Multi-ordEr Dependency approaches for managing cascading effects in ports' global sUpply chain and their integration in riSk Assessment frameworks

Medusa

MEDUSA will open new horizons in the area of port security, through producing and sharing knowledge associated with the **identification and assessment of cascading effects in the global ports' supply chain,** with a view to predicting potential problems but also to minimize the consequences of diverge security incidents. MEDUSA is carried out by a multidisciplinary team, which brings together port stakeholders (Europhar), security experts (AIT), experts in multi-dependency algorithms (UPRC, UCY) and experts in ICT modelling and simulation tools (SiLO).

http://medusa.cs.unipi.gr

MEDUSA Specific Objectives

01-3 ANALYSIS

Elicit and alleviate the cascading effects of port-related security incidents on interdependent infrastructures. Contact **100 stakeholders (port security officers/operators, security auditors) across more than 4 European ports**. Search and introduce algorithms for identifying **multi-order dependencies of security incidents and risks** in the scope of multi-sector cross-border scenarios. Analyze two alternative techniques based on game theory and graph theory. To identify and document **security measures that could minimize the consequences of cascading effects** in multi-sector cross-border port security scenarios.

04-6 IMPLEMENTATION

Implement **ICT tools for modeling, visualizing and simulating security scenarios and their cascading effects cross CIIs** and supply chain actors that are dependent on port CIIs: Integrate the project's algorithms within state-of-the-art methodologies for risk management and risk assessment associated with ports CIs.

07-8 PILOT & EXPLOITATION

Validate the project's results on the basis of **realistic scenarios and through the involvement of port stakeholders. More than 100 stakeholders in 4 ports** will be involved in the validation and evaluation processes of the project. Elicit and document best practices for the alleviation of the cascading effects of risks and security incidents on port CIs and dependent CIs. A set of eight core **best practices** will be produced in addition to secondary best practices. To ensure the sustainable adoption and wider use of the project's results based on the development and execution of appropriate **dissemination and exploitation plans**. Outreach of the project to more than **2000 relevant users and stakeholders**.

MEDUSA Expected Results

R1: Analysis of stakeholders' requirements associated with the assessment and mitigation of cascading effects in port security.
R2: A range of algorithms for handling multi-order events associated with port security.
R3: An integrated risk assessment methodology for alleviating the impact of the cascading effects.
R4: A set of ICT tools supporting port/security operators in the management and visualization of cascading effects and dependencies.
R5: A range of best practices and policy development guidelines.
R6: Multi-facet evaluation reports.
R7: Guidelines for the blending and integration of the MEDUSA tools with the legacy ICT infrastructures of the ports for risk management/assessment.

MEDUSA Partnership

UNIVERSITY OF PIRAEUS RESEARCH CENTER

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

University of Cyprus

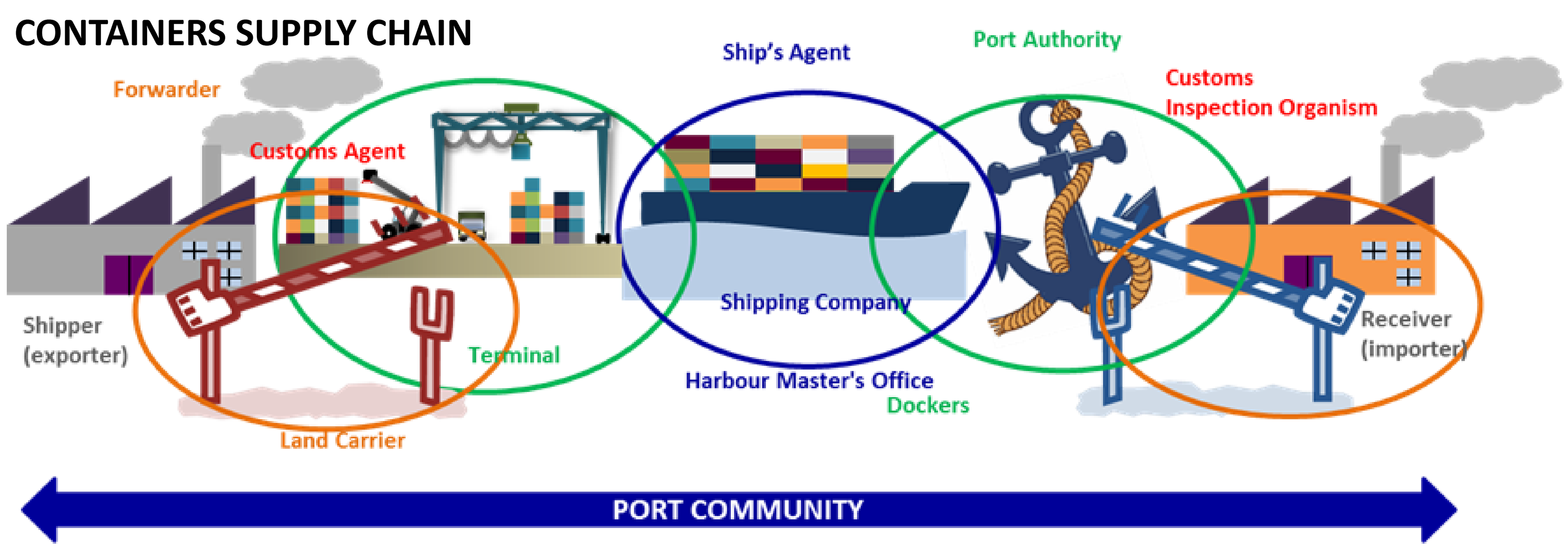
EUROPHAR

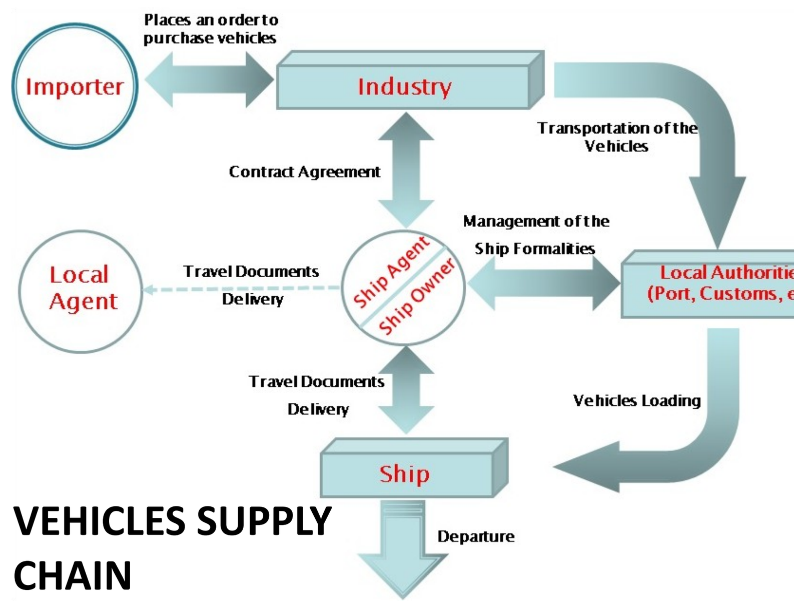
SingularLogic Innovation at your doorstep

MEDUSA cross-sector scenarios

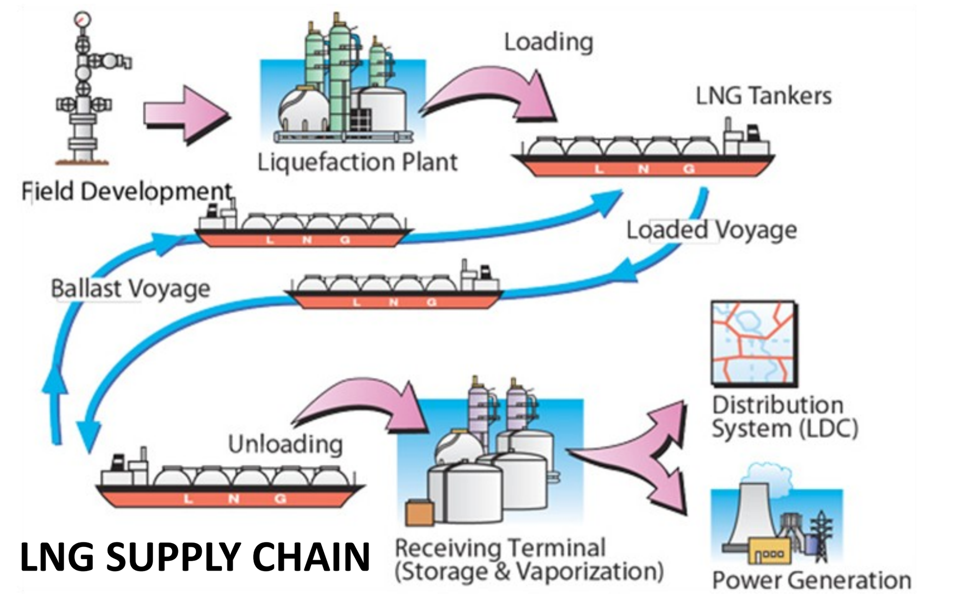
The following services have been selected by **Medusa** which will serve as the scenarios to apply the **Medusa risk assessment**.

CONTAINERS SUPPLY CHAIN





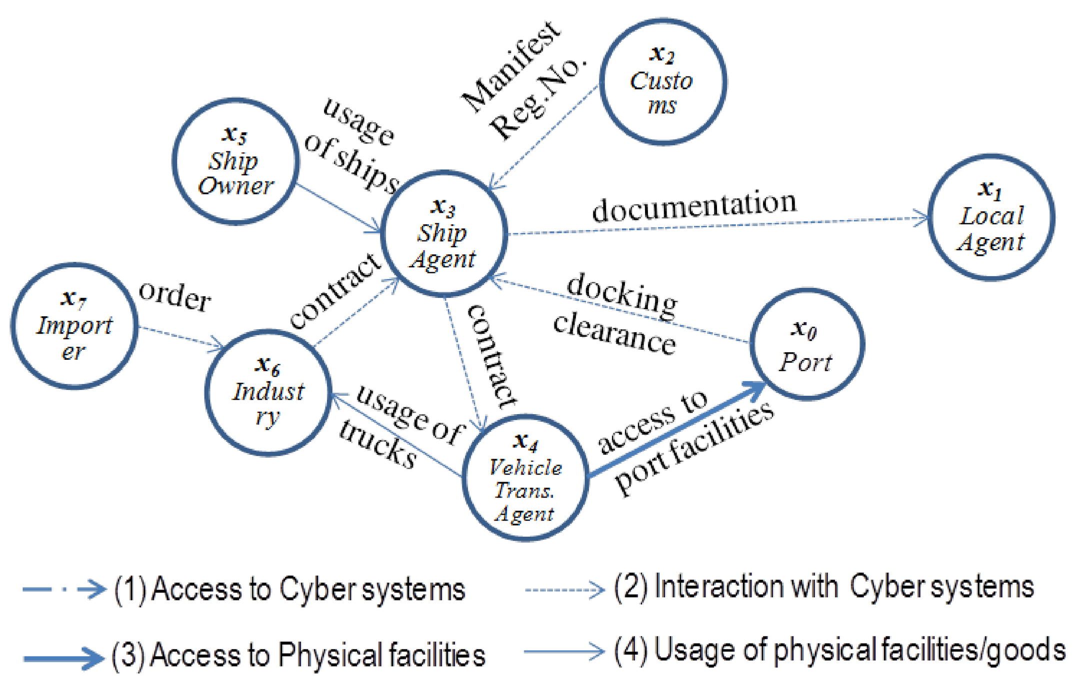
VEHICLES SUPPLY CHAIN



LNG SUPPLY CHAIN

MEDUSA Methodology

Supply Chain Dependency Graph



1 - Define a minimum and a maximum path length l_0 and l_{max} respectively. Typical values are dependency paths between 2 to 5 nodes (i.e. from 1st-order to 4th – order dependencies).

2 - Each node within a SC Graph will be examined as a potential initiator of a cascading dependency chain. Without loss of generality, say that y_0 is the source of a chain.

3 - For each examined source node y_0, identify all possible dependency chains that initiate from y_0 with length between l_{min} and l_{max}. Without loss of generality, say that $y_0 \rightarrow y_1 \rightarrow ... y_n$ is one dependency chain initiating from the node y_0.

4 - For each identified dependency chain, use the following steps to assess the risk of the dependency chain.

4.1 - For each threat scenario TS_j:

4.1.1 - For each node acting as a source node y_0:

4.1.1.1 - For each dependency chain $y_0 \rightarrow y_1 \rightarrow ... y_n$ initiating from y_0 (with length between l_{min} and l_{max}), compute the cumulative *cascading dependency risk* $R_{01...n}(TS_j)$ as:

$$R_{01...n}(TS_j)=\sum_{i=0}^{n}\left(\prod_{k=0}^{i} l_k(TS_j)\right)\cdot w_i(TS_j)\cdot c_i(TS_j)$$

Where l_i is the likelihood of occurrence of a threat scenario TS_j, $c_i(TS_j)$ is the consequence level on the node x_i for the threat scenario TS_j, and $w_i(TS_j)$ the weight of a business partner (node x_i), defined as the importance of x_i for the provisioning of the SC service. It represents *the business impact* of a business partner (node) for the provisioning of the SC service.

Project info and contact

Project duration: 24 months (from 1st July 2014 to 30th June 2016)
Project Leader: University of Piraeus Research Centre
Project Manager: Nineta Polemi— dpolemi@unipi.gr

Cofunded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks Programme of the European Union