Periodic Report Summary 4 - SUPPORT (Security UPgrade for PORTs)

Project Context and Objectives:
SUPPORT aims to raise the current level of port security by integrating legacy port systems with new surveillance and information management systems. SUPPORT will provide the necessary and sufficient security level to satisfy evolving international regulations and standards while efficiently supporting the complexity of the real port environment. As part of this, SUPPORT will also facilitate efficient and, where required, real-time exchange of security related information within the supply chain and between ports and authorities.

SUPPORT partners include a number of ports that have been selected to represent typical, but different operations. Starting from the perspective of the partner port operations, the project will use a cost-benefit method to identify the main security gaps and will describe security measures to maintain or augment the efficient and secure operation of these ports. The approach will combine creative and analytical techniques to identify as many relevant threats as possible. After making an inventory of security gaps these will be developed into generic port security models. The models will be used to suggest security upgrade solutions, taking into account the cost-benefit factors of the available technology.

Peer-to-peer communication and decision support tools incorporating semantic technologies will be developed, using as far as possible standard open architecture software, accessible to all the port security stakeholders. The results will be demonstrated at the ports of Gothenburg and Piraeus. SUPPORT will include policy and standardisation proposals and training for participating port personnel as well as dissemination activities for other ports and stakeholders. One aim of SUPPORT is to provide general methods and technology supported by training services that can be used by any European port to efficiently enhance its security level.

The SUPPORT project main objectives are to deliver
• 'validated' generic port security management models (capturing reusable state-of-the-art and best practices) that can be customised for specific ports;
• training and open standards based tools to aid security upgrade in EU ports.

Project Results:
All tasks in all of the work packages detailed in the description of work have been completed.
Work on WP1 has
1. Produced a set of major security gaps in large, small and medium sized EU ports to be addressed by the project.
2. Analysed the requirements of each stakeholder group in the context of security gaps and threat scenario analysis taking into account market analysis and regulatory obligations.
3. Undertaken assessment of key technologies to ascertain their potential impact on the stakeholder requirements and provided development trends.
4. Produced requirements specification for the core development work (WPs 2-5) with particular attention to human factors and ethical issues; specify criteria for measuring project success in terms of outputs, key performance indicators for EU ports security and impact.
Work on WP2 has
1. Provided classification of port security threats and related information sources.
2. Established a library of 'vetted' port security management models covering the whole security risk management cycle and security performance management.
3. Provided guidelines for co-operation strategies between port security stakeholders and for establishing security information exchange agreements.
4. Specified compliance management processes for security directives covering administration to administration and administration to business perspectives.
5. Developed formal specifications for key information exchange interfaces for port security stakeholders and surveillance technologies.
Work on WP3 has
1. Set up useable guidelines for principal stakeholders in port security to achieve a well balanced sensor suite with potential for future development; provide facilities for refining relevant sensor data into applicable higher level information to feed into event correlation and diagnostic modules in the decision support system.
2. Provided guidelines on the security communication infrastructure required to serve multiple applications such as

Research and Innovation

general voice and data communications with improved network quality of service and bearer independence.
3. ProvideD security management of container handling optimised with respect to different handling stages at the ports; provide enhanced solutions for efficient and reliable container scanning and screening that will minimise false positives.
4. Provided solutions for detecting underwater threats
Work on WP4 has
1. 1.Sspecified platform architecture to support the project requirements (T1.3) and provide a Base Platform including communications modules, service and workflow engine and security data management components.
2. Provided data fusion tools and an operational system able to recognise abnormal behaviours addressing specifically difficulties associated with detection of rare events to support the Decision Support Services utilising semantic technologies.
3. Provided Semantic Tools for Interoperability and Services Management to enable resolution of interoperability conflicts (on security related data, events, and services) and to provide design time mechanisms to support automated integration of services (within a port specific network of security peers) by semantics based discovery.
4. Developed port security operational decision support services.
WP5 has developed the following tools
1. Tools for analysis and design optimisation of security management systems to enable a port to effectively classify and model the current port security processes and to visualise the improvements that can be gained when their current port security processes are optimised. This allows the port to identify the changes that are needed to be made to implement the SUPPORT solutions.
2. Port security knowledge management facilities including a digital library and associated information observatory and competence management tools to help ports identify security knowledge gaps and training needs particularly for aligning the workforce in light of the changes.
3. A Training Programme including training simulators for port security operators and other relevant actors which was be integrated with the knowledge management tools and is made made available through EcoPorts in association with security National and European agencies and associations
WP6 has
1. Provided a Demonstrators Plan and associated evaluation criteria and assessment methodology.
2. Organised the Gothenburg Demonstrator.
3. Organised Piraeus Demonstrator.
4. Organised Specific Improvement Case studies.
5. Provided Evaluation-Cost Benefit Analysis

Potential Impact:
Key project measurable outputs and milestones are listed in the following table.
EU ports security gaps - Initial survey of port security threat. Library of value risks and vulnerabilities
Stakeholder survey - Review of security statistics. Market survey on influence factors for the adoption of security improvements per stakeholder group. Requirements specification for key improvements
Security technology assessment - Survey of surveillance technologies. Review of interoperability standards and technologies. Review of RFIDs and projected use scenarios in port security solutions
Port Security Models - Help ports define clearly what to protect and why, what to protect it against, how to protect it and with whom.
Security Upgrade Solutions - Guideline for selection and networking of port security sensors. Solutions for extracting and refining relevant sensor. Guideline for upgrading security communications infrastructure. Solutions for communication gateways. Optimisation of the scanning and screening process of containers.
SUPPORT ICT Platform - Data fusion tools. Complex security events processing. Semantic Port Security Services. Port security operational decision support services
Port Security Upgrading Management & Training - EU Ports Security Information Observatory. Analysis and design optimisation of port security systems. Port Security Knowledge Management. Training Programme including Training Simulators
SUPPORT demonstrators and test beds - Full scale demonstrators of SUPPORT based solutions in at least two representative European ports and test beds on specific improvements
Library of dissemination content - Series of articles and scientific papers / reports explaining fully the SUPPORT Solutions available from the project web site.
SUPPORT Standards proposals & Policy Recommendations - Policy recommendations for harmonisation and simplification of security regulations

List of Websites:
http://www.support-project.eu/

Contact

Caldeira-Saraiva, Fernando (Research Director)
Tel.: +442086144244
Fax: +442089779304
E-mail

Subjects

Security

Information source: SESAM

Last updated on 2015-03-18
Retrieved on 2016-07-07

Permalink: http://cordis.europa.eu/result/rcn/158157_en.html
© European Union, 2016

Security

*Research
and Innovation*