AMASS / Autonomous maritime surveillance system

© Volodymyr Kyrylyuk - Fotolia.com

Maritime surveillance

At present, Blue Border Surveillance is carried out predominantly by coast guard ships, aeroplanes and helicopters. These expensive measures are only fragmentary.

They are not suitable to locate small boats within a wider maritime area and they do not allow a continuous 24 h/7 surveillance as a countermeasure to illegal immigration.

Concept

The surveillance system developed under the AMASS project will form an array of autonomous, automated surveillance platforms with active and passive sensors.

The key sensors being used are high-end technology-un-cooled thermal imagers and highly sophisticated Hydrophones linked together via a wideband radio network.

Alarms from the sensors will be analysed and integrated with back ground details (location, speed, class,…) into a "Geographical Information System" situated within a blue border command centre.

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

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

Project objectives

Based on in depth research into the situational data a good understanding of the operational as well as technical requirements of such a highly sophisticated surveillance system is forming the basis of this project.

With AFM and ICCM acting as end users, tests at the end of the project will be under realistic conditions in territorial waters of countries (Malta / Canary Islands) highly affected by illegal immigration.

System configuration

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

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

Aim

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

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

Information

Acronym:
AMASS

Grant Agreement N°:
218290

Total Cost:
€ 4,970,709

EU Contribution:
€ 3,580,550

Starting Date:
01/03/2008

Duration:
42 months

Coordinator:

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

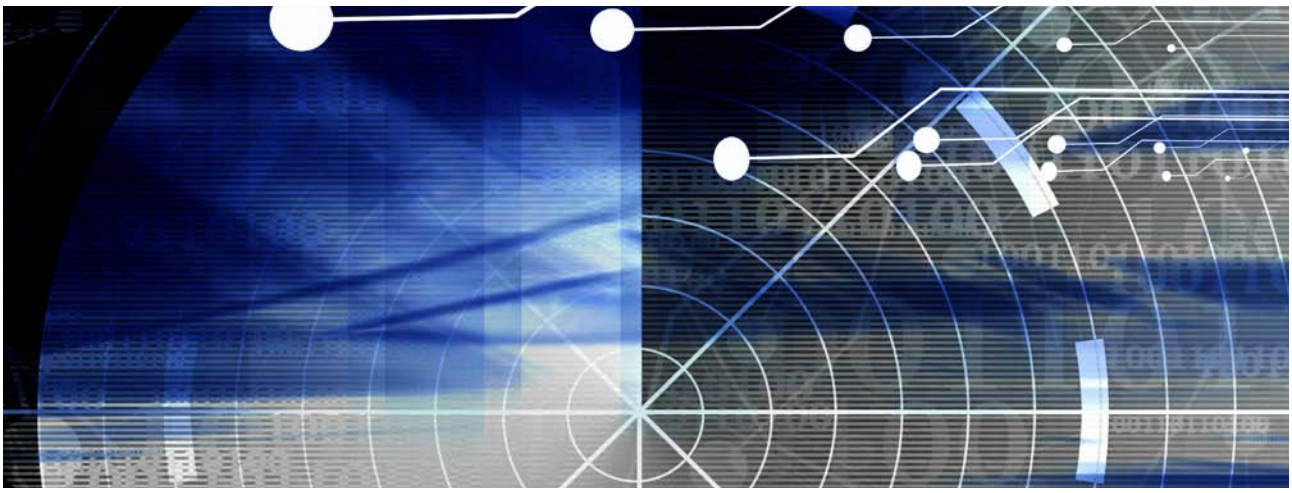
—

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

Partners

NAME	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 Institut Informations- und Datenverarbeitung	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

Project objectives

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

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

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

Description of the work

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

- The 3D PSR, a solution that, using a monopulse approach which exploits the difference of the gain of two radar beams of a conventional multi-beam 2D PSR, allows to obtain an estimation of the aircraft altitude.
- The Passive/Bistatic radars, special forms of radar systems that, rather than emitting pulses, rely on sources of illumination already available in the environment to illuminate potential targets and are able to detect and track objects by analysing the way these objects reflects the signals coming from the transmitters of opportunity.

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

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

- a Consistency function to compare the data from the different sensors and check their integrity;
- a Decision Support function to distinguish between cooperative and non-cooperative air traffic, thus providing a warning every time a risk of terrorist attack occurs and suggesting to the operators the right actions;
- a new Data Presentation function to show, in a dedicated display, further information in addition to conventional air traffic information.

The project includes:

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

Expected results

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

Information

Acronym :
ARGUS 3D

Grant Agreement N° :
218041

Total Cost :
€ 4.943.520

EU Contribution :
€ 3.262.050

Starting Date :
01/12/2009

Duration :
36 months

Coordinator :

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

—

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

Partners

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

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

© CASSANDRA

Project objectives

Main Objective is to enable and facilitate the combination of existing information sources in supply chains for containers into new and better visibility that allows the assessment of risks by business and government.
CASSANDRA is combining new tools, hardware, visibility platforms and other technical solutions in such a way that business and government are enabled to fully adopt a risk based approach to their operational activities, and in particular to combine two strategic customs approached: the Risk-based approach with the System-based audit approach. As such, it is a more balanced approach then the US driven approach towards 100% scanning of incoming containers.
CASSANDRA will facilitate the adoption of a risk based approach in designing and managing efficient and secure supply chains by business. In addition, CASSANDRA will facilitate a dialogue between business and government to gain acceptance of the risk based approach and risk self-assessment by business for supervision by government agencies. This principle of governments' piggy backing on businesses' own risk assessment is becoming a central theme in a number of long term strategies among supervision agencies, such as customs and police.

Description of the work

The main activities in the project are the development of risk based approaches in supply chains, the facilitation of information integration and sharing in the supply chain, by building interfaces between existing visibility platforms, and organizing a consensus building process among business and government agencies to arrive at a commonly accepted framework for risk assessment in the supply chain. CASSANDRA follows very much a data integration and business intelligence approach to risk assessment. As much as possible, this approach relies on existing data sources, data sharing and system integration. Hardware oriented solutions, such as satellite tracking and extensive container scanning, or building completely new platforms or tools are not part of this project.
The project will demonstrate and implement this approach to risk assessment in three so-called living labs. These are set up around major European tradelanes: Asia – North West Europe, North Europe – US and North Africa – Southern Europe.
The nine Work Packages are:

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

Expected results

CASSANDRA will:

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

Information

Acronym :
CASSANDRA

Grant Agreement N° :
—

Total Cost :
€ 14,813,514

EU Contribution :
€ 9,958,749

Starting Date :
01/05/2011

Duration :
36 months

Coordinator :

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

—

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

Partners

NAME	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

Project objectives

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

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

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

Description of the work

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

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

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

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

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

Expected results

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

- allowing systematic in depth controls of travellers, luggage and vehicles, for pedestrians and people inside vehicles, through the use of automatic gates and portable identity check and scanning equipment,
- providing objective criteria for submitting some travellers/vehicles/luggage to an extensive check in specific lanes.

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

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

Information

Acronym:
EFFISEC

Grant Agreement N°:
217991

Total Cost:
€ 16,310,974

EU Contribution:
€ 10,034,837

Starting Date:
01/05/2009

Duration:
54 months

Coordinator:

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

—

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

Partners

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

GLOBE / Global border environment

© Fotolia.com

Project objectives

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

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

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

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

Description of the work

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

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

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

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

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

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

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

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

Results

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

© Fotolia.com

Information

Acronym :
GLOBE

Grant Agreement N° :
218207

Total Cost :
€ 999,891

EU Contribution:
€ 999,891

Starting Date :
01/07/2008

End Date :
30/06/2009

Coordinator :

TELVENT INTERACTIVA S.A.
Mr. Manuel Parra
Av. Valgrande, 6
ES-28108 Alcobendas
Spain

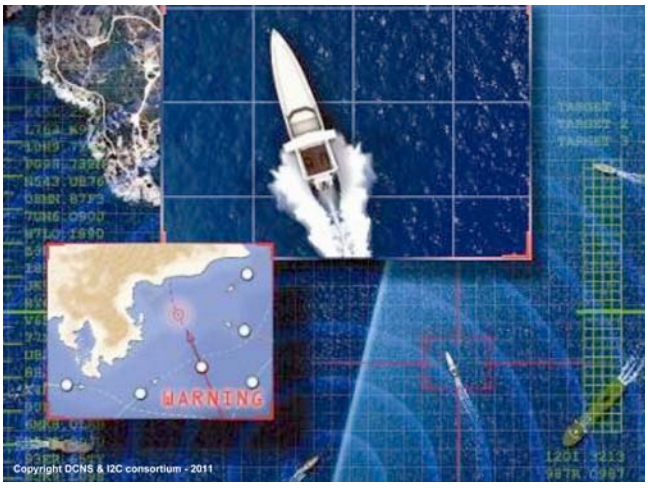
—

Contact :
Víctor Alejandro Luaces Bustabad
E-mail : victor.luaces@telvent.com
Website : http://globe.ti-projects.com/

Partners

NAME	COUNTRY
Telvent Interactiva S.A.	Spain
Amper Sistemas S.A.	Spain
GMV Aerospace and Defence, S.A	Spain
Fundación Robotiker	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

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



Project objectives

I2C new generation of maritime surveillance system must allow:

» Permanent and all weather coverage of border maritime areas.

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

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

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

» Generate electronic and formatted interpretation reports on the suspicious event to keep periodically informed decisional authorities.

Description of the work

The tasks to perform in the I2C integration project are:

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

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

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

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

Expected results

The main outcomes of I2C are:

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

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

» Demonstration, that the integrated system fulfil the operational needs with prototypes installed in a few operational centres.

Information

Acronym :
I2C

Grant Agreement N° :
242340

Total Cost :
€ 15,962,707

EU Contribution:
€ 9,869,621

Starting Date :
01/10/2010

Duration:
48 months

Coordinator :

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

—

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

Partners

NAME	COUNTRY
ROCKVELL COLLLINS France	France
FURUNO FINLAND OY	Finland
SES ASTRA TechCom SA	Luxembourg
KONGSBERG NORTCONTROL IT A/S	Norway
KONGSBERG SPACETEC A/S	Norway
CLEARPRIORITY SA	Belgium
ZLT ZEPPELIN LUFTSCHIFFTECHNIK GMBH ET CO KG	Germany
METEOSIM SL	Spain
AJECCO OY	Finland
AIRSHIPVISON INTERNATIONAL SA	France
ECOMER	France
INTUILAB	France
SOFRESUD	France
ERIC VAN HOOYDONK ADVOCATEN	Belgium
ARMINES	France
UNIVERSITE PAUL SABATIER III	France
ONERA	France
JOINT RESEARCH CENTRE	Belgium
DEUTSCHE ZEPPELIN REDEREI GMBH	Germany

IMCOSEC / Integrated approach to improve the supply chain for container transport and integrated security simultaneously

© Soleg - Fotolia.com

Project objectives

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

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

Description of the work

IMCOSEC was guided by the following approach:

- Identification of security gaps based on the current processes, e.g. using the resilience matrix approach.
- Elaboration of target processes for closing these gaps and ensuring product integrity is supported by technologies either already deployable or under development.
- Identification of existing technologies to support and improve the container transport chain and integrate security.
- Consideration of ongoing projects and their intended results as well as parallel actions.
- Identification of additional requirements for R&D actions where these gaps cannot be closed by existing measures or research.
- Provision of a roadmap for demonstration activities where target processes and supporting technologies can establish efficiency, effectiveness and acceptance.
- Development of a guideline to improve existing or develop new technologies in order to meet the requirement given by the developed research roadmap.

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

Results

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

Information

Acronym :
IMCOSEC

Grant Agreement N° :
242295

Total Cost :
€ 1,142,591

EU Contribution :
€ 930,718

Starting Date :
01/04/2010

End Date :
31/03/2011

Coordinator :

TSB INNOVATIONSAGENTUR BERLIN GMBH / BEREICH FAV
Fasanenstr. 85, 10623 Berlin
Germany

—

Contact :
Markus Podbregar
Tel : +30 46302 579
Office: +30 46302 563
Fax: +30 46302-588
E-mail: mpodbregar@fav.de
Website : www.imcosec.eu

Partners

NAME	COUNTRY
Bureau International des Containers et du transport intermodal (BIC)	France
CBRNE Ltd (CBRNE)	United Kingdom
INSTITUT FUER SEEVERKEHRSWIRTSCHAFT UND LOGISTIK (ISL)	Germany
International Container Security Organisation (ICSO)	Belgium
POLITECNICO DI MILANO (POLIMI)	Italy
STUDIENGESELLSCHAFT FUR DEN KOMBINIERTEN VERKEHR EV (SGKV)	Germany
TECHNISCHE UNIVERSITAET HAMBURG-HARBURG (TUHH)	Germany
TSB Innovationsagentur Berlin GmbH (FAV)	Germany
Union Internationale des sociétés de transport combiné Rail Route (UIRR)	Belgium

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

© Fotolia.com

Project objectives

The LOGSEC project had the following three main objectives:

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

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

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

Description of the work

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

- literature and project reviews,
- end-user expert interviews,
- user surveys, and
- user workshops.

Results

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

Information

Acronym :
LOGSEC

Grant Agreement N° :
241676

Total Cost :
€ 800,047

EU Contribution :
€ 753,373

Starting Date :
01/04/2010

End Date :
31/03/2011

Coordinator :

EFP CONSULTING (UK) LTD.
MOTHERWELL
BRANDON STREET - OAKFIELD HOUSE
ML1 1XA
UK

—

Contact :
Dana Remes
Phone : +44 141 649 3244
E-mail : dana@efpconsulting.com
Website : www.logsec.org

Partners

NAME	COUNTRY
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
EFP Consulting (UK) Ltd (EFPC)	United Kingdom
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

© Netfalls - Fotolia.com

Project Objectives

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

Description of the work

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

- **WP 1 (Concepts and Scenarios)** is dedicated to compilation and analysis of the operational concepts and scenarios of UAS use in the context of maritime and land aerial surveillance of European borders. The border surveillance missions that could be performed by UAS will be identified, and then further refined into scenarios in order to provide an operational framework to the architecture design. This task will propose complete concepts of data / information exchange between scenarios participants, including operational protocols. In this phase the end-user needs will be taken into account through direct exchange (Workshop).
- **WP 2 (Legislation Analysis)** intends to describe the current and emerging regulation framework for insertion of UAS into controlled civil airspace in order to identify its limitations regarding UAS border surveillance operations, and to recommend some legislation evolutions favouring the UAS use in border surveillance.
- **WP 3 (Technical Analysis)** is a central task dedicated to the parallel analysis and synthesis of the technical capabilities available for four main UAS components: the surveillance sensors, the aerial platforms, the datalink and communication networks and the ground stations. Generic classes of UAS components will be defined and described in terms of performances and costs.
- **WP 4 (Open Architecture Definition)** is dedicated to the identification of open architecture solutions to perform border surveillance missions. This task particularly focuses on cost-efficient solutions enabling maximum efficiency of UAS operations for European border surveillance.
- **WP 5 (Information Exchange and Dissemination)** is a Work Package dedicated to maintain a close communication level with the end-users, grouped in a User Advisory Board, in order to acknowledge and to check project consistency with the end-users requirements.

Expected results

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

- Fostering non-proprietary solutions for equipments and sub-systems (sensors, platforms, data links, and ground stations).
- Allowing smaller companies and SME's from many member countries to enter the market.
- Open-up the market for non-military companies.
- Develop the dialogue between European end-users and make international operations between different nations more feasible.
- Allow companies to share different parts of a more complex system which distributes development costs and risks to a broader basis. This will foster the development of industrial co-operation similar to the "Airbus model".
- Provide an overall benefit to the end-users by optimisation of costs (through lower development costs) and mission efficiency. The customer is expected to get a system of different classes of sub-systems which can be selected for joint operations for more performance instead of having heavily competing single systems.

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

Information

Acronym :
OPARUS

Grant Agreement N° :
242491

Total Cost:
€ 1,188,313

EU Contribution:
€ 1,188,313

Starting Date:
01/09/ 2010

Duration:
18 months

Coordinator :

SAGEM DÉFENSE SÉCURITÉ
27 rue Leblanc,
75015 Paris
France

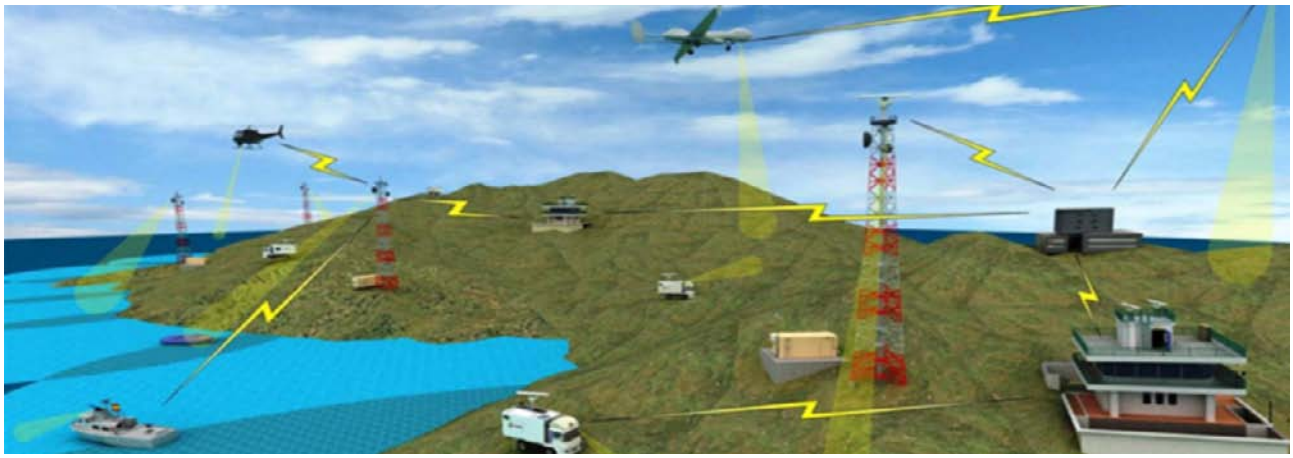
—

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

Partners

NAME	COUNTRY
Sagem Défense Sécurité	France
AFIT (Air Force Institute of Technology,)	Poland
BAE Systems	United Kingdom
Dassault Aviation	France
DLR	Germany
EADS-CASA	Spain
IAI	Israel
INTA	Spain
ISDEFE	Spain
ONERA	France
Selex Galileo	Italy
Thales Communication	France
Thales Systèmes Aéroportés	France

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


© PERSEUS

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 a EU Maritime surveillance System of Systems, on the basis of existing national systems and platforms, enhancing them with innovative capabilities and moving beyond EUROSUR's 2013 expectations, addressing key challenges:

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

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, to extend it to more countries, based on the user and provider feedbacks acquired through two real-life exercises operating in the Western and Eastern Mediterranean regions.

Information

Acronym :
PERSEUS

Grant Agreement N° :
261748

Total Cost:
€ 43,644,979.60

EU Contribution:
€ 27,847,579.00

Starting Date:
01/01/2011

Duration:
48 months

Coordinator :

INDRA SISTEMAS, S.A.
Security Systems
Av. de Bruselas, 35
28108 Alcobendas (Madrid)
Spain

—

Contact :
Mr Fernando Barbero
Tel : +34 91 2097937
Mobile : +34 647 624 121
E-mail : fbarbero@indra.es
Website : http://www.perseus-fp7.eu/

Partners

NAME	COUNTRY
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 INOVACAO, 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

Project objectives

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

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

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

Description of the work

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

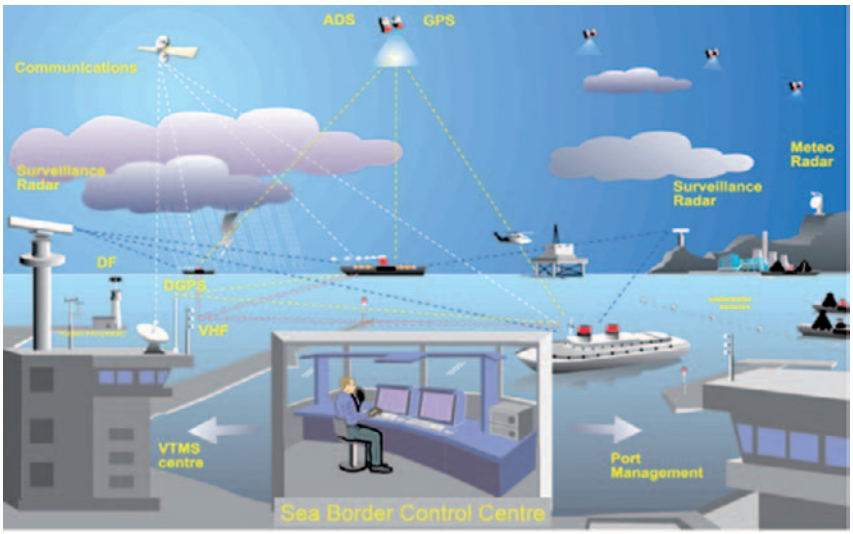
» for fighting drug trafficking in the English Channel;

» for addressing illegal immigration in the South Mediterranean; and

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

Expected results

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



Information

Acronym:
SEABILLA

Grant Agreement N°:
241598

Total Cost:
€ 15,549,679

EU Contribution:
€ 9,843,601

Starting Date:
01/06/2010

Duration:
45 months

Coordinator:

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

—

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

Partners

NAME	COUNTRY
SELEX Sistemi Integrati SPA	Italy
ALENIA AERONAUTICA	Italy
BAE SYSTEMS	United Kingdom
CNIT (CONSORZIO NAZIONALE INTERUNIVERSITARIO TELECOMUNICAZIONI)	Italy
CORRELATION SYSTEMS	Ireland
ADS Defence & Security	France
EUROCOPTER ESPANA	Spain
EDISOFT	Portugal
FOI	Sweden
HITT	The Netherlands
INDRA ESPACIO	Spain
INDRA SISTEMAS	Spain
JRC	Europe
MONDECA	France
SAGEM DEFENCE SECURITE	France
SPACE APPLICATIONS SERVICES	Belgium
TELESPAZIO (TPZ)	Italy
THALES ALENIA SPACE FRANCE	France
THALES ALENIA SPACE ITALIA	Italy
THALES DEFENCE DEUTSCHLAND	Germany
TNO	The Netherlands
THALES SYSTEMES AEROPORTES	France
TTI Norte	Spain
UNIVERSITY COLLEGE LONDON	United Kingdom
UNIVERSIDAD DE MURCIA	Spain
UNIVERSITY OF PORTSMOUTH	United Kingdom

SUPPORT / Security UPgrade for PORTs

© Herbert Rubens - Fotolia.com

Project objectives

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

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

Description of the work

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

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

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

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

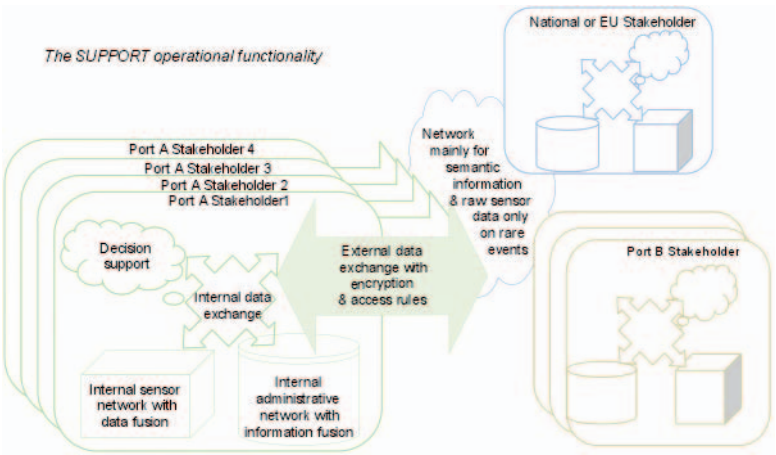
Expected results

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.



Information

Acronym :
SUPPORT

Grant Agreement N° :
242112

Total Cost :
€ 14,629,279.69

EU Contribution :
€ 9,920,607

Starting Date :
01/07/2010

Duration :
48 months

Coordinator :

BMT GROUP LTD
Research Directorate
Goodrich House, 1 Waldegrave Road
TW11 8LZ, Teddington
UK

—

Contact :
Jenny Gyngell
Tel : +44 (0)1933 625958
Mobile : +44 (0)7717 803105
Fax : +44 (0)1933 625958
E-mail : jgyngell@bmtmail.com
Website : http://www.support-project.eu/

Partners

NAME	COUNTRY
BMT Group (BMT)	United Kingdom
Swedish Defence Research Agency (FOI)	Sweden
Securitas (Securitas)	Sweden
Technical Research Centre of Finland (VTT)	Finland
MARLO (Marlo)	Norway
INLECOM Systems (ILS)	United Kingdom
MARINTEK (Marintek)	Norway
Nautical Enterprise (NECL)	Ireland
STENA (Stena)	Sweden
eBOS Technologies (eBOS)	Cyprus
University of Innsbruck (UIBK)	Austria
Cargotec Port Security (CA)	Finland
Maritime Administration of Latvia (MAL)	Latvia
INRIA (Inria)	France
MARAC Electronics (ME)	Greece
Port of Piraeus (PPA)	Greece
EUROPHAR -EEIG Port of Valencia - Marseille – Genoa (PV)	EU
ECO SLC (ECO SLC)	The Netherlands

TALOS / Transportable autonomous patrol for land border surveillance system

© TALOS

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

Project objectives

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

» Is capable of Detecting, Locating, Tracking and Tracing:
- individuals,
- vehicles,
- hazardous substance.

» Combines remote and autonomous platforms featuring:
- multi sensor data fusion (including biological and chemical),
- active imaging,
- data Fusion,
- command Control & Communication.

The TALOS project main objectives are as follows :

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

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

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

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

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

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

The main TALOS innovation covers :

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

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

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

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

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

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

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

Information

Acronym :
TALOS

Grant Agreement N° :
218081

Total Cost :
€ 19,906,815

EU Contribution :
€ 12,898,332

Starting Date :
01/06/2008

Duration :
48 months

Coordinator :

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

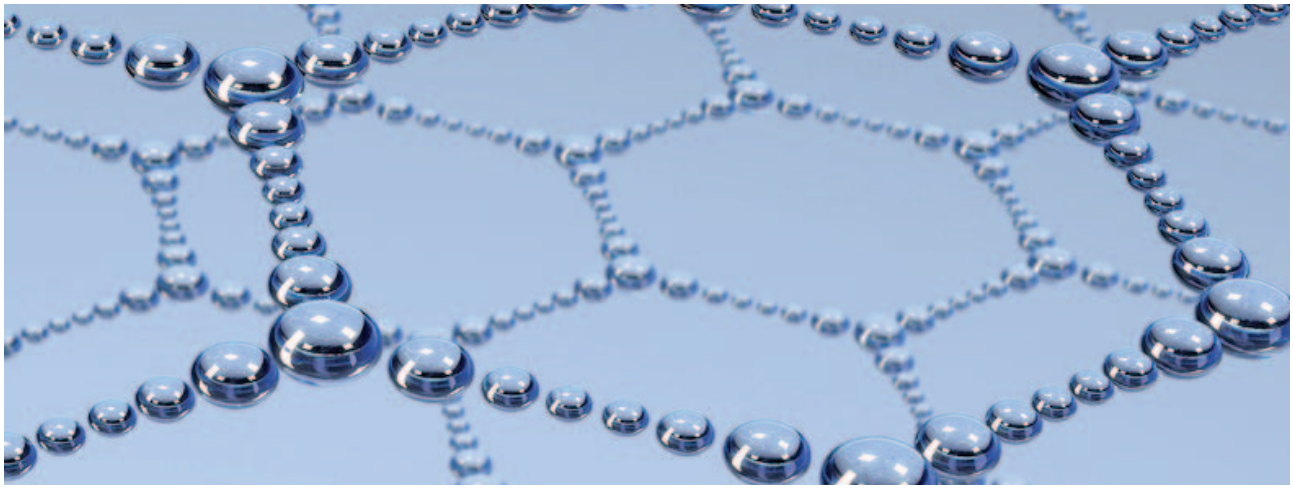
—

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

Partners

NAME	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



© beawolf - Fotolia.com

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:

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

Description of the work

The 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.

Information

Acronym:
VIRTUOSO

Grant Agreement N°:
242352

Total Cost:
€ 11,510,542.25

EU Contribution:
€ 7,999,182.55

Starting Date:
01/05/2010

Duration:
36 months

Coordinator:

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

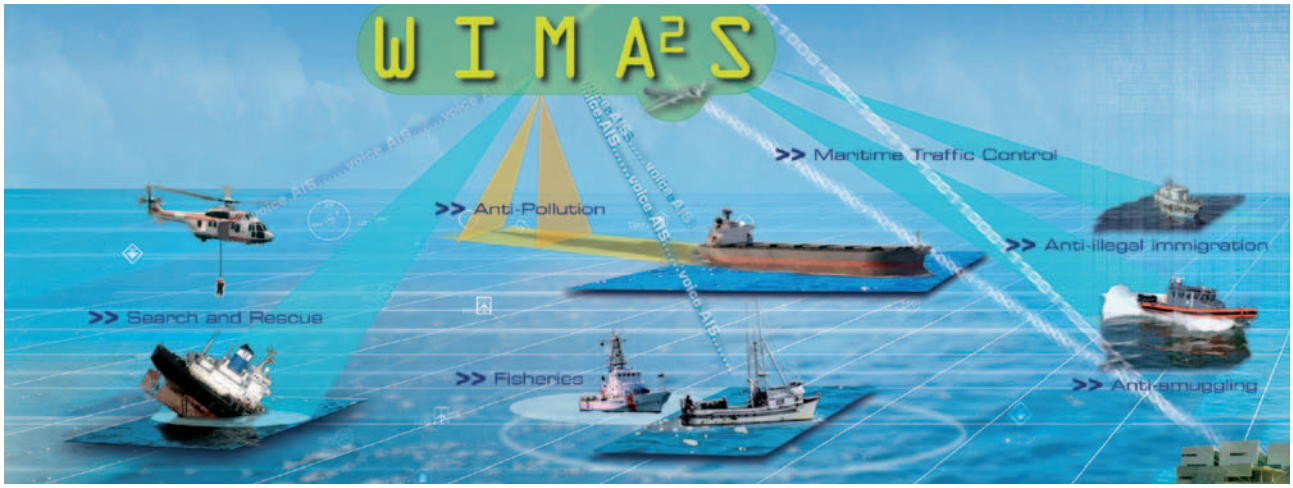
—

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

Partners

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

WIMA²S / Wide maritime area airborne surveillance



© WIMA²S

Project objectives

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

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

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

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

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

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

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

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

Description of the work

WiMA²S proposes solutions to these issues by:

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

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

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

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

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

© Kevin Bourdeaux - Fotolia.com

Information

Acronym :
WIMA²S

Grant Agreement N° :
217931

Total Cost :
€ 3,997,523

EU Contribution :
€ 2,737,169

Starting Date :
01/12/2008

Duration :
36 months

Coordinator :

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

—

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

Partners

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