

LOGSEC (GA-241676) Final publishable summary report

Summary description of project context and objectives:

Global supply chains and logistics systems are threatened. Theft, trade and customs law violations, counterfeit products, organized immigration crime, sabotage, cybercrime, sea piracy, terrorism and other illicit acts generate direct losses, logistics delays, damage to reputation, and other costs for the private sector, particularly for cargo owners and logistics companies, as well as for the society as a whole. The 2001 terrorist attacks in the USA (“9/11”) triggered an avalanche of governmental programs and regulations worldwide, including in the EU, to mitigate the risks from terrorism such as those from large scale destruction in the supply chain system itself and/or upon specific targets and locations, adding to the “traditional security cost burden” for the business and the society.

LOGSEC was a 12-month project which developed a strategic Roadmap for future Supply chain security (SCS) in Europe, taking into consideration the various strategic, operational, financial, legal and other expectations and constraints existing in real word supply chains. The LOGSEC-team had a balanced representation from the private sector (ESC, CLECAT) and public sector end-users (SC), from research and technologies (ICE, ATOS, POL, CBRA), and from management consulting (EFPC). The user requirement data was collected from a number of private sector organizations representing manufacturing, logistics and trade/retail sectors; as well as from a number of governmental bodies, including EU-level, national and global ones.

From project administration perspective, LOGSEC work was split into five Work packages: WP1 Project management; WP2 Dissemination and liaison with other initiatives; WP3 State-of-the-art review; WP4 User requirements collection; and WP5 Roadmap production. From the Roadmap content production perspective, the work was done in following four stages:

1. Setting up the LOGSEC Approach, with the overall framework, detailed scope and study objectives;
2. Identifying and prioritizing issues, weaknesses and gaps in Supply chain security today;
3. Developing and assessing relevant Clusters for the LOGSEC Roadmap, addressing the gaps; and
4. Converting the SCS Clusters into tangible recommendations, suitable for future Demonstration project(s).

Description of the work and Final Results:

As the main outcome for the project, LOGSEC recommends the implementation of multiple SCS sub-projects under the following three SCS Clusters:

Cluster A comprised sub-projects relating to security awareness and risk management, increasing knowledge of crime trends, awareness of security measures, SCS compliance management and the economics of SCS , builds a culture and approach that more proactively and successfully responds to security risks and threats.

Cluster B focuses on areas relating to the Authentication and certification of people, companies, documents and data in the supply chain. With improved assurances that the people and information in the supply chain are trustworthy, deception may be filtered out, uncovered and fraudsters deterred.

Cluster C centres around sub-projects aimed at protecting cargo, vehicles and drivers during transportation, logistics handovers as well as during breaks / stops / parking: in essence, it is a cluster of sub-projects focused on the Physical transportation security and on cargo monitoring.

The context for LOGSEC SCS Roadmap project is defined first by following supply chain related parameters and characteristics:

LOGSEC (GA-241676) Final publishable summary report

- End-to-end supply chains, covering sourcing, manufacturing, transport, distribution, trade and retail as well as reverse logistics.
- International (crossing customs borders), EU-level and national supply chain activities and transactions are included.
- Regarding manufacturing sectors and commodity types, a broad variety were covered, including "security-sensitive" sectors: food and pharmaceuticals (high consumer safety requirements); chemicals (as dangerous goods); alcoholic beverages and cigarettes (high tax / excise products); consumer electronics (as high value, easy-to-sell-on-black-markets – products).
- Manufacturing sectors also included "low security risk" products, e.g. low cost clothing, and lightning products.
- Regarding logistics services, all types were covered, including freight forwarding, warehousing, customs brokerage etc.
- Regarding modes of transport, most attention was paid to road transport, following the inputs from the study participants. Air and maritime were also included in the study, but to a lesser extent.

Secondly, the crime types and security responses considered cover the "maximum breadth":

- Initially, 25 crime types were identified by LOGSEC team, finally focusing on 12 most relevant ones (priorities coming from the study participants).
- The supply chain security management model for LOGSEC consists of eight layers, which are all addressed (at least to some extent) by the LOGSEC Roadmap

The culmination of the LOGSEC-project is the established recommendations for future large scale demonstration projects, formulated in a way that created a possibility for considerable flexibility in the number and scale of projects that could be undertaken in order to address specific supply chain security gaps identified by this project; and the analysis and assessments done helping to prioritise the issues that projects could address.

The three LOGSEC SCS Clusters (A, B and C) are listed, and "opened up" into six sub-projects each, in order to propose tangible, manageable items for Demonstration purposes. A number of deliverables were put forward that demonstrates very real tangible outputs from the proposed sub-projects; but these are merely intuitive; they would require more research and consideration during the project planning stage.

Cluster A - Security Awareness and Risk Management – consists of following six sub-projects:

- Risk management processes and tools;
- Knowledge on past incidents and modes of operation;
- Security economic models, metrics and KPI's;
- Security training and awareness building;
- Security compliance management and audit tools; and
- Intelligence on evolving threats.

Each of the sub projects above could deliver tools , identify and test technologies and create the foundations for networking among supply chain parties and public (governmental) agencies and organisations, all of which would, if successful, increase knowledge and awareness of crimes – current and emerging, costs of crime and the measures to implement them and fight crime.

Cluster B - Authentication, Certification and Data Protection - consists of the following six subprojects:

LOGSEC (GA-241676) Final publishable summary report

- Authentication of companies;
- Integrity of personnel;
- Authentication of documents;
- Protection of supply chain IT systems;
- Authentication of boxes, containers and seals; and
- Authentication of raw-materials and products.

The projects listed above might result in best practices, tools and processes which helped in the validation and authentication of people, documents (electronic or paper) and companies – all areas which the project found represented significant gaps in current supply chain security.

Cluster C - Physical Transportation Security and Cargo Monitoring - consists of the following six subprojects:

- Protection of drivers;
- Protection of vehicles;
- Protection of cargo, loads, containers;
- Inspection, scanning and screening of cargo;
- Ensuring integrity during logistics handovers; and
- Protection during stops/parking.

The sub-projects from Cluster C might deliver guides and means of validating the effectiveness and appropriateness of different equipment used to protect against, seal, secure, prevent, detect and deter crime.

Management tools, metrics and models to support the Demonstration project(s) include the following:

- Stakeholder participation;
- Integration requirements;
- Context dependencies;
- LOGSEC logistics flow map;
- 8-layer SCS management model;
- Demonstration metrics and KPIs;
- Principles of standardisation;
- Crime-security interdependencies; and
- Third-country involvement

The impacts of LOGSEC Roadmap are manifold, contributing to cost-efficient fight against crime and terrorism in the supply chain, as well as compliance with law and regulations. First, the Roadmap recommendations help to reduce theft, intellectual property rights violations, and customs law violations, among several other types of crime in the supply chain, as well as to mitigate the risk of terrorists exploiting supply chains for their destructive acts. Second, the Roadmap recommendations assist in cost-efficient compliance with various governmental regulations and voluntary programmes.

The Completed LOGSEC Roadmap can be downloaded from the Project Website:

www.logsec.org