Final publishable summary report

Grant Agreement number: 242112

Project acronym: SUPPORT

Project title: Security Upgrade for PORTs

Funding Scheme: SEC -2009-3.2.1 IP

Period covered: from 01/07/2010 to 30/06/2014

Name, title and organisation of the scientific representative of the project's coordinator:

Dr Fernando Caldeira-Saraiva, Project Manager, BMT Group Ltd

Tel: +44 (0)20 8943 5544

E-mail: fernando@bmtmail.com

Project website address: www.support-project.eu or www.supportproject.info

Contents

1 Executive Summary

About 90% of EU's external trade and 40% of internal trade is transported by sea. This corresponds to 3.5 billion tonnes of freight loaded and unloaded in EU ports each year. While individual port security breaches may cause much damage in themselves, the disruption that such security incidents cause to the supply chains can also become very costly. Thus, port security remains of paramount importance for Europe both due to direct threats to life and property as well as the potential for crippling economic damage arising from the effects on the supply chains.

Ports represent significant challenges when implementing new security measures. They cover large areas, they have very complex operations, they service large numbers of passengers and they process large amounts of goods. As well as efficient surveillance and access control, this requires efficient organisational and technological interfaces linking ports to border control authorities, the police and other intervention forces, as well as transport and logistics operators.

Ports also represent the intersection between supply chain security measures (e.g., the USA C-TPAT and CSI initiatives and the WCO SAFE Framework) and ship and port facility security measures (e.g., through the International Ship and Port Facility Security (ISPS) Code). A specific challenge for ports is to integrate these types of measures into an integrated security approach.

Considerable progress in port security has been achieved in recent years. 2004 saw the arrival of the International Ship and Port Security Code (ISPS), offering a consistent framework for evaluating risk. But, the lack of measurable detail and implementation processes, led to differing security practices across European ports. SUPPORT offers a new approach to maritime and logistics security via an interactive, real time, dynamic dashboard. The Port Security Management System (PSMS) is a web-based tool designed to assist security professionals in monitoring and developing port security in line with the ISPS code and other legislations. In particular, it addresses the concerns of EC regulation 725/2004 and EC directive 65/2005, thus facilitating the inspection regime defined in Commission regulation 324/2008.

SUPPORT engaged representative stakeholders to guide the development of upgraded preventive and remedial security capabilities in European ports. Daily port operations with actual security systems were analysed and good and bad practices seen in port managing organisations, port authorities, and other stakeholders were noted and "lessons learned" were used in the SUPPORT solutions.

SUPPORT delivered:

- '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 were complementary to and usable by other EU projects and initiatives. Emphasis was given to bringing together advances from international and European research on security and border control with results from the main EU projects in maritime and intermodal transport, specifically those concerned with security and interoperability issues.

The aim of SUPPORT was to address 'total' port security upgrade solutions encompassing legal, organisational, technological, training and human factors perspectives in order to facilitate:

1. Secure and efficient operation of European ports in the context of sustainable transport.
2. Uninterrupted flows of cargo and passengers.
3. The suppression of attacks on high value port facilities; illegal immigration and the trafficking of drugs, weapons and illicit substances.

All this was in line with the efforts of EU member states.

SUPPORT also liaised with European and other international organisations, including WCO, IMO and ISO/CEN, to ensure that SUPPORT solutions were consistent with security standards.

2 Summary description of project context and objectives

2.1 Context

1. Business challenge

The overriding challenge for next generation port security systems is to support *efficient secure port operations and border control*, in other words to provide enhanced security without cost penalties by:

- addressing security management as part of the mainstream strategic management of the port;
- integrating security solutions into operational processes with increased automation in monitoring and co-ordinating activities;
- supporting the development of security competencies in ports and leveraging the capacity of their collaborating organisations;
- promoting efficient collaboration between all stakeholders involved in port security at regional, national and European levels.

Enhanced security means reduced probability of a major incident, better access control, more efficient early threat detection and higher resilience. Higher resilience in this case means low impact of disruption and rapid recovery to normal operations.

2. Port security priorities

With reference to ISO 28001, the minimum threat scenarios to consider in security assessment are:

1. *Intrude and/or take control of an asset (including conveyances) within the supply chain.* This may be to damage or destroy the asset, damage/destroy outside target using the asset or goods, cause civil or economic disturbance or to take hostages/kill people.
2. *Use the supply chain as a means of smuggling*. This may be to smuggle illegal weapons or other contraband or terrorists or other criminals into or out of the country.
3. *Information tampering.* Locally or remotely gaining access to the supply chain's information systems for the purpose of disrupting operations or facilitating illegal activities.
4. *Cargo Integrity.* Tampering, sabotage and/or theft for the purpose of terrorism or other criminal acts.
5. *Unauthorized use.* Conducting operations in the international supply chain to facilitate a terrorist incident (e.g. using the means of transport as a weapon).

Note that also "Weapons of Mass Destruction" (WMD) is sometimes listed as a specific security threat. SUPPORT did not address this threat directly, but assumed it is covered through various combinations of the five threat scenarios above.
For SUPPORT, these scenarios have been condensed into three main cases:

1. Direct attacks to cause loss of life or on high value units in order to blackmail/embarrass authorities and disrupt the port processes.
2. Organised crime (including terrorism) involving illegal immigration, smuggling (narcotics, weapons, explosives, etc), large-scale or continuous theft and economic blackmail.
3. Information tampering within the SUPPORT infrastructure.

As the primary objectives of terrorist attack are to cause publicity and to disrupt normal operations (the supply chain in this case). Thus, for direct attacks, the most likely targets are passenger ship terminals, oil or gas terminals or other installations/buildings where attacks cause high public attention.
In line with most other security initiatives, SUPPORT mainly focused on the following security-enhancing measures:

1. Efficient exchange of information between port and supply chain, ship and authorities.
2. Inspection, tracking and surveillance, particularly of containers.
3. Comprehensive access control of passenger terminals, ferries and cruise liners, not only for passengers and crew but also for goods, cars, buses and personal belongings.
4. Detection of threats from the sea (small, fast boats, hijacked vessels, and underwater threats) and surveillance and protection of vulnerable port targets.

3. *Technical challenges*

It is suggested that the key technical challenge is *'optimising' the legal, electronic and human interfaces and flow of information between port stakeholder organisations and their security systems*. Such optimisation involved:

- rationalising and where possible harmonising legal requirements across Europe;
- establishing interoperable processes and systems between port security stakeholders;
- developing a security culture and competences in the whole network of stakeholders affecting or being affected by port security.

2.2 Project Objectives

The primary project objective was 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 facilitated optimised interchange of surveillance and administrative information as well as threat and risk alerts between port stakeholders, thus enabling cost effective multiple use of available data in tailored decision support systems. SUPPORT solutions:

- provide integrated state-of-the art surveillance/security systems for border control (ensuring persistent surveillance of port facilities, monitoring of goods, personnel and passengers, tracking of vessels, vehicles, containers and underwater threats);

- assist port security operators in decision making throughout the security management cycle (i.e. hazards prediction and modelling, risk assessment , preparedness, alertness and responsiveness);
- take into account the port's organisational structure and operational modalities (i.e. being adaptable to different port configurations and therefore allowing integration of any pertinent legacy applications);
- ensure that differing legal and regulatory constraints and international agreed standards for security are met in a cost effective manner.

The project aimed to launch co-ordinated training campaign to ensure that ports and authorities across Europe use similar standards to perform to the same level and are able to communicate with each other using 'the same language'. The specific implementation objectives were:

1. Analyse requirements along security, legal, market and technology perspectives to produce the detailed project requirements specification and success criteria**.** Special attention was to be given to security gaps and threat scenario analysis pertaining to the needs of Europe's main ports; Small to Medium Ports were also analysed in order to establish a classification of their specific requirements and make it possible to give them the same improvements.
2. Develop Generic Models for EU Ports Security including:
   a. Security hazards/threats classification for large and small ports and classification of related data sources.
   b. Security risk management models covering the whole security risk management cycle (i.e. hazards prediction and modelling, risk assessment, preparedness, alertness and responsiveness) for monitoring the port area and port facilities for both land and sea and monitoring of flows of goods and passengers.
   c. Organizational strategies taking into account the overall port list of critical indicators and supply chain security; also reference security information exchange agreements.
   d. Compliance management processes for security directives with particular attention to improved information exchange through National Single Windows.
3. Develop strategic Security Upgrade Solutions in line with the requirements analysis outputs from objective 1 focusing on:

   a. Security sensors for next generation port solutions. These address key issues such as stakeholder selection of a well-balanced sensor suite with potential for future development, networking and information handling to feed into event correlation and diagnostic modules in decision support systems.
   b. Security communications infrastructure solutions with specific reference to bearer independent technologies that allow seamless communications across diverse communications media and protocols.
   c. Optimising security management of container handling with respect to different handling stages at the ports, stakeholder communications and dealing with false positives.
   d. Deception recognition when tracking threats (i.e. addressing the problem of recognising vessels and underwater threats that are attempting to deceive or circumvent a port tracking system).
4. Provide an ICT Platform for designing, developing, deploying and maintaining next generation security solutions for large and small-to-medium ports. The

platform aimed to utilise a collaborative peer-to-peer architecture for the different port security organisations. The design of the platform leverages on existing technologies based on current state-of-the-art open software engineering standards and ongoing standardization efforts from W3C and OASIS. In particular the platform was to be mainly based on an event driven Service Oriented Architecture (SOA) concept and current research efforts towards Semantically Enabled Service Oriented Architecture (SESA). Special attention was to be given to the problem of security and confidentiality of shared data (in accordance with mandatory national law) and in dealing with privacy rated issues. The SUPPORT Platform aims to provide:

a. A base platform to implement the agreed architecture and to provide communications modules, service and workflow engine and security data management components.
b. Data fusion tools specifically designed for port security sensors and intelligence information streams to provide detection of abnormal behaviour. These specifically address difficulties in adapting to new scenes or to dynamic environments.
c. Tools to resolve interoperability conflicts and to provide mechanisms for automated discovery and integration of suitable services (within the port network of security peers).
d. Model based decision support tools for security operators and other legitimate users in ports. These tools were to adapt real-time information flows according to user role and communication profiles.

5. Provide Port Security Upgrading Management & Training support services (using the ICT Platform). These services assist ports and other security stakeholders both with the change management process and with the actual implementation SUPPORT solutions aided by knowledge management and training services**.**
The main services are:

a. Tools for the design analysis and optimisation of port security solutions. This allows port operators to assess their systems and to establish the right level of enhanced protective measures, given specific threats to critical assets, their vulnerability and criticality.
b. Port Security Knowledge Management tools including a digital library for port security and an information observatory. Competence management tools to help ports identify security knowledge gaps and training needs for aligning the workforce in light of the changes.
c. A Training Programme including training simulators for port security operators and other relevant actors. The training simulators prepare security operators to use effectively the SUPPORT decision support services.

6. Organise full scale demonstrators of SUPPORT based solutions in two representative European ports (Gothenburg and Piraeus). Each demonstrator was to be integrated with existing legacy systems and aided by simulation in order to economically apply the full concept. The demonstrators were to be used to evaluate the feasibility and the benefits of the SUPPORT approach. The demonstrators were to be used to carry out extensive technical evaluations as well as cost benefit analysis of the implemented solutions. The full scale demonstrators were to be augmented with a broader evaluation programme by members of a *European Ports Security Forum (PSF).* They were to provide case studies or test beds for specific upgrade solutions matching different types of security gaps.

7. Provide focused dissemination including:
   a. An Interactive web SUPPORT Prototype with ‘secure’ dissemination and acquisition interfaces for different categories of port stakeholders. These were to be used to facilitate browsing and navigating through SUPPORT models and tools, for participating in forums and also for submitting comments or reports in the key areas addressed by the project. During the later stages support for an implementation guideline was to be provided.
   b. A European Ports Security Forum was to be organised by ECO SLC to actively involve a growing number of port security stakeholders in SUPPORT.
   c. A dissemination programme including an annual conference and a programme of biannual stakeholder workshops. This aimed to allow us both to obtain early stakeholder feedback and to maximise the potential impact of the project results. An important part of dissemination was to be proposals for standardisation and policy recommendations.

8. Create important market opportunities for European industry and establish leadership in port security management by demonstrating the long term sustainability of the project outputs through concrete exploitation plans.

3 Main S&T results/foregrounds

3.1 Requirements Analysis and SUPPORT Specification

3.1.1 Gap and Threat Scenario Analysis

Initially, a list of port security threats was compiled. This work was based on a variety of sources and methods, in order to cover a broad range of threats. The approach combined traditional analytical techniques with more creative elements; the latter to ensure that the process would be proactive and not confined to risks that have materialized in the past, while the analytical element ensured that previous experience was properly taken into account and use was made of available data. Initially, a core list of 30 threats was generated using a combinatorial method. In a number of review rounds and working meetings, this list was edited and extended, producing a final list of 100 threats.

In the next step, a subset of these threats were selected for further analysis. The selection criteria were mainly representativity and diversity: they should each catch the essentials of several others and as a whole, cover the broad range in the initial list. The selected threats were then grouped according to common loss events. For each such loss event, a number of relevant risk control measures were identified. Using a quantitative risk analysis model, total risk figures for the events were derived. From this, it was possible to identify candidate security gaps, as those loss events showing a high risk level, despite the control measures in place.

The result from the risk analysis was the subject of review at two workshops, where invited port stakeholder, e.g. Police, Customs, Port owners and operators commented upon and added to the material. From these meetings, more observations concerning port security was recorded, both general and specific for the ports represented at the meetings.

In summary, this work identified a number of port security gaps that are perceived by port stakeholders as both real and serious.

We have also in the stakeholder dialogue identified broad groups of risk control measures that would significantly improve security: examples are access control; search of vehicles and persons; automated surveillance; awareness and sharing of threat information between stakeholders; employee vetting, and probably most important, training, so all measures can attain their full level of effectiveness.

3.1.2 Stakeholder Requirements

In order to identify and document the generic stakeholders' requirements several approaches have been followed. Among these are a regulatory regime analysis focusing on identification and classification of international, European and national regulations influencing port security either directly or indirectly; a qualitative data collection at three EU ports differing in size, region and cargo types handled; a quantitative market survey regarding the adoption of security upgrades and studies of existing initiatives related to security.

Main conclusions are that ports differ in many ways, such as owner structure, cargo types (types of terminals), whether the port handles international cargo, etc. In addition the large number of various stakeholders adds to the complexity. Hence, the process of establishing generic stakeholders' requirements is a lengthy process that will continue throughout the project. It is also clear that 'reference' solutions for enhanced port security to be produced in the project (WP5) will need to be customised / adapted on a case to case basis. Therefore, a key requirement for the SUPPORT ICT Platform, is to provide assistance for the customization processes. Customization efficiency could be assessed in producing the SUPPORT Demonstrators and Case Studies (WP6).

There are however similarities enabling us to create a set of generic stakeholders requirements. Such similarities include (but are not limited to) compliance with relevant rules and regulations, the need for operational efficiency and quantifiable measurements for successful implementation of security upgrades. It should be noted that compliance with relevant rules and regulation is in itself not necessarily dealt with in the same way by all ports and stakeholders but an initiative related to analysis of differences in the way regulations are interpreted and applied in different EU States did not provide conclusive results and further research is needed.

We were also able to create a generic information exchange model which proved applicable at all three ports. The model focus on information exchange related to port security and documents how information exchange should be supported in different ways such as direct (phone/VHF) and indirect (e-mail/information system to information system), structured or unstructured communication. Three layers of interaction have also been identified and this enabled us to focus on issues such as secure data transfer as well as challenges related to exchange of business sensitive information.

3.1.3 Security technology and assessment and forecasting

SUPPORT surveyed key technologies that should be considered in upgrading port security solutions and to develop technology scenarios for 2020 including estimates of impact on cost and security performance indicators. It comprised of

- a review of surveillance technologies for priority security-enhancing measures
- a survey of current XML-standards
- a review of European initiatives and projects dealing with interoperability issues
- a description of how SafeSeaNet can be evolved to a national single window allowing interconnection of all Member States.
- a review of a number of EU projects investigating how they deal with interoperability issues and how these technologies could be used within the SUPPORT project.
- a study of technologies enabling electronic and automated identification of vehicles, freight containers, returnable transport units and packages to maintain port information on expected movements advantages and selection criteria for security intelligence.
- an examination of the drivers for the deployment of RFID from a security management perspective and the ways of integrating Internet of Things technologies in security sensor networks.
- the development of technology scenarios for 2020 that illustrate groups of technologies that have been considered to be relevant for port security within

a ten year perspective. These scenarios were produced with a workshop method, in which a group of stakeholders and experts were involved in identifying technology related changes that they believed would have a very strong impact on port security in 2020 within the areas, security, transport & logistic and threat technologies.

3.2 Port Security Models

3.2.1 Classification of port security hazards/threats and information sources

A Port Security Threat Taxonomy as well as lists of information sources and their classification was developed. The final results were used in the demonstrators of SUPPORT. The Port Security Threat Taxonomy has a number of different components that are related to each other in the ontology produced in work package 4. The work was carried out mainly by distribution questionnaires on relevant terms to include to port stakeholders and experts.

3.2.2 Security Management Models

EU ports security stakeholder requirements and development consisting of the following components:

- Analysis of coverage and suitability of existing security management models.
- Classification of port security threats and related information sources.
- Procedures for the use of security management models in changing port environment.
- Library of port security management models (computer- readable models and associated vocabulary and detailed scenario descriptions of possible threats and possible responses to them).

The focus of the models is on the terminal operator and it's Port Facility Security Officer. The port area plenty or operating organisations, different regulatory requirements and large throughput is a challenging target for security management. The port is a one node in the supply chain network which has not fully view of the whole supply chain which must be taken into account in the security management planning and implementations. Security management framework and the practices used in a port have developed greatly since 2001. Global auditable security management requirements and standards have been published. Supply chain security management systems (ISO 28000 series) standard umbrella was published in 2007. The development to be seen in the near future is to leave the “supply chain” away from it, so the standard would be a general security management system standard. This will surely increase the use of the standard. The mutual recognition decision of the AEO and C-TPAT programmes in November 2011 will also harmonise the systems.

We presented the general port security risk management models and models related to the 11 Support port upgrade areas. The focus is in Threat and Vulnerability Assessment (hereunder continuous improvement), Security Upgrades and Operational Support. The models were used to suggest security upgrade solutions, taking into account the cost-benefit factors of the available technology. These models serve two purposes namely:

- As requirements for the SUPPORT ICT Platform development and associated applications development
- As a knowledge platform for terminal operators publicly available at the SUPPORT Knowledge Platform

3.2.3 Organisational models & security information exchange agreements

SUPPORT provided an organisational reference model to help port security stakeholders improve information exchange and co-operation.

SUPPORT addressed key organisational factors affecting port security management, covering the three SUPPORT applications:-

1. Threat and Vulnerability Assessment
2. Security Upgrade Requirements (covering the 11 areas of focus developed in the earlier stages of the SUPPORT project)
3. Operational Support

Organisational models for port security stakeholder networks were reviewed, examining roles and responsibilities, and will suggest moderating mechanisms to facilitate coordination.

3.3 Security Upgrade Solutions

3.3.1 Security sensors for next generation port solutions

SUPPORT provided a guideline for selection of sensor upgrades in ports and a description of a system for detection of Sea Side Intruders into a Port. The guideline can be used for three different purposes:

1. To give the PFSO or PSO a way to form an opinion of what sensors are needed independent of any security system provider.
2. To give the PSO or PFSO a systematic way to evaluate and motivate what security upgrades that are needed.
3. To supply a tool for security systems providers to facilitate the dialog with port security decision makers.

The Sea Side Intrusion Detection System was designed to be demonstrated in Gothenburg in 2014. The system resides in a grey area regarding what organisations which really are responsible for detecting and countering approaching threats from the sea side.

3.3.2 Security communications infrastructure

SUPPORT provided guidelines on the security communications infrastructure for improved quality-of-service (QoS) and bearer independence, comprising the following components:

- Guideline for upgrading security communications infrastructure
- Solutions for communication gateways

3.3.3 Security management of container handling

SUPPORT provided guidelines for optimising the monitoring process of containers with respect to different handling stages at the ports and facilities for implementing the guideline; it consists of the following components:

1. Optimisation of the monitoring process of containers with respect to different handling stages at the ports.
2. Guidelines for integration of monitoring technologies to port environments.

The work was performed in the following steps:

1. Modelling of the container processes in ports
2. Identification of loss events and threats
3. Identification of the sensors to respond to the threats
4. Scenario analysis and guidelines for improving the monitoring process
5. Requirements for integrating the monitoring technologies to port information systems
6. Testing guidelines and requirements in case studies
7. Evaluation and refinement in demonstrator.

The work was performed in collaboration with the CONTAIN project which is developing a European Container Safety Framework (ECSF).

3.3.4 Waterside Threat Detection in Ports

SUPPORT has investigated the state of the art and current methods of waterside threat detection in ports. Focussing on underwater threats a system has been created to address the current and emerging issues. The main focus of the system is being dynamic to prevent avoidance of the system and being low cost, so that it is affordable compared to currently available systems. Two homogenous AUVs have been designed and created with modularity to allow the use of different sensors as technologies improve and develop in the area. The AUVs have been designed to accomplish a number of tasks that allow them to work both with the SUPPORT system and as a standalone system. They can perform constant monitoring of the port and an area to ensure that no intrusions are made into the port, either from divers or fast moving vessels. They can also be used for monitoring the key infrastructure of the port for any possible threats or explosive devices. Finally they can be used as an on demand tracking and verification system when combined with the SUPPORT system. In order to create a working prototype for the project five main areas were developed:

- The design of a new low-cost AUV with full six degree of freedom motion control
- The building and creation of the AUV in a modular form allowing for multiple payloads and sensors.
- Simulations of sonar data to classify different noise signatures and allow the development of detection algorithms
- DATMO (Detection and Tracking of moving objects) algorithms for threat detection
- Integration of communications system to allow communications with the rest of the SUPPORT system

The system was tuned and calibrated against simulated data before being testing in multiple sites and geometries to fully test the capabilities of the system, the system has been trailed against divers both in inland reservoirs with divers in rebreathers and in the ports of Gijon, Lisbon and Piraeus against divers.

3.4 Security ICT Platform

3.4.1 SUPPORT Platform Architecture

We developed a features specification, usage scenarios and conceptual architecture for the platform. The complex operations and interactions within and between the various physical and non-physical components that make up the data streams required to reason about port security create a need of an innovative middleware dedicated to this domain. For this purpose the SUPPORT Security Semantics Layer (SSSL) architecture has been developed consisting of a modelling infrastructure, and data fusion framework. The Modelling Infrastructure is composed of the port risk assessment, terminal and port operations, and performance management including economic models. The Security Reasoning Engine component acts a Middleware to link these models and internal/external data systems together in a SUPPORT solution. The middleware also provides the link between this infrastructure and the graphical user interface of a SUPPORT Solution.

Adopted techniques include using the Service-Oriented Architecture (for standards based component re-use and technology independence) and Cloud Computing (scalable third-party hosting environments) hosting support. The platform component architecture should reflect enablement for these approaches.

The initial architecture is defined through the TOGAF framework, supporting the features of a platform through a multi-layered, service-based approach focusing on core applications, development, support, data, and management services. Additionally the platform incorporates sophisticated meta-data repositories for reasoning and in particular the quality assurance of SUPPORT solutions.

3.4.2 Data Fusion Tools

We described the current system design plans for the Gothenburg demonstrator a, including an illustrative scenario. We provided an introduction to information fusion and discussed the video analytics functionality that will be developed in SUPPORT.

Of the 11 focus areas of attention for SUPPORT, this work is primarily relevant for Access control, Monitoring and surveillance performances, and High resilience concepts.

3.4.3 Semantically-enabled Data Stream Processing

We provided an introduction to the support ICT platform and data stream processing. We described supporting ontologies for the port security domain. The semantically-enabled data stream processing software was detailed including architecture, internals and user guide. We provided a use-case scenario that demonstrates the capability of such a system in the context of port security.

3.4.4 Port security operational decision support services

We provided an introduction to decision support systems and described the tool Impactorium, which is used for information fusion and decision support in the SUPPORT Port Security Operational Support (PSOS) solution.

Of the 11 focus areas of attention for SUPPORT, this work is primarily relevant for Threat and vulnerabilities assessments and control measures and Monitoring and surveillance performances.

3.5 Port Security Upgrading Management and Training

3.5.1 Analysis and design optimisation tools for port security systems

- Performance indicators are an important part of performance measurement and can be used to good effect in a continuous improvement programme such as Six Sigma, ISO 9001and in particular with ISO 28000.
- Performance indicators which are directly related to the security performance of ports (that is, the ability to prevent any security related incidents, fraud, theft etc.) are proposed with the aim of producing a security rating for ports which can be used for comparative purposes by, for example, ship owners who need to decide which are the safest ports in a region to deliver cargo to/from.
- A three tiered approach to port security performance measurement (Security Performance Indicators, Key Performance Indicators and Performance Indicators) in line with the approach adopted by acknowledged experts in performance measurement techniques is proposed
- These indicators need further detailed definition and suitable mathematical relationships derived between the three different types of indicators before they can be applied to the SUPPORT model port for evaluation
- The performance indicators when agreed can be used to measure port security performance on a regular basis (year-on year for example) to ensure process improvement, set improvement targets, bench mark performance against that of similar terminals and ports, and to measure compliance against applicable standards and regulation
- The longer term aim is to provide a comprehensive list of performance indicators from which individual maritime and port stakeholders can select suitable performance indicators to suit their particular business and operational activities

3.5.2 Port Security knowledge management tools

- Performance indicators are an important part of performance measurement and can be used to good effect in a continuous improvement programme which is part of a Quality Management approach to security management.
- The Port Security Reference Framework is necessary for the cross-referencing of the different Maritime and Supply Chain Security Standards that

can potentially impact on port facility operations. The model that has been developed will require further refinement over the life of the project. It is proposed to use a series of pilot and case study deployments to achieve this.

- The Port Security Capability Maturity Model that has been defined in this document will require further refinement. It is proposed to use a series of pilot and case study deployments to achieve this.
- Security resilience indicators which are directly related to the capability maturity of ports (that is, the ability to prevent any security related incidents, fraud, theft etc.) are proposed with the aim of producing a security maturity rating for port facilities which can be used for comparative purposes by, for example, ship owners who need to decide which are the safest ports in a region to deliver cargo to/from.
- The maturity indicators need further detailed definition and suitable mathematical relationships derived before they can be applied to the SUPPORT model port for evaluation
- The security resilience indicators when agreed can be used to measure port security maturity on a regular basis (year-on year for example) to ensure process improvement, set improvement targets, bench mark performance against that of similar terminals and ports, and to measure compliance against applicable standards and regulation
- The longer term aim is to provide a comprehensive list of resilience metrics from which individual maritime and port stakeholders can select suitable measures to suit their particular business and operational activities

3.5.3 Education & Training Programme including examination services

The SUPPORT Port Security Management System (PSMS) contains a - Education, Training and Examination module. This web based module is based on best practices of ISPS related Maritime security education and offers an education / training part a manual for drills & exercises and an examination module. The education and training part enables security professionals to upgrade their knowledge and to train their personnel by using an e-learning method. PFSO's can test knowledge of Port Facility Security Personnel and Port Facility Personnel with specific security duties by a pre-loaded exam module containing multiple choice questions, thus keeping track of the knowledge level of all members of the security organization. All other personnel can be trained by the PFSO using the content of the module thus upgrading the awareness profile. The manual for drills & exercises gives guidance on how to perform these in order to assess security processes and procedures and improve if needed the security concept accordingly.

This module aims to upgrade knowledge and awareness of all personnel

The targeted benefits arising from the PSMS – education, training and examination module -

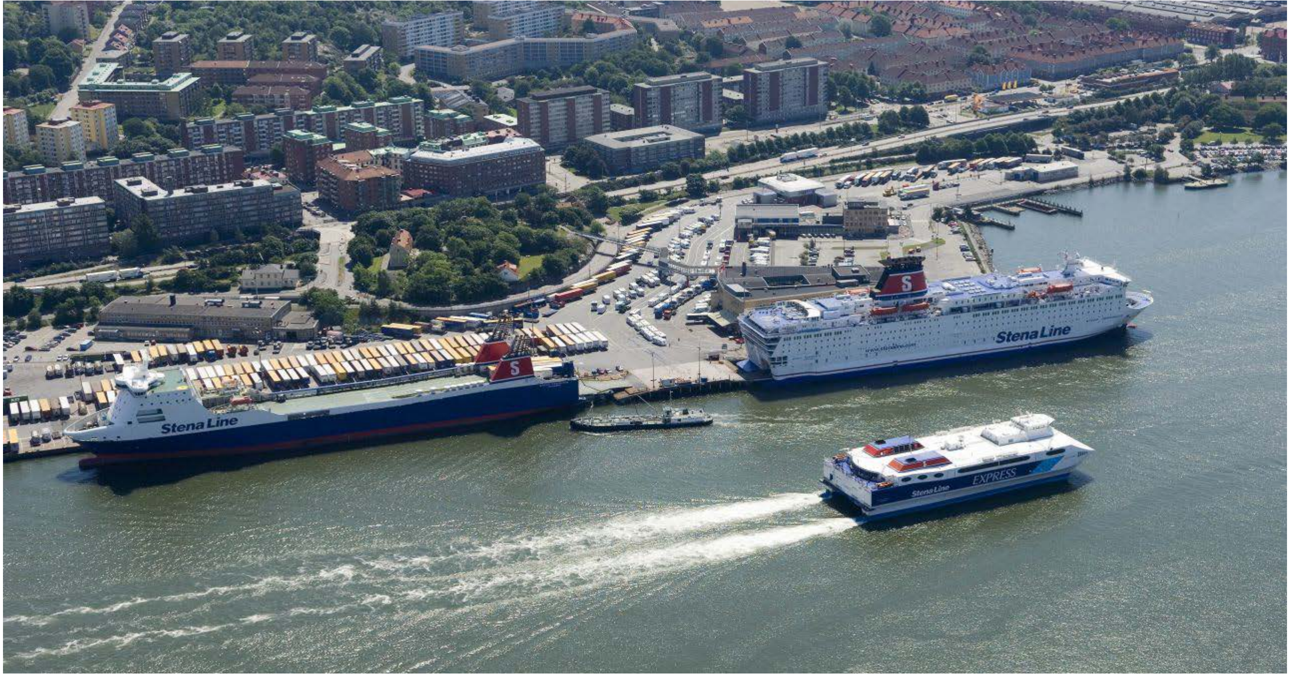
- Clarity will be brought to the complex challenge of port facility security education and training course;
- Port Facility Security Officers will be able to study the chapters of the course and upgrade their knowledge significantly;
- Investments in security education and training for security personnel can be made by a so called e learning process prioritized by the PFSO him/her self.

- Investments in security education and training of company personnel can be achieved by the PFSO using the course to abstract an awareness program.
- The education course and examine module are based on best practices and expertise of maritime experts related to security education and examination;
- The examination results by a web based examination module driven by multiple choice questions are immediately available for a PFSO to see of a candidate have failed or past a test;
- This web based program and services can be used to upgrade the maturity of a Port Security Organization and all company personnel improving clearly the knowledge / awareness level of all involved;
- Unity in the diversity of education and training concepts can be achieved.

3.6 SUPPORT demonstrators and test beds

3.6.1 Gothenburg

The SUPPORT demonstration in the port of Gothenburg in May 2014 was divided into three parts demonstrating four solutions to different aspects of port security.



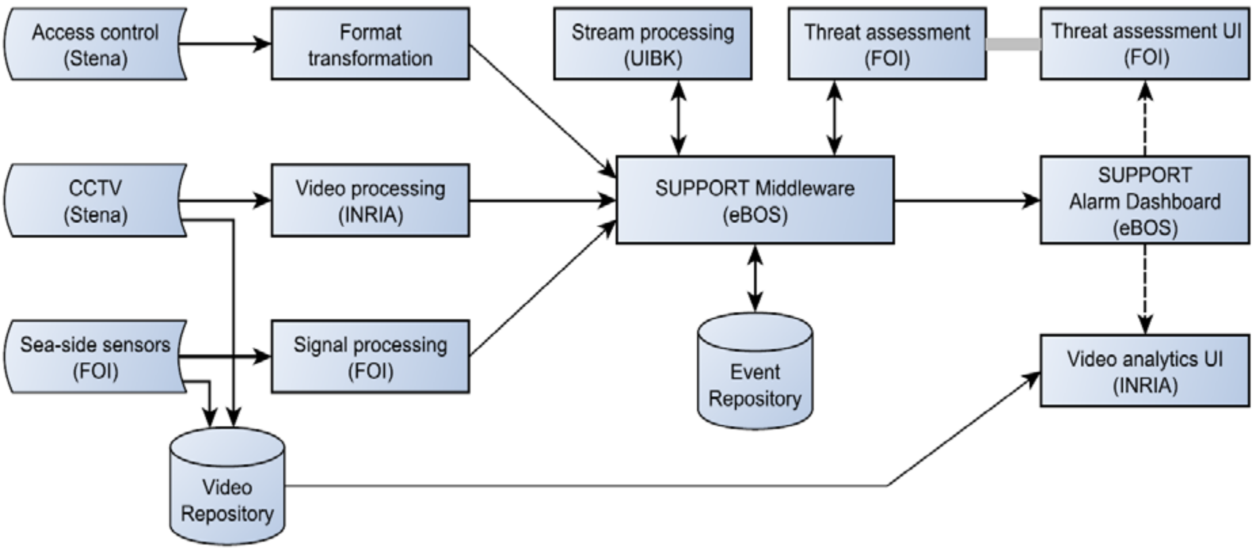


Figure – Schematic overview of the SUPPORT system demonstrated in Gothenburg.

An aspect that should be stressed is that even though this evaluation handles each demonstrated solution separately, the perspective and strength of SUPPORT is a system of systems approach. It is not the technological excellence of each solution that is in focus, but an improvement of the security system as seen from an operator's point of view.

Sea Side Intrusion Detection

This solution represents a combination of sensors working in unison to increase the surveillance on the sea side of ports, above as well as below the water surface. The Sea Side Intrusion Detection system, which was demonstrated at the Stena Germany terminal in Gothenburg, involved the following main components:

Passive detector line (hydrophones) for detection of underwater activity beside and under a ship at berth in the port. The sensor system is primarily designed to automatically detect the breathing apparatus of divers, but could also be used for detection of motor driven underwater craft and surface vessels. At the demonstration automated detection of divers in re-al time were demonstrated. In addition an underwater speaker was used to send warning messages to the divers once they had been detected.

A combination of IR, video and radar sensors for the purpose of surface activity detection. Presently it is rare for terminals to have any other area imaging or area scanning sensors than video. Video does not perform reliably if there is no artificial lighting at night-time. There is an option to use low-light-level video sensors but the cost of them approaches the IR sensors which are more reliable in terms of weather parameters. The most reliable sensor technology in harsh weather and in darkness is radar but the cost is somewhat higher than IR if swimmer detecting resolution is required. At the demonstration the ability of all three sensor types were demonstrated. However, automated detection and classification were implemented only for the IR sensor but similar methods could be used for video data. The sensors ability to detect and classify of the following targets were demonstrated, swimmers, kayaks and small boats.

The signals from these sensors were processed and transferred into the Information Fusion system described below.

Port Security Management System (PSMS)

PSMS providing maritime security practitioners, like PFSO´s and PSO´s, with a consolidated and up-to-date self-assessment instrument that also fits smaller ports with significant facilities and port facilities located in isolated areas. PSMS consists of an interactive real time dynamic web based dashboard designed to assist security professionals in developing and supervising port security in line with the ISPS code and other EU legislation. The PSMS has the potential to deliver information, skills and methodologies that enable security professionals to maintain, evaluate, upgrade and supervise security measures and create security awareness.

The whole PSMS package comprises five elements including:

1. a maturity module designed to enable security professionals to review and upgrade security plans to address terrorist threats;
2. a corporate security module which addresses crime risks such as loss events, related to corporate processes and procedures;
3. an e-learning education and examination module based on best practices of ISPS related maritime security education including drills and exercises;
4. a sharing and decision support module which enables security professionals to supervise facilities via the internet and to collaborate on a local, national or global scale and
5. an Authorised Economic Operator (AEO) security self-assessment module which provides a system to reach compliancy and submit AEO application.

The PSMS demonstration in Gothenburg was carried out by a combination of Power Point presentation and live demo. The Power Point presentation included a short introduction about the PSMS and the need for a web based system for PFSO's followed by some screenshots of the actual system and explanation including the navigation of the PSMS in order for the participants to get an idea.

After the presentation a live demo was followed, illustrating all the features of the system by allocation equally time to each module. The presenter described all steps needed to be followed by a PFSO or PSO in order to complete the self-assessment for his/her port. At the end of the live demo, a number of questions have been answered in relation to the system.

Operator Decision Support

One of the objectives in the SUPPORT project was to improve the situation awareness of the port facility security operators and help them discover security incidents more effectively. The objective was met using advanced video analytics and information fusion technology.

The demonstration part Operator Decision Support consisted of two subsection: (1) Video Content Analysis and (2) Information Fusion.

Video Content Analysis

The video analytics platform was developed by a team in INRIA, it process video streams from cameras and detect security related events or possible threats. Some events themselves are enough to trigger an alarm to the security officer and others are fused with other sensors / information to detect complex threats. The platform is designed in such a way that the user (security personnel) can easily include a new event of interest in a very simple and intuitive language. All of this processing is done and events are detected in real time, so that the security officer can respond to the threat immediately. The system is capable of fusing data from other sensors and other platform which is present in-market systems disadvantage.

During the demonstration, INRIA showed a quick look on how the processing is done which converts video frame (Low level information) to events or threats (High level information). INRIA collected some videos of interested from STENA (archive andacted videos) relating to interesting security threats that port facilities face. The system was modelled to detect such events and was tested on these videos, which were shown during the presentation such as Intrusion, ticketless travel, abandon luggage, objects thrown from outside the fence, spying activity from outside, people in restricted zones during restricted times, robbery etc. These events were then sent to pattern recognition engine to fuse with some information like security reports, door alarms, intelligence reports etc. to check for complex threats models and their risks. Finally future of video analytics, problem of present systems in the market and cost benefit analysis were discussed to wrap up the demonstration.

Information Fusion

The Information Fusion system combines information from multiple sources in order to give a decision maker a more complete and robust description of the current situation. In the SUPPORT project, data streams from a number of sensor systems (video cameras, IR-cameras, hydrophones) have been combined to generate a situation picture consisting of ranked events and alarms displayed in a list and on a map. The system reduces the number of false alarms and helps the operator to discover valuable connections between events.

In the SUPPORT project three challenges for information fusion in a port environment have been addressed. The resulting solutions were demonstrated at the Gothenburg demo.

1. Fusing information from heterogeneous sources. The port environment is increasingly being filled with new sensor and information systems. These are all potentially valuable sources for the information fusion system. However, in order to perform fusion, information from different sources needs to be comparable in a meaningful way, they need to be semantically aligned. In the support project we have demonstrated how semantic technology can be used to solve this issue.
2. Managing large data streams. Semantic technology is often considered to be computing intense. When adding more and more new sensors this could be a potential problem. In the SUPPORT project we have demonstrated how a sematic stream processor can be used to solve this.
3. Combining human knowledge and sensor data. An importance ranking of the alarms is a helpful tool for the security operator. When the threat situation is fixed over time, a simple way to accomplish this is to manually set a static importance score for each type of alarm. In the SUPPORT project we have demonstrated how to make the importance ranking dynamic, based on both human knowledge of the current situation and incoming sensor data.

3.6.2 Piraeus

Piraeus is the largest Greek port and one of the busiest ports in Europe in terms of passenger and commercial traffic. With a throughput of 1.4 million TEUs (twenty-foot equivalent units - containers), Piraeus is placed among the first 10 ports in container traffic in Europe and the top container port in the East Mediterranean.

Approximately 50% of the annual traffic is attributed to transhipment containers. Piraeus Port is structured as a complex of terminals serving the need for imports and exports of various goods.

The port services offered involve containers (Container Terminal), bulk cargo, such as metals & minerals, personal goods, car parts etc (Conventional Cargo Terminal), car imports (Car Terminal) and in general all the cargo to be distributed inland and overseas to third countries.

Given the aforementioned characteristics the port of Piraeus was ideally placed to serve the project objectives and provide a full demonstrator of the SUPPORT outputs.

The Hellenic Port security legal framework is based on the International Ship and Port Security

Code (ISPS) code (established on 2002), EU regulation 725/2004 and directive 65/2005 which refers to the upgrade of port security framework and infrastructures. All Hellenic Ports face security challenges which must consider the geographic place of the ports (geopolitics), traffic in the ports, national security policy etc.. Due to the heavy traffic in Piraeus Port (both in passenger and commercial facilities) these issues are exacerbated making security systems even more challenging.

Piraeus Port has a long history: built in ancient times, the port facility is established in a highly populated area, which during peak hours suffers from traffic congestion. All port passenger terminals, neighbouring civil buildings and port facilities may be considered as a potential target in a terrorist attack. In lower security level, there is a problem with the access control in the main passenger areas.

The problem is caused by the involvement of many authorities in access control. The same multiple authority involvement problems are found at the cargo control where customs officers take the lead. Finally, there is a problem with the equipment; more specifically with the C4I equipment that was acquired and installed for the Athens Olympic Games 2004 security. This equipment has proved difficult to maintain properly.

The list of security threats considered in various security breach scenarios include:

1. Scenario for Sea Vessel Piracy: where a sea vessel is attacked in the sea area of Piraeus port entrance.
2. Scenario for Sea Vessel attack with explosives: where a sea vessel is approached by another floating vehicle or vessel, carrying explosives.
3. Scenario for extemporary exploding devise: where an exploding devise could be place in any place among Piraeus Port facilities.
4. Scenarios for Cruising Sea Vessels: where terrorist attacks could contaminate drinking water or food.
5. Scenarios for Cruising Sea Vessels: where a cruising sea vessel is being pirated or encounters hostage situation.
6. Scenarios for Cruising Sea Vessels, carriers, tankers and others: where sea vessels are facing underwater sabotage.
7. Scenarios for next day plan: where multiple scenarios on crisis management are being created.

Piraeus Port authorities created a 7-axis security area plan in order to monitor and secure all Port facilities. For the purposes of the SUPPORT projects the focus was in the following two areas:

1. Cruise Area, Cruise terminal, Dodecanese, Crete and other main port passenger docks

   Within the cruise area, the cruise terminal and the passenger docks there are several cameras installed. In the cruise area, the monitoring and the access control is the responsibility of a Port Authority which is under the Ministry of Merchant Marine. This control includes ticket control and passenger and luggage check for cruise travellers. All luggage is checked with security equipment for metal objects and for other dangerous material. For the rest of the passenger port there is light security access control. The port authority performs a typical check of all passing vehicles and people, without the use of any kind of security identities. The use of special equipment for passenger and luggage checking is not anticipated because the ship-owners do not wish to incur the expenditure and because there is an aversion to causing the passengers inconvenience. There is no direct communication between the Port Authority and the Ministry Port Authority in terms of procedures and technological support.
2. C7 Container Terminal

   There are two parallel entrances, and one exit. The first entrance is monitored by customs officials and the second entrance is monitored by Port Authority Guards. The security monitoring in this terminal is strict. Cameras and guards are constantly monitoring key areas. All containers that are full are checked by customs officials while empty containers are checked by Piraeus Authority Officials. In some special cases where containers travelling to USA there is a special team consisting of Greek and US officials that scan these containers (through a special formed mobile scanning gate). All this special equipment is operated by customs officials. US officials have only a consulting role. The security needs in C7 Container Terminal are focused on the better perimeter security monitoring coverage with the application of more security cameras, other monitoring sensors and improved integrated decision support and communication systems.

The key security issues for the Piraeus Port considered in the SUPPORT project are as follows:

1. There is a need for better perimeter monitoring within Facilities. This need may be translated into more security cameras and better monitoring.
2. There is a need for more security patrols within Port facilities. Port areas patrolling isn considered to provide high security efficiency due to the timesaving correspondence over security breaching alerts.
3. The application of state of the art security technology, for perimeter monitoring implies high end software application over the existing systems. This software is expected to identify any potential threat that breaches the monitoring area security.
4. There is a need for a unified access control system with multiple control consoles. The creation of a backbone access control system and the installation of several control consoles are expected to de-centralize access control credentials while facilitating the control process in general. The lack of such a system creates vulnerabilities in security application and communication between all involved organizations.
5. There is a need for a unified communication system that will significantly enhance communication gaps between the involved organizations for port security. Communication gaps and failures create security weaknesses that may be used for terrorist attacks.
6. There is a need for better container scanning in terms of quickness and efficiency. Every technological solution that will be applied must take ensure that neither the current port procedures are disrupted nor cause delays. Therefore change management needs careful planning.

The demonstrator strategy for the port of Piraeus was:

1. Simulate an upgraded solution, with all the elements outlined above including access control / container screening etc, applying the ‘analysis and design optimisation of port security systems’ tools.
2. Demonstrate the full optimised solution combining simulation with real life implementation of an upgraded communications system, integration of a balanced set of sensors to the fusion engine and provide a decision support including co-operation with police and customs.

3.6.3 Specific Improvement studies

A number of case studies investigated issues not fully covered in the two main demonstrators.

CS2- National and EU level security interfaces

This case study investigated differences at national level (Spain, Italy, and France) of port security related practices by EUROPHAR -EEIG Port of Valencia - Marseille – Genoa.

The focus was on interaction practices with police and customs and on experience from interfacing with EU or National Single Windows. Of particular interest was the

comparison of a single authority in charge of all border control as Guardia Civil in Spain (responsibility for the entire Spanish border - land and sea since beginning of 2008) and traditional multi –agency authorities. Harmonisation options were identified together with associated policy recommendations. Improvement options offered by SUPPORT were identified and tested.
SUPPORT investigated the dynamics of migration control along the Spanish-African borders and compared this with the equivalent situation in Greece and UK.

CS3: Improved A2A and A2B systems for enhanced ports security in Latvia
This case study addressed:

1. The potential use of EU and National Single Windows in security management.
2. Support services for co-operation between Administrations in security risk management. The case study was co-ordinated by the Maritime Administration of Latvia (MAL) in close co-operation with Latvian ports, the Latvian Shipping Company, the customs, the police, and the coast guard.

MAL had completed the SSN National application and the case study developments included issues associated with National Single Windows.
A case study on improved information interchanges involving Latvian customs, police and transport authorities as well as neighbouring administrations specifically Estonia and Sweden
was set up.

CS4: Aqueous Threat Recognition
This study tested the deployment, running and operational effectiveness of the AUV platform developed throughout work package 3.4. This comprised of:

- an appraisal of the system installation, maintenance and recovery process;
- judgement of the system safety with respect to the port environment;
- benchmarking of area coverage, uptime and threat discrimination/classification algorithms (including a comparison with pre-simulated scenarios);
- user acceptance testing of the user interface

Studies were conducted in collaboration with the ports of Piraeus and Lisbon, where the AUVs were introduced to the harbours. Accompanying communications and IT systems were installed on the shore and attached to the port authority’s network. The practicalities of locating and running the system in an operational port were documented in consultation with the relevant port authorities and end users.

3.6.4 Evaluation Cost Benefit Analysis Recommendations

The data fusion techniques and ontologies utilized in Gothenburg, and the aqueous threat recognition platform demonstrated in Lisbon have been appraised with regard to their demonstrable improvement on the state-of-the-art, lessons learned following the demonstrators, and subsequent reassessment of economic costing and target markets. Projections for the investment required necessary to increase technology readiness level of these proofs-of-concept have been conducted.

Following identification of users and stakeholders that will be affected by the systems, we have further elaborated on the anticipated benefits and economies from adoption of mature, production level SUPPORT technologies. In particular, the ability of the SUPPORT systems to ameliorate the previously identified Port Security threats has been reevaluated and aligned with the ISPS Code (International Ship and Port Facility Security Code), highlighting security enhancements particular to these technologies.

System costs have been presented as a combination of 'at cost' fixed costs required to install the systems and set them up in the ports (including capital expenditure on physical servers, robotics and command and control, plus systems integration, initial management/operator training and associated deployment costs), and the operational costs required each year to run the system taking into account manpower, running and maintenance of the systems.

Benefits of the systems are quantified as the sum-product of the pre- versus post-installation risk-adjusted maximum economic loss arising from relevant loss events. These quantities are evaluated with respect to alternative systems with similar objectives (e.g. autonomous waterside detection is compared to periodic harbor patrols). Complementary to the economic benefits of the system arising from risk reduction, the increased security and protection of life from different threats has been analysed. It is envisaged that system extensions that enhance capability in domains outside of maritime security could provide a convincing case for their adoption; applications in logistics and environmental monitoring are outlined and an estimate is given of the market size.

4 Potential Impact

4.1 Potential Impact

SUPPORT views security as an important factor in the optimisation of the ports quality of service as well as that of the supply chains. By increasing the efficiency of security risk management, ports will realise substantial improvements in competitiveness. This will be particularly important for on the small and medium sized ports when it comes to integration of security with port processes.

A significant problem caused by the increased focus on security is that transhipments get more expensive and that it is more tempting to reduce the number of transhipments by using road transport. In Norway, as an example, the introduction of ISPS has required a raise in port fees to a level where some services have been abandoned as the minimum commercially viable freight volume is now too large to support them. This is the case for some services that specialized in "door to door" maritime shipping of consignments up to about 100 tonnes. It is also difficult to support "third level" transhipment from intercontinental carriers via advanced feeders to costal traffic, partly for the same reasons. Although efficient port operations require concentration to some degree, it is also an aim of SUPPORT to facilitate the third level of coastal shipping by increasing security while keeping associated costs under control. On top of that, improved security in intermodal chains will benefit the competitiveness of short sea shipping and will assist in the achievement co-modality objectives.

Another area where SUPPORT will impact European competitiveness is container handling. Worldwide, there are about 240 million containers. There are approximately 200 million container moves in any given year; of that 200 million, 143 million container moves occur on known shipping routes. As a major trans-shipment hub, the

EU handles over a quarter of the container moves throughout the world (approximately 58 million). Port security enhancement will generate significant demand levels for screening and tracking technologies. The financial importance of the future European port security market has been recently estimated to be roughly 250 million €. There is therefore a huge market potential for the solutions coming out of SUPPORT, to be exploited as described below in section 3.2.1.

On the other hand, the systems to be developed in SUPPORT are targeted at a global port security market, where competition is ferocious. Innovation, leadership and support at the EU (rather than national) level is therefore essential for the commercial and export impact of Europe's concepts and developed systems to balance the strong involvement of the US in this global market. Due to its innovative nature, its critical mass and its sound grounding on the end-user needs, SUPPORT is exactly the kind of initiative that has a real chance of success in this area.

Finally and perhaps equally important is the potential provided by SUPPORT to take a lead in e-Freight and e-Maritime markets which are potentially very lartge size markets and provide scope for innovation for both security product and service providers.

The quality, efficiency and reliability of security checks at ports are typical pan-European policy challenges. If equipment, procedures and policy at European ports differ from one member state to another, there will be a high risk that organized crime and terrorists will take advantage of the weaker checkpoints, jeopardizing the efforts of other member states and of the European Union as a whole.

Because of this international character of port security, the complexity of the enlarged EU, and the need to gather the best skills present in different EU countries, research in this area needs to be conducted on a wide basis.

Also, as SUPPORT promotes new operational concepts through increased integration between systems and organisations, it is clear that this cannot be achieved without international cooperation.

Furthermore, the planned RTD activities of SUPPORT are beyond the capability of individual partners and even beyond the capability of a single European country. For all these reasons it is clear that the research proposed can only be performed effectively at European level.

The SUPPORT Integrated Project will bring together 18 partners from 12 member states plus one EEIG European partner for a program of work that will cover 4 years and consume 843.5 person-months, addressing the development, validation and demonstration of an innovative framework for upgrading port security. The Consortium gathers all the operational critical mass necessary to conduct such a complex project. The size of the Consortium is kept to the necessary minimum as SUPPORT will reuse an extensive know how from related projects and incorporate existing products and prototypes, focusing effort on innovative improvement, adaptation and integration and not on the full development of completely new technologies. This approach focuses on producing real tangible results creating added value to the whole European port security community.

In SUPPORT, research is not an end in itself; instead it will be the basis for an ambitious and extensive Demonstration and Training Programme which will bring the results to a wide audience, train key managers and staff in the use of the new systems and collect feedback for further improvements.

In summary:

- The technical approach proposed is multi-disciplinary, associating partners who will cover all the necessary technical domains (see section 2.3 “Consortium as a whole” for more details).
- Technical and European interoperability require common work between the different types of partners.
- An efficient set of checkpoints cannot be ensured by a national surveillance infrastructure unable to communicate and be interoperable. Working together is the best and cheapest way to create common confidence. If such a project was developed at a national level there would be a high risk the technologies would be rejected by some member states leading to incompatible equipment and procedures.

As mentioned above, SUPPORT has its roots in previous European research. The extent to which SUPPORT will continue and build upon previous projects has been covered elsewhere in the proposal. For instance, section 1.2.5.2 explained the relationship with MarCOM whereas section 1.2.5.3 covered SENTRE, STACCATO, CRESCENDO and SMART Container Chain Management. Section 1.2.6.1 referred the connection with POMPEI and section 1.2.6.2 mentioned CoFRIEND, PROMETHEUS, SCOVIS, EARISE, SAMURAI and CARETAKER. Other relevant European projects are also mentioned in sections A1, A2.2.3 and A2.3.1 of the Appendix.

In conclusion, SUPPORT is an EU scale project answering to a key European policy challenge, allowing better integration of European R&D, and facilitating transfer of skills and knowledge across member states.

MRT is actively participating through ISO TC8 in development of the ISO 28000 series standards on supply chain security. MRT is currently in charge of development of the ISO 28005 Electronic Port clearance standard. Results from SUPPORT that are suitable for ISO standardization can be tabled by MRT and developed into standards through the appropriate ISO procedures. This may be particularly interesting for best practice type standards that give baseline requirements for "necessary and sufficient" security measures.

Through ISO, MRT is also participating in IMO FAL (Facilitation Committee) work and has, thus, the possibility to influence new IMO standards or promote other SUPPORT results to IMO. This may be relevant, although IMO today usually focus on relatively high level standards that are less prescriptive than technical standards from, e.g., ISO and IEC. It may also be possible to take results from SUPPORT into the UN/ECE (responsible for electronic trade documents, e.g., UN/EDIFACT) or WCO systems. These organizations have liaisons to ISO TC8 through which results can be promoted. These organizations are probably most relevant for ICT type standards, particularly on information exchanges between authorities and ports and between ports and ships. SUPPORT will give consideration to what channel is most appropriate for the different results that the project achieves.

The main target is to provide standard solutions that are cost-effective and which gives a sufficient level of security.

CEN may be channel for standardization, but as ports are part of international supply chains, the corresponding international organizations (e.g., ISO) are more appropriate.

SUPPORT will also liaise with other European and international interest organisations, including ESPO and EHMC to ensure that SUPPORT solutions are consistent with existing and emerging security standards while also being in line with the ports economical and organizational interests. It is also of particular interest to keep in touch with US interests as they tend to define state of the art standards in this area. The US interests are well represented within ISO TC8. Of particular interest here is the interplay between supply chain security measures (e.g., the USA C-TPAT and CSI initiatives and the WCO SAFE Framework) and ship and port facility security measures (e.g., through the International Ship and Port Facility Security - ISPS).
In cooperation with the ports, SUPPORT will identify port security implications for the EU e-Freight and e-Maritime policies and will submit policy recommendations. Again, the purpose is to promote good solutions to port security issues that do not create unnecessary obstacles to international trade and effective port operation.

4.1.1 Dissemination Activities

Dissemination were aimed at three main groups: port security operators, transports users and administrations (including coast guard, police and customs). Our approach assisted us to communicate in a consistent manner with a wide range of audiences across Europe.
There was a plan to deliver sustained dissemination to raise awareness of the advantages of SUPPORT aligned to the exploitation plan. The project partners were extensively involved to stimulate the heightened awareness of practical benefits.

The long term promotional plan for SUPPORT was through establishing in the second year of the project the *EU Ports Security Forum* initially with members from the Partners Forum and Advisory Committee and utilising the proposed *annual SUPPORT conference*.

The main Dissemination Objectives were to:

1. Create a suite of dissemination materials that explain the principles of SUPPORT and the tangible and quantifiable benefits that it can deliver.
2. Establish an efficient process for preparing dissemination instruments (articles, scientific papers / reports, demonstrators, etc) as part of the development work programme to ensure that a coherent communications programme can be sourced efficiently.
3. Provide a series of publications to establish the technological and scientific credibility of project outputs and to promote standardisation activities.
4. Maintain an interactive web site continuously updated with fresh material and links to demonstrators.
5. Devise and implement a dissemination programme, focused on the key audiences and regions that stand to gain the most from adoption of SUPPORT.
6. Create mechanisms to effectively handle enquiries from stakeholders, the media, and other interest groups.
7. Develop robust reporting and measurement techniques to evaluate the effectiveness of the dissemination activities.

Initial actions included

1. Preparing a comprehensive communications plan and schedule of activities to complement the exploitation plan.
2. Undertaking a detailed media audit by:
   - analysing SUPPORT related articles
   - interviewing carefully selected journalists to gain insights regarding proposed SUPPORT developments.
3. Devising key messages that underpinned all dissemination communications.
4. Creating a Digital library for port security, containing reference material that was used and updated throughout the four year programme. These documents included:
   - background briefing notes, that put SUPPORT and related security issues into context;
   - Questions & Answers that deal with commonly discussed issues and correct important misconceptions;
   - Project related publications and reports on the SUPPORT ICT Platform and Generic Models;
   - Project business cases and other evidence that outlines best practices
5. Distributing materials to promotional agencies
6. Establishing effective reporting procedures

We had a program of Press Releases and Media articles which included:

1. Devising schedule of Press Releases to mark the launch of the dissemination programme and project milestones.
2. Issuing press releases through selected agencies across the EU and internationally.
3. Publicising SUPPORT events such as the SUPPORT Annual Conferences (through drafting and issuing press material, arranging interviews with key spokespeople etc).
4. Handling enquiries from the media and other interested groups.
5. Ensuring all relevant websites utilise Press Releases materials.
6. Preparing a detailed evaluation report of all communications activities associated with each press release.

Target media groups, for the press releases, will included: Security, Ports, Transport operators, Governmental – EU, national and regional, Newswires, Economic, and Environmental.

The SUPPORT dissemination program consisted of

1. Organisation of the dissemination launch with press release and a fully operational web site.
2. Launch the EU Ports Security Forum with a special event during the first SUPPORT Annual Conference
3. Publication of a project brochure a with the project logo, for use at internal and external workshops and conferences

4. Organising the three SUPPORT Annual Conferences.
5. Initiating an electronic newsletter on SUPPORT to promote the broad engagement of target stakeholder in the SUPPORT Forum

Conferences where SUPPORT partners attended:

- Maritime Security International Exhibition (MSI)
- Annual Maritime Security Expo
- Port Security Conference
- Maritime & Port Security Conference & Expo
- Transport Security Conference

Results were published in a number of relevant journals, amongst were:

- Security Journal
- Security Management
- The Journal of Homeland Security
- The Journal of Security Sector Management (JofSSM)
- Journal of Homeland Security and Emergency Management
- The Journal of International Security Affairs
- International Security

A film of 5 minutes and two 30 second teasers were produced. They showed that the result of EU investment in R&D is workable, useful, well thought out technology, which has application and merit in the real world. The target audience included, but are not limited to:

- The general public
- Security
- Ports
- Maritime and technology communities

The video highlighted three main sub-projects:

1. Work Package 5 – Port Security Management

2. Work Package 3.4 – AUV for diver detection in ports. There were potentially 3 uses for this AUV:
   - To provide 24hr surveillance
   - To use it to monitor port infrastructure and look out for particular threats such as mines and explosive devices
   - Use it as an on-demand confirmation and response unit which complements existing cheaper and less reliable sensors that ports are utilising

3. Work Package 3.1 – Seaside Intrusion Detection (SSID), an analysis of all the different sensors available in the port

Regarding the media campaign, there were three key work packages which deserved particular focus and three further work package outcomes which required some recognition. The priority work packages included: WP5 PSMS (Port Security Management System), WP3.4 AUV (Autonomous Unmanned Vehicle) and WP 3.1 SSID (Sea Side Intruder Detection). The target audiences for the campaign were complex and included the general public, security,
ports, maritime and technology communities, as well as the EU.

The Key Communications Objectives were:

- To demonstrate that EU investment in R&D results in workable, useful, well thought out technology with application and merit in the real world.
- To make the case for future important, follow-on R&D investment

The priority work packages had multiple activities wrapped around them, promoting their individual key milestones and events and included: news releases, media briefings, and feature articles, as well as social media interaction. The non-priority work packages were supported primarily via news generation and news management.

4.1.2 Exploitation

The partnership of SUPPORT is strong in industrial and commercial partners of all types for whom exploitation was the sole reason for participating in the project. Many of these partners have a long and successful history in commercial exploitation of research. As a result they have developed a structured approach to exploitation planning which the consortium have assessed and approved.
The Exploitation Plan constituted a live document which started to be produced at the beginning of the project and will persist after the research project ends.

The Exploitation Plan covered the following topics:

1. **Objectives**. Detailed definition of the aims of the Exploitation Plan including (a) the mapping out of the way the Consortium and the security industry in general can derive commercial benefits during and after the project from the work conducted under SUPPORT and (b) the definition of the way the technical work should be conducted in order to maximise commercial benefits.

2. **Strategy**. Though the tools validated and refined in SUPPORT have potential application for a number of different port security market segments, their penetration in these markets will depend on how near to their specific problem and/or present procedures the potential customers perceive the SUPPORT solutions to be. The Exploitation Plan described these market segments (size, changes required to address their problems, cost of accessing the segments, main actors etc). The Exploitation Plan also covered market research. All these points were brought together in a detailed Market Analysis which utilises the market survey to determine decision influence factors for the adoption of SUPPORT per different stakeholder groups in representative regions of Europe.

3. **Mechanisms**. Once the Market Analysis was completed, the mechanisms for implementing the Strategy (marketing actions, demonstrations to main actors etc.) were defined.
4. **Plans of Action**. After markets were defined in detail (i.e. once potential customers were identified) and mechanisms were chosen and contacts established, we were in a good position to assess the costs and benefits of the exploitation.
5. **Impact**. Customer contacts, the results of market research and the definition of Plans of Action lead to suggested modifications in the research direction of the project to maximise its commercial impact. At pre-defined points during the project, the implications of the developing Exploitation Plan on research were considered by the Project Board.
6. **Scope of Commercial Agreement**. Though a Consortium Agreement existed, the detailed definition of the commercial implications of development may change. Then the Consortium Agreement will be revisited and expanded to include a more detailed Commercial Agreement.
7. **Future Actions**. The project delivered concrete and exploitable / implementable results and products. Exploitation is continuing after this period. Future exploitation actions were clear and well defined before the research project ended. In particular, the exploitation of the Port Security Management tool is being conducted vigorously (see www.mypsms.com) and has already led to significant sales.

5 Public Website and Contact Details

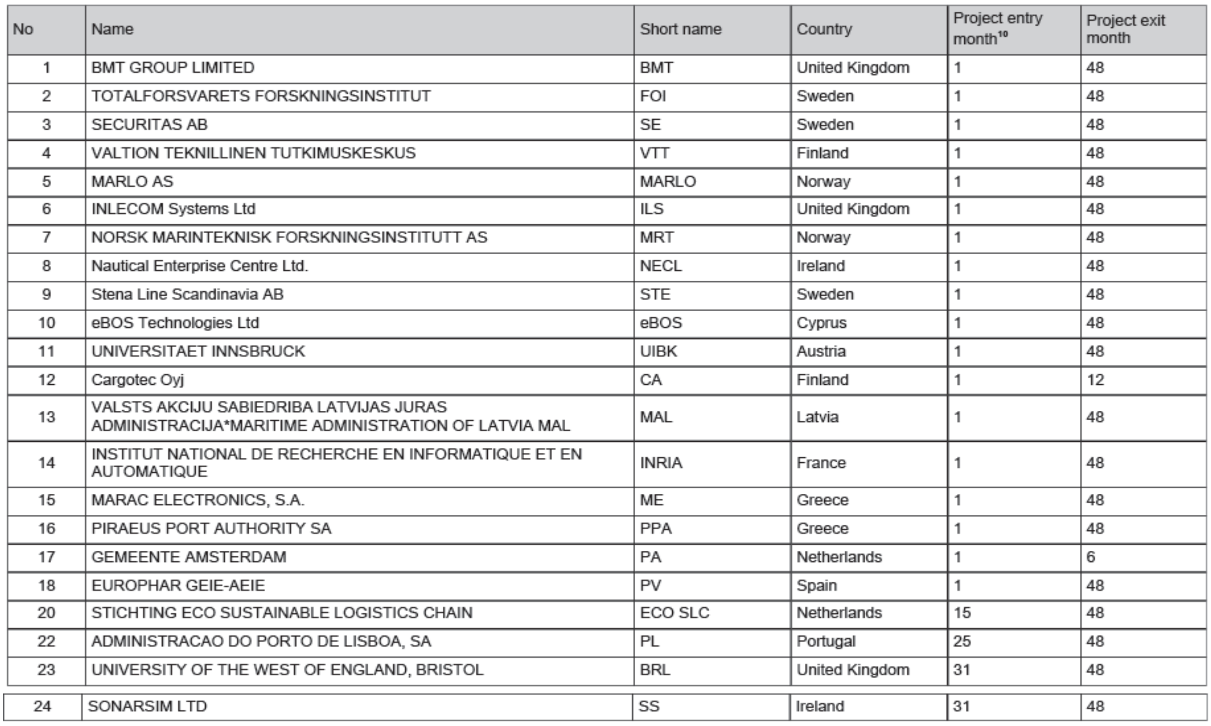
http://www.support-project.eu/

The project coordinator is BMT Group Ltd contact details below.
BMT Group
Goodrich house,
1 Waldegrave road,
Teddington Middlesex,
TW11 8LZ,
United Kingdom
Project Manager: Dr Fernando Caldeira-Saraiva
web: www.bmtgroup.com
email: supportproject@bmtproject.net

6 Project Logo

7 Image

8 List of beneficiaries



No	Name	Short name	Country	Project entry month[10]	Project exit month
1	BMT GROUP LIMITED	BMT	United Kingdom	1	48
2	TOTALFORSVARETS FORSKNINGSINSTITUT	FOI	Sweden	1	48
3	SECURITAS AB	SE	Sweden	1	48
4	VALTION TEKNILLINEN TUTKIMUSKESKUS	VTT	Finland	1	48
5	MARLO AS	MARLO	Norway	1	48
6	INLECOM Systems Ltd	ILS	United Kingdom	1	48
7	NORSK MARINTEKNISK FORSKNINGSINSTITUTT AS	MRT	Norway	1	48
8	Nautical Enterprise Centre Ltd.	NECL	Ireland	1	48
9	Stena Line Scandinavia AB	STE	Sweden	1	48
10	eBOS Technologies Ltd	eBOS	Cyprus	1	48
11	UNIVERSITAET INNSBRUCK	UIBK	Austria	1	48
12	Cargotec Oyj	CA	Finland	1	12
13	VALSTS AKCIJU SABIEDRIBA LATVIJAS JURAS ADMINISTRACIJA*MARITIME ADMINISTRATION OF LATVIA MAL	MAL	Latvia	1	48
14	INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE	INRIA	France	1	48
15	MARAC ELECTRONICS, S.A.	ME	Greece	1	48
16	PIRAEUS PORT AUTHORITY SA	PPA	Greece	1	48
17	GEMEENTE AMSTERDAM	PA	Netherlands	1	6
18	EUROPHAR GEIE-AEIE	PV	Spain	1	48
20	STICHTING ECO SUSTAINABLE LOGISTICS CHAIN	ECO SLC	Netherlands	15	48
22	ADMINISTRACAO DO PORTO DE LISBOA, SA	PL	Portugal	25	48
23	UNIVERSITY OF THE WEST OF ENGLAND, BRISTOL	BRL	United Kingdom	31	48
24	SONARSIM LTD	SS	Ireland	31	48