



SAURON Components





Sauron

Sauron Physical Situation Awareness (PSA)

Dr. Israel Pérez [UPV]

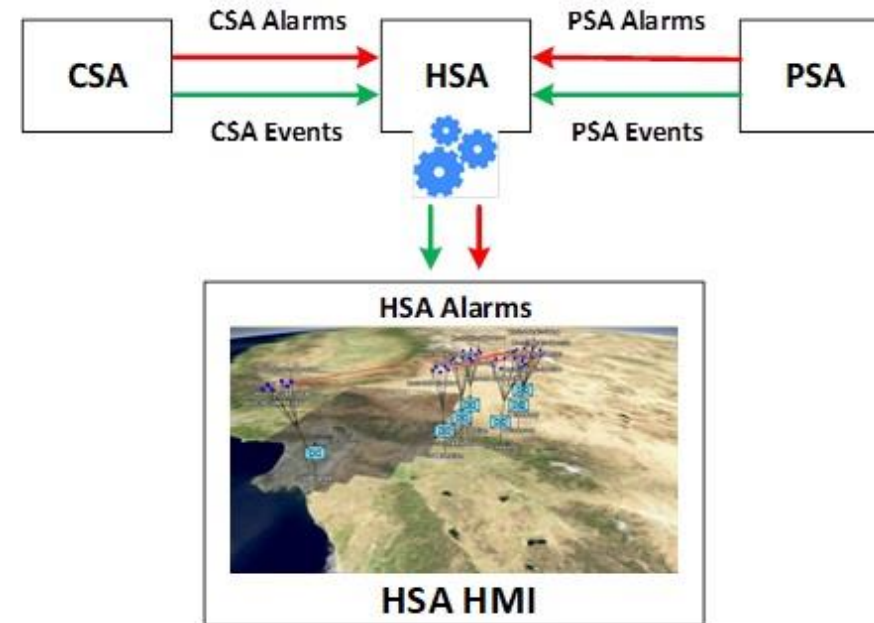
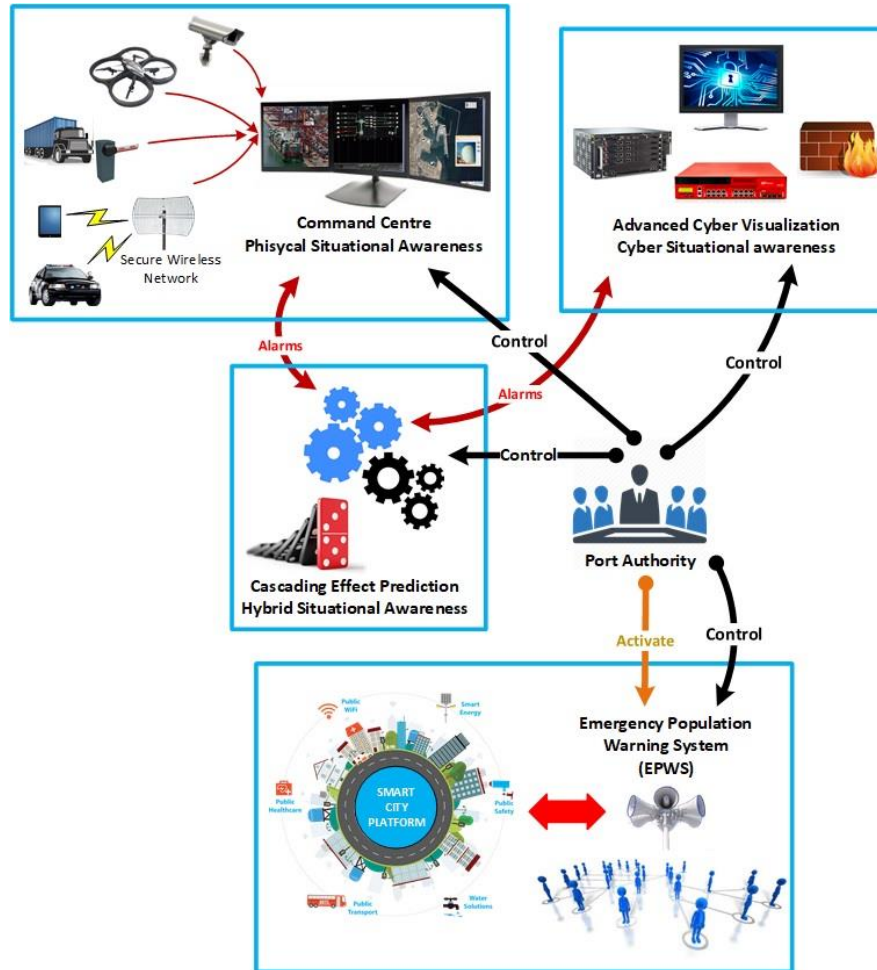
Xavier Mamy [IDEMIA]



Overall SAURON Architecture Definition



Sauron





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



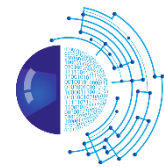
Adaptation to the port environment

- 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

SAURON -- PSA [MY USER: CENTRO DE CONTROL PRINCIPAL]

Mouth port camera north

Mouth port camera south

NT Camera Vial 15 TC07-MPF_1

NT Camera Vial 15 MTO-MPE_4

NT Camera FCC MTO-MPE_3

NT Smoke Sensor #1 Loss

NT Camera Vial 6 TC20-MPF_1

NT Camera Entry Gates TC11-MPF_1

NT Camera Entry Personnel GARITA-MPF_2

APV Camera Cosco perimeter #1

Presence sensor Y#1

CONFIGURATION

LAYER MANAGEMENT

SHOW 3D MAP

HIDE ELEMENTS

SHOW CAMERAS

HIDE NAMES

SHOW TRAFFIC

ALARMS

EVENTS

MESSAGES

INFORMATION

THREATS

OBJECTS

MEASURE

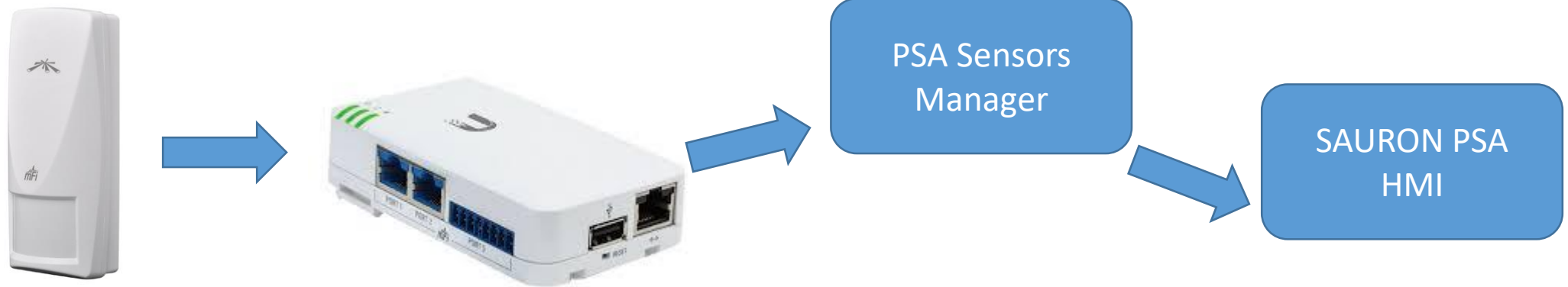
PERIMETERS

Sensors integration: Presence Sensors



Sauron

- Ubiquiti mFi series presence sensors have been used



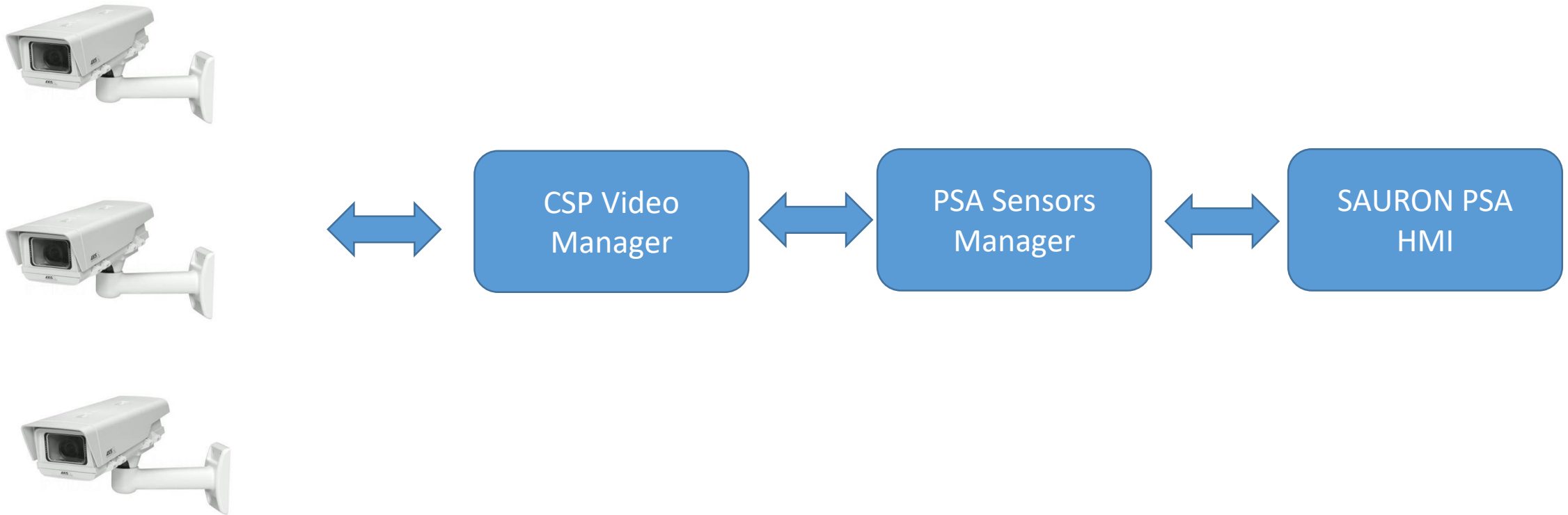
Sensors integration: Presence Sensors



The screenshot displays the Sauron PSA (Port Security Area) interface. The main view is an aerial satellite map of a port area with various sensor locations marked. A central window titled "PSA -- RECEIVED EVENT" is open, showing details for a "Presence sensor Y#1" event. The event details include: ASSET/SENSOR: Presence sensor Y#1; TYPE: Presence sensor; TITLE: Detected Presence; DESCRIPTION: prueba 1; EVENT TYPE: Detected Presence; EVENT DATE: 30/06/2020 12:29:46; CRITICALITY: Low; and IMPACT: (empty field). At the bottom of the event window are buttons for "CLOSE EVENT", "SEND TO HSA", and "CLOSE". On the right side of the interface is a vertical menu with options: CONFIGURATION, LAYER MANAGEMENT, SHOW 3D MAP, HIDE ELEMENTS, SHOW CAMERAS, HIDE NAMES, SHOW TRAFFIC, ALARMS, EVENTS, MESSAGES, INFORMATION, THREATS, OBJECTS, MEASURE, and PERIMETERS. The Windows taskbar at the bottom shows the search bar with the text "Escribe aquí para buscar" and the system tray with the date and time "12:30 30/06/2020".

Sensors integration: Video Surveillance

CSP cameras have been integrated



Sensors integration: Video Surveillance



Sauron

PSA -- SENSOR INFORMATION

GENERAL

NAME: NT Camera Vial 15. MTO-MPF_4

TYPE: Camera


AFFILIATION:

RANK:

ALLOWED AREAS:

LAT / LON: 39.428094 -0.323663

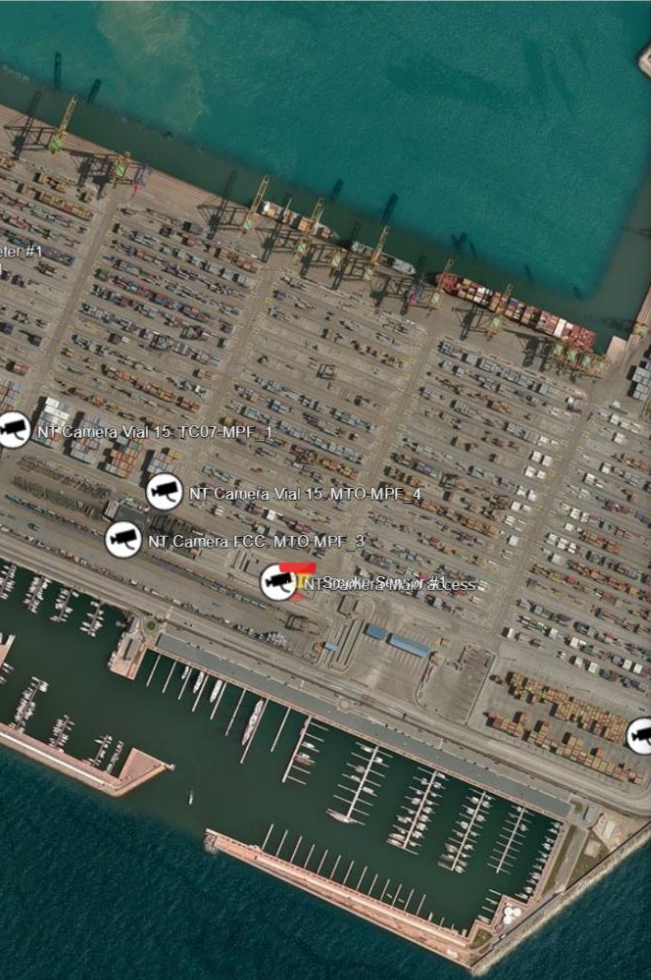
VIDEO URL: <rtsp://sauron.UPV.2020@192.168.48.230/axis-media/media.amp?videocodec=jpeg> HIDE



SENSOR EVENTS

EventName	EventDescription	Event Type	EventDate	EventCriticality	EventImpact	EventAlam
						<input type="checkbox"/>

CLOSE



PSA -- SENSOR INFORMATION

GENERAL

NAME: NT Camera FCC. MTO-MPF_3

TYPE: Camera


AFFILIATION:

RANK:

ALLOWED AREAS:

LAT / LON: 39.427353 -0.324485

VIDEO URL: <rtsp://sauron.UPV.2020@192.168.48.220/axis-media/media.amp?videocodec=jpeg> HIDE



SENSOR EVENTS

EventName	EventDescription	Event Type	EventDate	EventCriticality	EventImpact	EventAlam
						<input type="checkbox"/>

CLOSE

CONFIGURATION

LAYER MANAGEMENT

SHOW 3D MAP

HIDE ELEMENTS

SHOW CAMERAS

HIDE NAMES

SHOW TRAFFIC

ALARMS

EVENTS

MESSAGES

INFORMATION

THREATS

OBJECTS

MEASURE

PERIMETERS

Sensors integration: Video Surveillance



Sauron

SAURON -- PSA [MY USER: CENTRO DE CONTROL PRINCIPAL]

PSA -- SENSOR INFORMATION

GENERAL

NAME: NT Camera Entry Personnel. GARITA-MPF_2

TYPE: Camera

AFFILIATION:

RANK:

ALLOWED AREAS:

LAT / LON: 39.424301 - -0.314052

VIDEO URL: <rtsp://sauron:UPV.2020@192.168.48.218/axis-media/media.amp?videocodec=jpeg> HIDE

SENSOR EVENTS

EventName	EventDescription	EventType	EventDate	EventCriticality	EventImpact	EventAlarm
						<input type="checkbox"/>

CLOSE

PSA -- SENSOR INFORMATION

GENERAL

NAME: NT Camera Entry Gates. TC11-MPF_1

TYPE: Camera

AFFILIATION:

RANK:

ALLOWED AREAS:

LAT / LON: 39.42512 - -0.313528

VIDEO URL: <rtsp://sauron:UPV.2020@192.168.48.211/axis-media/media.amp?videocodec=jpeg> HIDE

SENSOR EVENTS

EventName	EventDescription	EventType	EventDate	EventCriticality	EventImpact	EventAlarm
						<input type="checkbox"/>

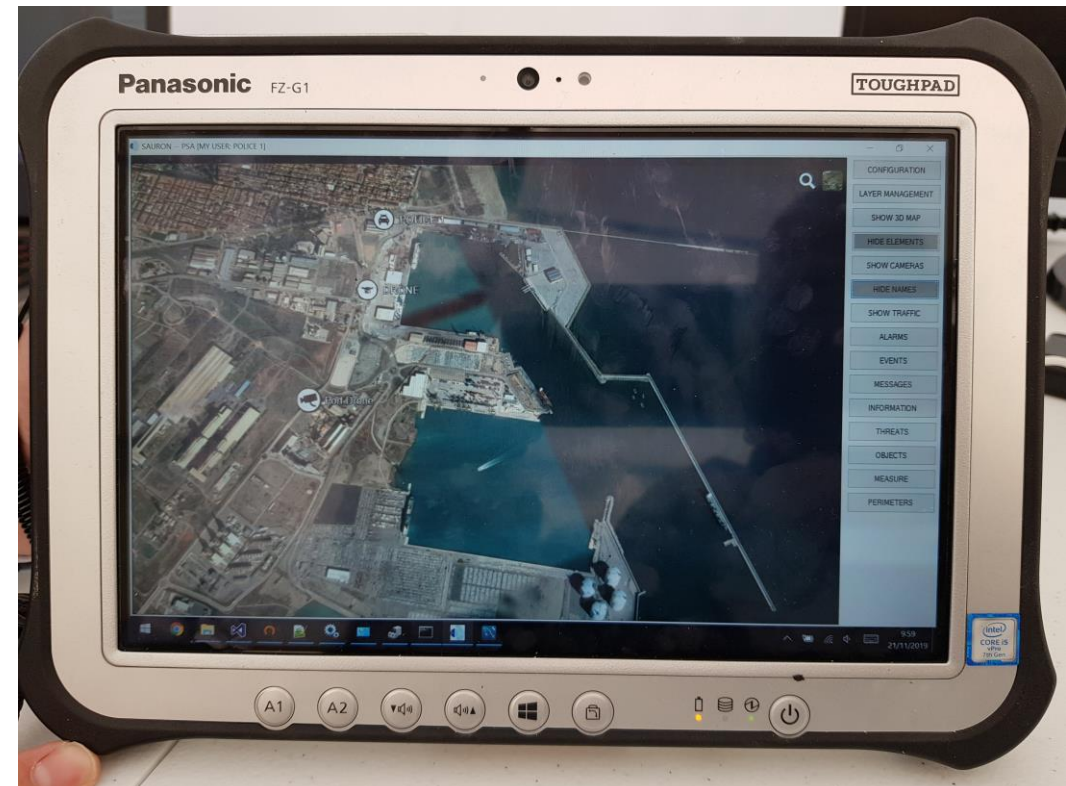
CLOSE

Sensors integration: Port Police Tablets



Sauron

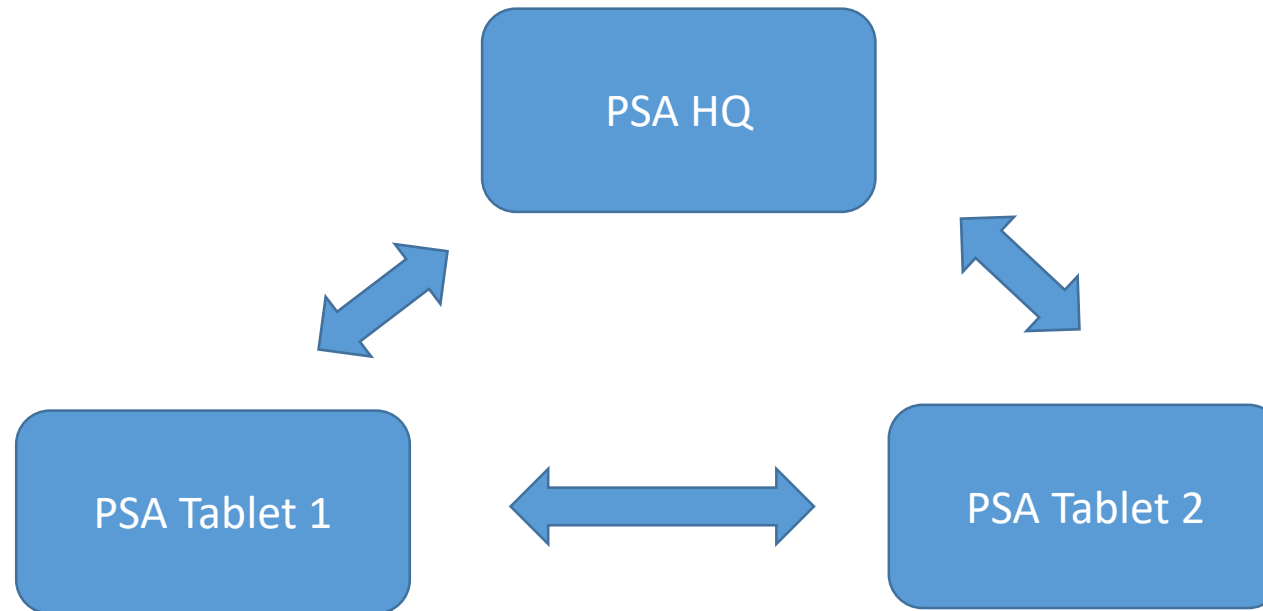
- Tablets have been integrated in the system
- Integration allows to exchange:
 - Messages
 - Alarms
 - Threats
 - Positions
- All in real time



Sensors integration: Port Police Tablets



- In-PSA communications architecture

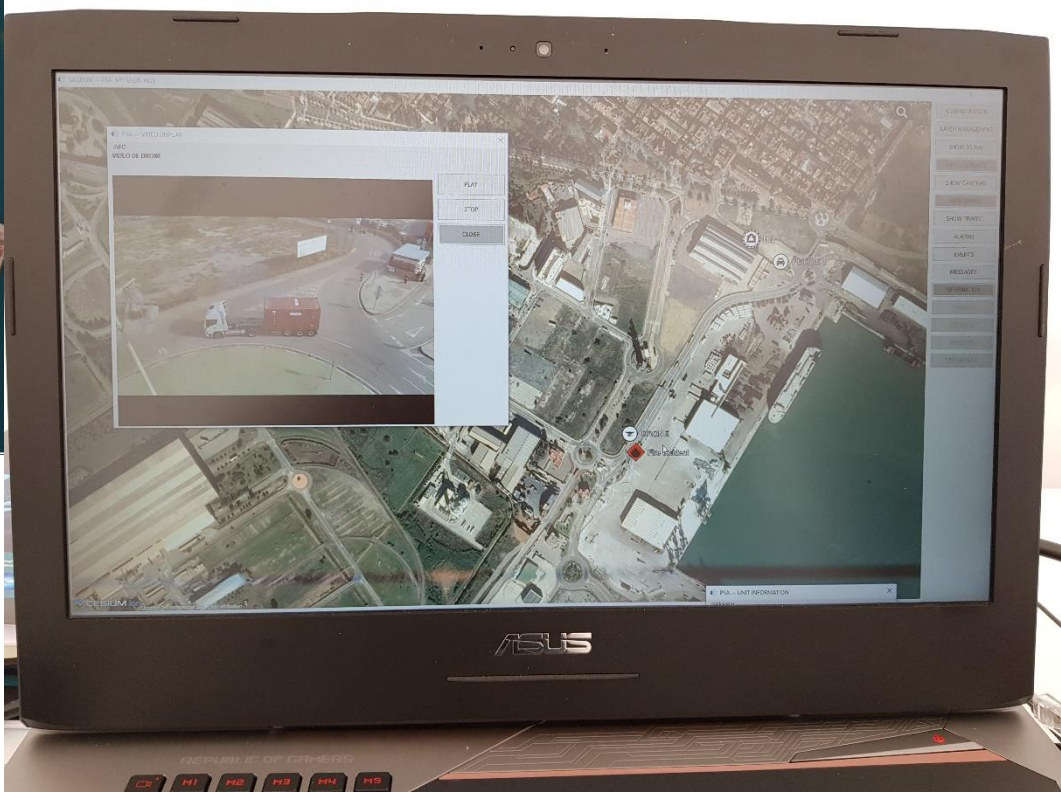
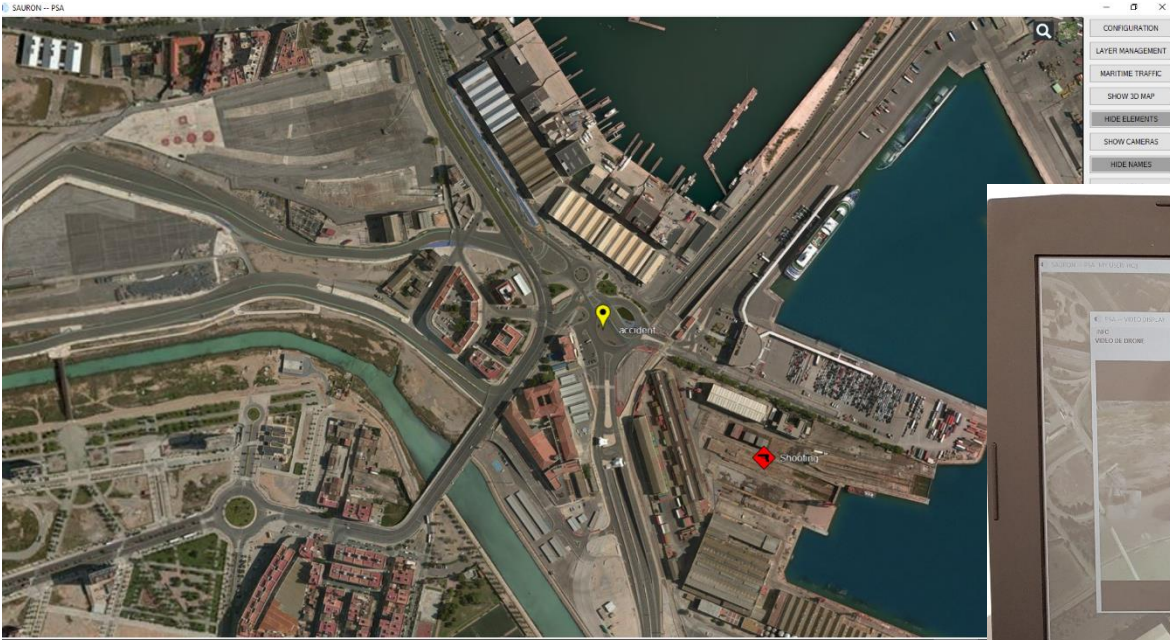


Sensors integration: Port Police Tablets



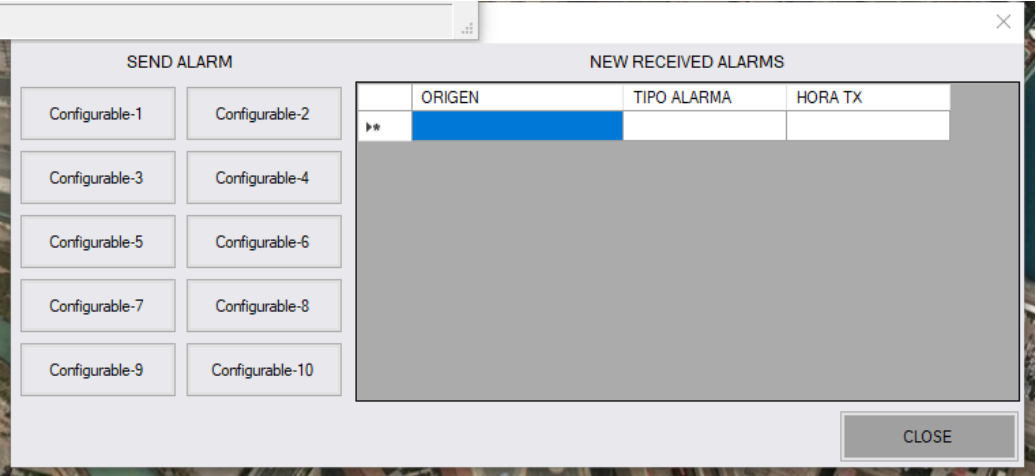
Real-time
Units
Position

Sensors integration: Port Police Tablets

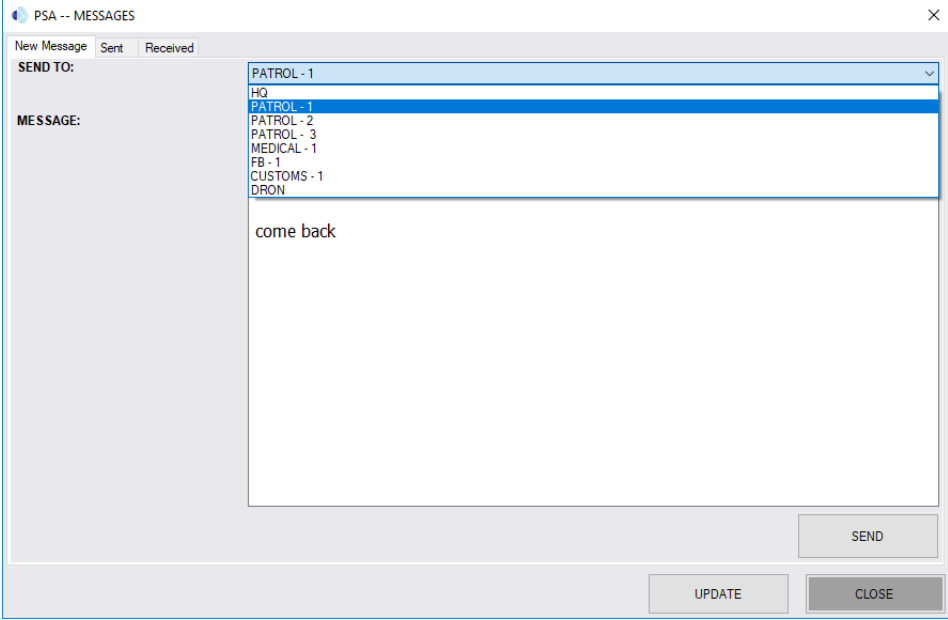


Real-time
Threats
Objects

Sensors integration: Port Police Tablets



Real-time
Alarms
Messages



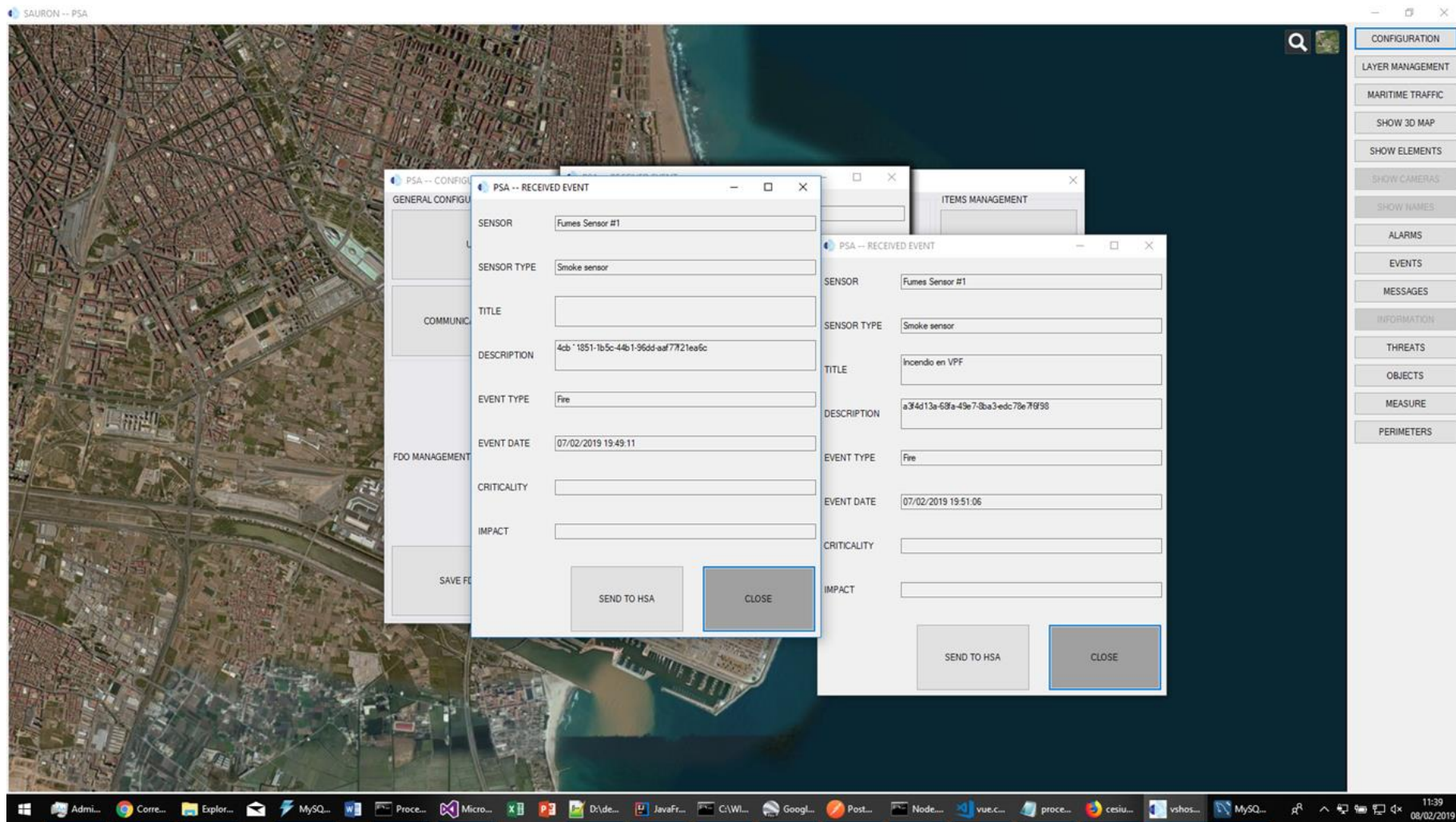
Sensors integration: Smoke Sensors



Sauron



Sensors integration: Smoke Sensors





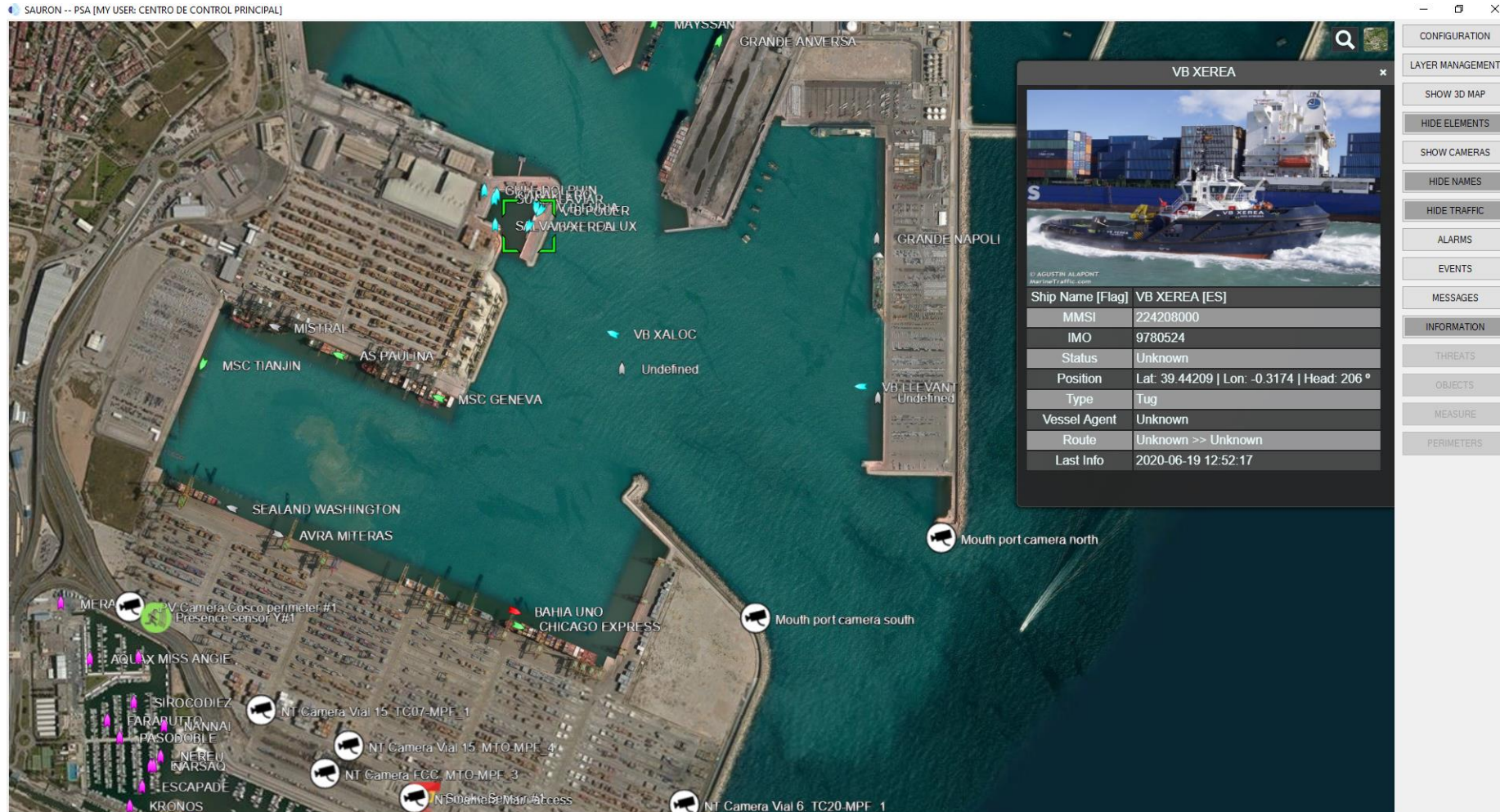
Sensors integration: AIS Processing

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



Sensors integration: AIS Integration

SAURON -- PSA [MY USER: CENTRO DE CONTROL PRINCIPAL]



The interface displays a satellite-style map of a port area with various ships and sensors. A detailed view of the ship VB XEREA is shown in a pop-up window.

VB XEREA	
Ship Name [Flag]	VB XEREA [ES]
MMSI	224208000
IMO	9780524
Status	Unknown
Position	Lat: 39.44209 Lon: -0.3174 Head: 206 °
Type	Tug
Vessel Agent	Unknown
Route	Unknown >> Unknown
Last Info	2020-06-19 12:52:17

Map labels include: MAYSSAN, GRANDE ANVERSA, GRANDE NAPOLI, VB XALOC, VB LLEVANT, MSC TIANJIN, AS PAULINA, MSC GENEVA, SEALAND WASHINGTON, AVRA MITERAS, BAHIA UNO, CHICAGO EXPRESS, Mouth port camera north, Mouth port camera south, ME RA, V Camera Cosco perimetro #1, Presence sensor Y#1, AQUAX MISS ANGIE, SIROCODIEZ, PARALUTTO, PASODOBLE, NEREI, MARSAQ, ESCAPADE, KRONOS, NT Camera Vial 15 TC07-MPE_1, NT Camera Vial 15 MTO-MPE_4, NT Camera FGC MTO-MPE_3, NT Camera Vial 6 TC20-MPE_1.

Configuration menu items: CONFIGURATION, LAYER MANAGEMENT, SHOW 3D MAP, HIDE ELEMENTS, SHOW CAMERAS, HIDE NAMES, HIDE TRAFFIC, ALARMS, EVENTS, MESSAGES, INFORMATION, THREATS, OBJECTS, MEASURE, PERIMETERS.



Sensors integration: AIS Integration

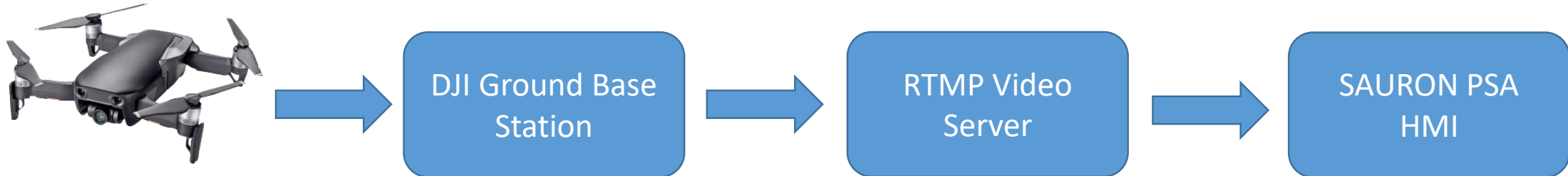
SAURON -- PSA [MY USER: CENTRO DE CONTROL PRINCIPAL]

MSC IMMACOLATA	
Ship Name [Flag]	MSC IMMACOLATA [PA]
MMSI	373124000
IMO	9463205
Status	Under way using engine Operating
Position	Lat: 39.42107 Lon: -0.29089 Head: 133 °
Type	Vehicles Carrier
Vessel Agent	GRIMALDI LOGISTICA ESPANA S.L.
Route	FOS >> HALIFAX
Last Info	2020-06-29 20:36:52

- CONFIGURATION
- LAYER MANAGEMENT
- SHOW 3D MAP
- HIDE ELEMENTS
- SHOW CAMERAS
- SHOW NAMES
- HIDE TRAFFIC
- ALARMS
- EVENTS
- MESSAGES
- INFORMATION
- THREATS
- OBJECTS
- MEASURE
- PERIMETERS

Sensors integration: Drone-based surveillance

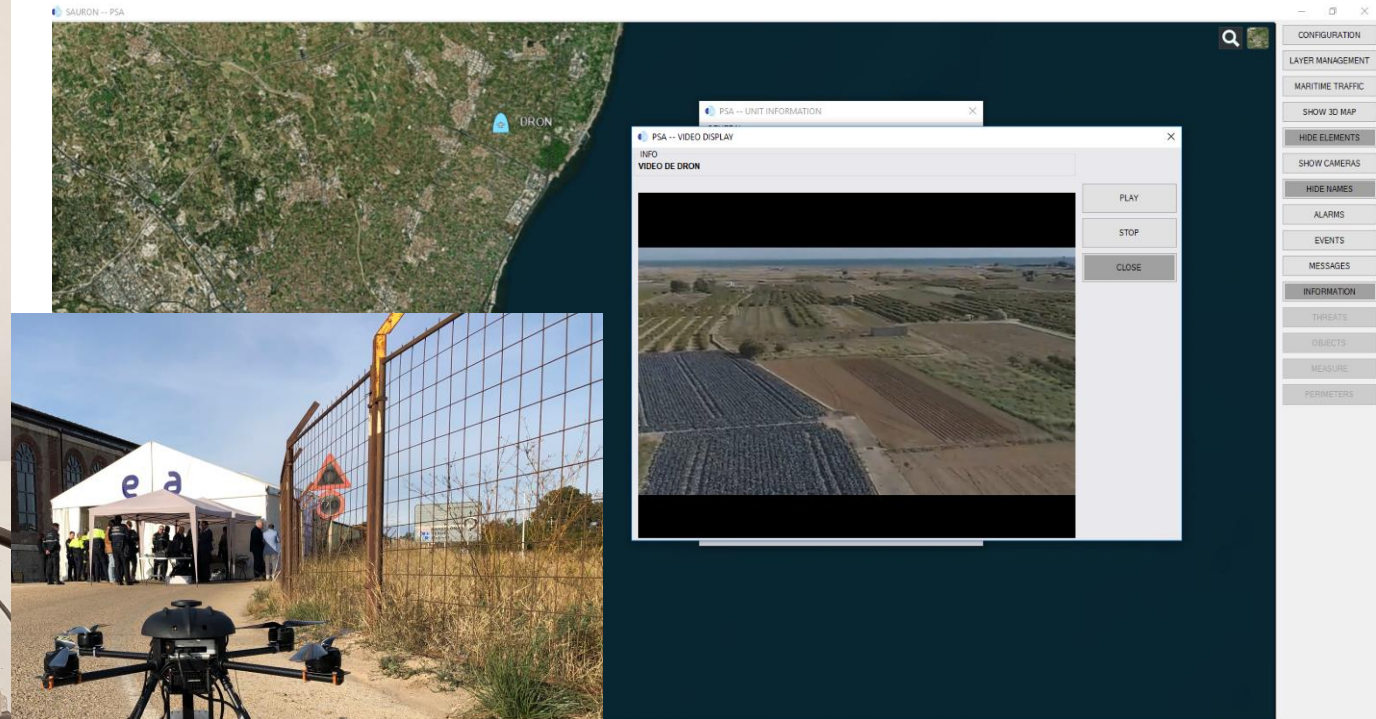
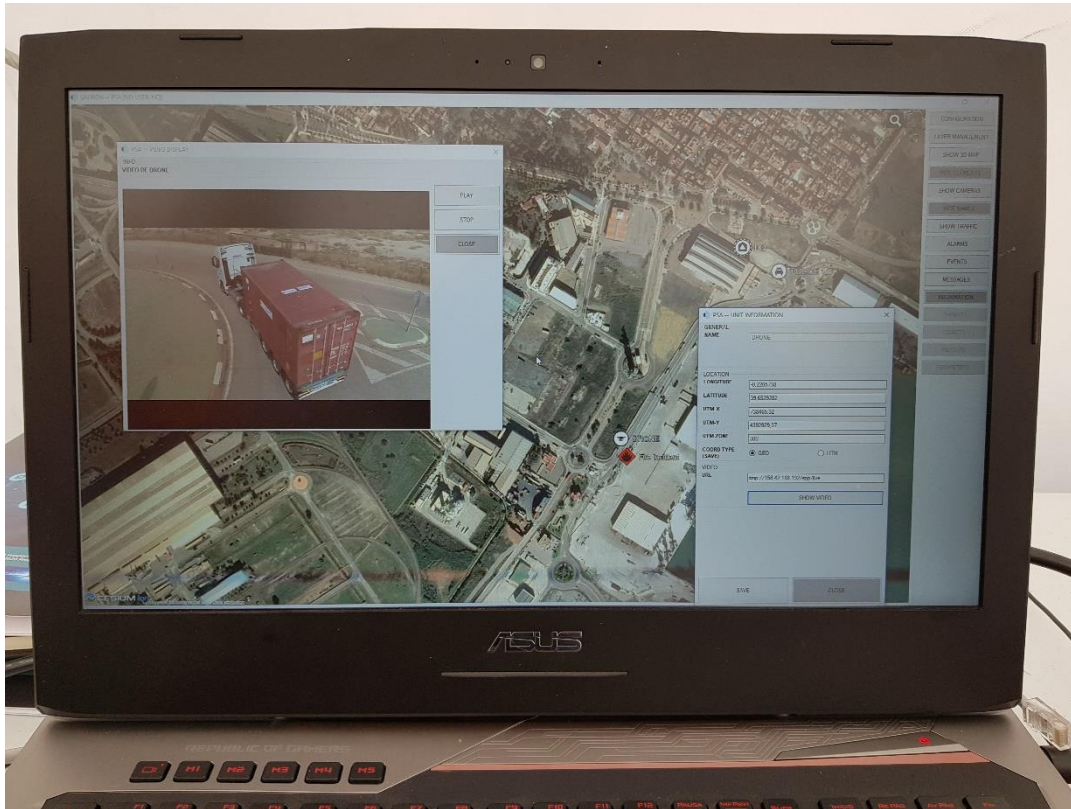
- DJI drones from a 3rd party company have been integrated



Sensors integration: Drone-based surveillance



Sauron

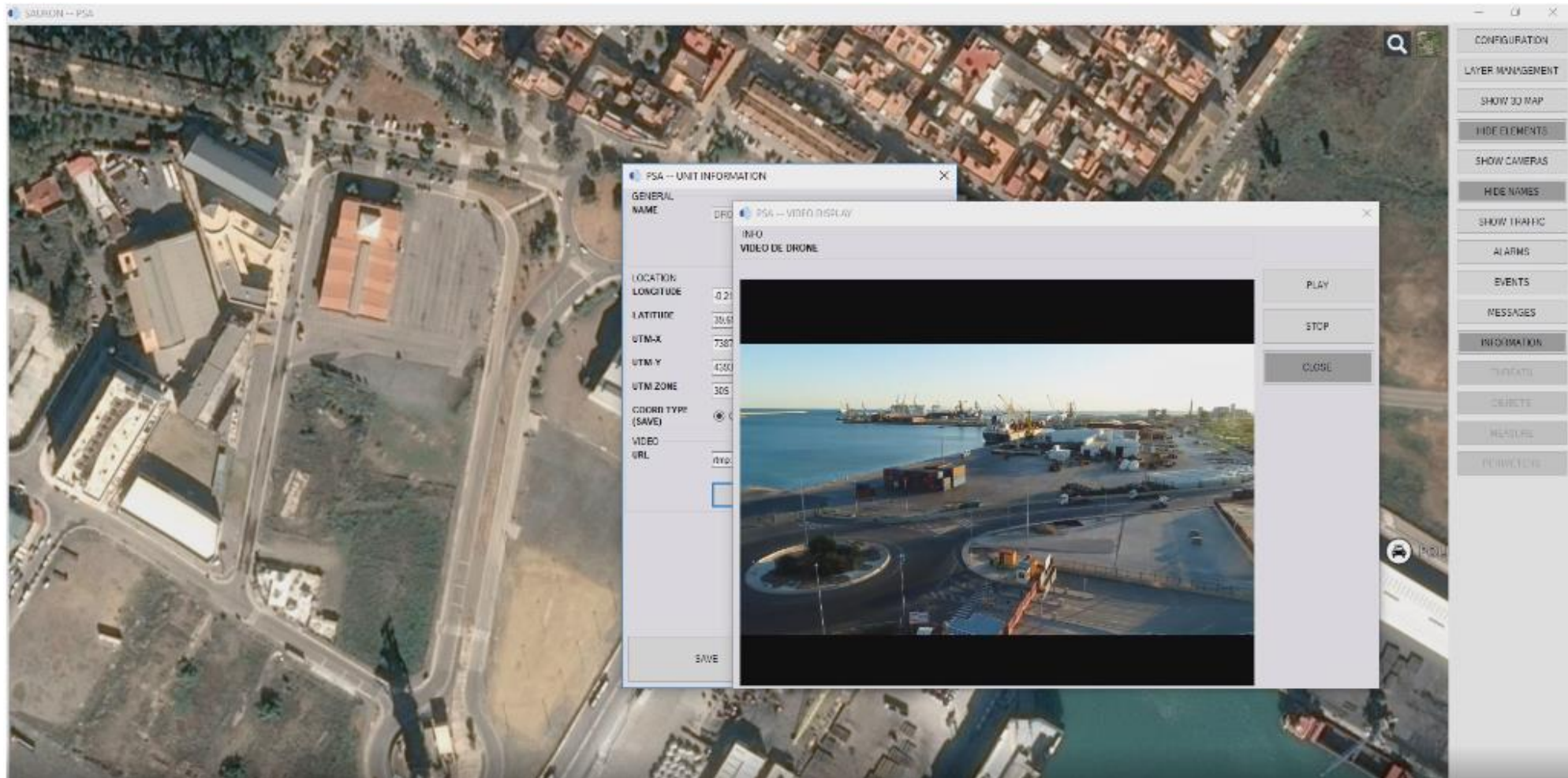


SAGUNTO Pilot
SAURON + ROCSAFE

Sensors integration: Drone-based surveillance

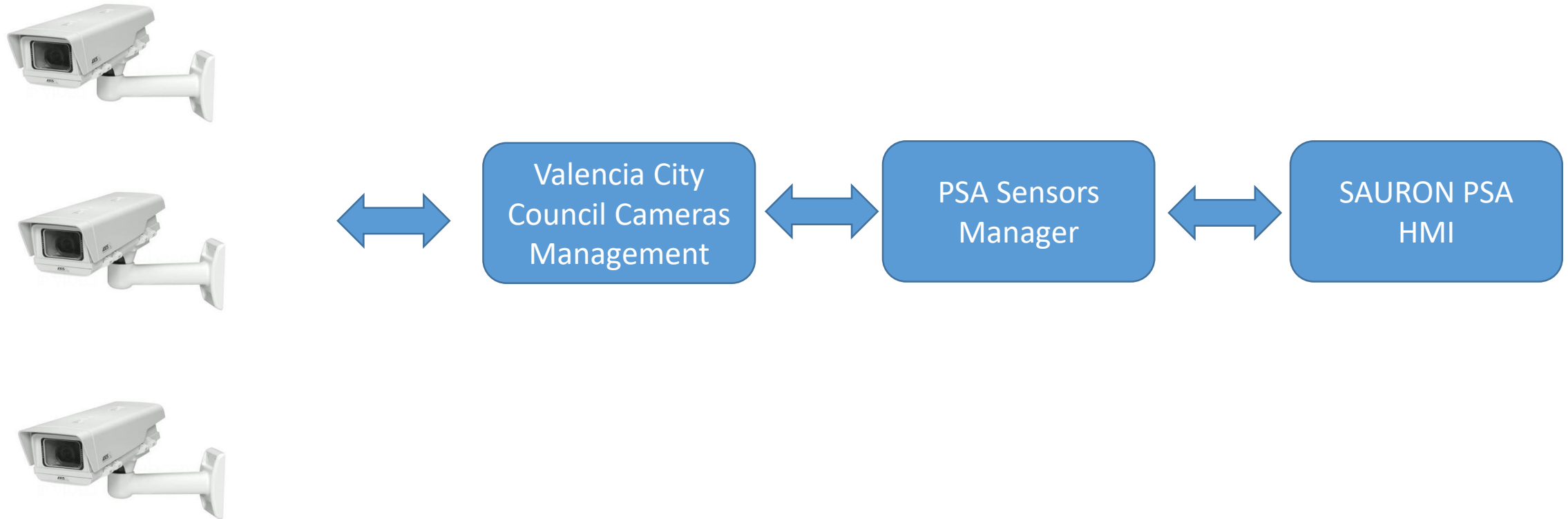


Sauron



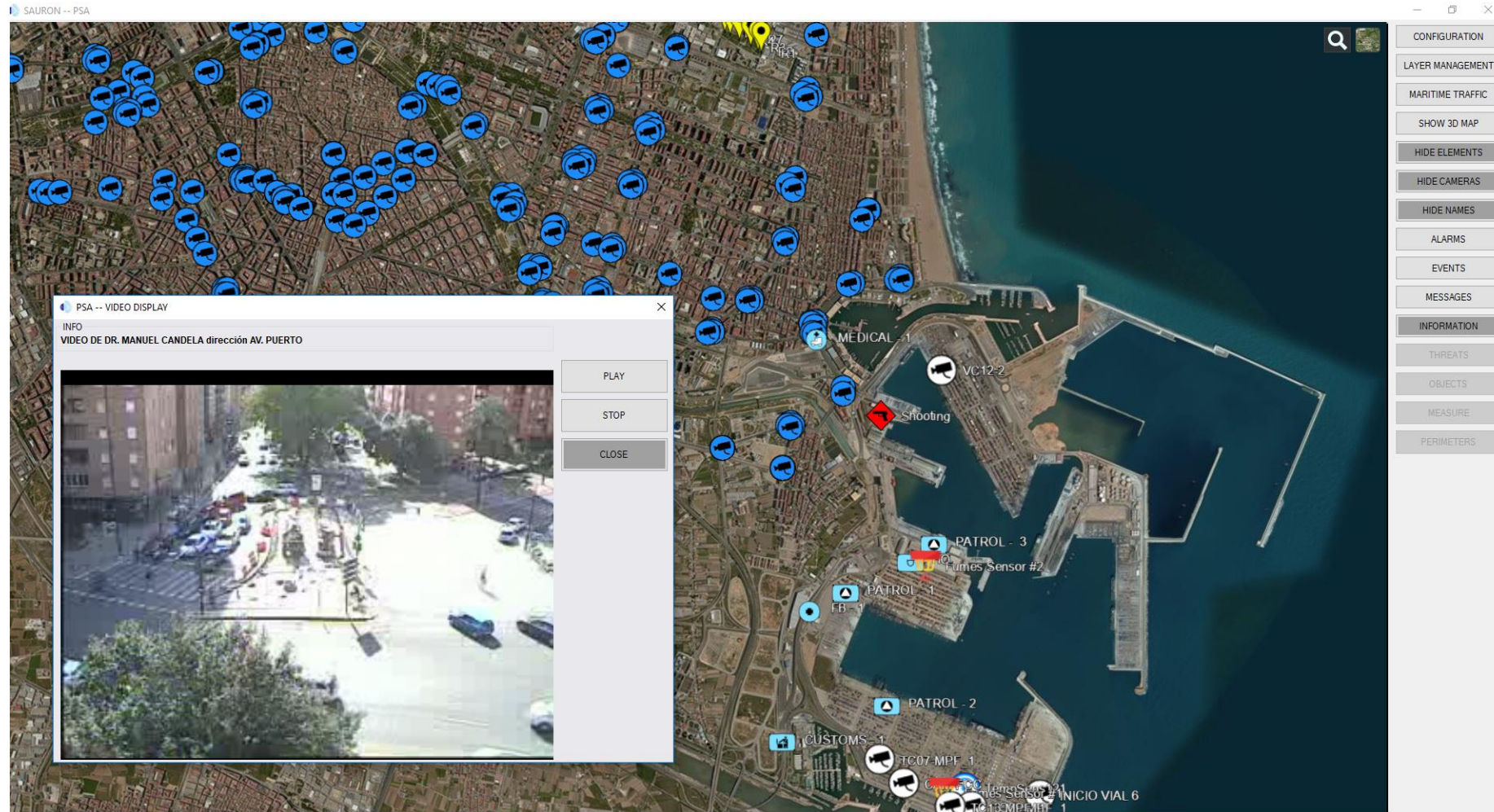
Sensors integration: Valencia City Council Video Cameras

Valencia City Council Cameras have been integrated





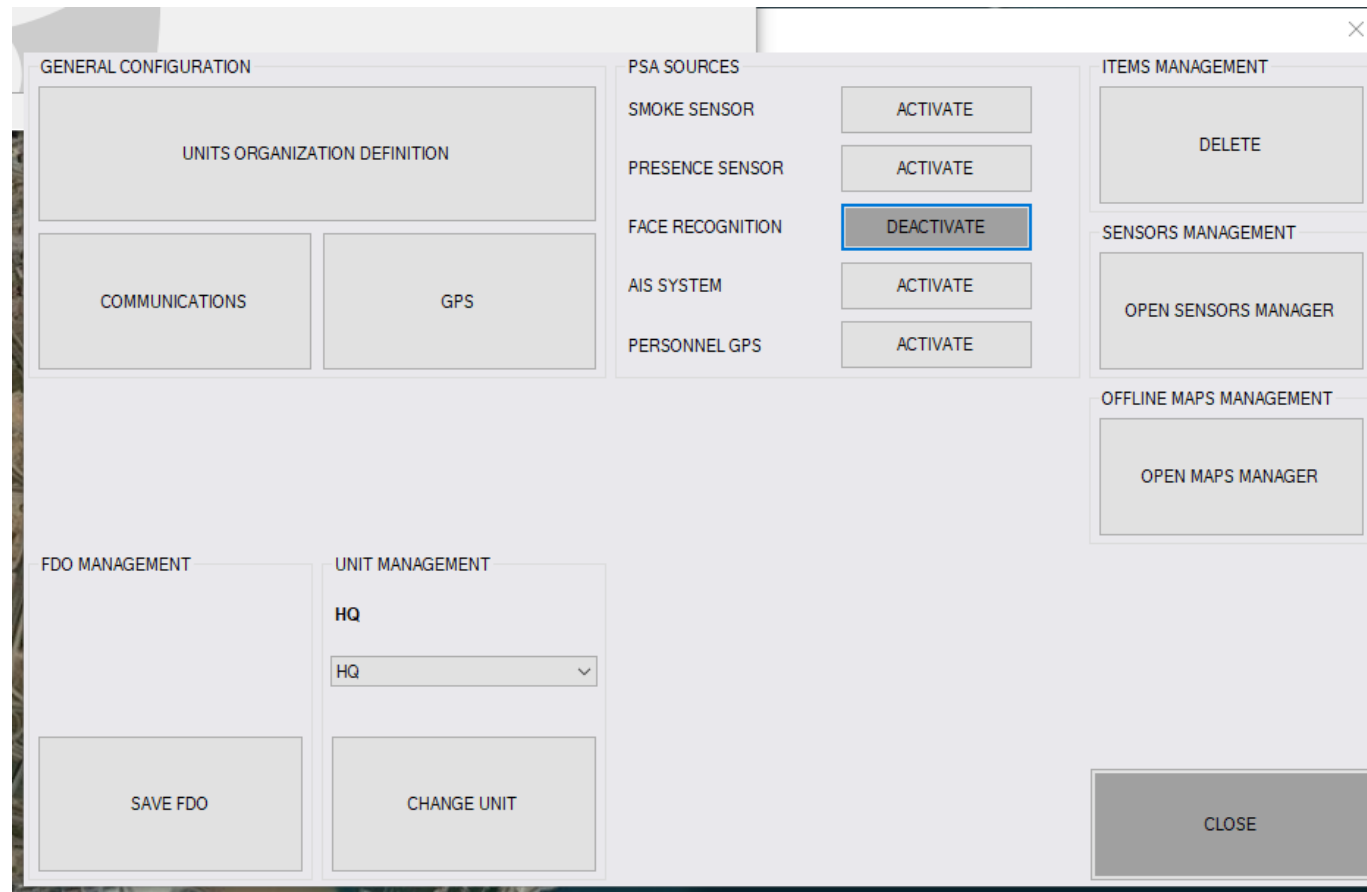
Sensors integration: Valencia City Council Video Cameras





Sensors integration: Management

- Sensors communication activation/deactivation





Sensors integration: Management

- Sensors management

PSA -- SENSORS

NEW SENSOR

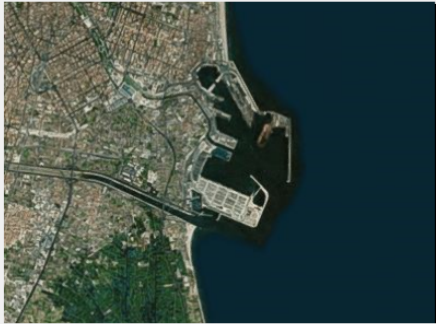
TYPE *

NAME *

AFFILIATION

RANK

LAT * / LON * -



ALLOW AREAS

FEATURES

DESCRIPTION

SAVE

CURRENT SENSORS

Id	Name	Type	Longitude	Latitude	Altitude	Affiliation	Rank
41	TC11-MPF_1	Camera	-0.313576	39.424233	0	Perim Accesos IB...	
42	TC13-MPF_1	Camera	-0.320237	39.425695	0		
43	TC09-MPF_1	Camera	-0.318285	39.425699	0		
44	TC07-MPF_1	Camera	-0.326703	39.429054	0		
45	CAM-FCC	Camera	-0.324485	39.427353	0		
46	VC12-2	Camera	-0.321	39.4567	0		
124	INICIO VIAL 6	Camera	-0.312002	39.42651	0		
79	Fumes Sensor #1	Smoke sensor	-0.320781	39.426652	0		
80	Fumes Sensor #2	Smoke sensor	-0.32249	39.442766	0		
38	TempSens121	Temperature Sen...	-0.318916	39.426989	0		

CLOSE DELETE CLOSE



Events delivery

- Events management & HSA Communication

The screenshot shows the SAURON interface with a satellite map of an industrial area. A window titled 'PSA -- RECEIVED EVENTS' is open, displaying a table of events. The table has columns for Description, Event Type, Alarm, Date & Time, Criticality, Impact, Sensor Name, and Sensor Type. Below the table are 'SEND TO HSA' and 'CLOSE' buttons. On the right side of the interface, a vertical menu contains options like CONFIGURATION, LAYER MANAGEMENT, MARITIME TRAFFIC, SHOW 3D MAP, HIDE ELEMENTS, SHOW CAMERAS, HIDE NAMES, ALARMS, EVENTS, MESSAGES, INFORMATION, THREATS, OBJECTS, MEASURE, and PERIMETERS.

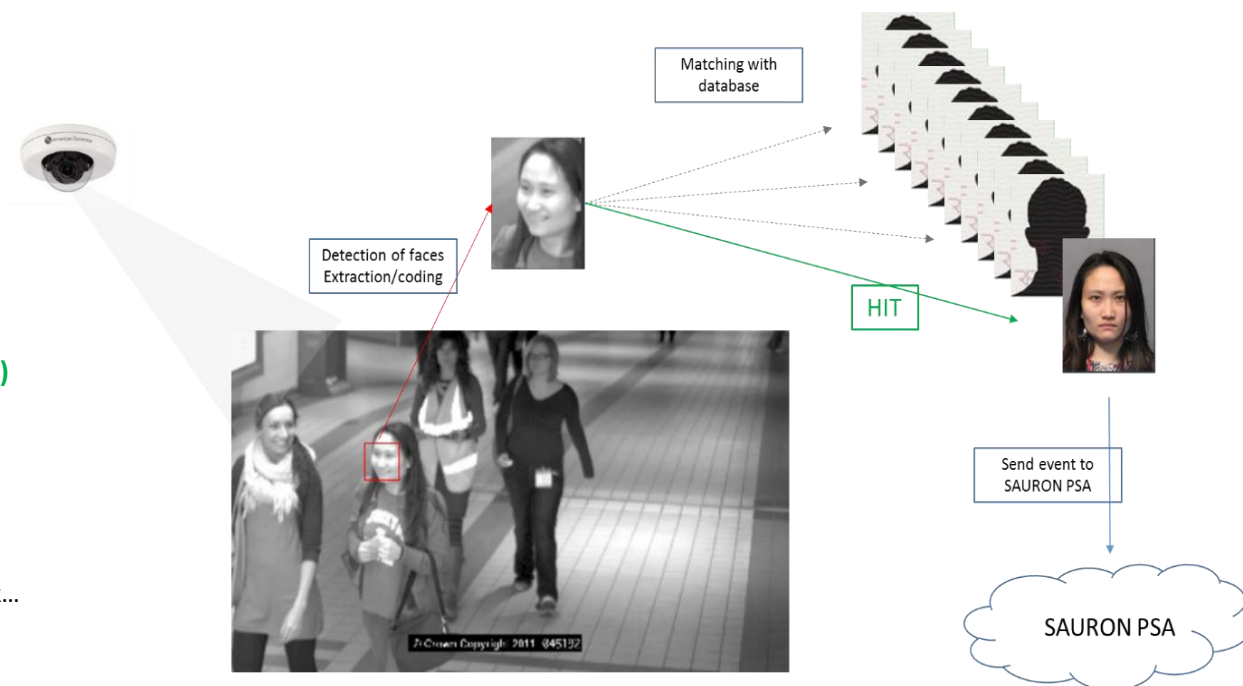
Description	Event Type	Alarm	Date & Time	Criticality	Impact	Sensor Name	Sensor Type
INTRAL CONTRA INCENDIOS EDIFICIO SIS	Fire	<input checked="" type="checkbox"/>	12/06/2018 11:41			Fumes Sensor #1	Smoke sensor
URADO EDIFICIO SISTEMAS	Fire	<input type="checkbox"/>	12/06/2018 11:45			Fumes Sensor #1	Smoke sensor
URADO EDIFICIO SISTEMAS	Fire	<input type="checkbox"/>	12/06/2018 11:40			Fumes Sensor #1	Smoke sensor
INTRAL CONTRA INCENDIOS EDIFICIO SIS	Fire	<input type="checkbox"/>	12/06/2018 11:44			Fumes Sensor #1	Smoke sensor
URADO EDIFICIO SISTEMAS	Fire	<input type="checkbox"/>	12/06/2018 11:41			Fumes Sensor #1	Smoke sensor
4D - INCENDIO 2a PLANTA	Fire	<input type="checkbox"/>	25/01/2019 10:35			Fumes Sensor #1	Smoke sensor
4P - INCENDIO 1a PLANTA	Fire	<input type="checkbox"/>	25/01/2019 10:44			Fumes Sensor #1	Smoke sensor
Ities	Fire	<input type="checkbox"/>	25/01/2019 10:56			Fumes Sensor #1	Smoke sensor
atum	Fire	<input type="checkbox"/>	07/02/2019 14:43			Fumes Sensor #1	Smoke sensor
lga	Fire	<input type="checkbox"/>	07/02/2019 19:49			Fumes Sensor #1	Smoke sensor
F	Fire	<input type="checkbox"/>	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



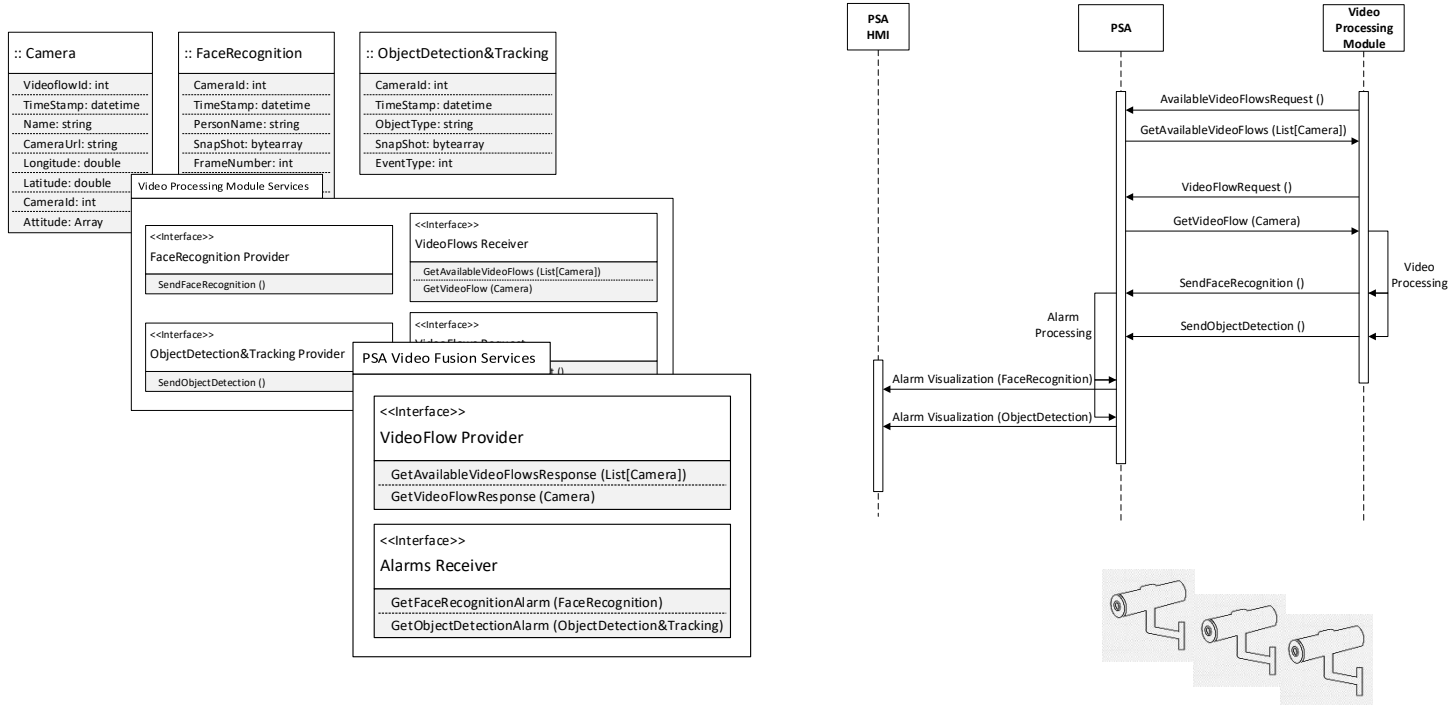
Vehicle detection
Source VALENCIA PORT



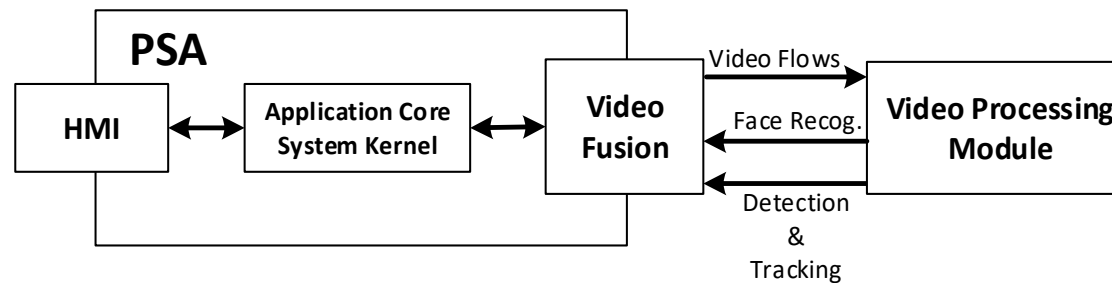
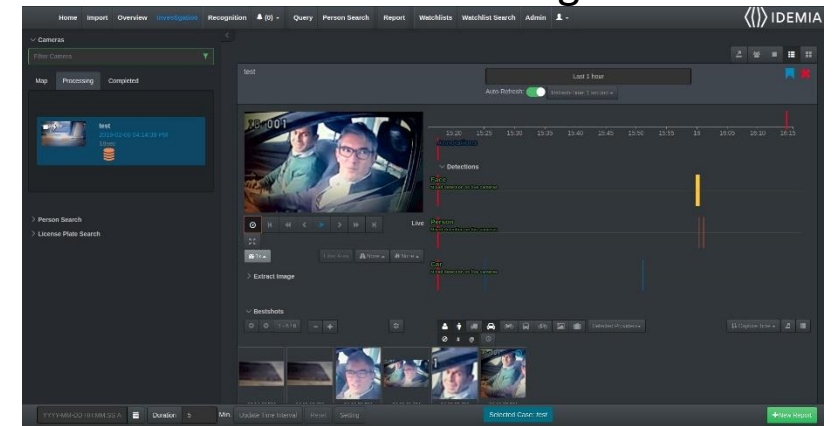
Boat detection
Source VALENCIA PORT



SAURON PSA integration



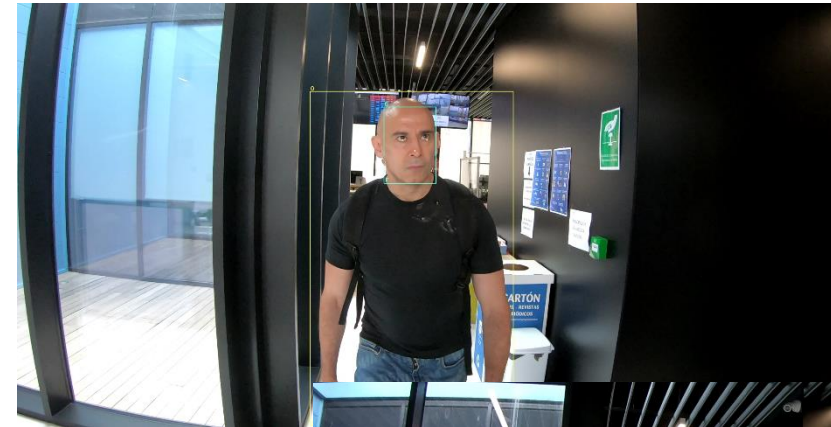
IDEMIA - Live monitoring interface





Valencia Scenario Pilot

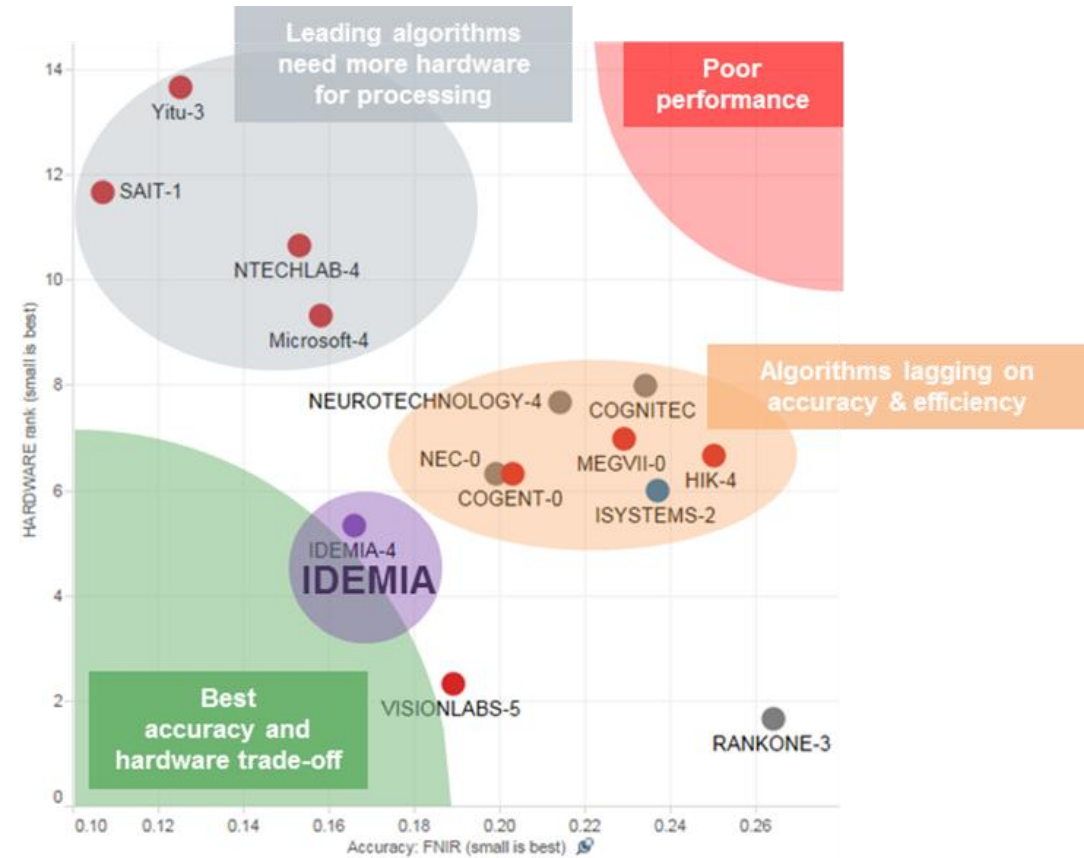
- 2 persons detected – NOT in the “authorized” database → Alert
 - Good quality of the faces → camera positioning for face recognition
 - Cooperation of authorized person
 - Database < 10 000 personnes
 - Access control gates (doors)
- Other events
 - Person/vehicle detected in an area where/when nobody 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

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

- 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



Hardware Rank vs Accuracy FNIR (False Negative Identification Rate)



Sauron

Cyber Situation Awareness (CSA)

Sergio Zamarripa [S2]





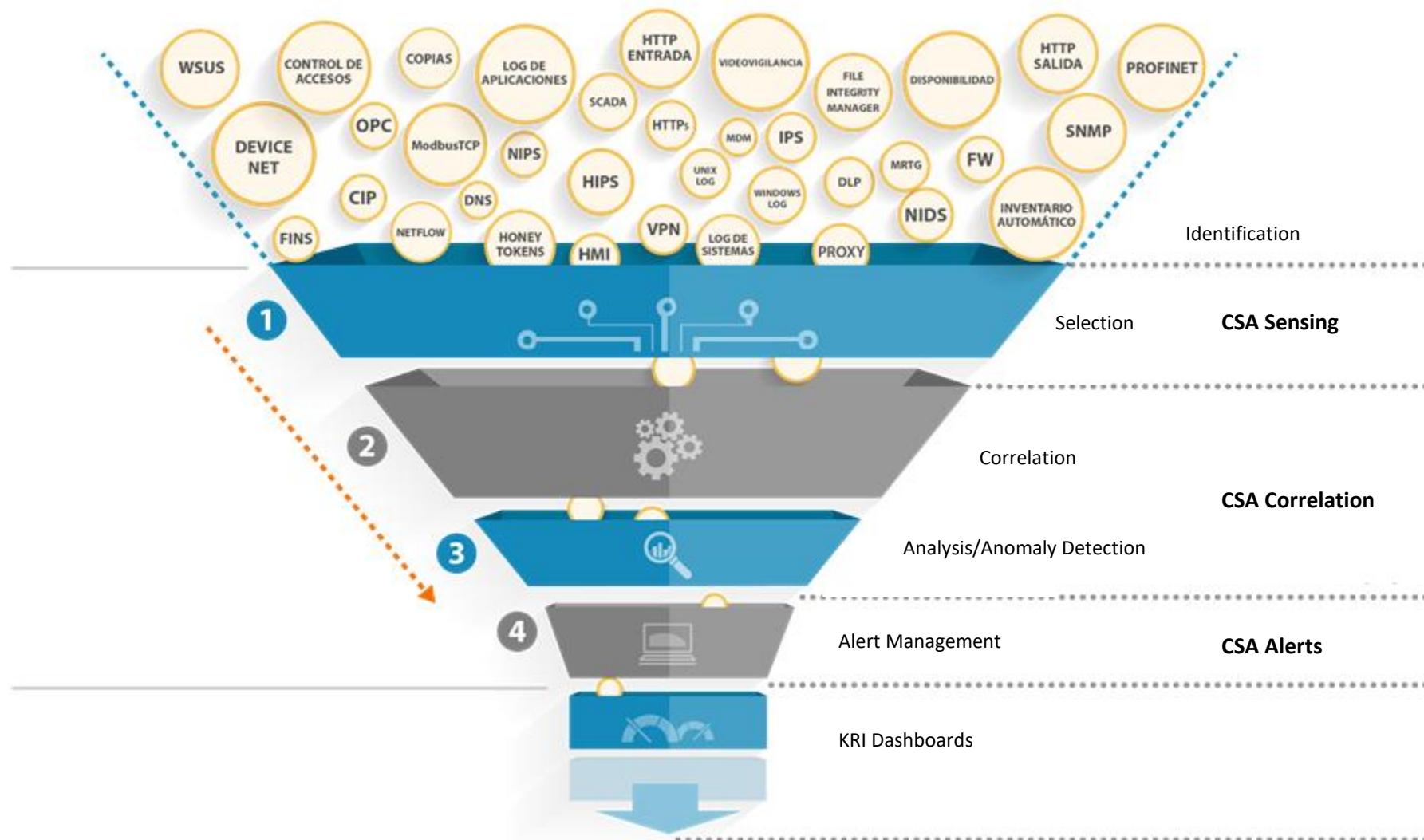
Summary Table

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

The screenshot displays the Sauron interface with the following components:

- Search Bar:** Search in the last 5 minutes. Query: `(*not found" AND http) OR http_response_code:{400 TO 404}`
- NIDS Section:** Found 69 messages in 191 ms, searched in 1 index. Results retrieved at 2018-12-05 14:17:30. Buttons: Add count to dashboard, Save search criteria, More actions.
- Fields and Decorators:** A list of fields including interface, ip_dst, ip_src, message, protocol, sensor, sig_class_name, and sig_iri.
- Quick Values for sig_name:** A pie chart showing the distribution of 68 messages. Below it is a table of top values.
- Table of Top Values:**

Value	%	Count
Top values		
ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection	27.94%	19
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection	27.94%	19
ET SCAN Suspicious inbound to MSSQL port 1433	22.06%	15
ET SCAN Potential SSH Scan OUTBOUND	14.71%	10
ET SCAN Suspicious inbound to PostgreSQL port 5432	5.88%	4
Others		
ET CURRENT_EVENTS Malformed HeartBeat Response	1.47%	1

- Histogram:** Shows a distribution of messages over time. A tooltip indicates 21 messages on Wednesday 5 December 2018, 14:16 +0100.

CSA Correlation Module



Automatic alert generation (without human intervention):

WHEN

1. New DMC security event
- destination user starts with
-Event id code indicates log in failed
- canal no debug
2. DC alerts times in less than seconds
-For the same user
-Event id code indicates log in failed
- destination user starts with
- destination user matches DMC Event
- canal no debug
3. There is no DMC alert in last hour from same rule 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 for rule
4. Attach sent mail as worknote
Generate Criticality Subject
5. event to EMas EBS

*UC16 Low fingerprint
UC18 Security Alert Generation*



CSA Alerts Module

Alert management: interacting with port office without impact

Events console

New event Create an event from event type Show event Refresh Print Last connection: 25/11/2018 20:...

Global View

Vista general Automatic refresh

Identifier: Text: Creation: Edition: Display: Status: Area: Project:

Clear Search

Dashboard List

Event Company Asset Client

Event Count: 24959 1 / 250

Pr.	Code	Description	Project	Status	Creation date	Criticality
	76083	Detected potential internal attack - ET SCAN Potential SSH Scan	Managed Secu...	Assigned	26/11/2018 16:57:33	High
	76082	Suspicious dropped file by C:\Program Files (x86)\Microsoft Office\Office16\OUTL...	Managed Secu...	Assigned	26/11/2018 16:53:00	High
	76081	A new program has been added to startup	Managed Secu...	Assigned	26/11/2018 16:41:10	High
	76080	Detected potential internal attack - ET WEB_SERVER Possible Apache Struts OGNL...	Managed Secu...	Assigned	26/11/2018 16:30:52	High
	76079	Detected potential internal attack - ET EXPLOIT Apache Struts Possible OGNL Allo...	Managed Secu...	Assigned	26/11/2018 16:28:19	High
	76078	Detected potential internal attack - ET WEB_SERVER Apache Struts Possible xwor...	Managed Secu...	Assigned	26/11/2018 16:28:18	High
	76077	Detected potential internal attack - ET EXPLOIT Mikrotik Winbox RCE Atte...	Managed Secu...	Assigned	26/11/2018 16:26:20	High
	76076	Detected potential internal attack - ET CURRENT_EVENTS Malformed Heart...	Managed Secu...	Assigned	26/11/2018 16:25:55	High
	76075	Detected potential internal attack - ET CURRENT_EVENTS Possible TLS He...	Managed Secu...	Assigned	26/11/2018 16:25:55	High
	76074	Detected potential internal attack - ET WEB_SERVER Possible CVE-2014-62...	Managed Secu...	Assigned	26/11/2018 16:25:46	High

ACTIONS

- Isolate the computer from the network and confirm the legitimacy of the activity.
- In the case of non-legitimate activity, notify SAURON CERT and investigate the infection route. Provide the user with another computer.
- If the capacity to carry out the investigation of this incident is not available, scale it up to IT-SEC to propose the activation of the RIT (Rapid Incident Response Team).
- After identifying how the equipment was compromised it is recommended to format and platform the system.

REFERENCES AND COMMENTS

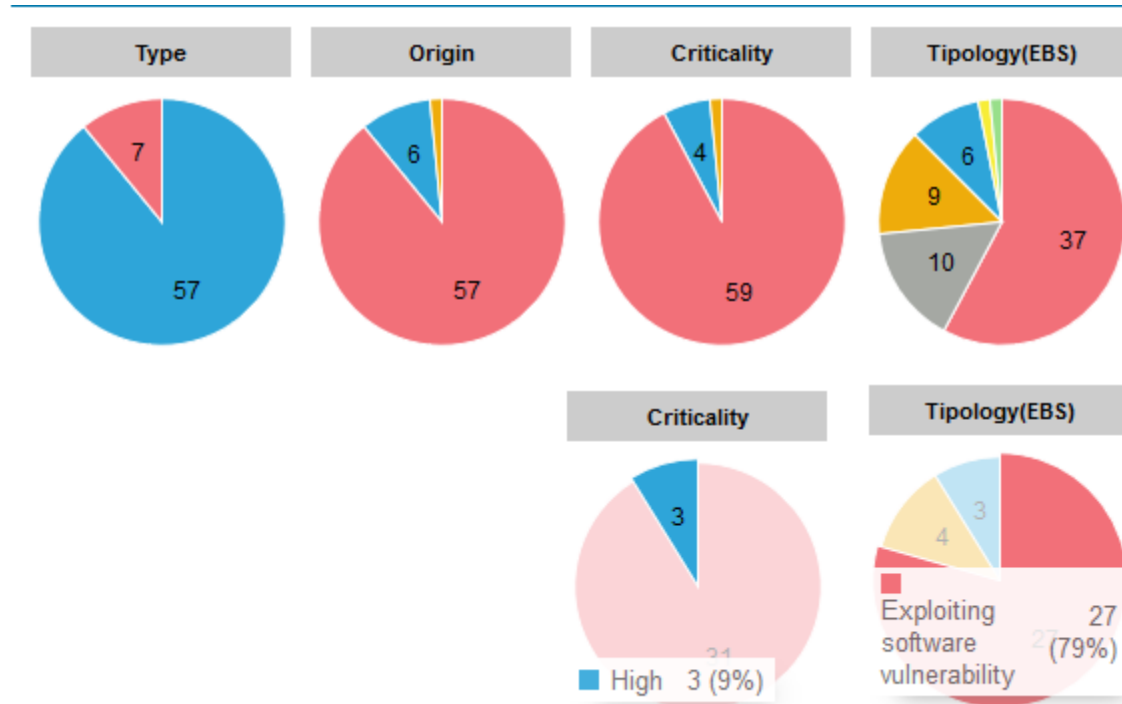
- It has detected possible malicious action executed on the assets of the organization.
- Specifically, an SQL injection attempt has been detected on the operative Web service in the organization.

UC18 Security Alert Generation
UC19 Alert Management
UC20 Export Information



CSA Alerts Module

Alert management: Situational risk



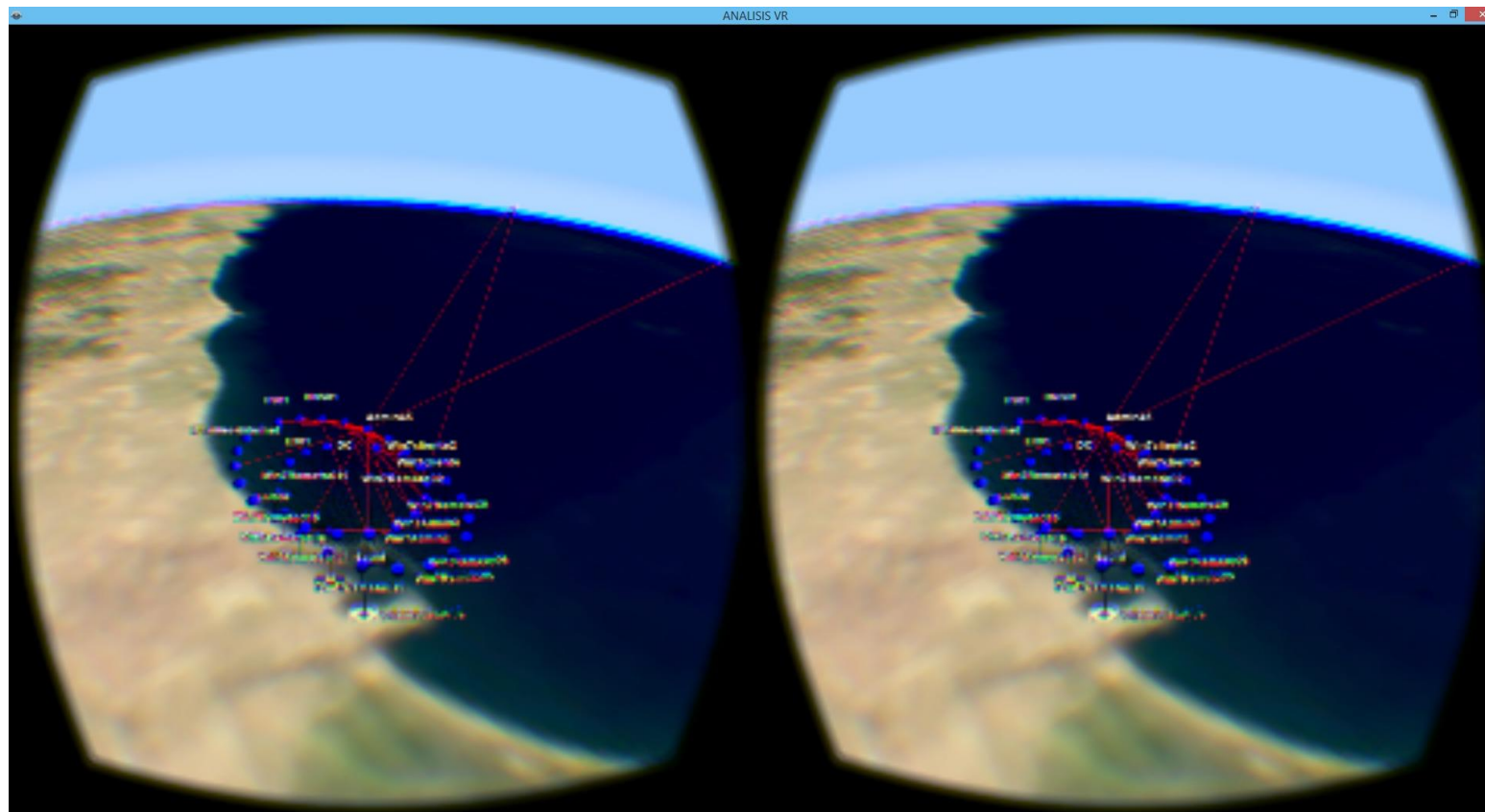
UC18 Security Alert Generation

UC19 Alert Management

UC20 Export Information



CSA Visualization: Cyber view



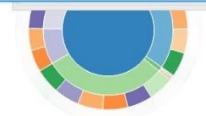
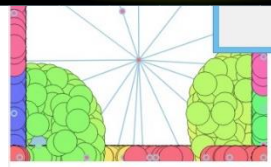
CSA HMI

CONFIGURACIÓN DE FUENTES

RTIR	NVG	NVG SERVER
Protocol: HTTPS	Protocol: HTTP	Port: 2122
Version: LUCIA	Version: TALOS	Service:
IP/URL: lucia.ertorno.tec	IP/URL: 192.168.5.24/5762/NvgSrv.aspx/GetNvg	SAVE STOP
Port: 443	Timeout (ms): 2000	GENERAL SETTINGS
User: root	Update Interval (ms): 5000	GET Requests Timeout (ms): 3000
Password:		POST Requests Timeout (ms): 3000
Cookie: RT_SID_lucia.ertorno.tec.443		Netflows Maximum Number: 50
SAVE	SAVE	Update Interval (mins): 3
		SAVE
		CLOSE

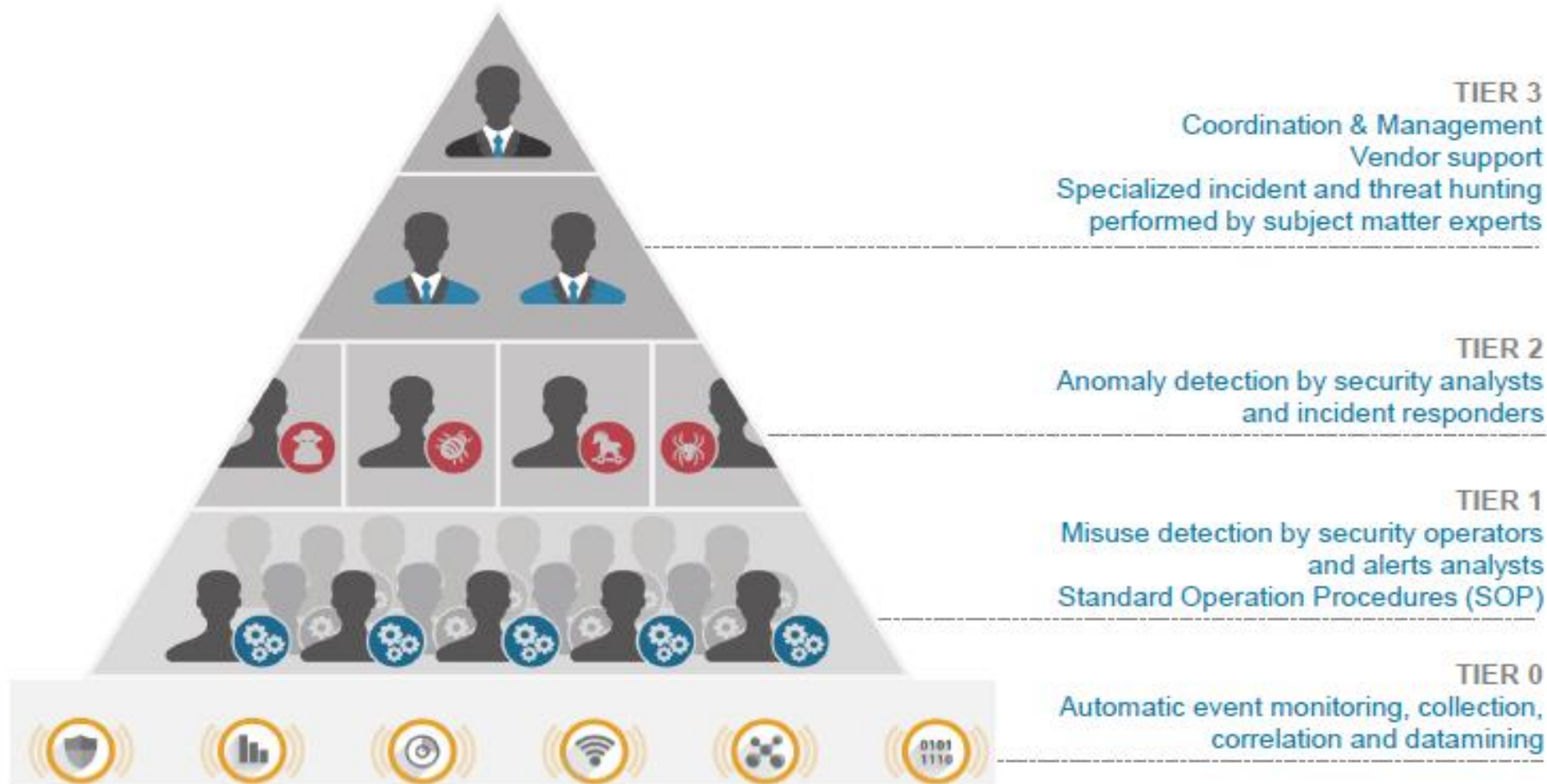
2019-01-15 19:11:55

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



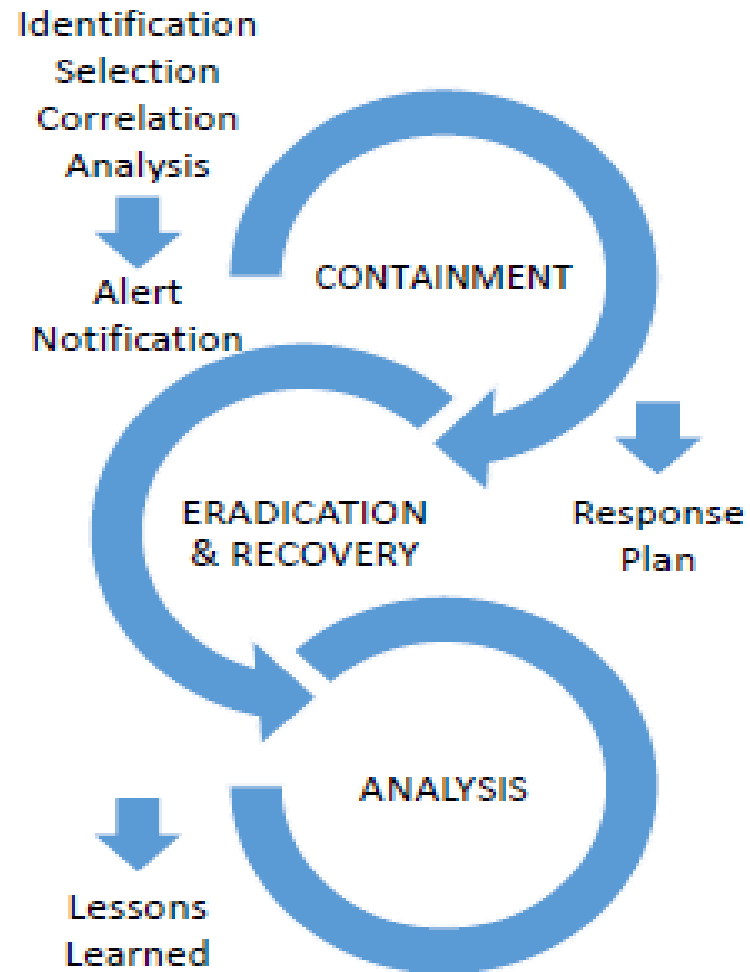


CSA team organization





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]

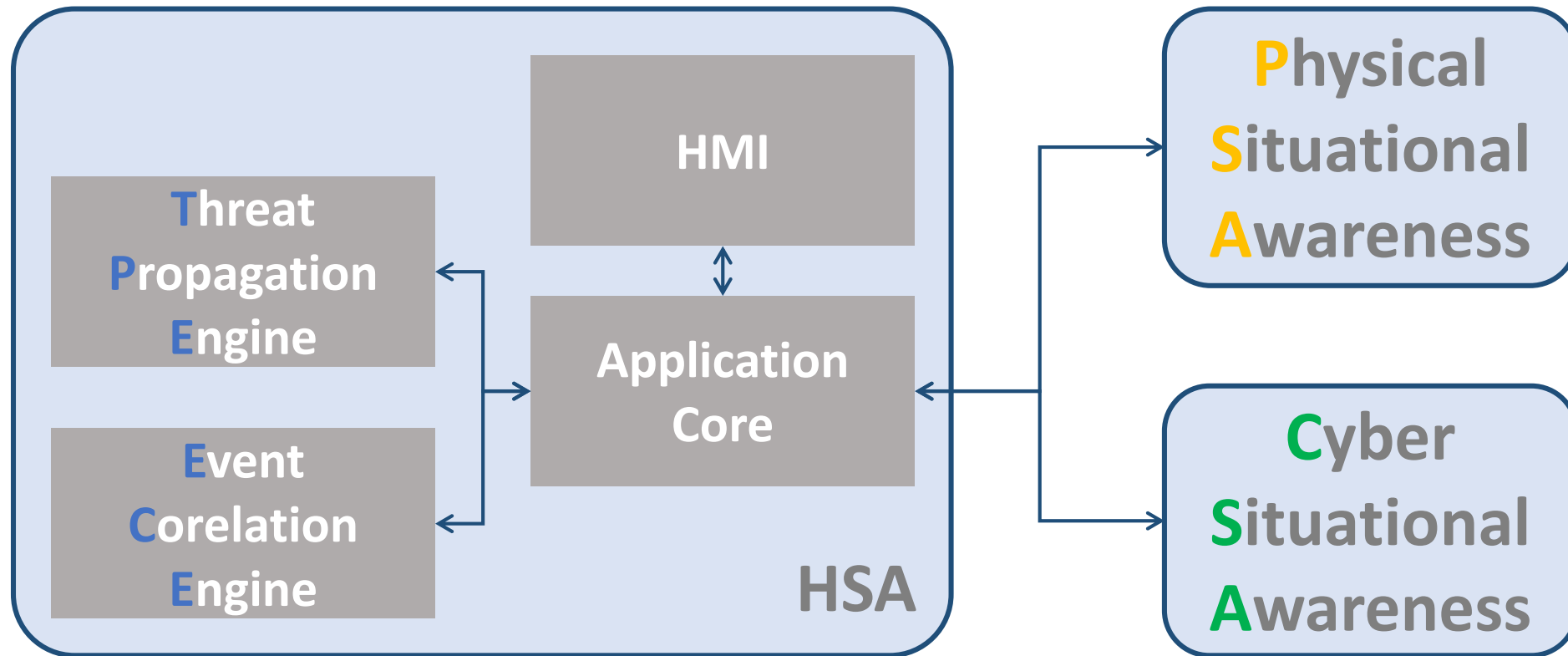




HSA : Hybrid Situational Awareness

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**



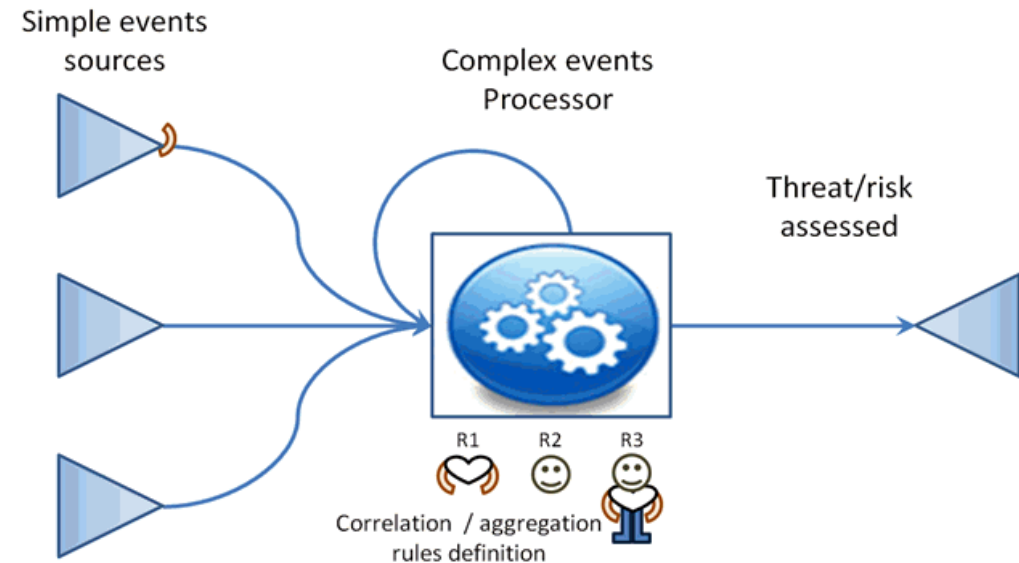
Application Core functionalities

- **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



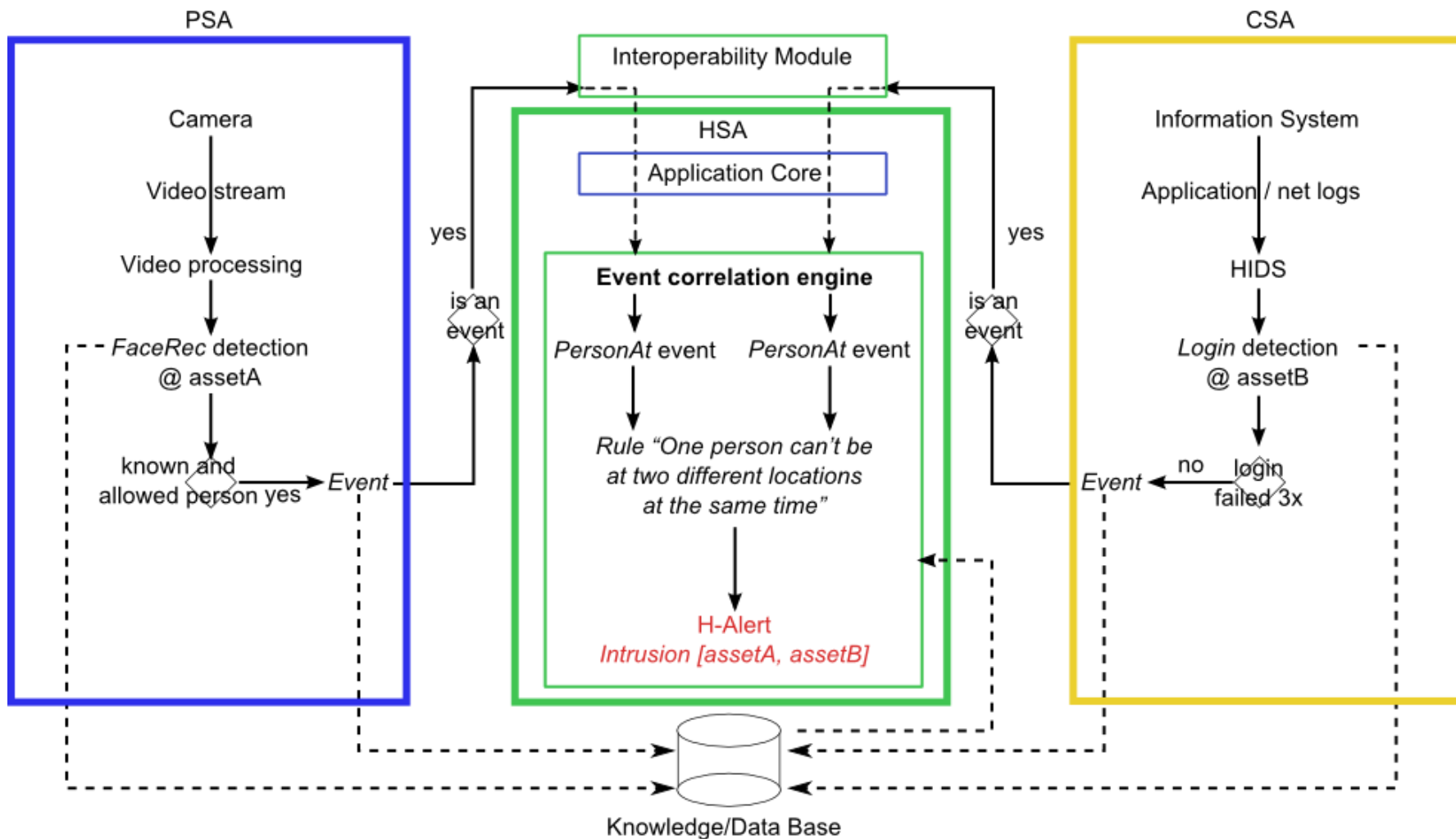
Event Correlation Engine

- 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

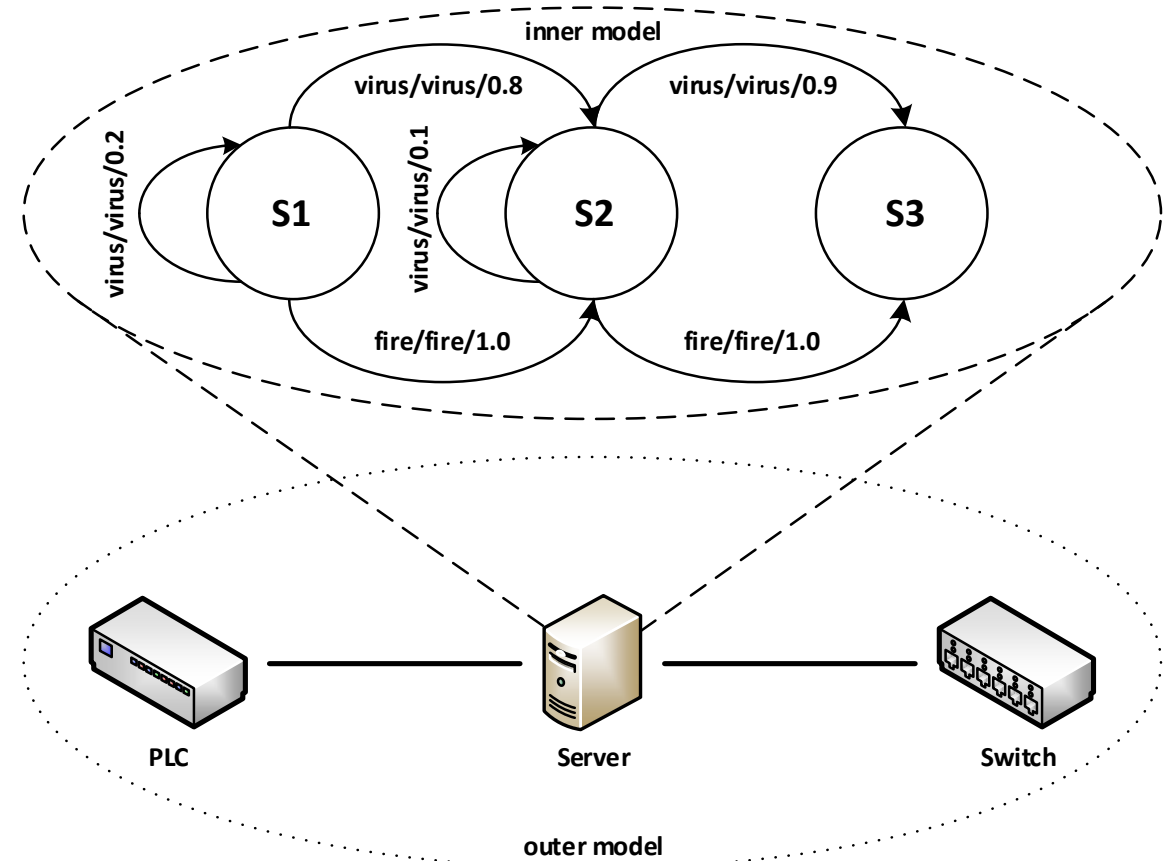


Sauron

- **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

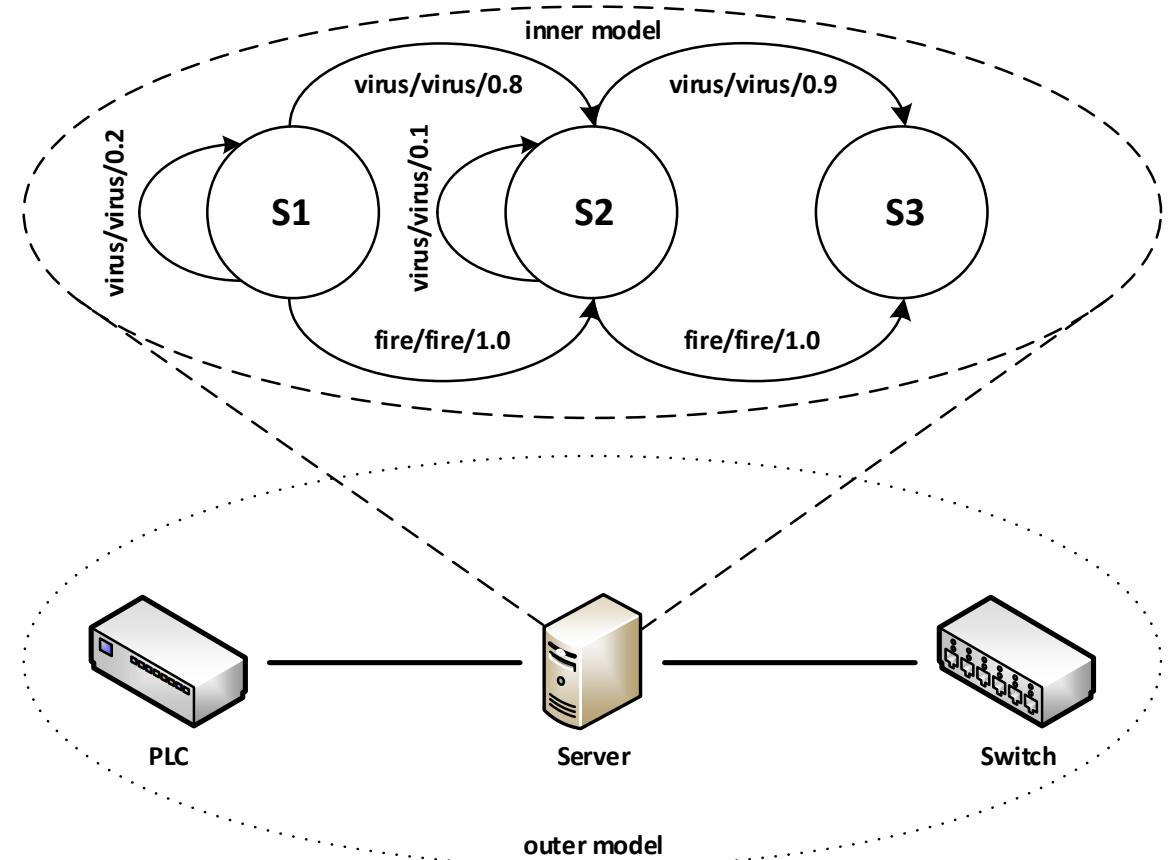
Threat Propagation Engine

- 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**



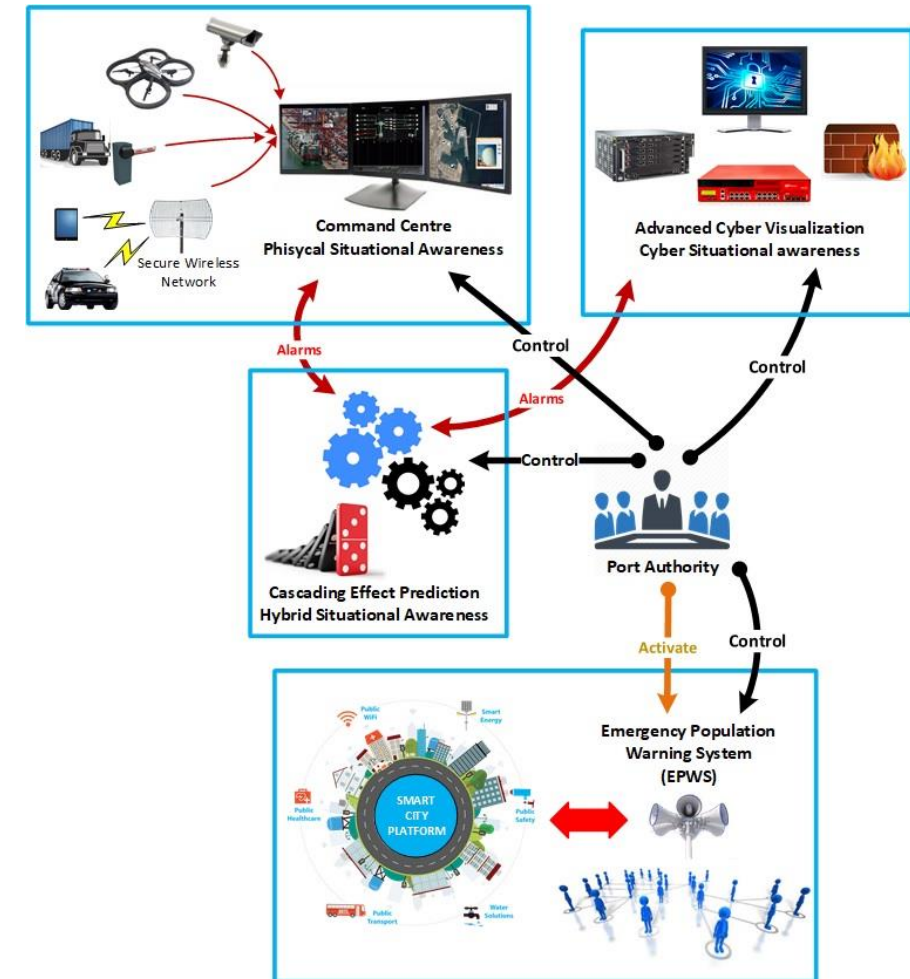
Threat Propagation Engine

- 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





Sauron

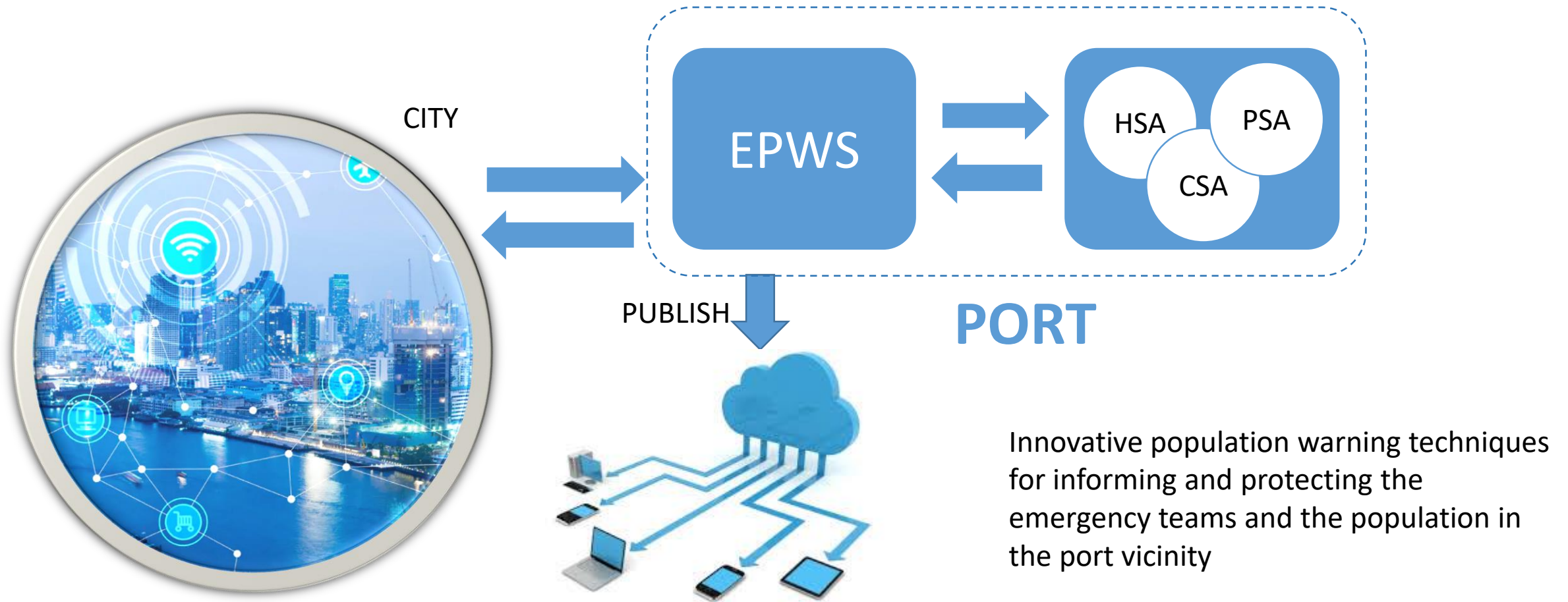
Emergency Population Warning System (EPWS)

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

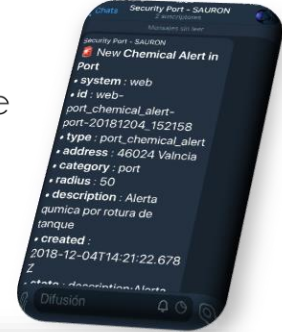
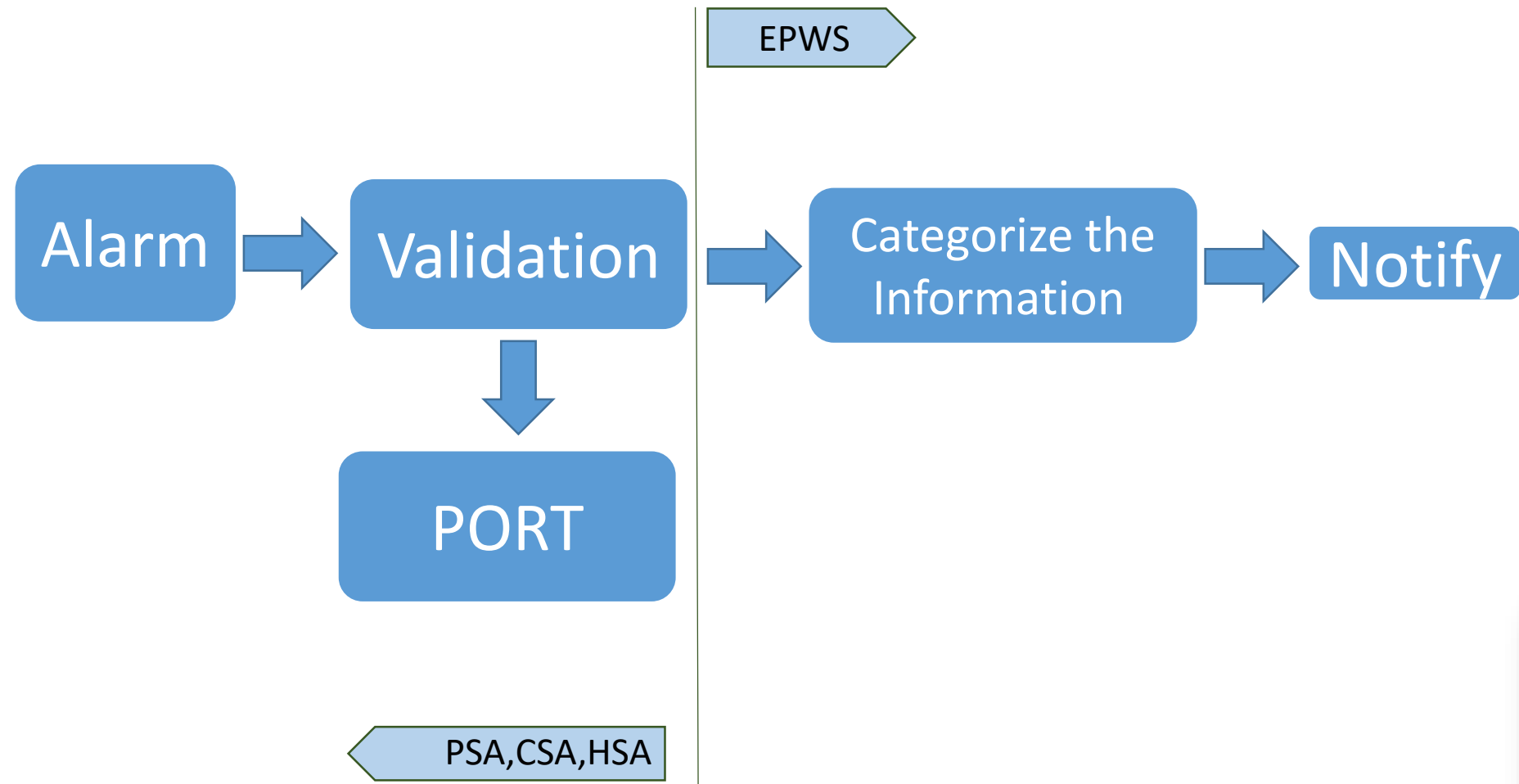
- ❖ Integrability
- ❖ Quickness
- ❖ Easiness
- ❖ Specificity

- 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



Sauron

EPWS Function

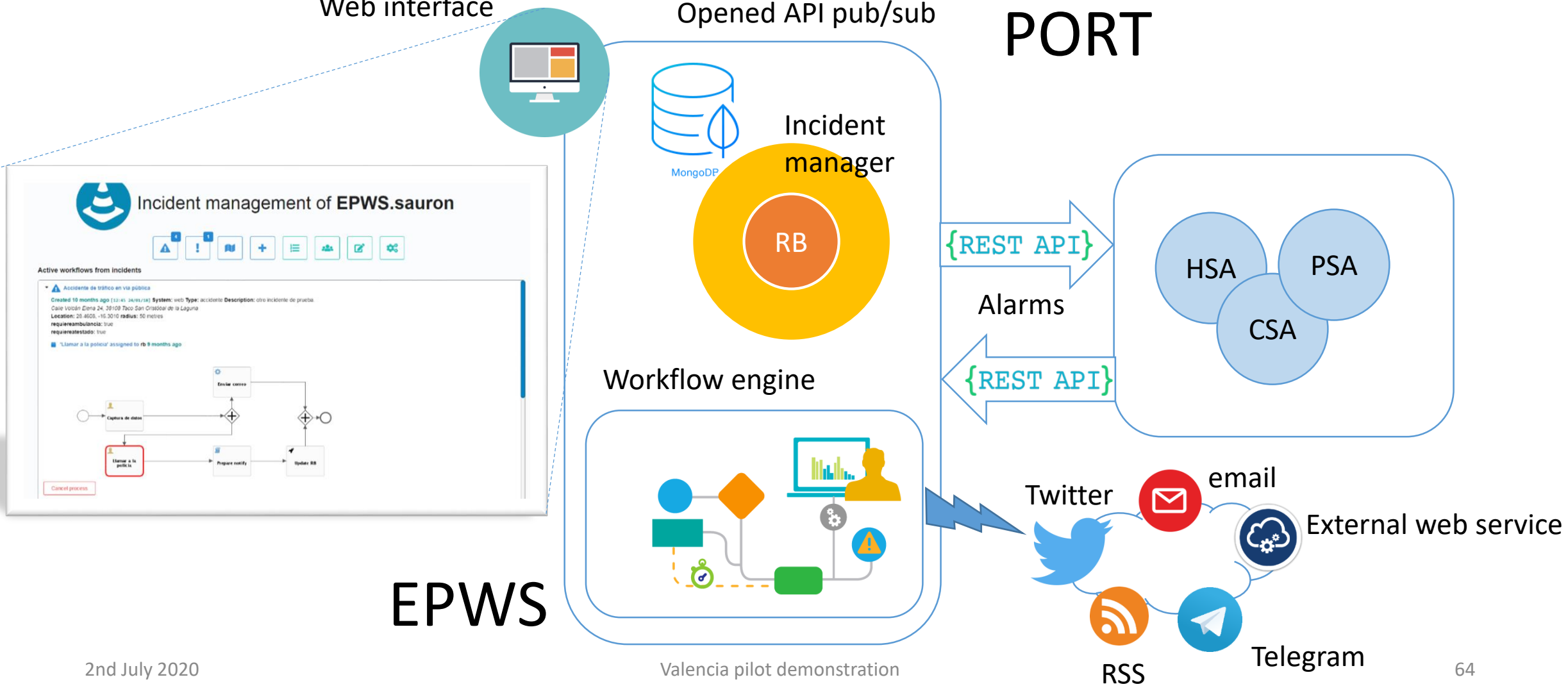


EPWS ↔ PORT

Web interface

Opened API pub/sub

PORT



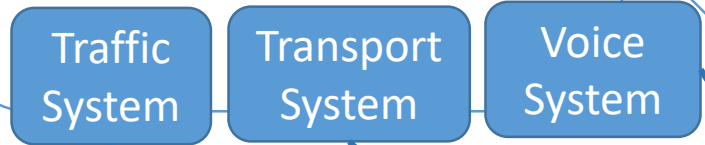
EPWS

CYTY ↔ EPWS



vici valència ciudad inteligente

112



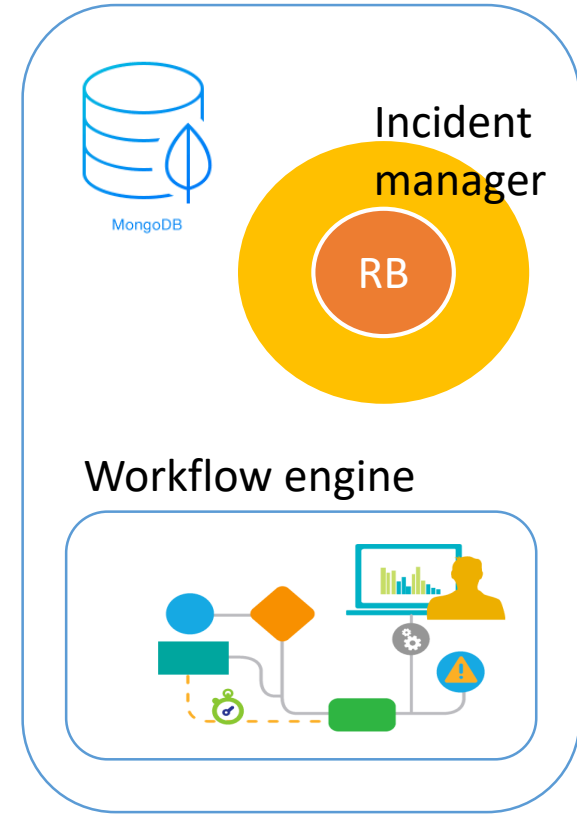
2nd July 2020



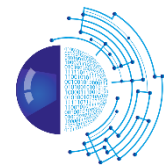
Valencia pilot demonstration



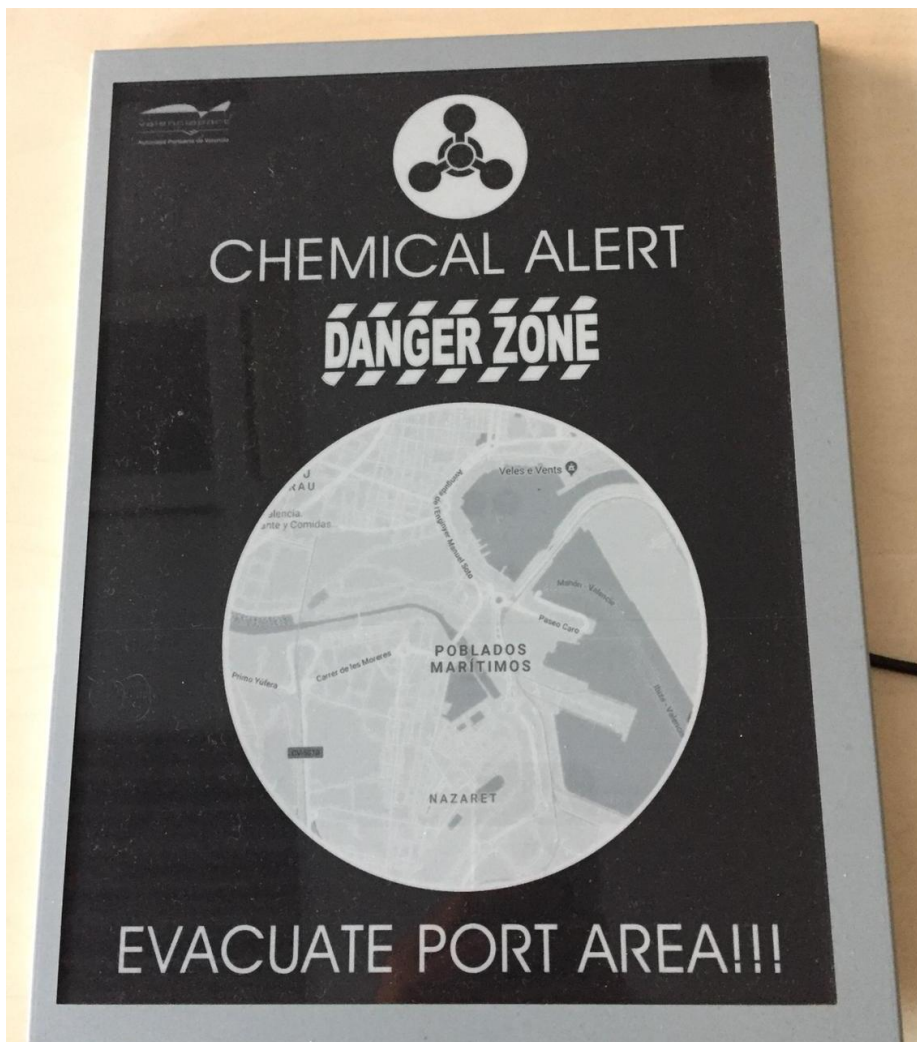
Opened API



EPWS



Alert on Public transport system



2nd July 2020



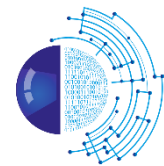
Valencia pilot demonstration





Alert on Valencia App



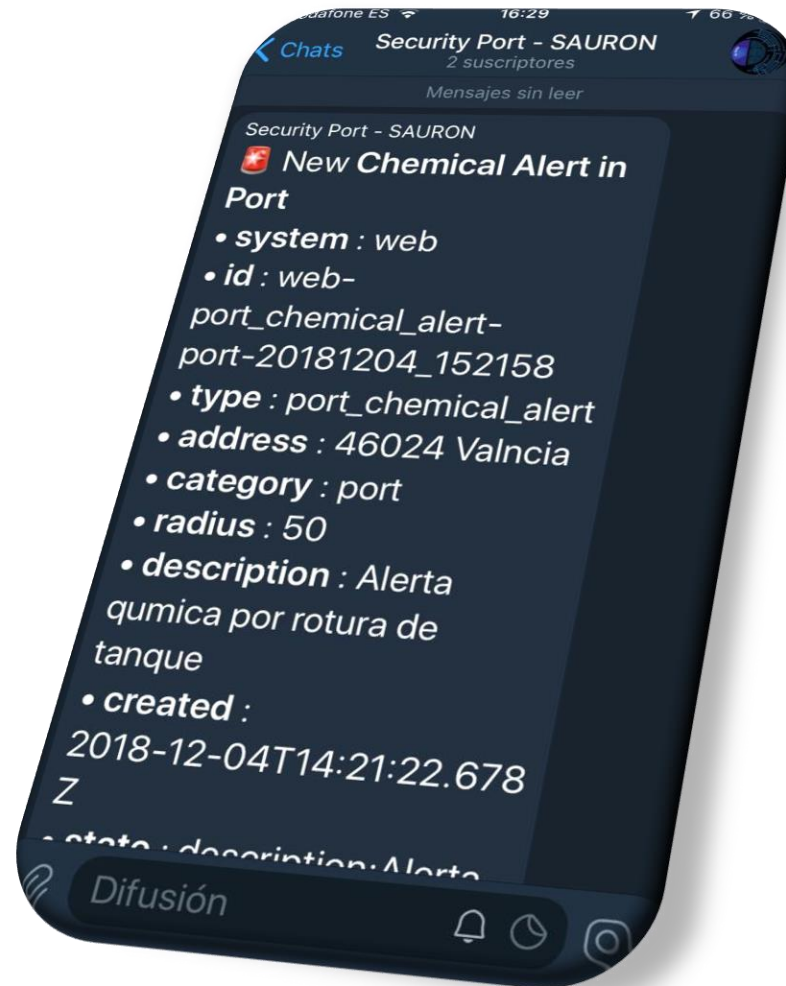


Alert on Traffic system





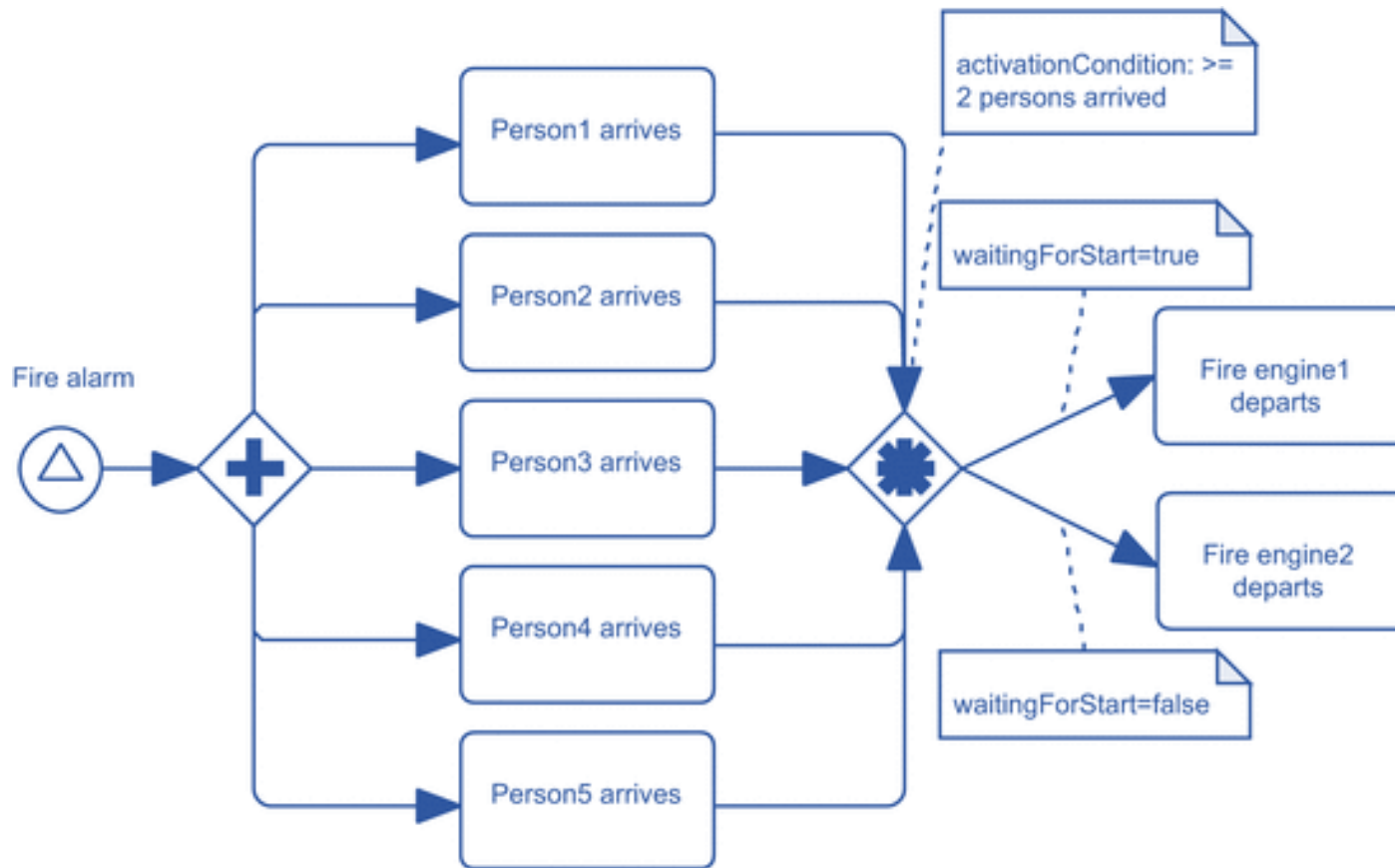
Private/Public-Telegram channels



- ✓ Rescue teams
- ✓ Police
- ✓ Firefighters



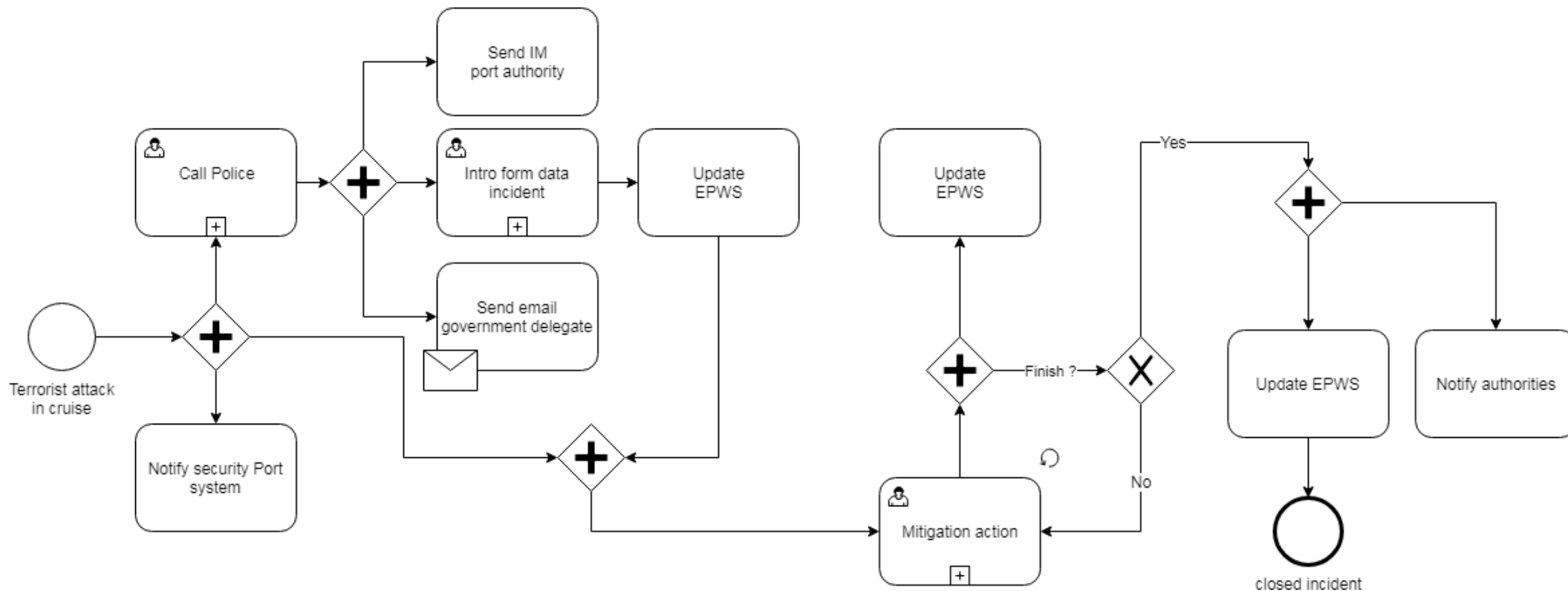
Workflow process



- ✓ 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)



Sauron

• Live Demo!



Incident management of Valencia Port

Open incidents

- sauron sauron-wether-Natural-2018-04-13T13:27:23+02:00**
Created a few seconds ago [13:26 13/04/18] Description: Heavy rain causing destruction
Location: 39.4587, -0.3150 radius: 50 metres
- sauron sauron-incident-Attack-2018-04-13T13:28:53+02:00**
Created a few seconds ago [13:28 13/04/18] Description: Bomb
Location: 39.4437, -0.3192 radius: 50 metres
- sauron sauron-incident-Attack-2018-04-13T13:28:38+02:00**
Created a minute ago [13:25 13/04/18] Description: Gas leak after terrorist attack
Location: 39.4483, -0.2969 radius: 50 metres
- sauron sauron-incident-Accident-2018-04-13T13:25:58+02:00**
Created 2 minutes ago [13:25 13/04/18] Description: Fire in an office
Location: 39.4529, -0.3157 radius: 50 metres

Created by: **etra** 2018. Contact information: soporte@grupoetra.com.

Incident management of Valencia Port

Opened incidents

- 13:25 13/04/18 accident accidente Description: Fire in an office
- 13:25 13/04/18 street accidente Description: Gas leak after terrorist attack
- 13:26 13/04/18 street accidente Description: Bomb
- 13:26 13/04/18 traffic meteorologico Description: Heavy rain causing destruction

Created by: **etra** 2018. Contact information: soporte@grupoetra.com.



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