Sauron

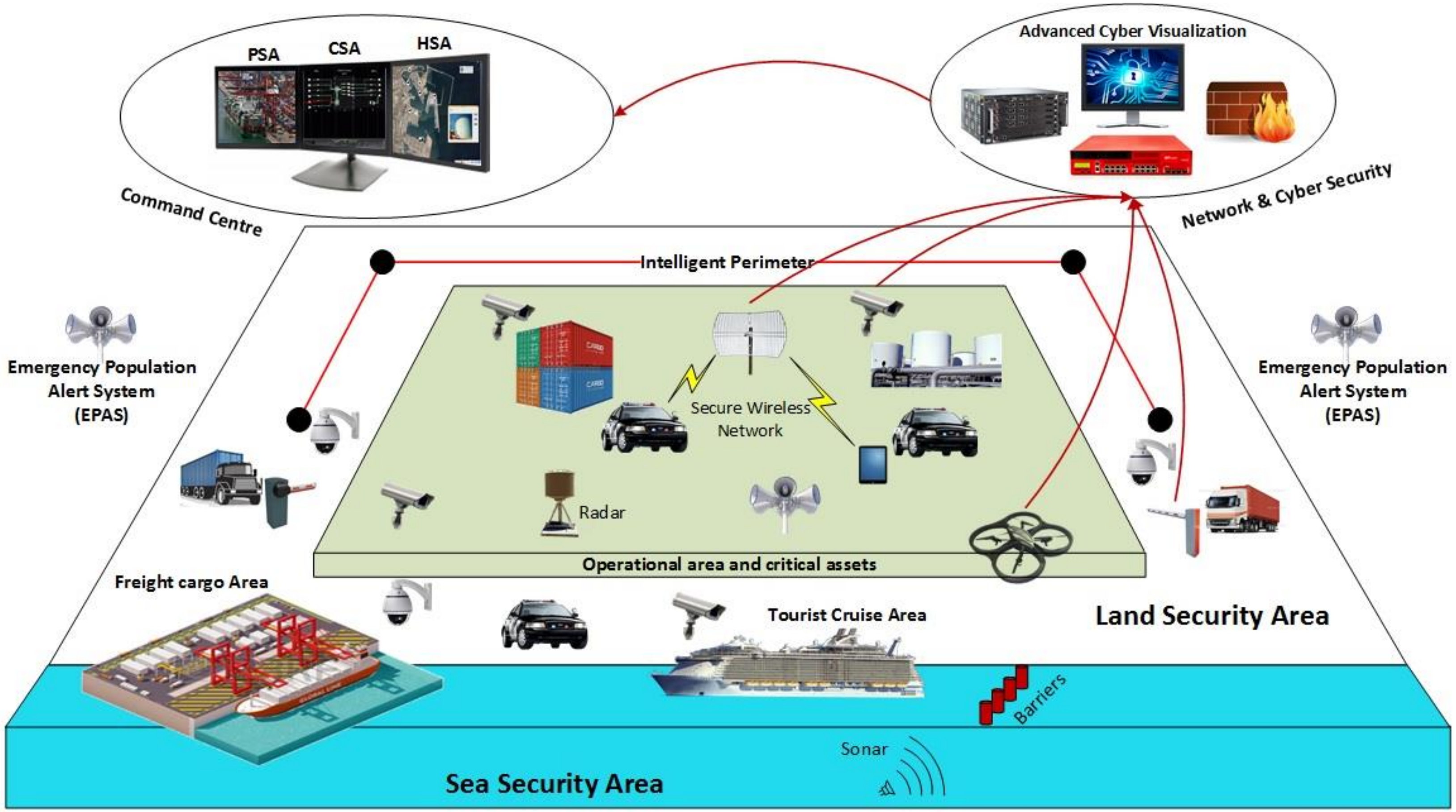
SAURON: From Physical to Hybrid Situational Awareness

Israel Perez

Universidad Politécnica de Valencia

SAURON Concept

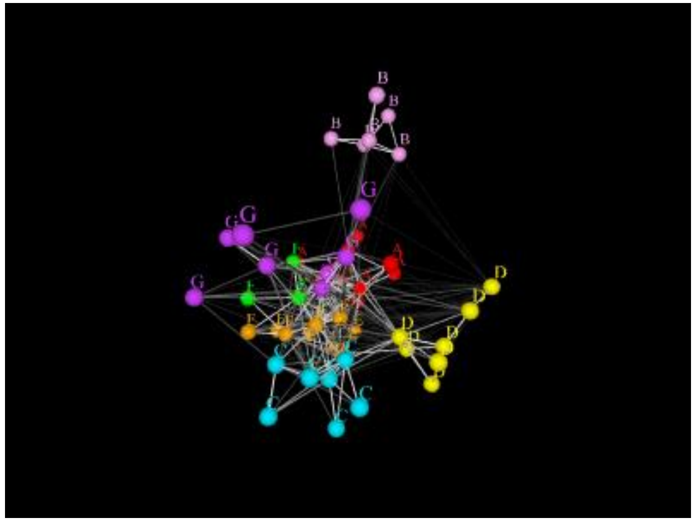
The **SAURON project proposes an holistic situation awareness concept**



SAURON Concept

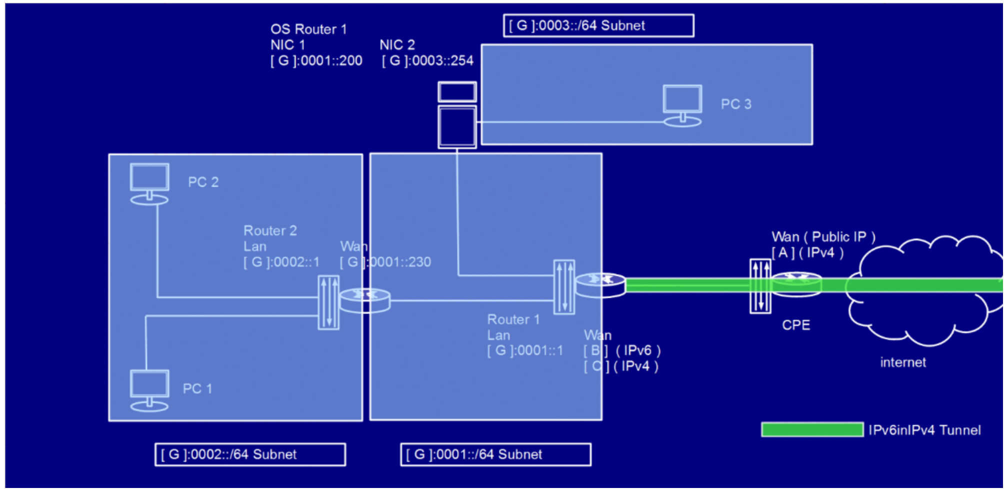
- This solution **combines the more advanced physical SA features with the newest techniques in prevention, detection and mitigation of cyber-threats**
- In addition, **a Hybrid Situation Awareness (HSA) application capable of determining the potential consequences of any threat will show the potential cascading effect of a detected threat in the two different domains (physical and cyber)**
- From the point of view of situational awareness, SAURON platform will provide three advanced features:
  - **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.
  - **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.
  - **HSA: A Hybrid SA (HSA) application receiving both physical and cyber alarms** on potential threats from the real world and the cyber space respectively. **The HSA application will show the potential consequences/effects of these threats in the other planes including cascading effects**.

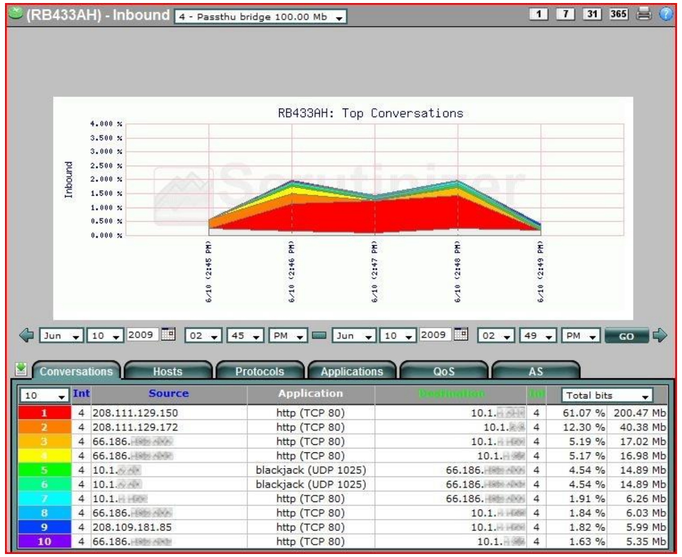
SAURON Cyber Security



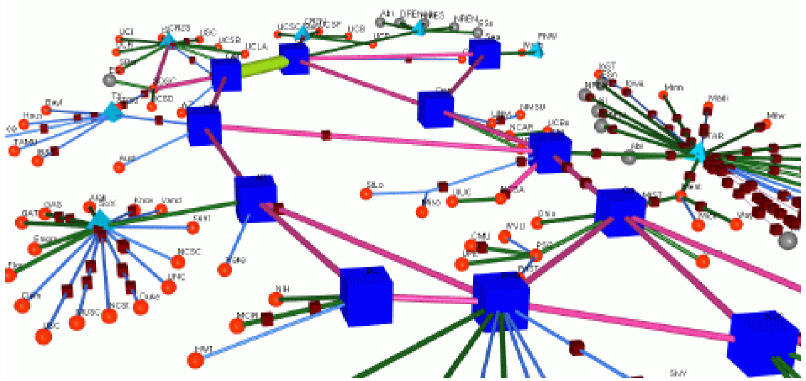
The individual detectors include traditional, well established threat detection measures, such as Intrusion Detection Systems (IDS), but also more innovative modules, such as Anomaly Detection (AD), aimed at detecting more complex and targeted attacks, such as Advanced Persistent Threats (APTs).

CYBER SA





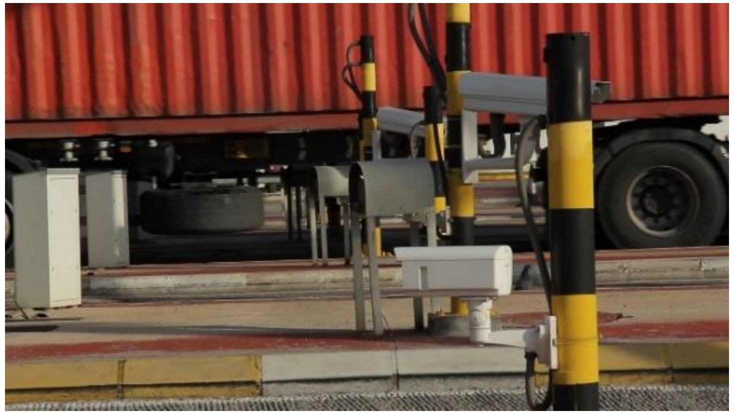
10	Int	Source	Application	Destination	Int	Total bits	
1	4	208.111.129.150	http (TCP 80)	10.1.[redacted]	4	61.07 %	200.47 Mb
2	4	208.111.129.172	http (TCP 80)	10.1.[redacted]	4	12.30 %	40.38 Mb
3	4	66.186.[redacted]	http (TCP 80)	10.1.[redacted]	4	5.19 %	17.02 Mb
4	4	66.186.[redacted]	http (TCP 80)	10.1.[redacted]	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

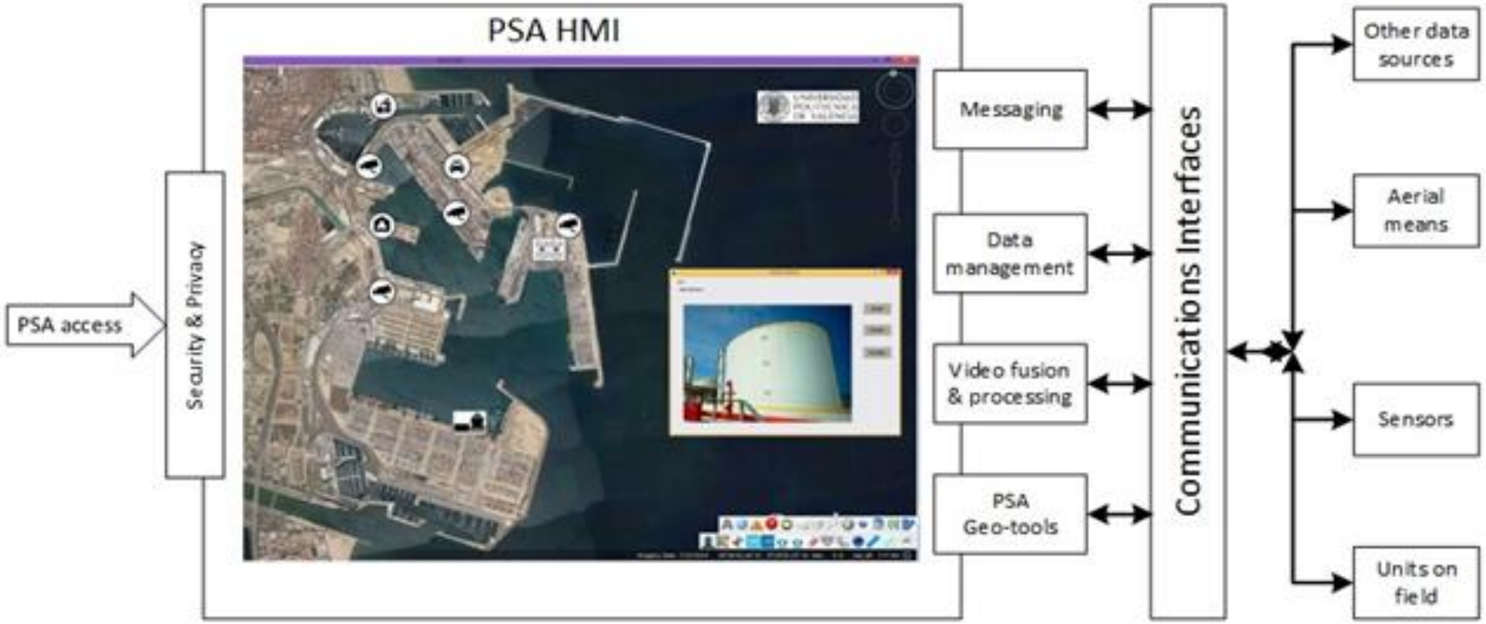


Physical Situational Awareness Application

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

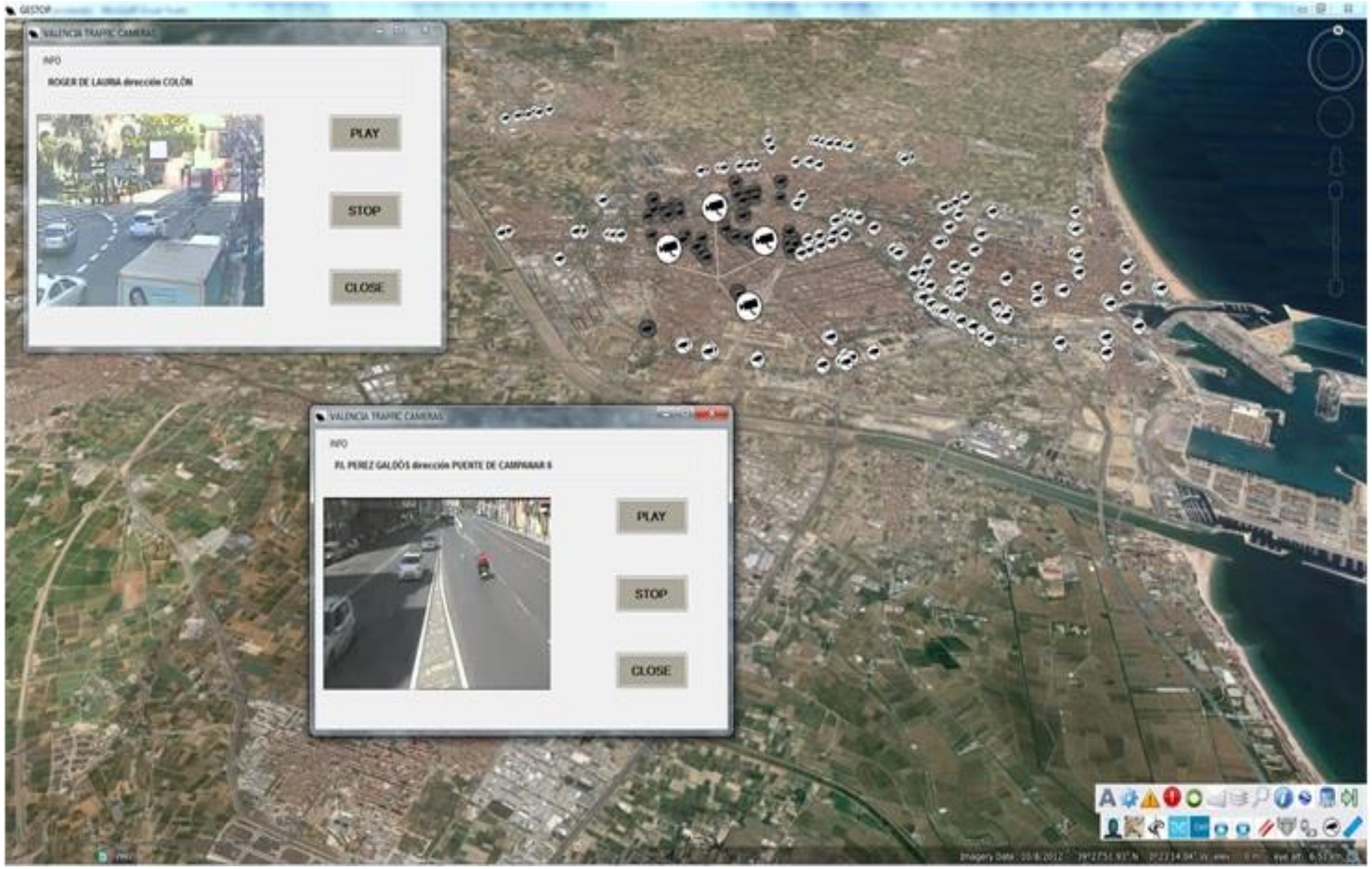




Physical Situational Awareness Application

- **The information represented in the PSA HMI is as follows:**
  - **Maps of the affected area:** The PSA is capable of managing the main Geographical Information System (GIS) standards in order to show the more appropriate map of the affected area for geo-locating the rest of the visualized information.
  - **Units on field location:** The GPS locations of the units (including vehicles) are received through the available communication interface, stored in the database and shown on the map. The refresh rate of these locations is configurable for the system administrator.
  - **Aerial means location:** The GPS locations of the aerial means, e.g., unmanned aerial vehicles (UAVs), are also received through the available communication interface.
  - **Real time video:** The units (including terrestrial vehicles or UAVs), which have a video camera mounted, transmit their video flows through the communication network. These different real time video flows are shown on the PSA HMI on demand in order to present the situation evolution to the operators in real time. Using the same display, it will be possible to access the fixed video surveillance cameras.
  - **Data from other sensors:** All data from other sensors deployed on the field that were connected to the PSA tactical network (e.g., fixed images, indoor safety detectors including smoke, fire and heat sensors, motion detection sensors, perimeter security sensors, etc.) is shown in a geo-referenced manner on the PSA HMI under the operator demand in order to see the sensors status and measurements/alarms.
  - **Available GIS layers:** Different GIS layers such as; roads, grid, 3D terrain view, 3D buildings view, borders, available water points, network firewalls locations and so on are shown on the PSA HMI on demand.

Physical Situational Awareness Application



GESTOP

VALENCIA TRAFFIC CAMERAS

INFO

ROGER DE LAURIA dirección COLÓN

VALENCIA TRAFFIC CAMERAS

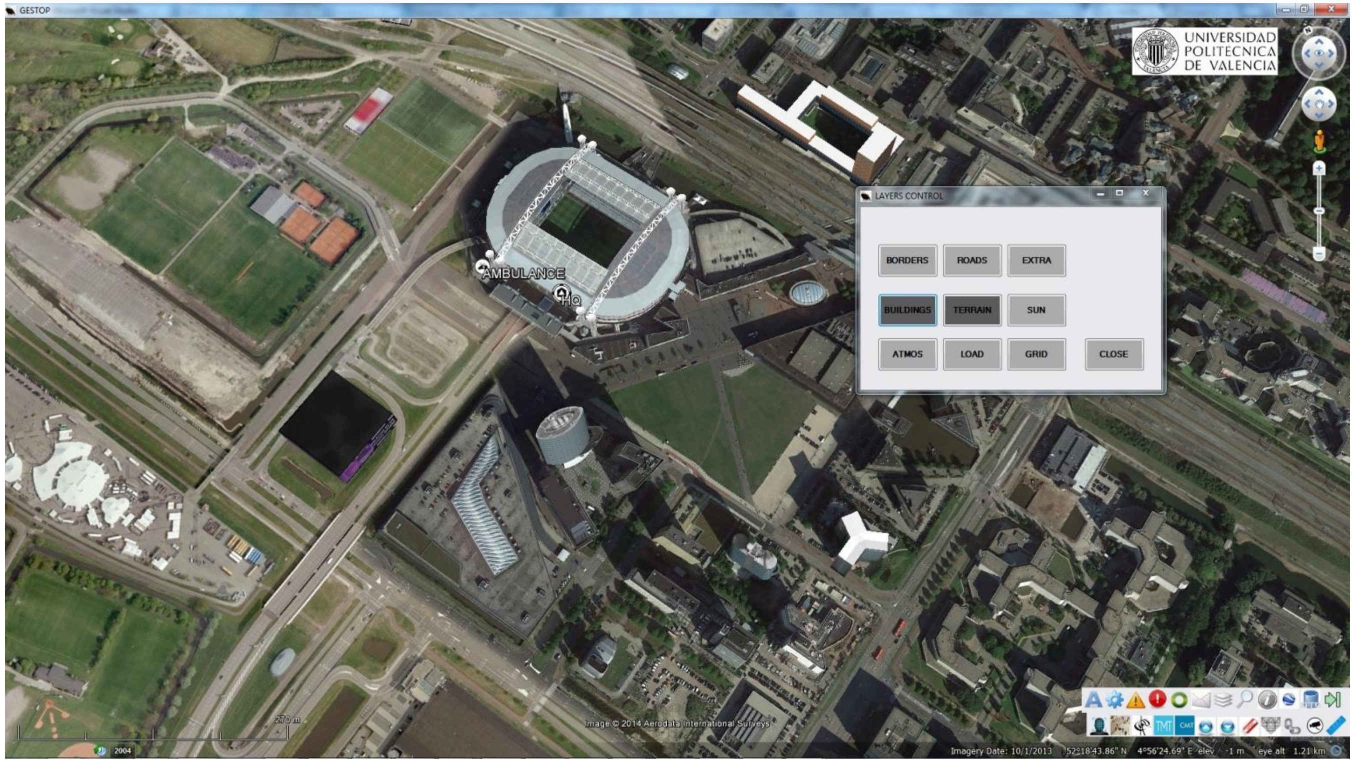
INFO

Pl. PEREZ GALDÓS dirección PUENTE DE CAMPANAR 6

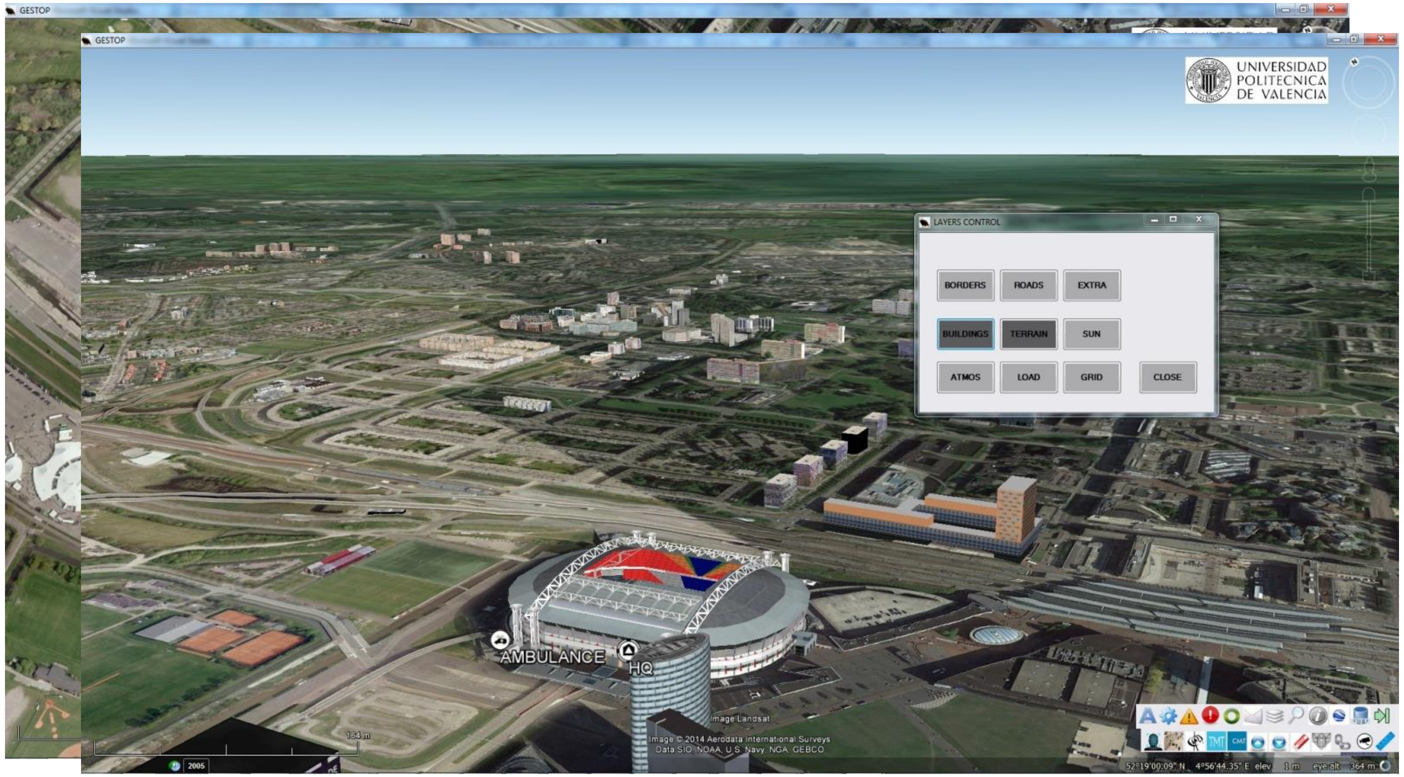
Physical Situational Awareness Application

- **Other SA and C2 capabilities of the SAURON PSA will be the following:**
  - **Messaging:** The PSA has a messaging module capable of sending and receiving text messages to/from the units on field. In addition, PSA has a voice over IP (VoIP) module capable of transmitting voice messages to the units.
  - **Data management:** Additionally, the PSA has a data management module in order to properly store all data received by the system from external sources or tools.
  - **Video processing and fusion unit:** This relies on innovative video analytics suitable for robust person/group tracking and multi camera calibration for mobile (e.g., UAV or body worn) and fixed cameras. All legal requirements regarding data protection and privacy will be taken into consideration with respect to these developments.
  - **PSA Communications interfaces and interoperability:** The PSA is currently fully compliant with the following communication technologies; Internet protocol (Ethernet), WiFi, LTE,,WiMAX, Satellite means Inmarsat, Iridium and Thuraya, Tetra, Tetrapol, 3G and 4G.
  - **PSA Security & Privacy:** The PSA includes a security access module based on the user profile, which allows access to different system capabilities depending on the user's role in the organization. In addition, security transmission protocols such as HTTPS or Transport Layer Security (TLS) are used for transmitting all data from the PSA.

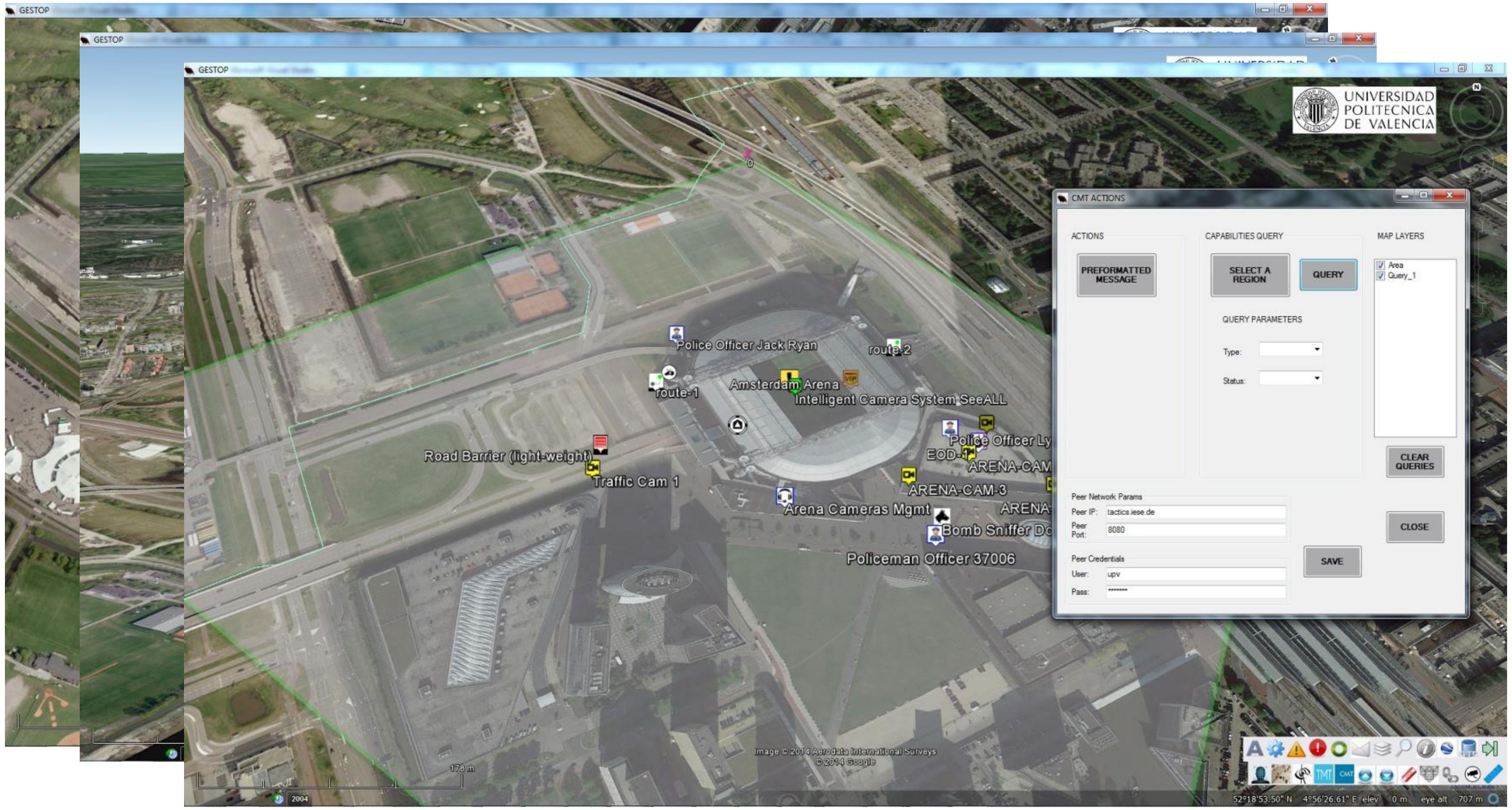
Physical Situational Awareness Application



Physical Situational Awareness Application


GESTOP
GESTOP
UNIVERSIDAD POLITECNICA DE VALENCIA
LAYERS CONTROL
BORDERS
ROADS
EXTRA
BUILDINGS
TERRAIN
SUN
ATMOS
LOAD
GRID
CLOSE
AMBULANCE
HQ
Image Landsat
Image © 2014 Aerodata International Surveys
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
TMT
CMT
2005
52°19'00.09" N 4°56'44.35" E elev 1 m eye alt 364 m

Physical Situational Awareness Application



Type:
Status:

☑ Area
☑ Query_1

Peer Network Params

Peer IP: tactics.iese.de

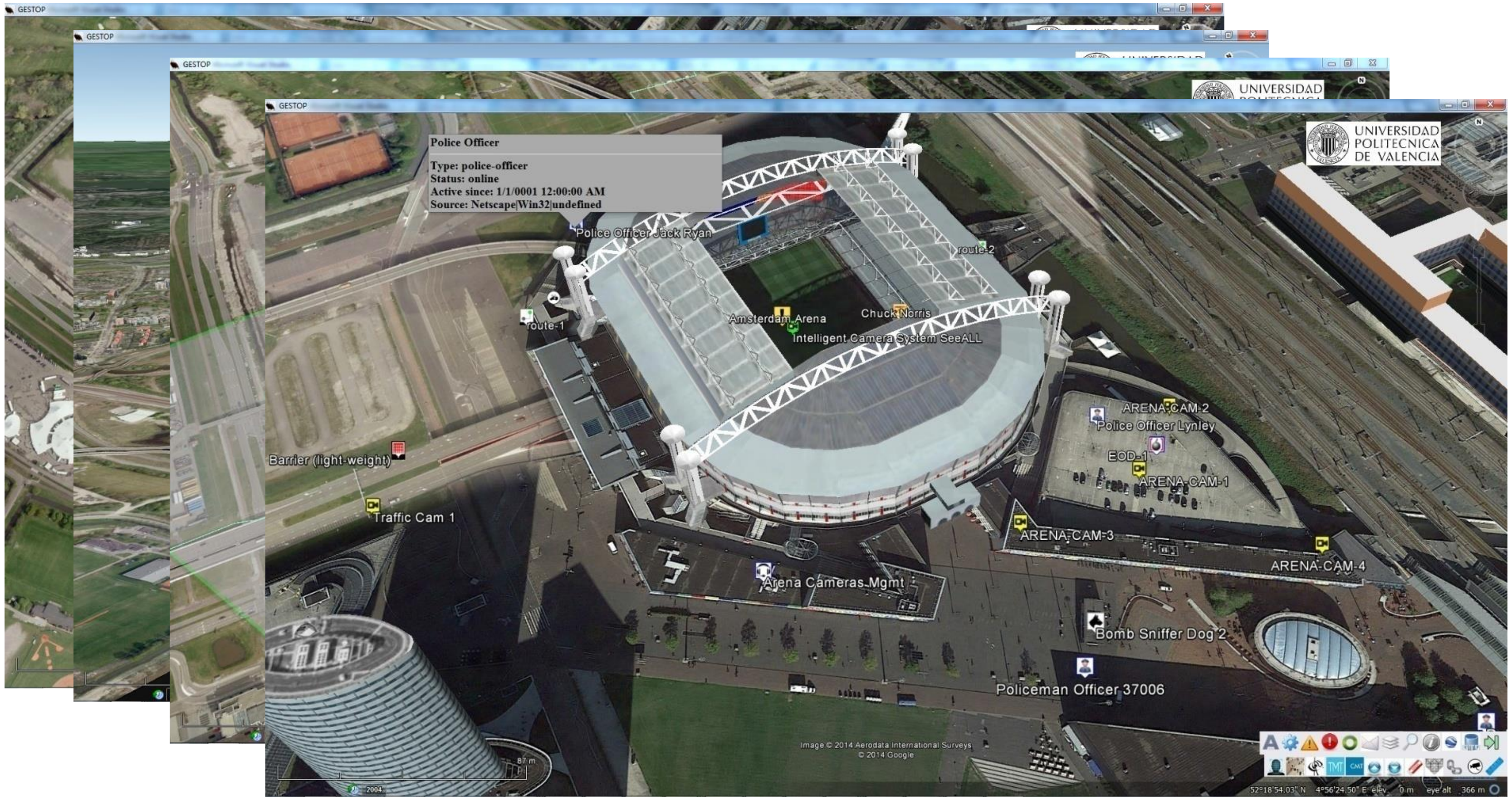
Peer Port: 8080

Peer Credentials

User: upv

Pass: ********

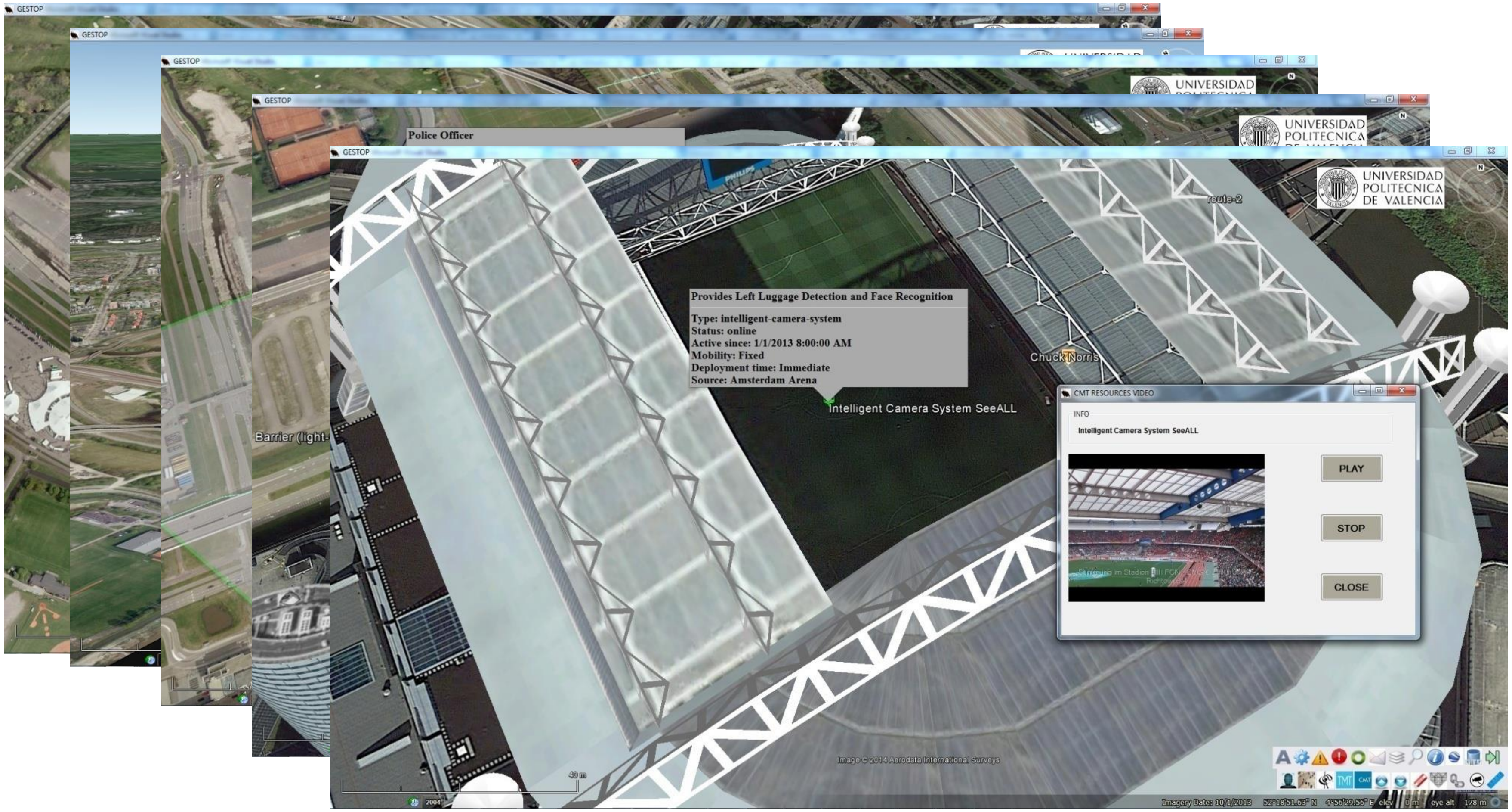
Physical Situational Awareness Application



Police Officer

Type: police-officer
Status: online
Active since: 1/1/0001 12:00:00 AM
Source: Netscape|Win32|undefined

Physical Situational Awareness Application



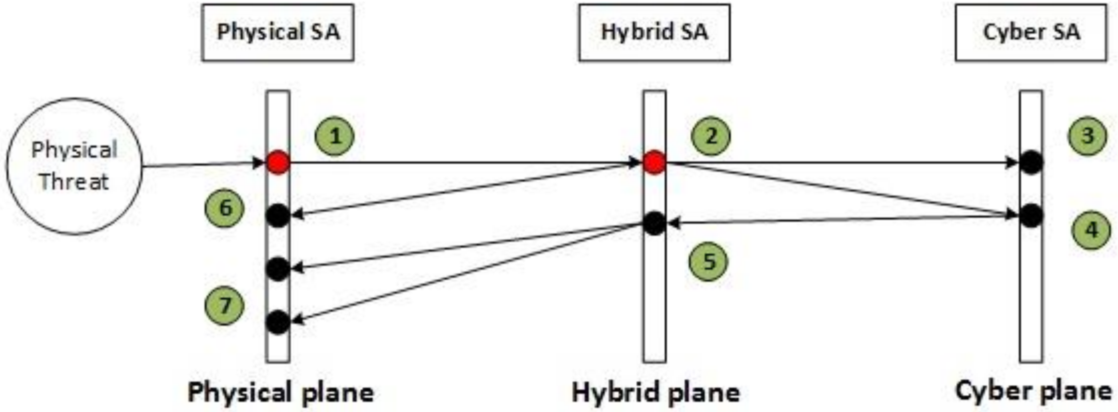
Provides Left Luggage Detection and Face Recognition

Type: intelligent-camera-system
Status: online
Active since: 1/1/2013 8:00:00 AM
Mobility: Fixed
Deployment time: Immediate
Source: Amsterdam Arena

Hybrid Situational Awareness

HYBRID SA

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



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

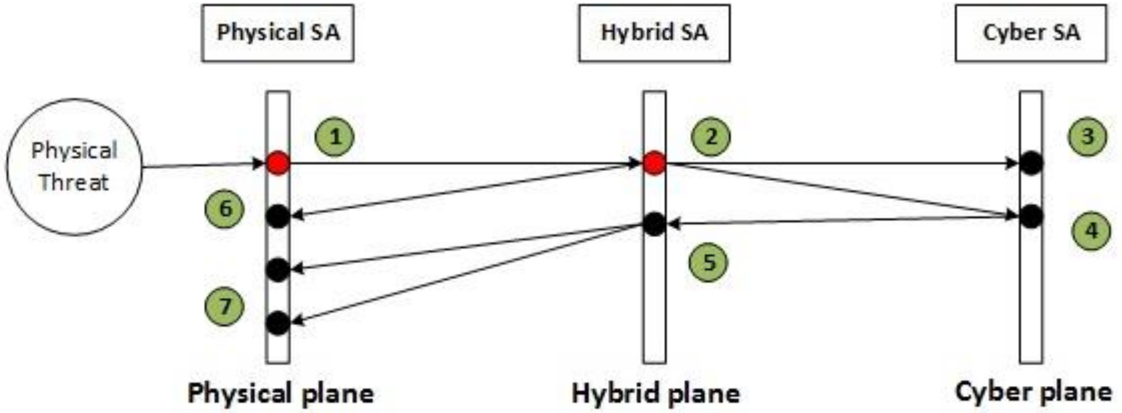
5 Potencial threat in the cyber plane as consequence of the initial detected threat with consequences in the physical plane visualized in the Hybrid SA application

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

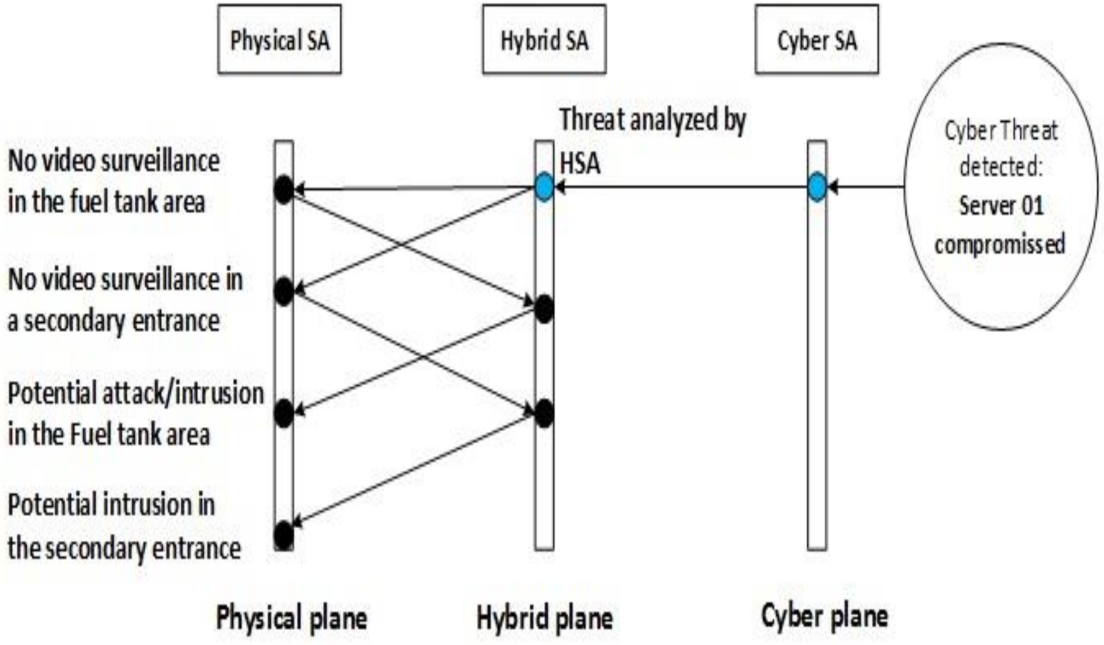
Hybrid Situational Awareness

- For example, an incident in the physical plane, e.g., an explosion/fire, is detected in a building of the port. This event is detected by the PSA and is analysed by the HSA.
- The HSA shows in real time what potential consequences/effects this accident/attack could have in the near future in both planes. In this case study, several servers have been destroyed by the explosion.
- Consequently, a freight shipping application of a large company is at risk of being hacked and video flows and data have been lost from surveillance cameras and access control assets.
- This warns the decision makers that a physical attack and/or cyber intrusion in these items could now happen, since that specific area now has no video surveillance and access control data are no longer being received.



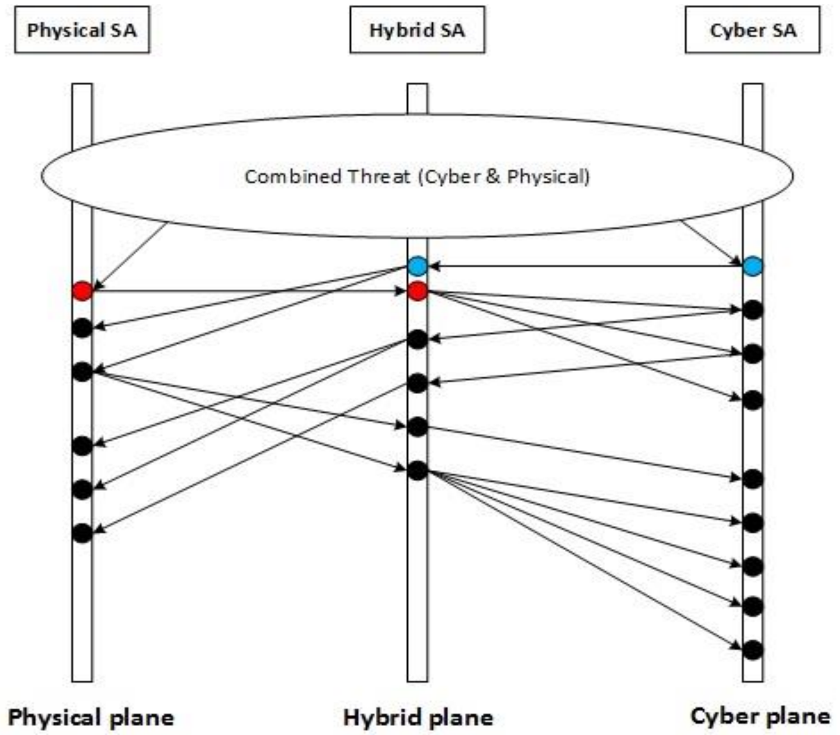
Hybrid Situational Awareness

- In the other hand, the Cyber SA detects that a video server has been compromised by a cyber-attack. The HSA system shows in real time the potential consequences/effects of this attack on the real world.
- These consequences could be the loss of video flows from the surveillance cameras watching over the fuel tanks' area as well as from video surveillance cameras at a secondary entrance of the port.
- This warns the decision makers that a potential attack/intrusion in these areas could now happen, since there is no video surveillance there.
- Additionally, advice is provided, for example, to send a security patrol, tracked by the PSA, to the fuel tank area to ensure the protection of this critical area and to reinforce and alert the security staff in the secondary entrance that have lost the video surveillance flows.


Physical SA
Hybrid SA
Cyber SA
Threat analyzed by HSA
Cyber Threat detected: Server 01 compromissed
No video surveillance in the fuel tank area
No video surveillance in a secondary entrance
Potential attack/intrusion in the Fuel tank area
Potential intrusion in the secondary entrance
Physical plane
Hybrid plane
Cyber plane

Hybrid Situational Awareness

- The complexity of the situation can be even larger and the cascading effect can be amplified in the presence of a combined threat, i.e., a combination of both of the above scenarios



Thanks for your attention!!