Final Newsletter

September 2020

Welcome to the final 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 final newsletter presents to the general public the latest results of the project which include the final architecture of the system, a description of the project pilots (drone pilot, Piraeus pilot and Valencia pilot) and finally some remarks on next steps for implementing SAURON in European ports.

SAURON FINAL ARCHITECTURE

Innovation for improving current ports' cyber security is one of the main objectives of SAURON project and therefore several developments have been performed for this purpose.

One of the main developments has been the definition of a comprehensive architecture that encompasses the physical domain, the cyber domain and the hybrid domain, allowing for the interaction and information exchange of all three domains, providing a unique and integrated perspective to first responders.

The defined architecture is as follows:

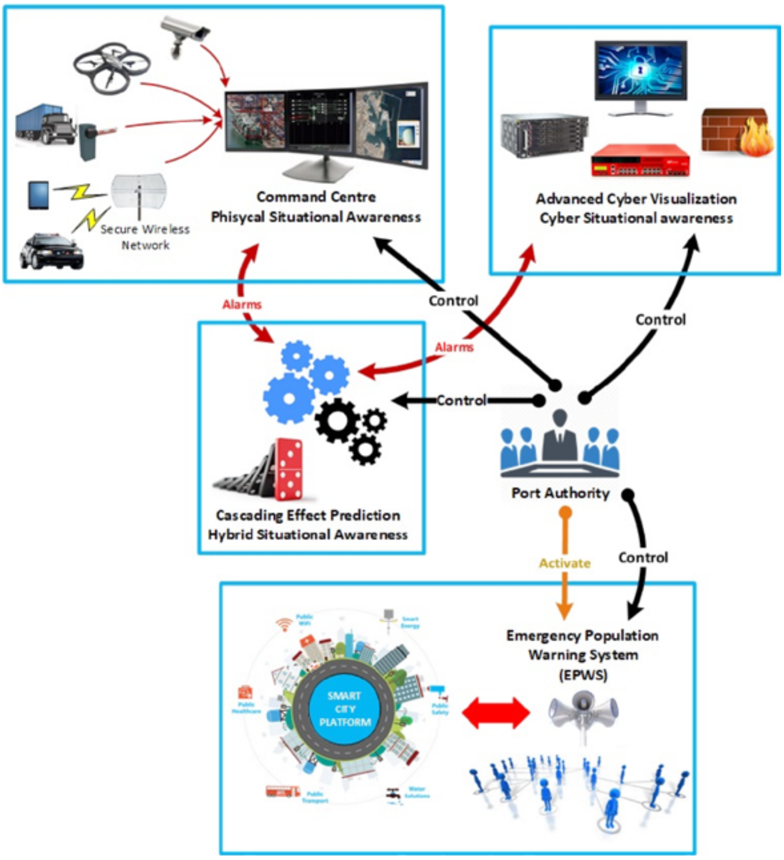
Secure Wireless Network
Command Centre
Phisycal Situational Awareness
Advanced Cyber Visualization
Cyber Situational awareness
Alarms
Control
Alarms
Control
Control
Cascading Effect Prediction
Hybrid Situational Awareness
Port Authority
Activate
Control
Emergency Population Warning System (EPWS)
SMART CITY PLATFORM

Figure 1| SAURON final architecture

As can be seen in figure 1, there are four main pillars in the overall SAURON system: (i) the Physical Situational Awareness tool (PSA), (ii) the Cyber Situational Awareness tool (CSA), (iii) the Hybrid Situational Awareness tool (HSA) and (iv) the Emergency Population Warning System (EPWS).

These four components produce information to provide situational awareness to their corresponding officials, while also exchanging information to synchronize their views to, most importantly, generate hybrid situational awareness which is the most significant contribution of the SAURON project.

With all this information, port authorities can coordinate particular domain operators and actors (e.g. port police), take proper decisions to mitigate attacks, and activate and control warnings to City council populations.

This architecture and corresponding tools have been tested in the three pilots performed in the SAURON project: November 2019 Sagunto Port ROCSAFE-SAURON combined demo, February 2020 Piraeus Port pilot and July 2020 Valencia Port pilot (despite being partially remote due to the COVID-19 crisis).

PILOT DEMONSTRATIONS

During the whole of the SAURON project the partners have designed and developed various Security Awareness Tools as discussed above, which can help the security operators in their decision making. After the laboratory testing it is important to test the components deployed in real infrastructures. This is a significant process to evaluate the results of the project and to get feedback from the and users with their impressions.

Sauron partners' have developed three different pilots, where the functionalities of the four Sauron components have been tested. The first one in the port of Sagunto tested some of the functionalities in addition to the two main pilots in Piraeus and Valencia at the end of the project.

DRONE PILOT

The drone pilot was a joint demonstration between the SAURON and ROCSAFE projects, where their main functionalities were shown. This pilot was held in Sagunto because of the legal restrictions preventing flying of drones near Valencia city.

The pilot was developed in an early stage of the project so only some capabilities were tested, including the integration of the video signal sent by surveillance drones monitoring a suspicious container going out of the port by the Physical Situational Awareness system (PSA) of the SAURON platform. Furthermore, it aimed to show how the Threat Propagation Engine (TPE) of the Hybrid Situational Awareness system (HSA) could identify any possible consequences that might occur in the overall infrastructure. SAURON also wanted to demonstrate how the alert generated by the PSA could be quickly communicated to all security forces and to the vicinity through an Emergency Population Warning System (EPWS) with the aim to prevent more serious incidents.

The Drone pilot consisted of a truck leaving the Intersagunto Container Terminal in the Port of Sagunto carrying an imported container with medical machinery, which might include radiological sources. The truck travelled through the port towards the North exit of the port. As the port authority terminal knew about the dangerous cargo, to try to avoid any possible problem with that container, the Port Security Officer decided to follow that truck during its exit route by a surveillance drone connected to the SAURON system. When problems were detected, the port police were sent to supervise the incident.

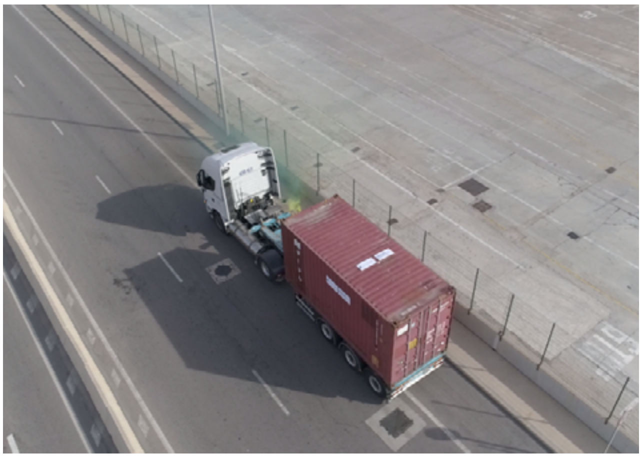

Figure 2| Truck stopped with technical problems (suspicious smoke) during the done pilot

PIRAEUS PILOT

The SAURON Piraeus pilot event was carried out in the Port of Piraeus, Greece at the Alkimos Cruise Terminal of the Piraeus Port Authority (PPA) premises. It aimed at assessing the performance of the SAURON system in a real port environment over the normal operations of the port's critical cruise service. Moreover, it validated its applicability to a large and busy EU port and its capacity to demonstrate to the port community how to get protected against physical, cyber and/or combined threats and provide safety to their employees, visitors, passengers and citizens in the vicinity.

The SAURON system was tested in the scenario of a coordinated terrorist attack which encompassed a number of hybrid threats (both cyber and physical) on the Piraeus port cruise service. Specifically, a terrorist group committed a series of cyber-attacks to breach the IT systems of the PPA infrastructure and take advantage of its components to provide a fake notification to cruise passengers, encouraging them to move to the cruise platform to embark on a cruise ship. Furthermore, they sent a misleading e-mail to the PPA personnel, which would enable a small heavily armed terrorist group to reach the cruise terminal gate with a van camouflaged as a food truck without raising any suspicion. The aim was to attack the cruise ship docked in the port, and to cause death and injuries to the large number of passengers situated in the vessel.

To run the pilot, a number of assets of the PPA cruise service infrastructure were engaged and some port physical sensors were integrated with the SAURON system to monitor the pilot activity and support the security process. During the pilot, the project's technical partners demonstrated the SAURON system components, namely the CSA, PSA and HSA and proved they can detect hybrid threats (cyber, physical or combined). The EPWS SAURON component was also demonstrated, to show how it can enable communication with the public to warn people in view of an emergency.

The PPA pilot event is available in:

https://youtu.be/J9qH1x3GmSQ .

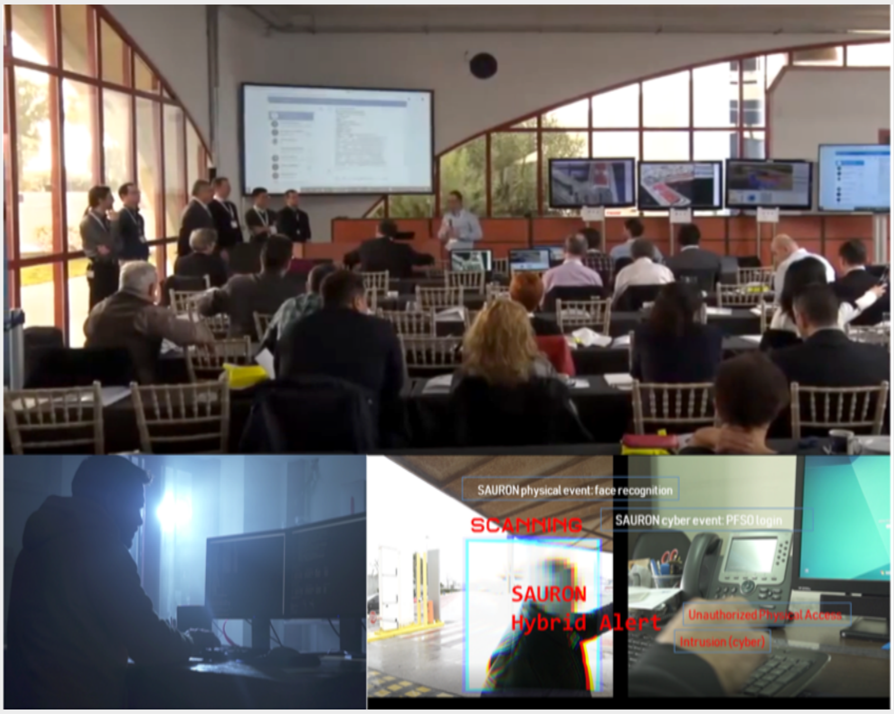
SAURON physical event: face recognition
SCANNING
SAURON cyber event: PFSO login
SAURON
Hybrid Alert
Unauthorized Physical Access
Intrusion (cyber)

Figure 3| Photos from the PPA pilot event and the terrorist attack scenario

VALENCIA PILOT

The Valencia pilot was initially planned as a physical event in the port of Valencia and in the CSP Iberian Valencia Terminal, where all stakeholders in the port community could attend and see the SAURON developments. However, due the COVID-19 situation, that was impossible and finally it was decided to run the pilot fully online, but connected with real systems and sensors. Despite this problem, the SAURON system was able to be run as planned with its different components distributed, and integrating real sensors from the terminal.

During the pilot, it was demonstrated how the SAURON platform can be used 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.

The pilot was focused on a terrorist attack in a container terminal where the attackers used a combined physical and cyber-attack to access the terminal. The attackers gained access to some systems in the terminal and they were able to relocate a container to an unguarded area and used a fire to disable the surveillance systems of the terminal perimeter. After that they could access to the terminal by jumping the fence and then activate a bomb inside that container.

An explanatory video can be found in https://www.youtube.com/watch?v=5x7F7GgFYac

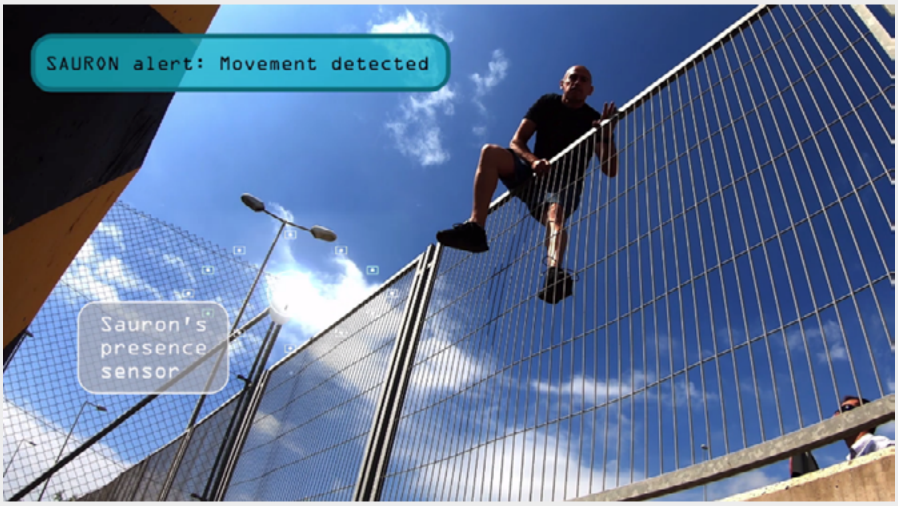

Figure 4| Terrorist jumping the fence to activate the bomb during the Valencia pilot

NEXT STEPS AND IMPLEMENTATION OF SAURON

EU Ports already use technically advanced Physical Security and Cyber Security systems and processes to resist attacks in the Physical or in the Cyber domain. However, if an incident is detected in one domain, none of the PSA and CSA systems currently available is capable of identifying potentially related events and analysing cascading effects across the domains as they concentrate their view on their particular domain. These isolated views of the cyber and physical domains also make it harder to combat hybrid attacks originating from both the physical and cyber domains, such as the attack on the port of Antwerp discovered in 2013 which combined spear phishing and malware attacks with physical entry to fit key-logging devices on to computers, to subvert several cargo tracking and release systems.

SAURON recommends (Adams et al, Journal of Transportation Security, to be published) that ports can reduce their vulnerability to cascading hybrid cyber-physical attacks by the following steps:

- Developing a cyber-physical interdependency map that is refined over time and that can be used to model cyber and physical cascading effects and design security measures;
- Developing an understanding of what normal means and incrementally developing rules defining normal/ abnormal events and activities;
- Changing security priorities and measures dynamically and using a hierarchical approach to maintain situational awareness.

It is recognised that most medium and large ports will have certain elements for detection of potential threats, such as physical sensors for fire and smoke or intrusion. **The individual tested and validated SAURON technology components (i.e. PSA, CSA, HSA, EPWS) can fill gaps and augment these existing port security capabilities. In particular, the HSA can provide a new capability to enhance ports' readiness to respond to the advancing hybrid cyber-physical threat. In addition, SAURON has developed an approach and a set of processes and protocols that ports with satisfactory physical and cyber security measures and capabilities in place can implement within their own systems in an incremental and evolutionary way.**

Continuing after the completion of the project, the partners will consider the best approach of taking the SAURON system and/or its component parts to market. This will include consideration of a number of factors, including refining the definition of the USPs, continuing competitor analysis, feedback from sales visits and formalising exploitation agreements, etc.