AMASS / Autonomous Maritime Surveillance System

RESEARCH **COMPLETED**

Information

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

Coordinator

CARL ZEISS OPTRONICS GMBH
Carl-Zeiss-Straße 22
DE – 73447 Oberkochen
Germany
Contact
Thomas Anderson
Tel: +49 73 64 20 - 2833
Fax: +49 73 64 20 - 3277
E-mail: t.anderson@optronics.zeiss.com
Website:
www.amass-project.eu

Project objectives

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

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

Results

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

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

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

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

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

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

PARTNERS	COUNTRY
Carl Zeiss Optronics GmbH	Germany
Crabbe Consulting Ltd	United Kingdom
Armed Forces Malta	Malta
Instituto Canario de Ciencias Marinas	Spain
Fugro Oceanor	Norway
OBR Centrum Techniki Morskiej	Poland
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)	Germany
IQ-Wireless	Germany
HSF	Czech Republic
University of Las Palmas de Gran Canaria	Spain

ARGUS 3D / AiR GUidance and Surveillance 3D

© Argus - Fotolia.com

Information

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

Coordinator

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

Project objectives

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

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

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

Description of the work

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

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

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

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

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

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

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

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

The project includes:

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

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

Expected results

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

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

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


© CASSANDRA

Information

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

Coordinator

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

Project objectives

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

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

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

Description of the work

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

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

The nine Work Packages are:

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

Expected results

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

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

EFFISEC / Efficient integrated security checkpoints

© Natalia Bratslavsky - Fotolia.com

Information

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

Coordinator

MORPHO
Le Ponant de Paris
27 Rue Leblanc
F-75015 Paris Cedex 15
France
Contact
Krassimir Krastev
Tel: +33 (0) 1 58 11 25 43
Fax: +33 (0) 1 58 11 87 01
E-mail: krassimir.krastev@morpho.com
Website: www.effisec.eu

Project objectives

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

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

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

Description of the work

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

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

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

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

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

Expected results

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

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

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

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

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

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

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

© mattjeacock - iStock

Information

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

Coordinator

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

Project objectives

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

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

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

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

Description of the work

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

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

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

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

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

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

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

Expected results

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

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

GLOBE / Global Border Environment

© Fotolia.com

RESEARCH **COMPLETED**

Information

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

Coordinator

TELVENT INTERACTIVA S.A.
Mr. Manuel Parra
Av. Valgrande, 6
ES-28108 Alcobendas
Spain
Contact
Víctor Alejandro Luaces Bustabad
E-mail:
victor.luaces@telvent.com
Website:
http://globe.ti-projects.com/

Project objectives

The GLOBE project aimed to produce a comprehensive approach to integrated border management in Europe that factors in the internal, border and global aspects of border management. It set out to assess the existing technical, legal, political and societal environment of Europe's borders, and to suggest information management and integration steps to be taken to enhance border security. GLOBE was a 'phase one' research project, whose feasibility results will inform a subsequent 'phase two' large scale demonstration project on border management, to be funded in the near future.

Results

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

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

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

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

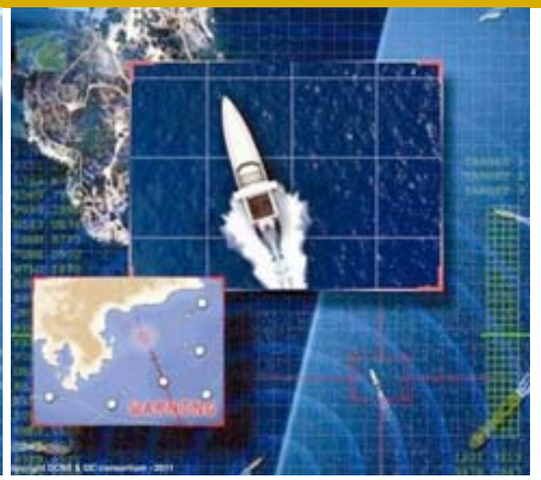
In the area of border surveillance, maritime border monitoring was identified as a priority. GLOBE works to achieve improved situational awareness and assessment via a fusion of surveillance information with information gathered by all relevant monitoring, reporting and information systems – including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

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

© Fotolia.com

PARTNERS	COUNTRY
Telvent Interactiva S.A.	Spain
Amper Sistemas S.A.	Spain
GMV Aerospace and Defence, S.A	Spain
Instituto Nacional de Técnica Aeroespacial	Spain
Altran Technologies	France
SETTCE	Slovenia
Econet Polska sp. z.o.o.	Poland
Eurosense Belfotop N.V.	Belgium
Skysoft Portugal, Software e Tecnologias de Informaçao, S.A.	Portugal
CES vision Ltd.	Hungary
PRIO	Norway
Empresa de Serviços e Desenvolvimento de Software, S.A.	Portugal
Cogent Systems GMBH	Austria
CIAOTECH Srl (CIAOTECH)	Italy
Fundación Tecnalia Research & Innovation (TECNALIA)	Spain

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



Information

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

Coordinator

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

Project objectives

The I2C new generation of maritime surveillance system must allow:

» Permanent and all weather coverage of border maritime areas;

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

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

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

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

Description of the work

The tasks to perform in the I2C integration project are:

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

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

To do so:

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

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

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

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

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

Expected results

The main outcomes of I2C are:

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

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

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

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

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

© Netfalls - Fotolia.com

RESEARCH **COMPLETED**

Information

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

Coordinator

TSB INNOVATIONSAGENTUR BERLIN GMBH / BEREICH FAV
Fasanenstr. 85, 10623
Berlin
Germany
Contact
Markus Podbregar
Tel: +30 46302 579
Office: +30 46302 563
Fax: +30 46302-588
E-mail: mpodbregar@fav.de
Website: www.imcosec.eu

Project objectives

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

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

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

Results

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

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

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

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

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

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

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

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

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

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

© Kaarsten - istockphoto.com

RESEARCH **COMPLETED**

Information

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

Coordinator

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

Project objectives

The LOGSEC project had the following three main objectives:

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

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

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

Description of the work

The LOGSEC project team consisted of organisations with in-depth experience in European and global supply chain security research and technology analysis and partners representing a broad set of European shippers and logistics operators and customs administrations. Key technologies and procedural aspects covered by the project include: container and goods/inventory, authentication, traceability, inspection and monitoring technologies; risk assessment systems and models; Information transfer systems; Intermodal transport security; modernisation of customs procedures; protection of supply chain infrastructure. User requirements and data collection steps included:

» literature and project reviews,

» end-user expert interviews,

» user surveys, and

» user workshops.

Results

The LOGSEC project delivered a roadmap for a large scale demonstration project in European logistics and supply chain security, characterised by adequate security for the benefit of business and governments, on low time-delay and other cost implications. LOGSEC identified the most relevant/promising research areas and research gaps, to be addressed in a possible follow-up demonstration project. An instrumental part of the roadmap project was to build a basis for future metrics necessary to evaluate supply chain and security performance and to monitor supply chain vulnerabilities.

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

OPARUS / Open Architecture for UAV-based Surveillance System

RESEARCH **COMPLETED**

Information

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

Coordinator

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

Project objectives

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

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

Results

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

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

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

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

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

» cost effective surveillance for "typical" border scenarios;

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

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

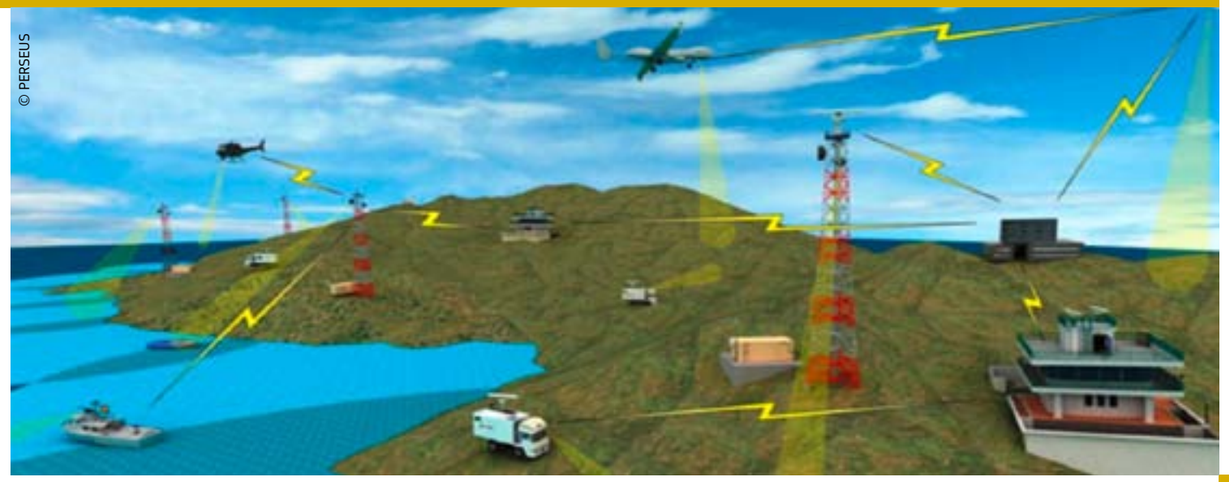
» the ability of companies to share different parts of a complex system which distributes development costs and risks on a broad basis – an advantage that would foster the development of industrial co-operation similar to the Airbus model.

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

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

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

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



© PERSEUS

Information

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

Coordinator

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

Project objectives

The PERSEUS scope is three-fold:

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

Description of the work

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

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

Expected results

PERSEUS will deliver:

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

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

SEABILLA / Sea border surveillance

© Colette - Fotolia.com

Information

Grant Agreement N°
241598
Total Cost
€15,558,125.80
EU Contribution
€9,841,603.55
Starting Date
01/06/2010
Duration
45 months

Coordinator

SELEX SISTEMI INTEGRATI SPA
Via Tiburtina km 12,400,
00131 Roma
Italy
Contact
Salvatore RAMPINO
Tel: +39 06 4150 2407
Mobile: +39 3357389405
Fax: +39 06 41502694
E-mail:
srampino@selex-si.com
Website: www.seabilla.eu

Project objectives

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

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

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

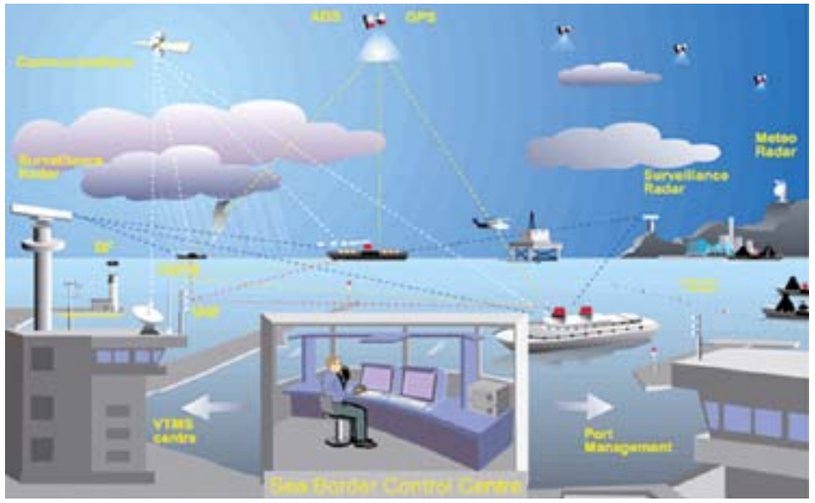
Description of the work

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

» for fighting drug trafficking in the English Channel;

» for addressing illegal immigration in the South Mediterranean; and

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



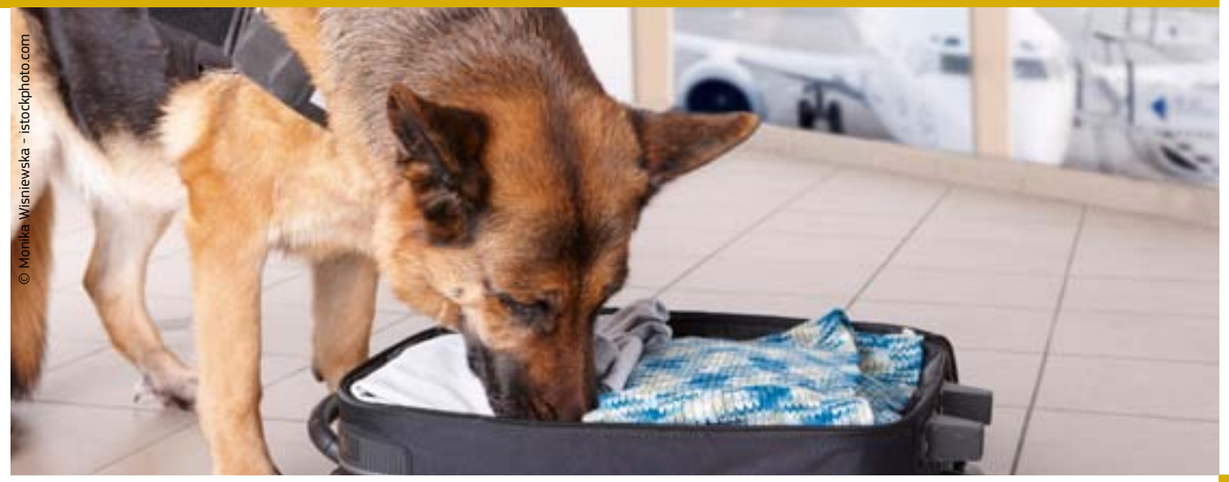
© Seabilla

Expected results

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

PARTNERS	COUNTRY
SELEX Sistemi Integrati SPA (SSI)	Italy
Alenia Aeronautica	Italy
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT)	Italy
BAE Systems (Operations) Ltd (BAES)	United Kingdom
Correlation Systems (CorrSys)	Israel
Cassidian S.A.S. (EADS DS)	France
Empresa de Serviços e Desenvolvimento de Software SA (EDISOFT)	Portugal
Eurocopter España (ECE) (ECE)	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Holland Institute of Traffic Technology BV (HITT Traffic)	The Netherlands
Indra Espacio S.A. (IE)	Spain
Indra Sistemas S.A. (INDRA)	Spain
European Commission - Joint Research Centre (JRC)	Belgium
Mondeca S.A. (Mondeca)	France
Sagem Défense Sécurité (SAGEM)	France
Space Applications Services N.V./S.A (SpaceApps)	Belgium
Thales Alenia Space Italia S.p.A. (TASI)	Italy
Thales Defence Deutschland GmbH (TMSS)	Germany
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)	The Netherlands
Telespazio S.p.A. (TPZ)	Italy
Thales Systèmes Aéroportés S.A. (TSA)	France
TTI Norte (TTI)	Spain
University College London (UCL)	United Kingdom
Universidad de Murcia (UMU)	Spain
University of Portsmouth Higher Education Corporation (UoP)	United Kingdom
Thales Alénia Space France (TASF)	France
Thales Communications & Security S.A. (TCF)	France

SNIFFER / A bio-mimicry enabled artificial sniffer



© Monika Wisniewska - istockphoto.com

Information

Grant Agreement N°
285203
Total Cost
€ 4,837,982.97
EU Contribution
€ 3,493,820.72
Starting Date
01/02/2012
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Diamond Sensors Laboratory
Centre d'Etudes de Saclay
91191 Gif-sur-Yvette,
France
Contact
Emmanuel Scorsone
Tel: +33 1 6908 6934
Fax: +33 1 6908 7819
E-mail:
emmanuel.scorsone@cea.fr
Website: Not available
(due month 3/end of April)

Project objectives

The SNIFFER project proposes a highly innovative one-stop shop approach to complement sniffer dogs and leverage their capabilities. This approach is based on state-of-the-art technologies centred on a new generation of olfactory biosensors. The SNIFFER devices to be developed integrate sampling, pre-concentration and pre-treatment with bio-mimicry, synthetic diamond sensor technology and multi-parametric training software. This will enable the detection of odours arising out of security threats which may occur in a panel of border security applications, such as the detection of illegal substances carried by people and in suitcases (open or on a luggage belt) and cars or the detection of hidden people in containers.

Description of the work

The SNIFFER project will be pulled and driven by concrete usage cases corresponding to major border security applications of artificial sniffing. To make sure that the SNIFFER project is efficiently managed, the consortium will work against common global milestones which structure the project in a set of V1 solutions (at midterm) and V2 solutions (at the end of the project).

A first work package will define the usage cases and corresponding metrics, validate them at midterm and at the end of the project and cover the societal and ethical implications of introducing SNIFFER technology in the respective usage contexts.

A second work package will deal with the integration and testing of different sub-systems, namely the sampling, pre-concentration and pre-treatment of target analytes module developed in a third work package, as well as the multisensory array developed in a fourth work package.

Multi-parametric training software will also be adapted in order to cover the broad range of different odours targeted by the SNIFFER project.

A whole work package will also be dedicated to odorant proteins engineering which is one of the core technologies of the SNIFFER project along with the innovative diamond based transducers.

Finally another work package will investigate different aspects of self-diagnostics for artificial sniffers.

SNIFFER is a two-step incremental project. A first version of the SNIFFER devices will be developed to answer the needs expressed by the users at the beginning of the project (month 1 to 23). A second version will then be consolidated taking into account the feedback given by the users on V1 (month 24 to 36).

Expected results

SNIFFER devices cover the variety of border security situations in which dogs are used today. Their capabilities will allow security forces to operate 24/7, while saving the use of real dogs for cases in which they can potentially make a difference.

Thanks to the SNIFFER devices, border security, especially at airports, will be significantly enhanced as regards illegal trafficking of all kinds (drugs, tobacco, illegal immigration…) as well as terrorist acts (thanks to explosive detection).

PARTNERS	COUNTRY
Commissariat à l'énergie atomique et aux énergies alternatives (CEA-LIST/LCD)	France
The University of Manchester (UNIMAN)	United Kingdom
Ministère de l'Intérieur - Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure (ST(SI)²)	France
Association pour la Recherche et le Développement des Méthodes et Processus industriels (ARMINES)	France
EADS Deutschland GmbH – Innovation Works (EADS)	Germany
Ecole Polytechnique Fédérale de Lausanne (EPFL)	Switzerland
Centre for Science, Society and Citizenship (CSSC)	Italy
The University of Padua (UNIPD)	Italy
Chambre de Commerce et d'Industrie de Paris (ESIEE)	France
GTP Technology (GTP)	France
TraceTech Security (TTS)	Israel
3D General Aviation Applications SA (3DSA)	Greece
Israel National Police (INP)	Israel
ARTTIC Belgium (ART)	France

SNIFFLES / Artificial sniffer using ion trap technology

© WAGTAIL

Information

Grant Agreement N°
285045
Total Cost
€ 5,226,007.41
EU Contribution
€ 3,493,625.00
Starting Date
01/01/2012
Duration
36 months

Coordinator

TWI LTD
Commercial Group
Granta Park
Great Abington. CB21 6AL.
Cambridge.
United Kingdom.
Contact
Debbie McConnell
Tel: +44 (0)1223 899000
Fax: +44 (0)1223 890952
E-mail:
debbie.mcconnell@twi.co.uk
Website: www.twi.co.uk

Project objectives

The goal of the SNIFFLES project is to develop a Linear Ion Trap Mass Spectroscopy (LIT MS) based device that has a mass range larger than other comparable MS techniques. Additionally, methods for miniaturisation and modularisation will be applied to allow reduced vacuum demand and upgradeability. Miniaturisation will be made possible through improved designs based on results from modelling, implementation of novel manufacturing techniques and improvements in the MS drive electronics and vacuum system.

The objectives of the SNIFFLES system are to be able to detect weapons, drugs and hidden persons at border crossings; identifying in parallel the elemental, molecular or biological composition all at a high speed of detection.

To ensure the suitability for real world applications the system will have a stand-off capability whilst being a complementary technique to that of sniffer dogs.

Description of the work

The areas of work that will: be undertaken within the project will be carried out in 3 phases:

» Phase 1 will concentrate on project road mapping that will provide a holistic overview of the gas sensor device development, within the context of creating a robust and reliable artificial sniffer. This will specify the device performance and enable all of the individual technical sub-system activities to be undertaken. After this initial output, it will continue to run, focussing on forming a structured approach to define the operational procedures of the final device;

» Phase 2 will be the technical development of each of the sub-systems that will be implemented into the artificial sniffer. Ion trap development will ensure a device with high sensitivity whilst using novel manufacturing techniques to create a device with a small footprint and small cost.

The electronic control unit development will ensure that the ion trap functions to its highest specification and the measurements taken are accurate and reliable.

The vacuum sub system will be technologically advanced to enable the high performance of the system whilst ensuring that the whole system can be contained within the smallest footprint possible.

The operating conditions of the linear ion trap will be adjusted to confirm that each stage of the mass spectrometer is operating at its highest performance with the best sensitivity and resolution. The sample inlet operation will be designed, enabling the correct operation of the device whilst sampling the multiple substances required.

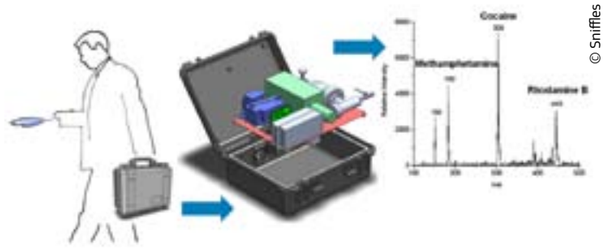
The end stage of phase 2 is the system integration to ensure that each sub system is working in synchronicity with its partners;

» Phase 3 is where the device will undergo its testing and validation program so that the SNIFFLES device is optimised for border control points. The testing will integrate a number of development stages including feedback from live field testing trials.

Expected results

The main outcome of the project will be a device that can work in collaboration with existing sniffer dog teams at border check points; this includes high speed detection and continuous monitoring of air and surfaces to prevent transport of illegal substances at crossing points on land and at airports and seaports.

The overall device will be a portable system aided by the integration of the vacuum system using new materials.



© Sniffles

PARTNERS

TWI Ltd (TWI)
The University of Liverpool (UOL)
Université Aix-Marseille 1 Provence (UdP)
DSM R&D Solutions BV (DSM)
Q Technologies Ltd (Qtec)
SAES Getters S.p.A (SAES)
Envisiontec GMBH (ENV)
Xaarjet AB (XAAR)
Wagtail UK Ltd (WAG)

COUNTRY

United Kingdom
United Kingdom
France
Netherlands
United Kingdom
Italy
Germany
Sweden
United Kingdom

SUPPORT / Security UPgrade for PORTs

© Herbert Rubens - Fotolia.com

Information

Grant Agreement N°
242112
Total Cost
€14,629,279.69
EU Contribution
€9,920,607
Starting Date
01/07/2010
Duration
48 months

Coordinator

BMT GROUP LTD
Research Directorate
Goodrich House, 1 Waldegrave Road
TW11 8LZ, Teddington
UK
Contact
Jenny Gyngell
Tel: +44 (0)1933 625958
Mobile:
+44 (0)7717 803105
Fax: +44 (0)1933 625958
E-mail:
jgyngell@bmtmail.com
Website:
http://www.support-project.eu/

Project objectives

The primary project objective is to support the principal stakeholder groups involved in the security of European main sea and/or inland ports to build distributed cooperative security systems. SUPPORT will facilitate optimised interchange of surveillance and administrative information as well as threat alerts between port stakeholders, thus enabling cost effective, multiple use of available data in tailored decision support systems.

SUPPORT solutions will: provide integrated state-of-the-art surveillance/security systems for border control; assist port security operators in decision making; take into account the port's organisational structure and operational modalities; and ensure that differing legal and regulatory constraints and standards for security are met in a cost effective manner.

Description of the work

The work programme will start with requirements analysis including Gap and Threat Scenario Analysis, Regulatory and Stakeholder Analysis and Security Technology Assessment and Forecasting. The output from these activities will direct the development of Generic Models for EU Ports Security. These will be validated by operational experts from the SUPPORT participants and will be used to support a 'European standardised approach for port security information exchange and training'. The Generic Models will be installed in the SUPPORT Models Repository and will be used to produce service registries for specific ports. These registries will support their specific circumstances and will contain the information they wish to share with whom on a peer-to-peer basis. Each peer will have its own (possibly unique) view on the total security information and will hence need its own tailored decision support system. The Generic Models will also provide the basis for assessing existing systems and simulating appropriate upgrade solutions.

Evaluation will be undertaken in terms of both improvements in security performance and cost benefit analysis.

Two full scale demonstrators have been planned, one to represent a state of the art situation and the second to represent typical conditions in European ports.

These demonstrators will simulate a full scale installation of the SUPORT Platform with integration with existing systems facilitating measurements of the impact on both the security and efficient operation of the port.

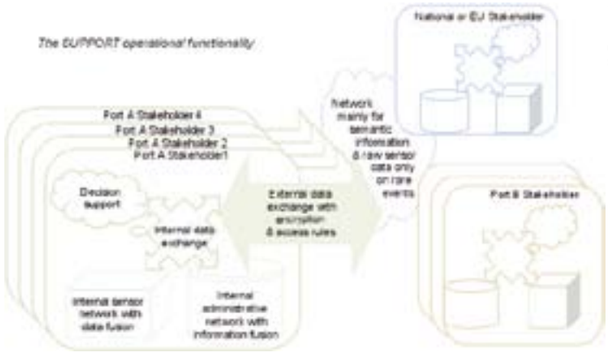
Expected results

SUPPORT will deliver:

» 'validated' generic port security management models (capturing reusable state-of-the-art and best practices) that can be customised for specific ports;

» training and open standards based tools to aid security upgrade in EU ports.

These will be complementary to, and usable by, other EU projects and initiatives.



© Support

PARTNERS

BMT Group Ltd. (BMT)
Totalförsvarets Forskningsinstitut (FOI)
Securitas (Securitas)
Technical Research Centre of Finland (VTT)
MARLO (Marlo)
INLECOM Systems (ILS)
MARINTEK (Marintek)
Nautical Enterprise (NECL)
STENA (Stena)
eBOS Technologies (eBOS)
University of Innsbruck (UIBK)
Cargotec Port Security (CA)
Maritime Administration of Latvia (MAL)
INRIA (Inria)
MARAC Electronics (ME)
Port of Piraeus (PPA)
EUROPHAR - EEIG Port of Valencia - Marseille – Genoa (PV)
Gemeente Amsterdam (PA)
Stichting Ecoports (EP)

COUNTRY

United Kingdom
Sweden
Sweden
Finland
Norway
United Kingdom
Norway
Ireland
Sweden
Cyprus
Austria
Finland
Latvia
France
Greece
Greece
Spain
The Netherlands
The Netherlands

TALOS / Transportable autonomous patrol for land border surveillance system

© TALOS

RESEARCH **COMPLETED**

Information

Grant Agreement N°
218081
Total Cost
€19,878,692
EU Contribution
€12,898,332
Starting Date
01/06/2008
End Date
31/05/2012

Coordinator

PRZEMYSŁOWY INSTYTUT AUTOMATYKI I POMIARÓW
Aleje Jerozolimskie 202
PL – 02486 Warsaw
Poland
Contact
Mariusz Andrzejczak
Tel: (48 22) 874 01 99
Fax: (48 22) 874 01 13
E-mail: mandrzejczak@piap.pl
Website: www.talos-border.eu

Project objectives

TALOS is an innovative, Adaptable Land Border Large Area Surveillance System, based on transportable surveillance integrated with rapidly deployable, mobile, unmanned ground and air vehicles, which will address new challenges of external land borders of the enlarged European Union.

The TALOS project proposes to develop an integrated, adaptable land and large area (including devastated environment) surveillance system that:

» Is capable of Detecting, Locating, Tracking and Tracing:

- individuals;
- vehicles;
- hazardous substance.

» Combines remote and autonomous platforms featuring:

- multi sensor data fusion (including biological and chemical);
- active imaging;
- data Fusion;
- command Control & Communication.

The TALOS project's main objectives are as follows:

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

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

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

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

» To promote the usage of the TALOS system concept all over Europe, and to contribute to the ongoing efforts of their standardization in Europe;

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

The main TALOS innovation covers:

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

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

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

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

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

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

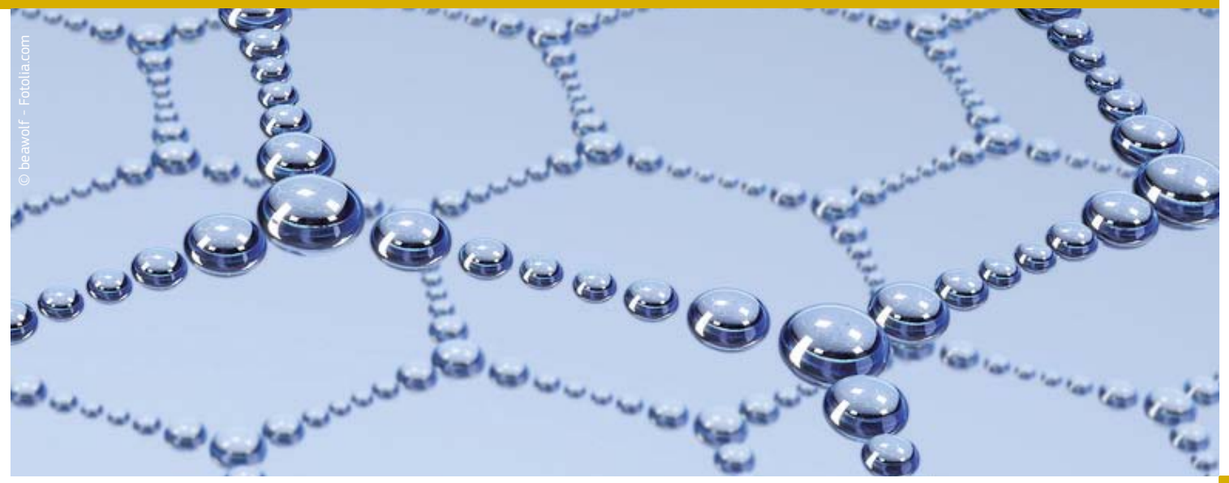
» Usage of "green" energy – in remote locations (where it is impossible to connect to standard power lines) the energy will be drawn from natural sources e.g. by means of solar panels (sunny area), wind towers (windy area), water wheels (near rivers).

Results

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

PARTNERS	COUNTRY
Przemysłowy Instytut Automatyki i Pomiarów	Poland
ASELSAN Elektronik Sanayi ve Ticaret A.S.	Turkey
European Business Innovation & Research Center S.A.	Romania
Hellenic Aerospace Industry S.A.	Greece
Israeli Aerospace Industries	Israel
ITTI Sp. z o.o.	Poland
Office National d'Etudes et de Recherches Aérospatiales	France
Smartdust Solutions Ltd.	Estonia
Société Nationale de Construction Aérospatiale	Belgium
STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.	Turkey
Telekomunikacja Polska SA	Poland
TTI Norte S.L.	Spain
Technical Research Center of Finland	Finland
Politechnika Warszawska	Poland

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



Information

Grant Agreement N°
242352
Total Cost
€11,497,567.53
EU Contribution
€7,999,182.55
Starting Date
01/05/2010
Duration
36 months

Coordinator

COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Centre de Saclay- Bât 476
F91191 Gif-Sur-Yvette Cedex
France
Contact
Géraud Canet
Tel: +33 1 46 54 82 59
Fax: +33 1 46 54 75 80
E-mail: geraud.canet@cea.fr
Website:
http://www.virtuoso.eu/

Project objectives

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

» Improve the situational awareness of those organisations and individuals charged with securing Europe's borders;

» Help anticipate risks such as terrorism, illegal migration and the trafficking of goods and people using OSINF;

» Create the kernel of a pan-European technological platform for the collection, analysis and dissemination of open source information, thus ensuring greater interoperability among European actors involved in border security;

» Provide the tools for crisis management response if anticipation fails or in the event of a rupture scenario.

Description of the work

The VIRTUOSO Project places considerable importance on the involvement of end-users. The project will be developed incrementally in response to their specific requirements.

During the first end-user requirements phase, a state-of-the-art set of tools will be demonstrated to help end-users better understand the utility of the VIRTUOSO toolkit.

Three versions of the VIRTUOSO Toolkit will be delivered:

» *VIRTUOSO-V0:* A very basic version of the framework, integrating basic functions and demonstrating its potential;

» *VIRTUOSO-V1:* A first version of the framework integrating some operational functions;

» *VIRTUOSO-V2:* A second version of the framework with all operational functions adapted and/or developed.

Work Packages:

» *WP0:* Management;

» *WP1:* End-users requirements (10 workshops organised with end-users);

» *WP2:* Architecture and infrastructure tools;

» *WP3:* Privacy, ethical and legal aspects;

» *WP4:* Data acquisition;

» *WP5:* Processing;

» *WP6:* Knowledge management;

» *WP7:* Decision support and visualization;

» *WP8:* Integration and demonstration;

» *WP9:* End-Users validation (10 workshops organised with end-users);

» *WP10:* Dissemination.

Expected results

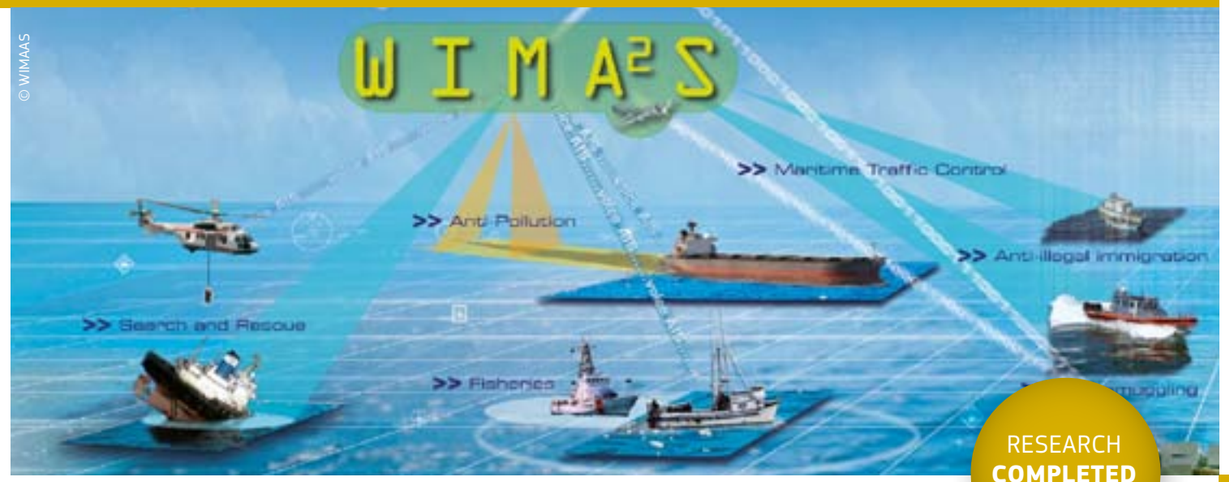
This seamless OSINF platform will aggregate, in realtime, content from the internet, leading subscription providers, and broadcast media. This content will be filtered and analysed using text mining and other decision support technologies to improve situational awareness and provide early warning to end-users.

The project's deliverables include a demonstrator of the VIRTUOSO toolkit (one that integrates various information services and intelligence applications) and full documentation on the platform itself.

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

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

WIMAAS / Wide maritime area airborne surveillance



© WIMAAS

RESEARCH **COMPLETED**

Information

Grant Agreement N°
217931
Total Cost
€4,001,123
EU Contribution
€2,737,169
Starting Date
01/12/2008
End Date
30/11/2011

Coordinator

THALES SYSTEMES AEROPORTES S.A
25 Avenue Gustave Eiffel
FR-33608 Pessac
France
Contact
Gilles JURQUET
Fax: +33(0)5 - 57 26 71 60
E-mail: gilles.jurquet@fr.thalesgroup.com
Website: www.wimaas.eu

Project objectives

WIMAAS aimed to assess the potential cost reduction, efficiency and enhanced border control benefits for European maritime domain surveillance to be gained via a large-scale integration of unmanned or otherwise remotely piloted airborne vehicles. The project explored the application of such systems for tracking illegal immigration, illegal fishing, smuggling, pollution and terrorist threats.

The final outcome aimed to develop simulation models based on operational scenarios, innovative concepts and technologies for unmanned systems, in-flight experiments, a detailed cost benefit analysis and, finally, a roadmap for the wider use of unmanned aerial vehicles (UAVs), including R&T priorities and future program suggestions.

Results

The primary outcome of the project was the exploration of a future "system of systems" (SoS) architecture incorporating UAVs to produce complete maritime domain awareness.

The first step of the project was to gather and analyze the future needs of potential End-Users in charge of maritime surveillance on European borders. End-user consultations included 10 national and military authorities, plus Frontex. This led to the generation and simulation of scenarios such as drug trafficking between North Africa and Spain, illegal fishing in the Aegean, illegal immigration between Libya and Italy and a theoretical terrorist hijacking in the strait between Cyprus and Turkey.

WIMAAS was considered as a generic system including all airborne platforms (PF) in the maritime 3rd dimension. The notion of system covers the platforms, their sensors, airborne or ground Command and Control system to coordinate PF tasks, to exploit data before transmission to SoS, and the communication system enabling data exchange between platforms with crews, and between PF and SoS.

Further research aimed to develop the multi-sensor concepts required to integrate UAVs into existing maritime domain awareness processes.

On board processing and fusion is analysed for observation payloads to reduce data throughput transmission, to improve levels of automation, to decrease the amount of exchanged data and to reduce data link bandwidth, paving the way for miniaturisation of the airborne mission segment.

The Sensor and data fusion concepts on the ground address the definition of a solution to reach a level of situation awareness, which allows the timely detection and prevention of events threatening maritime security and the environment. The challenge is rather to process and represent them in an intelligent and meaningful way to give sufficient information support to human decision-makers.

Dynamic tasking provides an aid to decide the path of aircraft in the area of interest. The issue is to dynamically plan the path of the airborne platform in order to comply with the mission objective (reach in a specified time an observation position) periodically updated by real time detection or objects of interest generated by its own sensor or by an external sensor. An algorithm has been developed and experimented.

A crew concept was also developed to assess the personnel requirements and workload management needed to operate UAVs from a central base station. An optimal mission length and crew size was aggregated from a series of mission scenarios.

A communication study has defined an innovative architecture for complete data communications between air vehicles and the ground segment, introducing innovative access techniques and interfaces.

The project concludes that there is no single multi-purpose UAV platform capable of covering every altitude and maritime environment. A multi-platform category system-of-systems would be required.

To facilitate further research into this, WIMAAS concluded with a cost estimate based on varying degrees of mission intensity and the use of multiple (up to 10) types of UAV platforms. These cost estimates, excluding training and maintenance expenses, can now form the basis of a policy assessment for implementing a wide maritime area surveillance network based on UAVs.

PARTNERS	COUNTRY
Thales Systemes Aeroportes S.A	France
SELEX GALILEO	Italy
Dassault Aviation	France
SENER Ingeneria y Sistemas	Spain
Totalförsvarets Forskningsinstitut (FOI)	Sweden
Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer-IITB)	Germany
European Commission - Joint Research Centre (JRC)	Belgium
Air Force Institute of Technology	Poland
EUROSENSE	Belgium
SATCOM1 Aps	Denmark
SETCCE	Slovenia
Aerovisión Vehículos Aéreos S.L	Spain
Thales Communications S.A.	France
Mediterranean Academy of Diplomatic Studies	Malta