Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Safety management (TQM, ISM code, inspections, principles of co-operation on safety) – PART 2
A practical example

Koliousis, Ioannis
Papadimitriou Stratos
Ernestos Tzannatos
Department of Maritime Studies
University of Piraeus
And
Yannis Papagianopoulos
Piraeus Port Authority

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

Today's Agenda

- Introduction – Port Community Systems
- Port Risk Assessment Methodology
- Case Study: CYSM Project
- Automated Board Control and Risk Management

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

- Introduction – Port Community Systems
- Port Risk Assessment Methodology
- Case Study: CYSM Project
- Automated Board Control and Risk Management

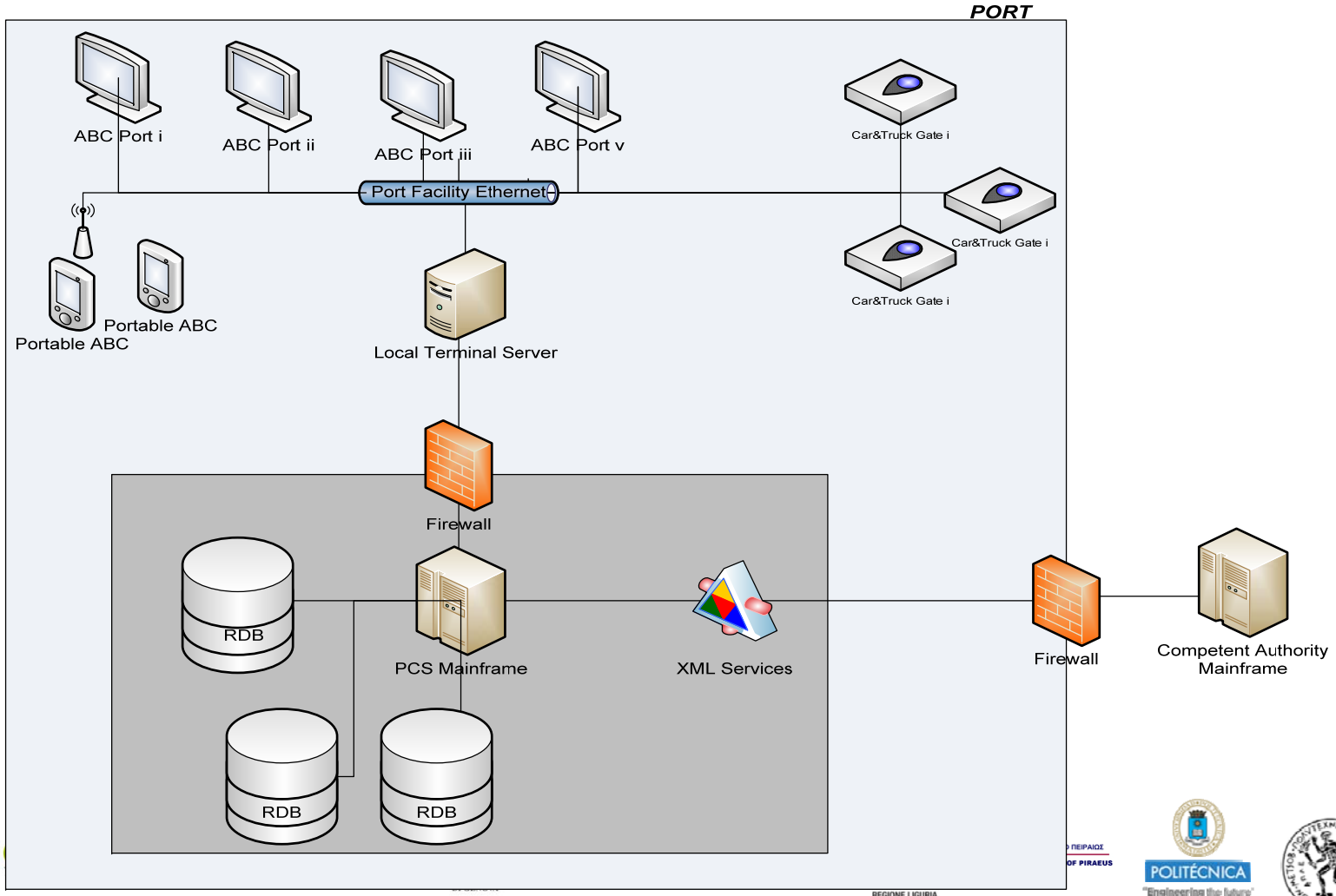
Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Access control in Ports calls for efficiency upgrade through automated systems

- Unauthorized access in port facilities is a threat with a high impact level
- International Ship and Port Facility Security Code (ISPS) has provisions for border control but ports are heavily relying on manual inspections.
- FRONTEX practical handbook with generic requirements (FRONTEX, 2012) for the ABC systems
  - ⇨The case of Finish Ports in Europe
  - ⇨Malaysian and Taiwan Ports are piloting ABC systems

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Port Community Systems (PCS): Architectural Overview



Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Risk management of PCSs

- PCS account for certain risk mitigation measures (firewalls, xml communications to reduce DB exposure, etc.)
- But also entail blackspots and weakest links…
  - Infrastructure-wise, the distributed nature of the ABCs and Gate Controls expose part of the system to higher risks especially to outsiders and
  - Process-wise, there is an increased need to implement and execute stricter and more robust processes regarding the risk mitigation

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

- Introduction – Port Community Systems
- Port Risk Assessment Methodology
- Case Study: CYSM Project
- Automated Board Control and Risk Management

University of Strathclyde Glasgow
Circle Touch your ideas
FCSH Faculdade de Ciências Sociais e Humanas
CIMNE
Università degli Studi di Genova
magellan
OceanFinance
Regione Liguria
Πανεπιστήμιο Πειραιώς University of Piraeus
Politécnica "Engineering the future"

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

High Level Classification of Port related Threats

- ***Physical infrastructure Threats***, including all port facilities (e.g. terminal facilities, warehouses, parking areas, manufacturing areas);
- ***ICT Infrastructure Threats***, including networks, ICT related hardware systems/equipment;
- ***Systems and Software Threats***, including servers, RDBs, systems, software;
- ***Port services Threats*** (e.g cargo management, reservation, navigation) hosted by the PCS systems;
- ***Information*** **and Electronic data** ***Threats***, including information, databases, log files and log books;
- ***Users and Procedural Threats*** from /to all users (internal, external, freight, cargo) that interact with the port physical and cyber assets and they procedures that they operate under.

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Indicatively, a Threat & Vulnerability assessment includes assessing following:

- Malicious human activity related threats, e.g. a member of the port authority staff apprehends passwords and domain names, or infiltrates malicious software;
- Physical attacks from outside the port perimeter ;
- Weather conditions (heavy winds, severe cold, heat waves, rain) may cause disruption of ABC systems operation; Physical disasters (e.g. fire) and phenomena are threats for the port facilities;
- Unauthorized access in areas based on access permits;
- Inadequate equipment and material ;
- Inadequate or incapable access control and authentications processes ;
- Cyber attacks that affect the availability of information (DDOS attacks, Trojans, etc.);
- Improper execution and documentation of processes and procedures.

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

In order to cope with this situation this Port Security Risk Assessment Methodology is proposed (I/II)

- Develop a security awareness process
  - Define a framework for the activity and an agenda for identification;
  - Identify the security awareness level of the port;
  - Develop an exhaustive list of all physical and cyber assets of the port and their interdependencies.
- Understand and establish the risk analysis
- Identify the physical and cyber threats that the port facitlities face as well the cyber threats targeting the PCS systems;

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

In order to cope with this situation this Port Security Risk Assessment Methodology is proposed (II/II)

- Identify external existing and potential threats that arise from external interdependent entities (e.g. customs, maritime companies, logistics service providers);
- Calculate the impact levels of the identified threats;
- Develop a set of vulnerabilities based on the identified threats;
- Calculate the risks for each asset and each threat;
- Categorize risks into internal and external per port asset.

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

The Port Security Risk Assessment is based on:

- The **ISPS Code** (International Maritime Organization, 2012)
- **IMO Provisions** (International Maritime Organization, 2002)
- **ISO 9000** family of standards, (International Standardization Organization, 2009), (International Standardization Organization, 2008)
- **ISO 27000** family of standards, (International Standardization Organization, 2005)
- **ISO 31000** family of standards, (International Standardization Organization, 2009)
- Independent risk consultants assessments

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

- Introduction – Port Community Systems
- Port Risk Assessment Methodology
- Case Study: CYSM Project
- Automated Board Control and Risk Management

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Case Study: Security Awareness in four E.U. Ports (I/II)

A survey in the context of the CYSM Project identified the following relevant issues:

- A broad range of definitions and the security concepts
- Port Facility Security Officers (PFSOs) give particular attention to physical security (safety), oftentimes tacitly ignoring the three components of security, i.e. confidentiality, integrity and availability
- Ports are ISPS compliant, effectively covering the safety within the ports,
- The security standard approach is not holistic in terms of risks identified, assessed, and mitigated.
- Very recently the ports started coping with cyber threats
- Lack of a comprehensive and exhaustive risk matrix,

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

Case Study: Security Awareness in four E.U. Ports (II/II)

- The value of information security is not entirely realized as of value to the business model and to the business offering
- No Critical Infrastructure Protection planning standards or methodologies.
- The ports are planning to install diverse technologies, from access control (e.g. smart cards, Automated Border Control, RFIDs) to access awareness (e.g. firewalls, intrusion detection systems, etc).
- The reporting framework put in place from the Competent Authorities is weak and doesn't provide adequate Knowledge Sharing between authorities.
- There is no adequate training for Cyber Security for Ports

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

- Introduction – Port Community Systems
- Port Risk Assessment Methodology
- Case Study: CYSM Project
- Automated Board Control and Risk Management

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Some initial thoughts on Port ABCs (I/II)

Future ABC systems in order to become appropriate for the port environments need to be:

- **Situated in various locations of the port** (e.g. on ship, arrival/departure areas, Warehouses, on/in vessels, etc);
- **Adequate in number** to ensure that controls are carried out quickly and efficiently;

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

Some initial thoughts on Port ABCs (II/II)

- **Extensive in nature of operational attributes**:
  - Indoor ABC gates in the ports' indoor terminals for passengers and crew;
  - Mobile ABC gates on board ship or in an area set aside;
  - ABC portable devices held by the patrol officers in case the ship arrives outside the port terminal and the border guard need to reach it by boat;
  - Large Cargo Gates for vehicles, Containers and Cargo.
- **Strong Cross certification procedures and** mechanisms between the Country Verifiers Certification Authorities (CVCA) communicating with the ABCs ensuring the interoperability of ABCs;
- **Harmonize** all ABCs in all entry points (i.e. railways, roads, airports) in order to accelerate the checking process.

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

TrainMoS II

- Questions?
- Comments?

University of Strathclyde Glasgow
Circle Touch your ideas
FCSH Faculdade de Ciências Sociais e Humanas
CIMNE
Università degli Studi di Genova
magellan
OceanFinance
Regione Liguria
Πανεπιστήμιο Πειραιώς University of Piraeus
Politécnica "Engineering the future"

Co-financed by the European Union
Trans-European Transport Network (TEN-T)

End of Session

Thank you for your attention!

Q&A

More info?

igk@unipi.gr