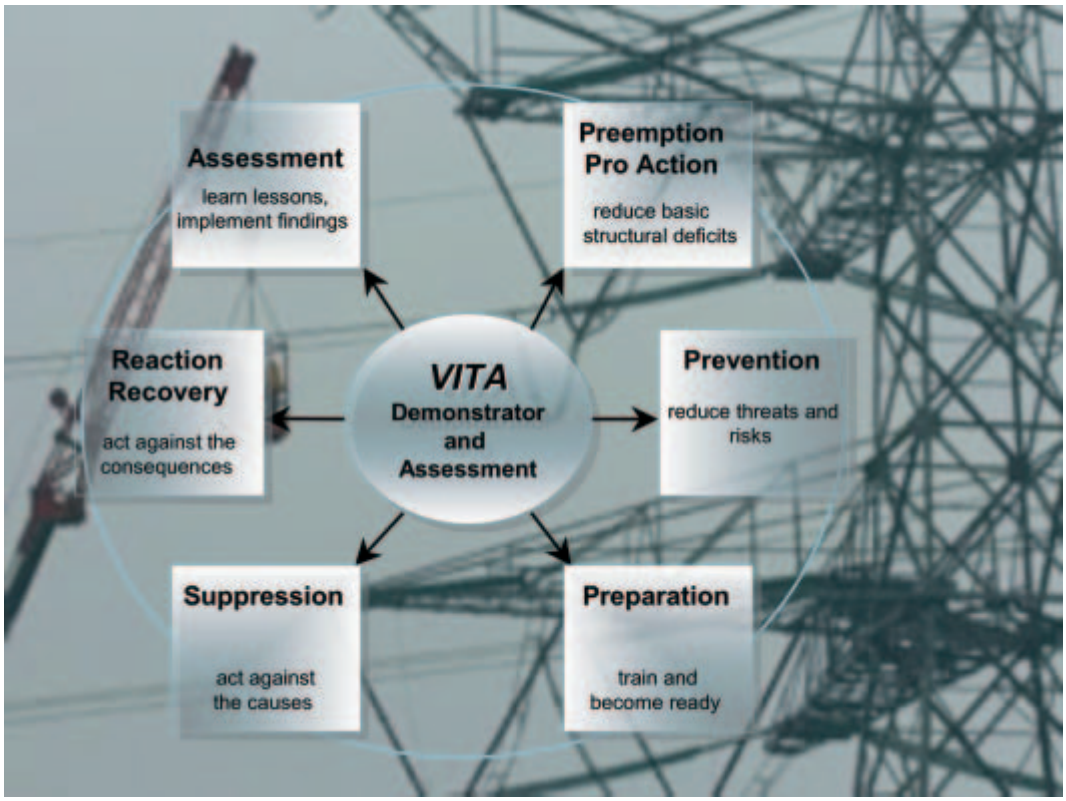
Partners:

Thales Security Systems SAS – CEACI	**FR**
Université Paul Cezanne Aix-Marseille III - CERIC	**FR**
Charles University in Prague	**CZ**
Teletel Telecommunications and Information Technology SA	**GR**
Thales Communications SA	**FR**
Technische Universität Berlin	**DE**

Preparatory Action for Security Research

(PASR 2004)

VITA VITAL INFRASTRUCTURES THREATS AND ASSURANCE



The **VITA** project has delivered assessment on the threats to and assurance and protection of highly networked infrastructures. Most of these are operating trans-nationally, and their disruption is critical to Europe's security, the well being of its citizens, and the functioning of its economy. **VITA** has provided:

1. Methods to raise awareness and the sense of urgency on the need for vital infrastructure protection;
2. An approach on methods, tools and technologies required for the protection improvements;
3. A demonstrator experiment by a scenario exercise with focus on electrical energy.

The initial threat analysis was followed by the proof of concept of highly innovative modelling and simulation, assessment and decision support tools, including human behaviour representation. The results have been disseminated among infrastructure stakeholders, and recommendations for the European Security Research Programme-agenda derived.

Results Status (Dec. 2005)

Threat and Risks: Information has been synthesised into threat taxonomy and an analysis matrix.

Methods and Tools: selection of the methodology criteria, capturing of the format, capturing of available methodologies, the evaluation and recommendations for the demonstrator and experiment have been defined.

Human Factors: methodological approach developed; test-bed equipment for the operator attention monitor demonstrated.

Framework Scenarios: the objectives of the experiment and the associated evaluation criteria have been specified. Two scenarios have been developed; one to be implemented.

Demonstrator Preparation and Experiment

An arrangement of tools and equipment was integrated into the demonstrator:

- DEMOCRIT: Demonstrator and Model for Critical Infrastructure (CI) Analysis
- OTS: Operator Training Simulator of the electrical energy provider
- HBR: Human Behaviour Representation measurement and evaluation tool set.

In a synthetic, however realistic scenario, the phenomena of CIs under severe threats, and the behaviour of systems and organisations involved, were demonstrated. Stakeholder representatives covered all levels of an international CI environment: the individual operators; the management of individual infrastructures; end users like health, rescue and transportation systems; local crisis management teams and cross-border coordination. This was the first experiment of its kind in Europe.

Results, findings and recommendations

The results ranged from detailed technical and operational data up to the high level findings on the required inter-sector cooperation and international crisis management. The recommendations resulting from **VITA**'s analytical and experimental work were presented to and evaluated in the final international project conference. Interested parties in the CI stakeholder community can obtain those results of the project which have been classified as public via http://vita.iabg.eu.

G.A. SEC4-PR-004400
Total Cost : € 1,364,944
EU Contribution : € 1,023,248
Starting Date : 1/1/2005
Duration : 18 months

Coordinator:
IABG InfoCom (IK)
Germany

Contact:
Rudolf Schäfer
Tel : +4989 6088 3061
Fax : +4989 6088 2460
E-mail : schaeferru@iabg.de

Partners:

Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek	**NL**
QinetiQ Ltd	**UK**
Red Electrica de Espana, SA	**ES**
Swedish Defense Research Agency	**SE**
Institute of Biocybernetics and Biomedical Engineering Polish Academy of Sciences	**PL**
Projectmanagement GmbH	**DE**

Preparatory Action for Security Research

(PASR 2006)

WATERSAFE ON-LINE MONITORING OF DRINKING WATER FOR PUBLIC SECURITY FROM DELIBERATE OR ACCIDENTAL CONTAMINATION

The project will harness breakthrough nanotechnologies in sensing and detoxification to protect European citizens against contamination of networked drinking water systems from either terrorist/criminal attack or accidental spillage. The aim is to give maximum protection by developing on-line systems that can be widely deployed for "early warning" and detoxification, which are not available today. New sensing and detoxification methods with tenfold improvement in efficiency will be integrated into combined systems that are intelligent, sensitive, flexible, compact and inexpensive, making them suitable for installation at vulnerable points in water systems. The project joins 4 SME with research groups and a major water company that is responsible for providing water for Brussels, federal and regional governments, NATO, the National Airport, and the EU offices. The project will provide advanced technology to give European companies, many of them SME, competitive advantages in growing strategic world markets.

WATERSAFE will develop the following overall approach:

- Detection: comprehensive on-line sensing; intelligent supervisory control & data acquisition; instant warning signal in response to significant deviations from the norm.
- Response: immediate isolation of the contaminated volume to protect the public; initiation of detoxification methods based on novel high performance technologies that are integrated with the sensing system for operation at the point of detection.

Objectives for PASR 2006

- Assure the security of the populace by integrated detection and detoxification of contaminants added to drinking water distribution systems through terrorist action, sabotage, and accidental occurrences such as industrial chemical spills or other incidents,
- On-line detection of contaminants in drinking water to provide an emergency alert signal at the earliest possible time, therefore preventing distribution to the public,
- Initiation of prompt remedial action, either through an immediate automatic response or mobile treatment unit
- Implementation of the systems at potentially vulnerable points in water distribution systems, in particular local piped distribution systems, water tanks, water towers, and water treatment facilities,
- Integration of a detection and response capability, incorporating new monitoring and detoxification technologies,
- Integration of improved data analysis from existing basic on-line monitoring systems (e.g. pH, conductivity) and other developed technology.

The project Kick-off meeting was held in January 2007, and the research is now well under way.

G.A. SEC6-PR-205000
Total Cost : € 2.565,300
EU Contribution : € 1,923,975
Starting Date : 01/01/2007
Duration : 24 months

Coordinator:
C-Tech Innovation Ltd, UK

Contact:
Neil Wright
Tel : + 44 151 347 2917
Fax : + 44 151 347 2901
E-mail : neil.wright@ctechinnovation.com

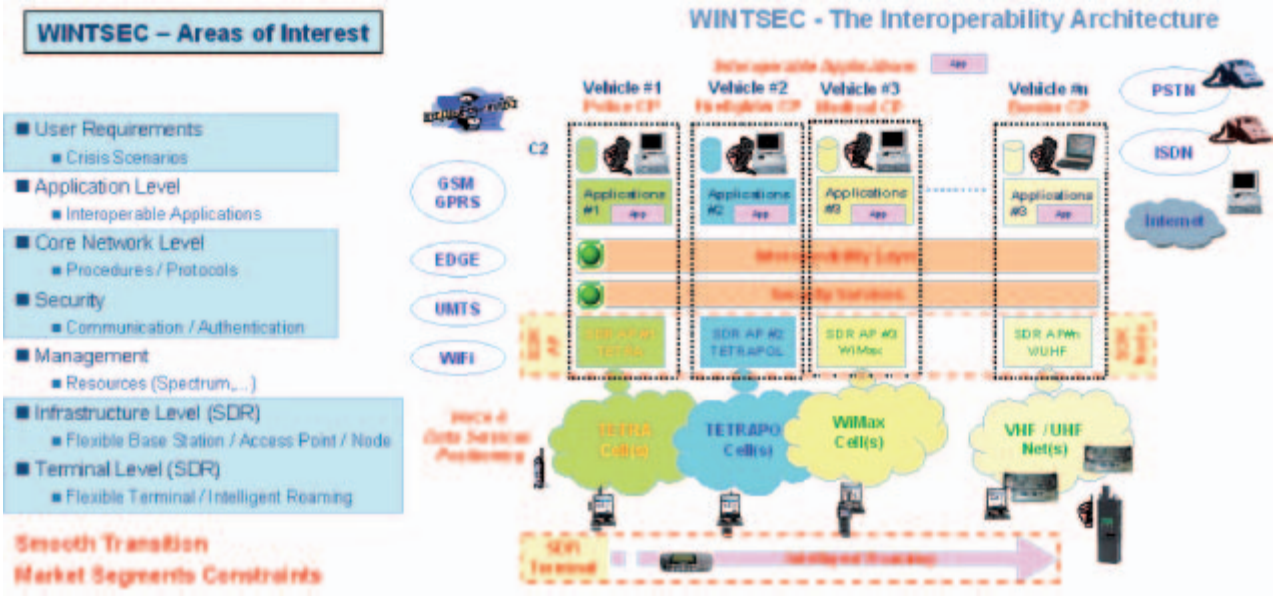
Partners:

Commissariat à L'Energie Atomique	**FR**
Forschungszentrum Karlsruhe GmbH	**DE**
University of Wales Bangor	**UK**
UC Technologies B.V.	**NL**
PW Circuits Ltd.	**UK**
Vivaqua	**BE**
Delta-Umwelt-Technik GmbH	**DE**

Preparatory Action for Security Research

(PASR 2006)

WINTSEC: Wireless INTeroperability for SECurity



OBJECTIVES

With the support of a User Group involving emergency and security End-Users from 6 EU nations, taking into account daily operations, along with complex interventions at national or multinational level, **WINTSEC** explores a mix of complementary solutions to overcome the barriers for wireless interoperability across different security agencies, taking into account the constraints of the security services and the legacy base.

WINTSEC studies the deployment of standardised Internetworking layer at Core Network level and Software Defined Radio (SDR) added value for Base Station and Terminal. **WINTSEC** addresses Information Assurance, elaborates the European "SDR Architectural Framework" and the concepts for the "SDR Certification Environment", explores the impacts of flexible spectrum management for security applications, and illustrates the interoperability concepts elaborated through tangible proof-of-concept demonstrations.

Formed by 22 organisations from 12 nations, **WINTSEC** federates current efforts done in these areas and promotes solutions acceptable by the European actors, paving the way for further standardisation and refinement.

EXPECTED RESULTS

WINTSEC aims at achieving a shared view of interoperability in the public & governmental security (P&GS) domain among a large base of European actors on the following topics

- User Requirements for P&GS Wireless Interoperability in Europe (End User Group)
- System Architecture Definition for Interoperability: Core Network & SDR
- European SDR Architecture Framework (ESRA) Draft Standard
- Initial Concepts for the European "SDR Certification Environment"
- SDR Technological Roadmap

G.A. SEC6-PR-214 300
Total Cost : € 3,600,000
EU Contribution : € 2,700,000
Starting Date : 02/01/2007
Duration : 24 months

Coordinator:
Thales Communications S.A.
FRANCE

Contact:
Dominique Ragot
Tel : +33 (0)1 46 13 24 41
Fax : +33 (0)1 41 30 30 70
E-mail : Dominique.RAGOT@fr.thalesgroup.com

Christian Serra
Tel : +33 (0)1 46 13 23 55
Fax : +33 (0)1 46 13 22 98
E-mail : Christian.SERRA@fr.thalesgroup.com

Partners:

ETHERSTACK	UK
SAGEM	FR
The UNIVERSITY of SURREY	UK
EADS SECURE NETWORKS	FR
ELEKTROBIT LTD	FI
ERICSSON	SE
ROHDE & SCHWARZ	DE
Universität KARLSRUHE	DE
SELEX COMMUNICATIONS	IT
ACORDE	ES
INDRA SISTEMAS S.A.	ES
SKYSOFT Portugal	PT
RADMOR S.A.	PL
INTRACOM DEFENSE ELECTRONICS	GR
TNO	NL
PRISMTECH	UK
FOI	SE
JRC Joint Research Center / IPSC - ISPRA	EU
GMV	ES
AMPER PROGRAMAS	ES
FEE CTU	CZ