ZONeSEC

FP7-607292

Towards a EU framework for the security of Widezones

ZONESEC CONFERENCE REPORT

Deliverable Identifier:	D.13.3
Delivery Date:	**Sep** 30, 2018
Classification:	Restricted
Editor(s):	**Aljosa Pasic,** Jose Ramon Martinez(ATOS)
Document version:	**1.0** - 2018
Contract Start Date:	December 1st, 2014
Duration:	48 months
Project coordinator:	EXODUS S.A. (Greece)
Partners:	EXO (GR), DXT (FR), TEK (ES), ATOS (ES), TUD (DE), ISIG (IT), EADS (DE), ITINNOV(UK), ICCS (GR), CPLAN (NED), ADIT (CY), GAP (GR), SIL (UK), THALES (FR), TEL (GR), ATTD (GR), AQS (RO), GASU (NED), ACCI (ES)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607292

Document Control Page

Title	ZONeSEC Conference Report	
Editors	Name	Partner
	Aljosa Pasic	ATOS
	Jose Ramon Martinez	ATOS
Contributors	Name	Partner
Peer Reviewers	Name	Partner
Format	Text – Ms Word	
Language	en-UK	
Work-Package	WP13	
Deliverable number	D.13.3	
Due Date of Delivery	30/09/2018	
Actual Date of Delivery		
Dissemination Level	Restricted to other programme participants (including the Commission Services)	
Rights	ZONeSEC Consortium	
Audience	☒ public ☐ restricted ☐ internal	
Date	01/10/2018	
Revision	None	
Version	1.0	
Edited by	Aljosa Pasic	
Status	☐ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	17/08/2018	Template with initial index	Aljosa Pasic
0.2	24/08/2018	Generic event data introduced	Aljosa Pasic
1.0	01/10/2018	Final version	Jose Ramon Martinez, Aljosa Pasic

Table of Contents

List of Figures

Executive summary

This document describes the final ZONeSEC event that was co-located with the major conference in critical infrastructure protection. The objectives of this event were to present the final results to a wider audience and to receive feedback and consolidate one last set of inputs for the exploitation plan and cost benefit analysis. The report is describing the main event, that included ZONeSEC presentation and different sessions organized by ZONeSEC after the main conference. These session are clustering presentations of other related EU projects, ZONeSEC technological presentations and discussions about future of these technologies, and ZONeSEC non-technical issue presentations including market adoption, standardization or legal and ethical issues. Finally, event was closed with panel session that was introducing several open questions about the way forward and the trends that will have impact on uptake of ZONeSEC results. The report is also including additional information about event context. It was a direct result of activities executed in task T13.1.4 Workshops and Conferences that also covers ZONeSEC local workshops for facilitating the collection of the users' requirements and that scheduled end of the project conference in order to provide all the potential stakeholders of the ZONeSEC foreground knowledge with a comprehensive presentation of the results of the project.

1. Introduction

1.1 Context

ZONeSEC final event "Widezone Surveillance for Critical Infrastructure Protection" was organized on September 27th 2018. It was co-located with CRITIS 2018 conference, one of the most important conferences for stakeholders working in critical infrastructure protection area, at Vytauto Didžiojo universitetas (in English, Vytautas Magnus University) in Kaunas (Lithuania). Registration was separated from the main conference since it was decided to have free entrance. Critical infrastructure (CI) protection is the closely related to surveillance of widezones around critical infrastructures (e.g. gas or oil pipelines, highways, electricity networks, water supply networks). These are defined as an area or stretch of land having a characteristic, purpose, or use, or is subject to restrictions, but in many cases are not directly considered by the CI operators. However, members of the program committee of the main conference recognize that a failure or threat materialized at one critical point along the Widezone can compromise the integrity of the whole critical infrastructure. In additions, during the preparation of this conference, additional challenges have been discussed, e.g. lack of affordable solutions for the surveillance of widezones, complexity and diversity of employed systems; efficiency, robustness and resilience; compliance with EU policies and societal values, data protection and privacy; and the difficulty to coordinate surveillance activities in transboundary settings. For this reason, the call for presentations was issued at the same time approximately as the main call for papers of CRITIS conference. To cover all these different challenges in a single day, a maximum number of sessions and presentations has been set in a first template of agenda, disseminated on 24th of October 2017. The original text published on CRITIS website[1], as well as distributed to different stakeholders was:

"*Conventional surveillance systems that mainly consist of a network of visual sensors and one or more processing and storage nodes, are not directly applicable in wide area zones, where a larger redundant number of sensors and cameras is necessary. More recently, complex interconnected sensor systems are deployed in wide geographic areas, which communicate collected data to storage servers with supporting software services for aggregation, processing, decision making or alarms. ZONeSEC project (http://www.zonesec.eu/) is a four year demonstration project finishing in November 2018 and the final result is a system-of-systems (with integration of new and legacy sensors) for visualizing the critical infrastructure and the sensors deployed for widezone surveillance, detecting illicit activities and alerting operators and other features. ZONeSEC final event brings opportunity for sharing the results of four-year project, as well as hearing about similar initiatives, analyzing joint possibilities for collaboration, and discussing the future of widezone surveillance for critical infrastructure protection, in light of the forthcoming challenges and technology trends*."

The response to call for participation was positive, and agenda was already finished in April 2018, with only remaining open slots in panel session at the end of the event.

1.2 CRITIS main Conference

In 2018, it was already the 13th edition of the International Conference on Critical Information Infrastructures Security, one of the first conferences in the world with specific focus on this segment of security. During the 12th edition in Lucca, where ZONeSEC project was also participating with a presentation, decision has been made that 13th edition will be held in Kaunas, Lithuania. The conference focus is presenting innovative research, but also exploring new challenges and fostering

[1] http://www.lei.lt/critis2018/

the dialogue between all CI stakeholders, which is exactly the main objective of the final ZONeSEC event. What are the remaining gaps, after the project ends? What are the lessons learned? What is the way forward? Thanks to co-location with CRITIS 2018, final ZONeSEC event had a goal of listening to different perspectives: academia, users (CI operators), industry, defence sector or governmental organisations had discussions and multi-disciplinary approaches to relevant problems, including the widezone surveillance. There was also Projects Dissemination Session, with an opportunity to listen to presentations of ongoing European, multinational, and national projects, with a focus on sharing experiences related to project approach (e.g. cross-sector versus single sector protection focus).

Within CRITIS 2018 conference, there was a special focus on current and future energy infrastructures with speakers from electricity and/or gas Transmission System Operators (TSO), some representatives from European electricity and gas Distributed System Operators (DSO), NATO and European policy-makers.

Dr. Stefan Lüders, Head of Computer Security at CERN, Switzerland, was addressing the issue of finding common culture and views. Another keynote, Dr. Hayretdin Bahşi from Tallinn University of Technology, Estonia, did Comparison of Nordic and Continental Europe Grids from the Cyber Resilience Perspective. The comparison is conducted at five levels, transmission system operator, energy sector, critical infrastructure, national and grid levels. Other interesting presentation was about building a network of trust among European utilities to foster proactive security though info sharing, perspective from Massimo Rocca, Enel Security representative and EE-ISAC Chair, Enel, Italy. EE-ISAC is a no profit association founded by Enel and other European utilities with the aim to build a trusted community, where the members can discuss on threats and vulnerabilities that are affecting their infrastructures and cooperate in building awareness and security culture dissemination. Other interesting presentations in this session included speakers from European Commission's Directorate General for Energy and from World Energy Council, covering issues such as implications of political and policy decisions to energy security.

Role of Public - Private Partnership in Critical Energy Infrastructure Protection is yet another interesting cross-cutting discussion topic, presented by Artūras Petkus, Head of Strategic Analysis Division, NATO Energy Security Centre of Excellence. Although the focus was once again on energy sector, some conclusions are useful for widezone surveillance as well.

Finally, the overall presentation of ZONeSEC for CRITIS participants was done by Jose Ramon Martinez from Atos.

2. Description of sessions

The agenda (included in the annex of this deliverable) was dividing presentation into separated sessions, namely EU project session with external speakers, technical session and a session dedicated to market, standardization and other issues. There was also an envisaged Keynote from LITGAS (Lithuanian gas) representative, but it had to be cancelled, so after the opening with welcome from ZONeSEC event organizers, some changes in agenda have been done. Finally, at the end of the event panel session took place in a form of open dialogue with the audience.

2.1 EU Projects and Initiatives

The first presentation was from Dimitris Petrontonakis (EXODUS), who is also the coordinator of ZONeSEC project. He presented project at glance, with all basic data and objectives, before focusing

on specific results such as a System-of-Systems based on the ZONeSEC Capillaries/Clusters approach for the surveillance of Wide zones. He also stressed importance to address EU lack of affordable solutions for large ground areas surveillance such as for instance rail tracks, energy lines, pipelines, highways, etc. The combination of different surveillance or sensoring technologies is well suited to the protection of pipeline and distribution systems, the most vulnerable parts of the critical infrastructures and the most expensive to protect. Combined data sets provide enough detail for the operator to make the appropriate decisions and dispatch the correct response teams in appropriate numbers. He presented ZONeSEC technology canvas, as well as modes of operation, normal and alerted modes, before moving to on-site testing pilots, where the emphasis of the presentation was on lessons learned.

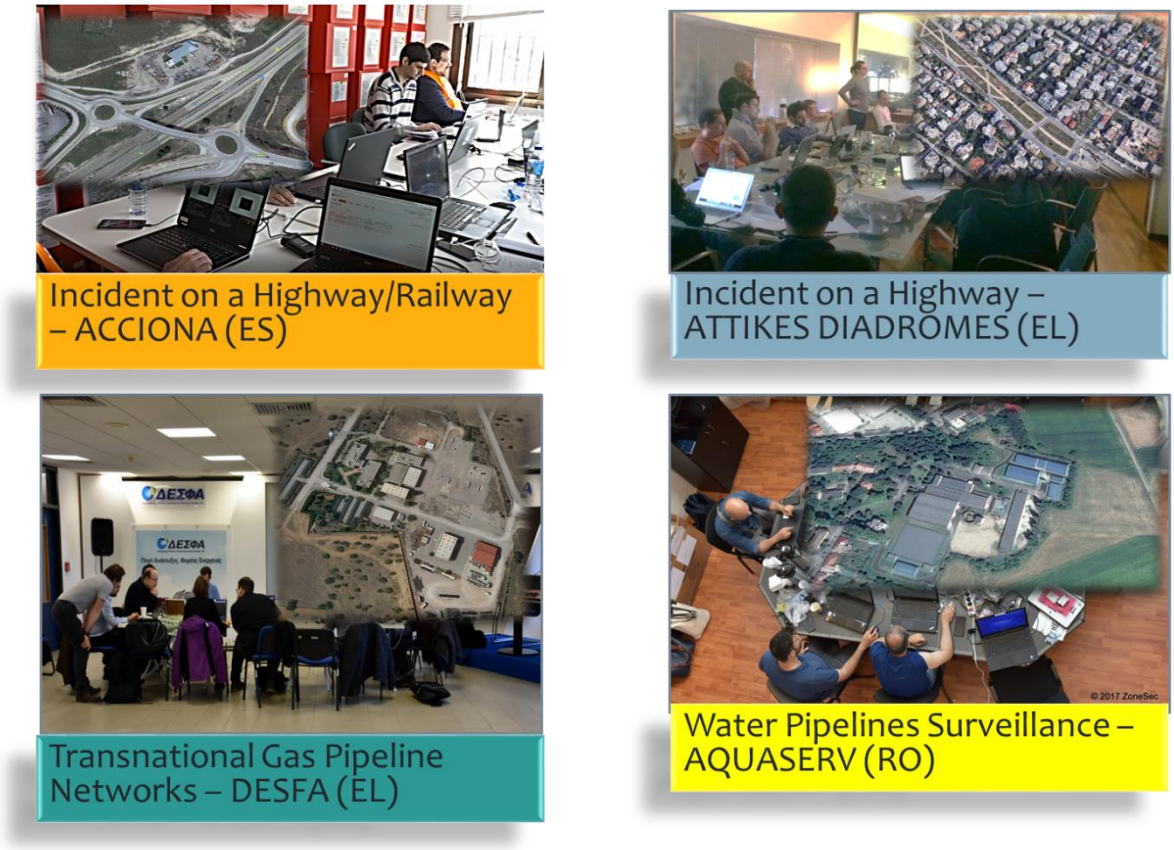


Figure 1: ZONeSEC team on the field

With illustrations from different pilots (Figure 1), Dimitris made recommendations for the future demonstration project with a similar set-up, based on the project team experiences e.g. with the testing infrastructure facilities and preparations. At the end of this presentation, all participants were invited to attend ZONeSEC final pilot in Athens on October 25 and 26th 2018. It will be hosted by Attikes Diadromes (highway operator) in Athens, and participants interested in joining should send a short description of expertise and motivation for attending the event to Lavinia Cadar at cadar@crisisplan.nl by October 3rd, which would make them eligible for free invitations available (i.e. travel and accommodation costs covered by the ZONeSEC consortium).

The second presentation was about CIPSEC (Enhancing Critical Infrastructure Protection with innovative SECurity framework). The project introduced common doubt related to CI-specific security solutions (e.g., Financial CIP-COMIFIN, SG CIP–INSPIRE, Transport CIP–RAIL4U) versus cross-CI solutions. CIPSEC takes the second approach, claiming that sector specific solutions are more expensive, since they rely on customized & technology-specific modules. The project main idea was to identify common aspects across CI's to result in a "generalized and evolvable" CIP framework that can subsequently be customized for the desired specific CI target.

CIPSEC aims towards a unified security framework that orchestrates state-of-the art heterogeneous security products to offer high levels of protection (detect, identify, mitigate threats) in IT (information technology) and OT (operational technology) departments of CIs. The project targets a data-centric "data-flow" approach abstracting across varied CI's. CIPSEC offers a comprehensive security ecosystem of additional services that can support the proposed technical solutions to work reliably and with professional quality. These services include vulnerability tests and recommendations, training courses, forensics analysis, standardization and protection against cascading effects. The project solution and services will be validated in three pilots performed in three different CI environments (transportation, health, environment).

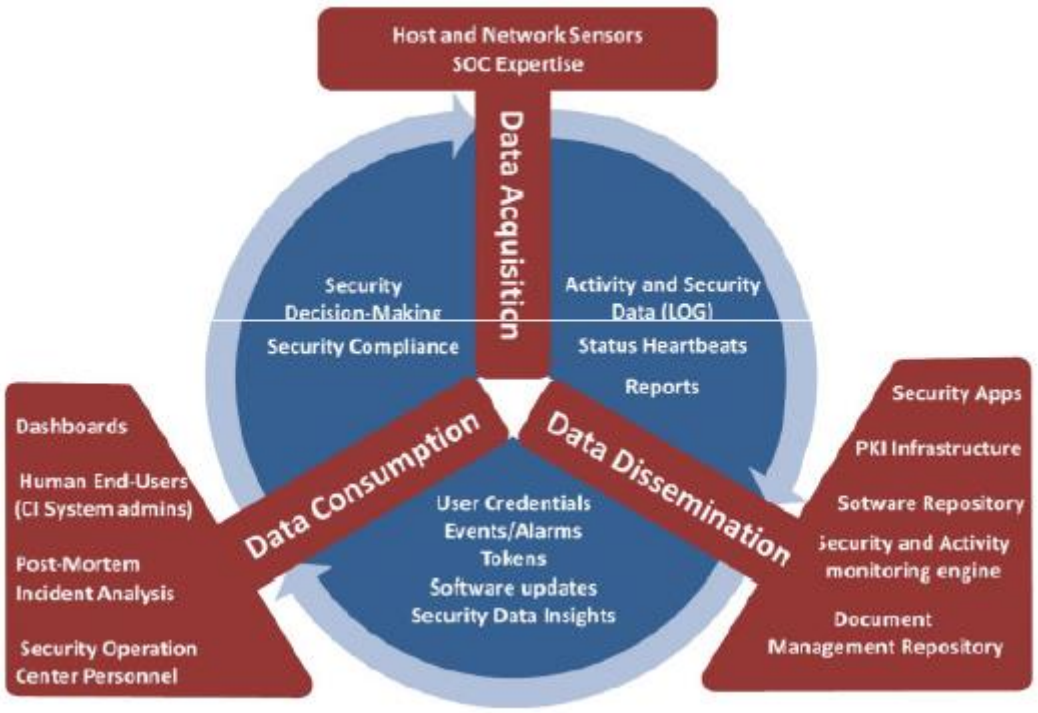


Figure 2: Data-centric approach in CIPSEC project

These three pilots will all follow data-centric approach (Figure 2) and security lifecycle that was presented together with the architecture and the main elements. Similar to ZONeSEC there is reuse of the previously existing tools and integration into what is called "unified security framework".

The third presentation was related to EU project STOP-IT (Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats). Again, the presentation started with general introduction and list of project partners. This project has a specific end user approach with frontrunners (early adopters) and followers (end users with smaller involvement in the project that would adopt solution at a later stage).

The objectives of this project are multiple:

- Raise awareness and cooperation in the water sector on cyber-physical security
- Enhance water utilities ability to identify and test alternative risk treatment options
- Improve the water industry's procedures for assessing the vulnerability of their systems to physical, cyber, as well as combined physical-cyber security threats
- Strengthen current response and recovery capacities and improve preparedness through enhanced event detection and prevention capabilities
- Protect the inhabitants in the vicinity of the CI of the water utility by providing an innovative method based on public warning systems for sharing information
- Enhance practical knowledge on effective cyber-physical water infrastructure protection through advanced, interactive and hands-on modular training and accreditation schemes for water system operators
- Contribute to the pre-establishment of certification mechanisms crossing boundaries between different CI sectors

STOP-IT project is integrating existing tools into modules and a system of systems, similar to ZONeSEC approach. There are 33 selected tools from 14 technological partners, but the main difference is that here tools are adapted for modules specific for water sector. Workpackages and interconnections have also been presented, as well as video of one tools used in the project. The questions raised after the presentation were about technology transfer, as well as privacy report for surveillance. Another question was about threats selected to treat in the project, and the process of risk assessment, which seems to be like ZONeSEC. An interesting technology that was not even considered in ZONeSEC is detection of persons in the area based on reflection of wifi signals, so there was also question about maturity of this technology and responsible partner.

The final presentation in this session was about ALADDIN - Advanced holistic Adverse Drone Detection Identification & Neutralization. The project started in august 2017 with consortium of 18 partners, including 12 technical partners and 6 Law Enforcement Agencies (LEAs).

The main objectives are related to solutions to:

- Detect, Localise, Classify, and Neutralize suspicious, and potentially multiple, light UAVs over restricted areas
- Develop a Counter-UAV system

The project builds on BOREADES system (previous French project) and existing sensor suite with multi-mode detection capability, including 2D & 3D radar, optronic, thermal and acoustic sensors. There will be innovative neutralization capability and advanced Command and Control (C2), together with cutting-edge processing including deep learning filtering and data fusion. It is important for the project to consider Operational Constraints and to address ease of use and deployment, Quality of detection, Safety, as well as to provide tools for operational support to LEAs, together with training. Besides LEA, other stakeholders targeted by the project are governmental agencies such as ministries of defence or transport, as well as critical infrastructure operators.

As a conclusion of this session, it can be said that two different approaches, namely cross-infrastructure and single sector solutions are still being considered as valid approaches to build system of systems. All projects are reusing previous projects results and building blocks, and there is some limited collaboration between projects that run in parallel. Few participants were claiming that this cross-project collaboration should be stronger since many lessons can be learned, and many tools could be reused from one project to another. The EU projects should reduce fragmentation of the pan-European market. Finally, the importance of operational environment was underlined in all presentations. While in some other areas DevOps became almost standard approach to reconcile development and operational team requirements and perspectives, in the

critical infrastructure sector this is more difficult since stakeholder ecosystem, both on demand and on supply side is more complex.

2.2 Technological Challenges

The second session was dedicated to technological challenges related to the widezone surveillance and it started with a general overview about ZONeSEC architecture and integration: challenges and lessons learned, presentation given by Jose Ramon Martinez, technical coordinator of ZONeSEC. Initial challenges were presented:

- Near real time: Time has to be reasonable short between incident and notification
- No lost of any alert: Alert data should be “reliable”. It is mandatory that alerts don’t get lost in transit
- No false alerts: Operator need real alerts, not false alerts
- All kind of networks: All kind of networks are in use in wide-zones simultaneously
- Flexibility: Plug and play: All the security capillaries can enter or leave the system at any moment without affecting the stability of the entire system
- Scalability: The resulting system or framework should be scalable to any number of security capillaries and any arbitrary extended area
- Security by design: Security has to be taken into account in all possible layers including tampering the physical devices
- Portability: The resulting framework should be portable to any localization
- Legacy sensors: Already existing sensors (aka “legacy sensors”) should be included in the framework as seamlessly as possible
- Lack of standards in sensor: Every sensor (new or old) has its own ways
- Open platform: The system has to be open allowing the possible addition of new Security capillaries and old legacy systems
- Arbitrary extensive area: Area covered can reach hundreds of km
- Arbitrary number of sensors: The number of sensor involved can be literally any, including new and old sensors

In the continuation, all components, sensors and modules were described, together with the main achievements. It was a summary of the project outcomes and their value propositions.

Modular architecture with the use of micro services was explained, together with the principles of separation of data transport from common services. In a matter of fact, core of ZONeSEC has two separated sub-components:

- Data hub: Responsible for all the data flow, namely: reception, classification and sending between: DDS-REST-RabbitMQ
- Micro Services: This sub-component will hold all the support services needed by the rest of ZONeSEC

The second challenge related to data was addressed through common data model and common protocol for all sensors/adaptors. Each sensor has its own protocol and capabilities. While some just send “raw data” there is a need for adaptors.

- Adaptors normalize data flow
- Adaptors add common functionality (discovery protocol)
- Adaptors translate to a common data model

Common data model is based on sensor standards, while discovery and incorporation protocol (self-register in metadata) is enforced by adaptors.

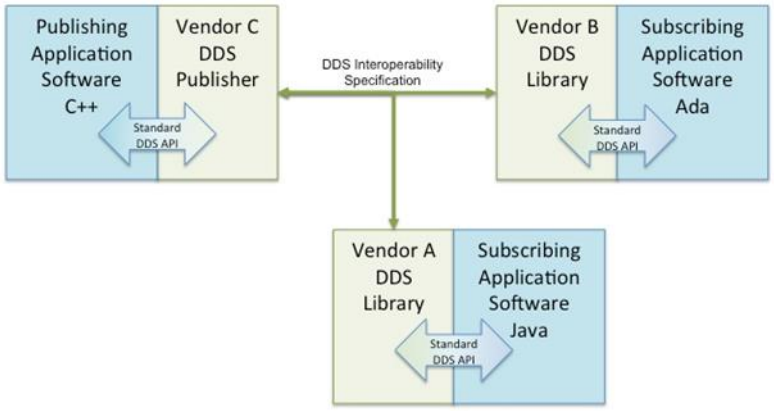


Figure 3: Use of DDS protocol for connection to any network

Metadata service provides meta information about sensors and this information “normalizes” sensors capabilities. Interfaces include different protocols like REST with COP and DDS with Core, while it is envisioned to have future interface with SDAIM via Rabbit MQ.

The third challenge was related to the use of a decoupled communications framework tailored for any kind of networks and widezones. Here, Jose Ramon presented advantages of using DDS protocol (Figure 3). DDS is a “scalable, real-time, high-performance and interoperable data exchanges using a publish–subscribe pattern”. It allows the connection of thousands of elements over heterogeneous networks in arbitrary extended areas.

The fourth challenge is about scalable automatic processing of data (including fusion of data, see Figure 4). SDAIM [Surveillance, Detection and Alerts Information Management] performs data and information fusion to aid and improve the decision-making process of the Widezone operatives. Security Clusters are solving the issue of processing of sensor data that are related by geographical criteria or any other common criteria are aggregated locally and processed locally (using same SDAIM logic). This provides scalability to the full framework. Data and information fusion is fulfilled by data and information fusion algorithms configured and executed as event stream processing workflows. The output of the fusion process are alerts for possible illicit situations and behaviors and also supporting information, aimed at the Widezone operatives, and provided over a standard messaging interface.

Security in devices and in net (including tampering and cyber) is presented as the fifth challenge. Here, after the brief presentation of all mechanisms (including e.g. TPM (trusted platform module) chipsets) more detailed information was given about cyber agents, software agents able to detect any cyber intrusion and to be trained to detect new threats. The multi-agent system provides continuous analysis of security events in the cyber-domain, aggregating data from many sources and providing the ability to consolidate and correlate monitored data to generate reports and alerts

Once again, the main lessons learned came from operational pilots (OIPs), such as:

- Need to test integration in remote and “in the field” for a long time in advance
- If the architecture works, the communication links can still create problems
- Pay attention to language barrier and cultural barrier: companies come from different countries

From these problems the most important one seems to be related to local network infrastructure (or lack of it) since it is an area where no partner is directly accountable (not clear in project Description of Work - DoW). Certain network features are critical for the project, so there was a need a voluntary acceptance of task.

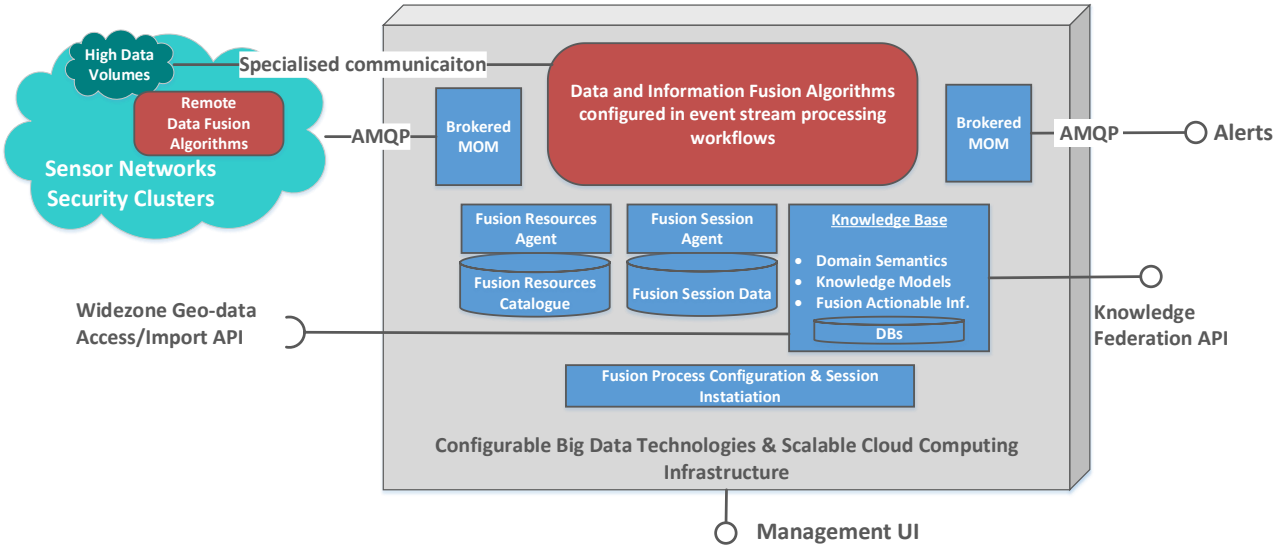


Figure 4: SDAIM module

This message, that ZONeSEC team managed to solve all problems at operational pilot site and to break all barriers was the final message end of the presentation, where technical manager underlines once more team spirit with a photo from one of the integration meetings at operational pilot site.

Network issues at partners site resulted in overhead for partners, so one issue is to how to operate zonesec in areas where network infrastructure does not exist or communication is not working as expected. One idea was to use a car or special vehicle to collect data. The post-presentation discussion focused on this issue and other possibilities were mentioned. LoRa and LoRaWAN, for example, permit inexpensive, long-range connectivity for Internet of Things (IoT) devices in rural, remote and offshore industries. LoRaWAN is network layer protocol for managing communication and ZONeSEC could consider LoRaWAN to replace WiFi to connect new sensors. It could send very short one burst per day, containing some Kbytes of data. It also has low battery requirements, but no way to resolve conflicts. There were other ideas suggested, e.g. protocols that mobile industry uses for M2M communications, such as Narrowband IoT (NB-IoT). It is a Low Power Wide Area Network (LPWAN) radio technology standard developed by 3GPP with low cost, long battery life, and high connection density. Other suggestions were related to the architecture, e.g. about use of raspberry PI to collect data, edge computing idea, real time issues etc.

Due to travel arrangements there was a change in agenda and the next presentation was “Technical Evolutions of the UAV Systems in the Surveillance of Wide Zones”, given by Michael Skitsas. After the introduction about mini-UAV systems and payloads (cameras etc), Michael focused on the main challenge on how to identify and select a Mini-UAV Platform/Sensor and a GCS (ground control station) in an intelligent way. GCS refers to the complete system used to control the UAV, including the Human-Machine Interface, computer, telemetry, video capture card and aerials for the control, video and data links to the UAV. Other open questions include.

- Can we fly about one hour?
- Who defines the flying duration?
- Automated versus manual flight?

One of the main issues is related to the UAV team, which is in ZONeSEC external to the widezone surveillance or critical infrastructure operator. It includes Mission Planner, GCS Operator – RPAS Pilot, Mini-UAV Operator – Safety Pilot and Payload Operator.

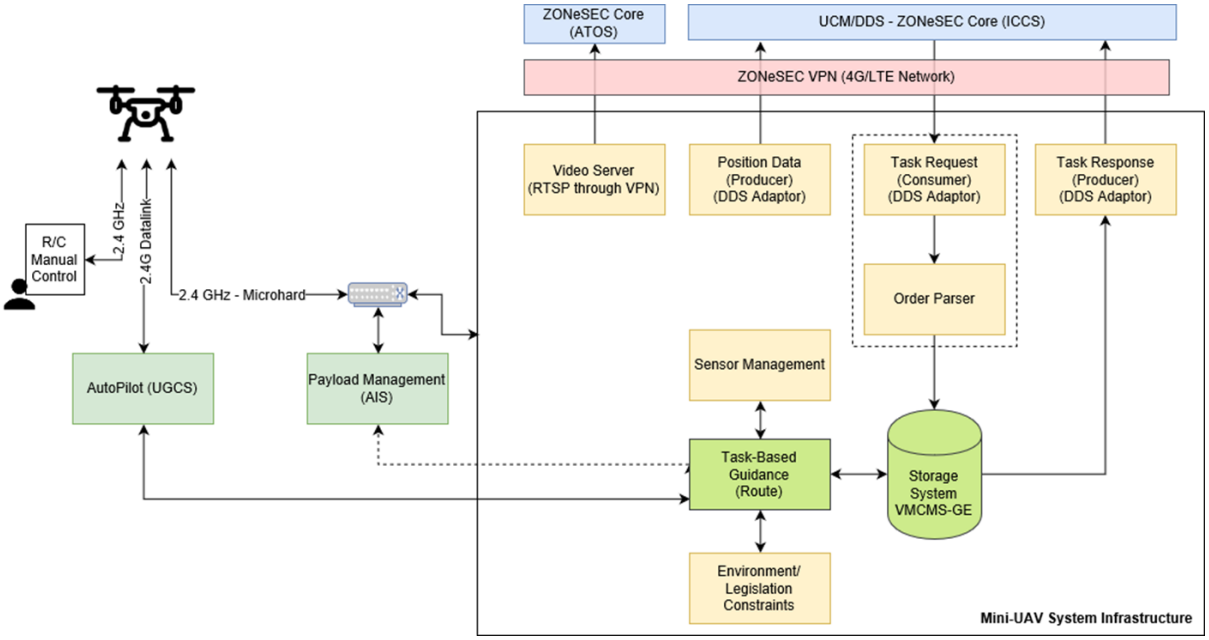


Figure 5: UAV in ZONeSEC

In Figure 5, the overall setup in ZONeSEC was presented with an architecture and the presentation focused then on Task-Based Guidance (TBG), different orders to UAV and different screenshots of the systems (Figure 6).

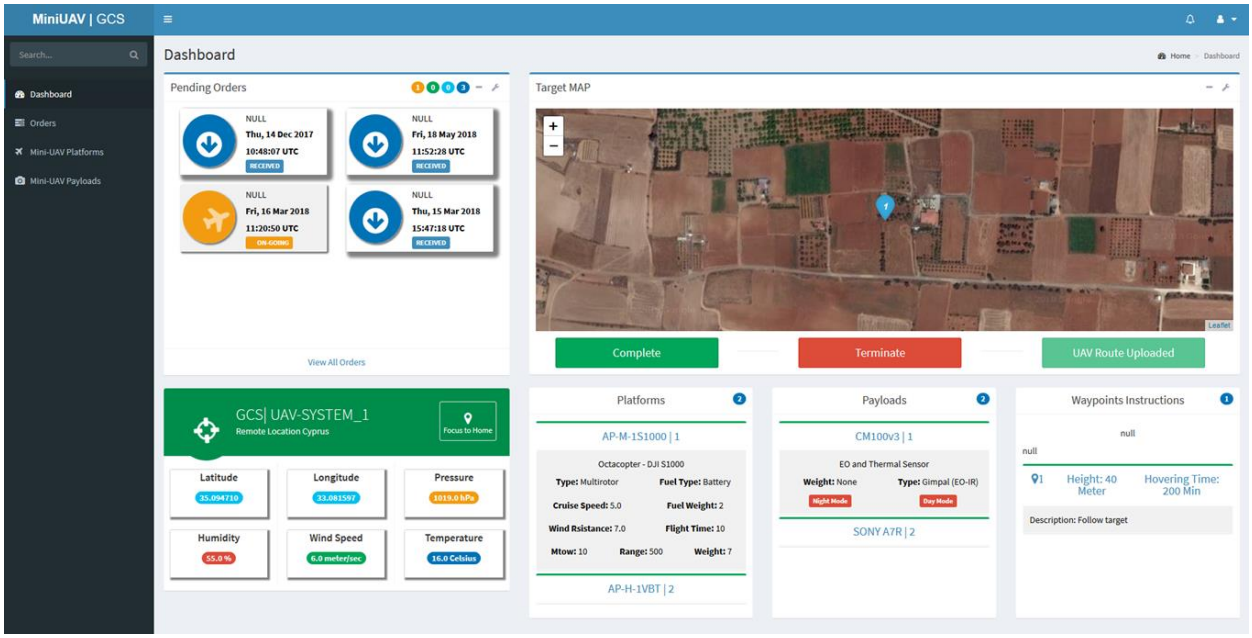


Figure 6: User interface for task-based guidance of UAV

The post-presentation questions were about latency of UAV data and status of task based guidance in control room. It was commented that deployment time is less than 5 min from receiving the order,

but there is a strong dependency on field operators. There should be minimum 2 persons, one for safety one for logistics. The future plans involve development of an app for fleet management, assessment of weather, planning, automation of takeoff and landing and other functionalities. As a response to flighting time maximum, it was also commented that fixed wing UAV can fly more than 100 km. Furthermore, there was a question about business model and the answer was that it can have two variations:

- for emergency and real time situations there is a need to train operator staff to act in the field or, as an alternative to subcontract TBG (task based guidance)
- for situations such as regular patrolling, there is possibility to have it leased or used as a service (lease staff and equipment for a limited number of hours or flights)

Next presentation was about lowering the total cost per km of surveillance with a focus on Security Capillaries/Clusters and Plug&Play&Forget Wireless Sensors. In addition to the previous challenges, presenter also mentioned cost related issues, namely

- Equipment distributed along many KMs
- Not everything can be managed/available from a central control.
- Individual information coming from every system
- Need for periodical and per-subsystem analysis, maintenance and surveillance

Novel detection technologies offer new opportunities and they are more affordable. There is real possibility to monitor the whole infrastructure, e.g.: with a single fiber cable and thanks to the deployment of “tons” of low cost wireless sensors or by using novel cost-efficient radar solutions. Connectivity and processing needs are no longer the barriers, thanks to the IoT boom. However, there is also a lot of legacy, so the real challenge is to seamlessly adopt new technologies, while keeping all the available data, and combine/fuse everything in a useful and affordable way.

ZONeSEC concept of Security Capillaries, as an abstraction of the different sensor systems within ZONeSEC platform, was explained. Concept of Security Clusters that does virtual aggregation of capillaries and has embedded intelligence towards distributed illicit activity detection, is the key for cost efficiency. It is configurable and autonomous, and the presentation showed the main features, such as easy deployment and PPF (plug, play and forget) paradigm. The main goal is to reduce the overall cost of surveillance per km:

- Not requiring high-skilled staff to install and operate the systems, especially wireless ones
- No need for highly proactive maintenance
- Dynamic and automatic operation
- Overall reduction of costs by scaling hardware, processing and complexity
- The automatic aggregation of Capillaries to be performed by Security Clusters
- The autonomous operation, dynamic configuration and self-monitoring of Security Clusters
- Security Capillaries data model is generic enough to support any PPF information that could come from a system underneath, like e.g. the TEK PPF sensors.
- Software tools to support the deployment of WSNs

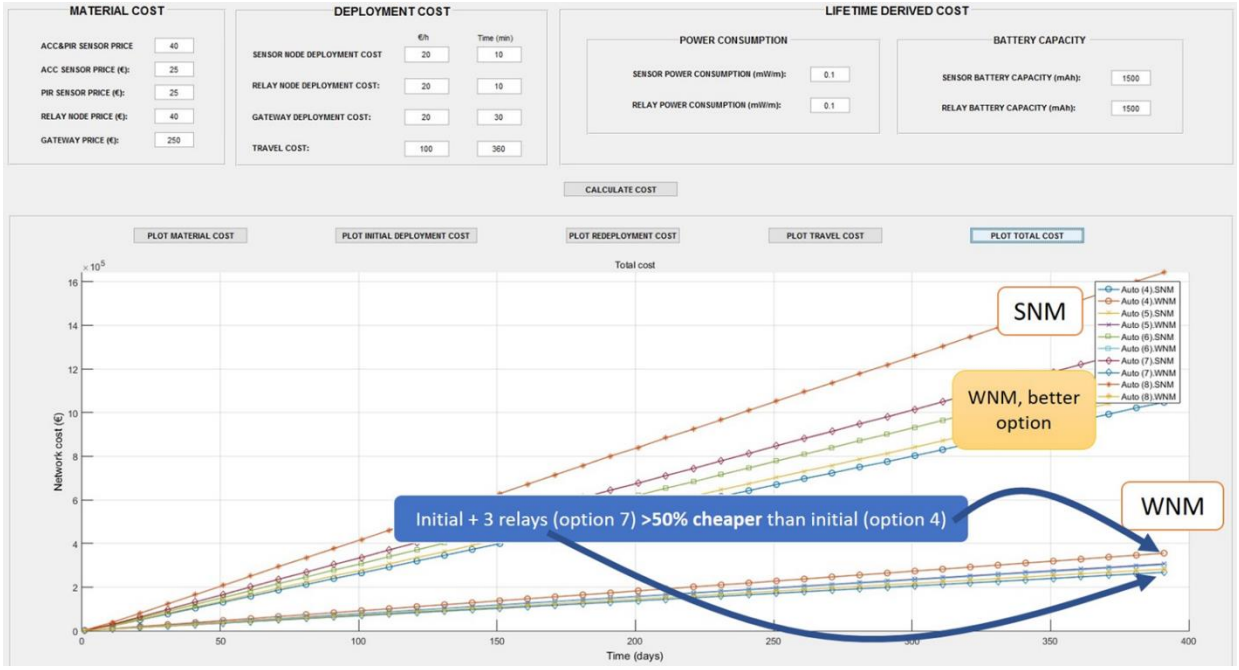


Figure 7: Cost simulation for different sensor deployment options

Tekniker also developed software tools to support the deployment of Wireless Sensors. It simulates deployment of wireless sensors on a map according to a given set of parameters. Considering the limitations of the scenario and the values set for the sensor parameters, the tool (Figure 7) suggest the minimum viable deployment in terms of coverage (by adding relay/repeater nodes). An estimation of the overall power consumption per node/sensor is given. In order to choose the most convenient option, the user can add more nodes until the consumption between the different nodes gets more balanced (ideal situation to avoid some nodes running out of battery shortly).As a conclusion it can be stated that ZONeSEC contributes to cost-efficiency through three main vectors:

- enable a seamless integration of heterogeneous subsystems, either novel or legacy.
  - Self-descriptive models based on standards
  - Abstraction layer for a uniform communication
- dynamically scale the whole widezone in terms of:
  - Processing (distributed intelligence)
  - Communication (flexible data distribution)
  - Data (low level information kept locally)
- reduce the overall cost of deployment and maintenance:
  - For the Capillaries and Clusters components themselves
  - By adopting PPF ideas when designing novel sensing solutions

After this presentation there was an interesting discussion once again. It was stated that everything (sensors, data processing etc) is getting cheaper and many things were not existing in the start of ZONeSEC or when the proposal was written. Technology changes so rapidly that some choices in ZONeSEC seem to be obsolete already. Taking into account communication infrastructure, solution that would place clusters in an edge box (edge computing paradigm was not there some 6 years ago), could be the way forward, but it would not be a difficult adaptation for ZONeSEC. Discussion about standard mode of operation (1 sensor per section of fence) also took place. Depending on the fence characteristics, the placement actually can be every 5 meters or 10 meters, but probably not more than 10. One sensor gateway could be needed for N sensors and the number N would depend on the physical characteristics of the area (not same for lineal fence, as to other shapes). There was a question about simulation that is now existing only for motion sensors and accelerometers and only for Attikas use case (square shape of fence, not linear). In Aquaserv demo there was a fusion

of motion and vibration data, a single system internal fusion, but it could be extended for indoor motion detector to also connect camera, even to add environmental sensor e.g. humidity. Teknalia used commercial sensors in the pilot but together with own software development, common connector and some adaptations to support ZONeSEC protocol. There was also question about angle of detection area which is about 70% degrees around sensor, and it needs to be taken into account when number of optimal sensors and their placements are calculated. In a matter of fact, in software developed by Teknalia there is way to detect overlapping between detection areas of two sensors. Other questions included wind considerations, which does not seem relevant for sensor placement (but it does affect detection). Tool will not be open source. In the start and idea is to have it as a software library and then one could make own interface on top. In the future open source version is also considered. The final question was about interaction with WSRT (Widezone Surveillance Reference Tool) if possible match between two tools that will also be considered.

The following presentation was about CRIMSON (Figure 8), Common Operational Picture (COP) that has been partially developed in ZONeSEC project. It is an innovative product line for operational preparedness, crisis management & site supervision, in all kinds of settings including urban areas as well as indoor or underground areas. It is result of three European research projects co-funded by the European Commission. A modular cloud-based platform is interoperating with third-party systems and tools and is supporting multiple users (in interconnected command centres or operating in the field). The objective is to simplify the exploitation of the mass of information available about the real-world and operations through:

- Data filtering and fusion
- More interactive and legible display of Common Operational Pictures
- Advanced User Experiences (UX)

Its application in ZONeSEC was focused on surveillance, namely operational surveillance of a multi site / area with geo-localized alert and real-time aggregation, fusion, and visualisation of multiple sensor information.

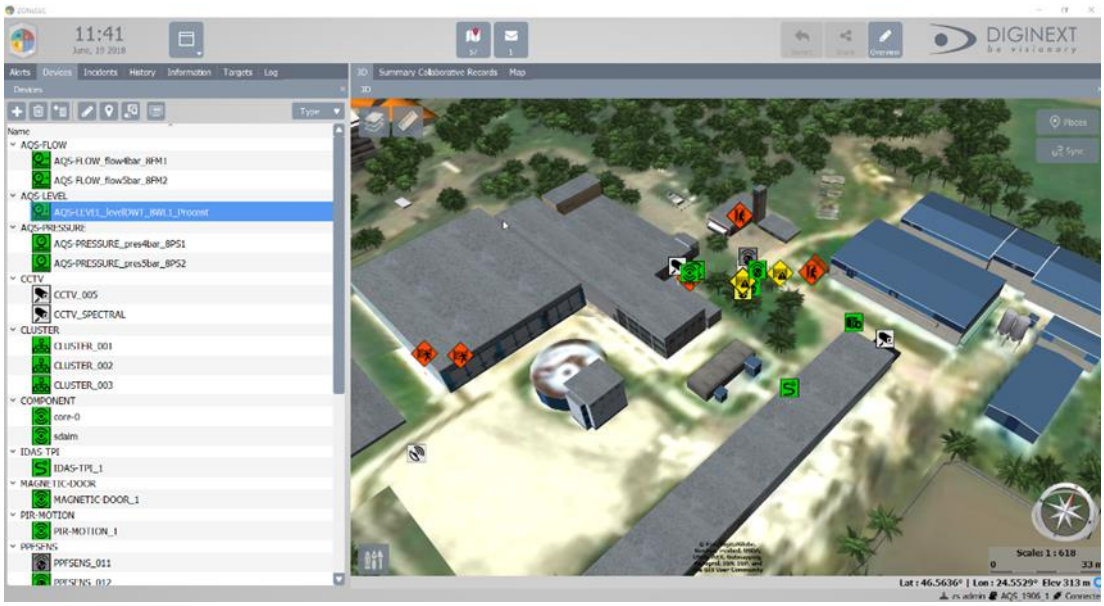


Figure 8: CRIMSON COP in ZONeSEC

In the continuation, the presenter discussed technical components such as state-of-the-art 2D/3D visualization engine, video stream integration or real-time reprojection of video streams on the map (STANAG 4609), as well as sensor data integration.

There were some questions about sensor data. For simplicity COP is hiding info about all signals coming from field. In case there is alerting from hidden sensor, system can enable visualization, but there is a need to trace alert manually. It appears on map and list of sensors, and operator gets notification including sound so that he can focus on this specific event. Another question was if there is black out and COP is not available, if system will memorize information coming from field? This is not possible since if it is system blackout information will be lost. Discussion then focused on next steps of improvement of COP. In ZONeSEC there is communication layer, but for COP it would be useful to connect directly to sensors and to be compliant with all standard protocols, to add more intelligence, e.g. for camera to open stream directly without user intervention.

Next presentation was about widezone surveillance reference toolkit (WSRT) which is one of the project outcomes of ZONeSEC. The vision of EU-WSRT is:

- to support Widezones surveillance solutions Strategy of Europe
- to support national deployment strategies and activities to promote security of citizens
- to support Widezones surveillance related decision making processes to be more efficient and faster

It will do that via an easy to access (single entry), consistent (linked to all necessary data sources and processed to one information source), up-to-date (maintained) toolkit implemented as a service and is free of charge. The first part of the presentation was about Security Management System (SeMS) assessment. SeMS questionnaire included in WSRT enables the identification of possible gaps and weaknesses in terms of organizational structures, accountabilities, policies, procedures and resources dedicated to security. There are 9 common topics in the questionnaire:

- Security Operations Principles
- Control of Conflicts
- Knowledge of Threats
- Risk Assessment
- Security Operating Procedures
- Human Factors in Error Management
- Personnel Competence and Training
- Supervision and Checking
- Incident/Accident Analysis

Each topic is linked to questions that aim at assessing the level of compliance with the respective provisions and questions are linked to possible answers. The second part of WSRT, Risk Assessment tool, aims at supporting Widezone owners, operators, managers and decision makers in identifying, assessing and evaluating risks related to their Widezone security. Examples of semi-quantitative risk assessment and consequence assessment were presented for water sector. As a conclusion it was mentioned that the integration of the various components and tools into one unified user experience (using SSO - umbraco) incl. self assessment tool, was judged as very positive by users. Deployment of WSRT to the cloud (AZURE) and definition of main features and progressing on inference engine development (future work) is also explained. Finally, to the participants free registration was offered for acquiring your Username and Password through the following link: https://goo.gl/forms/QaHigLUQ5tJ6NELu2

At the end of this session big data issues were also briefly commented. Due to a flight cancellation, presentation “Surveillance, detection and Alerts Information Management - Event processing” had to be cancelled, but it was commented that two prominent facets of Big Data, namely velocity and heterogeneity were considered in ZONeSEC. The Big Data solutions analysed were Spark Streaming and Storm but they had limitations in the context of Zonesec. An architecture combining edge-computing for data and centralised steams aggregation and processing for information was realised instead (see Figure 4).

2.3 Market and Standardisation

Kalman Kontz (Aquaserv) and Natalia Kalfa (ATTD) presented their respective use cases for adoption of widezones surveillance for critical infrastructure protection operators. They represent very different types of users and their infrastructures are also very different. While Aquaserv has more than 1300 km2 pipes plus the need to protect central resources, ATTD operates 70 km2 of highway in Greece. They also have different operating and business models (e.g. regarding external contractors.

Kalman presented challenges generic to all CIP operators, before moving to specific issues of widezone surveillance. The 3rd OnSite Integration Pilot (OIP) and 2nd Pilot Demonstration was hosted by Aquaserv in Tirgu Mures, Romania, so he illustrated presentation with a solution for this pilot (see Figure 9) and lessons learned.

Figure 9: Pilot site at Aquaser premises in Romania

ZONeSEC system was capable to perform during the first pilot iteration:

- detection of denial-of-service (DoS) (in the SCADA system) and brute-force attack
- detection of human presence along perimeter fence areas
- detection of physical intrusion and movement inside a secure perimeter
- detection of fire/ near the water pipeline
- detection of intrusion into the water treatment room
- detection of asset manipulation (water contamination)
- assignment of UAV mission at the remote site (Cyprus) and tracking of target

In 2018, the second iteration was held, and more functionalities have been tested such as:

- Detection and geolocation of trespassing inside facilities
- Remote Mission assignment to mini-UAV (tracking of suspecting car)
- Analysis of footage using deep learning techniques in real time
- Integration of legacy system integration (SCADA, PIR Motion and Door sensor)

- Field data (pictures and operators position) using mobile COP

Some security capillaries were included in the Security Cluster, such as acceleration sensors, iDAS, Spectral system, IP camera (for video analytics), Magnetic sensor (door sensor) and movement sensor (PIR sensor). Outside of the cluster, MIMO Radar was tested.

Additional demonstration cases were:

- Detection of cyber intrusion using cyber agents
- Demonstration of scalability of clusters and distributed processing; it included:
- Simulation running 20 virtual sensors simultaneously (including COP Scenario Editor and SDAIM)
- Scalability demo (including COP Scenario Editor and SDAIM)

Users in Aquaserv were satisfied with functionalities and performance of the demonstrated ZONeSEC system with regards to latency, processing and response time. Remote connection with Mini-UAV System deployed in location 1500 Km from the control room area was also demonstrated and integrated.

Motorway infrastructure use case was presented by Margarita Kostovasili, Transport Engineer in Attikes Diadromes. As mentioned before, this company operates 70 km of urban motorway, but also 39 Toll Stations, 195 Toll Gates (92 ETC capable), operates surveillance through patrolling of 100 Overpasses and 25 Underpasses, 12,6 km of tunnels and many Cut & Cover sections. They have 200 cameras for traffic monitoring and 200 for toll operation monitoring. With average of 216.893 vehicles per day it can be considered as very critical but today there are many open challenges such as:

- Alarm events verified by human operator
- No automatic fusion of events
- High dependence on human factor (experience / alertness)

Presentation highlighted list of tested functionalities, like the previous use case but also list of perceived benefits, which are not always quantitative:

- Illegal activity detection
- Identification of combined threats
- Identification of existing gaps
- Improvement of facility protection
- Further and broader provision of safety
- Crisis management processes enhancement
- Avoidance of event escalation
- Standardization of proposed systems and prototypes

Once again, invitations to the final pilot demonstration were distributed.

Adoption of surveillance and detection technologies by critical infrastructure operators was also subject of the next presentation. The methodology of ZONeSEC exploitation was presented with different phases and outcomes (Figure 10), including market analysis, results positioning, value proposition etc. Difficulty to establish pricing range and strategy, as well as complex value network were the main weakness and obstacles for the further commercialization of results. While situation in EU homeland security and defense markets is still fragmented, there is a trend of convergence and acquisitions to create “integrated solutions” combining system of systems approach with tailor made services including operation of some elements as a service.

ZONeSEC as a whole bridges the gap between surveillance, sensor, software and service (4S) offerings. Primarily target in ZONeSEC are Energy (Oil & Gas, and Electricity), Water and Transport Sector (Railway and road infrastructure). Pipelines used for transportation of oil, gas and other products have an approximately extension of 38.375km^2 through the EU. Train railway lines have an approximate length of 237.035 km while the road infrastructure has more than 4.500.000 km. The CIP market size is estimated to growth from 94 Billion EUR in 2017 to 130 billion by 2022, at an estimated CAGR of 6.8%. With all these data, widezone surveillance for CIP operators is still not an easy market to define and to measure, since it is partially subsegment of CIP market, and partially new market with dedicated surveillance equipment not integrated with CIP legacy.

Survey among users was done in 2017 with questions such as

- what are the main drivers for you to make investments in wide area surveillance technologies, equipment and tools?
- The importance of different value parameters in acquiring and maintaining a wide area surveillance system
- The most important characteristics of a new solution for wide area surveillance?
- Most important aspects of data acquired and events detected

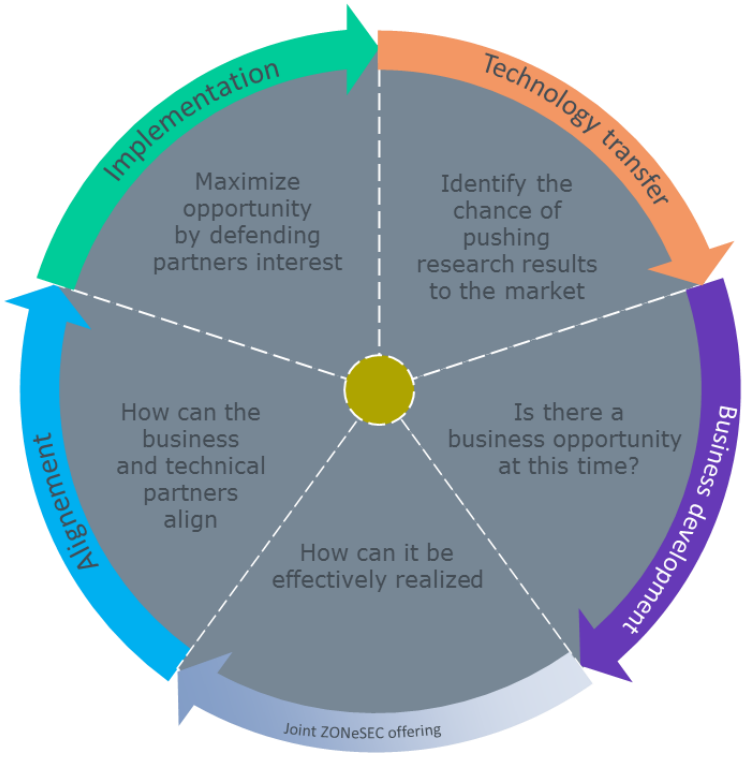


Figure 10: Strategy for technology implementation plan

Study revealed not only challenges and user preferences, but also differences in looking at ZONeSEC as a solution integrated with the existing legacy system, and ZONeSEC as a new system replacing or added to, an existing system. While cost saving, interoperability and security were the main concerns of a new system, an integrated system was expected to score high on user friendliness or compliance to an existing policy. Distinct value propositions were presented, namely flexibility, scalability, cost-efficiency and support team. Cost benefit analysis was also presented with many assumptions, and the final outcome that compares approach taken from demand side (and

expectation to have price range around 6500 €/km^2) and from supply side (that expects price to be higher, if we take into account all modules and sensors of ZONeSEC).

Strategy for project results exploitation, named technology implementation plan, was also presented with the approach having value network around ad-hoc business opportunity. The idea for post project engagement and collaboration between project partners, based on 3 step approach with light weight agreement framework was presented. Validation of the business offering with partners and proposed approach with proof of concept (PoC), might be enhanced or complemented with individual selling propositions of ZONeSEc project partners.

Questions from audience came related to the positioning difference in integration with existing CI tools and in placing ZONeSEC as a new solution for Widezone surveillance. Emphasis seems to change from efficiency to interoperability. Some discussion about pricing took place, for example what is the criteria to tag some sensor or solution as “low cost” (e.g. reduction of factor of 5 compared to the existing solutions).

The next presentation was about CEN WS process – Defining a pre-normative standard on the interoperability of security systems for the surveillance of widezones. CEN workshop agreement (CWA) is an open procedure, used to disseminate innovative technology solutions - a quite popular mechanism among R&D projects. It is designed to meet a market need, where an innovative technology has not reached a sufficient degree of maturity and it reflects the consensus of identified individuals & organizations responsible for its content. The CWA does not represent the level of consensus and transparency required for a European Standard (EN) and is not designed to support legislative requirements. The ZONeSEC CWA “scoping” meeting took place on October 18, 2017, parallel to the user validation meeting. British Standards Institute (BSI) attended the meeting, as the nominated secretariat, to assist with the CWA details and procedures. Final CWA project team review (final version/ approval of deliverable) will take place in October 2018 and publication is expected in January 2019. In the continuation few concepts from draft CWA were presented.

Questions from the audience came about nature of comments raised during the CWA drafting meetings. The answer is that some were about terminology, while others were about technological issues and in total they have received 155 comments. Examples include definitions of what is capillary, clusters, interoperability described from tech point of view etc. It is not mentioning specific protocols e.g. OGC, and the focus is on what can be indicated is abstracted way. There was also a question about outcome or impact, in ZONeSEC exploitation and on security in general. Some standards have certification, that proves conformance with it, but CWA is 2-3 steps ahead of that stage, it is only guideline. There was a question whether someone who wants to start similar effort, need mandatory to prove there is no conflict with CWA of ZONeSEC. The answer is no, but ZONeSEC did analysis to prove what is overlap with existing standards, and there was no ongoing CWA that treats similar issues. In principle there should be someone in CEN checking overlap regularly.

Final presentation in this session was about Ethics in Security Research. Ethics is the systematic reflection on what is moral: where “morality” is defined as the totality of opinions, decisions and actions with which people express what they consider is good or right. Prof Mitrou explained links between law and ethics, for example that law is (legally) binding while ethics do not a have a binding nature. However, law should reflect the values of a particular society representing (and enforcing) minimum ethical behaviours of human beings. Security measures and surveillance are sometimes accompanied by nuisance, incident, or annoying and irritating situations or cases of interference into dignity and fundamental rights and freedoms. An example could be UAV/ video surveillance/ sensors that record human presence and behaviour, such as in the case of ZONeSEC.

Responsible Research and Innovation and Security Research (RRI) proposes dialectical process where every security research project/security tool should identify ethical, societal and legal issues to be faced, while research and innovation co-define the aims, the scope and the outcome of security

research and security policy. Presenter then shifted focus towards privacy and data protection with a special emphasis on data protection risk assessment (DPIA). DPIA is only required when the processing is “likely to result in a high risk to the rights and freedoms of natural persons”. In a case of ZONeSEC a systematic monitoring of a publicly accessible area on a large scale” could be maybe applicable to MIMO Radar surveillance while evaluation or scoring, including profiling and predicting might have link to use of acceleration sensors.

Given that ZONeSEC is a project in the transition phase between old national data protection legislaions and new general data protection regulation (GDPR), the new framework has to be taken into account as well. A DPIA is necessary/ advisable to be performed in those technologies (video surveillance, UAVs, mobile COP) that their outcomes may identify, directly or indirectly individuals (data subjects), their features and behaviour with implications for their rights and freedoms. The use of UAVs is especially important since it expands the scope of surveillance -they may become more intrusive as they penetrate and monitor places that are normally inaccessible and they can register indiscriminately information concerning a large number of people. From the ethical perspective it represents risk of potential “dehumanization of the monitored” as a result of the distance and the diminishing of sense of moral responsibility.

2.4 Panel session

Panel session was focused on policy and economic issues behind the widezone surveillance. Exposure to risk due to the need to achieve productive efficiency, and priority given to CI protection itself (as opposed to widezone around CI), are important challenges. Monitoring and/or data collection technology may negatively affect individual privacy, but this is also studied in public area surveillance by CCTV, for example in urban security domain. Issues such as permanent/long-term data storage are mentioned during the event, but not treated in detail. The efficiency and security trade-off in widezone surveillance is more challenging than in CI protection also because there are more stakeholders, including external services e.g. patrolling. When it comes to use cases and customization, it all depends on how the area around infrastructure is owned and operated and it is very different in different members states. The divergence between private payoffs from reduction of operational cost and the public payoff might trigger policy actions.

From an economic perspective, widezone surveillance cost benefit analysis suffers from incomplete information, i.e. difficulty to take informed decisions on how to set priority. In this sense, ZONeSEC is an important step forward in solving the difficulty of locating the potential sources of threat. Advantages of total security approach are discussed, as well as “rational ignorance” (all else being equal, the costlier info gathering, the lower value of new data). Since ZONeSEC uses lots of Commercial Off The Shelf software (COTS) the risks related to the integration of COTS are also discussed.

Finally, other issues, such as societal acceptance and future technologies (e. g. artificial intelligence) have also been discussed.

3. Conclusions

The final ZONeSEC event organized with CRITIS conference was a major opportunity to present the final project outcomes, to explore collaboration with the other projects, as well as to collect additional feedback which might be incorporated in the last two months of work (e.g. final pilot or exploitation work package deliverable). It was also very useful reflection from project partners about lessons learned and the possible future work including joint exploitation. The long duration of the project and the fast evolution of technology is changing the initial assumptions, but the project team was able to adapt and to make most of the conceptual solution thanks to the modular architecture. Open issues remain, among others related to the social acceptance, ethical and legal issues in relation to the use of drones for widezone surveillance. The final pilot in Athens, scheduled for October 26th, and the set of final deliverables, will try to address some of these open issues.

Annex 1: Event Agenda

ZONeSEC event

Widezone Surveillance for Critical Infrastructure Protection

September 27th 2018

co-located with CRITIS 2018 conference at Vytauto Didžiojo universitetas (in English, Vytautas Magnus University), Kaunas (Lithuania)

Agenda

9.00 – 9.10 Opening and logistics

9.10-9.40 Invited keynote: Kristina Rimkunaite, LITGAS

9.40-11.00 Session 1: EU projects and initiatives

9.40-10.00 Dimitris Petrontonakis (EXODUS) – ZONeSEC project

10.00-10.20 Neeraj Suri (Technical University Darmstadt) – CIPSEC project

10.20-10.30 Aljosa Pasic (Atos) - STOP-IT project

10.30-10.40 Guillaume Inglese (DXT) – ALADDIN project

10.40- 11.00 Coffee break

11.00 – 13.00 Session 2: Technology challenges

11.00- 11.20 Jose Ramon Martinez (Atos): ZONeSEC architecture and integration: challenges and lessons learned

11.20-11.40 Joseba Izaguirre (TEKNIKER): Lowering the total cost per km of surveillance: Security Capillaries/Clusters and Plug&Play&Forget Wireless Sensors

11.40-12.00 Nicolas Museaux (Thales) – Surveillance, detection and Alerts Information Management - Event processing

12.00-12.20 Guillaume Inglese (Diginext): CRIMSON COP - operational supervision system applied to ZONeSEC

12.20-12.40 Nikolaos Koutras / Michalis Skitsas (ADITESS): Technical evolutions of the UAV systems in the Surveillance of wide zones.

12.40-13.00 Evita Agrafioti (GAP) and Dimitris Petrontonakis (Exodus) - European Widezones Surveillance Reference Toolkit

13.00 – 14.00 Lunch

14.00 – 15.20 Session3: Market and standardization

14.00-14.20 Kalman Kontz (Aquaserv) and Natalia Kalfa (ATTD) – Use cases for adoption of widezones surveillance for critical infrastructure protection

14.20-14.40 Aljosa Pasic (Atos): Adoption of surveillance and detection technologies by critical infrastructure operators

14.40-15.00 Dimitris Drakoulis (Telesto) : The CEN WS process – Defining a pre-normative standard on the interoperability of security systems for the surveillance of widezones

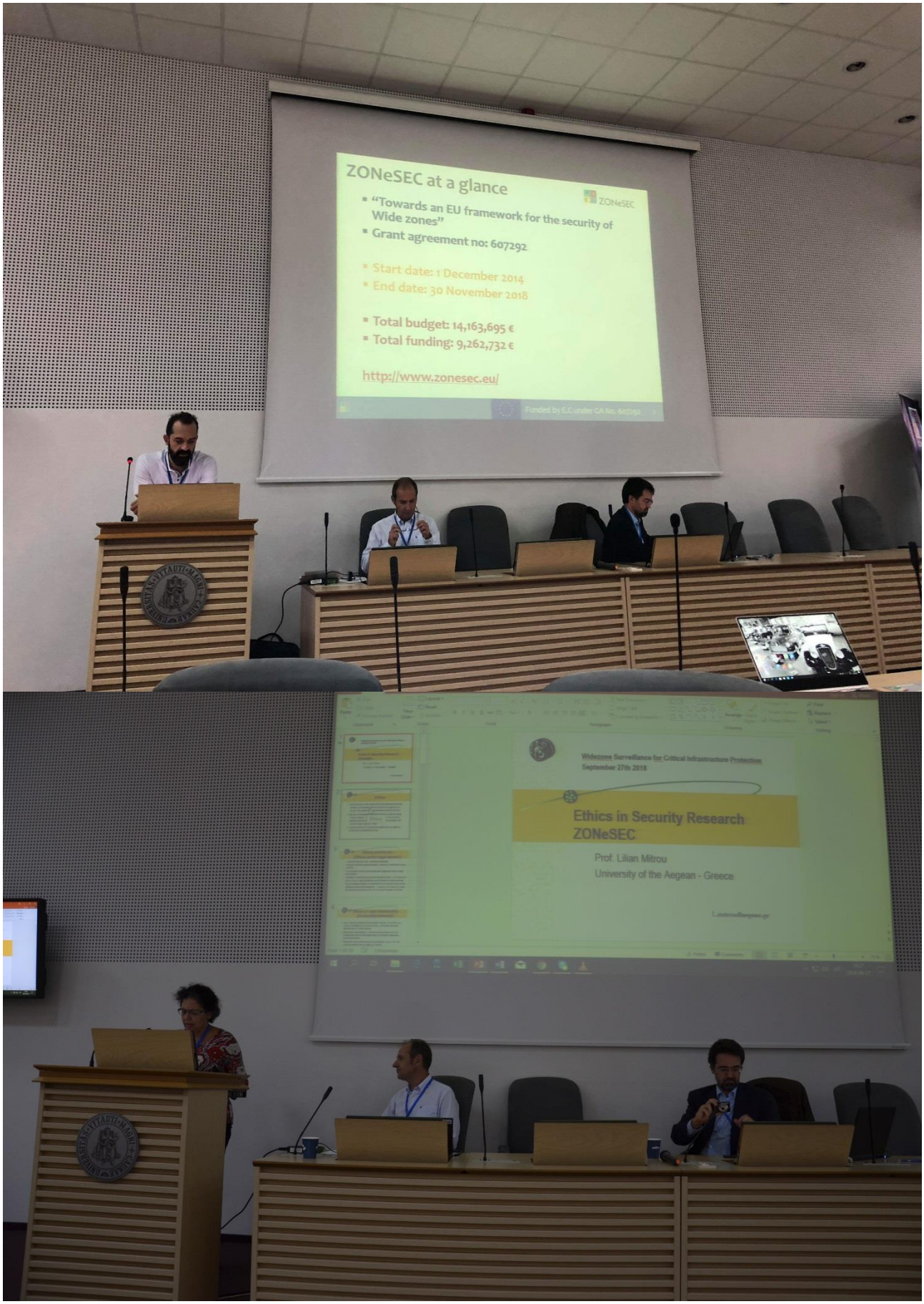
15.00-15.20 Prof. Lilian Mitrou (Professor of Privacy and Information Law , University of the Aegean), Ethics in security research : from the ZONeSEC case

15.20 – 15.50 Coffee break

15.50 – 16.50 Panel: European perspective on surveillance of areas around critical infrastructures: Simon Dathan (Silixa), Dimitris Petronakis (EXODUS), Neeraj Suri (University of Darmstad)

16.50 – 17.00 Closing

Annex 2: Event Photos


ZONeSEC at a glance
ZONeSEC
"Towards an EU framework for the security of Wide zones"
Grant agreement no: 607292
Start date: 1 December 2014
End date: 30 November 2018
Total budget: 14,163,695 €
Total funding: 9,262,732 €
http://www.zonesec.eu/
Widezone Surveillance for Critical Infrastructure Protection
September 27th 2018
Ethics in Security Research
ZONeSEC
Prof. Lilian Mitrou
University of the Aegean - Greece


ZONeSEC
Use cases for adoption of widezone surveillance for critical infrastructure protection – Motorway infrastructure
ATTIKES DIADROMES SA (ATTD)
End-User
Margarita Kostovasili, Transport Engineer, Attikes Diadromes SA
mkostova@attikesdiadromes.gr, aodos.gr


How?
Sensor Integration
Water pressure & flow
Vehicle detection systems
Intrusion detection
Weather station


ZONeSEC
Lowering the total cost per km of surveillance:
Capillaries, Clusters and
Plug,Play&Forget Wireless Sensors
Joseba Izaguirre
IK4 TEKNIKER
Research Alliance
ZONeSEC Final Event, KAUNAS – 27th September 2018


ALADDIN
CERTH
Fraunhofer
PIAP
VUB
SIRC
acciona