COOPERATION

Ex-post Evaluation of PASR Activities in the field of Security and Interim Evaluation of FP7 Security Research

Maritime Security and Surveillance - Case Study

January 2011

C S E S

Centre for
Strategy & Evaluation
Services

P O Box 159
Sevenoaks
Kent TN14 5WT
United Kingdom
www.cses.co.uk

Contents

Introduction

1.1 7th RTD Framework Programme 2007-2013

The 7th Framework Programme for Research and Technological Development (FP7) 2007-2013 period is the EU's main instrument for funding research and development. FP7 has a budget of €50.5bn over 7 years, a significant funding increase compared with previous RTD Framework Programmes. The RTD FPs are a key tool in achieving the aims of the Europe 2020 strategy, which includes *'smart growth: developing an economy based on knowledge and innovation'* as a key priority. There are four different programmes within FP7: Cooperation**,** Ideas**,** People and Capacities**.** FP7 Security Research is part of the Cooperation objective, which fosters collaborative research across the Europe Union and with other Associated States and partner countries.

1.2 FP7 Security Research, Maritime Security and Surveillance

Following the implementation of the PASR Preparatory Action on Security Research in 2004-2006 by the European Commission, an EU Security Research Programme (ESRP) was included for the first time in the RTD Framework programme in FP7. FP7 Security has a budget of €1.4bn. The objectives of FP7 Security Research are to: make Europe more secure for its citizens, strengthen industrial competitiveness; promote research excellence and state-of-the-art; prevent the fragmentation of research efforts and to strengthen critical mass. Among the specific objectives of the programme include: stimulating the development of a European market for new and emerging security products and systems; ensuring the security of EU citizens from new and emerging threats; delivering mission-oriented research results to reduce security gaps; ensuring the optimal use of existing and emerging technologies, and stimulating cooperation between providers and users of civil security solutions.

FP7 SEC provides support for transnational collaborative research in a number of areas, including maritime security. Research topics relating to maritime security, such as secure container-screening, biometric ID port perimeter security, satellite-based tracking of maritime areas and blue border surveillance, have been addressed in a number of work programmes. The extent of prioritisation of this theme under PASR and FP7 SEC calls, and the degree of continuity in particular areas of maritime surveillance are assessed in this case study. Appendix B provides a summary of calls that have addressed this domain.

1.3 Case study methodology and structure

The following case study outlines support for maritime security through EU Security Research, with a particular focus on surveillance. The case study research draws on a combination of desk research and field work. An interview programme was undertaken with a number of lead coordinators and partners in Maritime Security research projects. In addition, an interview was carried out with the relevant project officer at the Commission responsible for these projects. The case study is structured as follows:

Section 2 - provides an overview of the policy context in respect of maritime surveillance, and the main challenges and issues being addressed through security research

Section 3 – examines projects that were supported through PASR and FP7 Security in the field of maritime security

Section 4 – outlines conclusions, and reviews progress towards the achievement of objectives.

Policy context and key issues 2

2. POLICY CONTEXT AND KEY ISSUES

In this section, the EU policy and regulatory context is first outlined, and then recent developments, and the main threats and challenges in the maritime security domain are summarised.

2.1 Policy and legislative context

Maritime security and border surveillance is an important area supported through the ESRP. In the context of EU enlargement, Europe's maritime borders have expanded with Europe's coastline containing 85 per cent of the EU's international borders.

This will require increased surveillance to tackle problems such as illegal immigration, and other illicit activities linked to organised crime, such as drugs smuggling, human trafficking and the trafficking of illicit materials such as WMD and explosives. Effective monitoring of EU external borders requires increased cooperation between relevant stakeholders in maritime surveillance, such as coastguards and law enforcement agencies.

Maritime security was stepped up on a global scale following the September 11th 2001 terrorist attacks with the maritime community agreeing the need for international maritime security requirements. Prior to 9/11, the majority of terrorist surveillance, and response measures, put in place throughout the EU were as a result of individual action at Member State level. The International Maritime Organisation (IMO) adopted new international maritime security requirements in December 2002 (new Chapter XI-2) under the 1974 SOLAS Convention, and a new International Ship and Port Facility Security (ISPS) Code.

Following the adoption of the new IMO security regime, the EU Member States agreed on the need for measures at Community level and for monitoring their effective implementation. As a result, Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security was adopted. The purpose of the Regulation is to introduce and implement in a harmonised manner measures aimed at enhancing the security of ships engaged on international voyages and domestic shipping, including associated port facilities.

The Commission subsequently adopted a Directive laying down procedures for conducting inspections in the field of maritime security to monitor the application of Regulation (EC) No 725/2004. Following the coming into force of Directive 2005/65/EC on enhancing port security, a revised Commission Regulation (EC) No 324/2008 was adopted on 9 April 2008 to incorporate procedures for monitoring Member States' implementation of the Directive jointly with the Commission's inspections under Regulation 725/2004. On the basis of this legislation, inspections are prepared and coordinated by the European Commission.

A number of initiatives have been put in place between local and regional authorities in the three main zones of maritime cooperation: the Euro-Mediterranean, the Northern Dimension Policy Framework and the Black Sea Synergy. The aim of setting up these zones was to evaluate progress to date in improving maritime surveillance and to identify possible future challenges.

The **Mediterranean Basin** is a strategically important region for the EU, and it is necessary to construct a strong economic area there capable of contributing to the Union's regional balance by assuring peace, stability and prosperity. The Barcelona Initiative was launched with these objectives in mind and is now a central element of the EU-Mediterranean Policy.

Another important area of cross-border cooperation that also prompts the need for a common maritime surveillance policy is the **Northern Dimension** which covers vast areas in the European Arctic and Sub-Arctic region, to the Baltic Sea, the Scandinavian countries, Iceland and Russia. In this respect, the Northern Dimension Policy Framework, as one of the main instruments of maritime policy, came into existence through a number of common initiatives between the EU and its trading partners.

The third important initiative which completes the chain of regional cooperation frameworks in the EU's neighbourhood along with the Euro-Mediterranean Partnership and the Northern Dimension is the **Black Sea Synergy**. It aims to develop the collaboration between the countries in the Black Sea Region as well as between the region itself and the EU in the areas of maritime surveillance policy, but also energy and the environment. The Commission established a Black Sea Cross-Border-Cooperation programme under the European Neighbourhood and Partnership Instrument (ENPI) focusing on supporting regional level cooperation in Black Sea coastal areas.

The **programme decision** establishing FP7 in 2006 (DECISION No 1982/2006/EC of 18th December 2006) provides the legal base for the FP7 Security programme and determines the types of research projects that can be funded. However, it is worth noting that there have been further policy and legal developments since the programme was adopted, which will necessarily need to be taken into consideration in future planning for FP8.

On 10 October 2007, the Commission published the Communication CM(2007) 575 ('Blue Paper') on an **Integrated Maritime Policy** for the European Union. This Communication advocated the need for the development and implementation of integrated, coherent, and joined-up decision-making in relation to the oceans, seas, coastal regions and maritime sectors. The Integrated Maritime Policy promotes a cross-sectoral approach to maritime governance in order to identify and exploit synergies between all EU policies relating to the oceans, seas, coastal regions and maritime sectors - namely the environmental, maritime transport, energy, research, industry, fisheries and regional policies. A Programme has been adopted in 2010 to support the further development of an Integrated Maritime Policy (SEC(2010) 1097 final).

The Commission Communication of February 2008 on **EUROSUR** (COM (2008)68) examined the parameters for establishing an **integrated border surveillance system** focusing on the EU's southern and eastern maritime borders. The Communication underlines the importance of FP7 Security Research in promoting the development of advanced and innovative surveillance and information-sharing technologies in the maritime border surveillance field. The European Council endorsed the European Commission's Eurosur proposals for a hi-tech European border surveillance system.

The Commission will present a legislative proposal to set up EUROSUR in 2011 to contribute to internal security and the fight against crime. EUROSUR will establish a mechanism for Member States' authorities to share operational information related to border surveillance and for cooperation with one another and with Frontex at an operational and strategic level. EUROSUR will make use of new technologies developed through FP7 funded research projects, such as satellite imagery to detect and track targets at maritime borders, e.g. tracing fast vessels transporting drugs to the EU. In this regard, there are important links with projects financed through the GMES initiative funded through FP7 Space.

Another important development was the adoption of the **Lisbon Treaty** in December 2009. This raises issues relating to closer cooperation between civil and military aspects of maritime security and surveillance. However, FP7 SEC is a civil security programme, and therefore the implications of the evolution in the legal base can only be explored through the framework of the Cooperation Framework Mechanism signed between the European Commission, the EDA and the ESA.

Maritime security remains a politically sensitive issue whose aims are subject to different interpretations at national, European and international levels. This case study therefore focuses on maritime surveillance projects supported through PASR and FP7 SEC.

2.2 Maritime security and surveillance - key threats and challenges

The large size of the European maritime area and the multifaceted nature of the challenges related to ensuring effective wide-area maritime surveillance requires a European and global approach to maritime security. Tackling threats such as illegal immigration, terrorist threats to port infrastructure and to security containers requires strong European cooperation between relevant public agencies and port operators, and demands a European response.

Technology plays an important role in addressing key security challenges for the EU in the area of maritime surveillance. In particular, there are a number of emerging space-based technologies of satellite earth observation, communication and global positioning for ship traffic surveillance and the identification of security threats provide the tools to address these issues. There have also been improvements in Geographic Information System (GIS) and in networking sensor systems.

Research undertaken in the frame of FP7 fits within the objectives of the GMES (*Global Monitoring for Environment and Security*). Satellite surveillance of maritime traffic is an essential part of the European Maritime Security strategy. Through the development of space technologies better adapted to meet the needs of maritime surveillance, initiatives at the EU level, such as the Maritime Policy Task Force, FRONTEX, EUROSUR, the European Maritime Safety Agency and EDA projects need to be better integrated so as to ensure the seamless unification of surveillance requirements with technological provisions.

Furthermore, EU funded research on maritime surveillance supports the study of areas far from the EU's coastal borders with the aim of identifying traffic patterns, ensuring compliance with international legislation and addressing threats to supply lines.

Effective maritime surveillance requires cooperation along EU external borders and cooperation with non-EU Member States. Maritime surveillance activities focus on both internal and external security aspects: e.g. illegal immigration, piracy and unlawful trafficking. The establishment of an integrated approach to maritime surveillance through common information sharing to promote interoperability and to make best use of existing systems on a cross-sectoral basis has been promoted by the EU through FP7 Security Research.

The current security scenario is dominated by a combination of asymmetric threats of a varying nature. Threats relating to maritime security primarily concern unlawful activities such as trafficking in human beings and narcotics, illegal migration, terrorism, and piracy. The external maritime borders of the EU are most exposed to these types of threat, particularly the EU’s South Eastern borders. Many of the security threats involve the use of small craft, rubber boats, and even semi-submersibles.

Policy context and key issues

A key challenge is to detect and track small objects and to distinguish possible threats from legitimate shipping, fishing and other maritime activities. A number of projects have attempted to address this challenge under FP7 Security. Other maritime security threats involve illicit activities under the cover of regular shipping activity (e.g. on board merchant vessels and passenger ferries). Illegal migrants or illicit goods can be hidden among the cargo and can then be dispersed en route or when arriving at seaports.

Among the main shortcomings with regard to the current situation in respect of maritime security are:

- Lack of wide-area maritime surveillance, using integrated satellite and sea-based technologies and networked sensors. In the open seas, there is only partial coverage, and a need for continuous and persistent surveillance

- Coastal waters: gaps in detection of small targets

- Partial coordination and information sharing between costal surveillance systems in the Member States (linked to fragmentation of organisations in the maritime security domain)

- Limited interoperability between sectoral stakeholders and systems, a need to link up networks of heterogeneous sensors

- The need for further investment to improve technologies for secure containers (e.g. equipped with Intrusion Detection Sensors, electronic seals and data device reading capabilities)

- Maritime Surveillance systems have been developed mainly for maritime safety purposes, and were not designed with sufficient attention to security aspects

- The need for improved surveillance of port perimeters and investment in research on new technologies to facilitate this, such as biometric ID to secure areas

- Lack of early warning systems

By sharing relevant information between different sectors at Member State and EU level, which has to be achieved in full compliance with the sovereign prerogatives of the Member States, a common information-sharing environment could improve situational awareness in the EU maritime domain.

Ensuring effective maritime security is paramount to economic well-being. More than 80% of world trade depends on safe maritime routes, and bringing about more effective surveillance of maritime traffic poses a significant challenge. The EU needs to pool its global maritime surveillance capabilities. The main challenges to ensuring interoperability and information sharing in the maritime domain are:

- Ensuring effective coordination and the integration of different national authorities involved in maritime (border) surveillance at national and EU levels

- Strengthening cooperation with neighbouring third countries

These overarching challenges require capabilities and standards to be developed on a technical level as well as on tactical, operational and strategic levels.

Section 2 Policy context and key issues

ESRIF and maritime security

The ESRIF stakeholder consultation exercise led to the publication of a strategic agenda for security research in December 2009. This included a focus on maritime security research. ESRIF stressed the importance of strengthening interoperability in the field of maritime security and of ensuring that an integrated approach is adopted that extends well beyond maritime border surveillance alone and towards establishing seamless, real-time, and wide-area surveillance of vessels, people and goods.

For instance, cognitive sensor technology is identified through the ESRIF as providing added-value to security users and operators. In addition to addressing issues relating to technical aspects of maritime security, ESRIF stressed the importance of an integrated approach to strengthening maritime security, by improving technical and operational systems for effective maritime surveillance, by strengthening regulations and by promoting greater inter-institutional cooperation and information sharing between relevant EU agencies and the Member States, as well as with international actors in this field.

2.3 Key stakeholders in Maritime Security

Directorate General for Maritime Affairs and Fisheries (DG MARE) is the policy lead within the European Commission on issues relating to maritime security.

The **European Maritime Safety Agency (EMSA)**, an EU agency, has since 2004 been given tasks and responsibilities in respect of maritime security with the entry into force of Regulation 724/2004. EMSA provides scientific and technical advice to the Commission in the field of maritime safety and prevention of pollution by ships in the continuous process of updating and developing new legislation, monitoring implementation and evaluating the effectiveness of the measures in place. The Agency facilitates co-operation between the Member States and disseminate best practices in the Community and responds to specific requests in relation to the practical implementation of Community legislation. Some of the areas where the Agency is especially active include: strengthening the Port Control regime; and the establishment of a Community vessel traffic monitoring and information system.

The Treaty of Amsterdam provides for the involvement of EU-wide organisations as well as national agencies of the Member States in relation to maritime border control. Coordination between member states is being increasingly supported by European agencies in particular through the establishment of **FRONTEX** (**European Agency for the Management of Operational Co-operation at External Borders)** and the Eastern Mediterranean Sea Borders Centre. Although maintaining national sovereignty over maritime borders, these developments are intended to facilitate more effective cooperation between member states in information gathering and exchange.

At national level, users include **border control agencies**, **customs and excise agencies, Coast Guard and** interception units and **police forces** and **intelligence agencies** (organised crime and anti-terrorism units). In some cases, these agencies may be intermediaries responsible for the provision of information to partner organisations in other government departments. Stakeholders at national level also include port infrastructure authorities and companies.

Project assessment

3.1 Maritime Security in PASR and FP7 Security – overview

Maritime research has been supported through a number of PASR and FP7 Security projects. The projects selected for analysis are summarised in the table below:

Table 1: PASR and FP7 Security Projects supported in the field of maritime security

Project	Full name	Programme	Call	EU Contribution	Budget
SOBCAH	Surveillance of Border Coastlines and Harbours	PASR	PASR 2005	€ 2,010,600	€ 3,007,109
SECCONDD	Secure Container Data Service Standardisation	PASR	PASR 2005	€ 399,851	€ 533,628
AMASS	Autonomous Maritime Surveillance System	FP7 Security	SEC-2007-3.3-02	€ 3,580,550	€ 4,970,709
OPERAMAR	Interoperable Approach to the EU's maritime security management	FP7 Security	SEC-2007-7.0-02	€ 669,132	€ 669,132
SECTRONIC	Security System for Maritime Infrastructure, Ports and Coastal Zones	FP7 Security	SEC-2007-2.3-04	€ 4,496,414	€ 7,080,433
UNCOSS	Underwater Coastal Sea Surveillance	FP7 Security	SEC-2007-3.3-02 SEC-2007-1.3-01	€ 2,760,000	€ 4,260,000
WIMAAS	Wide Maritime Area Airborne Surveillance	FP7 Security	SEC-2007-3.3-02	€ 2,740,000	€ 4,000,000
EFFISEC	Efficient Integrated Security Checkpoints	FP7 Security	SEC-2007-3.2-03	€ 10,030,000	€ 16,360,000
SEABILLA	Sea Border Surveillance system	FP7 Security	SEC-2009-3.2-02	€ 9,840,000	€ 15,550,000
IMCOSEC	Integrated approach to IMprove the supply chain for COntainer tranksport and integrated SECurity simultaneously	FP7 Security	SEC-2009-1.1-01	€ 930,718	€ 1,140,000

In the 2nd Call for Proposals in FP7 Security Research, two large-scale demonstrator projects were supported, EFFISEC and SEABILLA. Since these are of 4 years in duration, it is difficult at this early stage in the research to assess research results for the larger-scale projects supported that have strong potential to improve Sea Border Surveillance. However, other projects, such as those funded under PASR, have already been completed, and project achievements can already be assessed.

Maritime Security in ESRP work programmes

A number of PASR and FP7 Security Research work programmes supported to date included scope for addressing issues relating to strengthening **Maritime security.** A detailed list of relevant topics in calls is provided in the appendices by type of calls for proposals. In summary, among the topics supported which have included maritime security aspects through the Work Programmes include: Demonstration of concepts, technologies and capabilities for situation awareness systems, and for enhancing surveillance of land and sea borders.

Through PASR between 2004 and 2006, the focus of maritime security research was on improving situation awareness in terms of sea border surveillance, antiterrorism, and crisis management more generally. This coincided with an expansion in the size of the EU's external maritime borders following EU enlargement.

In 2004, 2005 and 2006, PASR funding was made available for activities relating to the demonstration of concepts and technologies in general border surveillance and to tracking and tracing persons, goods and assets. PASR projects therefore promoted the development of sensor technologies. Furthermore, in 2006, PASR encouraged projects that focused on the development and demonstration of new technologies for locating illegal immigrants crossing EU maritime borders.

The FP7 SEC Work Programme 2007 emphasised the objective of improving situation awareness in maritime areas through the development of integrated novel surveillance technologies (i.e. covering land, sea, air and space) combining tracking and tracing sensor devices with sophisticated data management and data fusion processes. The 2007 Call also promoted the development of main port area security systems with the aim of creating an integrated port area (i.e. land, sub-surface, water). Funding was made available for technologies providing accurate situational awareness in the context of the continuous arrival and departure of cargos, ships and persons, based on various sources such as mobile and fixed detection and recognition systems. There was also a focus on the need to improve data integration.

The FP7 Security Research Work Programme 2009 (2nd Call) reiterated the importance of prioritising main port area security. Funding was made available for technologies able to satisfy border control constraints at main ports. The 2009 Call under FP7 SEC also promoted the development and demonstration of technologies facilitating information sharing within and between main sea ports, and/or between sea ports and hinterland terminals and operational services, such as the police and customs. Integrated and interoperable sea border surveillance systems via the networking of relevant and heterogeneous sensors, and other information sources was also supported, with a large-scale demonstrator project funded in this area.

The development of integrated and interoperable sea border surveillance systems was further emphasised in the 2010 FP7 SEC Work Programme through support for a Phase 2 demonstrator of a European-wide integrated maritime border control system demonstration programme. This followed the introduction of Joint Maritime Operations involving various services (navies, border police,) and assets (patrol boats, helicopters etc) by FRONTEX.

The monitoring and tracking of shipping containers was also a major theme of the FP7 2010 work programme. This was previously a subset of the wider main port area security theme under the FP7 2007 programme. The 2010 call promoted therefore the development of situational awareness technology and information gathering mechanisms contributing to the implementation of a system for the monitoring and tracking of EU inbound and outbound container traffic effectively identifying security threats.

A number of key areas of support for research projects were identified in the field of maritime security under the PASR and FP7 SEC work programmes:

Project assessment

Integration projects have gained in importance through the strong emphasis placed on the continuous collection and fusion of heterogeneous data provided by various types of sensors and the gathering of other intelligent information from external information sources both for border control and anti-terrorism purposes. The gradual integration of land, sea and air border surveillance services and assets is reflected in the latest FP7 calls for projects. This corresponds to the ever greater operational cooperation taking between Member States in terms of EU external border surveillance through the activities carried out by FRONTEX.

The terrorist threat was specifically addressed through security research topics in the 1st and 2nd Calls in 2007 and 2009 respectively. These focused on the promotion of port area security and more specifically through the promotion of technologies concentrating on the **detection, recognition and monitoring of cargos and containers.** A project was supported under PASR in the field of **container security:** SECCONDD (PASR 2005) a container tracking system based on the scanning of container barcodes – the data storage interface is yet to be standardised. The use of technologies to transition towards smart containers was also addressed under the 3rd cal in FP7 2010, with an extended scope covering the integration and standardisation of various tracking and monitoring systems (i.e. the development of protocols) on a global scale to counteract security threats in container movement. Additionally, in the frame of FP7, there are currently two project proposals on smart containers – CONTAIN (tracking system) & CASSANDRA (risk analysis) – that are yet to be implemented.

In the 4th Security Call in 2011, the annual work programme mentions funding for capability projects to analyse relevant constraints affecting the security and efficacy of maritime border checks under the wider theme entitled 'border crossing points of the future'. Illegal immigration into the EU appears to be a major theme for 2011. It appears that research topics in FP7 SEC calls in the maritime security field have been selected in coordination and cooperation with the FRONTEX agency, which deals with land and maritime border control to support their activities.

A detailed overview of the treatment of Maritime Security in PASR and FP7 SEC calls is provided in Annex B.

3.2 PASR and FP7 project assessment – Maritime Security

3.2.1 Improved maritime surveillance systems

A key priority of EU support for maritime security research is working towards improved interoperability of local and national surveillance systems through the pooling of cross-sectoral surveillance information and its fusion into a central database. This approach consists of promoting a seamless information sharing system to increase the effectiveness of interventions by ending the fragmented approach of 'Blue Border' Surveillance which stems from a perceived lack of coordination between the predominant actors of maritime security such as coast guards, aeroplanes and helicopters.

The **AMASS** project (FP7 SEC, Call 1) focused on strengthening maritime surveillance and on better integrating information and data between relevant agencies. The focus was on developing a cutting-edge early-warning system that provides maritime authorities and law enforcement agencies with information about attempts at illegal immigration, and other criminal activities at sea.

Project assessment 3

Project(s):	**AMASS Autonomous Maritime Surveillance System**
Project timeframe:	01/03/2008 – 1/09/2011 (42 months)
Lead Partner:	Carl Zeiss Optronics GmbH
Total Cost and EU Contribution:	€ 4,970,709 and € 3,580,550
Start Date:	01/03/2008
Project type*:	FP7 Capability project

This project involves taking a ‘green border approach’ and applying it to ‘blue border’ (maritime) environments. AMASS is comprised of a network of unmanned platforms positioned at a considerable distance from shore. Each platform is fitted with cutting-edge sensors and operates self-sufficiently, i.e. without the need for manual intervention. Data captured by the sensors is transmitted to a central command centre where an operator views it on screen. If a suspicious object is detected, a crew can be dispatched to investigate or intervene. The technology aims to improve capacity for the control of small unidentified boats.

The first year of the project was marked by an intensive exchange of knowledge between end-users and solution providers. This led to a good understanding of actual and potential operational scenarios and the resulting performance requirements on the system. These requirements formed the basis for the development of the proposed technical solution and concrete specifications for sub-systems. Initial results have already been achieved in several key areas: platform design, sensor development, image processing strategy, communications and power system. An energy source simulator was generated in the initial stages of the project. The data gathered in the initial stages has also been very valuable for scenario planning. The project is now in its testing phase, which consists in integrating the first buoy in Las Palmas.

Waterways and coastal areas are important economic areas, for trade as much as for tourism, however such areas remain vulnerable to terrorism attacks especially against underwater improvised explosive device (IED) threats. A major challenge is to provide new tools for keeping naval infrastructure safe. The **UNCOSS** project (FP7 SEC, Call 1) is a cost-effective response to such new terrorism threats and provides a fundamental technology for the global issue of maritime surveillance and port/naval infrastructure protection.

Project(s):	**UNCOSS: Underwater Coastal Sea Surveyor**
Project timeframe:	01/12/2008 – 01/12/2011 (36 months)
Lead Partner:	ECA SA
Total Cost and EU Contribution::	€ 4,520,000 of which € 2,780,000
Start Date:	01/12/2008
Project type:	FP7 Capability project

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

The main objective of UNCOSS project is to provide tools for the non-destructive inspection of underwater objects mainly based on neutron sensor. This technology used has already been experimented for Land Protection (especially in the frame of FP6/Euritrack project). The application of this technology for

Project assessment

underwater protection will be a major achievement.

The availability of sophisticated surveillance systems is instrumental in reducing the risk of terrorist attacks. There has long been a need to further enhance maritime surveillance means through the utilization of more advanced available sensors, increased connectivity and through a shift toward net centric capabilities. The **SOBCAH project** (PASR, 2005), attempted to combine and maximise the use of existing surveillance technologies to model the most effective operational procedures for enhancing the surveillance of borders, coastlines and harbours.

Project(s):	**SOBCAH – Surveillance Of Borders, Coastlines And Harbours**
Project timeframe:	01/02/2006 – 01/08/2007 (18 months)
Lead Partner:	Galileo Avionica S.p.A.
Total Cost:	€ 3,007,109
EU Contribution:	€ 2,010,600
Start Date:	01/02/2006
Project type:	PASR demonstration project

The SOBCAH project supported under PASR involved an assessment of currently applicable security systems to identify any possible gaps in systems' capabilities and to find solutions to close those gaps through the identification of appropriate technologies.

The main aim of SOBCAH was to reinforce the security of European Borders through a well defined process which planned to identify the main threats relevant to ”green” and “blue” borders and to elaborate the most suitable architectural solutions based on the most advanced existing sensors and network technologies. The technology was tested and validated in the port of Genoa.

The project also focused on the use of sensors and data fusion to improve situation awareness for operators at the Security Centre console, a Common Operational Picture through the SOBCAH Complex Event Processing with a full situation awareness of external events and automatic identification of possible threats.

Under the 2nd FP7 SEC Call (2009), a project was supported that seeks to build on the initial results achieved through SOBCAH. The **SEABILLA (Sea border surveillance)** project aims to define the architecture for cost-effective European sea border surveillance systems, integrating space, land, sea and air assets, including legacy systems. The project is applying advanced technological solutions to improve the performance of surveillance functions. SEABILLA will provide field demonstrations of detection, tracking, identification and automated behavioural analysis of all vessels. This should lead to significant improvements in the effectiveness of surveillance in these areas.

End-user dimension - maritime surveillance systems

The **AMASS** project involved two users, AFM (the Maltese Armed Forces) and ICCM (Instituto Canario de Ciencias Marinas). Tests at the end of the project will be carried out under realistic conditions in the territorial waters of both Malta and the Canary Islands in Spain. Both countries have been highly affected by illegal immigration and there is a need to improve surveillance in order to detect illegal boat entry to the EU earlier.

AFM is a genuine user and is likely to adopt the technology for helping to track small vessels carrying illegal immigrants, while ICCM is a coordinating body that has been able to bring together groups of end users depending on their information needs. ICCM governmental institute has over 30 years of experience in coastal and ocean monitoring, working directly with search and rescue organizations in the Canary Islands.

Both end-user organisations have played a helpful role in guiding technological developments. However some aspects of the ICCM's relationship with the project leader were difficult as it required significant coordination. Nevertheless, their network is of a scope that would be hard to match without their wealth of contacts. The end users are especially important:

- During the testing phase
- When matching the technology to operational realities
- In drawing on appropriate planning scenario
- When defining the parameters of the application
- In understanding the implementation process
- In understanding cost thresholds for types of technology (both upfront and ongoing costs)

Some components could have been developed without the input of users, but this would have been based on a different set of assumptions (i.e. it would have been technology-driven rather than operations-driven). It was helpful for the project leader to have these two end users on board before the technical design stage as this led to a more user-friendly product. Initial results have already been achieved through the project in several key areas: platform design, sensor development, image processing strategy, communications and power system.

The first phase of the project involved setting out technical parameters for the technology. For this phase, the team relied heavily on user input to provide knowledge of the operational requirements and details related to how the technology would be used. The actions taken thus far include:

- Set up of an international project team
- Definition of end user operational scenarios and system performance requirements
- Development of a proposed total technical solution and sub-system specifications
- Provision of simulation software to model component energy charge-discharge characteristics
- Gathering of real data from the maritime environment for detection algorithm development.

The benefits for end-users likely to be considerable for the type of technology being developed through the AMASS project. There is expected to be wide take-up when the product goes to market. Overall, interest is high and some direct dissemination strategies have started.

With regard to the **UNCOSS project**, the main types of future prospective end-users are European port authorities. However, end-user involvement has mainly included research organisations so far. Therefore only a small amount of cooperation has taken place. Furthermore, the full benefits of the project will be realised over a period of time which is actually longer than the project timeframe itself. This can be explained by the fact that the project requires some considerable technological input which is being led by research bodies with expertise in maritime security research. Therefore, the introduction of the technology by end-users for operational purposes will take quite some time.

The project achieved a breakthrough in the miniaturisation of technology. This will open up the technology to new types of applications in areas such as airport security. Some successes in miniaturisation include a reduction in the size of electronic motherboards. It is very likely that end-users in the maritime and aviation security industries will make use of this technology in future. One of the main requirements of the project's electrical components was that they should be fast and secure. This led to a step by step development of electrical components such as the VMI format cupboard which was reduced from 150 kilograms to 5 kilos. The company ACRE (potential end-user) was an important external resource used for testing the product.

It must also be noted that the UNCOSS project features a dissemination strategy which involves producing academic publications, conference presentations and papers, and other forms of documentation (briefs to authorities, technical papers).

The only direct end-user in the **SOBCAH** project (PASR) was the Port of Genoa where the demonstration aspects of the project took place. One of the most important benefits is to have allowed for the realisation of improvements in situation awareness for the 'man in the loop'. The sharing of technologies and collaboration between participants in the consortium from industry was evaluated positively. Target end-users for the technology itself were port authorities and coastguards. SOBCAH demonstrated the extent to which the integration of data from other systems is needed to improve coordination in sea-based surveillance. The project promoted the importance of sharing and disseminating information between end-users, although their involvement was mainly indirect. The intention of the research results is to promote the pooling of operational know-how between end-users that presently use a range of different technologies so as to improve overall standards in maritime border surveillance systems.

While some successes can be noted in engaging with end-users, some projects experienced difficulties in engaging with operational end-users sufficiently early on during the R&D process and technical development of maritime surveillance technologies.

3.2.2 Interoperability in Maritime Security

Effective management of Maritime Security activities requires the capability to collect and merge data into a common and comprehensive picture to be shared among relevant organisations. However, the achievement of this capability is hampered by the fragmentation in the Maritime Security domain.

At Member State level, a wide range of organisations are involved in different aspects of Maritime Security. Furthermore, the EU still lacks an effective framework for ensuring better coordination on

Maritime Security issues, which could potentially maximise synergies with Maritime Safety initiatives. In this context, the main challenge is to ensure the smooth functioning of cross-sector operational cooperation between multinational authorities (e.g. the police, coast guard, intelligence, security rescue officials) through interoperable communication and rescue systems.

The **OPERAMAR** project attempted to fill an important gap by solving the issue of fragmentation between Member States caused by the persistence of national-specific procedures, legislations and systems that hamper interoperability, greater information sharing and improved coordination.

The project supported the definition of common requirements and operational procedures, as well as new common interoperability standards that should be adopted at national and local level.

Project(s):	**OPERAMAR - InterOPERAble Approach to European Union MARitime Security Management**
Project timeframe:	01/03/2008 – 01/05/2009 (15 months)
Lead Partner:	Thales Underwater Systems SAS
Total Cost:	€ 669,132
EU Contribution:	€ 669,132
Start Date:	01/03/2008
Project type*:	FP7 System Interoperability, Contextual Integrity

OPERAMAR consisted in the establishment of an EU and Associated Countries network of maritime stakeholders tasked with identifying interoperability challenges, for improving operational coordination. This study promoted cross-fertilization into organizations, structures and systems and provided, as a result, common requirements and guidelines, to increase situation awareness in maritime environment. OPERAMAR also suggested to the EU Commission recommendations in terms of future research programmes, projects and new standards.

OPERAMAR was about pooling the competence of national users belonging to EU Member States and Associated countries, European agencies and industrial partners all actively involved in the Maritime domain. This enabled the stakeholders to acquire better knowledge of Maritime Security user needs and define interoperability models, taking into consideration the challenging characteristics of the organizational environment in which they will be implemented. Common interoperability requirements were developed and translated into technical requirements. A strategic research roadmap was designed on the basis of recommendations made by the stakeholders.

As such, the OPERAMAR roadmap will contribute to future FP7 and other European security linked activities taking into account the work of the ESRIF.

With regard to progress in strengthening interoperability and standardisation outside the area of maritime surveillance, the **SECCONDD (SECure CONtainer Data Device)** project funded under PASR 2005 was designed to initiate the international standardisation of the technical interface between a secure container or vehicle and a data reader at a port or border crossing. The interface should enable law enforcement and trade officials to read security data, including stored information from internal security and location sensors. This project sought to find an easily applicable and interoperable solution in a context where stakeholders the transportation industry had already been working on and debating about the financial and operational benefits of 'smart containers' for several years. The standardisation of the interface is soon to be achieved.

Interoperability in Maritime Security – the end-user dimension

The **OPERAMAR** project led to the formation of a network of external end-users, comprised of between 20 and 30 stakeholders across Europe. In this context, the effectiveness of the methodological approach developed by OPERAMAR was tested in three scenarios, i.e. in the Mediterranean, the Black Sea and the Atlantic Ocean (Canary Islands). Then, the OPERAMAR network translated these interoperability requirements, into guidelines for technical requirements, common architectures and system specifications.

These incorporated suggestions from end users and stakeholders for improvements in the compatibility of all interfaces for data exchanges. The OPERAMAR strategic roadmap described the evolution of an interoperable approach to the European Union maritime security management from the multiple perspectives of organisations, institutions, legislation and regulations. The roadmap also aimed to identify priority areas for additional security research to facilitate development at Regional and European levels.

This project illustrates the extent to which cooperation among agencies and countries will be crucial in responding to commonly identified threats. OPERAMAR also shows how necessary it has become to engage with stakeholders in long term planning to take into consideration the predicted evolution of threats.

With regard to user involvement in **SECCONDD**, there was some user input into the project, however, because the technology is at an early stage in development, the exploitation of research results achieved through the project has been slow. However, it is expected that the initial progress achieved under SECCONDD will be strengthened through a follow-up project on secure containers with a strong demonstration element and a much larger budget under FP7 Call 3.

Various end-users took part in the activities of SECCONDD, such as shipping companies, port authorities and law enforcement bodies. This reflects the complexity of the supply chain in the container security industry. Regular consultations were undertaken with end-users and these organisations were also invited to participate in 2 workshops. While there was feedback on the project itself, there were disagreements between stakeholders as to who should bear the costs of developing the smart container technology.

Although the project made progress towards interoperability through technical standardisation work, promoting uptake of new technical standards was found to be highly dependent on the extent of willingness among relevant stakeholders to absorb the financial costs of technological upgrades. Another lesson was that technical standardisation requires long-term commitment and can be a complex process, with continuation needed as a research topic.

3.2.3 Protection of critical maritime infrastructure

Shipping carries 90 % of the world's trade. Cruise liners carry more than 12 million people each year. European liquid natural gas (LNG) imports from Africa and the Middle East are expected to quadruple by 2030. Incidents of piracy increased an estimated 10 % in 2007.

Increased maritime activity undoubtedly increases the risk of security incidents, including incidents near shore. As such, a considerable number of projects have focused on critical infrastructure protection in the field of maritime security. For instance, **SECTRONIC** attempted to improve the security of civilian ships (passenger and cargo carriers), energy platforms and facilities, and ports through advanced information, sensor, and response technologies. It aimed to develop an integrated security system combining surveillance, intrusion detection, and response to events and incidents.

Project(s):	**SECTRONIC Security System for Maritime Infrastructure, Ports and Coastal Zones**
Project timeframe:	01/02/2008 – 01/02/2011 (36 months)
Lead Partner:	Marine & Remote Sensing Solutions Ltd
Total Cost and EU Contribution:	€ 7,080,433 and € 4,496,414
Start Date:	01/02/2008
Project type*:	FP7 Capability project

The SECTRONIC initiative addresses observation and protection of critical maritime infrastructures: Passenger and goods transport, Energy supply, and Port infrastructures. All accessible means of observation (off shore, onshore, air, and space) of those infrastructures are networked via an onshore control centre. The proposed system is a 24h small area surveillance system that is designed to be used on any ship, platform, container/oil/gas terminal or port and harbour infrastructure. The end-users themselves can access a composite of infrastructure observations in real-time and will be able to shield the infrastructure by protective means in security-related situations.

The initiative is an end-users driven R&D activity. The overall objective of the SECTRONIC research project is to develop an integrated system for the ultimate security of maritime infrastructures covering ports, passenger transport and energy supply against being damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour.

In the field of critical maritime infrastructure protection, a similar project to SECTRONIC under FP7 is the **SUPPORT (Security Upgrade for Ports)** project, which aims to raise the current level of port security by integrating legacy port systems with new surveillance and information management systems. Furthermore, the SUPPORT project has a special focus on border control, aiming to secure uninterrupted flows of cargos and passengers while allowing for the effective elimination of illegal immigration and trafficking.

End user dimension - critical maritime infrastructure

SECTRONIC is an end-users driven R&D activity. The end-users represent the major market player in each of the three infrastructures: passenger transport, energy production, energy transport, commercial ports and combined military/commercial ports. The main end-users of SECTRONIC are port authorities.

Central to the project is the advice and testing by system end users, hence six shipping and energy related industry partners are also included as members of the SECTRONIC consortium.

R&D developers and end-users regularly discuss and exchange practical solutions for the security challenges faced by the commercial maritime infrastructures with the representatives of the three major maritime infrastructures stated above. Also the end-users are present to ensure that the developments do fit in their way of working.

End users have been particularly helpful in providing their input to the project's focus on efforts to develop new technologies that enable proactive capabilities in a security system through unambiguous warning, evasion, screening, and applying non-lethal force.

Project assessment

Finally, the eventual system developed under SECTRONIC will be able to demonstrate its effectiveness in field trials with a variety of end-users involved in the project. These include the Port of Rotterdam (Europe's busiest port), the Port of Spezia in Italy (a significant port for Mediterranean cruise ships), cruise ship operator Carnival Corporation, and BW Gas ASA who operate liquefied natural gas (LNG) and liquefied petroleum gas (LPG) carriers and other energy infrastructure elements.

The **SUPPORT** project directly involved end-users in technical design. Peer-to-peer communication and decision support tools incorporating semantic technologies were developed, using as far as possible standard open architecture software, accessible to all the port security stakeholders. The main advantage of using open architecture software was that the port security users could design add-on systems, therefore sharing their inputs both with other users and project coordinators. SUPPORT also included policy and standardisation proposals and training for participating port personnel as well as dissemination activities for other ports and stakeholders. End-users were therefore extensively present in research, information sharing and dissemination activities.

It appears that users often played a more significant role during project design and implementation in the field of critical infrastructure protection compared to other fields of activity such as improving surveillance systems. This can be explained by the fact that such projects have a strong practical aspect in the sense that they offer solutions directly applicable to already existing infrastructures. As such, end users can directly identify what works well and not so well and provide guidance to project coordinators and other stakeholders as to how solutions could be technically improved.

Conclusions & Recommendations 4

4.1 Conclusions

Compared with other thematic areas within FP7 SEC, Maritime Security research has longer research and development lead times making it difficult to assess the likely effectiveness of research results. Many projects involve early-stage research. Systems and systems of systems integration is required in order to ensure greater interoperability so that technologies can be deployed.

Notwithstanding, promising technological developments and progress towards key objectives was identified. For example, some projects helped to develop algorithm-based technologies that should improve the detection of abnormal vessel behaviour in future.

Progress has been made towards integrating maritime border surveillance systems that bring together existing monitoring and tracking systems and ensure their interoperability. Land and sea-based sensor networks belonging to different agencies responsible for maritime security across different EU countries are in the process of being networked and made interoperable. However, completing the systems integration process will take time.

Progress has also been made in the implementation of integrated maritime border surveillance systems that incorporate new surveillance technologies with more conventional monitoring sensors. For example, through the SEABILLA project, **a** large-scale demonstration project, an integrated, net-centric approach to blue-border control will be promoted through the linking and networking of sensors and information fusion from satellite-based GMES data, Unmanned Aerial Vehicles (UAVs) and coastal and maritime-based surveillance stations to help improve common intelligent operational picture. Achieving the full integration of different data systems will take considerable time.

Some projects have utilised a combination of space-based technologies and GMES technologies funded through the FP7 space programme such as SEABILLA and SECTRONIC. This provides a useful illustration of synergies between the FP7 space and FP7 security programmes.

Maritime security projects have promoted the development of improved detection systems and their better inter-connectedness across wide maritime areas. Demonstrations have been organised of innovative radar systems better able to detect, track and classify small vessels moving at relatively high speeds. This is a distinct advantage when protecting against threats such as pirate or terrorist attacks**.**

Common information sharing mechanisms are being developed at EU level to encourage data sharing on maritime surveillance. These will draw on the different data sources mentioned above (i.e. land, sea, air and space-based) and have strong potential to achieve cost savings for public end-users involved in maritime security through improved data sharing leading to economies of scale in terms of the level of investment needed to improve national maritime border surveillance systems.

Areas of common research interest were identified between civil and defence research[1], such as the use of Unmanned Aerial Vehicles (UAVs) and maritime surveillance stations to improve common operational picture for public agencies. The Cooperation Framework Agreement between the European Commission, the EDA and ESA provides a mechanism for exploring potential research synergies.

Conclusions & Recommendations

4

Public authorities have played a key role on critical maritime infrastructure protection projects in assisting researchers to identify gaps and vulnerabilities in protection systems in the event of terrorist attacks. End-users such as port authorities and law enforcement bodies have been critical stakeholders in projects such as SECTRONIC and SUPPORT. This has been vital in developing a better understanding of new and emerging threats.

A comprehensive approach to the protection of critical maritime infrastructure has been promoted through FP7 Security that encompasses legal, organisational, and technological aspects. The objective is to ensure the secure and efficient functioning of European ports with uninterrupted flows of cargos and passengers.

With regard to research quality, it is too early to assess the achievements given the long-term R&D time horizon required to implement complex projects in the maritime surveillance field. These often require technological innovation to solve interoperability problems, systems of systems integration and information fusion. They furthermore require coordination between a diverse range of stakeholder organisations.

However, the types of organisations that have been involved in maritime security and surveillance projects are indicative of research quality. The programme has attracted the participation of a number of large companies active in the maritime surveillance field, such as Indra, Selex Integrated Systems, EADS and Thalys etc. They have also attracted the active participation from end-user organisations, such as port authorities, the Civil Guard (Spain), the Maltese coastguard, the French navy and police forces. Key players at EU level, notably Frontex have also actively inputted as a potential user to some projects.

Over the long term, European citizens should benefit from investment through FP7 SEC in maritime security and surveillance projects. Threats such as terrorism, illegal immigration and people trafficking, drug smuggling and the need to improve surveillance of the EU's enlarged external borders are among the primary concerns of many citizens.

4.2 Recommendations

A number of recommendations are now provided. It should be noted that the evaluation scope focuses on PASR 2004-2006 and the first two calls in FP7 SEC (2007 and 2009). Some recommendations are already being addressed and will require ongoing funding commitment during the remainder of FP7 SEC, reflecting the long-term nature of achieving the goals set in the area of strengthening the integration of maritime surveillance systems and improving technologies for wide-area surveillance and the detection of small vessels.

Ongoing support is needed to achieve interoperability through systems integration, the networking of maritime sensors and the development of common interfaces for heterogeneous sensor technologies. Some progress in this regard has already been achieved via the SEABILLA project.

There is a need for further investment in secure data sharing between relevant public authorities responsible for maritime security. This could be accomplished through the development of a harmonised Global Maritime Surveillance Architecture, and setting a common framework for the validation of "EU Reference Solutions" that could be developed through FP7 SEC R&D projects with minimum common technical requirements for interoperability and uniform technology standards.

Conclusions & Recommendations 4

Strengthened information-sharing is needed to derive synergies between maritime safety and security thereby maximising the efficiency and effectiveness of security measures in sea and coastal areas. A Commission Communication on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain (COM (2010)584) represents the first step towards achieving this objective.

Research topics in the area of maritime security within FP7 Security need to be planned in line with evolving EU policy developments. In particular, the adoption of EUROSUR, which requires the development of an integrated border surveillance system will need to be taken into account in defining research topics in Calls for Proposals during FP7 and in planning for FP8.

There remains further scope in future to better integrate GMES and satellite based technology into integrated maritime surveillance systems. This will ensure the seamless unification of maritime border surveillance requirements with end user needs.

Interview list A

No.	*Name/ position*	*Organisation*	*Organisation type*	*Project (where applicable)*
1.	Sonia Gracia Anadón	Indra, Spain	Large firm	SOBCAH – Surveillance Of Borders, Coastlines and Harbours
2.	Vukovar Port Autority	Croatia	User	UNCOSS
3.	Guillaume Sannie	Commissariat Energie Atomique Cea	User	UNCOSS
4.	Julien Deleu & Nicolas Dosselaere	Eurosense	Large firm	WIMAS
5.	Michael Naylor	Thales Underwater Systems Ltd	Large firm	SECCOND
6.	Tom Metz	HSF (software and applications development)	SME	AMASS
7.	Thomas Anderson	Carl Zeiss Group	Large firm	OPERAMAR
8.	Paolo Saltieri	European Commission	Security Research Unit, Maritime Security project officer	NA

Maritime Security in PASR / FP7 work programmes B

Maritime security

Work Programme/ Calls	Types of Maritime Security Activity Supported
PASR 2004	**Improving situation awareness** Aim: to identify the main threats that could affect Europe, particularly land and sea borders and assets of global interest, by appropriate information gathering, interpretation, integration and dissemination leading to the sharing of intelligence. Concepts and technologies for improved situation awareness at the appropriate levels could be developed and demonstrated. Relevant issues for Projects: - Demonstration of concepts, technologies and capabilities for situation awareness systems, to enhance surveillance of land and sea borders, especially supporting measures for new land borders in EU-25 and assets of global interest. - Demonstration of appropriateness and acceptability of tagging, tracking and tracing devices by static and mobile multiple sensors that improve the capability to locate, identify and follow the movement of mobile assets, goods and persons, including smart documentation (e.g. biometrics, automatic chips with positioning) and data analysis techniques (remote control and access).
PASR 2005	**Improving Situation Awareness (e.g in Crisis Management, Antiterrorism Activities, Or Border Control)** Similar aims to those set out above for 2004
PASR 2006	**Improving situation awareness (e.g. in crisis management, anti-terrorism activities, or border control)** Similar aims to those set out above for 2004 and 2005. But also provides support for projects involving the development and demonstrations of: Novel concepts, architectures and technologies for locating illegal immigration at the EU borders
FP7 2007	**Topic SEC-2007-3.2-01 Main port area security system (including containers)** Technical content / scope: The task is to create an integrated port area (land, sub-surface, water) security system capable of providing accurate situational awareness, based on various sources and integrating all result streams, and alerting security operators to required interventions, while doing uninterrupted logistics business. The system will improve situation awareness at main ports through the monitoring and tracking of complex port environments as a consequence of the continuous arrival and departure of cargo (containers), ships, vehicles, staff and passengers, and also the potential threats by boats and swimmers etc. This will include mobile and fixed detection and recognition systems in order to provide intelligent event detection, supporting the decision control; investigation into cargos scanner outputs fused with shipping manifest information, external risk assessment and a-priori threat knowledge which allows for automatic anomaly detection. Call: Security Research Call 1, Funding scheme(s): Collaborative project. **Function: Situation awareness & assessment (surveillance)** **Topic SEC-2007-3.3-02 Surveillance in wide maritime areas through active and passive means** Technical content / scope: The task is to develop novel, automatic surveillance capabilities through manned and unmanned platforms (land / sea / air / space), equipped with several sensors and sophisticated data fusion processes. This could involve the combination of tracing technologies, digital signal processing, image and pattern processing with data and information management. Call: Security Research Call 1 Funding scheme(s): Collaborative project
FP7 2009	Area 10-3.2: **Integration projects** The Security Research Call 2 calls for the following actions:

Maritime Security in PASR / FP7 work programmes B

	Topic SEC-2009.3.2.1: **Main port area security system** Technical content / scope: The task is to conceive and design a state-of-the art integrated surveillance / security system capable to satisfy border control constraints at main ports. The system shall take into account their organizational structure and operational modalities, including, if appropriate, sea hinterland traffic and transport-logistics relations. The system should be adaptable to different configurations of ports and it should allow the integration of existing legacy components. This system should combine and integrate preventive measures to protect port facilities against threats of intentional unlawful acts. It should be suitable for implementation in the complex port environment and should fit into the normal flow of operations without introducing delays. It should provide persistent surveillance of port facilities, monitoring of goods, personnel and passengers, tracking of vessels, vehicles and containers and should be capable of alerting port security operators for activation of immediate and effective reactions. The system will integrate, in a single security network: • information acquisition, • handling and exchange tools, • consideration should also be paid to the facilitation of information sharing within and between main sea ports, and/or between sea ports and hinterland terminals and operational services, such as police or other intervention forces. The system should be based on a sound security gaps analysis and should also include elements for the training of security operators enabling them to act whenever required minimizing the loss of lives, goods and the interruption of logistic business. Call: Security Research Call 2 Funding scheme: Collaborative project. Activity 3: **Intelligent surveillance and border security** -Sea borders surveillance system - Extended smart borders The task is to improve sea border surveillance. Key problem areas in achieving this are: • Networking of relevant (heterogeneous) sensors, sensor networks and other information sources. Interoperability and integration are the key elements. • Integration and fusion of data and information from the sensors, sensor networks and other information sources
FP7 2010	**Demonstration programme (SEC-2010.3.1-1 European-wide integrated maritime border control system - Phase II** The EU has recently introduced Joint Maritime Operations coordinated by FRONTEX involving various services (Navies, Coastguards, Customs, Border Police, etc.) and assets (patrol boats, frigates, helicopters, aircraft, etc.) with limited interoperability (modus operandi, procedures, language, communications assets). Further development of joint operations calls for interoperability and standards, operational as well as technical, between the different units. This concerns many technical systems, including communications and geographical information systems. For the 2015 time horizon, innovative solutions should be set up to permanently monitor and track all type of ship traffics, vulnerable trading lanes, maritime ports and extended border zones, and to detect abnormal behaviour to understand and identify risks and threats at an early stage and to respond as appropriate in full respect of human rights and in particular the rights of asylum seekers. This future generation of maritime surveillance capabilities should allow:

	• Permanent and all weather coverage of maritime areas; • Continuous collection and fusion of heterogeneous data provided by various types of sensors and other intelligent information from external information sources; • Supervised automatic detection of abnormal vessel behaviours (tracks and activities) and to generate documented alarms; • Understanding of suspicious events and early identification of risks and threats from series of detected spatiotemporal abnormal vessel behaviours (alarms); • Detection and tracking of scrapping vessels used for illegal migration; • Detecting and preventing illicit movements of persons and goods through multilayered and end-to-end surveillance. **Integration project - SEC-2010.3.2-1 Monitoring and tracking of shipping containers** The aim of the research is to provide the technology and information gathering mechanisms contributing to the implementation of a system for the monitoring and tracking of EU (inbound and outbound) container traffic, possibly at the global scale, effectively identifying (and possibly coping with) security threats. Such traffic may come in on a variety of vectors (i.e. trucks - trains, barges and increasingly feeder vessels, but predominantly by intercontinental sea transport). The system should be based on a sound risk based approach to container security, i.e. the system should be capable of identifying possible manipulations and all those containers that pose a threat to security. The system should combine different technologies, like container tracking and localization, tamper proof sealing, container-integrated sensor technologies, statistical methods and data available on the container to provide a holistic approach.