Newsletter January 2018

Welcome to the first SAURON project newsletter. SAURON was funded in the H2020 SEC-2016 call under 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. This first newsletter presents to the general public the concept and the main objectives of the project and shares with the reader in the next sections, the project pilots description and projects achievements till end of January 2018. These main achievements got by the project are the following: the complete set of user requirements for SAURON system and the overall system architecture. In addition, will be commented the next achievements foreseen for 2018.

SAURON APPROACH

THE PROBLEM

In the European Union (EU) **ports play a vital role facilitating the 90% of EU's external trade and 43% of all the internal market exchanges.** Industries and services belonging to the maritime sector directly contribute between 3% and 5% of EU Gross Domestic Product (GDP) and maritime regions produce more than 40% of Europe's GDP.

In addition, according to Eurostat[1] figures, the maritime sector is critical for European society. Recent statistics show that within Europe, 52% of the goods traffic in 2013 was carried by maritime transport, an increase of 7% from one decade ago. **This continuous increase in dependency upon maritime transport underlines its vital importance to our society and economy.** The total gross weight of goods handled in EU ports is estimated at close to 3.8 billion tons in 2014, an increase of 2 % from 2013. According to the latest figures, this represents a trend that continued throughout 2015. The 20 largest EU ports accounted for about 38 % of the total tonnage of goods handled in the countries reporting data in 2014. In addition, the number of passengers passing through EU ports increased 0.6 % between 2013 and 2014, to 402 million.

For a better understanding of the impact on the above of a terrorist attack, we can take the example of 9/11 attacks in New York; even if the attackws were not seaport-specific, they did have a direct impact on U.S. seaports, which were closed for one week following the attacks. As a result, **container shipping industry lost a billion dollars a day for months[2].** After 9/11 a Port Security War Game simulation involving senior U.S. administration and industry representatives was conducted . This simulation included cyber, physical and combined attacks to selected seaports, and focused on the impact of such attacks on U.S. supply chain. The results achieved included losses of more than 55 billion dollars and a backlog of 60.000 containers.

Ports are organisationally complex components of Critical Infrastructure (CI) involved in the reliable movement of goods and the safe transport of people. 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. An attack on a big EU port (cyber, physical or a combination) could damage the CI and seriously impact its vicinity. 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.

This would have severe economic consequences for the interconnected and interdependent EU countries and countries outside Europe, covering multiple sectors. EU ports have an acceptable level of physical security and undertake reviews and exercise regularly, but most are not capable of anticipating and withstanding a complex cyber-attack or a combined cyber-physical attack.

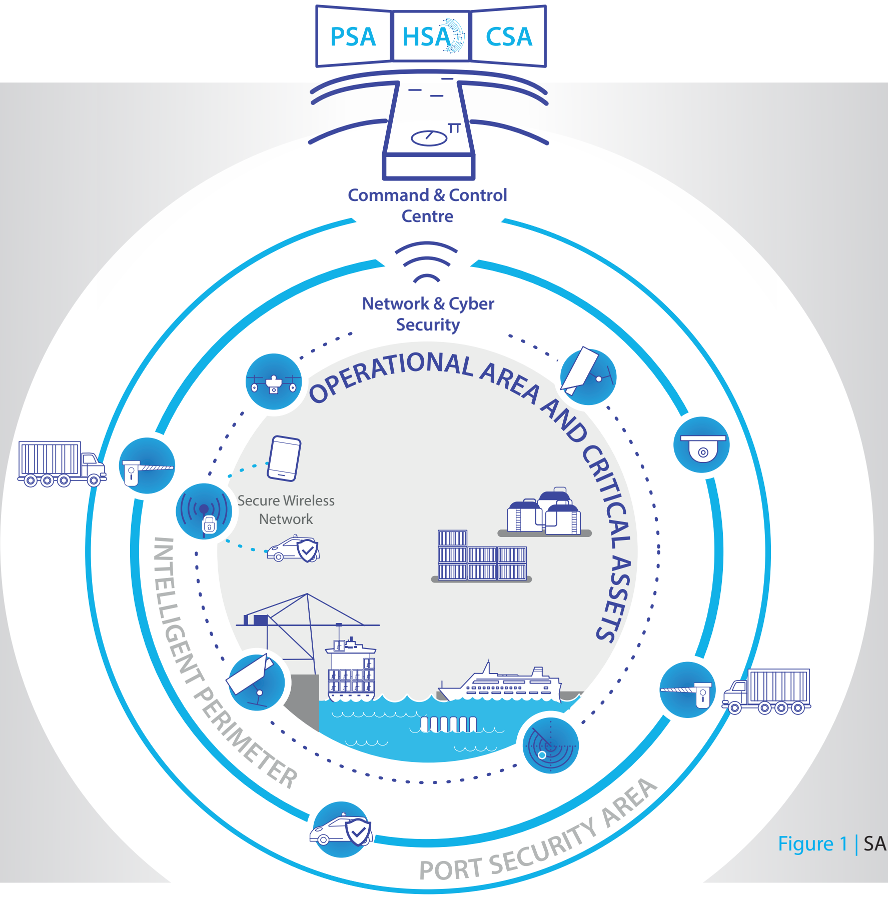

Figure 1 | SAURON Concept

THE CONCEPT

SAURON project proposes a holistic situation awareness concept as an integrated, scalable and yet installation-specific solution for protecting EU ports and its surroundings.

This solution **combines the more advanced physical SA features with the newest techniques in prevention, detection and mitigation of cyber-threats**, including the understanding of synthetic cyber space through the use of new visualization techniques (immersive interfaces, cyber 3D models and so on).
In addition, **a Hybrid Situation Awareness (HSA) application capable of determining the potential consequences of any threat will show the potential cascading effect of a detected threat in the two different domains (physical and cyber).**
During an incident SAURON will provide information that can be used to protect the general public in the vicinity and specific rescue/security teams of any potential situation that could put in risk their integrity.

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

- **PSA: A complete physical SA (PSA)** system which includes novel features such as; dynamic location of resources and assets, location, management and monitoring of sensors, including cameras mounted on drones (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 (CSA)** framework capable of preventing and detecting threats and in case of a declared attack, capable of mitigating the effects of the infection/intrusion. This CSA system will include new visualization paradigms for the cyber space.

- **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 (EPWS)**, allowing local, regional, or national authorities to contact members of rescue/security teams and the public (also integrating Smart City Platforms (SCP)) in order to warn them and draw their attention to an immediate hazard. This will encourage them to take a specific action in response to an emergency event or threat.

These three SA approaches (Physical, Cyber and Hybrid) along with the EPWS will ensure the protection and resilience of the ports and their surroundings against any kind of threats or declared attacks (Physical, Cyber or a combination of both).

SAURON 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: To achieve this SAURON will use the results of previous dedicated projects (e.g. CYSM, MEDUSA, MITIGATE) which analysed the EU ports real physical and cyber vulnerabilities and risks in order to assess and adapt their results to the ports current protection systems

O2. To produce a multidimensional and scalable SA platform: To develop (to TRL7) and test a multidimensional and scalable SA platform easily deployable for EU ports comprising a Physical Situation Awareness (PSA) application, a Cyber Situation Awareness (CSA) application and a Hybrid Situation Awareness (HSA) application in order to prevent, detect, respond and mitigate any physical, cyber or combined threat.

O3. To fuse the physical environment, including external events and the cyberspace in order to achieve a hybrid operation theatre capable of detecting potential cascading effects for helping the decision makers to prevent, understand and face any kind of potential threat.

O4. To develop and integrate innovative population warning techniques for informing and protecting both, the inhabitants in the vicinity of the ports and the emergency teams in charge of intervening in case of attack

O5. To validate the project results in a cost effective way under real conditions through 2 pilot demonstrations in real EU ports (Valencia Port and Piraeus Port).

O6. To assure compliance with legal and ethical principles and requirements, identify lacunae and hurdles and develop concrete recommendations to policy makers and pertinent stakeholders with the aim to ameliorate the current level of protection in the EU ports.

SAURON ACHIEVEMENTS

SAURON PILOTS

In order to cover the wider range of potential end users as possible in its pilot demonstrations, SAURON project will test and demonstrate its results under real conditions in two of the more representative EU ports (considered as CI) in their countries and that encompass the main seaports categories in terms economic impact and people protection

These two pilots are complementary, since in both the whole SAURON potential will be demonstrated, but in the first pilot SAURON system will be used mainly for protecting the cargo area of the ports and in the second pilot it will be used for protecting the passengers' area.

- **Valencia Port pilot scenario description:**

A terrorist group plans a cyber-attack against the IT systems of the port. They want to access the Terminal Operating System (TOS), storing all container movements and their positions, and the Port Community System (PCS), which contains all the communications between the port and their stakeholders. Their goal is to change/hide the ID of a specific container to ensure that it 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 to the cargo area, potentially remotely for activating the bomb and which would affect the whole port facilities and a large part of the city.

- **Piraeus Port pilot scenario description:**

A cyber-attack is planned for creating a limited disruption inside the port facilities, i.e., due to false perimeter intrusions, false fire alarms, the shutdown of surveillance systems, trucks traffic jam, etc. The main purpose of this cyber-attack is to keep the majority of the security personnel 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, hundreds of people could be killed before the authorities could arrive.

As soon as SAURON platform is 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 aforementioned scenarios will be recreated through physical and cyber threats simulations during the two foreseen project demo days and SAURON platform will be used to face them, trying to detect and avoid the attacks, or to minimize its consequences if finally could not be stopped.

SAURON USER REQUIREMENTS GATHERING PROCESS

The SAURON user requirements gathering process was divided into several steps. The first one was defining the pilot scenarios for SAURON. This task was performed by the consortium members with extensive end-user involvement and refined in an iterative process through e-mail and teleconferences. These scenarios have been described in the previous section of this newsletter.

In parallel, based on the preliminary scenarios defined and the expertise of the consortium members, a draft questionnaire for gathering user requirements was proposed and refined by the whole consortium. In addition, bilateral interviews with internal and external end users were performed using a structured approach. The questionnaire refinement and interview design tasks were also performed by all the consortium members (including end-users) in an iterative process through e-mail and teleconferences. The result of this task was the final version of the questionnaire agreed by the whole consortium and questions and guidance for use in the bilateral interviews.

Once the final version of the questionnaire was approved by the consortium, the document was sent to a large number of SAURON end-users in order to obtain a wide range of opinions and feedback from the external end-users. Finally, 15 completed questionnaires were received along with the responses from end users during the bilateral meetings. Finally, the results of the questionnaires and the responses from the bilateral meetings were processed by the consortium and the final set of SAURON user requirements was produced which will be the basis for the SAURON system design and development phases.

SAURON ARCHITECTURE

The system architecture proposed by the consortium for developing these applications in order to form a holistic port protection solution is as follows: the proposed SAURON architecture will guide all partners during their implementation efforts by constituting a basis for software systems' behaviours, and provide design decisions that affect the SAURON platform's development, deployment and maintenance life. It is a translation of the user requirements into a description of the software structure, software components, interfaces, and data necessary for the implementation phase. In essence, the proposed architecture becomes a detailed blueprint for the implementation activity.

The architecture describes in detail which user requirements are associated with each of the SAURON system components in order to ensure that each development team is aware of which user requirements have to be accomplished in their software modules. Moreover, the different entities/classes that model each part of the SAURON components have also been described in this deliverable.

These entities/classes will be the main basis for the next development phase. Following the architecture design process, once the entities/classes have been modelled each of the methods or logic interfaces that comprise the different classes of each SAURON component have been described in order to cover all component functionalities. Finally, the internal information flow of each SAURON component has been stated in order to give a clear idea to the developers of how the system has been designed for further implementation.

The SAURON system comprises the full integration of the four components mentioned above (i.e., PSA; CSA; HSA and EPWS), which will produce a synergy driving SAURON beyond the current port security paradigm. The results of the project will prepare the new generation of ports security systems to face more sophisticated physical and cyber-attacks including combined ones. The overall SAURON system architecture is described in Figure 2.

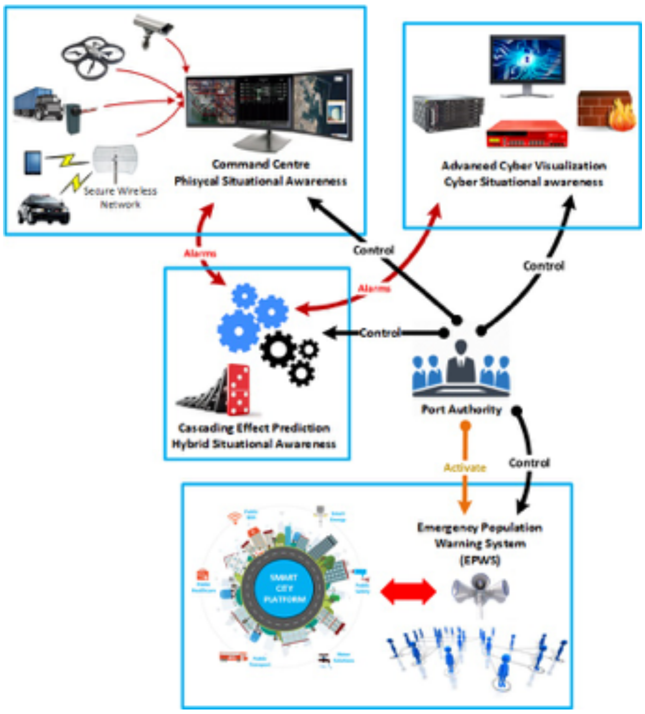

Figure 2 |SAURON Architecture description

NEXT ACHIEVEMENTS

During 2018 it is foreseen to finish the development and the integration of the four applications that comprises SAURON system. In addition, the first test in lab of the whole system will also start at the end of 2018.