SAURON
Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports

Agenda

Time	Item
10:00-10:10	Welcome and opening
10:10-10:30	SAURON project Overview
10:30-11:30	**SAURON main components** Physical Situational Awareness (PSA) Cyber Situational Awareness (CSA) Hybrid Situational Awareness (HSA) Emergency Population Warning System (EPWS)
11.30-11.40	SAURON Valencia pilot presentation: Terrorist attack at CSP Container Terminal
11:40-12:30	SAURON Valencia Pilot Demonstration
12:30-12:45	Questions and conclusions
12:45-13:00	Evaluation questionnaire https://forms.gle/QLkmHwydStuU3abHA

SAURON project Overview

Rafa Company, Project coordinator [Fundacion Valenciaport]

Background

An attack on a big EU port (cyber, physical or a combination) could damage the CI and seriously impact its vicinity.

Most recently Rotterdam, Antwerp and others have been subject to combined attacks on their IT and physical infrastructure for criminal gain and in future this may grow to include acts of terrorism. The damage to a big port in an EU country could cause a dramatic loss of life and mass casualties, as well as major social disturbance.

MAERSK | MARKETS | PEOPLE | HARDWARE | INDUSTRIES | INVESTOR RELATIONS

Maersk IT systems are down

We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack. We continue to assess the situation. The safety of our employees, our operations and customer's business is our top priority. We will update when we have more information.

Follow our Twitter feed for more information.

'Petya' ransomware attack strikes companies across Europe and US

Ukraine government, banks and electricity grid hit hardest, but companies in France, Denmark and Pittsburgh, Pennsylvania also attacked

Police warning after drug traffickers' cyber-attack

By Tom Bateman
Reporter, Today programme

🕐 16 October 2013 | Europe   f 🐦 💬 ✉ ◁ Share

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

Earlier this year drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

His comments follow a cyber-attack on the Belgian port of Antwerp.

Drug traffickers recruited hackers to breach IT systems that controlled the movement and location of containers.

✠ Home / Shipping News / Piracy and Security News / Maritime cyber security

Maritime cyber security

■ in Piracy and Security News 🕐 12/08/2017

The recent NotPetya malware attack, which affected Maersk in the shipping sector as well as a large number of other firms, has served as a wake up call to the maritime industry. Cyber security isn't something that just affects land-based businesses; it can have a major impact on maritime operations, too.

There are currently a number of organisations conducting research into preparedness and resilience in order to gain a better overall picture of the current level of security in the maritime industry.

Futurenautics Intelligence is currently undertaking the largest research project in the industry into maritime cyber security, combining the data from its bi-annual seafarer survey 'Crew Connectivity 2017' – which in 2015 had over 3,000 respondents – and client-commissioned research on cyber-security strategies. The resulting dataset will provide the most detailed and comprehensive information about the maritime cyber-landscape and will be made available free of charge.
Source: Maritime Security Review

Scalable multidimensionAl sitUation awaReness sOlution for protectiNg European ports.

The vision of SAURON is to provide **a multidimensional yet installation-specific Situational Awareness platform** to help port operators anticipate and withstand **potential cyber, physical or combined** threats to their freight and cargo business and to the safety of their employees, visitors, passengers and citizens in the vicinity
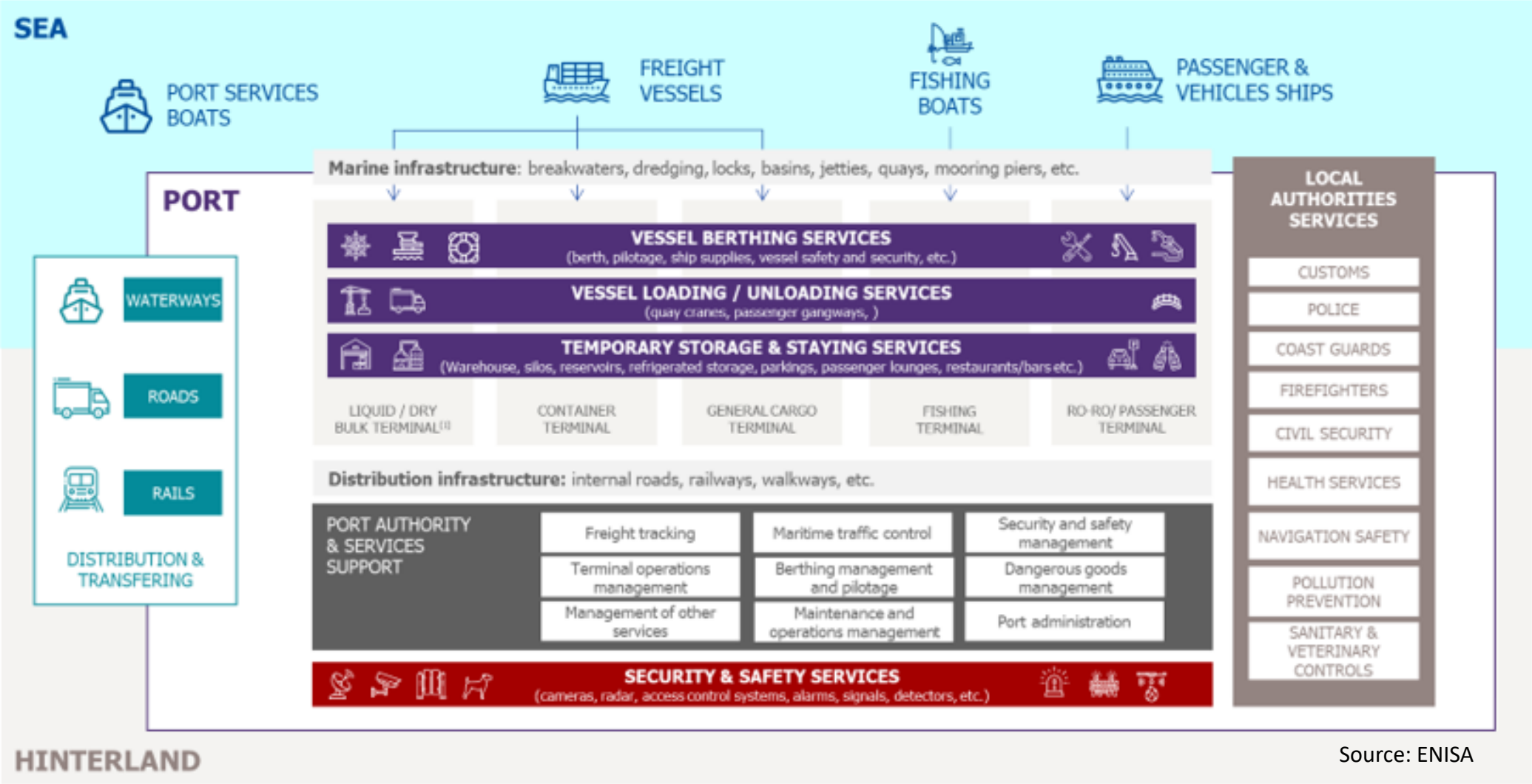

Hacked

Maritime Port Infrastructure and Services

Source: ENISA

Maritime Port Infrastructure and Services

PORT AUTHORITY

CEO	Harbour Master	Administration & Finance	Infrastructure & OT Management	Information Technology
Human resources	Safety & Security	Marketing & Communications	Environmental & territorial management	Cybersecurity

PORT TERMINAL OPERATORS

CEO	Administration & Finance	Infrastructure & OT Management	Cybersecurity
Human resources	Marketing & Communications	Information Technology	

Source: ENISA

AUTORITIES

Customs

Fishery Control

Coast Guards
(Navigation safety)

Border control

Civil Security

Police
(Law enforcement)

Prevention of pollution
(Environnement protection)

EU Agencies
(EMSA, EFCA, FRONTEX, EUROPOL, ENISA)

International bodies
(IMO, WCO, IMB, IMSC...)

Source: ENISA

Maritime Port Security

PORT SECURITY (FIRST PRACTICIONERS LINE)

- PORT AUTHORITIES (<u>PARTNERS OF SAURON</u>)

  1. VALENCIA (Spain)
  2. PIRAEUS (Greece)
  3. LIVORNO (Italy)
  4. KOPER (Slovenia)

Contacted / cooperation with:

- COAST GUARDS
- RESCUE MARITIME TEAMS
- HARBOUR MASTER
- NAVY
- PORT, NATIONAL AND LOCAL POLICE (CIVIL SECURITY)
- CUSTOMS (BORDER CONTROL)
- INTERPORTPOLICE - INTERNATIONAL ORGANIZATION OF AIRPORT AND SEAPORT POLICE (AB)
- IMO

SAURON, **led by a critical infrastructure operator**, will achieve its objectives through 4 specific, exploitable results which will be validated in **real conditions** with the direct involvement of **4 EU PORTS and 1 PTO**.
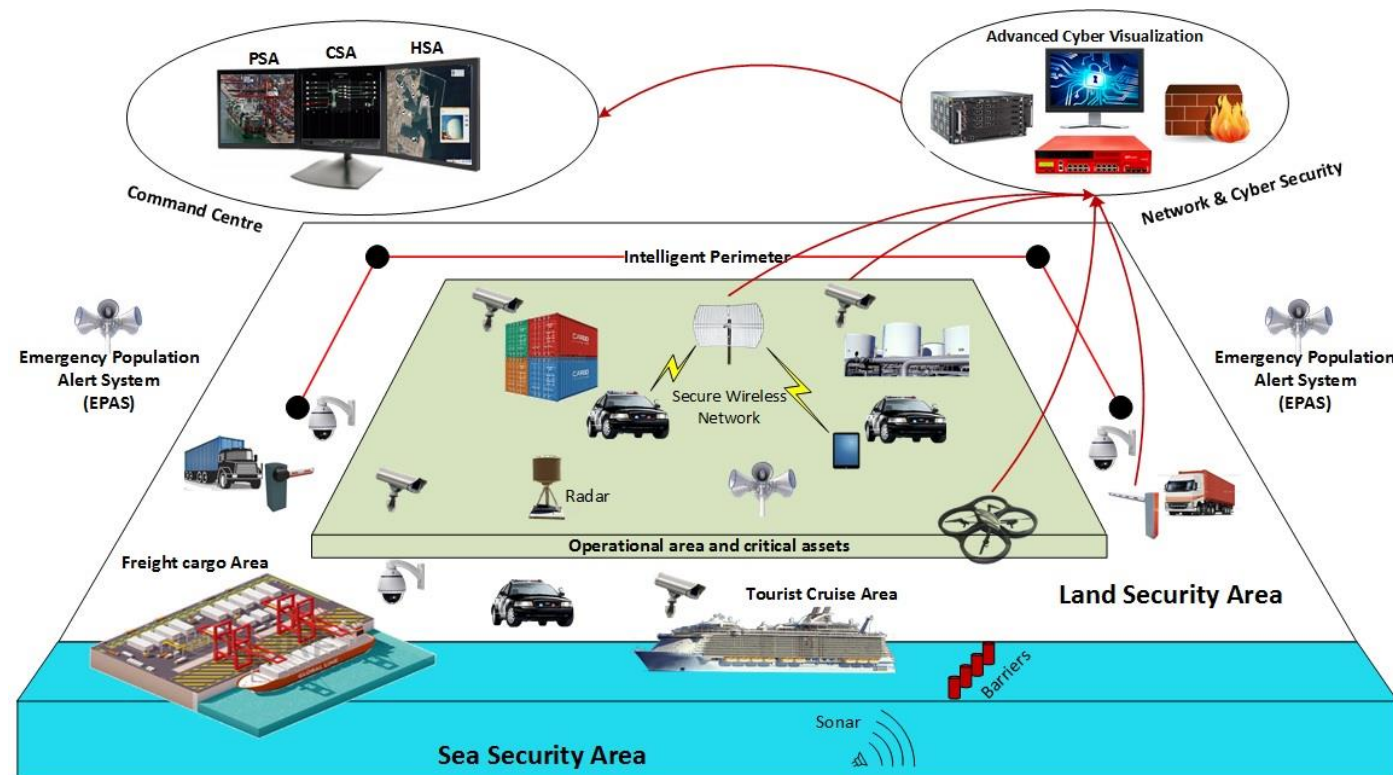
Sauron Partnership
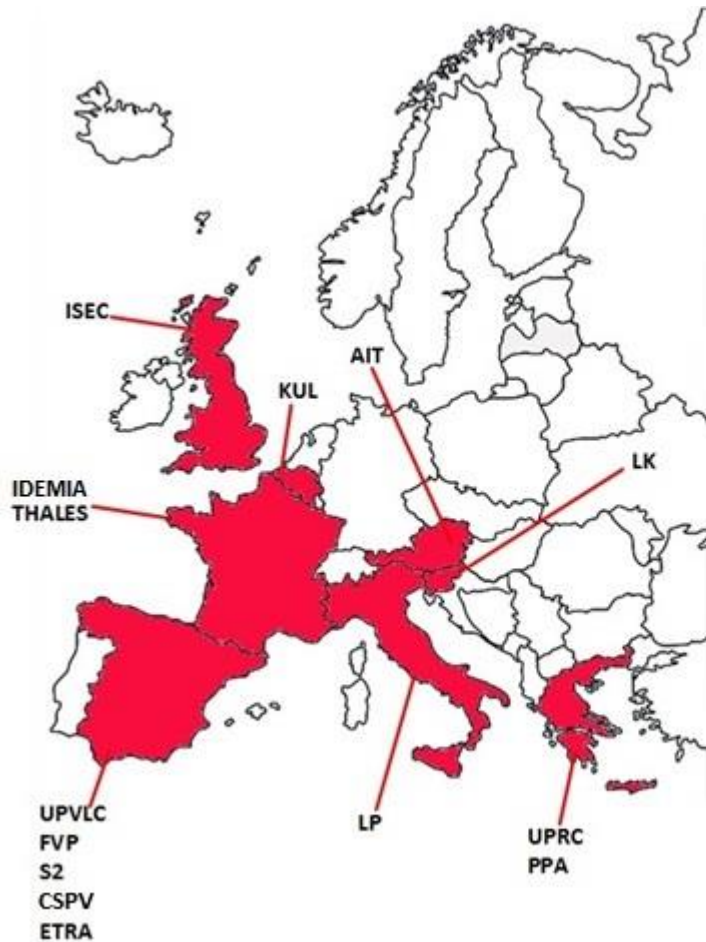
OPERATORS/END USERS	
FVP	ES
CSPV	ES
PPA	GR
LP	IT
LK	SI

BIG INDUSTRY	
THALES	FR
IDEMIA	FR
ETRA	ES

| UNIVERSITY/RTO	
UPVLC	ES
UPRC	GR
AIT	AUS
KUL	BE

SME	
S2	ES
ISEC	UK

Advisory Board

- ICHCA AND BROUGHT MARINE LIMITED
- SECURITY SERVICE/ NATIONAL CENTER FOR CRITICAL INFRASTRUCTURE MINISTRY OF INTERIOR, SPAIN
- OTHO LIMITED
- SPANISH ARMY
- EUROPEAN ASSOCIATION OF AIRPORT AND SEAPORT POLICE

Sauron Concept

The SAURON project proposes an holistic situation awareness concept

- PSA: A complete **physical SA** system, which includes novel features such as; dynamic location of resources and assets, location, management and monitoring of sensors, including cameras mounted on unmanned vehicles (under the conditions of and in compliance with all pertinent legal requirements at national and European level), security perimeter control, robust and secure tactical communication network and so on. This PSA system will be adapted to the EU ports characteristics, requirements and needs for protecting them against any kind of physical threat.

- CSA: An advanced and scalable **cyber SA system** capable of preventing and detecting threats and in case of a declared attack, capable of mitigating the effects of the infection/intrusion.

- HSA: A **Hybrid SA** system receiving both physical and cyber alarms on potential threats from the real world and the cyber space respectively. The HSA application and will show the potential consequences/effects of these threats in the other planes including cascading effects.

- EPWS: An **Emergency Population Warning System**, allowing local, regional, or national authorities to contact members of rescue/security teams and the public (also integrating Smart City Platforms (SCP))

*
PSA : Physical System Awareness
CSA: Cyber System Awareness
HSA: Hybrid System Awareness
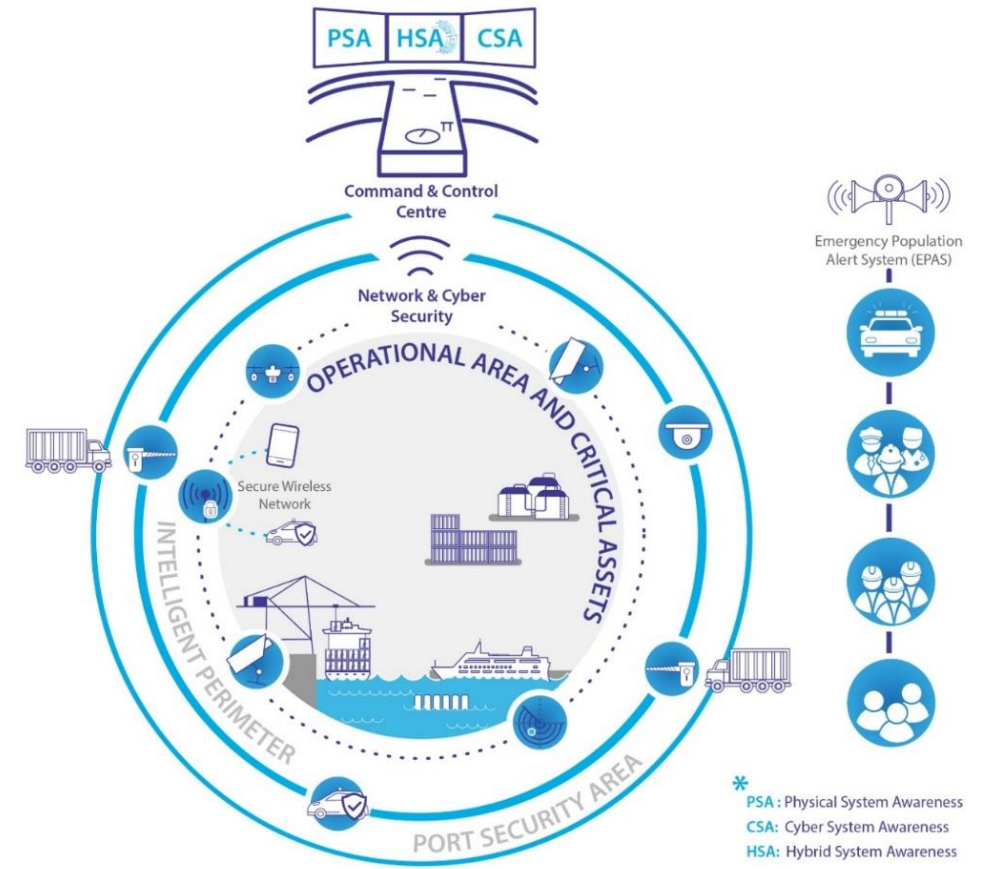
Innovative aspects

SAURON will help to avert potential threats, but should an incident occur, it will provide tools to support a rapid, more effective and safer response that fit into ports' existing incident management procedures.

- ✓ New video processing techniques for increasing the port security
- ✓ Hybrid Situation Awareness for detecting potential cascading effect – PSA, CSA and HSA
- ✓ Cyber Incident Correlation
- ✓ Intelligent Cyber-Anomaly Detection
- ✓ Advanced visualization of the cyber space
- ✓ Emergency Population Alert System

SAURON Pilots

Testing the SAURON platform : to demonstrate in a preliminary status the integration / correlation of the PSA, CSA and HSA.
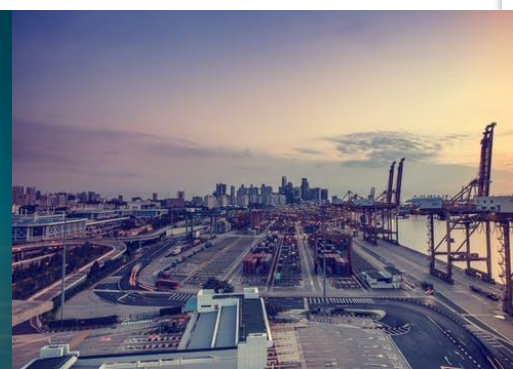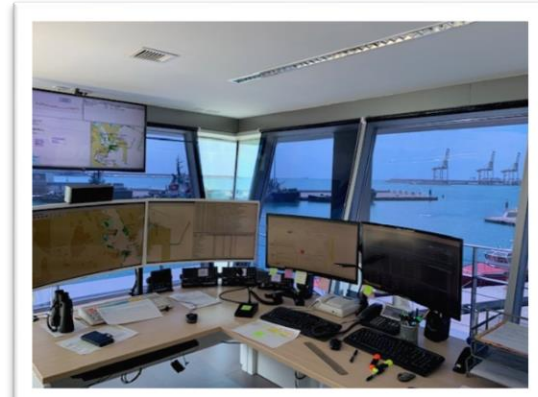
Physical sources:

- CCTV. Land and maritime side
- Presence sensor
- Fire and smoke sensors
- Drone UAV
- AIS
- GPS /tablets (Port Police)

Cyber sources:

- Threats in network communications (Intrusion Detection Systems)
- Port management databases
- Host-based intrusion detection systems (HIDS)
- Port assets' vulnerabilities

IT systems
- Terminal Operation System (TOS)
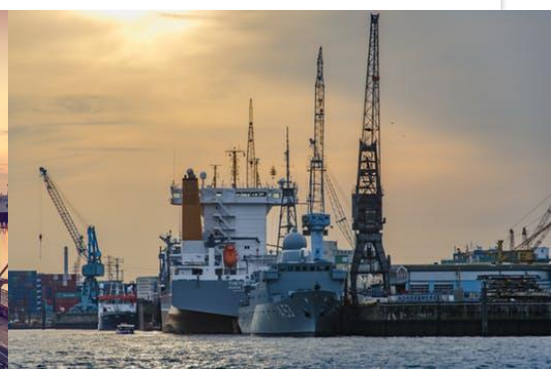
Piraeus pilot

Pilot at the Port of Piraeus (Greece) February 13th , 2020

Terrorist attack a large Cruise Ship with passengers aboard, berthed at the Port of Piraeus.

Sagunto pilot

Pilot at the Port of Sagunto (Spain) November 21st , 2019
(in collaboration with ROCSAFE Project)

Drone detects a truck accident in a transit zone inside the Port of Sagunto.
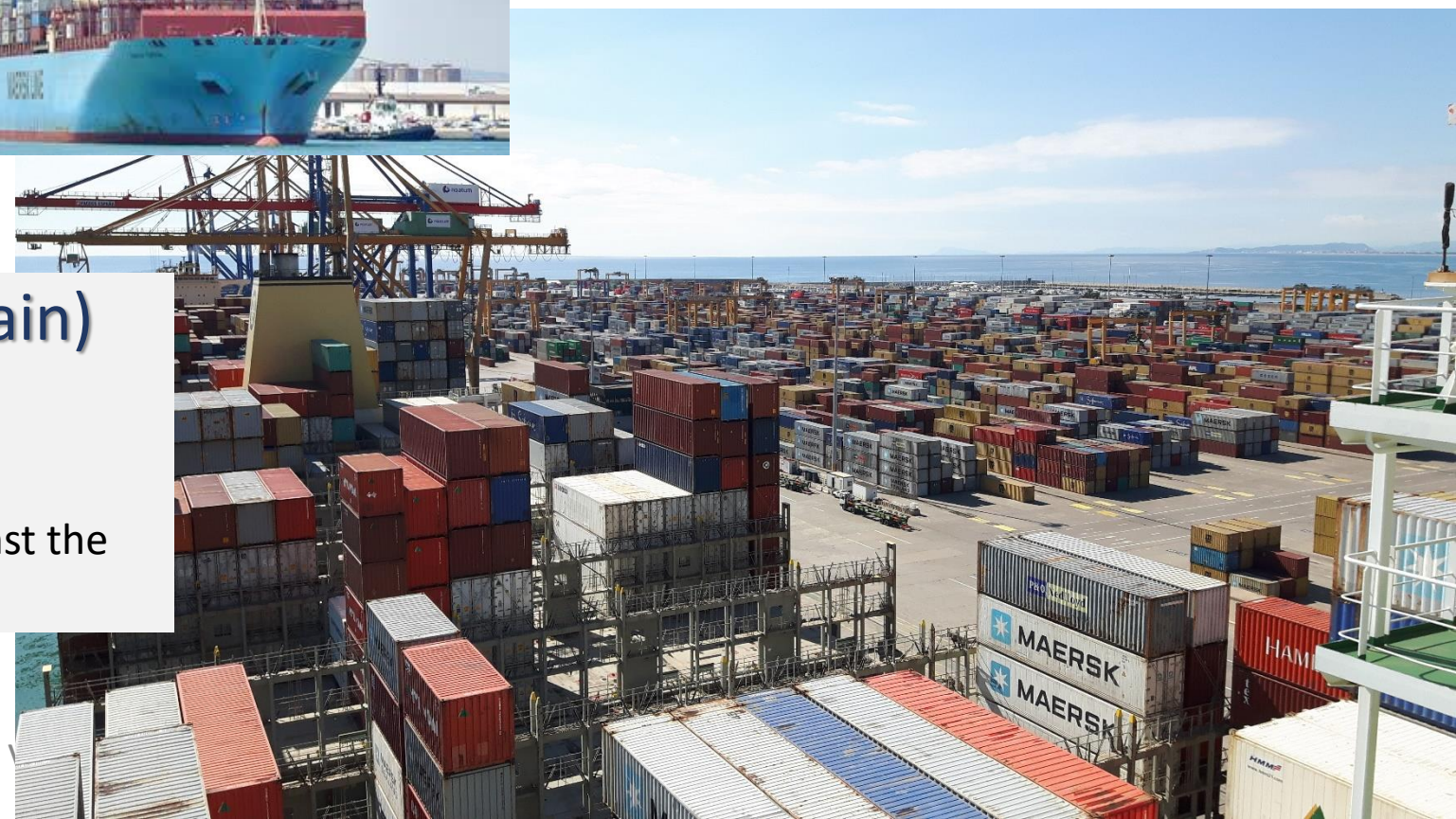
Valencia pilot

Final Pilot - Port of Valencia (Spain)
June 2020

A terrorist group plans a combined attack against the
container terminal to detonate a bomb.

2nd July 2020

Thanks for your attention!

Rafael Company
SAURON project coordinator
rcompany@fundacion.valenciaport.com

https://www.sauronproject.eu/
@SAURONprj