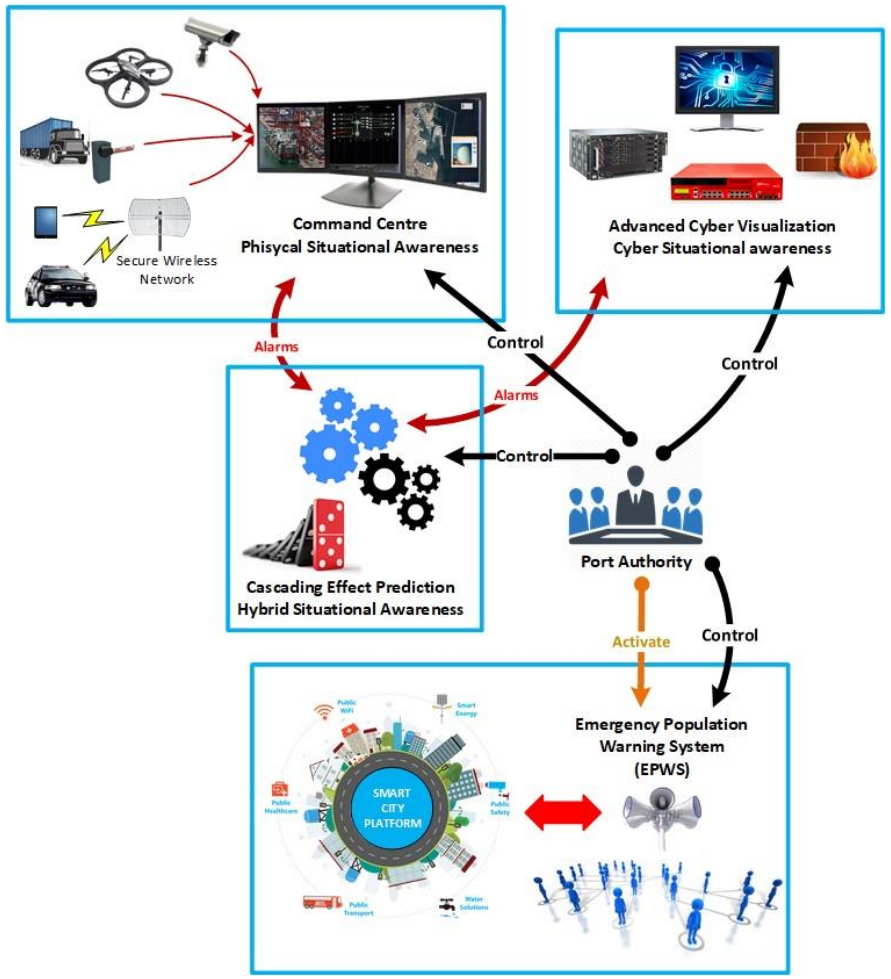
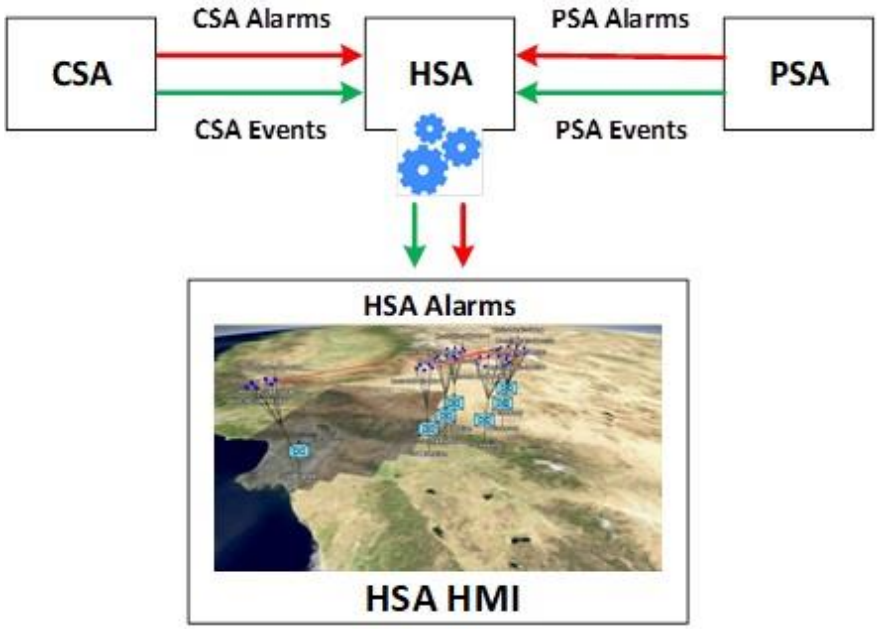
SAURON Components

Sauron Physical Situation Awareness (PSA)

Dr. Israel Pérez [UPV]
Xavier Mamy [IDEMIA]

Overall SAURON Architecture Definition





Adaptation to the port environment

- PSA is based on an existing Command and Control (C2) system (GESTOP)
    - has been adapted to the port environment in order to increase the physical security and the situation Awareness (SA).

- PSA application proposed by SAURON can be adapted to different types of ports in order to cover their detected vulnerabilities and risks as well as effectively protect their main critical areas.

Adaptation to the port environment

- PSA is based on the civil (GESTOP) version of the Spanish Army Friendly Force Tracking system (SIMACET-FFT) developed by UPVLC and deployed in:
    - Afghanistan
    - Lebanon
    - Mali.

- This system is a complete SA solution capable of integrating a wide range of sensors and offering advanced SA and C2 capabilities

Adaptation to the port environment

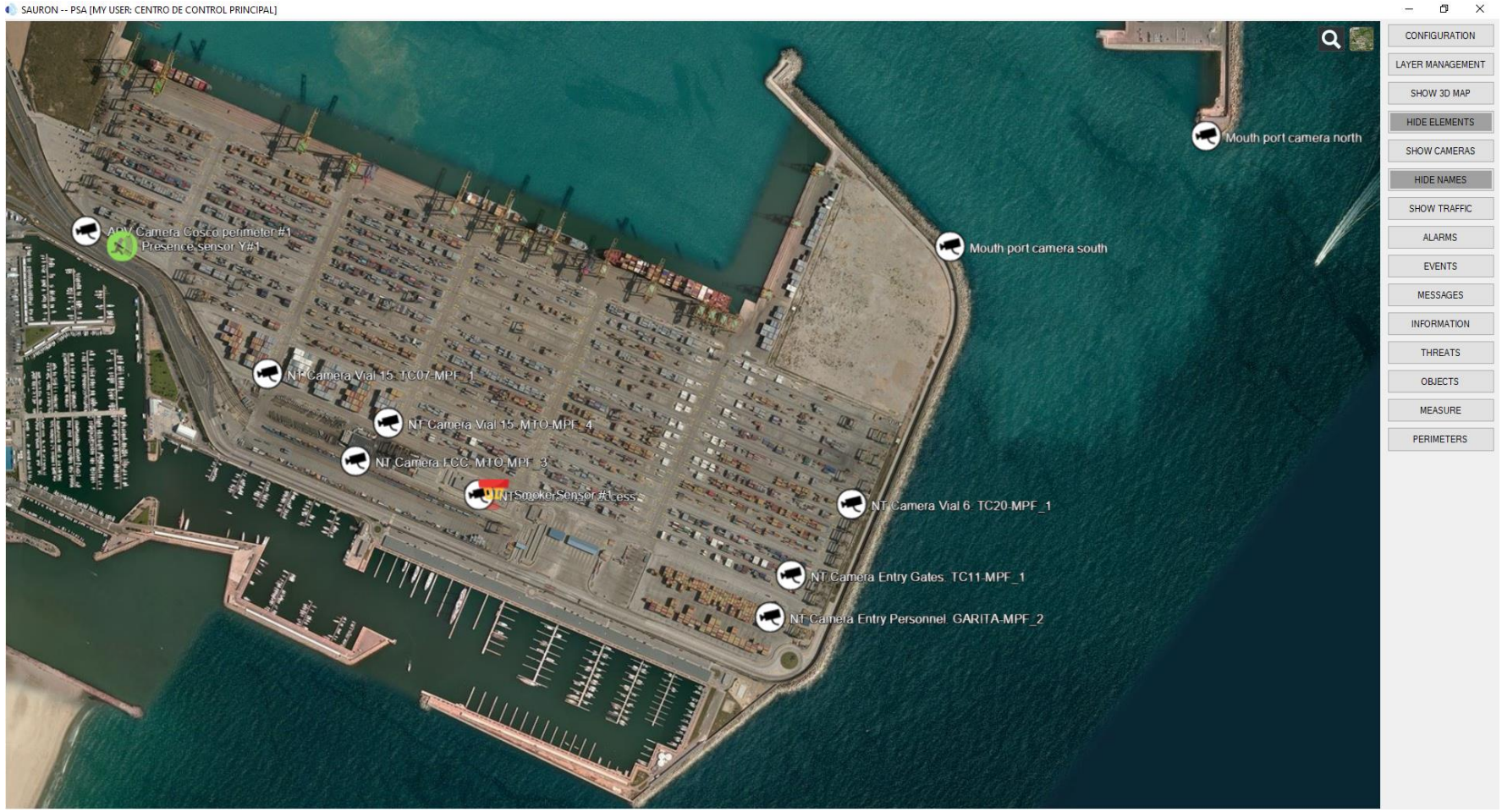
- During the development process the consortium has taken into account the ports physical vulnerabilities found during the “Physical Situational Awareness” WP and the user requirements stated by the end users for the PSA in:
  - Physical vulnerabilities stated in “Physical Risks and Vulnerabilities Report “
  - PSA User requirements accomplishment (“User Requirements Specification”), in particular:
    - PSA general requirements accomplishment
    - PSA HMI requirements accomplishment
    - PSA Data storage requirements accomplishment
    - PSA User Requirements from Interviews
- The whole adaptation process is described in “Physical SA Application Adaptation and Integration with Existing Systems“

Sensors integration

- In order to cover the physical security needs of the ports pilots the following sensors have been integrated in the PSA:

  - **Presence detectors**
  - **Video surveillance cameras**
  - **Port Police tablets**
  - **Smoke detectors**
  - **AIS processing**
  - **Drone-based Surveillance**

Sensors integration: Access



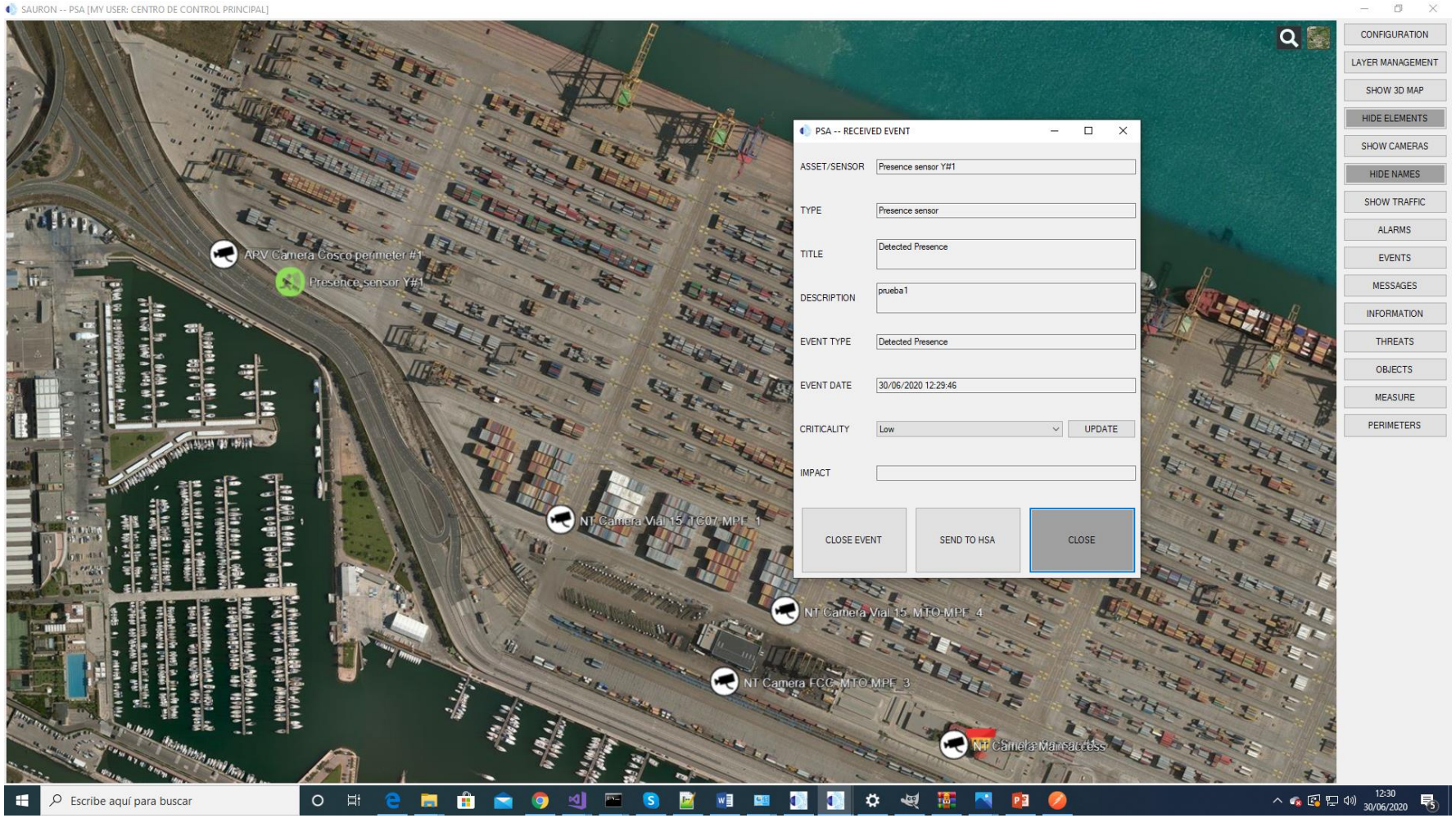
Sensors integration: Presence Sensors

- Ubiquity mFi series presence sensors have been used

PSA Sensors Manager

SAURON PSA HMI

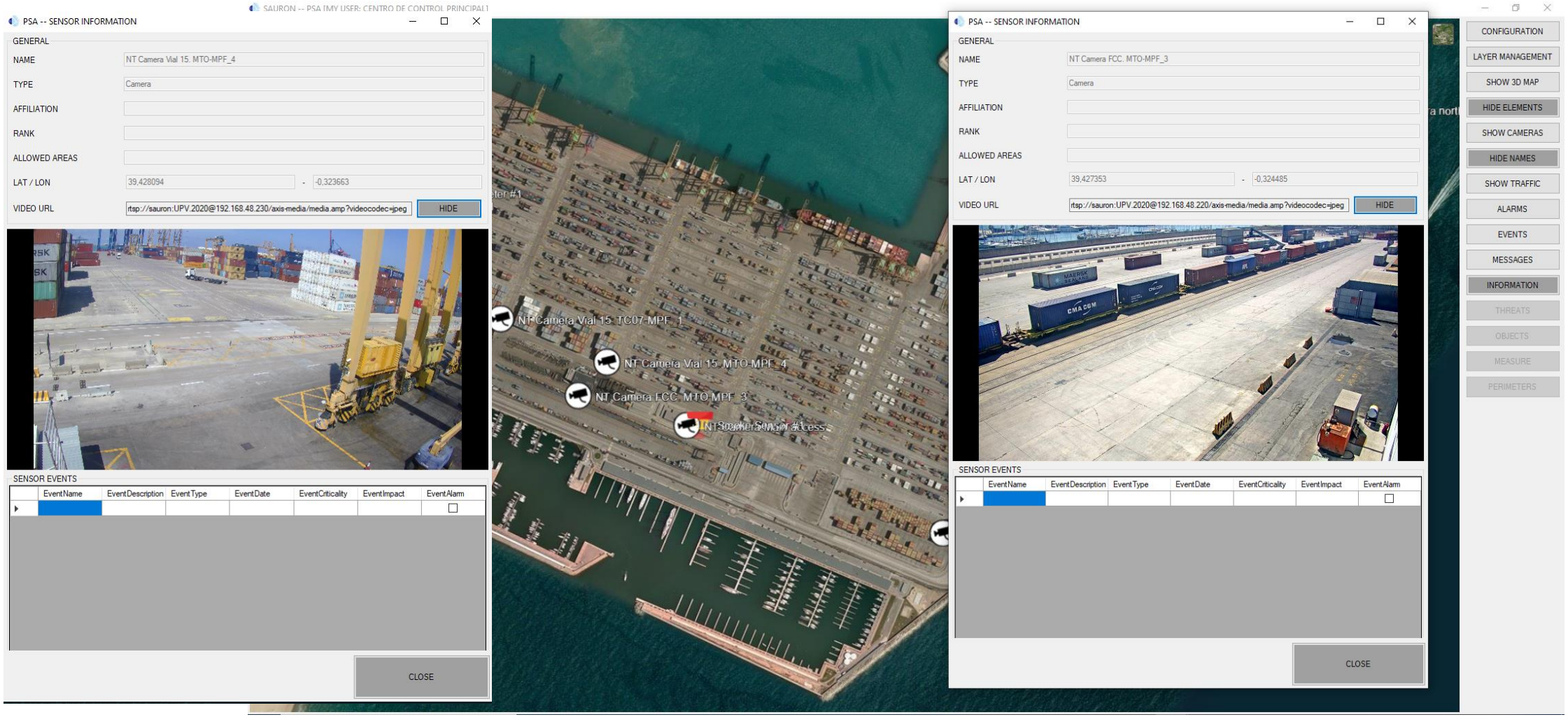
Sensors integration: Presence Sensors



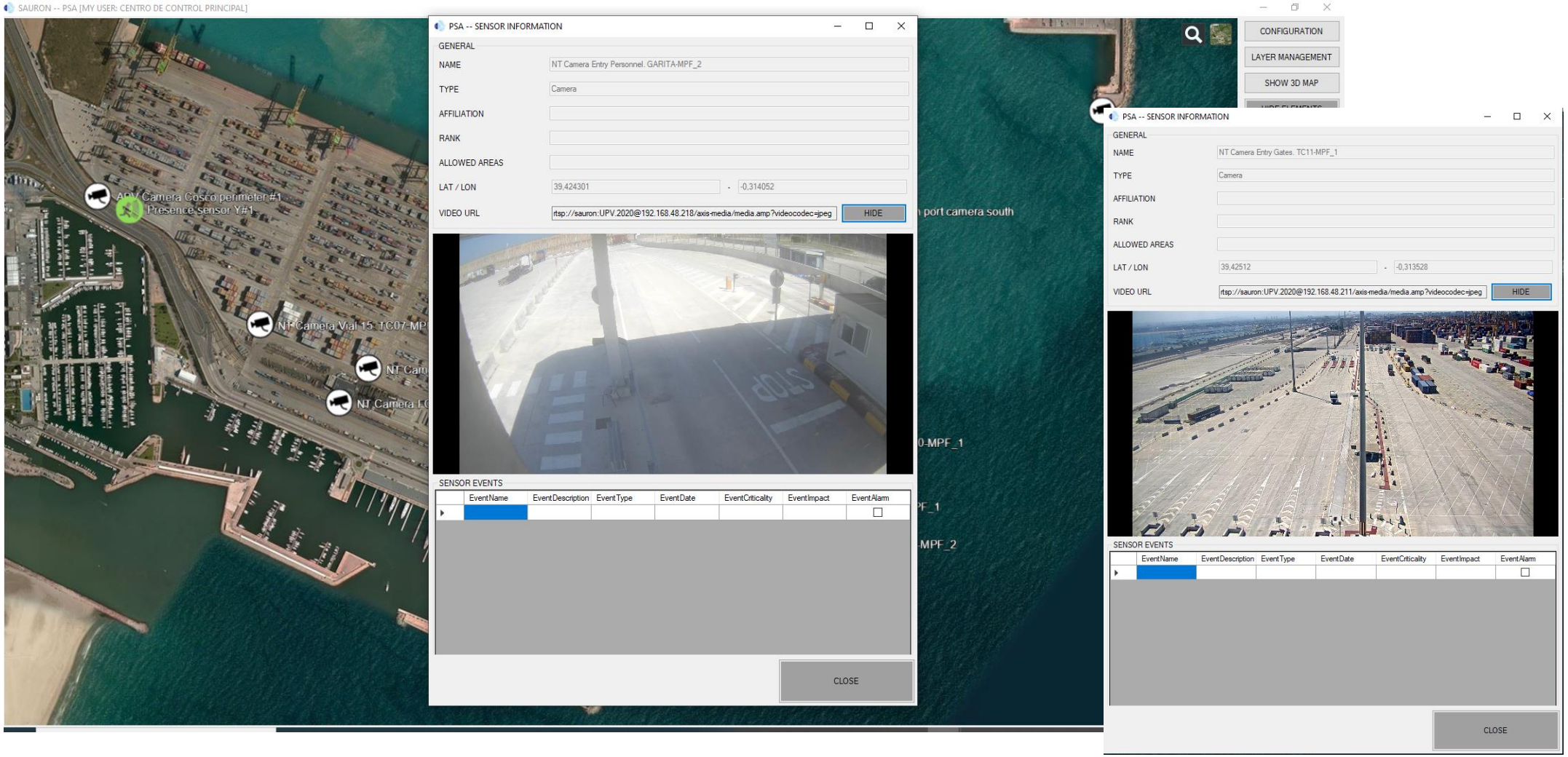
Sensors integration: Video Surveillance

CSP cameras have been integrated

Sensors integration: Video Surveillance

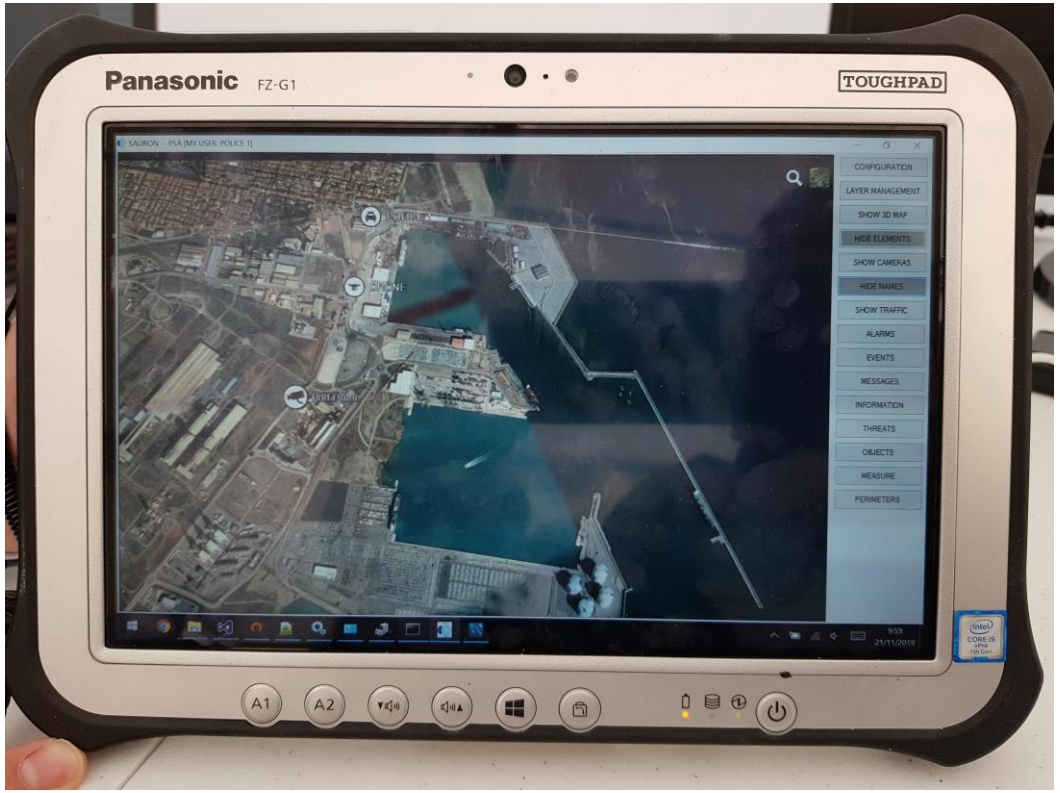


Sensors integration: Video Surveillance



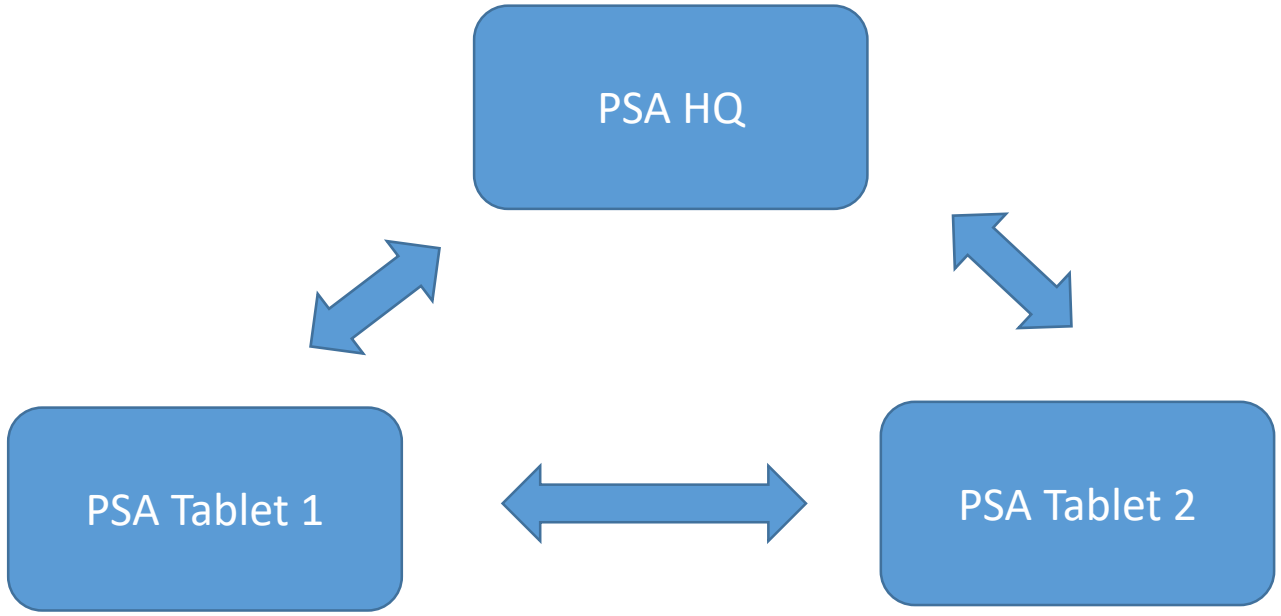
Sensors integration: Port Police Tablets

- Tablets have been integrated in the system
- Integration allows to exchange:
  - Messages
  - Alarms
  - Threats
  - Positions
- All in real time

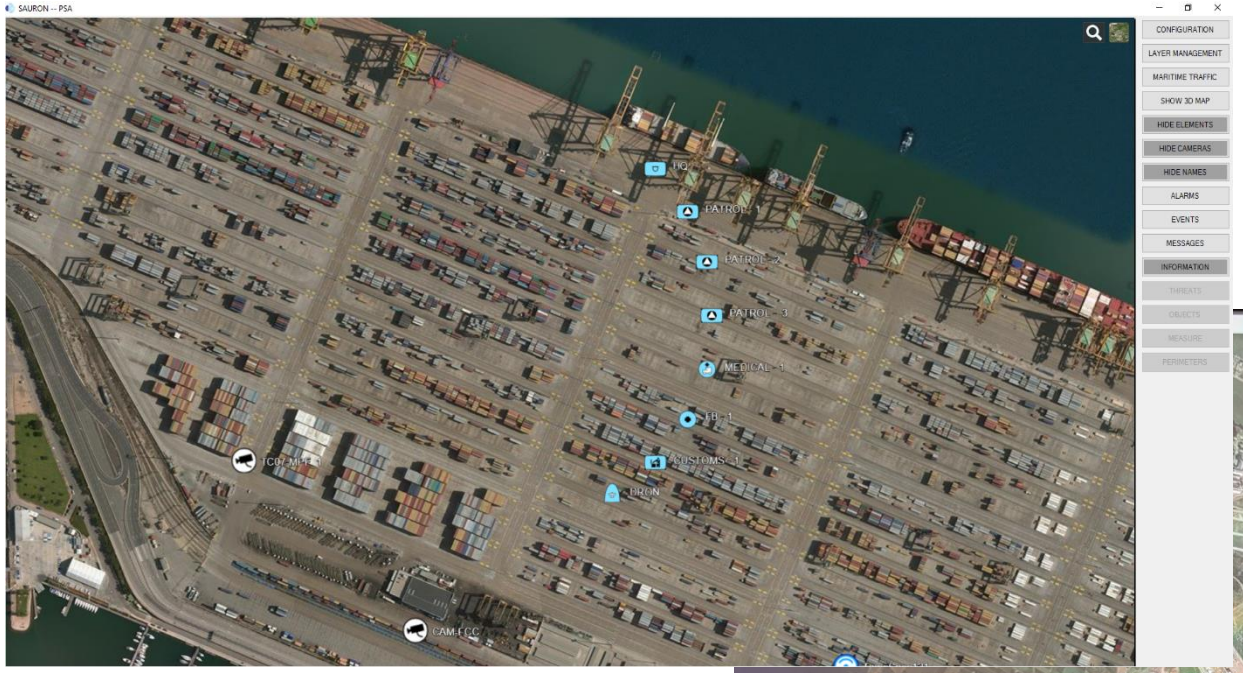


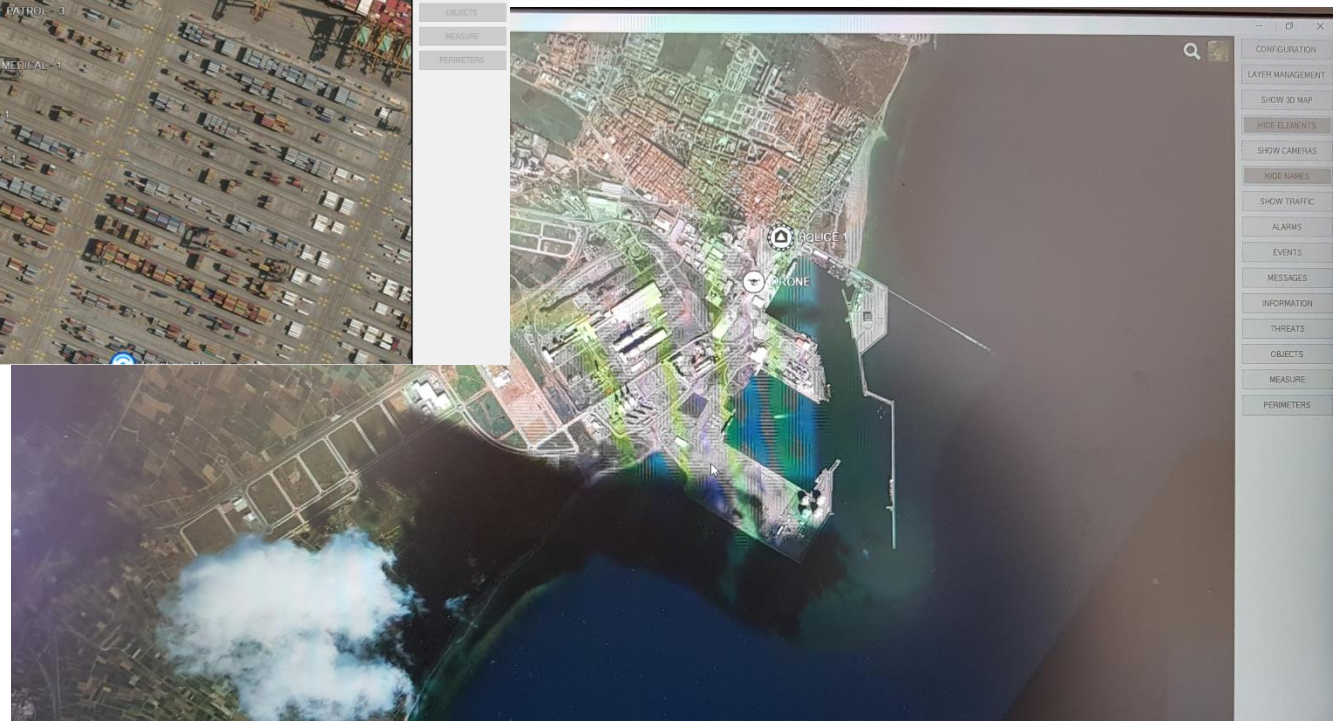
Sensors integration: Port Police Tablets

- In-PSA communications architecture



Sensors integration: Port Police Tablets

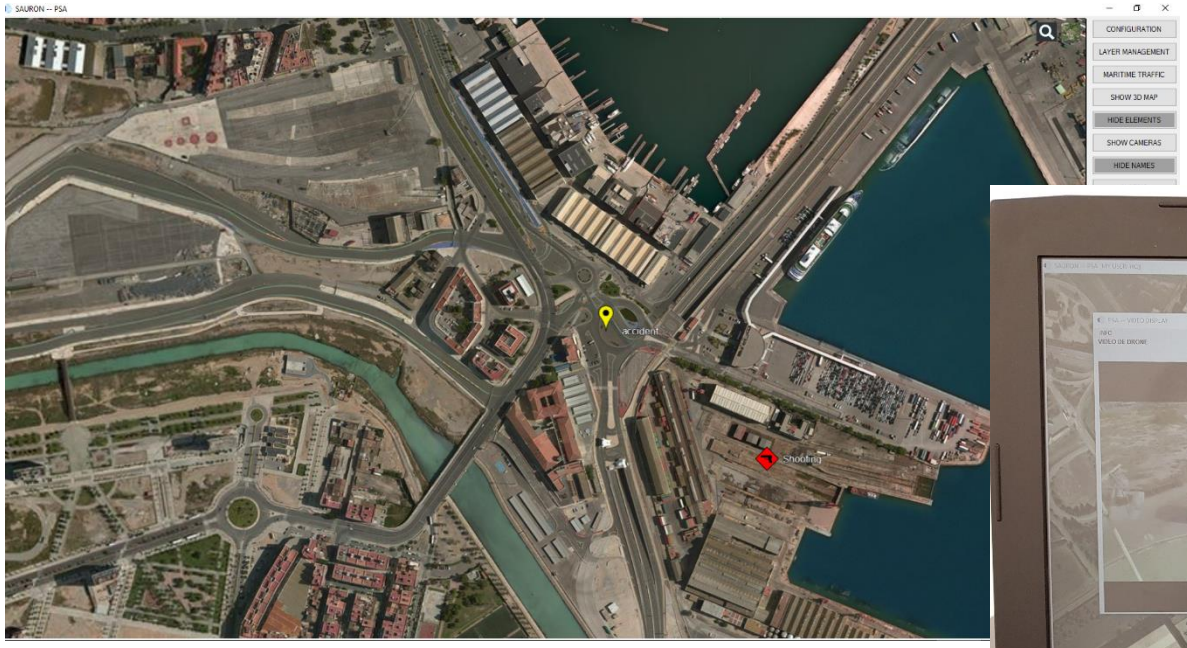


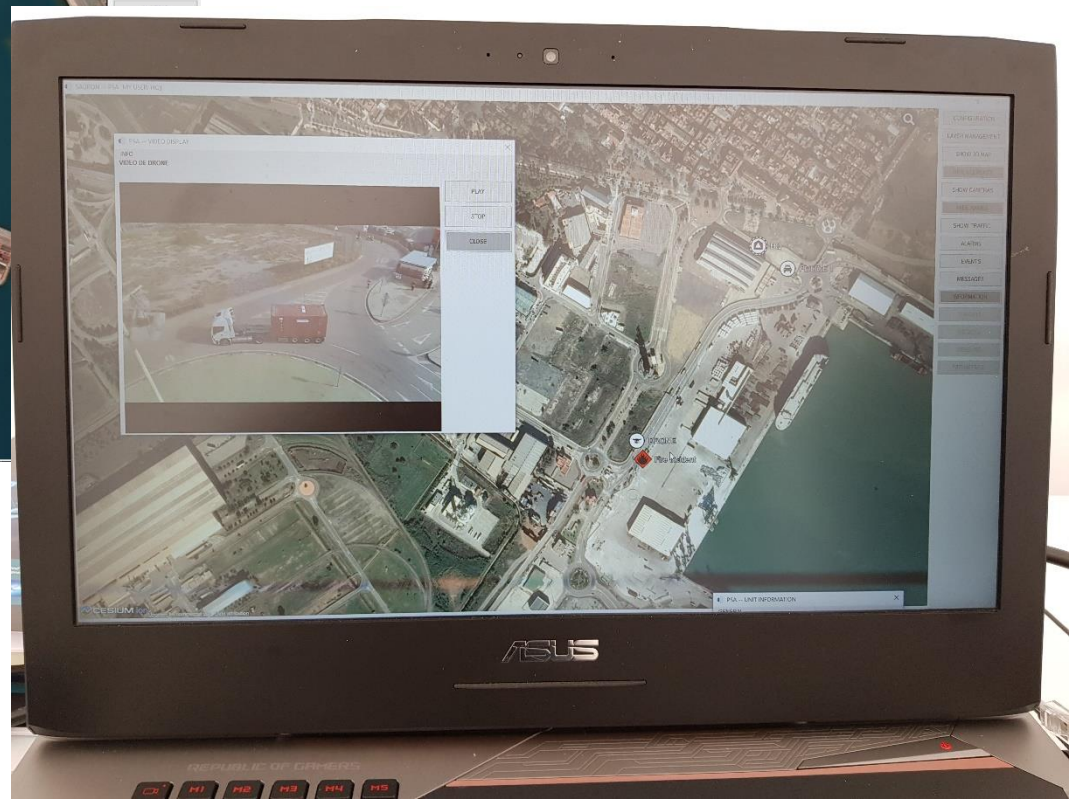


Real-time

Units Position

Sensors integration: Port Police Tablets



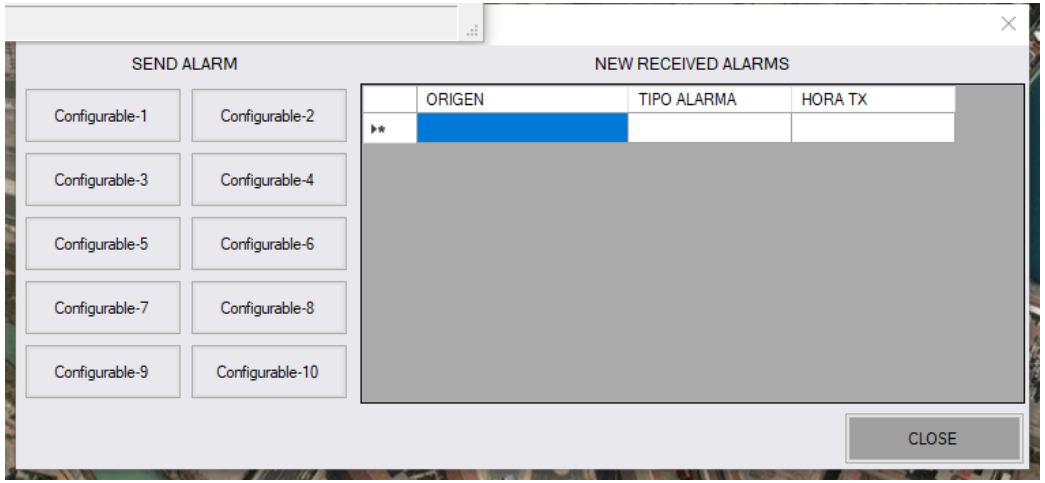


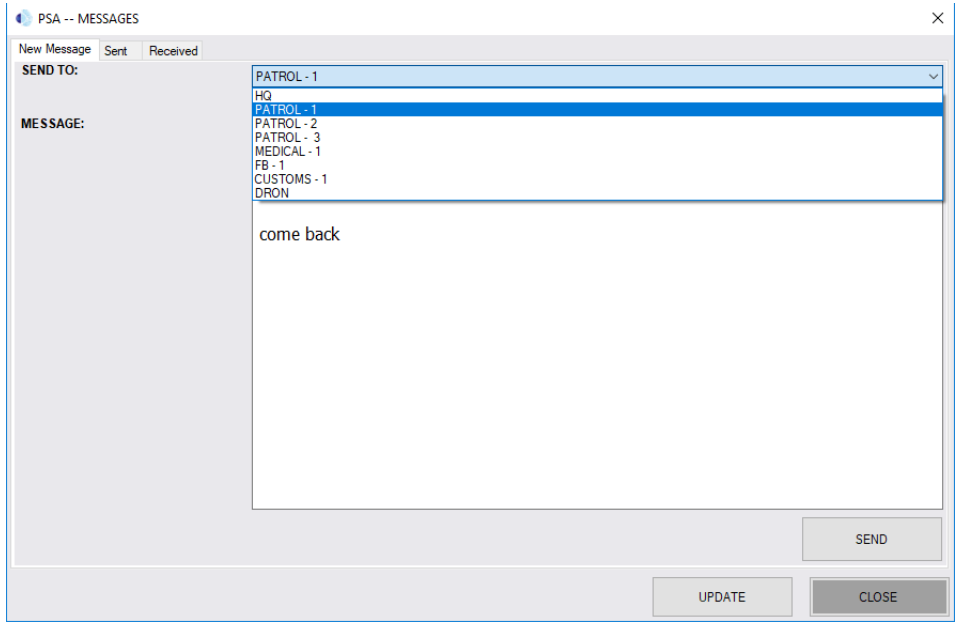
Real-time

Threats

Objects

Sensors integration: Port Police Tablets



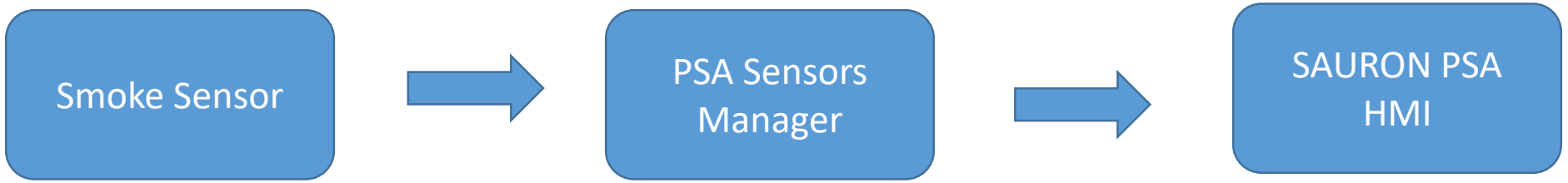


Real-time

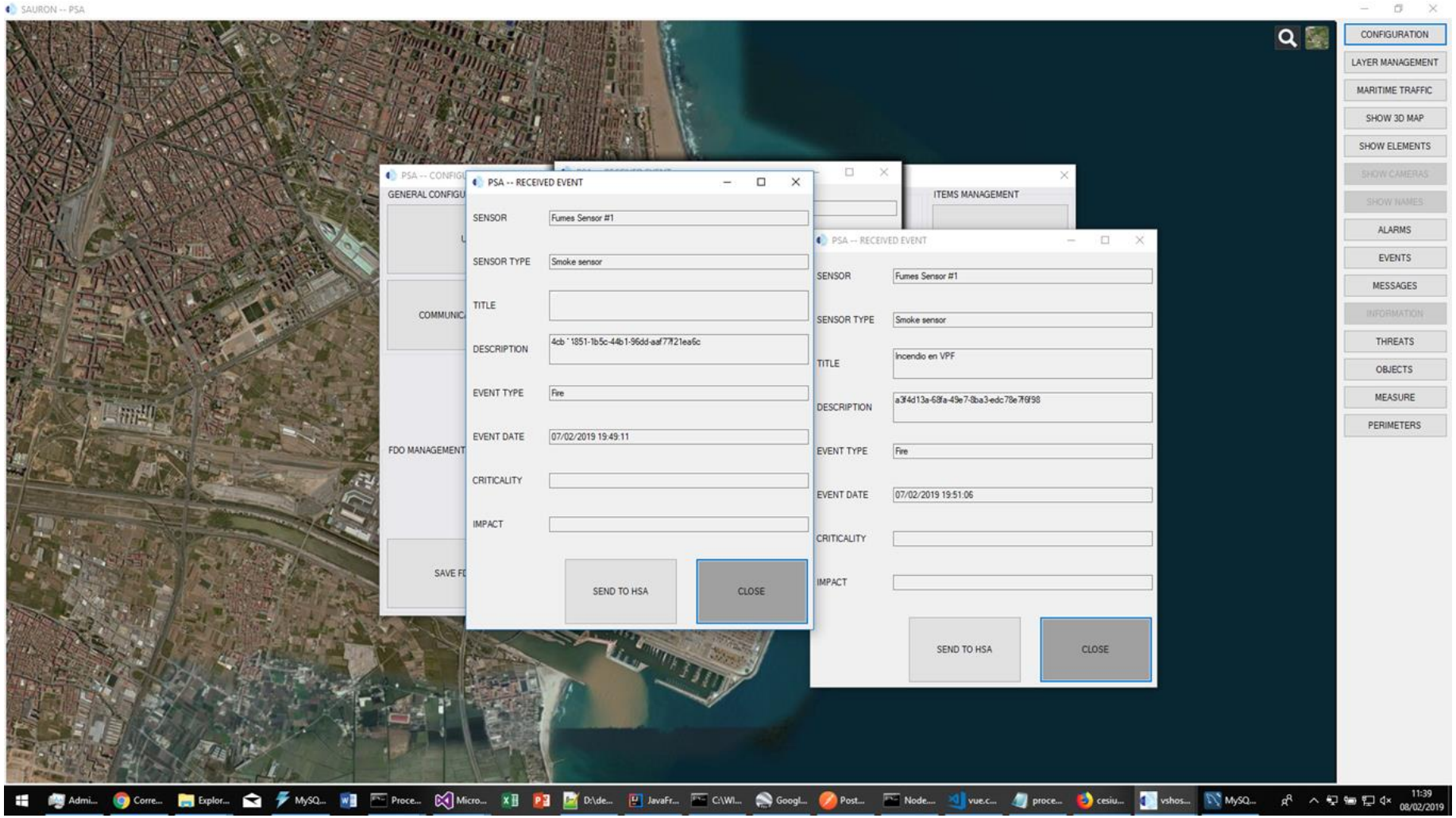
Alarms

Messages

Sensors integration: Smoke Sensors

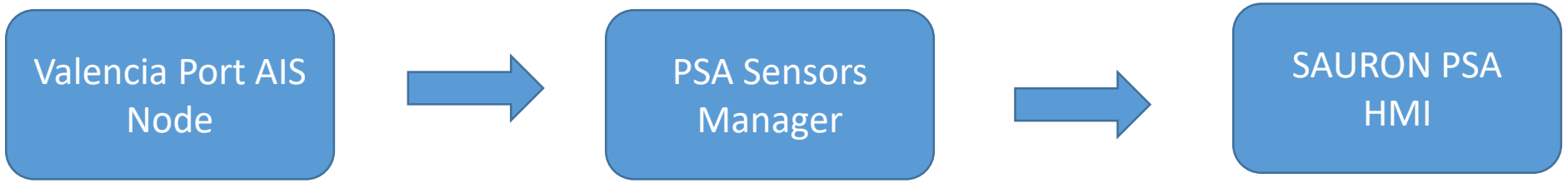


Sensors integration: Smoke Sensors

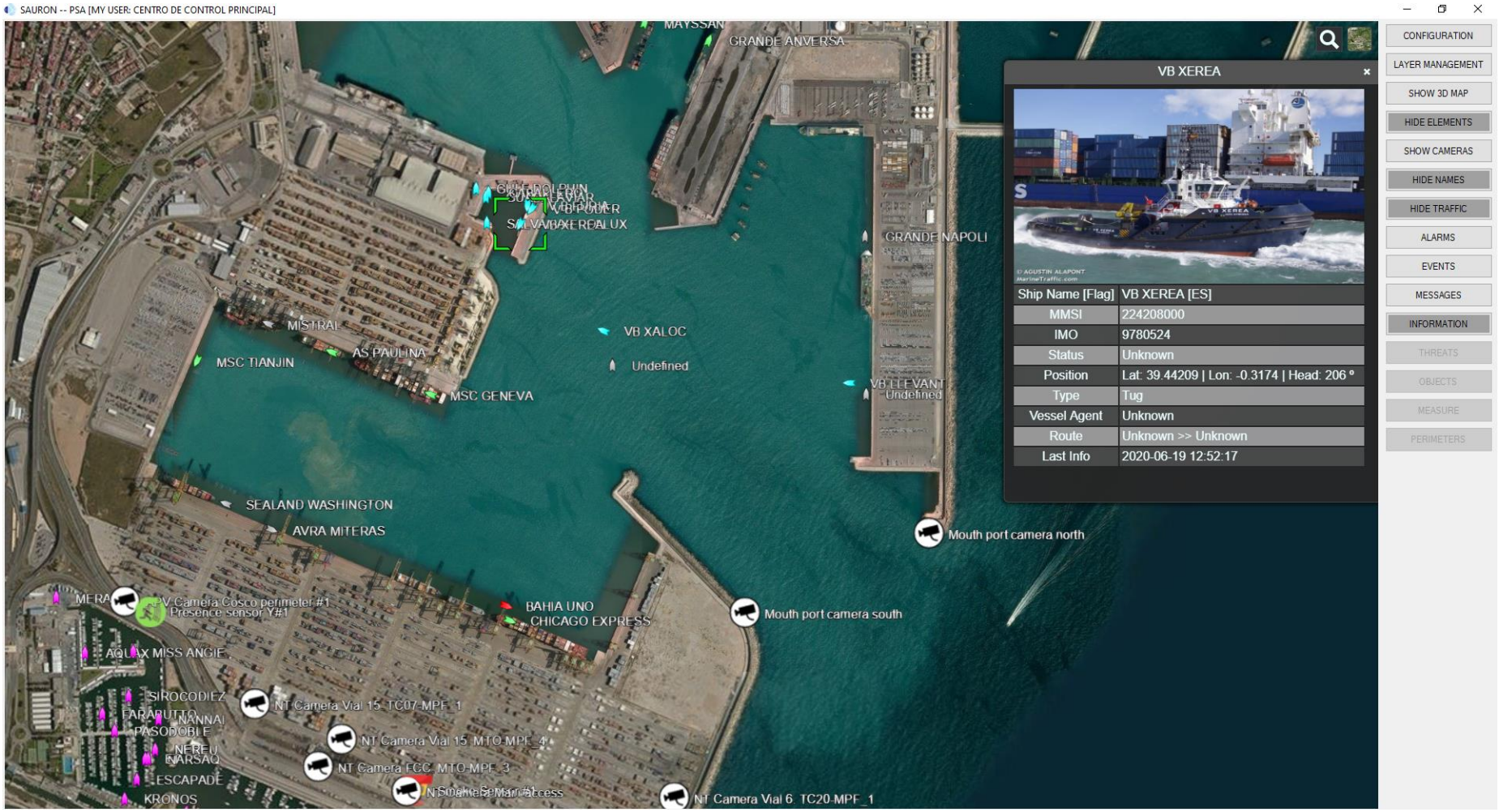


Sensors integration: AIS Processing

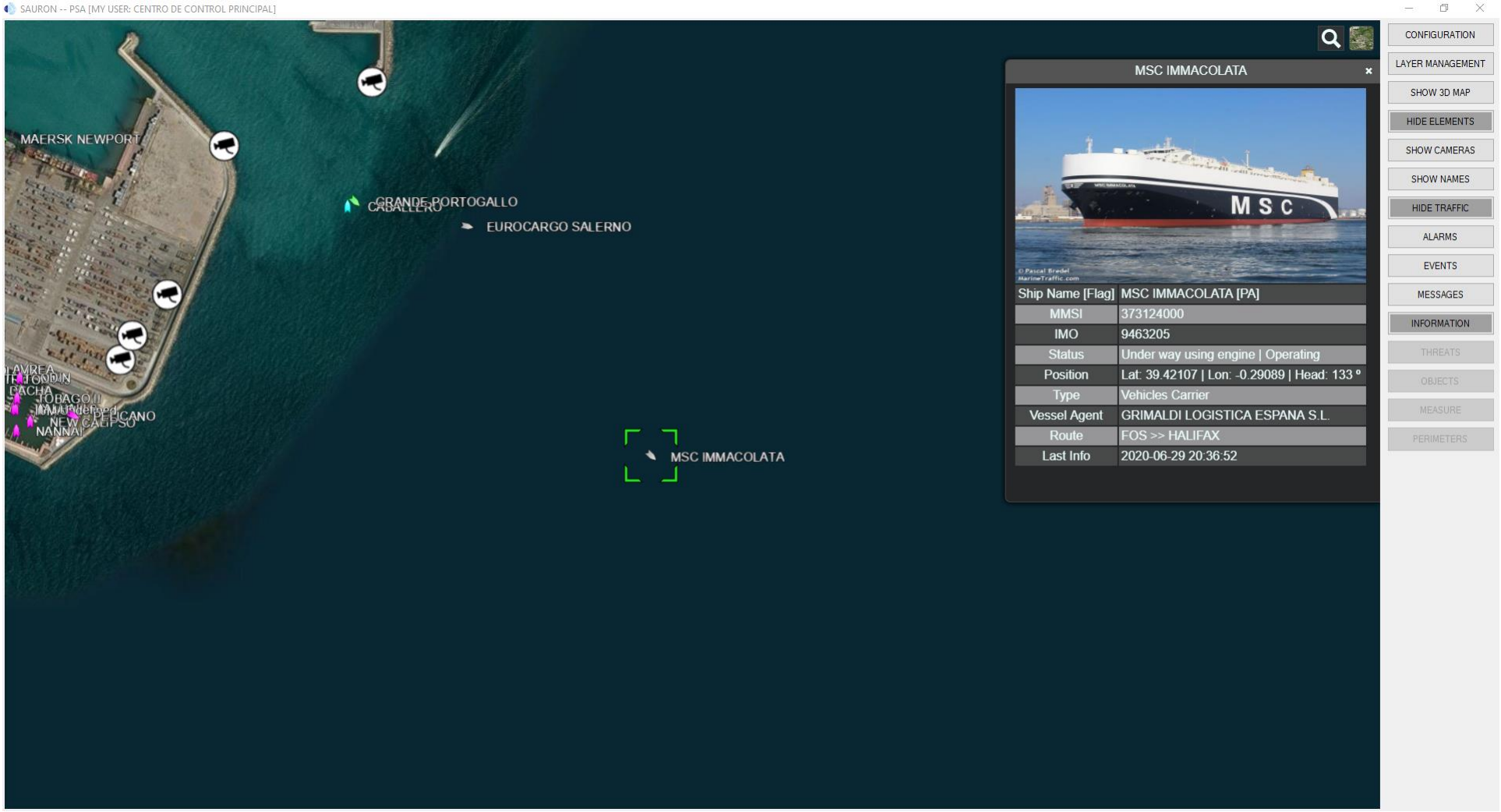
- Valencia Port AIS infrastructure has been integrated
- Real-time vessels data included in PSA



Sensors integration: AIS Integration



Sensors integration: AIS Integration

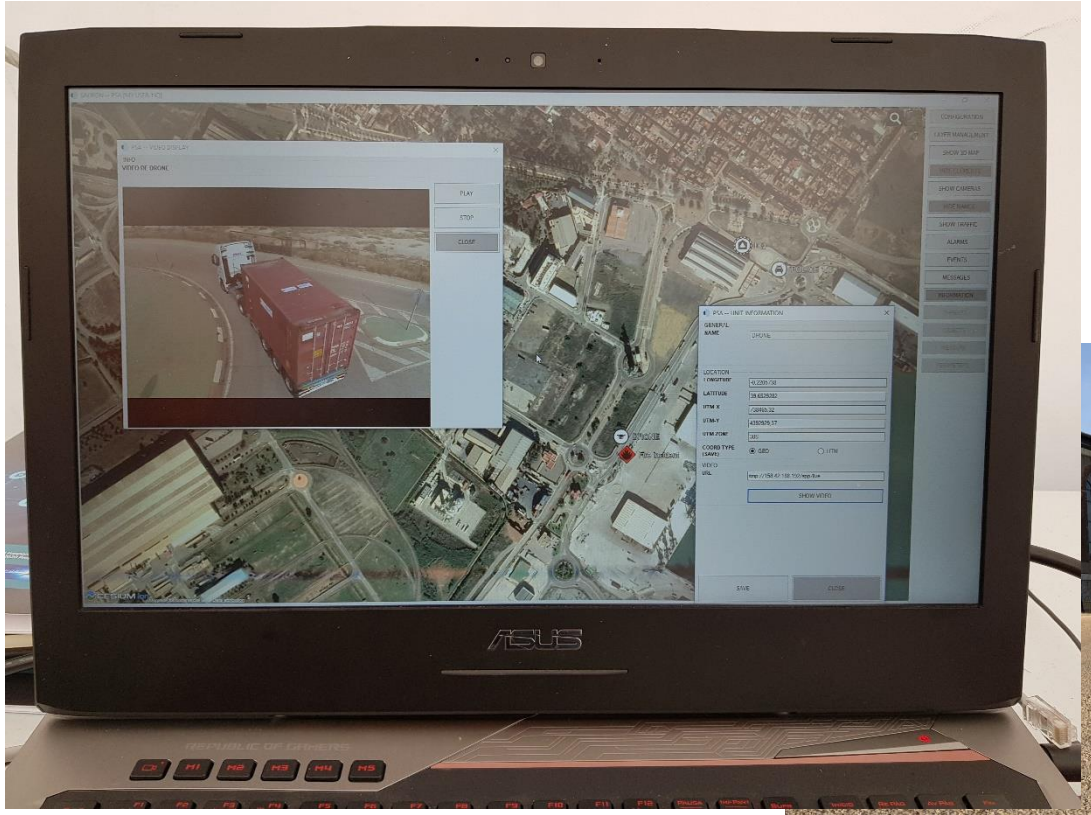


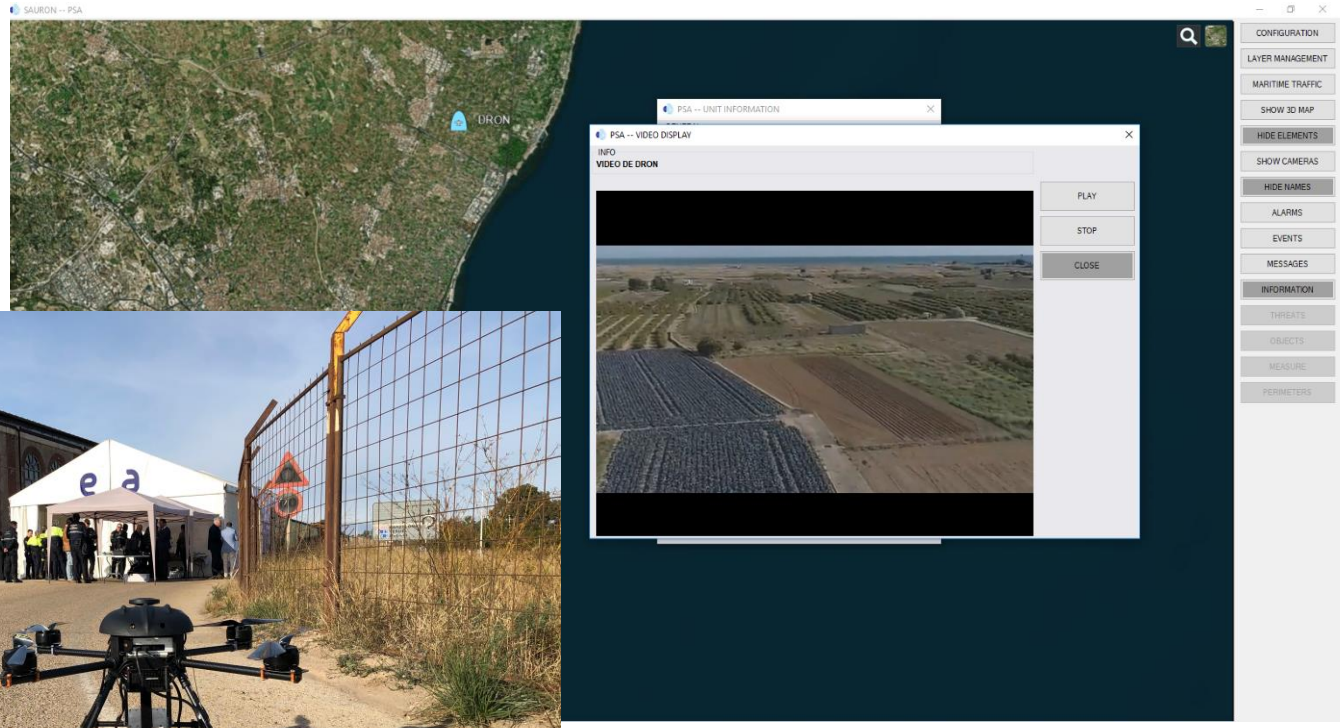
Sensors integration: Drone-based surveillance

- DJI drones from a 3rd party company have been integrated

DJI Ground Base Station → RTMP Video Server → SAURON PSA HMI

Sensors integration: Drone-based surveillance

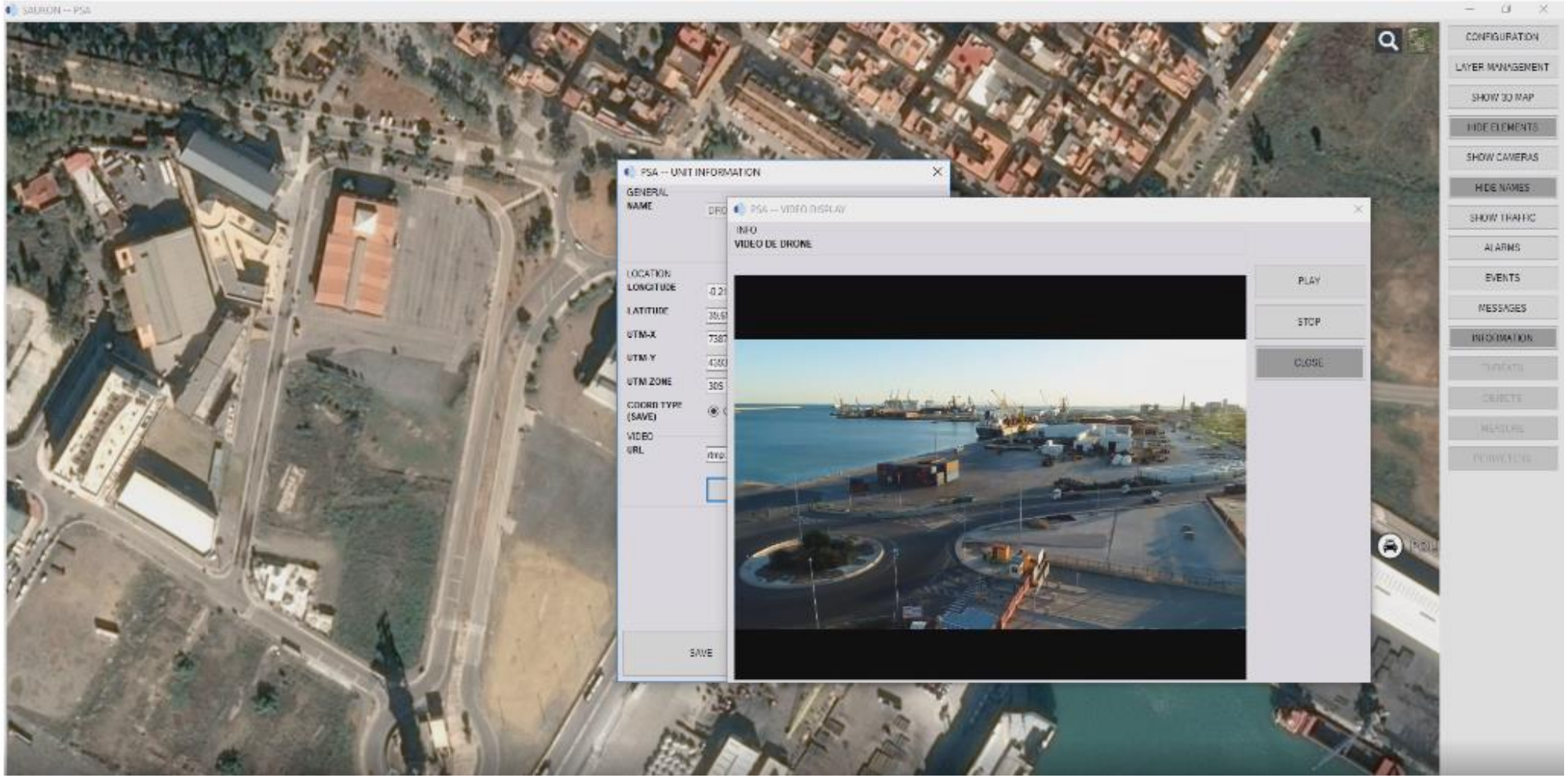




SAGUNTO Pilot

SAURON + ROCSAFE

Sensors integration: Drone-based surveillance

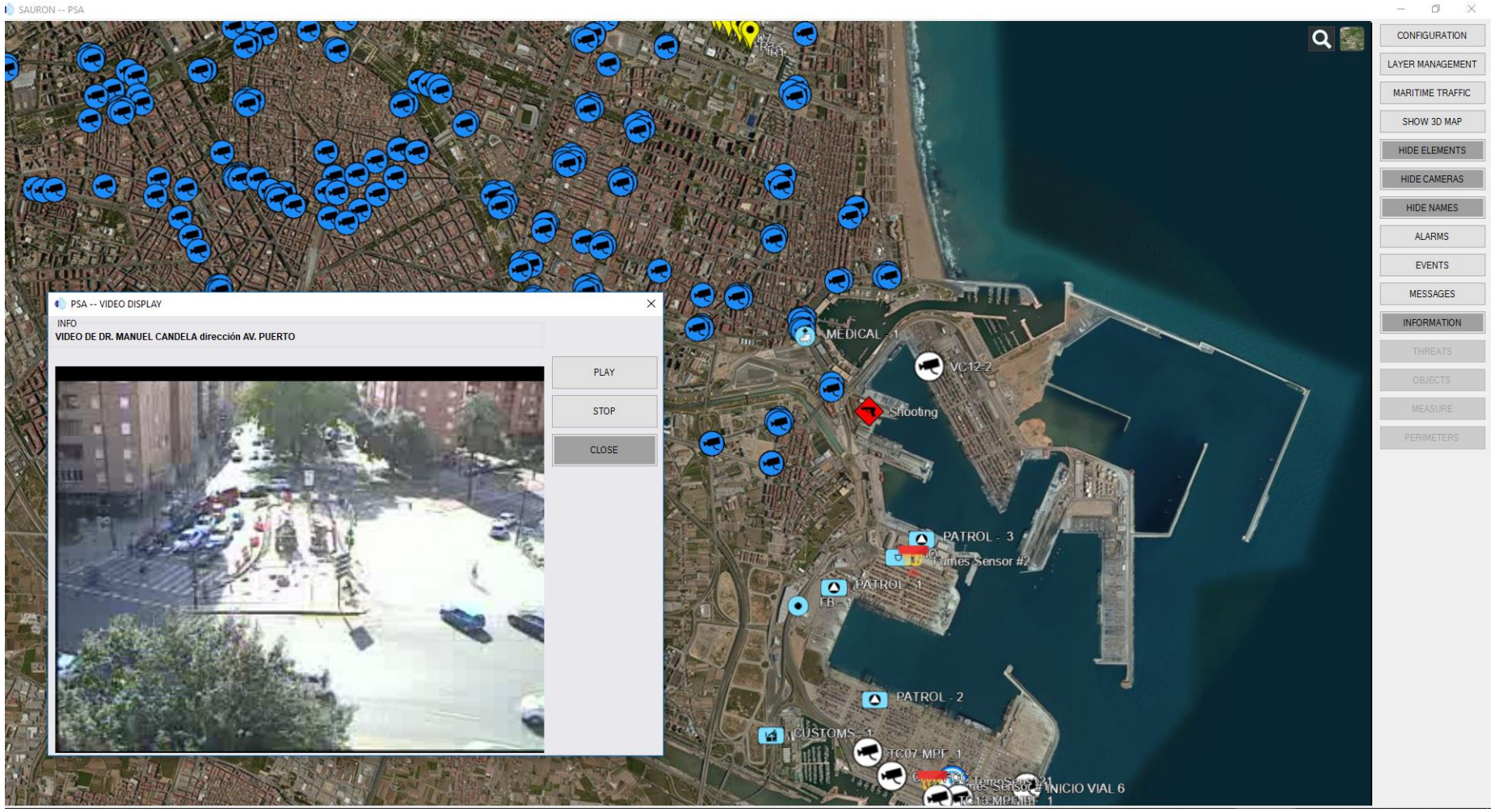


Sensors integration: Valencia City Council Video Cameras

Valencia City Council Cameras have been integrated

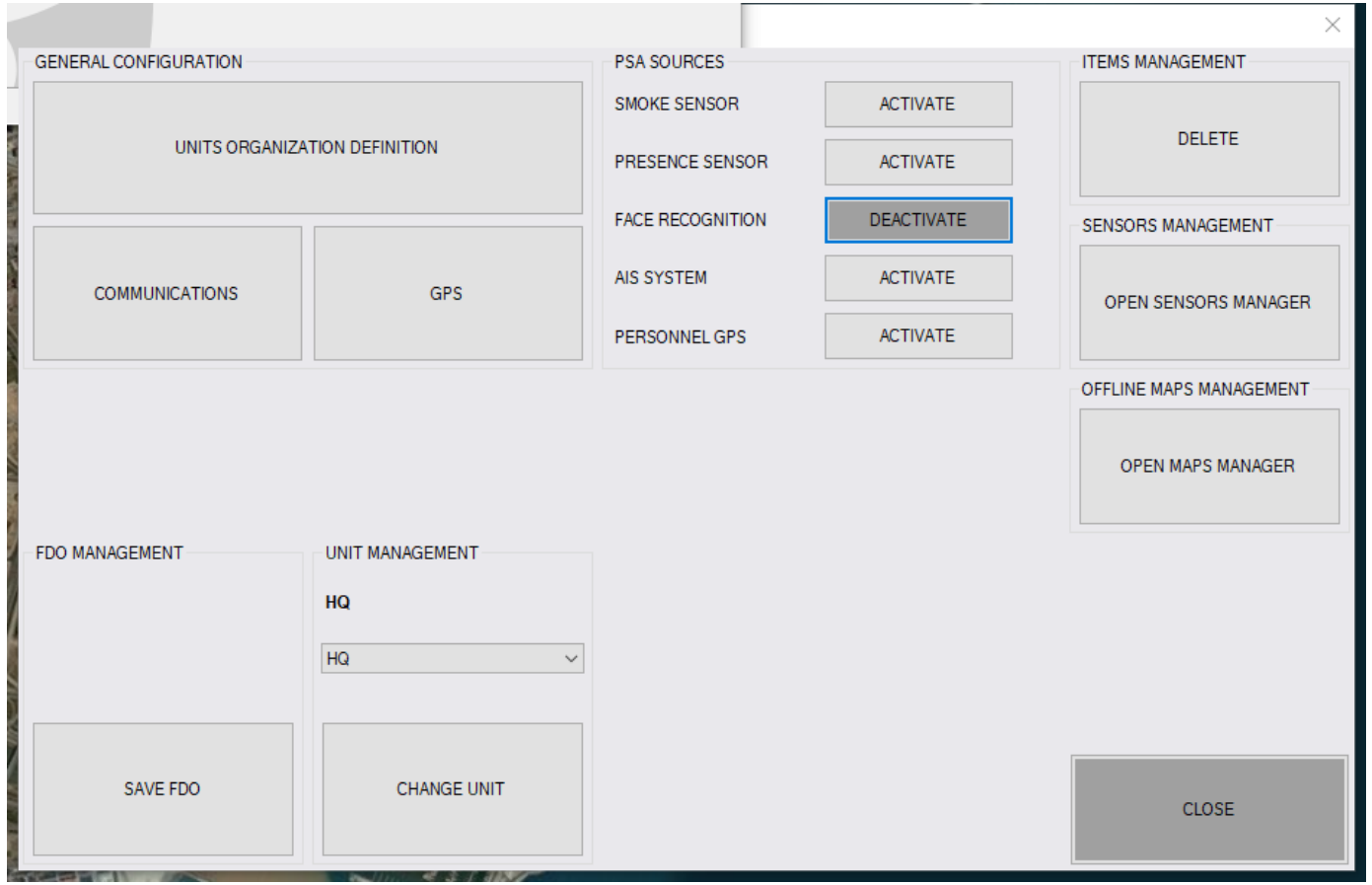
Valencia City Council Cameras Management ↔ PSA Sensors Manager ↔ SAURON PSA HMI

Sensors integration: Valencia City Council Video Cameras



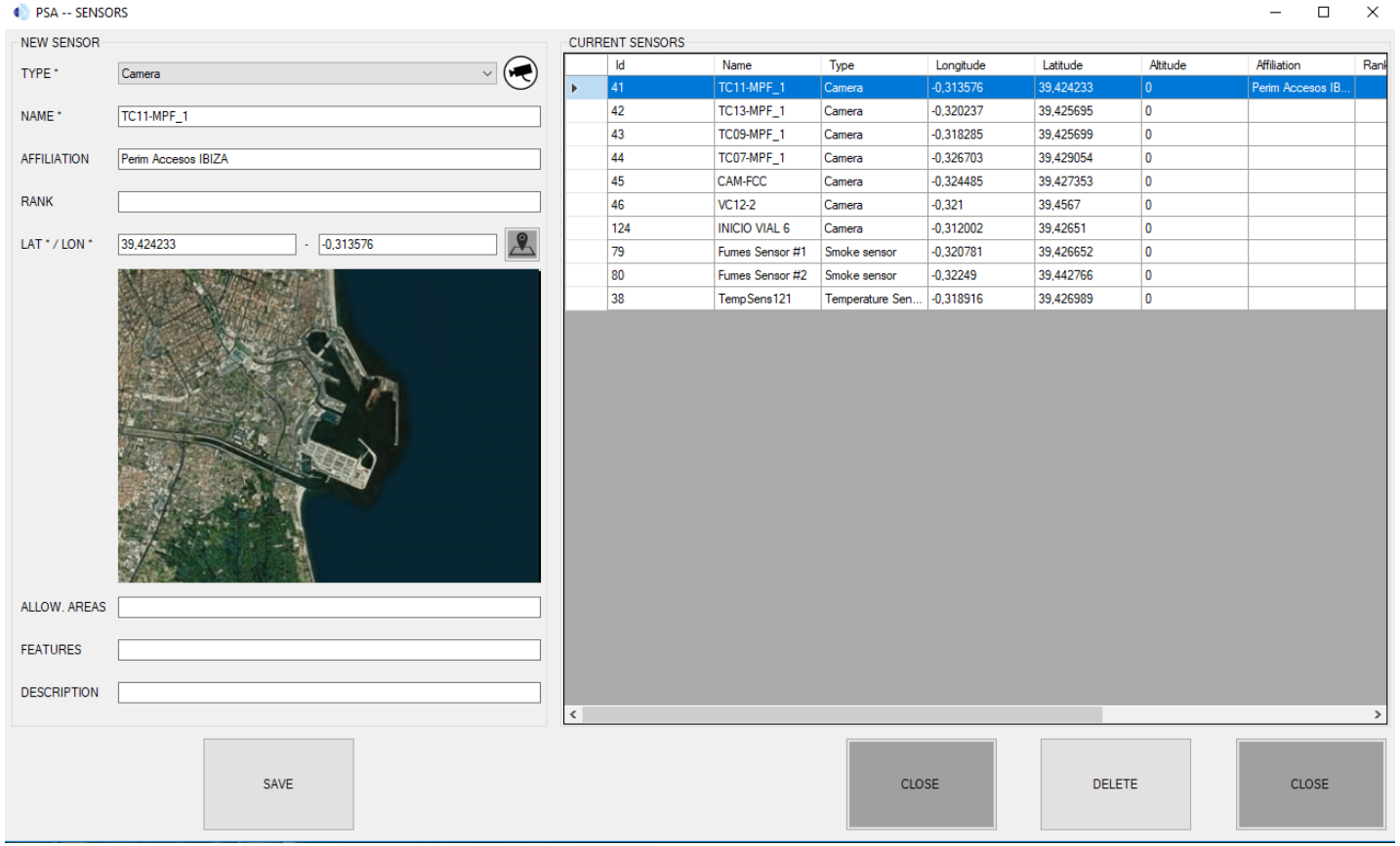
Sensors integration: Management

- Sensors communication activation/deactivation



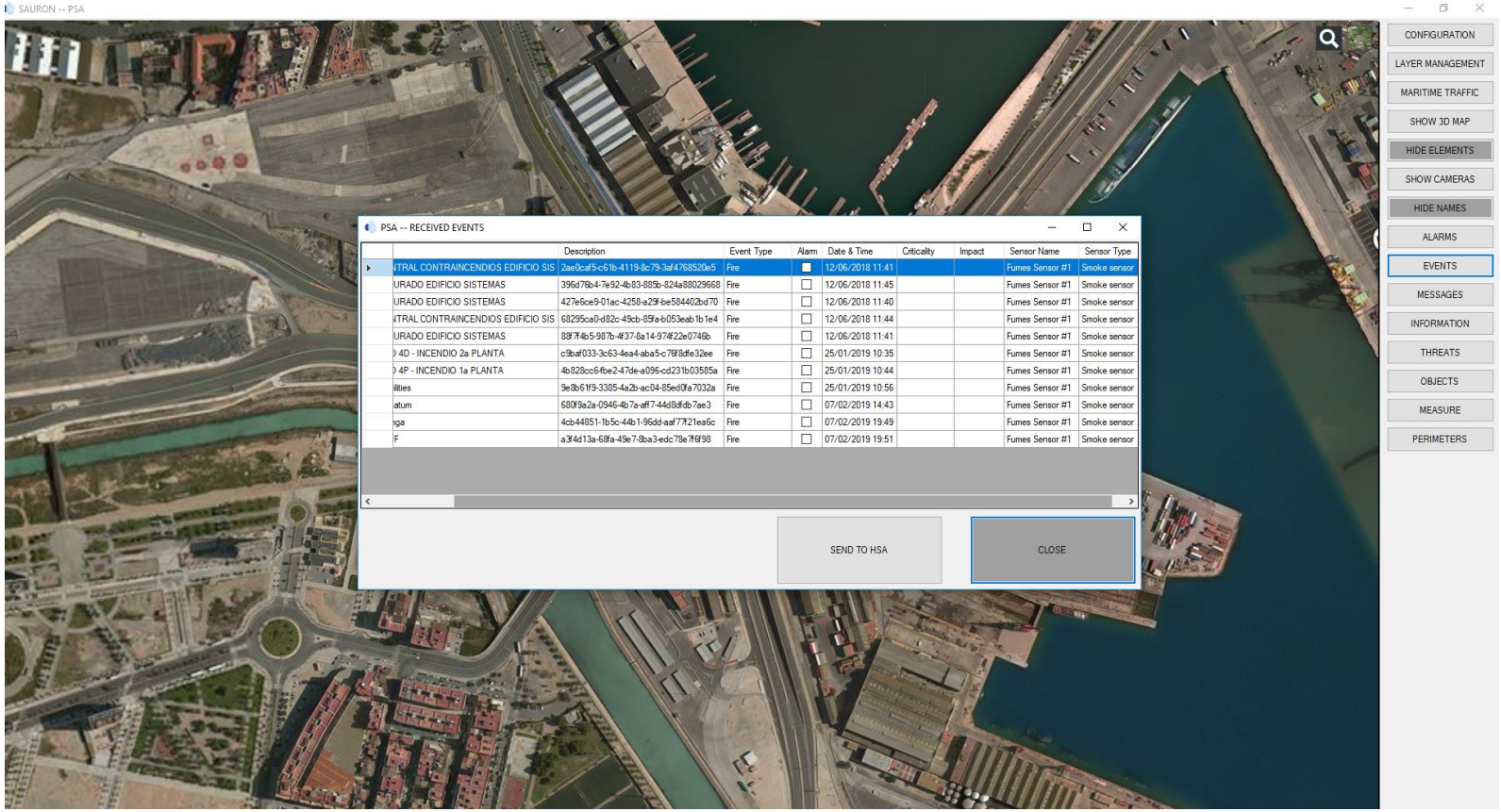
Sensors integration: Management

- Sensors management



Events delivery

- Events management & HSA Communication



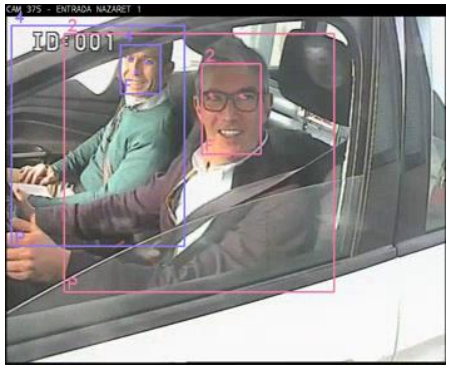
	Description	Event Type	Alarm	Date & Time	Criticality	Impact	Sensor Name	Sensor Type
NTRAL CONTRAINCENDIOS EDIFICIO SIS	2ae0caf5-c61b-4119-8c79-3af4768520e5	Fire	☐	12/06/2018 11:41			Fumes Sensor #1	Smoke sensor
URADO EDIFICIO SISTEMAS	396d76b4-7e92-4b83-885b-824a88029668	Fire	☐	12/06/2018 11:45			Fumes Sensor #1	Smoke sensor
URADO EDIFICIO SISTEMAS	427e6ce9-01ac-4258-a29f-be584402bd70	Fire	☐	12/06/2018 11:40			Fumes Sensor #1	Smoke sensor
NTRAL CONTRAINCENDIOS EDIFICIO SIS	68295ca0-d82c-49cb-85fa-b053eab1b1e4	Fire	☐	12/06/2018 11:44			Fumes Sensor #1	Smoke sensor
URADO EDIFICIO SISTEMAS	88f7f4b5-987b-4f37-8a14-974f22e0746b	Fire	☐	12/06/2018 11:41			Fumes Sensor #1	Smoke sensor
) 4D - INCENDIO 2a PLANTA	c9baf033-3c63-4ea4-aba5-c76f8dfe32ee	Fire	☐	25/01/2019 10:35			Fumes Sensor #1	Smoke sensor
) 4P - INCENDIO 1a PLANTA	4b828cc6-fbe2-47de-a096-cd231b03585a	Fire	☐	25/01/2019 10:44			Fumes Sensor #1	Smoke sensor
ilities	9e8b61f9-3385-4a2b-ac04-85ed0fa7032a	Fire	☐	25/01/2019 10:56			Fumes Sensor #1	Smoke sensor
atum	680f9a2a-0946-4b7a-aff7-44d8dfdb7ae3	Fire	☐	07/02/2019 14:43			Fumes Sensor #1	Smoke sensor
ga	4cb44851-1b5c-44b1-96dd-aaf77f21ea6c	Fire	☐	07/02/2019 19:49			Fumes Sensor #1	Smoke sensor
F	a3f4d13a-68fa-49e7-8ba3-edc78e7f6f98	Fire	☐	07/02/2019 19:51			Fumes Sensor #1	Smoke sensor

Face Recognition Innovation

- Live alerts for video surveillance
  - Detection/identification
  - Faces/persons/vehicles
  - Real-time
  - Network/IP cameras
  - Integration with PSA
- Innovative R&D
  - **AI (Artificial Intelligence) – DL (Deep Learning) – CNN (Convolutional Neural Networks)**
    - Multi-modal features (face, person, attribute, vehicle)
    - Identity fusion
    - Neural networks architectures / accuracy / optimizations (CPU, GPU)
    - Data management. Dataset of videos created, collected from Pixabay, Shutterstock…
  - UAV
    - Tests
    - Specific learning

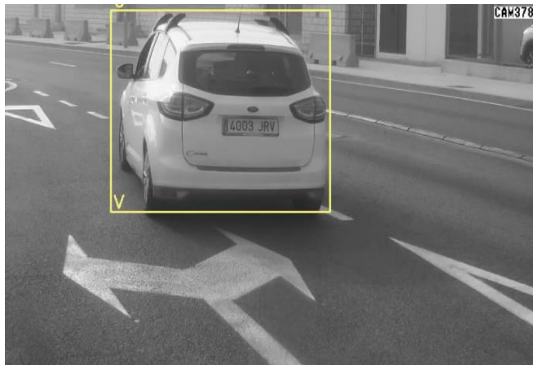
Live acquisition → detection → extraction → matching

Multi-objects detection and tracking by deep learning

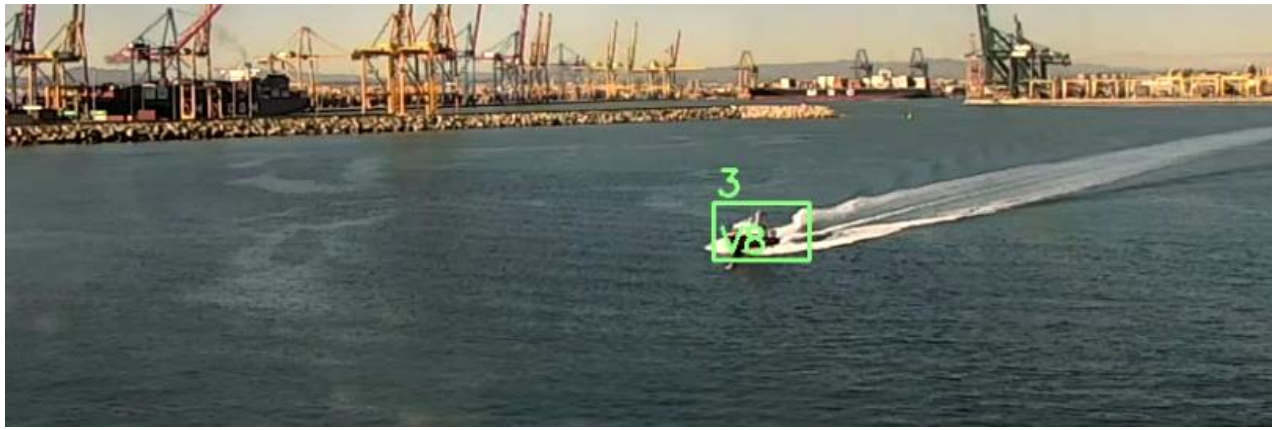


Face detection
Source VALENCIA PORT

Person detection
Source Luka Koper PORT

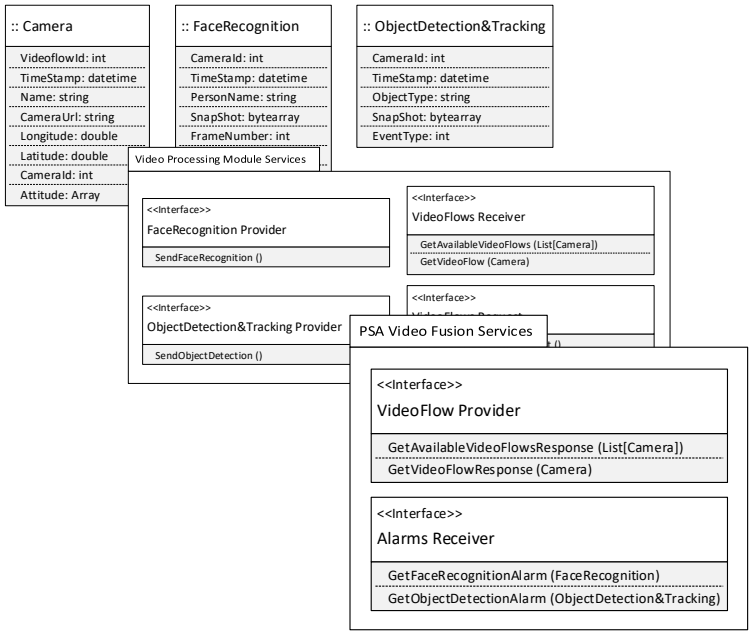


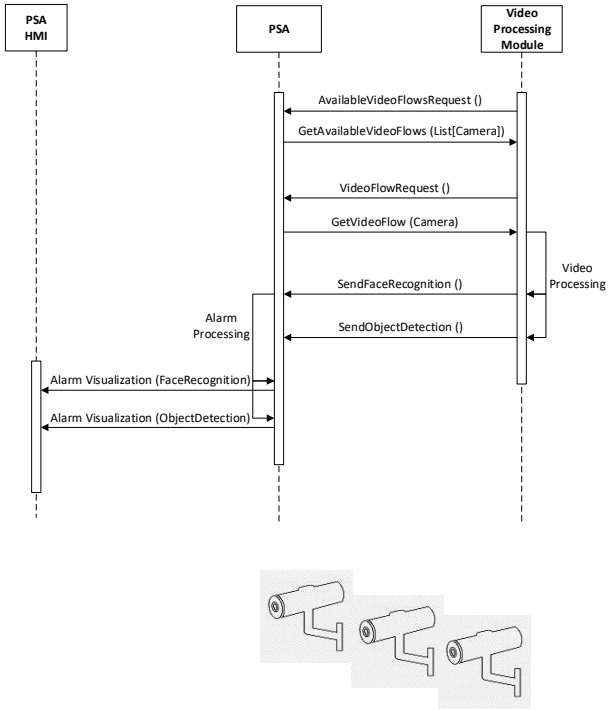
Vehicle detection
Source VALENCIA PORT



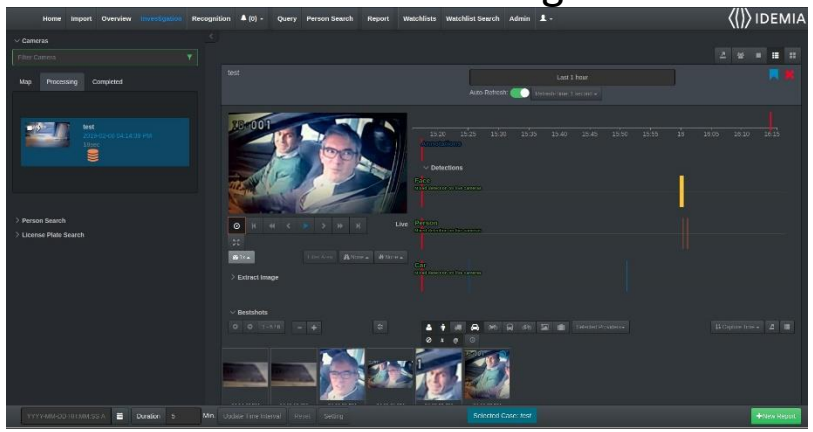
Boat detection
Source VALENCIA PORT

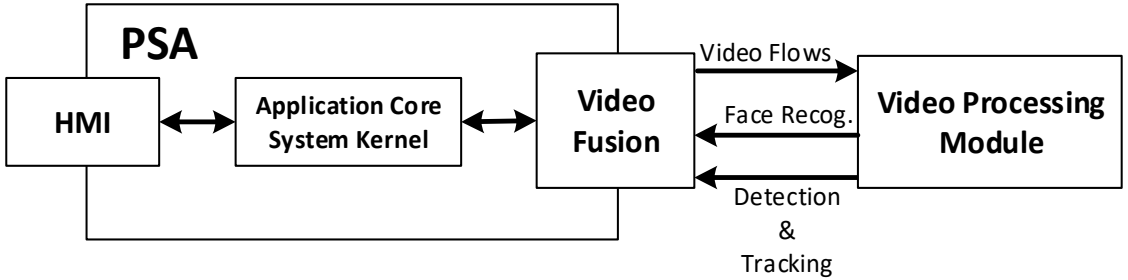
SAURON PSA integration





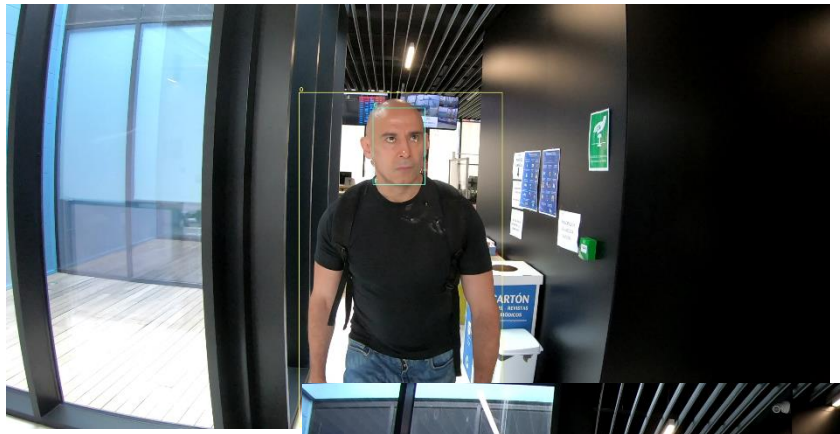
IDEMIA - Live monitoring interface

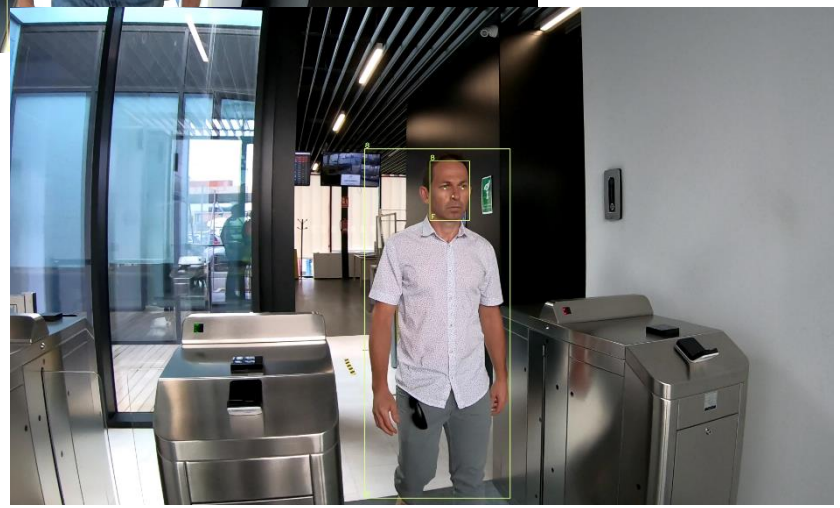




Valencia Scenario Pilot

- 2 persons detected – NOT in the “authorized” database → Alert
    - Good quality of the faces → camera positioning for face recognition
    - Cooperation of authorized person
    - Database < 10 000 personnes
    - Access control gates (doors)
- Other events
    - Person/vehicle detected in an area where/when nobody should be
    - Person recognized in a personal database (while list) and authorized
    - Person recognized in a personal database (while list) but **not** authorized
    - Person recognized in a “terrorist” database (black list)





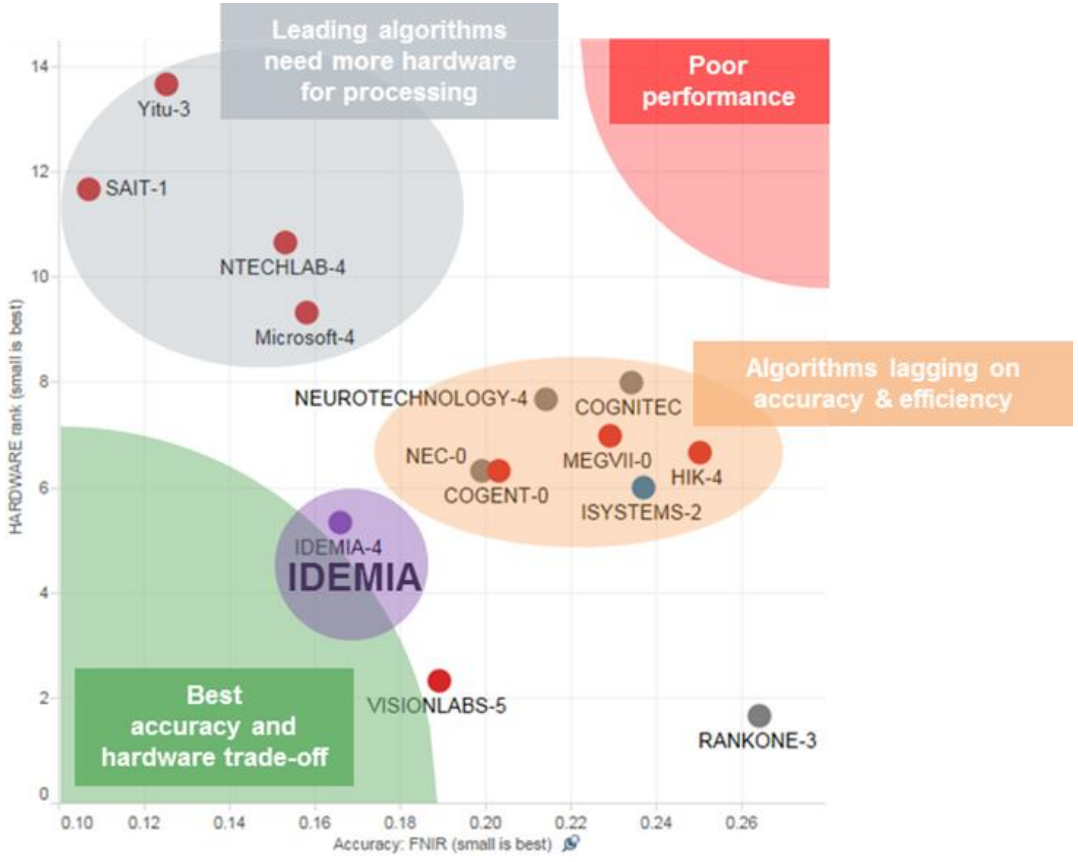
Face recognition benchmarking

- New technologies → new competitors

- Performances depend on
  - Use-cases
  - Cameras/devices deployments
  - Trade-off accuracy/hardware
  - Adaption to customer data

- Other NIST benchmarks & tests
  - FRVT (Face) 2020 – IDEMIA ranked #4
  - IREX 10 (Iris) 2020 – IDEMIA #1
  - Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture (Fingerprint) 2019 – IDEMIA ranked #1

NIST benchmark FRVT = Face Recognition Vendor Test 1-N (2nd semester 2018)



Hardware Rank vs Accuracy FNIR (False Negative Identification Rate)

Cyber Situation Awareness (CSA)

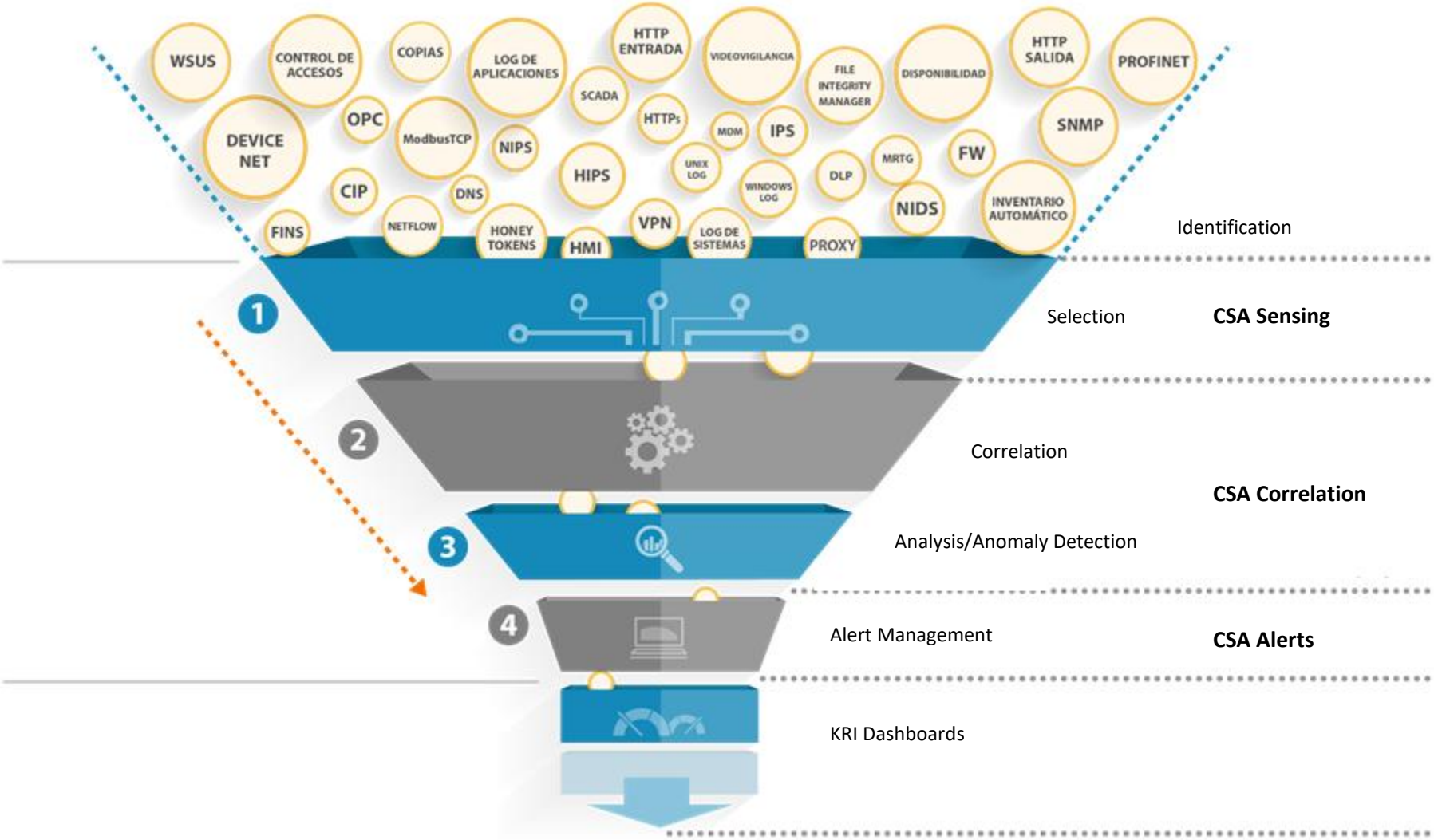
Sergio Zamarripa [S2]

Summary Table

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.

CSA Sensing → Security monitoring information gathering
CSA Correlation → Automatic cyber incident detection in real-time
CSA Alerts → Cyber incident and alert management
CSA Visualization - Cyber view → Advanced visualizations techniques. HMI from multi-dimensional approach to improve CSA

CSA Layers: Information Processing



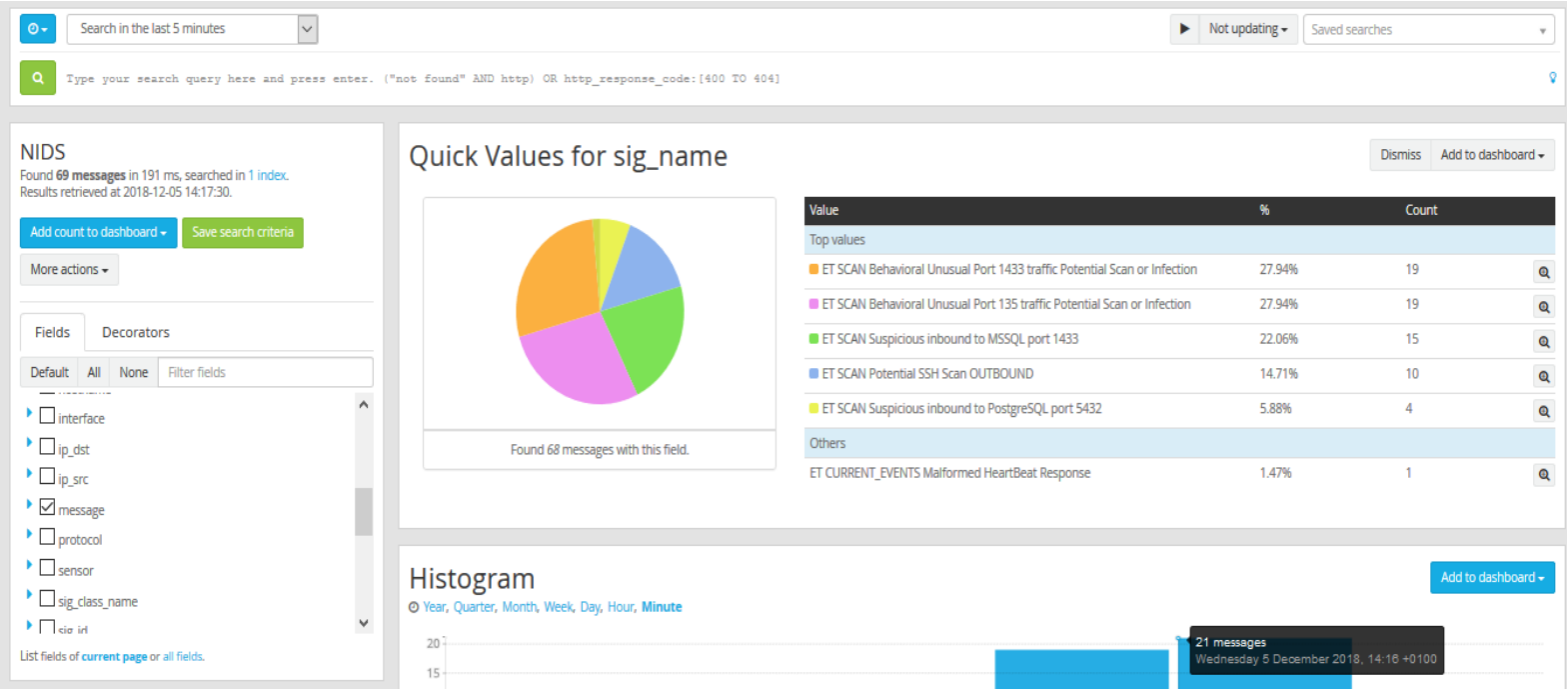
Main technologies and libraries

- CSA Sensing (php, Python)
  - Graylog
  - Sensors: NIDS (Suricata), HIDS (OSSEC), Vulnerability (Nessus)
- CSA Correlation (Java)
  - Drools (correlation engine)
  - Spring Integration
- CSA Alerts (Java)
  - Google Web Toolkit

CSA Sensing Module

Monitoring threats (NIDS and HIDS):

UC15 IT Monitoring
UC16 Low fingerprint



CSA Correlation Module

Automatic alert generation (without human intervention):

WHEN

1. New DMC security event
   - destination user starts with dad-
   - Event id code indicates log in failed
   - canal no debug
2. DC alerts 4 times in less than 3 seconds
   - For the same user
   - Event id code indicates log in failed
   - destination user starts with dad-
   - destination user matches DMC Event
   - canal no debug
3. There is no DMC alert in last hour from same rule RULE01 user and source

THEN

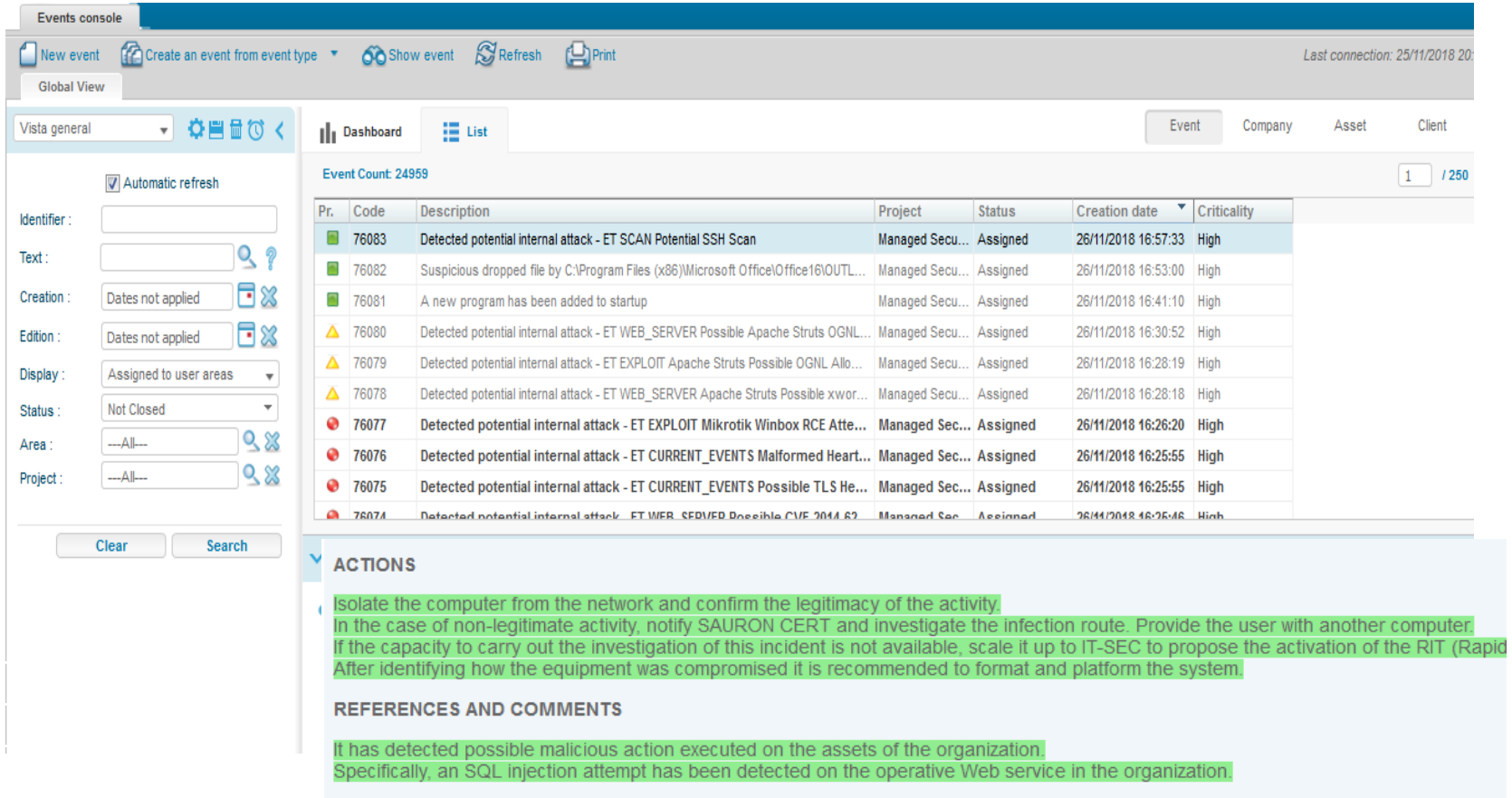
1. Log DMC security matched rule
2. Disable the creation of these DMC alerts for this User And Source for one hour
3. Send List Formatted Email to group RULE01 for rule RULE01
4. Attach sent mail as worknote
5. Generate DMC event to EMas EBS: Commitment of user accounts Buscar Criticality LOW Subject DMC-01 Domain Admin failed login attempt

UC16 Low fingerprint

UC18 Security Alert Generation

CSA Alerts Module

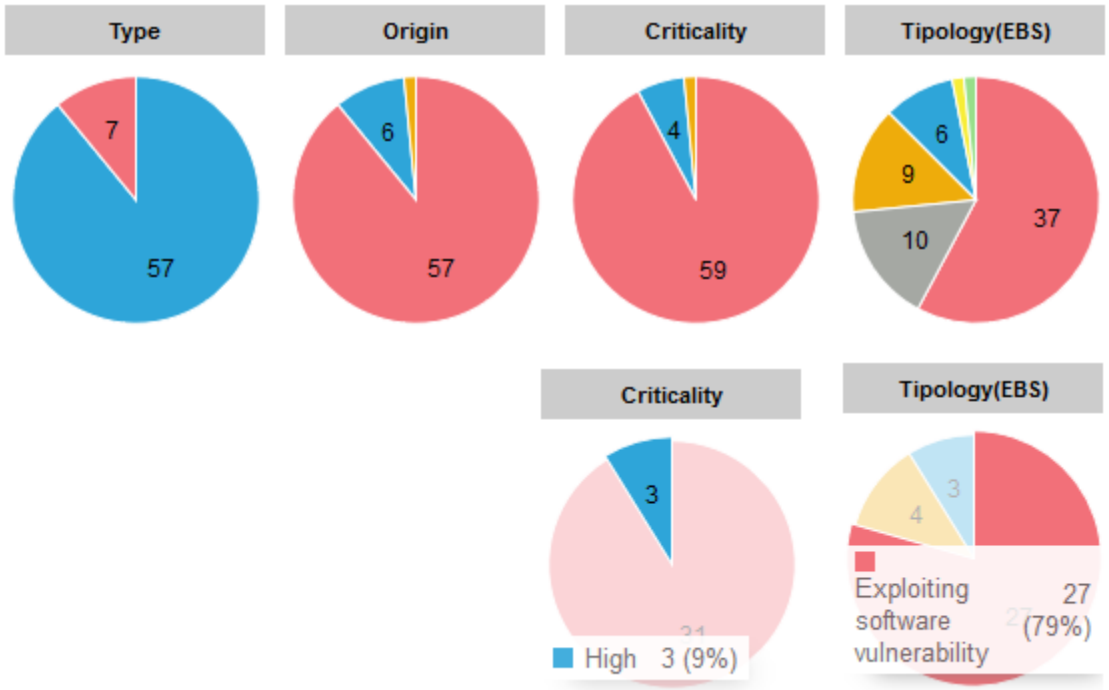
Alert management: interacting with port office without impact



UC18 Security Alert Generation
UC19 Alert Management
UC20 Export Information

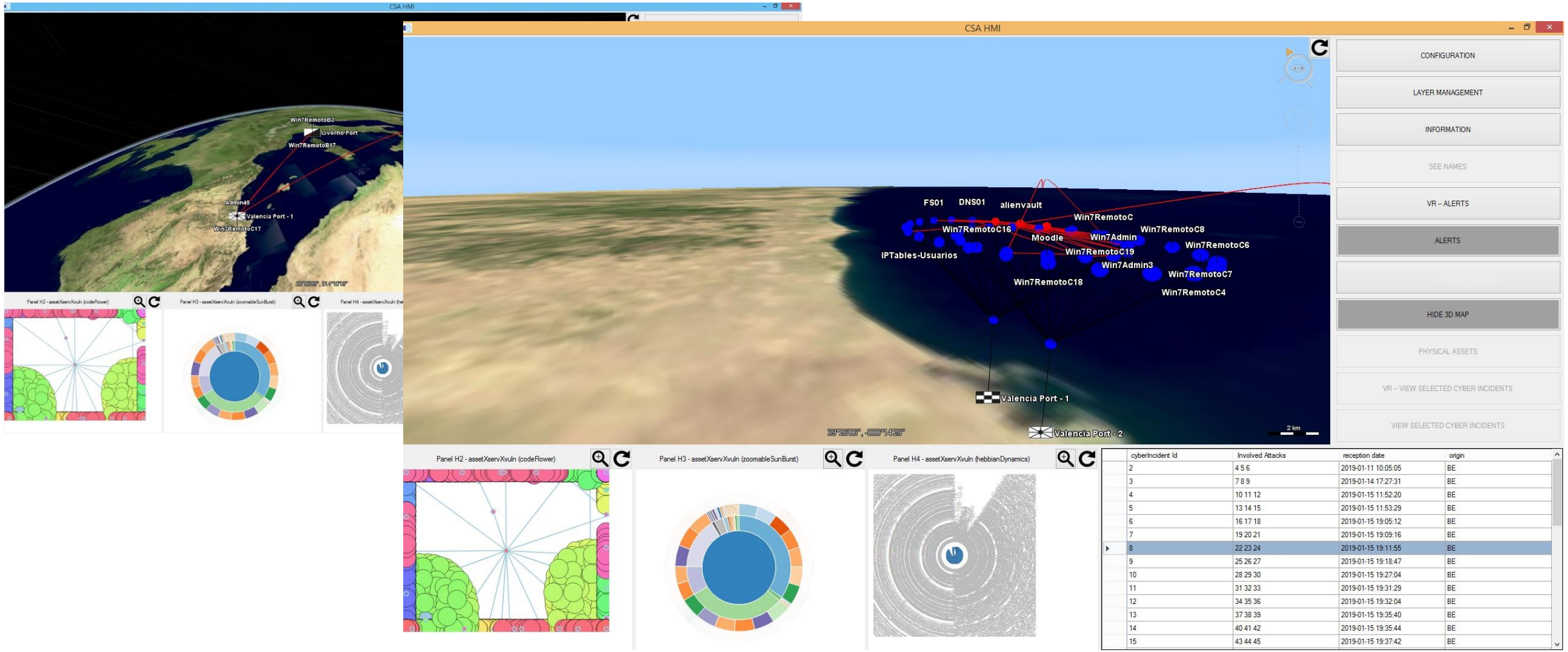
CSA Alerts Module

Alert management: Situational risk



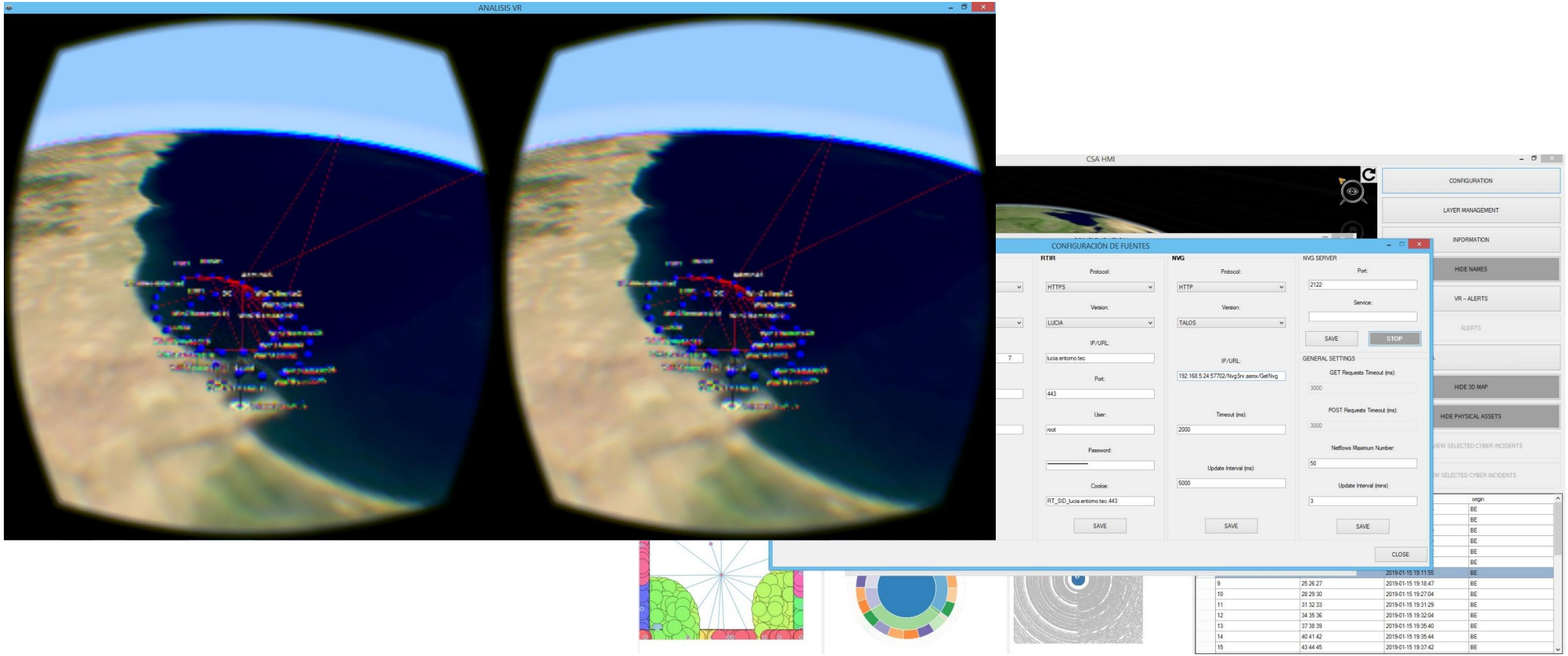
UC18 Security Alert Generation
UC19 Alert Management
UC20 Export Information

CSA Visualization: Cyber view

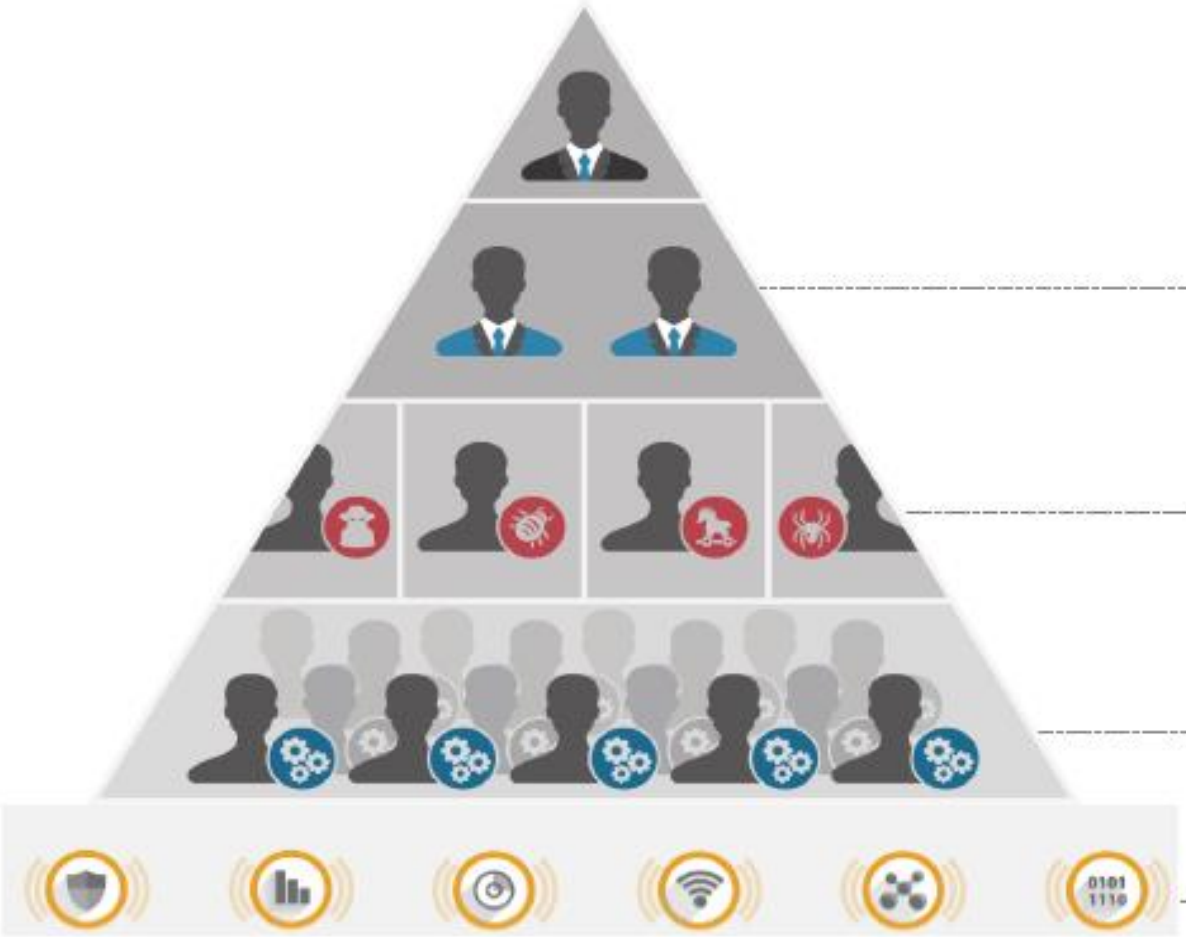


cyberIncident Id	Involved Attacks	reception date	origin
2	4 5 6	2019-01-11 10:05:05	BE
3	7 8 9	2019-01-14 17:27:31	BE
4	10 11 12	2019-01-15 11:52:20	BE
5	13 14 15	2019-01-15 11:53:29	BE
6	16 17 18	2019-01-15 19:05:12	BE
7	19 20 21	2019-01-15 19:09:16	BE
8	22 23 24	2019-01-15 19:11:55	BE
9	25 26 27	2019-01-15 19:18:47	BE
10	28 29 30	2019-01-15 19:27:04	BE
11	31 32 33	2019-01-15 19:31:29	BE
12	34 35 36	2019-01-15 19:32:04	BE
13	37 38 39	2019-01-15 19:35:40	BE
14	40 41 42	2019-01-15 19:35:44	BE
15	43 44 45	2019-01-15 19:37:42	BE

CSA Visualization: Cyber view



CSA team organization



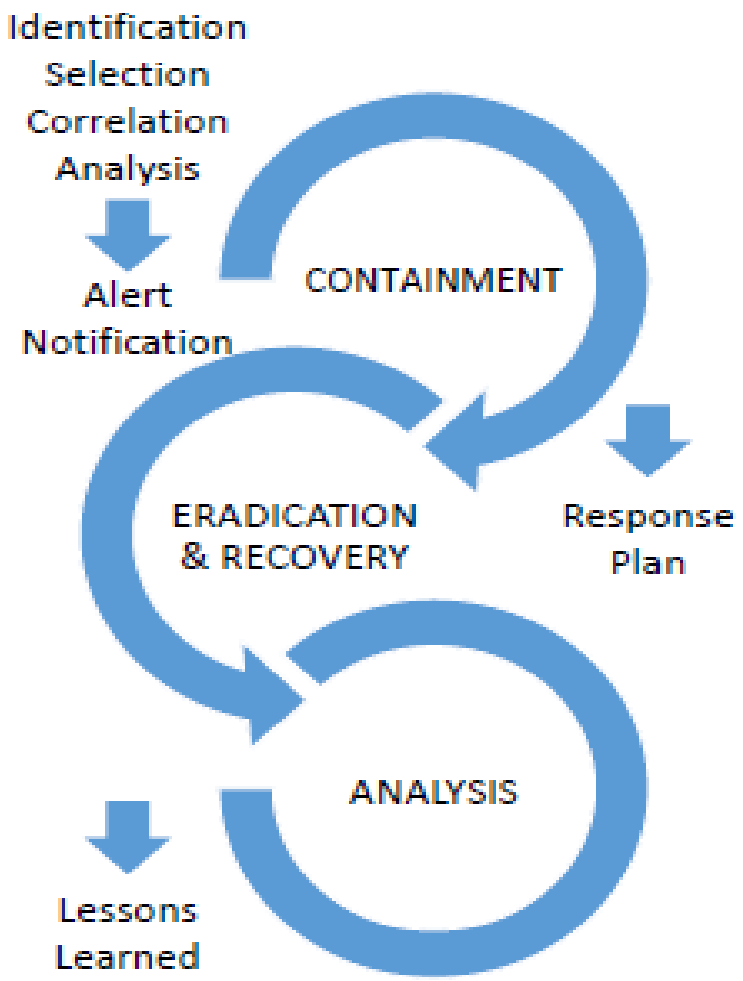
TIER 3
Coordination & Management
Vendor support
Specialized incident and threat hunting performed by subject matter experts

TIER 2
Anomaly detection by security analysts and incident responders

TIER 1
Misuse detection by security operators and alerts analysts
Standard Operation Procedures (SOP)

TIER 0
Automatic event monitoring, collection, correlation and datamining

CSA Incident Response



Advance beyond SoTA – Innovative items

- Visualization techniques
  - Alert location map view, Network-oriented cyber-incident view (typology code of colours allow to **identify incident at a glance**). We can visualise: Where? What? How? Who? And now what?
  - **Impact visualization** (asset vulnerabilities)
- Seaport cyber critical infrastructure
  - **External awareness** of possible port authority targets
  - Enhance **real-time cyber-incident detection** over seaport infrastructures
  - Cyber-incident contextualization and **required action guidance**
  - **Scalable** (for small and big IT Security Teams)

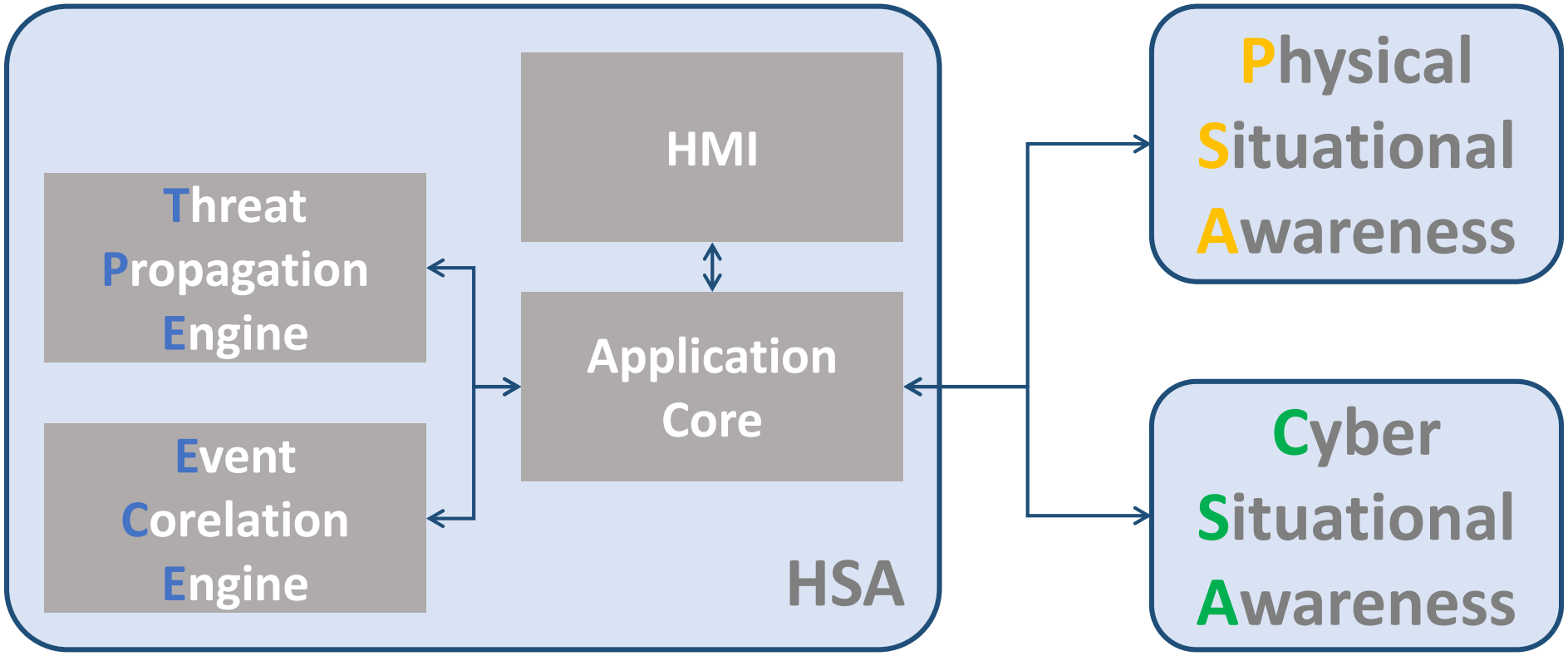
Hybrid Situation Awareness (HSA)

Romain Caillière [THALES]
Stefan Schauer [AIT]

HSA : Hybrid Situational Awareness

Combined **physical** and **cyber events to enhance** the **situational awareness**

« The whole is greater than the sum of its parts »



Application Core

- **The Application Core module manages the communication of the system**
  - Checks the validity of the messages, invalid messages are not propagated
  - Route them to the correct subscriber, misrouted messages are not propagated
- **Designed to follow the system evolution**
  - Easy to integrate new types of messages,
  - Easy to integrate new HSA modules dealing with events and alerts coming from PSA or CSA,
  - Easy to integrate new modules outside the HSA that needs to exchange with the HSA.
- **Easy to update and maintain**

Application Core functionalities

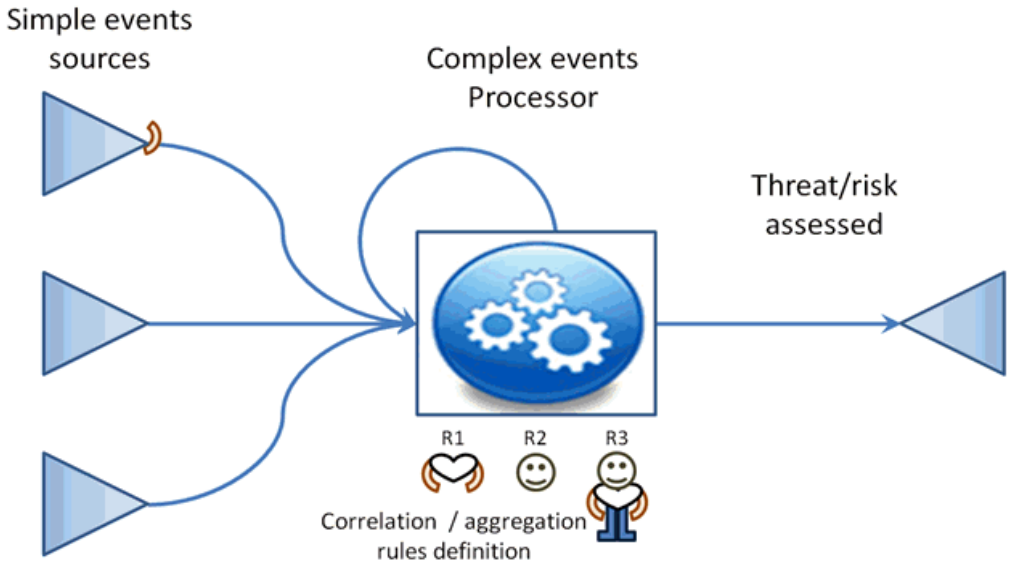
- **Validate messages before routing them**
  - Gives confirmation that messages are sent
  - Gives confirmation that messages are received and valid
  - Provides content of messages

- **Gives an overview of the status of the exchange server**
  - Monitor users connections
  - List the current connections
  - Monitors all exchanged messages going through the broker

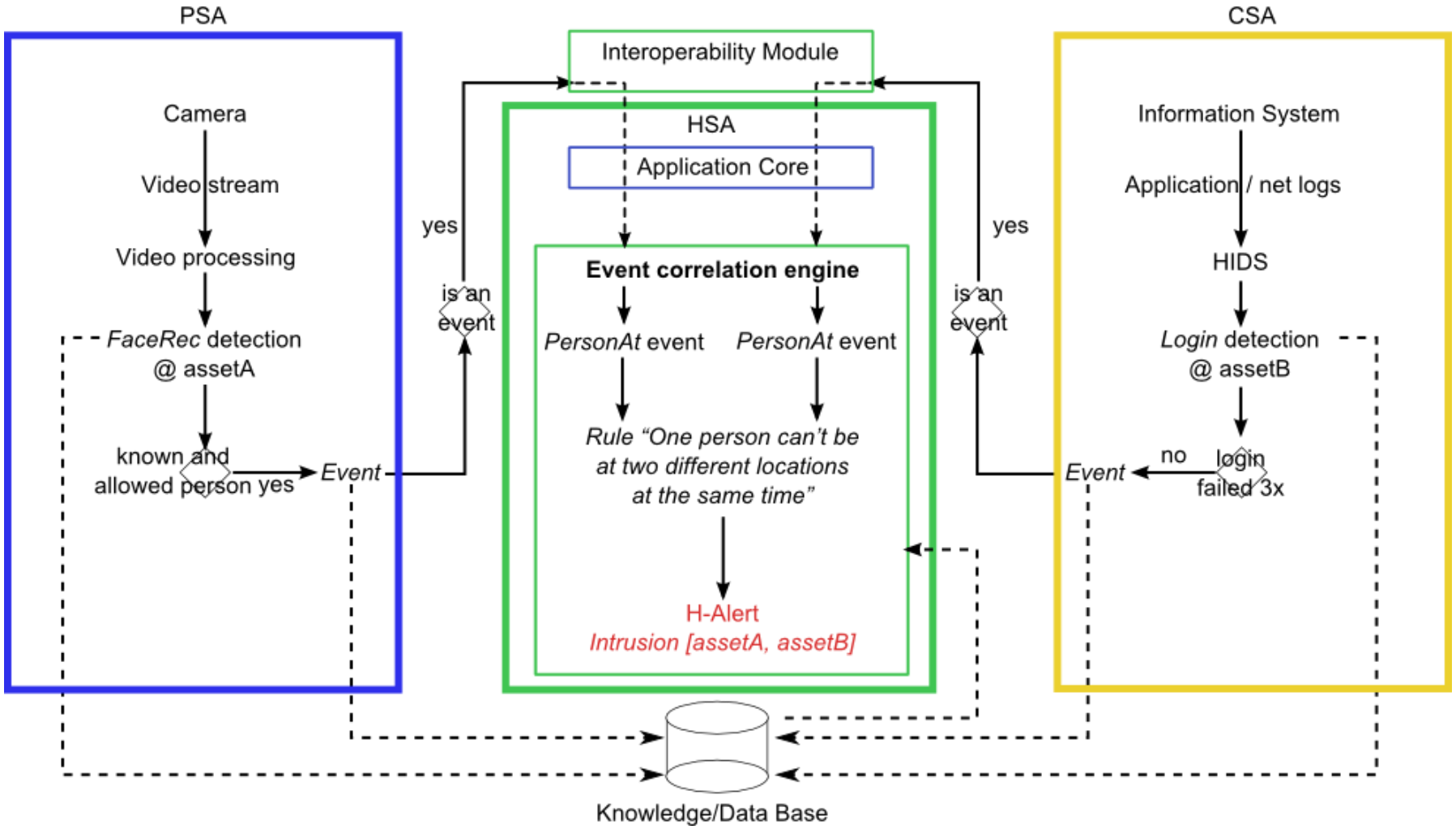
Event Correlation Engine

- The ECE identify **related** cyber and physical **events**

- Automated **reasoning** engine to **enhance hybrid** situational **understanding**
  - It **receives** the **messages** from the **physical** and **cyber** monitors,
  - It **interprets** and **correlates** them, depending on **conditions** and **filters**,
  - It **triggers alerts**, based **on inconsistency** analysis.



Scenario for hybrid correlation

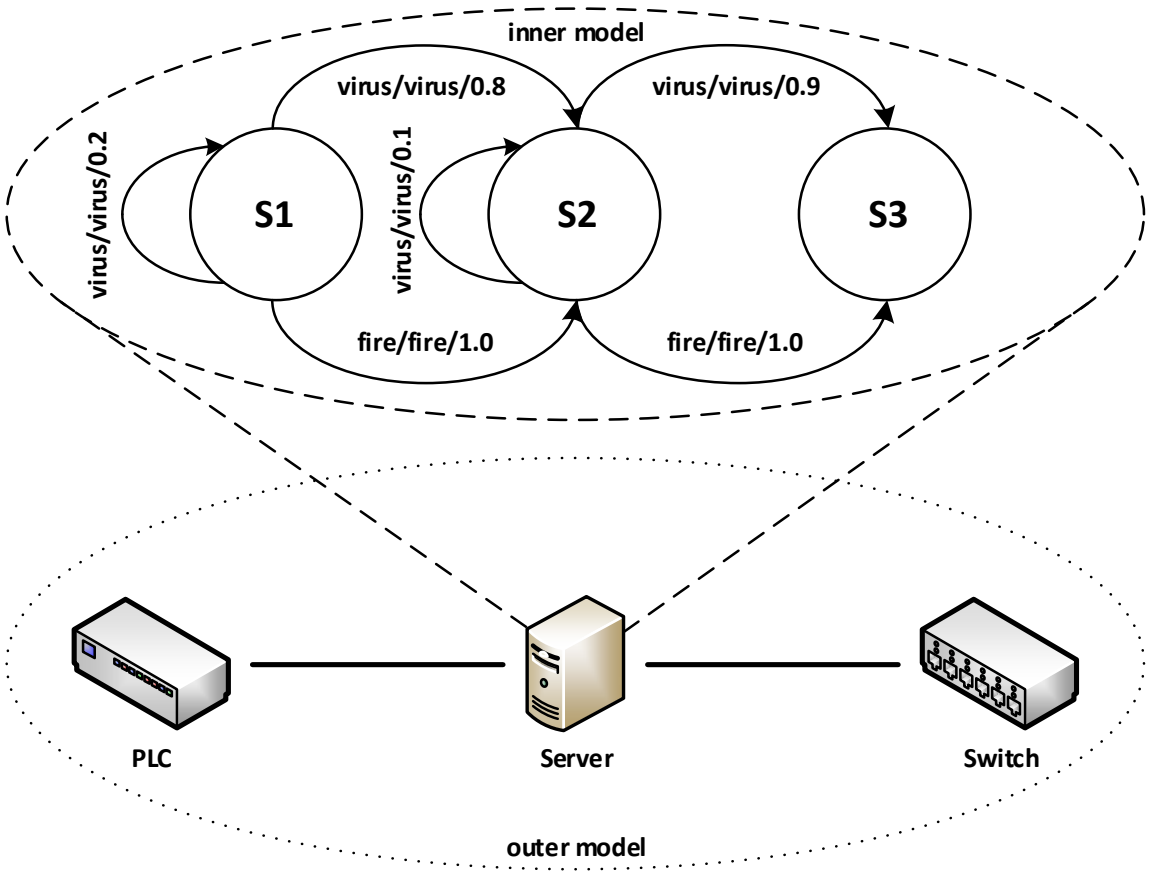


Added values of Event Correlation Engine

- **Correlation**
  - From all events and alerts the system is able to detect inconsistencies
  - Correlations can combined several events and alerts following different patterns
- **Hybrid correlation**
  - PSA and CSA are aware of there specific parts but some failures can still exist
  - When evidences of known-people activities from CSA is **as usual** (e.g., login)
  - When evidences of known-people activities from PSA is **as usual** (e.g., card reader)
  - **BUT** the combination about same people is **NOT as usual** => **spatial-temporal inconsistency**
- **The system takes into account only interesting information**
  - In this case spatial-temporal events

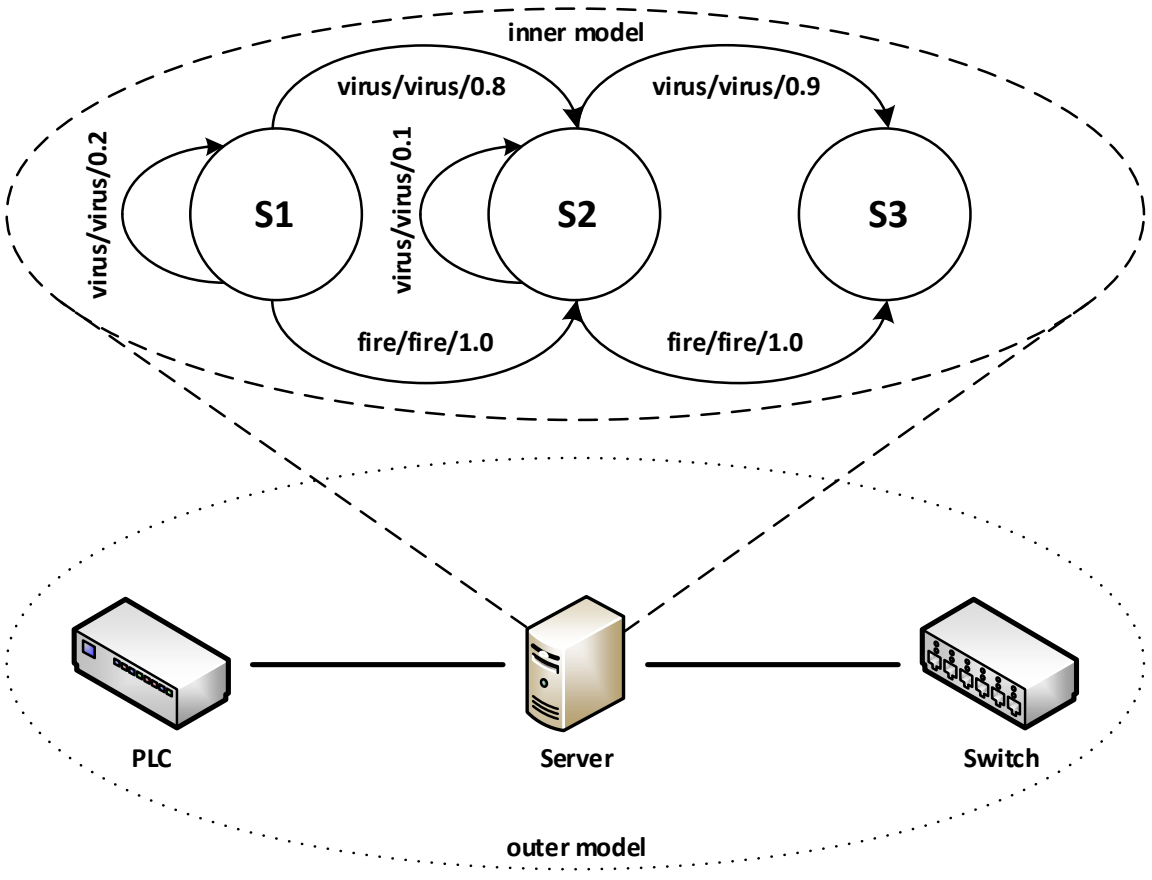
Threat Propagation Engine

- The Hybrid Threat Propagation builds upon a **graph representation** of the critical infrastructure's physical and cyber assets and their interconnections
- Assets can be in different states describing their **operational condition**
- Alerts from the Physical and the Cyber Situational Awareness are collected to model **cascading effects**



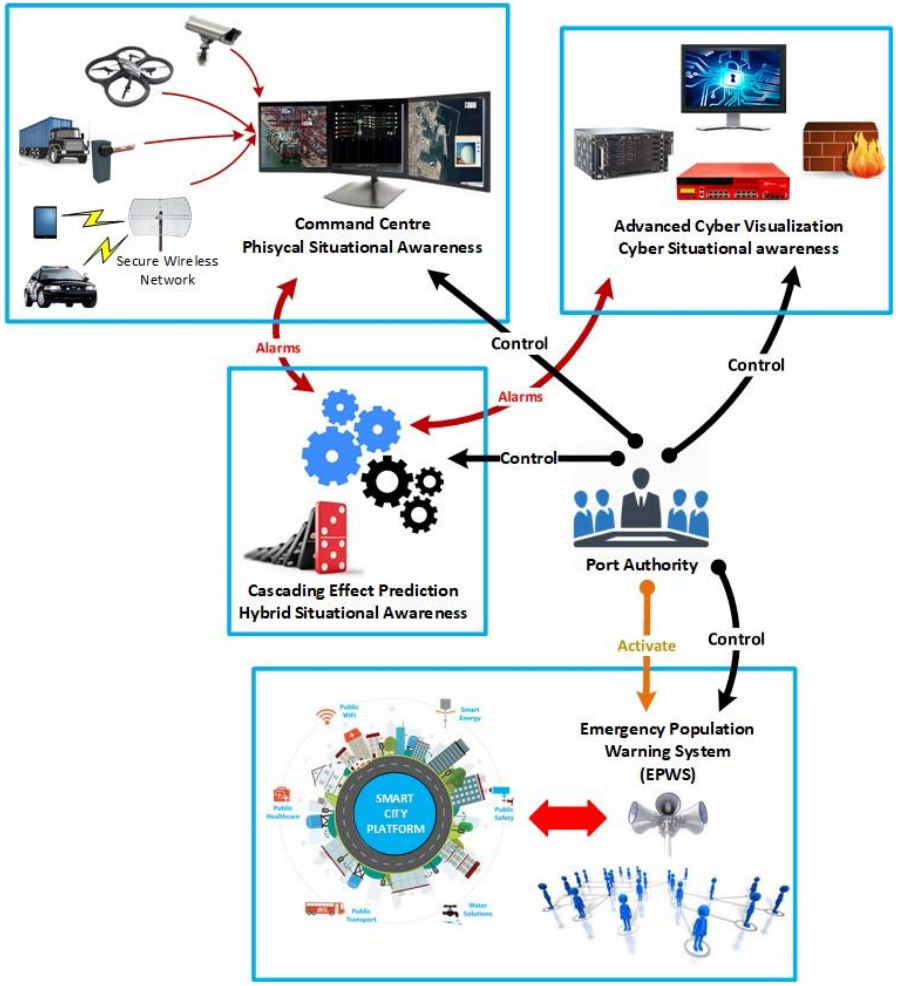
Threat Propagation Engine

- Estimation of the impact of the cascading effects is done using a **simulation approach**
- Incident/attack changes the **operational state** of the target asset
  - Dependent assets **change their state**, too (according to the probability distribution)
  - Effects of the incident **propagate** through the infrastructure's assets the network
- Total impact is measured based on the **final state of all assets** after the simulation has finished



Hybrid Situational Awareness

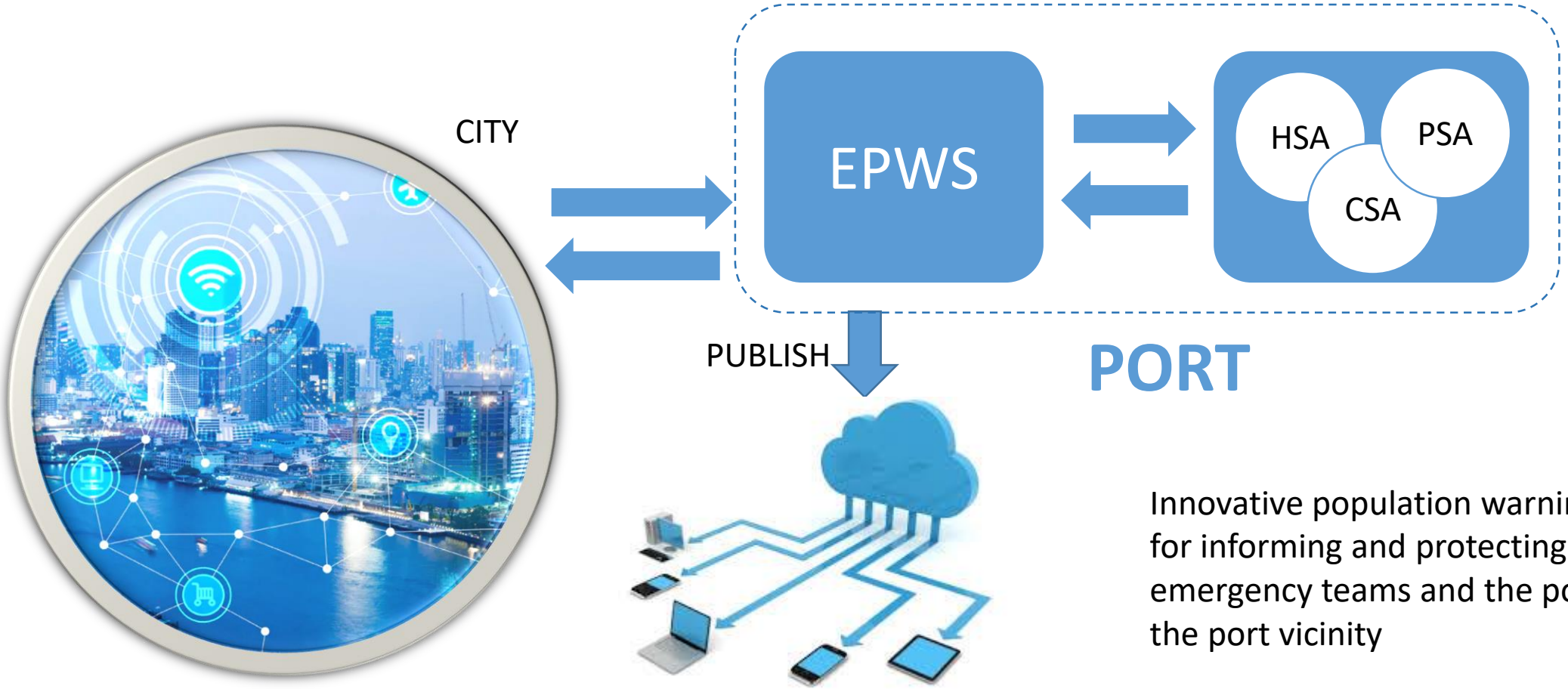
- Hybrid Situational Awareness facilitates the detection of complex sophisticated attacks
  - HSA **combines information of both physical and cyber** situational awareness
  - HSA **correlates incidents** that are otherwise **not taken into account** by individual physical and cyber situational awareness systems
  - HSA indicates **cascading effects** across the physical and cyber domain
- HSA **recommends mitigation actions** to counter sophisticated attacks
- Main goal of the SAURON project is to
  - support security officers within **critical infrastructures**
  - keep **emergency organizations** updated on incidents



Emergency Population Warning System (EPWS)

Jordi Arias [ETRA]

EPWS General Overview



Innovative population warning techniques for informing and protecting the emergency teams and the population in the port vicinity

EPWS Goals

- ❖ Integrability
- ❖ Quickness
- ❖ Easiness
- ❖ Specificity

- Flexibility to integrate with City Platforms by configuration. E.g. FiWare platforms
- Flexibility to integrate with Vertical Control Systems in cities: Traffic system, Information Systems, 112 … by customized data schemas and web services
- Publish text feed in CAP (Common Alert Protocol) format
- Publish on message public networks.
- Use of workflow systems to manage incidents specifically for each type and for each city/port

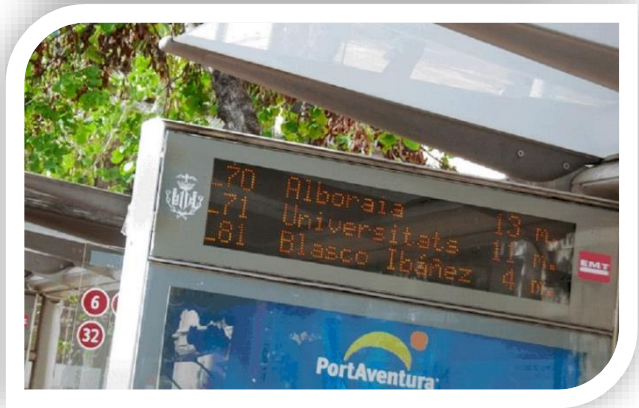
EPWS Function

Alarm → Validation → Categorize the Information → Notify

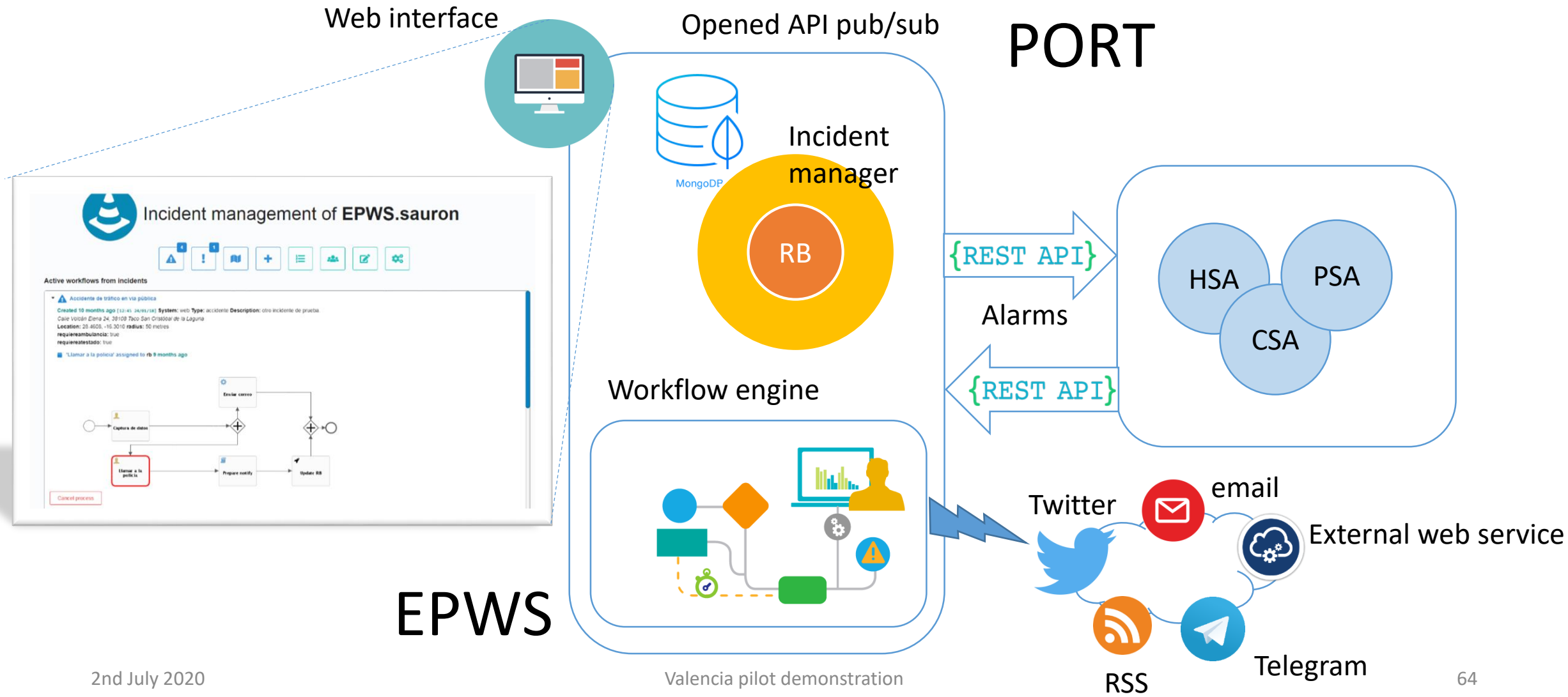
Validation → PORT

EPWS

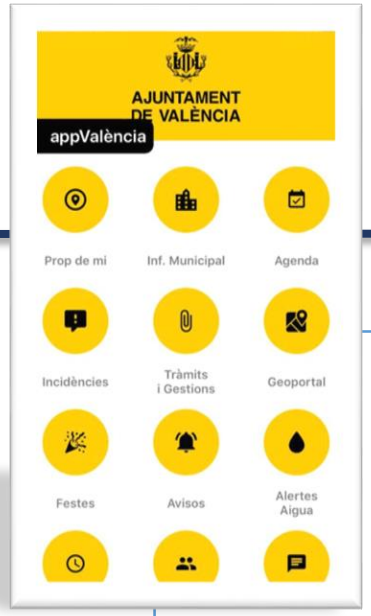
PSA,CSA,HSA



EPWS ⇄ PORT


Web interface
Opened API pub/sub
PORT
Incident manager
MongoDB
RB
Workflow engine
{REST API}
Alarms
{REST API}
HSA
PSA
CSA
Twitter
email
External web service
RSS
Telegram
EPWS
Incident management of EPWS.sauron
Active workflows from incidents

CYTY ⇄ EPWS



Traffic System

Transport System

Voice System

Opened API

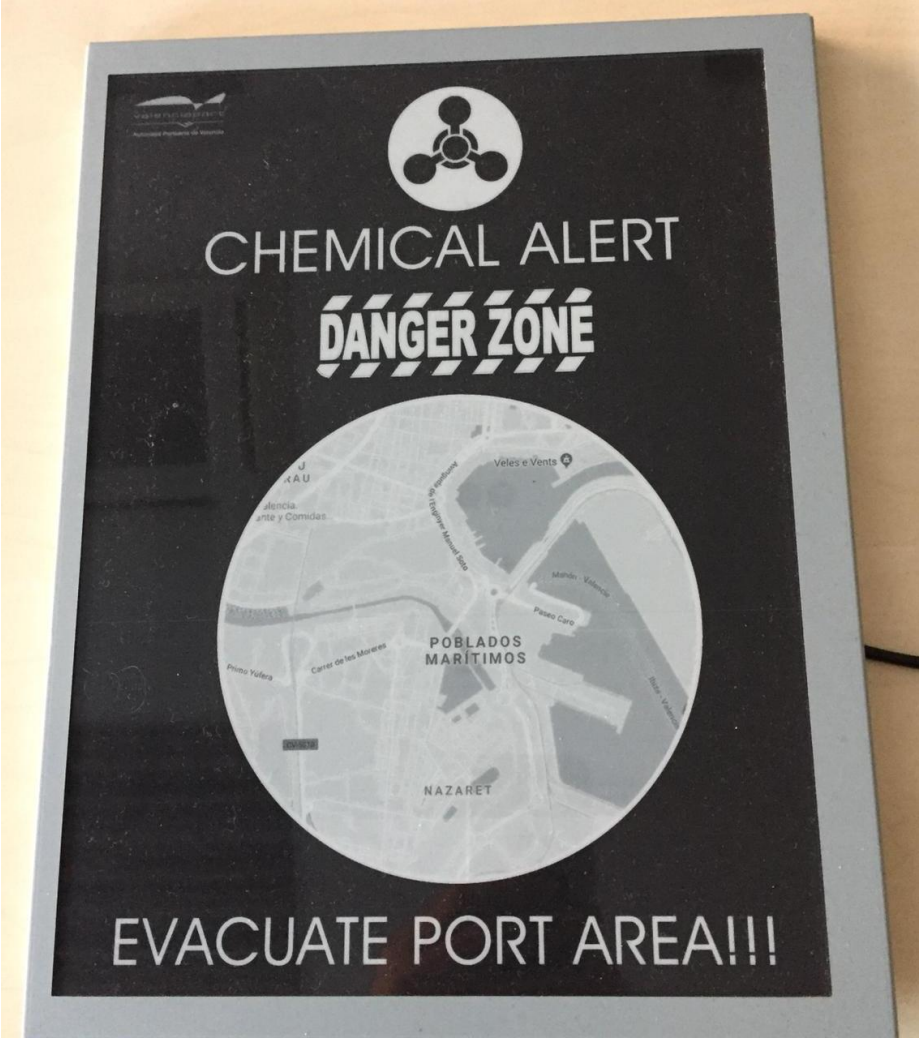
Incident manager

RB

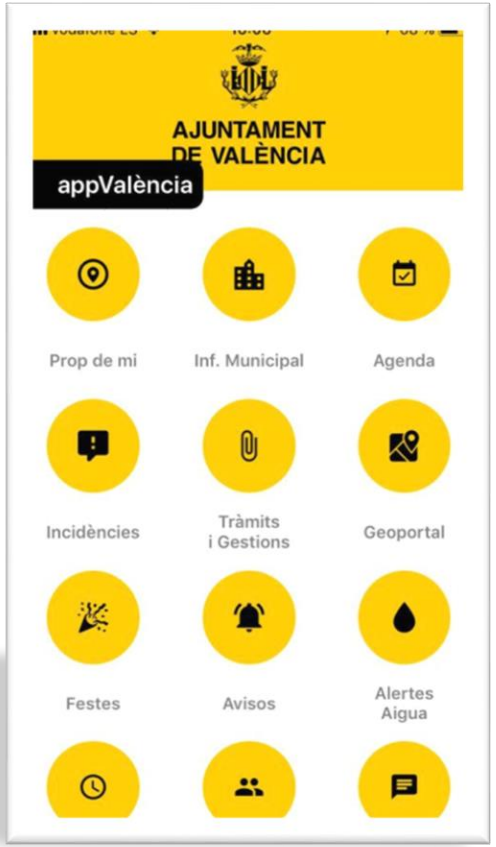
Workflow engine

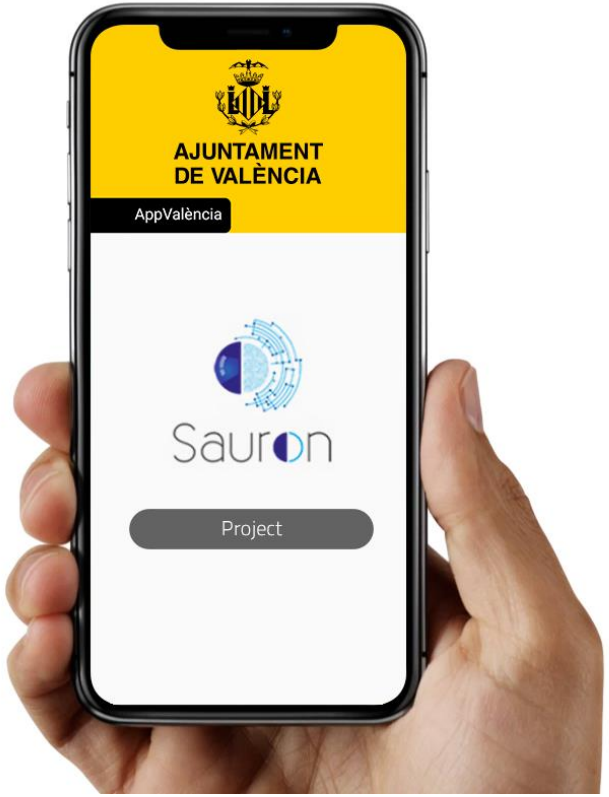
EPWS

Alert on Public transport system



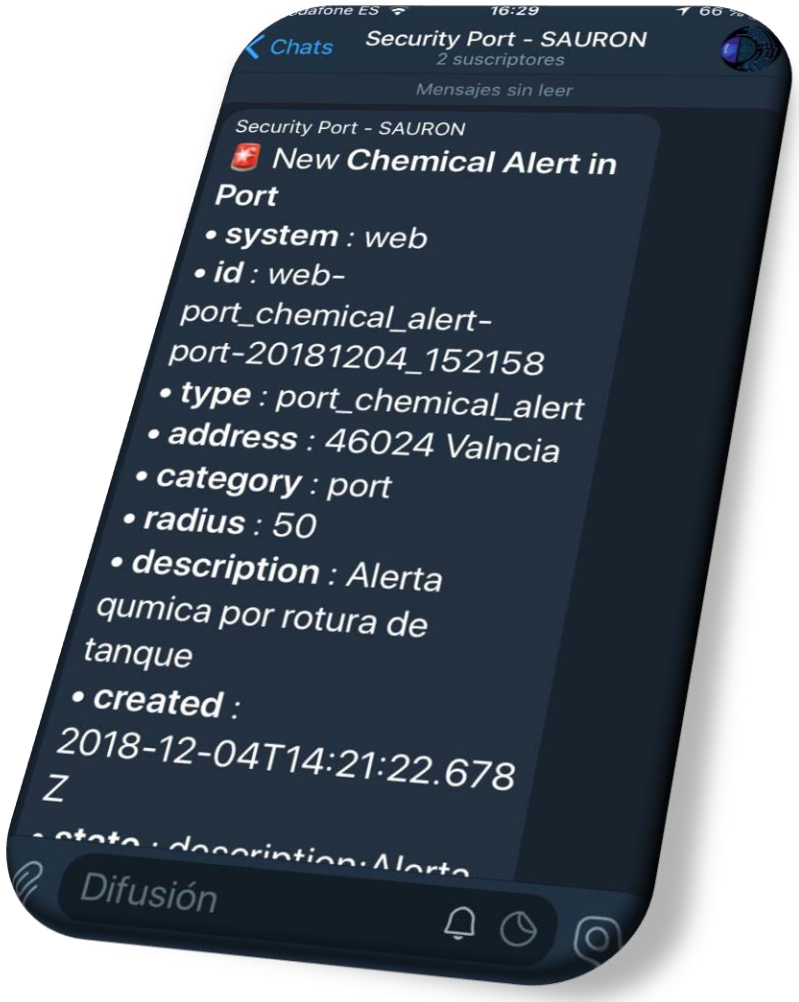
Alert on Valencia App





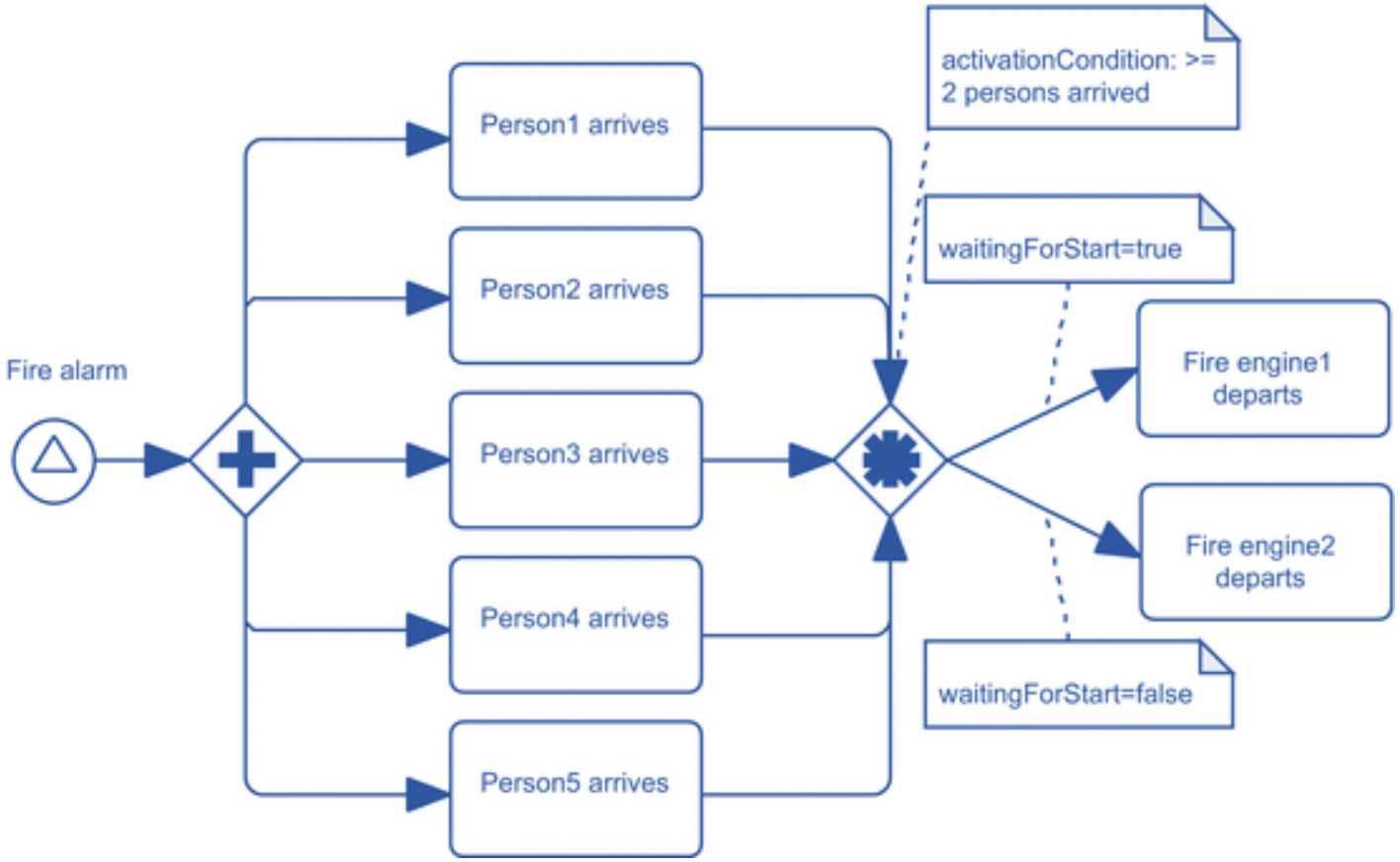
Alert on Traffic system

Private/Public-Telegram channels



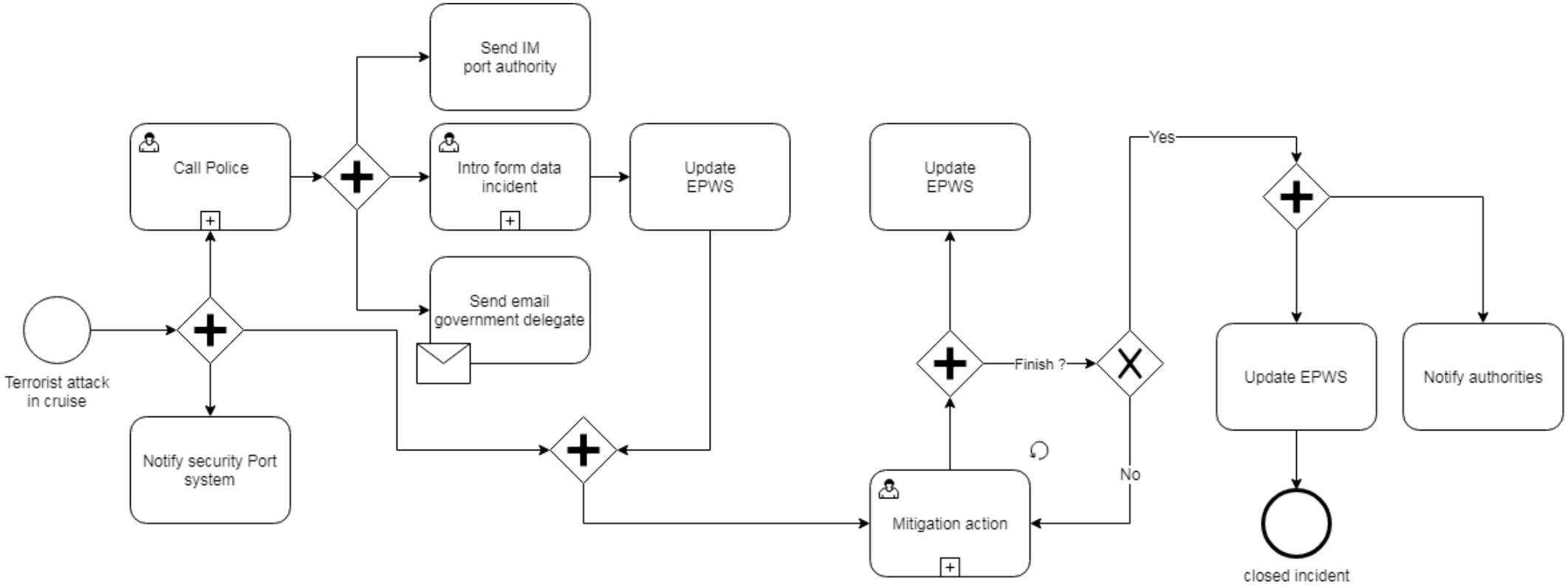
- ✓ Rescue teams
- ✓ Police
- ✓ Firefighters

Workflow process



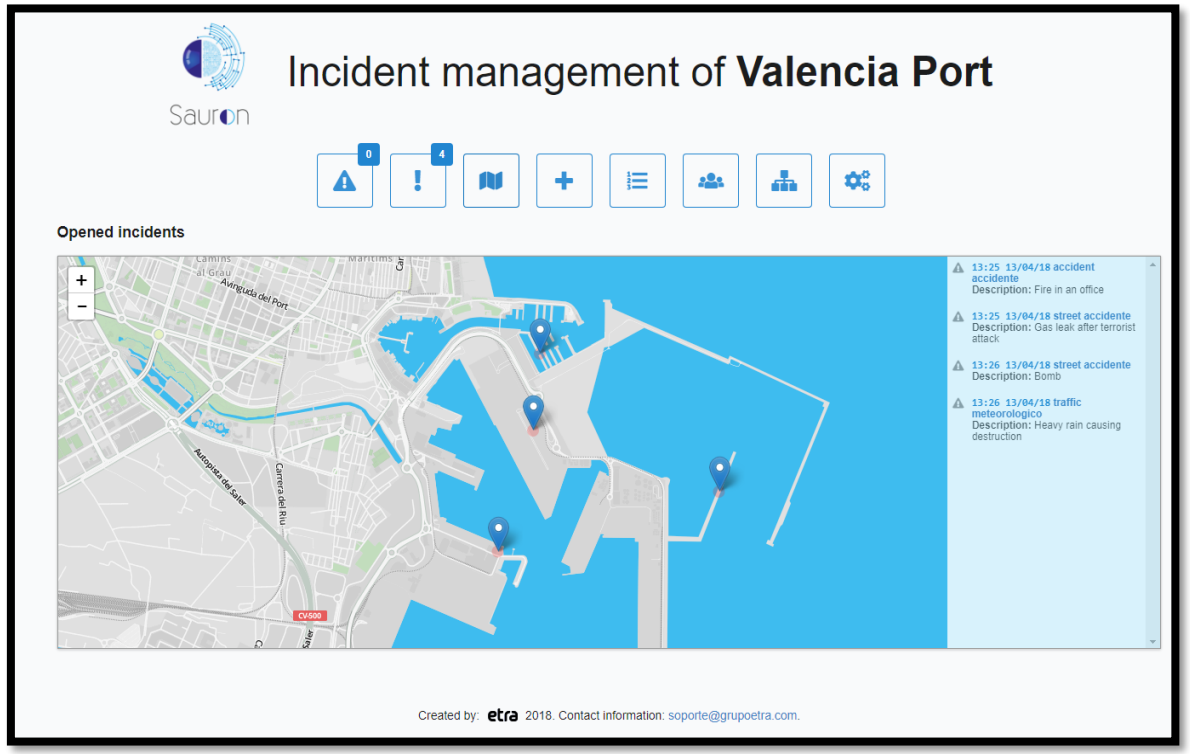
- ✓ Specific process for each type of alarm
- ✓ Specific for each port
- ✓ User tasks with forms
- ✓ Email notify
- ✓ Embed code
- ✓ Integrable with other systems

Workflow example



SAURON EPWS Solution (Incident Management)

- **Live Demo!**



Thanks for your attention!

Dr. Israel Pérez ispello0@upvnet.upv.es
Xavier Mamy xavier.mamy@idemia.com
Sergio Zamarripa sergio.zamarripa@s2grupo.es
Romain Caillière romain.caillere@thalesgroup.com
Stefan Schauer stefan.schauer@ait.ac.at
Jordi Arias jarias.etraid@grupoetra.com

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