Scalable multidimensionAl sitUation awaReness sOlution for protectiNg European ports.

Sauron

CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

Rafael Company
Valenciaport Foundation
rcompany@fundacion.valenciaport.com

Vienna, 19 and 20 of September, 2017

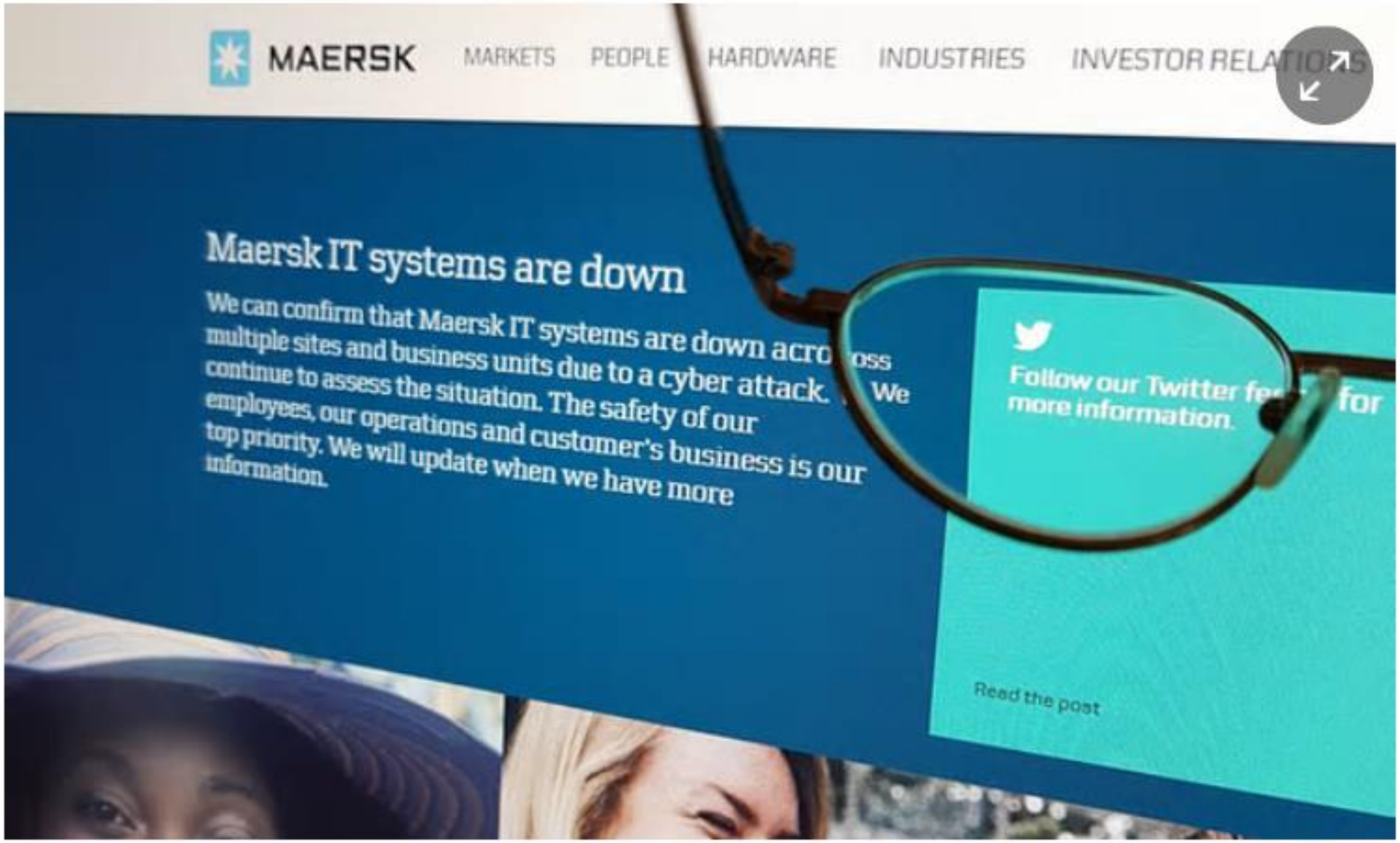
SAURON_ background

Scal
multidim
sitUation a

'Petya' ra
compani

Ukraine governm
France, Denmark

:s



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.

Shipping company Maersk's IT system was impacted by the cyber-attack. Photograph: Mauritz Antin/EPA

Ukraine has blamed Russia for previous cyber-attacks, including one on its power grid at the end of 2015.

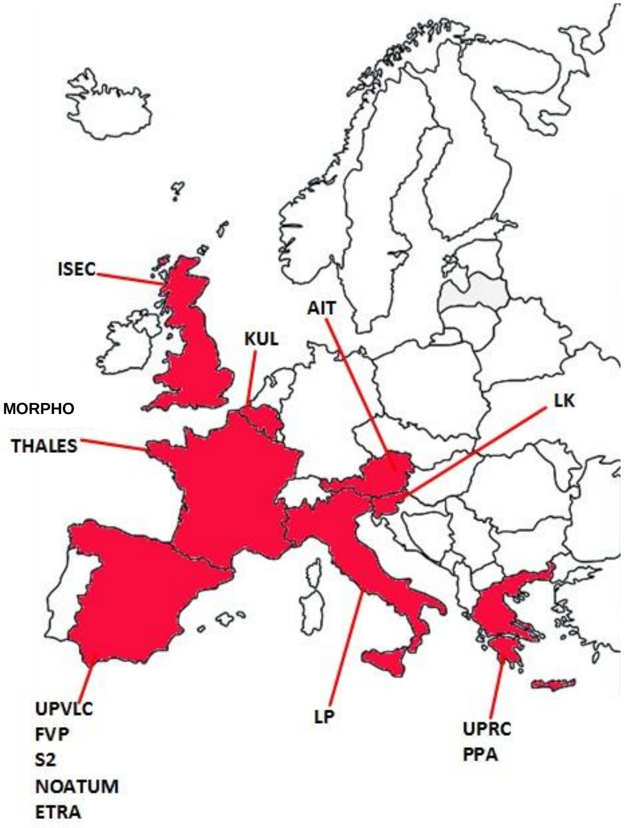
each IT systems that controlled the

//www.bbc.com/news/world-europe-24539417

SAURON_ scope & partnership

European Union ports are currently facing **cyberphysical threats** which can potentially cause **hundreds of thousands of casualties** and have an impact of **tens of billion euros** in the EU economy.

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**.



OPERATORS/END USERS	
FVP	ES
NOATUM	ES
PPA	GR
LP	IT
LK	SI

BIG INDUSTRY	
THALES	FR
MORPHO	FR
ETRA	ES

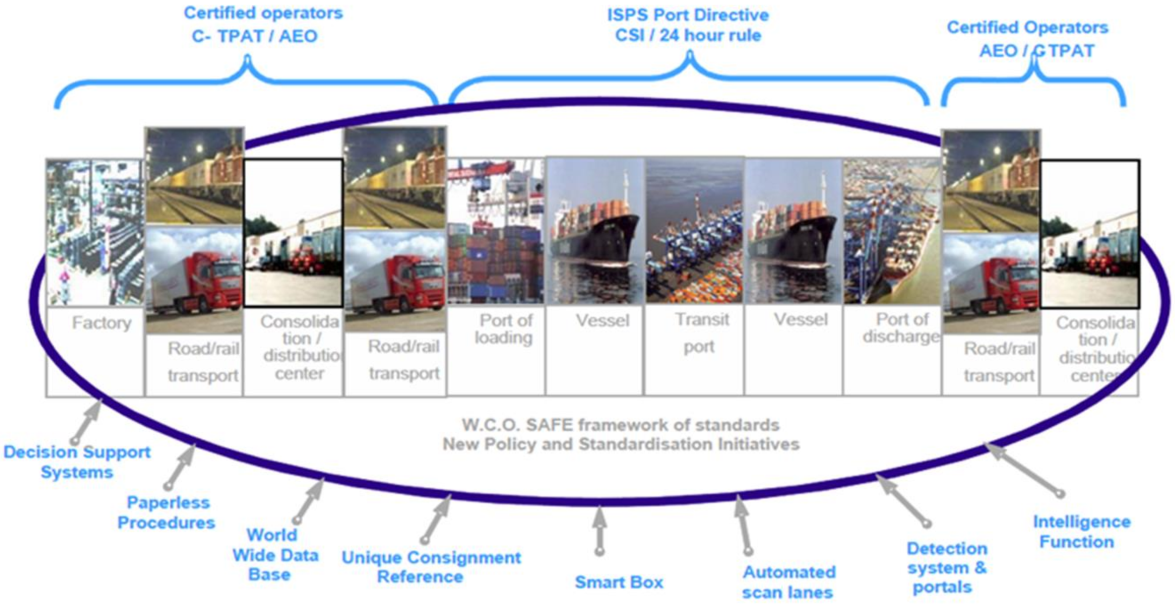
UNIVERSITY/RTO	
UPVLC	ES
UPRC	GR
AIT	AUS
KUL	BE

SME	
S2	ES
ISEC	UK

FUNDACIÓN valenciaport
S2 GRUPO
UNIVERSITAT POLITÈCNICA DE VALÈNCIA
OΛΠ PIRAEUS PORT AUTHORITY S.A.
UNIVERSITY OF PIRAEUS RESEARCH CENTER
InnovaSec
Innovation in Cyber-Physical Security
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Autorità di Sistema Portuale del Mar Tirreno Settentrionale
etra I+D
KU LEUVEN
CENTRE FOR IT & IP LAW
THALES
OT MORPHO
noatum
CONTAINER TERMINAL VALENCIA
LUKA KOPER
Port of Koper

SAURON_ vision

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



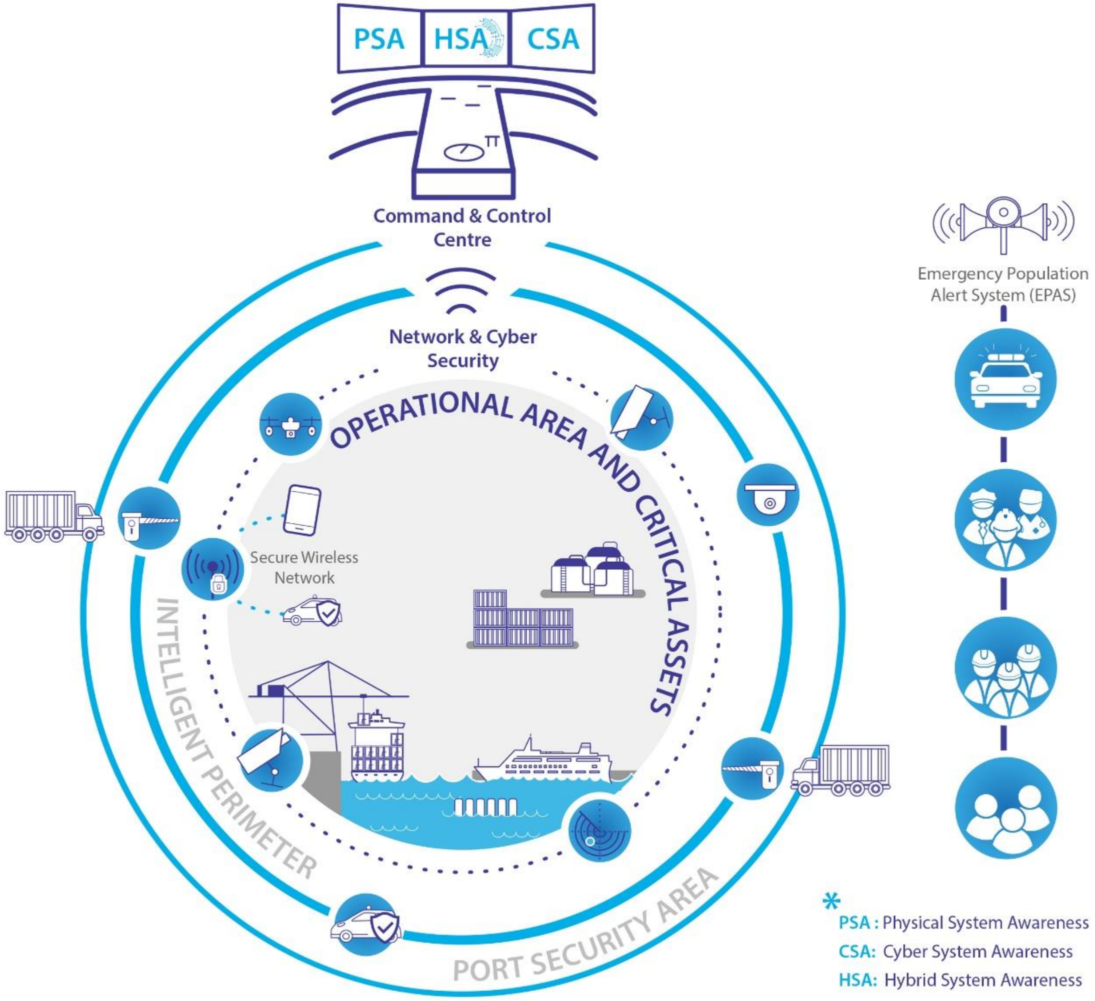
SAURON_ added value

There is currently no integrated system to protect major ports' infrastructure, personnel, goods and surroundings against physical, cyber and combined threats.

COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of <u>European critical infrastructures</u> (CIs) considers EU ports as one of the main CIs in the EU5 and its protection is a key issue for the EC.

SAURON_ concept

The **SAURON project proposes an holistic situation awareness concept**



*

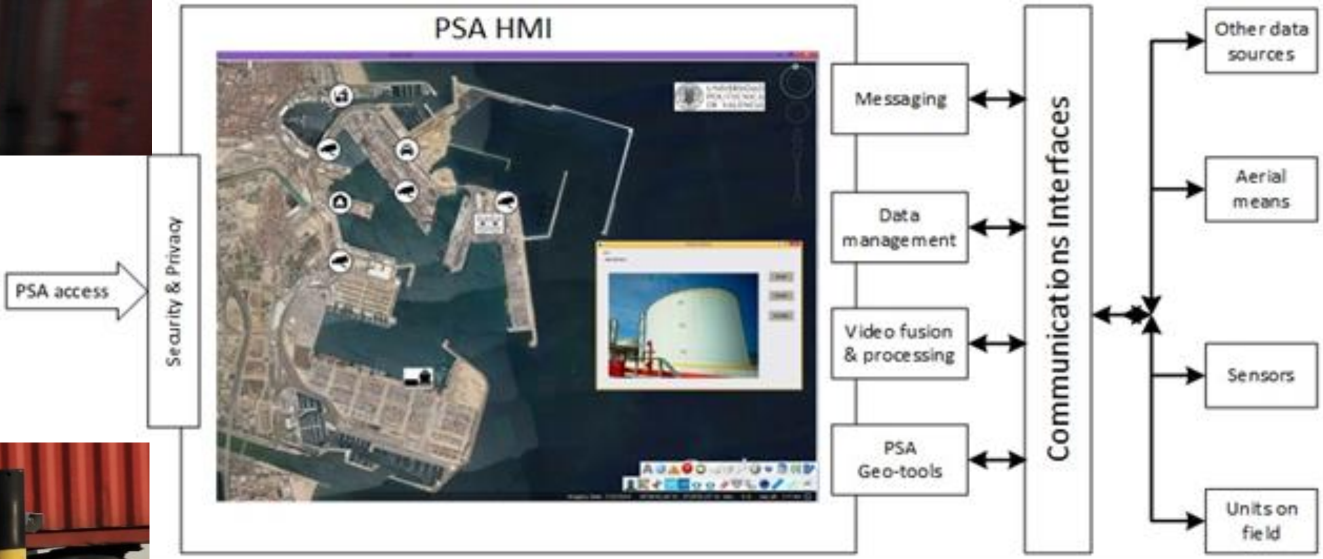
PSA : Physical System Awareness

CSA: Cyber System Awareness

HSA: Hybrid System Awareness

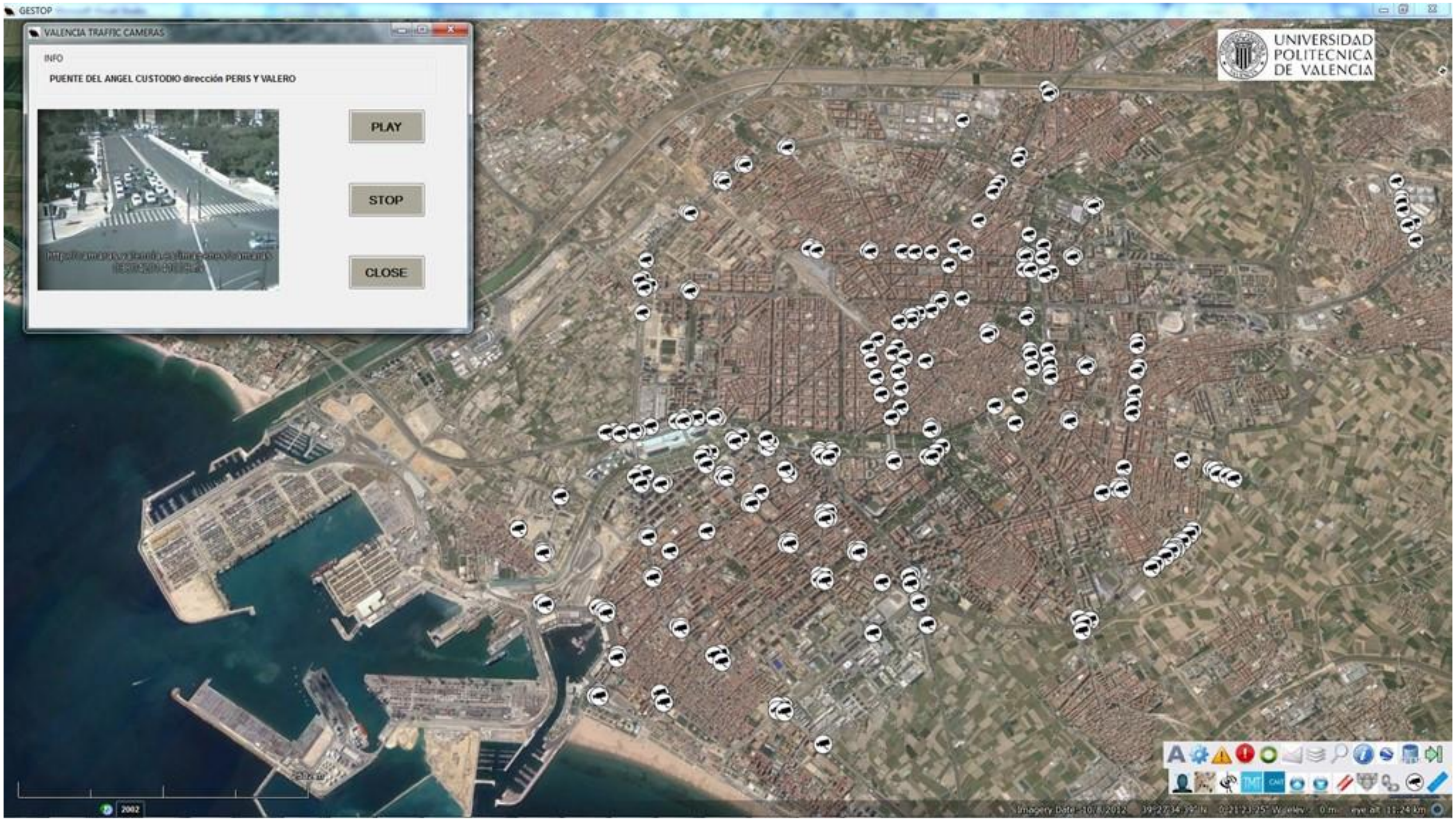
PHYSICAL SA

The PSA will be based on the civil version of the Spanish Army Friendly Force Tracking (FFT) system developed by UPVLC. This system is a complete SA solution capable of integrating a wide range of sensors and offering advanced SA and Command and Control Capabilities



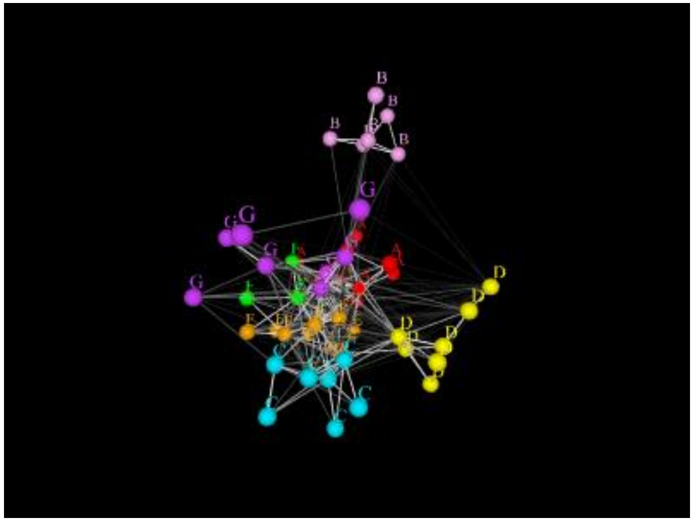
SAURON_ physical security

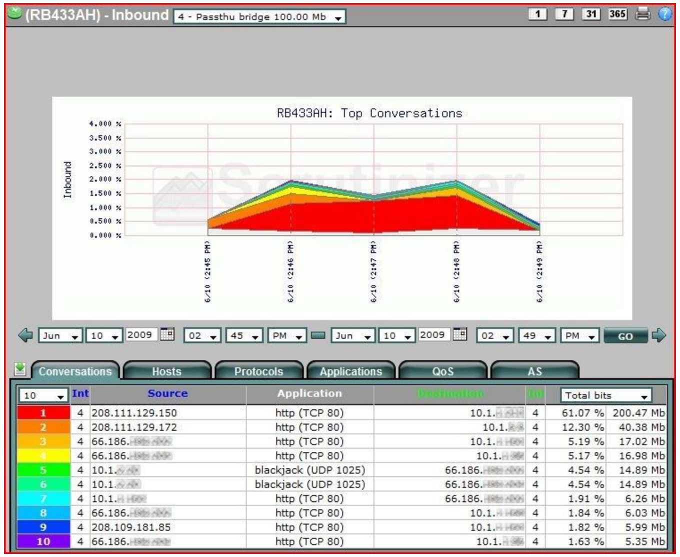
PHYSICAL SA



PUENTE DEL ANGEL CUSTODIO dirección PERIS Y VALERO

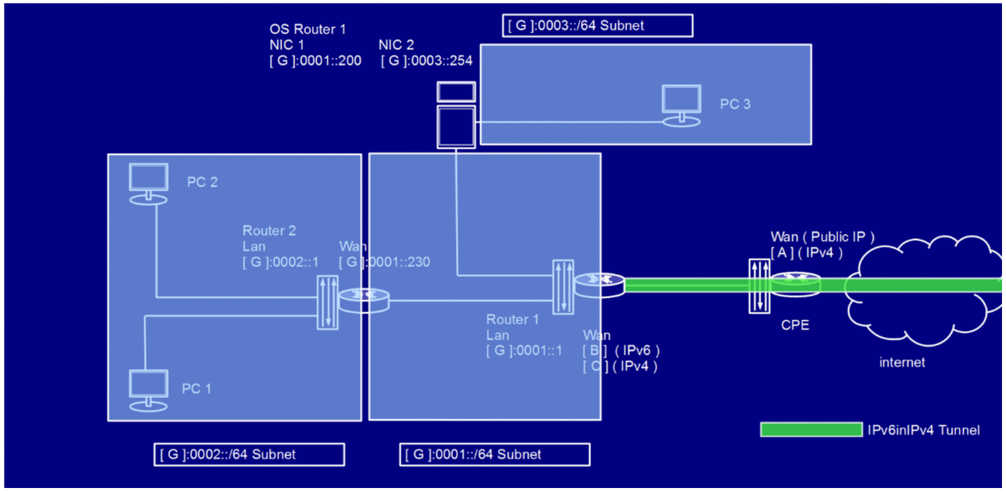
CYBER SA

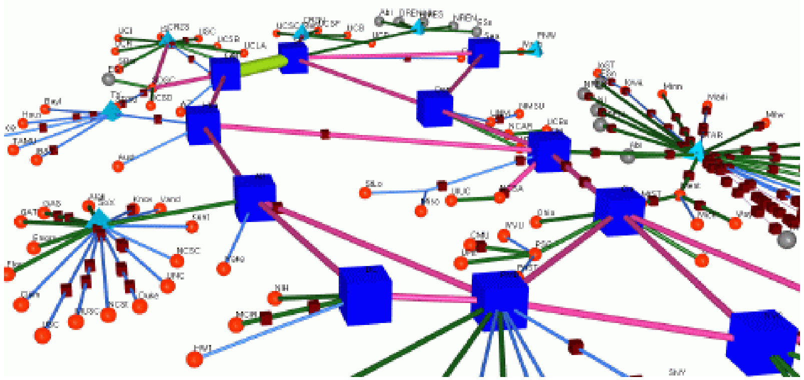




10	Int	Source	Application	Destination	Int	Total bits	
1	4	208.111.129.150	http (TCP 80)	10.1.[redacted]	4	61.07 %	200.47 Mb
2	4	208.111.129.172	http (TCP 80)	10.1.[redacted]	4	12.30 %	40.38 Mb
3	4	66.186.[redacted]	http (TCP 80)	10.1.[redacted]	4	5.19 %	17.02 Mb
4	4	66.186.[redacted]	http (TCP 80)	10.1.[redacted]	4	5.17 %	16.98 Mb
5	4	10.1.[redacted]	blackjack (UDP 1025)	66.186.[redacted]	4	4.54 %	14.89 Mb
6	4	10.1.[redacted]	blackjack (UDP 1025)	66.186.[redacted]	4	4.54 %	14.89 Mb
7	4	10.1.[redacted]	http (TCP 80)	66.186.[redacted]	4	1.91 %	6.26 Mb
8	4	66.186.[redacted]	http (TCP 80)	10.1.[redacted]	4	1.84 %	6.03 Mb
9	4	208.109.181.85	http (TCP 80)	10.1.[redacted]	4	1.82 %	5.99 Mb
10	4	66.186.[redacted]	http (TCP 80)	10.1.[redacted]	4	1.63 %	5.35 Mb

The individual detectors include traditional, well established threat detection measures, such as Intrusion Detection Systems (IDS), but also more innovative modules, such as Anomaly Detection (AD), aimed at detecting more complex and targeted attacks, such as Advanced Persistent Threats (APTs).

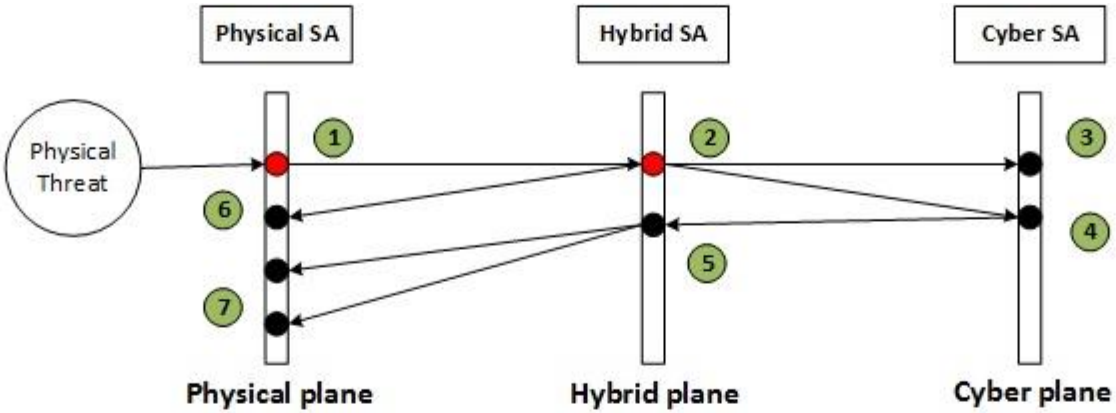




SAURON_ innovative solution

The Hybrid SA application goes one step beyond to the integration of the PSA and CSA applications. This innovative solution takes into account the real detected alarms of both applications and identifies and evaluates inter-correlations among different potential threats

HYBRID SA



1 Detected Physical threat visuaized in the Physical SA application

2 Detected Physical threat visualized in the Hybrid SA application

3 Potencial threat in the cyber plane as consequence of the initial detected threat without consequences in the physical plane

4 Potencial threat in the cyber plane as consequence of the initial detected threat with consequences in the physical plane

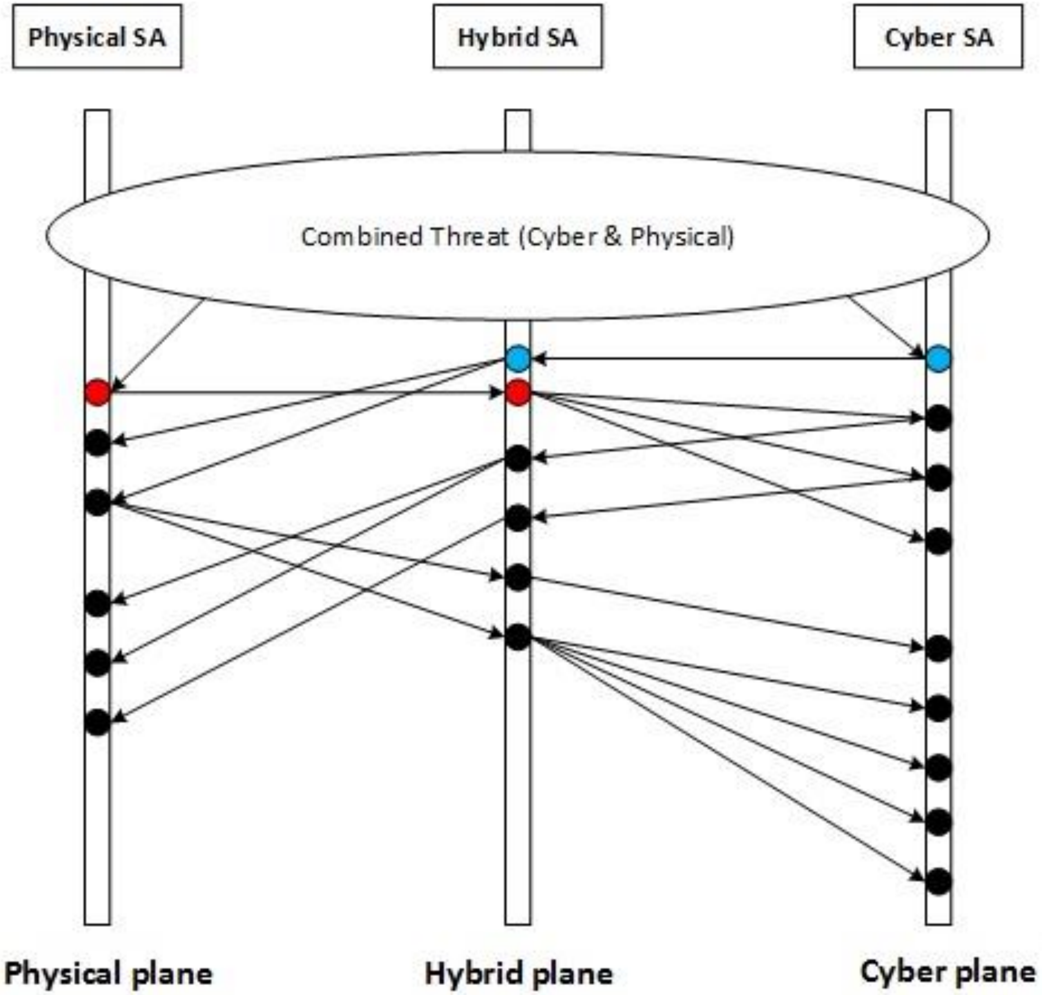
5 Potencial threat in the cyber plane as consequence of the initial detected threat with consequences in the physical plane visualized in the Hybrid SA application

6 Potencial threats in the physical plane as direct consequence of the initial detected threat in the physical plane

7 Potencial threats in the physical plane as consequence of the potential cyber threat visualized in the physical SA application

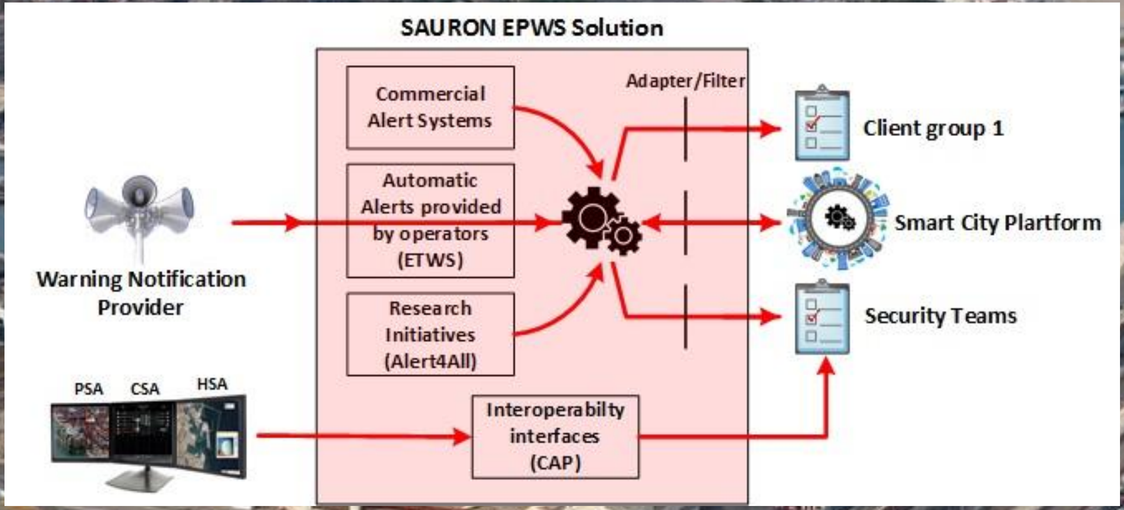
SAURON_ innovative solution

HYBRID SA



SAURON_ emergency population warning system

Emergency Population Alert System (EPAS)



SAURON EPWS Solution

Commercial Alert Systems

Automatic Alerts provided by operators (ETWS)

Research Initiatives (Alert4All)

Adapter/Filter

Interoperabilty interfaces (CAP)

Warning Notification Provider

PSA

CSA

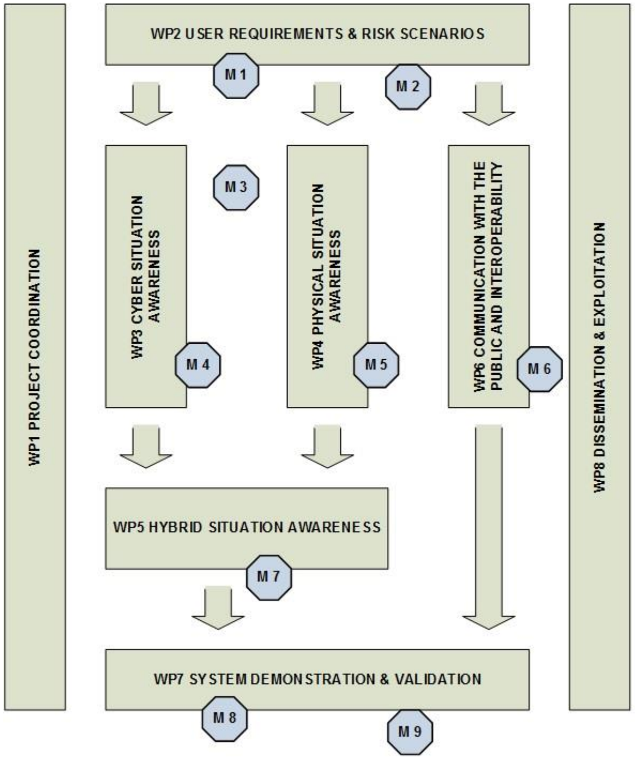
HSA

Client group 1

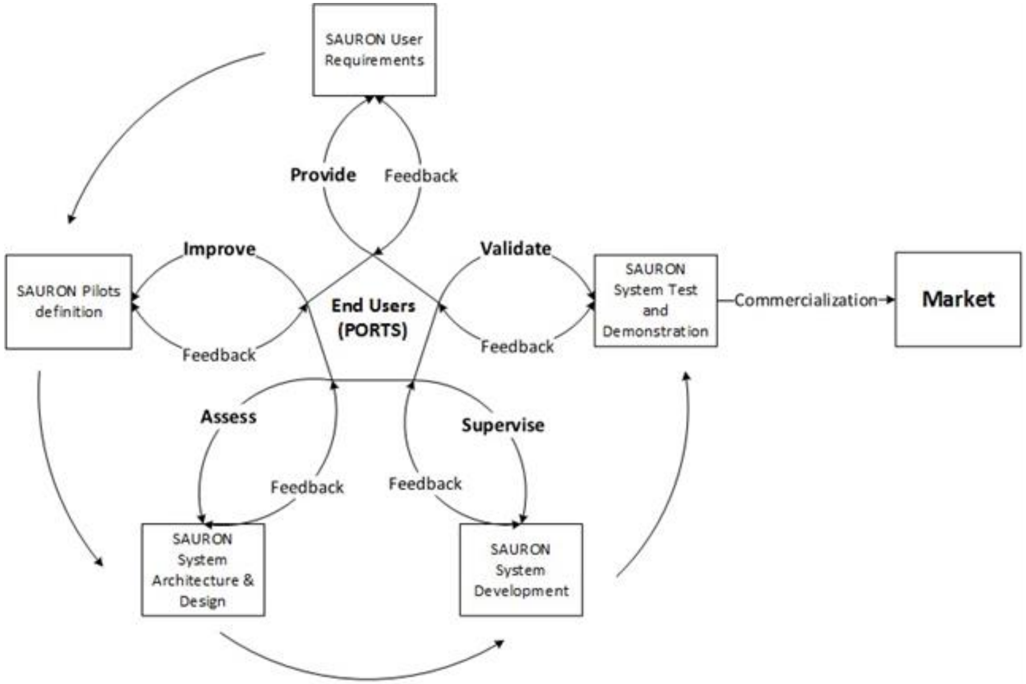
Smart City Plartform

Security Teams

SAURON_activities


WP1 PROJECT COORDINATION
WP2 USER REQUIREMENTS & RISK SCENARIOS
M 1
M 2
M 3
WP3 CYBER SITUATION AWARENESS
M 4
WP4 PHYSICAL SITUATION AWARENESS
M 5
WP6 COMMUNICATION WITH THE PUBLIC AND INTEROPERABILITY
M 6
WP8 DISSEMINATION & EXPLOITATION
WP5 HYBRID SITUATION AWARENESS
M 7
WP7 SYSTEM DEMONSTRATION & VALIDATION
M 8
M 9

M 1	User requirements gathered
M 2	System architecture released
M 3	Physical & Cyber vulnerabilities analysis done
M 4	CSA application ready for testing
M 5	PSA application ready for testing
M 6	SAURON EPWS ready
M 7	HSA application ready
M 8	First project pilot done
M 9	Second project pilot done



SAURON_ scenario definition

- *Dangerous substances are regularly transported by sea including explosives, chemicals, nuclear materials, and also agricultural fertilizers*
- *Vessels that could potentially be used to cause significant damage to ports and surrounding areas include: oil, gas, LPG and LNG tankers, chemical tankers, nuclear waste transport vessels*
- *There has been growing concern about terrorists transporting weapons of mass destruction by sea – threat of chemical, biological or radioactive dirty bombs*
- *Greatest risk may be container ships carrying radiological or nuclear materials, illegal substances/goods and weapons material.*

SAURON_ pilot / scenario

Case of Port of Valencia (Spain)

“A terrorist group plans a cyber-attack against the IT systems of the port”

*They want to access the TOS (Terminal Operating System) where are stored all **container** movements and their position and the PCS (Port Community System) where there are all the communications between the port and their stakeholders, in order to change/hide the ID of a specific container to ensure that is hidden within the port and not subject to inspection. This container contains a small nuclear/dirty bomb (or radiological substance hidden), which would be detonated/spread by some members of the group that could access the cargo area, potentially remotely for activating the bomb and which would affect the whole port facilities and a large part of the city*

SAURON_ pilot / scenario

Case of Port of Piraeus (Greece)

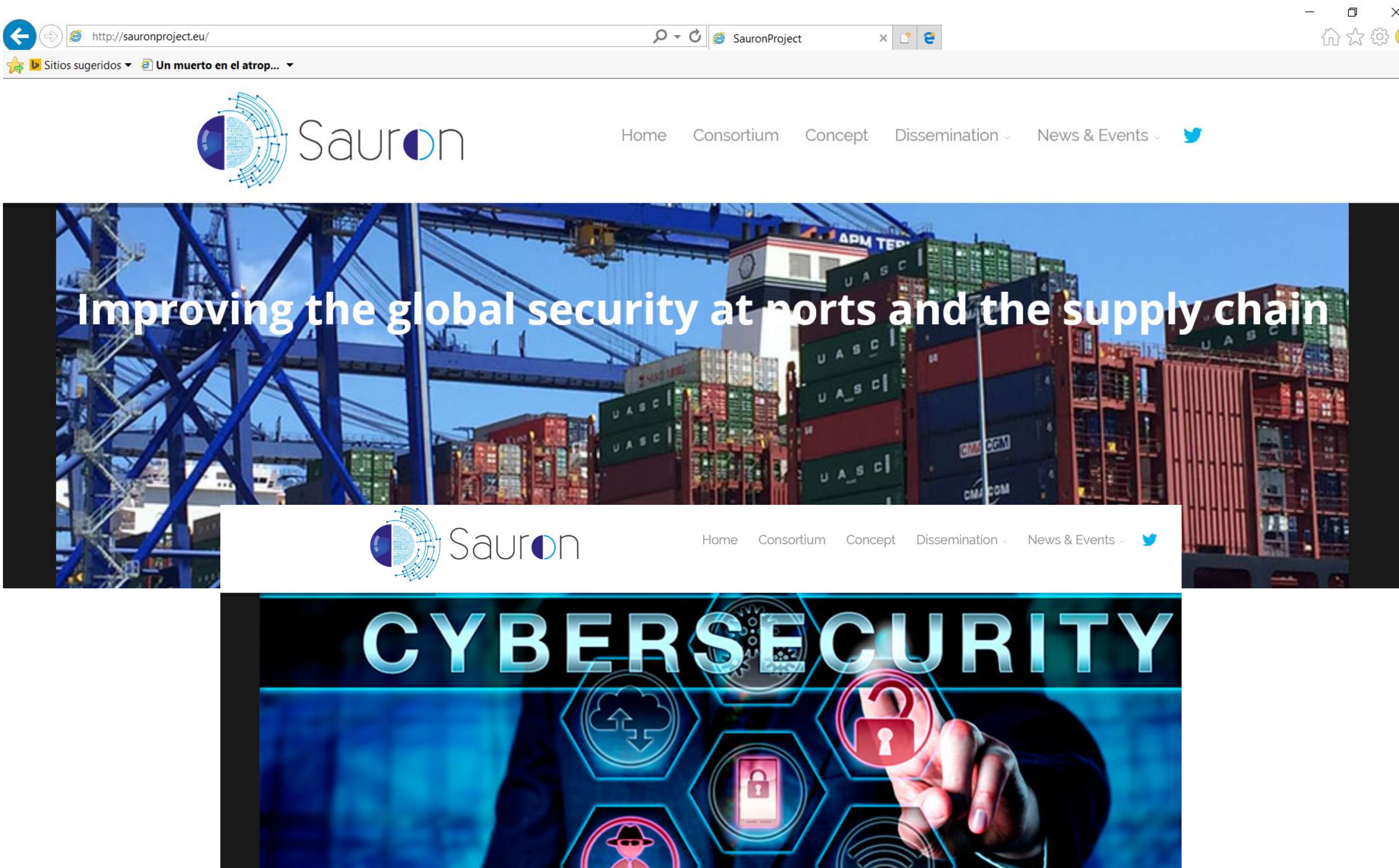
“Terrorists attack a large Cruise Ship with passengers aboard,

berthed at Port”

*A cyber-attack is planned for creating a limited disruption inside the port facilities (false perimeter intrusions, false fire alarms, surveillance system shut down, trucks traffic jam, etc.) with the purpose that the majority of the security personnel will be occupied in addressing these false problems. As a consequence normal activity and transport inside the port will be disrupted. In this situation a small heavy armed terrorist command would attack a large **cruise** ship docked in the port containing a large number of tourists. As a result of this hundreds of people could be killed before the authorities could arrive. As soon as SAURON platform was ready it will be installed in the pilots premises and tested along with the real port systems and port security personnel in order to adapt it to the different environments of the two pilots. Once the tests are finished the above described scenarios will be recreated through physical and cyber threats simulations during the two foreseen project demo days and SAURON platform will be used for facing them trying to detect and avoid the attacks or minimizing its consequences if finally they happen.*

The Port of Piraeus is a major destination for cruise ships in the Mediterranean.

SAURON_ web site



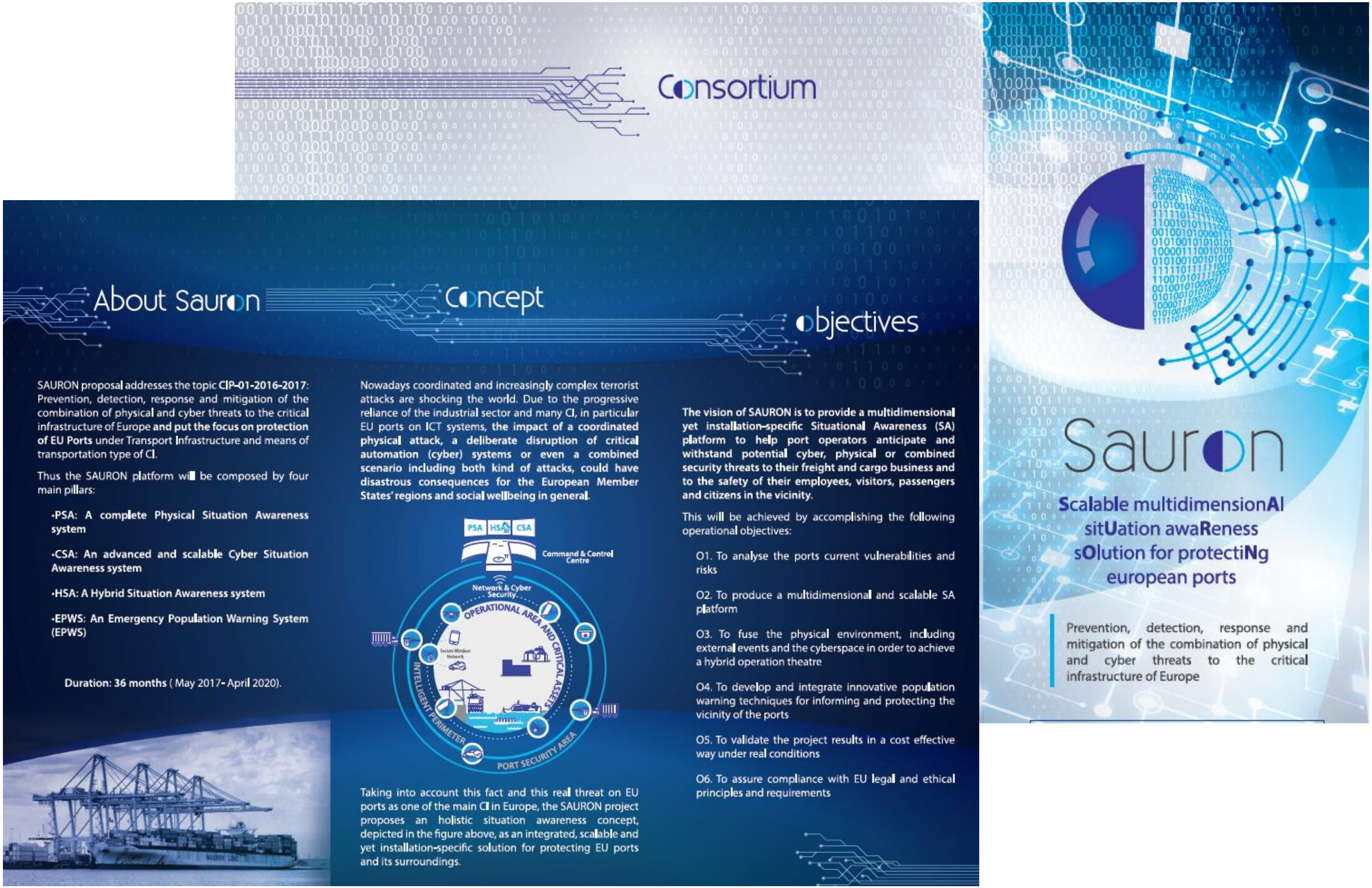
http://sauronproject.eu/

Improving the global security at ports and the supply chain

FUNDACIÓN valenciaport

SAURON_ brochure

Sauron



Consortium

About Sauron

SAURON proposal addresses the topic **CIP-01-2016-2017**: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe **and put the focus on protection of EU Ports** under Transport Infrastructure and means of transportation type of CI.

Thus the SAURON platform will be composed by four main pillars:

- **·PSA: A complete Physical Situation Awareness system**
- **·CSA: An advanced and scalable Cyber Situation Awareness system**
- **·HSA: A Hybrid Situation Awareness system**
- **·EPWS: An Emergency Population Warning System (EPWS)**

Duration: 36 months (May 2017- April 2020).

Concept

Nowadays coordinated and increasingly complex terrorist attacks are shocking the world. Due to the progressive reliance of the industrial sector and many CI, in particular EU ports on ICT systems, **the impact of a coordinated physical attack, a deliberate disruption of critical automation (cyber) systems or even a combined scenario including both kind of attacks, could have disastrous consequences for the European Member States' regions and social wellbeing in general.**

Taking into account this fact and this real threat on EU ports as one of the main CI in Europe, the SAURON project proposes an holistic situation awareness concept, depicted in the figure above, as an integrated, scalable and yet installation-specific solution for protecting EU ports and its surroundings.

objectives

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

This will be achieved by accomplishing the following operational objectives:

O1. To analyse the ports current vulnerabilities and risks

O2. To produce a multidimensional and scalable SA platform

O3. To fuse the physical environment, including external events and the cyberspace in order to achieve a hybrid operation theatre

O4. To develop and integrate innovative population warning techniques for informing and protecting the vicinity of the ports

O5. To validate the project results in a cost effective way under real conditions

O6. To assure compliance with EU legal and ethical principles and requirements

Sauron

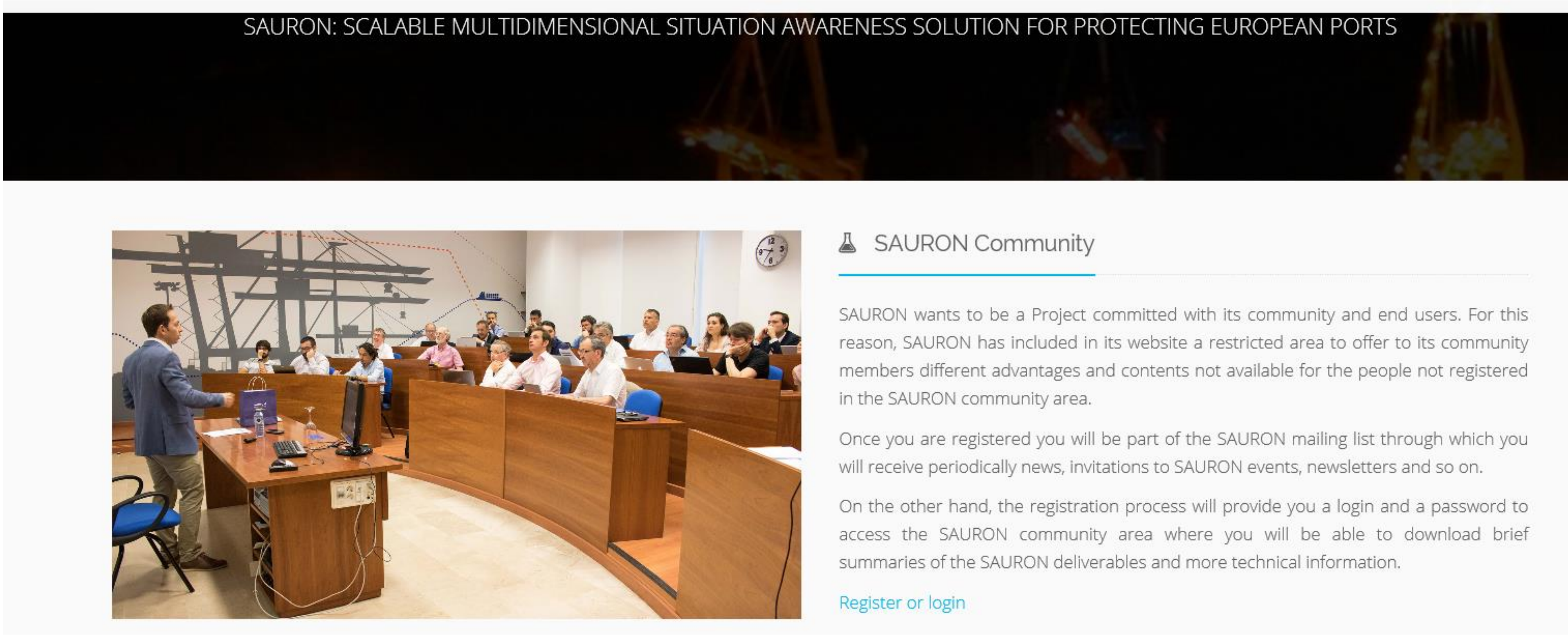
Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports

Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

SAURON_ community

Rafael Company
SAURONproject coordinator
rcompany@fundacion.valenciaport.com

Thanks for your attention!!



SAURON: SCALABLE MULTIDIMENSIONAL SITUATION AWARENESS SOLUTION FOR PROTECTING EUROPEAN PORTS

SAURON Community

SAURON wants to be a Project committed with its community and end users. For this reason, SAURON has included in its website a restricted area to offer to its community members different advantages and contents not available for the people not registered in the SAURON community area.

Once you are registered you will be part of the SAURON mailing list through which you will receive periodically news, invitations to SAURON events, newsletters and so on.

On the other hand, the registration process will provide you a login and a password to access the SAURON community area where you will be able to download brief summaries of the SAURON deliverables and more technical information.

Register or login