SUPPORT

A NEW APPROACH TO PORT SECURITY

Port security is of paramount importance for Europe - about 90 per cent of the EU's external trade and 40 per cent of its internal trade is transported by sea; 3.5 billion tonnes of freight is loaded and unloaded in EU ports every year[1]. Port security breaches pose direct threats to life and property. They also have the potential to cause serious economic damage to operators and users directly, as well as throughout the supply chain.

The **EU SUPPORT** project aims to help port stakeholders establish the security levels sufficient to meet evolving international regulations and standards, and which work in the complexity of the real port environment.

SUPPORT will provide methodology, technology and training for any European Port to upgrade their security capability focusing on:

- Secure and efficient Port operations in the context of sustainable transport
- Uninterrupted flows of cargo and passengers
- The suppression of:
  - terror and attacks on high value units
  - illegal immigration
  - trafficking of drugs, weapons and illicit substances
  - large scale or continuous theft and economic black mail

1: Maritime transport policy, Improving the competitiveness, safety and security of European shipping, October 2006.

For more information on the SUPPORT project, downloadable material and news items, please visit the project website www. support-project.eu or contact:

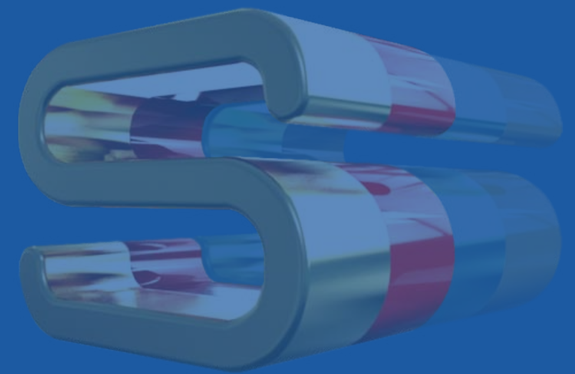
BMT Group Ltd
Goodrich House
1 Waldegrave Road
Teddington Middlesex
TW11 8LZ
United Kingdom

Project Manager: Jenny Gyngell
email: supportproject@bmtproject.net

SUPPORT receives funding from the European Commission, Security Research under the Seventh Framework Programme for Research and Technological Development.

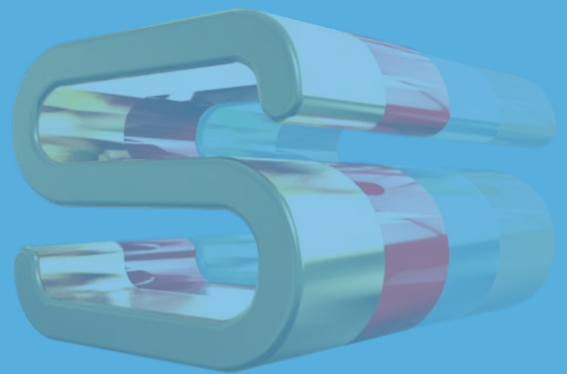
Our partners

- BMT Group Ltd
- Swedish Defence Research Agency, FOI
- Securitas AB
- VTT Technical Research Centre of Finland
- MARLO AS
- INLECOM Systems L:td
- MARINTEK
- Nautical Enterprise Centre Ltd
- Stena Line Scandinavia AB
- eBOS Technologies Ltd
- University of Innsbruck
- Cargotec Oyj
- Maritime Administration of Latvia
- INRIA
- Marac Electronics SA
- Piraeus Port Authority SA
- EUROPHAR - EEIG Port of Valencia
- ECO SLC



SUPPORT

A NEW APPROACH TO PORT SECURITY



The Port Security Challenge

Ports represent significant challenges when implementing new security measures. They cover large geographical areas, they are complex, they service large passenger numbers and process large volumes of goods. Enabling competitive operational efficiency while improving security is vital to any port. Besides efficient surveillance and access control, this requires organisational and technological interfaces connecting ports to border control authorities, police, other intervention forces as well as transport and logistics operators.

Ports have supply chain security measures (e.g., the USA CTPAT and CSI initiatives and the WCO SAFE Framework of Standards based on AEO programmes[2]) alongside ship and port facility security e.g., through the International Ship and Port Facility Security (ISPS) Code). The challenge for ports is to combine these into an integrated security approach.

Research has also shown that the complexity and cost of port operations for intra-European freight is a major obstacle to shifting more freight from roads to sea. The introduction of new security measures can easily make this worse and so it is important to not only improve security, but also to reduce complexity and cost.

2: CTPAT Customs-Trade Partnership Against Terrorism, CSI – Container Security Initiative, World Customs Organisation SAFE Framework of Standards to secure and facilitate global trade

The SUPPORT Solution: A Systems approach

Stakeholders with tasks and responsibilities in ports and the supply chain need to adopt a 'systems' approach rather than ad hoc problem solving. This is necessary for efficient implementation of 'first port of call' measures or the 'Authorised Economic Operator' certification. These require transparency from ports about the impact of their behaviour on all stakeholders in the logistic chain as port security must be considered in the broader context of secure EU and international supply chains.

The Need

Although major players, mainly container operators already have state of the art solutions, there is still a need to:

- Upgrade risk and vulnerability assessments
- Improve access control
- Set standards for fencing, intrusion alarm and CCTV systems
- Secure cargo through scanning and screening technology
- Improve monitoring and surveillance
- Integrate security management information into overall supply chain information flows and decision support systems
- Set up of guidelines for screening of personnel, improving background checks and profiling functions
- Improve security training, awareness programmes and management training.
- Promotion of higher resilience concepts (low impact of disruption, rapid recovery to normal operations)

The Solution

SUPPORT will provide practical guides to achieve all the above by delivering:

- A fully documented Risk Model, highlighting the relationship between threats, loss, consequences and risk control options
- A Port Security process Framework from which information exchanges between stakeholders can be derived and standardised
- An advanced Financial Model allowing ports to conduct Cost-Benefit Analyses against individual Risk Control options and investigation of potential security and economic gains
- An ICT platform to provide the necessary information infrastructure for all stakeholders which will facilitate improvements in security and information exchange as well as promoting better interrelationships between them
- Pilot projects demonstrating how port security can be upgraded

SUPPORT will be a broad forum for port stakeholders and security experts to come together and form new standards for port security.

Introducing the SUPPORT Risk Model

The SUPPORT Risk Model identifies:

- Loss Events, including:
  - Threats causing Loss Events,
  - Consequences
  - Preventive Controls
  - Reactive Controls
- Gaps where Controls don't match the Threat Probabilities and Loss Event Consequences
- Links between common threats, follow-on Loss Events and common Controls
- Quantification of Consequences
- The effectiveness of control measures, the consequence costs, etc by supporting simulation testing

And the SUPPORT ICT Platform

An effective security network needs to acquire data, manage it, interrogate it and share it efficiently among a wide variety of stakeholders at different geographic locations. The SUPPORT ICT platform will help the security stakeholders in different ports establish their own data exchange systems and communications with other ports or national and EU applications. Essentially it will help stakeholders establish interoperable applications consistent with the Port Security Framework.

The Pilots: Showing how SUPPORT will upgrade security

To show how SUPPORT outputs work, we will run two pilots in Gothenburg and Piraeus to show how the developed solutions can work effectively in a real life environment.

A cluster of stakeholders will use their own version of the ICT platform to show how information can be exchanged between platforms, how it communicates with disparate technologies and fuse information from stakeholders with data from various sources. This will support preparation and support for risk assessments. These will also produce a Risk Model plus a set of standardised processes and procedures to demonstrate how changes in processes and procedures can help increase port security for very little (if any investment).

Port security specialists will create a number of Key Performance Indicators (KPIs) to set targets for the ICT solution and security processes developed so the pilots can collate data to check whether these are being met. This will include collecting active and passive as well as qualitative and quantitative data. The ICT platform will collect systems-level data autonomously, whilst users of the ICT platform and operators in new operating processes will be interviewed to supplement the quantitative data.

Port environment permitting, we will collect data both in a 'normal' operating use scenario, and in an 'attack' scenario where one or more threats will simulate attacks on the port. This will ensure that results of the SUPPORT project are validated by real users in a real environment.