European Surveillance Systems: Technological and Threat Assessment

Christos Ntrigkogias, Associate Prof. Nineta Polemi
University of Piraeus, Piraeus, Greece

Abstract

Modern European societies face growing terrorism threats alongside with other criminal activities and security incidents. Furthermore, the European zone experiences a migration crisis that reinforces the need for development of innovative surveillance systems. The primary objective of this paper is to conduct firstly a cyber-threat assessment of now-days surveillance systems and secondly to concretely assess specific systems developed in various research projects.

1. Introduction

Modern European societies face varied terrorism threats alongside with other criminal activities and security incidents, adding risks to citizen's life and national safety. Furthermore, the last decade, the European zone experiences a migration crisis that increases the need for high-tech surveillance systems. The primary objectives of this paper are to identify and analyze the threats and vulnerabilities of current surveillance systems and then to conduct a systematic technological as-sessment on newly developed surveillance systems from vari-ous research projects.

2. Cyber-Threat Analysis Of Surveillance Systems

As most of the modern surveillance systems architectures are Web based, they are obviously becoming more and more susceptible to current cyber threats. Furthermore, high level personnel awareness and daily security policies are required, to ensure their security. The current session, defines the most common surveillance systems' related vulnerabilities that lead to higher risks of cyber-attacks.

2.1. OS Vulnerabilities

The majority of the modern surveillance systems include components like Video Management System (VMS), Digital Video recorder (DVR) and Network Video Recorder (NVR) all based on operating systems, either Windows or Linux.

1. Windows based OS: Windows OS vulnerabilities are usually well known and should be monitored and fixed, before they pose a major threat. The most common vulnerabilities are: weak administrator passwords, absence of security patches and OS updates, open useless remote and network ports, external application vulnerabilities (e.g. Adobe Reader) and the use of
2. Vulnerable, insecure and deprecated operating system like Windows XP.
3. Linux based OS: Although for many years the Linux based OS regarded to be less vulnerable than Windows OS, nowadays many Linux high severity vulnerabilities have been exposed (like shell shock), proving that Linux are not always more secure than Windows OS. Like Windows, Linux vulnerabilities are most commonly related to weak root passwords, lack of frequent OS updates, open ports and peripheral application faults.

2.2. Wireless Network Vulnerabilities (Wireless)

Most of the current surveillance systems architecture consists of components that use wireless connections, exposing the whole architecture, if not carefully designed and maintained, into severe cyber threats, like following:

1. Unencrypted Connections: A number of surveillance systems use no connection encryption at all or they adopt deprecated, insecure wireless encryption protocols such as Wired Equivalent privacy (WEP), ending at high risk of cyber-attacks like Eavesdropping, man-in-the-middle, Identity Spoofing, Password based attacks, Application-Layer or even Denial of Service (DDoS) attacks. The way the surveillance data (video, image) are being transferred (encrypted or in clear-text format) and the use or not of data or password encryption algorithms, make it more or less possible for a hacker to access and probably manipulate the data, replacing for example real time video data with prerecorded ones.
2. IP Cameras Weaknesses: The IP cameras are widely used in video based mass surveillance systems, aggregating the possibility of network hacking, if the default, insecure and sometimes public available access credentials are in use. Re-

cent researches show that a huge number of IP based cameras are exposed to hackers, by keeping the default access pass-words.
3. Firewall: Another factor that places a possible security gap into modern surveillance networks is the lack of latest generation firewalls, capable of implementing various filtering rules, like mac address filtering, managing to efficiently analyze the protocols going over the open ports and authenticate only the proper protocols.

2.3. Data storage threats

The surveillance systems' internal components that are re-sponsible for data storage and handling should be always security patched and use the latest advanced techniques in data storage and handling, otherwise they could easily expose the surveillance system to data breaches. Regardless of the architecture of the surveillance system (classic or cloud based), modern data encryption methods like symmetric and asymmetric encryption or even steganography should be applied, so as to avoid data distortion.

2.4. Hardware Vulnerabilities

According to [17] many surveillance systems are not set up in the right way, leaving the data transfer units completely unmasked, with no hardware labeling protection. Every malicious person could easily identify the specifications (product name and manufacturer) of the hardware, being then able to perform a research on the specific hardware exploits and vulnerabilities and gain access thus, to the surveillance network. Also all supported hardware security features, like mesh network nodes and build in security modules, should be always enabled.

3. Technological Assessment Criteria

This section, enhances the related work in [1] and [2], de-fining criteria that are taken into consideration during the technological assessment of innovative research surveillance systems studied in this paper.

3.1. Data Management

The way that a surveillance system collects (e.g. from open data providers) and stores these enormous and heterogeneous volumes of information and the mining and fusion algorithms that it uses during the analysis process, have a strong impact on its total effectiveness.

3.2. Applicability per Sector

Although surveillance is needed in many areas of public life, this paper focuses mainly on surveillance systems used in the following sectors:

- Border control: Among the most important challanges the European Union is asked to face is the illegal immigration which in combination with the drug trafficking incidents and the rest of security cases sharpened the need for increased border surveillance.
- Public transport infrastructures security: Train stations, Airports and Metro areas are Critical Infrastructures (CIs) that modern surveillance systems should be able to determine whether unusual action takes place, like people loitering on metro platforms, unattended baggage etc.
- Maritime surveillance: The elevated threats of terrorism and other criminal activities that all type of ships face up, lay the necessity for innovative solutions to be set up for continuous tracking and monitoring ship traffics and ports in vulnerable trading zones aiming at early identification of threatening situations.
- Public or private CIs security: Most surveillance technologies applied out of the military zone are focusing on the early detection and prevention of the terrorism and/or criminal events, occuring other CIs as Malls, public/private power supply companies, sports infrastructures, schools etc.

3.3. Operational Capabilities

Nowadays, latest demands bring the necessity for surveillance systems with extended operation capabilities. More specifically, the implemented surveillance architectures should embed monitoring sensor networks that are independent weather conditions and can meet the indoor or outdoor requirements for continuous monitoring. The extensive use of the latest technology in monitoring means like UAVs or other mobile electronic devices, could also affect system's total effectiveness.

3.4. Cyber nature

The new generation surveillance platforms need to interact with the organizations' ICT systems, this leads to the need in being designed and implemented as interactive cyber assets. As a result, they need to be implemented in web based architectures, cloud based frameworks, capable to offer surveillance as a service (SaaS). Regarding Cloud-based video surveillance systems, and Video surveillance as a Service (VsaaS) solve traditional video surveillance problems (e.g. high-maintenance, cost of laying communication, poor performance, reliability including decision analysis difficulties.

3.5. Ease of use.

Another factor that could assist a surveillance system in achieving higher score in efficiency is its level of interaction with the user. It should facilitate the work of the operators involved in a surveillance task, from configuring and modelling an installation, to monitoring alarms that occur in a complex environment. Systems that use natural user interfaces permitting wide views of the surveillance areas and clear image - sound alerts, alongside with easier to deploy infrastructures, allow the operators to focus on incident detection and management within the shortest feasible time.

3.6. Scalability

The scalability of a surveillance system is one of the most significant evaluation criteria. Scalability describes a system's ability to integrate extra components according to surveillance requirements and is indispensable for recent complex distributed environments. So, in order to comply with current needs for extensibility, a surveillance system should incorporate an architecture that allows simpler components integration together with flexible algorithms that are able to recognize the additional hardware without disrupting the overall ability of the system to evaluate the alarm conditions.

3.7. Interoperability

Interoperability is defined as the ability of a collection of communicating entities to share specified information and operate according to shared operational semantics in order to achieve a specific purpose within a given context [3]. There can be data (syntactic or semantic) interoperability or legacy interoperability. Ongoing security environment is highly characterized by heterogeneity, as it is composed of many surveillance systems that need to interoperate and perform their tasks efficiently, while they are consisting of different platforms and components.

1. Data Interoperability: An interoperable video surveillance system for example, should be able to exchange data with other systems, namely it should not only efficiently handle all common video or images format but also should produce common file layout. To address this problem integrated surveillance frameworks should utilize technologies including techniques for tagging different multi-media types with descriptive metadata to support multi-level correlation of surveillance and other data intelligence from distributed heterogeneous sources and networks. Generally an essential key to interoperability in data sharing is to ensure that surveillance systems incorporate architectures able to adhere to standards and mutually acceptable solutions available on the market rather than custom and proprietary solutions.
2. Legacy Interoperability: Legacy surveillance system interoperability enables data and information generated by a surveillance system to be accessed and (re-)used in a meaningful way by another system, whether or not the latter is based on outdated technologies. To address this problem, modern surveillance systems should incorporate frameworks that subscribe to common, all-encompassing data models, compatible with pre-existing systems and thus resolving their syntactic and semantic differences.

3.8. Decision support

A decision support system (DSS) is a computer-based in-formation system that supports end-users in their decision making processes and is mainly employed to speed up decision making processes and to improve the decision maker's abilities [10]. Surveillance systems should incorporate advanced decision and knowledge management technologies and visualization techniques to facilitate rapid analysis of action data. Recent architectures support distributed intelligence platforms that enable decision support for automated detection, recognition, geolocation and mapping, including intelligent decision support at various levels to enhance situation awareness.

4. Surveillance Systems Technological Assessment

4.1. The VANAHEIM System

VANAHEIM developed innovative surveillance components for autonomous monitoring of complex audio/video surveillance infrastructure, such as the ones prevalent in shopping malls or underground stations [4]. This sub-section evaluates the project based on the predefined criteria:

1. Data Management (Open data - Big data): VANAHEIM audio-video recording system has been deployed, configured and finally integrated into RATP Paris [6] and GTT Torino [5] existed surveillance platforms, resulting to a more innovative

and efficient system, that maintains existing open data management techniques [5], [6].
2. Applicability per Sector: VANAHEIM serves: CCTV end-users such as security/safety operators, public infrastructure managers, Surveillance system designers, Security related hardware or software manufacturers and suppliers, both from the public and the private sector [4].
3. Usage Capabilities: By using human behavioural cues and social modes like space occupancy the system architecture consists of subsystems capable of detecting anomalies in human behaviour and it is mainly applicable to indoor surveillance monitoring of crowded, big scale infrastructures.
4. ICT (Web, Cloud, SaaS): The VANAHEIM system was deployed in Turin and Paris metro areas security surveillance systems, that do not currently provide either Cloud Infrastructures nor Surveillance as a Service (SaaS), according to [4].
5. Ease of Use: During the evaluation methodology that included both a qualitative and a quantitative assessment of VANAHEIM results, the involved GTT/RATP personnel was requested to answer specific questions expressing their point of view while operators were asked to play with the prototype system autonomously with the only help of a user. The highest score after the end of the process was given to the ease of use [4].
6. Scalability: The VANAHEIM system has been deployed in two different CCTV surveillance platform already used in European metros (Turin and Paris). Its team managed to develop efficient video analytics modules that were finally integrated into a Video Management Solution featuring an innovative video wall module, guaranteeing the system's scalability.
7. Architecture is highly modular, able to handle any common audio or video format derived from the algorithms . On the subject of legacy interoperability some audio/video datasets could be provided in open data format and used by relevant security surveillance systems, allowing common information sharing.
8. Decision support: The build in audio based alongside the event based selection mechanisms that were implemented allow the selection of the most "meaningful" audio/video streams, achieving the right balance between the empty and occupied content to present to the experts so as to lead them to the correct decision making.

4.2. The SV3D System

The federating objective of the SV3D project consists in developing the technology required to offer the surveillance operator the facilities required to navigate into a virtual 3D world, by incorporating 3D-positioning technology in all as-pects of an integrated security system, with the support of a dedicated information system for storing and retrieving all necessary spaces, objects and events which are part of the whole process, as defined in [7].

1. Data Management (Open data - Big data): The database model used for data storage and handling is a traditional RDBMS (MySQL Server v5.2.1) and it is not capable of efficiently adopting latest mechanisms in data mining like those applied to Big / Open Data modern databases and large scale Cloud Infrastructures.
2. Applicability per Sector: SV3D is a modern, open and secure platform introducing new 3D and geometrical features, enhancing human based alarm detection and aiming primarily at security surveillance of cramped public critical infrastructures (train stations, schools etc).
3.Usage Capabilities: Since its main achievement is based on introducing the features and benefits of the virtual 3D world to the existing surveillance infrastructures according to [7], it is capable of efficiently cooperating with both indoor and outdoor end – point equipment.
4. ICT (Web, Cloud, SaaS): The SV3D architecture could easily adopt some of the new ICT trends such as virtualization, bearing in mind its scalability design. Furthermore the fact that the SV3D system is designed to be highly flexible and to integrate on demand, new drivers for external devices or platforms, the current architecture allows the dynamic loading of additional drivers through a very simple integration mechanism.
5. Ease of Use: During the evaluation of the SV3D video-surveillance system the involved staff conducted an experiment in which two similar tasks carried out; one with the SV3D platform and the other with a traditional multi- screen surveillance system. The results pointed out that both user's satisfaction and visual comfort obtained reasonable rates [8].
6. Scalability: Following the modern market needs which require a surveillance architecture that allow more than one unified platforms, the SV3D surveillance system allows more than one integrated platform (like Milestone XProtect or ONNSI Ocularis) and/or individual devices such as video analytics components, cameras or video recorders be simultaneously connected, thereby proving its scalability [8].
7. Interoperability: Many issues concerning data and legacy interoperability were resolved, for example video data format compatibility issues with some

Web browser applications demanded, in the case of Milestone platform for instance, the implementation of video transcoders in order to obtain a unique standardized video format and to also guaranty data interoperability of the final platform [8].

8. Decision support: The SV3D architecture based on the System Manager was designed in a way that new virtual 3D features could be introduced at any level of the processing chain in a surveillance system, in order to optimize video analytics, operator visualization task and decision making [8].

4.3. The MOSAIC System

The MOSAIC Platform involves multi-modal data intelli-gence capture and analytics including video and text collaterals enabling decision support during the surveillance investigation.

1. Data Management (Open data - Big data): A text mining component was created suitable for crawling web sites that allows users to crawl internet sources and obtaining documents of various formats, that are being stored at the appropriate data store component [10]. The Mosaic's architecture and its manner of data management (crawling, storing, mining) gives it the ability to follow the new trends in data and extract knowledge even from open data, derived from various open sources (see Figure 1).

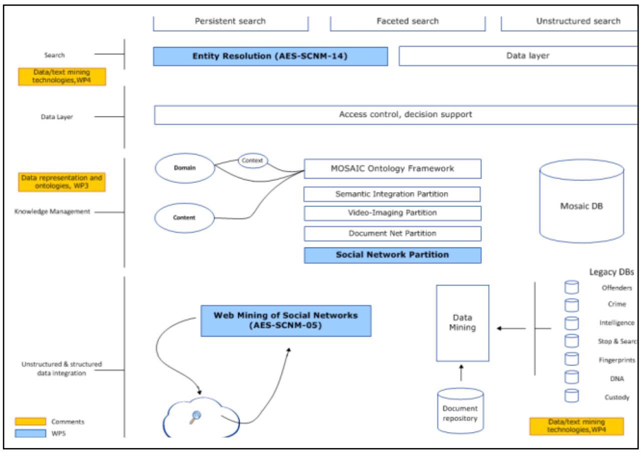

Persistent search
Faceted search
Unstructured search
Search
Data/text mining technologies,WP4
Entity Resolution (AES-SCNM-14)
Data layer
Data Layer
Access control, decision support
Data representation and ontologies, WP3
Knowledge Management
Domain
Context
Content
MOSAIC Ontology Framework
Semantic Integration Partition
Video-Imaging Partition
Document Net Partition
Social Network Partition
Mosaic DB
Legacy DBs
Offenders
Crime
Intelligence
Stop & Searc
Fingerprints
DNA
Custody
Web Mining of Social Networks (AES-SCNM-05)
Data Mining
Document repository
Unstructured & structured data integration
Comments
WP5
Data/text mining technologies,WP4

Figure 1. MOSAIC System design.

2. Applicability per Sector: Mosaic platform could be used by national and local law enforcement authorities, video surveillance infrastructure operators, private security service providers. The developed system aims to support police end users including analysts, administrators, CCTV operators, and staff supervisors in crime prevention and crime fighting operations [10].

3. Usage Capabilities (Indoor/Outdoor Weather Dependence): Part of the assessment process consisted of the evaluation of a number of long surveillance videos, recorded in outdoor environments [10], proving that MOSAIC system is independent of weather conditions and could be used both in indoor and outdoor conditions.

4. ICT (Web, Cloud, SaaS): Regarding Information Technology the project led to the development of a Social and Criminal Network Analysis component (see Figure 2) which embeds a web crawler tool. The implementation of web crawler responsible for searching the web and feeding the platform's built-in components with all the gathered information, confirms the incorporation of a web based platform architecture.

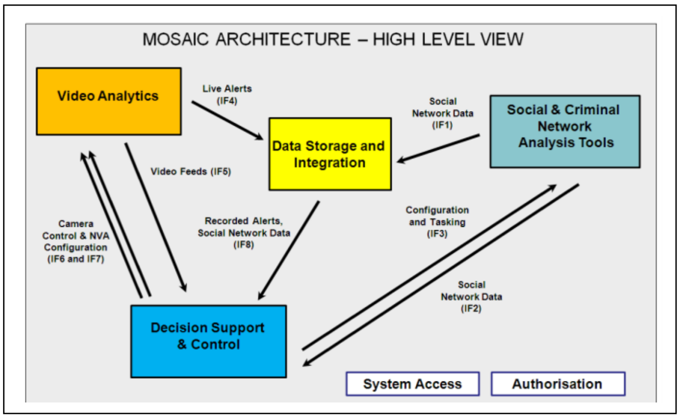

MOSAIC ARCHITECTURE – HIGH LEVEL VIEW
Video Analytics
Live Alerts (IF4)
Data Storage and Integration
Social Network Data (IF1)
Social & Criminal Network Analysis Tools
Video Feeds (IF5)
Camera Control & NVA Configuration (IF6 and IF7)
Recorded Alerts, Social Network Data (IF8)
Configuration and Tasking (IF3)
Social Network Data (IF2)
Decision Support & Control
System Access
Authorisation

Figure 2. Mosaic Architecture – High Level

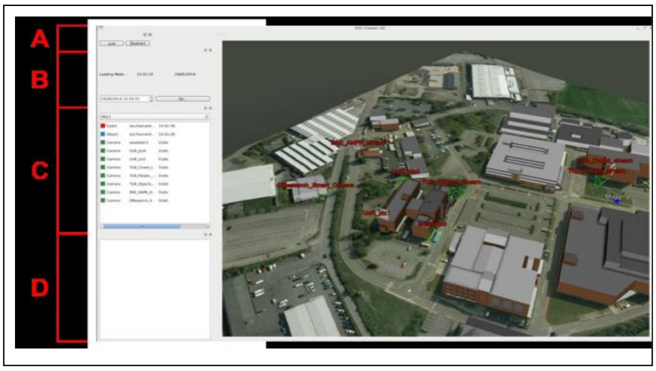


Figure 3. VIKI Main Window

5. Ease of Use: Despite the lack of a multi functional final user interface, the developed platform provides the users with graphical tools enclosed to its main components, adding thus points to MOSAIC's ease of use and gaining an overall satisfaction level of approximately 80% during the evaluation process[10].

6. Scalability: In order to help data analysts in their data mining process, the developed SCN component offers the user the ability to generate a candidate

social or criminal network for each specific investigation. The fact that the user can not only add nodes to the network manually but also importing them from an available source [10], raises MOSAIC's platform scalability.
7. Interoperability: The MOSAIC system incorporates a visualisation system (VIKI) (see Fig. 3) that has been initially developed by BAE SYSTEMS and later has been properly amended in order to be compliant with the ONVIF standard [10]. The agreement with this global standard that presupposes system's specifications like interoperability between IP-based physical security products regardless of manufacturer, ensures platform's interoperability.
8. Decision support: MOSAIC managed to provide a decision support system for ensuring the safety and security of critical assets, by combining data intelligence and advanced video analytics techniques [9]. Both software (e.g. semantically enriched 3d visualization tool) and hardware (e.g. hardware-based detection of camera tampering events) solutions have been implemented aiming to achieve better decision support results.

4.4. The SECTRONIC System

SECTRONIC is a 24 hours surveillance system which communicates with a local response system (e.g. alarms, sound waves) and with an onshore control center, for early detection and prevention of any kind of malicious behavior, providing response capability. Its main objective of the project was to develop an integrated system for increasing the security of maritime infrastructures covering ports, passenger transport and energy supply against these threats [10].

1. Data Management (Open data - Big data): Regarding data, an in depth assessment of open data as earth observation suitable for retrieval of sea state (wind, waves, current and sea surface temperature), sea ice state (ice concentration and drift), improved ship detection and route anomalies estimation had been made and the appropriate algorithms had been developed. [10].
2. Applicability per Sector: SECTRONIC is an integrated system which, by the combination of radar, sonar, infrared and visible cameras, AIS receivers and auxiliary sensors, anomaly detection algorithms, aims primarily at the security surveillance of maritime infrastructures covering ports, passenger transport and energy supply against terrorism and piracy.
3. Usage Capabilities: SECTRONIC is capable of ob-serving, characterizing and tracking any object that could affect a maritime infrastructure's security, acting independently of weather conditions and with the ability of remaining efficient both indoors and outdoors even at dark night operations [10].
4. ICT (Web, Cloud, SaaS): A web based integration plat-form has been implemented, integrating some of the latest wireless technology techniques, that embeds an online information hub which enables security related observations to be exchanged between the maritime units and an onshore control and response unit [11].
5. Ease of Use: The long-term evaluation methodology included daily tests performed by end-users at the port of Rotterdam. The evaluation results showed that an intuitive, user-friendly human interface has been developed, and most operators were "impressed by the command and control display and the possibilities of the system. The functionality and ease of use of the touch screen make it very intuitive and requires little training" [11].
6. Scalability: SECTRONIC is in full compliance with the objectives of an integrated e-navigation system [11]. Ac-cording to [12] one of the core objectives of an e-navigation system is to be scalable in order to be successfully integrated and used by any kind of vessel.
7. Interoperability: In the direction of avoiding potential conflicts between vessels or between vessels and navigation / traffic management agencies, the e-navigation system approach requires among others that all the compliant systems, need to facilitate the mutual compatibility and interoperability of equipment.
8. Decision support: A draft type program for a Routing Decision Support System (RDSS) certification scheme had been developed, that incorporates the minimum safety, security and efficiency requirements for the functions provided by RDSS.

4.5. The PERSEUS System

PERSEUS is an EU maritime surveillance system that inte-grates existing national and communitarian installations and at the same time incorporates innovative technologies. It enhances maritime surveillance from coastal regions to high seas through a collaboration manner across European Member States.

1. Data Management (Open data - Big data): A common Information Sharing Environment was developed, incorporating improved data algorithms, resulting to the integration of various open data sources like weather forecasts, geographical data,

space born AIS and thus allowing the online data sharing.

2. Applicability per Sector: PERSEUS intends to enhance maritime infrastructures security surveillance, from ports to open seas, through the intelligence use of surveillance.

3. Usage Capabilities: PERSEUS system’s developed platform consists of built in interoperable components and is externally supported by ground, aerial and sea platforms that enhance its usability under almost any weather conditions.

4. ICT (Web, Cloud, SaaS): PERSEUS architecture design is mostly web based and include the National Control Centre (NCC), the Regional Control Centre (RCC) and the Local Control Centers (LCC) which are connected hierarchically, ending at an entirely web oriented user correspondence [13].

5. Ease of Use: The web based user interaction component support an easier system deployment and also manages to empower a rich usage for all end-users, through a fully integrated surveillance picture.

6. Scalability: The PERSEUS scalable data model that is used for the scope of interconnecting different systems is fully expandable and ready for further evolutions. It represents a unique experience of research in the area of maritime surveillance. A lot of surveillance assets like surveillance air-vehicles and drones, coastal stations, mobile units, ad hoc communication networks, software applications implementing new operational functionalities such as task orders were put to concurrent operations, according to [13].

7. Interoperability: The PERSEUS Data model delivers the capability to exchange data in a common framework by consolidating all potential information exchanges required to create an integrated maritime surveillance space, managing to maximize the interoperability between multinational heterogeneous systems.

8. Decision support: PERSEUS enhances decision sup-port by enhancing Command and Control capabilities on regional level. Moreover one of the objectives of the PERSEUS deployed exercises was to demonstrate the benefits of real time information sharing between different Member States, incorporate new sensors/assets and channels of communications for better decision making, and it was achieved by evaluating the technologies, standards and operational processes and procedures within real operational environments that facilitated the collaboration between industry and end users [13].

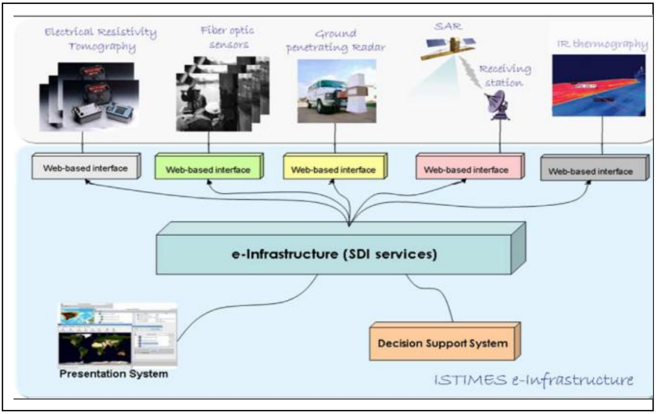


Figure 4. ISTIMES system architecture

4.6. ISTIMES System

ISTIMES is a modular and scalable ICT based system, exploiting distributed and local sensors, aiming at non-destructive electromagnetic monitoring, achieving to enhance the reliability and safety of critical transport infrastructures. In addition, the system is able to provide real and near real time information about the infrastructure status to improve decision support for emergency and disasters stakeholders.

1. Data Management (Open data - Big data): ISTIMES uses web techniques and service -oriented - technologies for data processing and data correlation/integration in order to gain the ability to analyze massive volumes of data arising from the use of different sensing techniques.

2. Applicability per Sector: The ISTIMES approach has enhanced the reliability and safety of critical transport infra-structures, while its modular architecture extended its applicability to other critical infrastructures, like dams.

3. Usage Capabilities: The extensive network of various electromagnetic static or mobile sensors supported by specific

Satellite and airborne measurements that can be remotely controlled increases system’s capabilities regardless of the weather conditions.

4. ICT (Web, Cloud, SaaS): The developed ICT architecture is based on web sensors and service-oriented-technologies that comply with specific end-user requirements, including economical convenience, exportability, efficiency and reliability provide web services in order to exchange data and to control the dynamic sensor’s network, taking advantage of all the new ICT trends. The architecture

5. Ease of Use: The developed system e-infrastructure architecture incorporates a built in user friendly, multi informational web interface, managing to present the monitoring results in a very

comprehensible way to the experts (see Fig. 4).Also the integration of electromagnetic technologies with new ICT information systems facilitate remotely controlled monitoring and surveillance and near-real time data imaging of the critical transport infrastructures.

6. Scalability: ISTIMES achieved to implement a scalable System Architecture able to provide services via Web. The network architecture accommodates a wide range of heterogeneous sensors, static and mobile, and can be easily scaled up to allow the integration of additional sensors, according to the field operation needs.

7. Interoperability: System's high interoperable ICT architecture is based on web sensors and service oriented technologies, allowing the connection and control of other network interfaces, enhancing the modularity of the monitoring system.

8. Decision support: ISTIMES uses web techniques and service -oriented - technologies for data acquisition and pro-cessing, leads to an efficient presentation of the monitoring/diagnostics results to Decision Makers. The system inte-grates many different non-invasive technologies like data cross correlation and novel concepts of information fusion which permit a multi-method, multi-resolution and multi-scale evidence detection and improves the process of decision making.

4.7. The TALOS System

TALOS is a mobile, autonomous land border surveillance system based on unmanned vehicles for protecting European land borders. The complete system is composed of both aerial and ground unmanned vehicles, supervised by command and control center (C&C Center).

1. Data Management (Open data - Big data): The geo-graphical data, used by the ground and aerial unmanned units command center was collected and being stored in a standard GIS database (PostgreSQL) using traditional techniques. The data storage architecture is most probably not able to cope and with and endorse new ICT trends in data management.

2. Applicability per Sector: TALOS aim to be used for European border surveillance. Unlike the conventional border protection systems which are based mainly on expensive ground facilities installed along the entire length of the border complemented by human patrols, the TALOS system proved to be more versatile, efficient and flexible.

3. Usage Capabilities: The developed architecture is limited to outdoor conditions working. Additionally the extensive use of aerial and ground unmanned vehicles, on which TALOS platform is based, places restrictions in its outdoor usage capabilities, depending on the operation limits of the vehicles.

4. ICT (Web, Cloud, SaaS): Even though the implemented platform endorses the results of various researches in the fields of mapping and localization (GIS), artificial intelligence, low level vehicle control and robotic navigation it seems that does not endorse many of the modern ICT tendencies regarding data management (e.g. Big data architectures, Cloud technology).

5. Ease of Use: The developed e-Infrastructure consists of various components; all being controlled by web based graphical user interfaces facilitating the operators. The built in soft-ware components allow for better planning, monitoring and control of the mission from the commander and operator point of view, with a high degree of autonomy letting the Commander and Operator to work in a comfortable way [14].

6. Scalability: TALOS developed the ability to easily change the system scale due to the development of scalable algorithms and the use of mobile unmanned vehicles instead of a fixed infrastructure. It is easily configurable to meet the requirements of a particular mission area, by selecting an accordant set of unmanned vehicles to be deployed.

7. Interoperability: TALOS network infrastructure is based on the JAUS protocol. This protocol is used at application level for interoperability between subsystems and along with the adoption of the WIMAX technology in the communication subsystem, manages to maintain system's interoperability [14].

8. Decision support: The project's e-infrastructure incorporates features and components that could be used to generate a sufficient decision support system.

4.8. The I2C System

I2C is a new generation end to end sea border surveillance system integrating key existing or in development capacities to track all vessel movements and detect abnormal behavior.

1. Data Management (Open data - Big data): I2C is a surveillance platform incorporating new techniques of data acquisition, with the ability to handle data obtained from various sensors and/or open data providers, using new algorithms for data correlation and fusion.

2. Applicability per Sector: It uses intelligent surveillance aiming to enhance European maritime security. It is able to elaborate a common intelligent situational picture enriched with a lot of information appending to vessel tracks, activities and

characteristics, to detect abnormal vessel behavior and early identify possible threats and also has the ability to sup-port common information sharing.
3. Usage Capabilities: This new platform enhanced with information from data service providers led to a continuous and all weather coverage of the European sea borders, acting mainly to the open sea.
4. ICT (Web, Cloud, SaaS): I2C generates an enriched common operational traffic picture, through the establishment of web connections to existing databases (Trafic2000, Lloyd's Register etc.), leading thus to the development of a web based architecture [15].
5. Ease of Use: A Human Machine Interface was developed to provide the operators the common intelligence operational picture and visualize the generated alarms, enhancing platform's "user friendliness".
6. Scalability: The I2C surveillance platform integrates a multi system, operational network capable of adjusting its scale in order to be adapted to all operating conditions.
7. Interoperability: I2C data exchange is based on telecommunication satellite (DVB) and Distributed System Inter-communication Protocol (DSiP), demonstrates system of systems secured interoperability.
8. Decision support: Its adapted supporting tools led to the development of a multiuser, multi-pointer tactile human machine interface (based on the INTUILAB prototype) appropriate for collaborative decision makers (multi – hypothesis decision tree).

4.9. The P-REACT System

P-REACT is a low cost surveillance platform able to detect Petty Crime incidents. The solution will encompass intelligent video and audio sensors to detect petty crime incidents, a cloud based monitoring, alert detection and storage platform [16].
1. Data Management (Open data - Big data): Regarding data management the P-REACT proposes an architecture solution that is divided into two core building blocks: the Embedded system and the Cloud. The main component of the embedded platform (see Fig. 5) is the Embedded System Manager (ESM) that utilizes a number of traditional databases used for storing data related to sensors or analytics algorithms. Furthermore, the cloud approach, utilizes more novel methods following the new trends in cloud storage, enabling the operator to perform content – based queries [16].
2. Applicability per Sector: P-REACT is a surveillance platform that focused on increasing the ability of the security personnel to react when a security incident (petty crime) oc-curs.
3. Usage Capabilities: All the audio and video sensors adopted by the P-REACT platform are capable of efficiently working both in outdoors and indoors environments, increasing the detection of petty crimes in several conditions.
4. ICT (Web, Cloud, SaaS): The cloud part of the project's architecture serves as a centralized knob where all the embedded subsystems are reporting. It hosts a storage network, consisting of cloud databases, where all the uploaded data is stored, as well as advanced analytics modules.

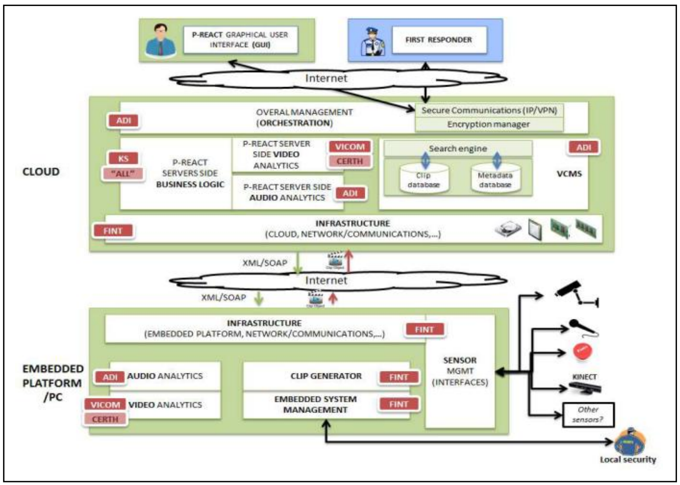

P-REACT GRAPHICAL USER INTERFACE (GUI)
FIRST RESPONDER
Internet
ADI
OVERAL MANAGEMENT (ORCHESTRATION)
Secure Communications (IP/VPN)
Encryption manager
CLOUD
KS
"ALL"
P-REACT SERVERS SIDE BUSINESS LOGIC
P-REACT SERVER SIDE VIDEO ANALYTICS
VICOM
CERTH
P-REACT SERVER SIDE AUDIO ANALYTICS
ADI
Search engine
Clip database
Metadata database
ADI
VCMS
FINT
INFRASTRUCTURE (CLOUD, NETWORK/COMMUNICATIONS,...)
XML/SOAP
Internet
XML/SOAP
INFRASTRUCTURE (EMBEDDED PLATFORM, NETWORK/COMMUNICATIONS,...)
FINT
EMBEDDED PLATFORM /PC
ADI
AUDIO ANALYTICS
VICOM
CERTH
VIDEO ANALYTICS
CLIP GENERATOR
FINT
EMBEDDED SYSTEM MANAGEMENT
FINT
SENSOR MGMT (INTERFACES)
KINECT
Other sensors?
Local security

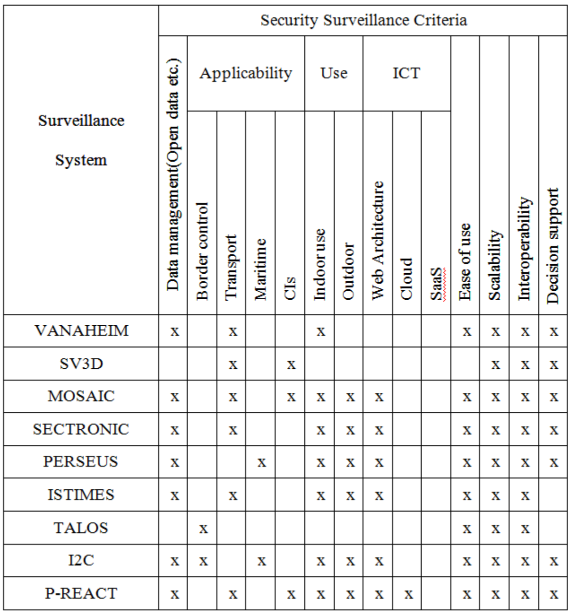
Figure 5. P-REACT system architecture

5. Ease of Use: For the needs of human operators inside the Business Logic Component, a graphical user interface (GUI) has been implemented enabling user interaction and control, facilitating the work of operator [16].
6. Scalability: The overall architecture is highly modular as additional embedded systems, cameras and cloud resources will be seamlessly added on demand, conversely with other commercial solutions that minimize their scalability factor by
having an upper limit on the number of sensors (video /audio) they can manage [16].
7. Interoperability: According to [16] many interoperability issues have been addressed, regarding both Embedded System and the Cloud that are able to cope with several interoperability requirements stemming from the different needs of project's stakeholders.
8. Decision support: The decision making process is undertaken by the Business Logic module (see Fig. 5), which is the key component that brings the final results of all the analytic algorithms to the experts.

4.10. Surveillance Systems Assessment table

The next table summarizes the assessment of various innovative surveillance systems developed in current European research projects:

Table 1. European Security Surveillance Systems Assessment



Surveillance System	Security Surveillance Criteria													
	Data management(Open data etc.)	Applicability				Use		ICT			Ease of use	Scalability	Interoperability	Decision support
		Border control	Transport	Maritime	CIs	Indoor use	Outdoor	Web Architecture	Cloud	SaaS				
VANAHEIM	x		x			x					x	x	x	x
SV3D			x		x							x	x	x
MOSAIC	x		x		x	x	x	x			x	x	x	x
SECTRONIC	x		x			x	x	x			x	x	x	x
PERSEUS	x			x		x	x	x			x	x	x	x
ISTIMES	x		x			x	x	x			x	x	x	
TALOS		x									x	x	x	
I2C	x	x		x		x	x	x			x	x	x	x
P-REACT	x		x		x	x	x	x	x		x	x	x	x

5. Conclusions and Further Research

Vulnerabilities of surveillance systems have been identified in this paper. Specific controls need to be undertaken by the developers with which they will prevent their exploitation. In this paper we assessed, based upon specific criteria, innovative (research-based) European Surveillance systems. Similar assessment will be useful for all commercial systems. The privacy component of these systems remain among the open research problems and will be considered in our future work.

6. References

[1] SAPIENT Project Deliverable 1.1, Smart Surveillance - State of the Art, [Online]. Available: http://www.sapient project.eu/ (Access Date: 10 September, 2015).

[2] Common Criteria, Common Methodology for Information Security Evaluation, V3.1, July 2009.

[3] Kennedy O. Ondimu, Geoffrey M. Muketha. Challenges in Achieving Interoperability in Distributed Systems: a Survey of Literature.Int. J. Emerg. Sci., 2(4), 619-631, December 2012.

[4] Integrating innovative audio/video analysis in real-world surveillance platforms: VANAHEIM legacy publication, C. Carincotte, A. Forchino, J.-M. Odobez, F. Bremond, F. Sabourin, B. Ravera, A. Grifoni, K. Grammer, 2014.

[5] Ratp and Open Data, [Online]. Available: http://www.ratp.fr/opendata (Access Date: 10 September, 2015)

[6] Torino Open data, [Online]. Available: http://opendata.5t.torino.it/gtfs/torino_it.zip (Access Date: 10 September, 2015).

[7] Final Report Summary - SV3D (Surveillance platform based on multi-source video analytics, localized data and cognitive interfaces), [Online]. Available: http://cordis.europa.eu/result/rcn/148676_en.html (Access Date: 16 September, 2015).

[8] SV3D Public Summary, [Online]. Available: http://cordis.europa.eu/docs/results/286/286801/final1-sv3d-publishablesummary-25apr13.pdf (Access Date: 16 September, 2015).

[9] Guidelines and recommendations for using Milestone XProtect in a virtual server environment, John Rasmussen, September 22, 2014.

[10] MOSAIC Project, [Online]. Available: http://mosaic-fp7.eu/ (Access Date: 18 September, 2015).

[11] SECTRONIC final publishable summary report_v2.1 [Online]. Available: http://cordis.europa.eu/docs/results/218245/final1-final-publishable-summary-report-v2-1.pdf (Access Date: 21 September, 2015).

[12] Development of an E-Navigation Strategy. Sub-Committee on Safety of Navigation, International Maritime Organization, London, 12 May. IMO NAV 53/13 2007.

[13] PERSEUS European project [Online]. Available: http://www.perseus-fp7.eu/ (Access Date: 22 September, 2015).

[14] TALOS (Transportable Autonomous patrol for Land bOrder Surveillance) final report v4 [Online]. Available: http://cordis.europa.eu/docs/results/218081/final1-talos-final-report-v4.pdf (Access Date: 22 September, 2015).

[15] Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification, M Morel, S Claisse - IEEE Conference Publishing, 2010 - i2c.eu

[16] P-REACT_Deliverable_D.2.3_V3.0.pdf, [Online]. Available: http://p-react.eu/ (Access Date: 23 September, 2015).

[17] Does CCTV put the public at risk of cyberattack, [Online]. Available:https://securelist.com/blog/research/70008/does-cctv-put-the-public-at-risk-of-cyberattack/ (Access Date: 22 December, 2015).

[18] 12 Security Camera System Best Practices – Cyber Safe, [Online]. Available:http://www.eagleeyenetworks.com/security-camera-system-cyber-best-practices/ (Access Date: 23 December, 2015).