The maritime environment is rather complex, since it involves and interacts with many entities including ships, port authorities, maritime and insurance companies, customs, banks, ministries, ship-building executives and other commercial providers, as well as with other critical infrastructures (e.g., railroads, airports, etc.). Complex and heterogeneous information and telecommunication (IT) systems are a prerequisite for an efficient management and operation in such an environment.

Commercial ports are considered a transportation critical infrastructure, as they are large-scale infrastructures and their degradation, interruption or impairment of their Port IT (PIT) Systems may have serious consequences on the national security as well as on the health, safety, economy and welfare of citizens and nations. PIT Systems are characterized with a multiplicity of interdependencies with the other entities in the maritime environment.

The normal functionality of the ports depends largely on the proper operation of their IT systems. The large amount of critical and sensitive data, the information and services that are managed on a daily basis, the large number of entities called to be served, and the interdependencies with the other infrastructures require effective security management.

Nevertheless, the current maritime legislation and/or standardization efforts do not cover the IT security of commercial ports sufficiently. By identifying these needs, S-PORT offers a collaborative environment that hosts security management services and guides commercial ports to monitor and self-manage their PIT security.

### S-PORT Outcomes

S-Port views the ports as critical infrastructures and addresses their PIT security needs by offering:

- **A collaborative environment** (S-PORT Environment) enabling PIT users to get informed about the latest threats, vulnerabilities, best practices and legislation and to interact and network in addressing their daily PIT-security concerns.

- **A targeted security management collaborative methodology** (S-PORT RM) for the PIT-sytems based on IT security management standards (ISO-27001) and the ISPS code involving all PIT users. The various phases of the S-PORT RM methodology are implemented as collaborative e-services (S-PORT-RM services) hosted in the S-PORT Environment.

S-PORT is a prototype of a new generation, collaborative and innovative security management environment, which provides the necessary level of confidentiality, reliability, interactivity and interoperability for the PIT systems.

### S-PORT Environment

The overall architecture of the S-PORT collaborative environment consists of four main entities:

- **S-PORT Main Platform:** A three-tier architecture that includes:
  - **Web Interactive Tier:** Based on Web 2.0 technologies and open source solutions (for example, Ajax forms, popup help menus, charts, etc.) offering graphical and user-friendly representation and collaboration among S-PORT users.
  - **Enterprise Tier:** Consists of all the systems that are responsible for the offering of the S-PORT RM services.
  - **Database Tier:** Hosts all the S-PORT information assets (e.g., PIT assets, impact categories, threats, vulnerabilities).

- **Business Process Management System (BPMS):** Undertakes the accountability to identify and depict the business procedures of critical e-services of PIT in order to facilitate the production of a graphical representation of these procedures as well as of their primary assets.

- **IAM System:** Responsible for the identity and access management, implementing security mechanisms and policies that enhance the S-PORT environment with proper authentication and authorization policies enforcing end-user’s preferences and requirements.

- **Middleware System:** An enterprise service bus (ESB) that is a lightweight messaging framework, ensuring that the four S-PORT entities interplay through a common channel.

### S-PORT Services

- **Risk Management Service:** Identifies the vulnerabilities of each asset with the use of open source VA tools (e.g., nmap, openvas).

- **Security Policy/BCP Service:** Designs and keeps updated the PIT security policy and business continuity.

- **Communication Services** (forum, wiki, chat rooms, blog, document library): Enabling the users to interact, resolve their risk assessment / management concerns, and find solutions about daily PIT problems.