PROTECTING WATER INFRASTRUCTURES: ZONeSEC RESEARCH PROJECT – PILOT DEMONSTRATION FOR WATER COMPANIES

Kálmán KONCZ[1], László KAJCSA[1], Guillaume INGLESE[2], Evita AGRAFIOTI[3], George A. PAPADAKIS[3], Anastasia CHALKIDOU[3], Marina ANDEVA[4] , José-Ramón MARTINEZ-SALIO[5] and Dimitris PETRANTONAKIS[6]

[1]Kálmán KONCZ - Aquaserv S.A. Company, 1 Kos Karoly, Tîrgu Mureș, Romania, E-mail: kkoncz@aquaserv.ro
[1]László KAJCSA - Aquaserv S.A. Company, 1 Kos Karoly, Tîrgu Mureș, Romania, E-mail: lkajcsa@aquaserv.ro
[2]Guillaume INGLESE - Diginext, 370, rue René Descartes, 13857 Aix-en-Provence Cedex 3, France, E-mail: guillaume.inglese@diginext.fr
[3]Evita AGRAFIOTI - Gap Analysis, 21 Karaiskaki, 73135 Chania, Crete, Greece, E-mail: agrafioti@gapanalysis.gr
[3]George A. PAPADAKIS - Gap Analysis, 21 Karaiskaki, 73135 Chania, Crete, Greece, E-mail: chalkidou@gapanalysis.gr
[3]Anastasia CHALKIDOU - Gap Analysis, 21 Karaiskaki, 73135 Chania, Crete, Greece, E-mail: gpap@dpem.tuc.gr
[4]Marina ANDEVA - Istituto di Sociologia Internazionale di Gorizia (ISIG), via Mazzini13, Gorizia, Italy, E-mail: andeva@isig.it
[5]José-Ramón MARTINEZ-SALIO - ATOS IT Solutions, 25 Albarracín, Madrid, Spain, E-mail: jose.martinezs@atos.net
[6]Dimitris PETRANTONAKIS - EXODUS, 73-75 Mesogeion Av & Estias Str 1, 115 26, Athens, Greece, E-mail: dpetr@exodussa.com

Abstract
The challenges presented by the protection of critical infrastructures (CIs), including water networks represent a pressing issue for the European Union. Physical and cyber threats have to be counteracted by using early detection and situation awareness technologies. Adding to the problem, many European CIs are spread over wide areas. Furthermore, existing security measures has to be integrated with any new sensors. Critically, the ethical and societal aspects have to be addressed from the beginning.
Included on the 7th Framework Program (FP7) projects, ZONeSEC proposes a complete and multidisciplinary solution based on the combination of already existing and novel sensors, taking into account the ethical and societal aspects and setting a framework for security recommendations. The final objective of the project is to create a complete solution framework where novel sensors can be seamless integrated with existing sensor platforms providing data fusion, situation awareness and a common operational picture.
The new sensors involved in ZONeSEC have the requisite of being inexpensive solutions that present the possibility of plug&play and seamless integration. Some of the challenges addressed by the project are related with the interoperability of sensors, the use of heterogeneous networks over arbitrary wide areas, the combination of legacy and new solutions, near real-time requisites, the fusion of data, the use of simulation and the presentation of a common operational picture for the final user.
Ethical and privacy aspects have also being addressed from the early stages of the project. It is very easy to trespass the lines between security and privacy invasion, especially considering the wide area and the use of aerial unmanned solutions (UAVs). The security solutions proposed has to be ethically acceptable to be considered suitable for real installation.
ZONeSEC is the perfect use case to experiment, develop, integrate and test the solutions for these challenges. ZONeSEC has a clear practical vision and it is strongly user oriented; during its lifecycle it includes four Online Integration Pilots and three final demonstrations involving final users of different European countries.

Keywords
Water network; sensors; simulation; COP; fusion of data; wide area communication; plug&play solutions; critical infrastructures protection; wide area protection; integration of legacy sensors; risk assessment.

1. INTRODUCTION: CHALLENGES IN GENERAL

Critical infrastructures protection (CIP) has been identified as a critical issue for the European Commission. Thus in 2008, the Directive on European Critical Infrastructures [1] set the procedure for identifying and designating Critical Infrastructures in Europe and stablished an approach for improving their protection. Also worth mentioning, is the European Programme for Critical Infrastructure Protection (EPCIP) (published in 2006 [2] and modified in 2013 [3]) that set the framework for activities aimed at improving the protection of critical infrastructures (CI) using an all-hazards cross-sectoral approach (thus not limited to terrorism hazard for example).

In particular, the protection of CI extended over wide areas had been put in focus by the European commission with the call SEC-2013-1.6-3 - Surveillance of wide zones: from detection to alert – Integration Project [4]. The objective of protection of CI addressed in this call is:

"Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible."[5]

There is clearly a need to provide proper security for critical infrastructure against illicit actions and against incidents that may escalade to crises. ZONeSEC consortium was created as an answer to this challenge. As stated in its abstract (ZONeSEC Description of Work):

The advancement of 24/7 surveillance systems for the security of WideZones with multiple assets at localized scales is of extreme strategic relevance to European economies, industries, authorities and Citizens. Nevertheless, the cost for large deployments and maintenance of ground sensing networks for local surveillance across these WideZones is extremely high. Hence, large areas of high economic importance, particularly those situated at Member States cross-borders, may be exposed to undetected local illicit activities. These could lead to large systemic failures of the processes operating in wider zones, while economic stability, safety and security in Europe can be potentially compromised. Hence, the integration of affordable ground and airborne sensor observation technologies for the critical surveillance of large spatial areas of high economic values in Europe needs to be imminently prioritized. Secure and interoperable observation data and information management services using open standards shall be deployed in ZONeSEC with the aim of cost-effectively reusing them in the surveillance of many other European WideZones. These services are part of an advanced Knowledge Base (KB) and primarily focused on large scale surveillance with high performance detection of localized abnormal activities and alerts. Semantically-enriched domain knowledge representations shall be stored in the KB for supporting high level data fusion and reasoning with reduced uncertainties and false alerts. Surveillance professionals will securely subscribe to the scalable KB services of the ZONeSEC system of systems with customisable visualization features. Several pilots specializing in the detection of illegal unauthorized entrances to or trespassing premises; or actions to damage to or deployment of harmful devices on installations shall be fully demonstrated. These concern (sic) Water, Oil and Transnational Gas Pipelines; Highways and Rail tracks conveyed in six European countries.

2. CHALLENGES IN THE PROTECTION OF CI EXTENDED OVER WIDE AREAS

Critical infrastructures (CI) extended over wide areas (of arbitrary extension) present some particular challenges that are typically not present in CI localized in "located" areas. These include:

- necessity of covering as much infrastructure as possible or in some cases, the most critical nodes;

- physical protection of the sensors that are installed remotely;
- necessity of sensor solutions that can go unattended most of the time with low maintenance rates and low energy demands;
- low false positives rates;
- clear information about the alarm generated;
- dynamic approach in the installation of new sensors under demand;
- potentially huge number of heterogeneous sensors: this creates a dual problem, scalability and the existence of a unique point of control;
- security and cyber security;
- problems of multi-territorially, especially the ones related with the laws harmonization;
- challenge of addressing privacy laws when considering more than one territory;
- difficulty on deciding the number and appropriateness of the different security measures.

The necessity of covering as much infrastructure as possible: There are many different wide areas infrastructures (highways, gas pipes, electricity grids, drinking water facilities, etc). In some cases, there it is important to try to cover the entire infrastructure (e.g. in water pipelines) while in others we can identify some critical "nodes" that need to be protected. We will study two examples covering both cases to address the particular challenges.

1. Water facilities; mandatory protection in the entire infrastructure: as an example of "mandatory" protection of the complete infrastructure in all its longitude, we can consider a drinking water distribution network. Most of the time, the protection of such infrastructure is "passive" by keeping it underground. However, there is a clear necessity of protecting all the infrastructure against physical attacks, sabotages and damages (e.g. bursts, leakages, illicit connections). Some particular challenges are:

a. The sensor solutions have to be inexpensive since they need to have many instances;

b. The maintenance rate has to be low;

c. The status of all the sensors has to be clearly stated to have a complete "security status awareness";

d. The particular signal of each sensor needs to be aggregated as much as possible to avoid overflowing of information towards the operator;

e. The rate or false positives has to be very low: e.g. "cars" passing over the underground pipeline has to be discarded as an alarm before reaching the operator;

f. The alarms need to be as specific as possible, telling the difference between a loss of pressure due to a leakage and due to a burst;

g. Data sent will use any available kind of transition mean.

2. Maritime surveillance costal radar; node protection: costal radars extend over hundreds of kilometers (e.g. in Spain the SIVE[1] - Sistema Integrado de Vigilancia Exterior - covers more than 300 km with many stations). In this case, the critical elements to be protected are the fixed radar towers scattered along the coast. Particular challenges to address are:

a. The prevention of physical tampering; sabotage, theft, electronic jamming is very important;

b. The sensors can be incremented dynamically using mobile units, this asks for a plug&play approach with a seamless integration of the new elements.

The physical protection of the sensors that are installed remotely: Remote sensors can be tampered in many possible ways, between others:

[1]http://www.guardiacivil.es/es/prensa/especiales/sive

- Sabotage (e.g. in CCTV);
- Vandalism;
- Theft for any reason (economical);
- Theft for reading memory cards and other stored information;
- Duplication of sensors to send false information;
- Use of sensors entry point to hack the system.

The mandatory necessity of sensor solutions that can go unattended most of the time with low maintenance rates and low energy demands: wide areas concept implies arbitrary long areas with an arbitrary number of sensors. This in turn calls for low maintenance and low energy consumption (in some cases the remote localizations have to use solar power, for example when protecting a water reservoir).

Low false positives rates: wide areas imply many sensors along an extensive area. In this scenario, the number of false alarms should be near zero since each alarm implies checking in potentially remote areas (sending people or through UAV).

Clear information about the alarm generated: for the same reason, each alarm has to include as much information as possible avoiding the use of generic alarm messages.

Dynamic approach in the installation of new sensors under demand: One of the more typical strategies to protect wide areas is the existence of sensors that can be deployed on vehicles to support, substitute or replace existing sensors. This approach makes necessary an architecture of the system that is able to integrate new sensors dynamically and in near real time.

Potentially huge number of heterogeneous sensors: The extensive number of sensors creates the necessity of a scalable system, able to cope with all of them. Also, the extension of the areas makes impossible, in many cases, to guarantee the same level of communications for all sensors. Resulting system has to support data coming from many different sources with different bandwidth, quality, strength, etc. Finally, the point of control is usually unique, so the signal of many sensors need to be concentrated or aggregated using clusters of them or/and fussing the data coming from them.

The security and cyber security: A sensor net means an internal net that has to be secure by design. In this net the external access has to be minimized (ideally to zero). If any external access is available, cyber security has to be stablished.

The problems of multi-territorially, especially the ones related with the laws harmonization: Even in the EU environment, country-wide laws are different for example in UAVs and other relevant issues.

The challenge of addressing privacy laws in more than one territory: The privacy laws and also the ethic-related social sensibilities change from one territory to the next. For example in some countries, the use of CCTV in public spaces is widespread [6] with a relatively low societal concern; in UK for example the number there are 4,9 million (British Security Industry Authority 2013) [7] while in Greece the number and public concern is bigger [8], [9].

The difficulty on deciding the number and appropriateness of the different security measures: In a critical infrastructure extended over a wide area, there are security measures that are in place. Deciding (in terms of risk avoidance, costs and other relevant factors) which security measures to add is not an easy task. Infrastructures operators need simple tools to create a risk assessment profile that can help them in deciding what measures to implement.

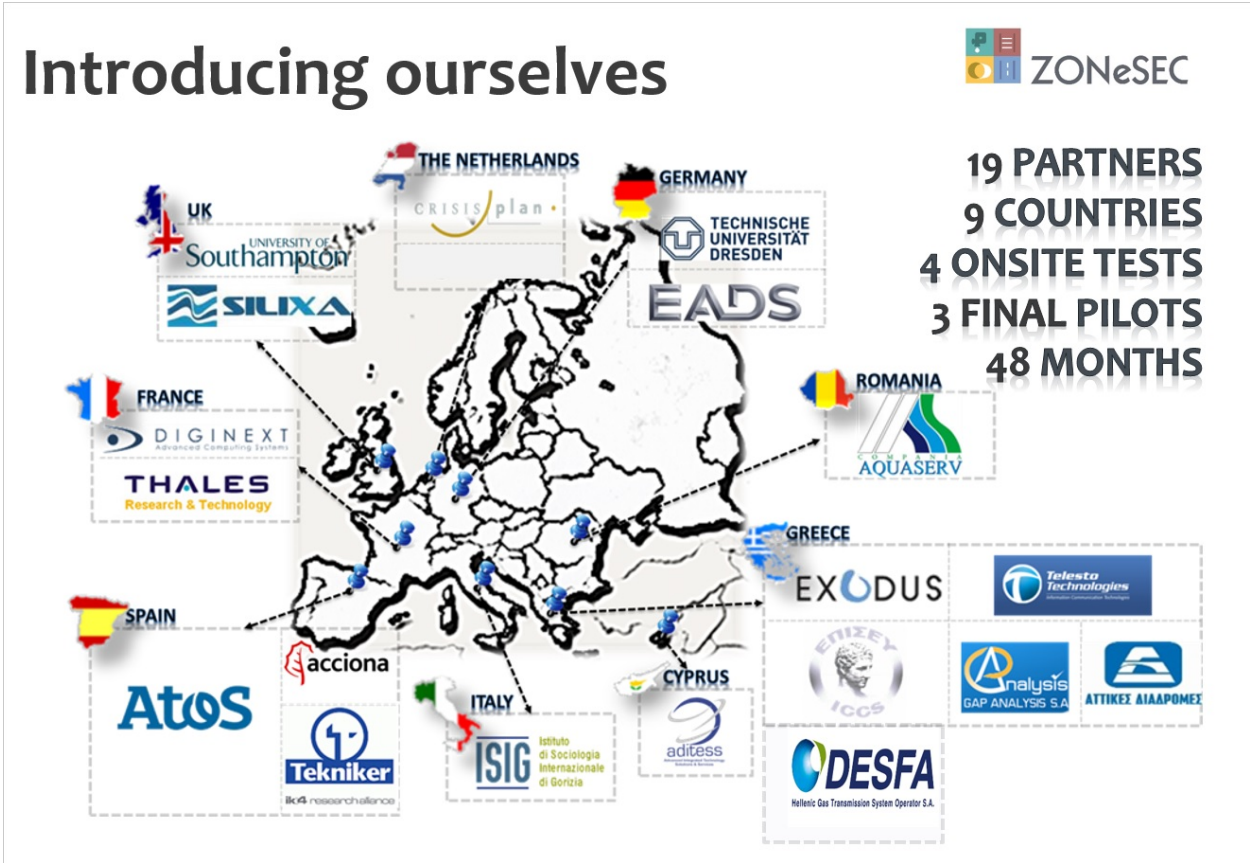

Figure 1. ZONeSEC partners

3. HOW ZONeSEC ADDRESSES COMPLETE SOLUTION

The aim of ZONeSEC from its conception is to answer to all these challenges using a multidisciplinary approach going beyond the pure technological solution [10]. Thus, the project addresses the challenges from three directions:

- Decision support approach;
- Technical approach for enhanced situation awareness;
- Ethical and privacy approach.

Moreover, as part of standardisation and regulatory activities, ZONeSEC with the secretariat held by British National Standards Body (BSI), currently working on the development of CEN Workshop Agreement (CWA) Widezones on '*Interoperability of security systems for the surveillance of widezones*'. The final text of this CWA will be submitted to CEN by the end of 2018 for publication. This CEN Workshop Agreement will be publicly available as a reference document.

4. PARTS OF SOLUTION: EU-WSRT

One of the outcomes of the ZONeSEC project would be the European Widezones Surveillance Reference Toolkit (EU-WSRT), which is a web application that serves as a decision support tool providing recommendation and guidance to Widezone owners and operators with regard to their CIs security. The EU-WSRT, which will be publicly accessible upon registration,

provides 3 distinct (sub)tools, namely: Security Management System (SeMS) Assessment tool, CI Risk Assessment tool and Inference Engine.

SeMS Assessment tool

The SeMS assessment module is intended to be used by all interested parties/entities (e.g. organizations, companies, stakeholders) who wish to augment their understanding of SeMS requirements and/or to assess whether the components of a SeMS are present and functioning adequately within their Widezones. Through the assessment procedure, the tool enables the identification of possible gaps and weaknesses in terms of organizational structures, accountabilities, policies, procedures and resources dedicated to security. The assessment is performed through a questionnaire (approximately 100 questions) that covers the main requirements of a comprehensive SeMS.

In sight of the questionnaire development the SeMS was regarded as a control and monitoring loop of activities that need to take place for the protection against security threats (Figure 2). The loop consists of 11 Components (A-K) that compose the entirety of the system and provide the requirements for establishing, implementing, monitoring, reviewing and improving operator's SeMS. For the 11 loop Components there are 9 common Topics that run through them. These Topics reflect the key management tasks that need to take place to have a complete SeMS and refer to issues related to security operations principles, risk assessment, security operating procedures, personnel competence and training, etc.

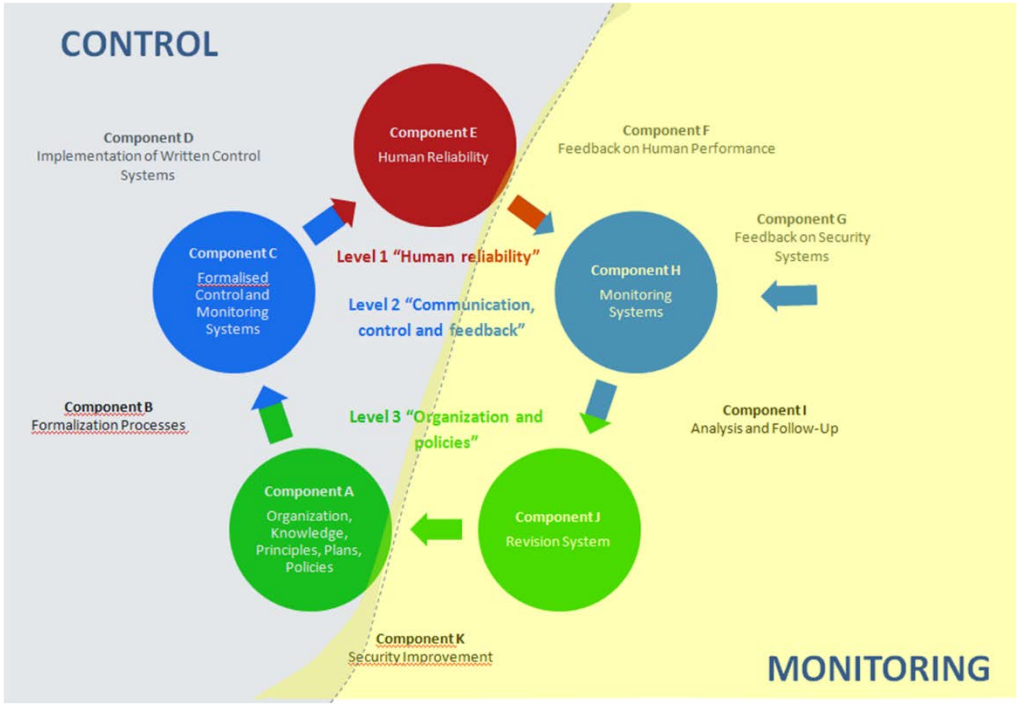

Figure 2. SeMS control and monitoring loop

Each Topic is linked to a specific question that can be replied as: i) Present, ii) Weak or iii) Absent. Following questionnaire completion, a summary report provides the achieved score, indicating company's/organization's level of compliance with the requirements of a comprehensive management system. In that way, the user can identify the potential areas where gaps and weaknesses may lie and thus allocate available resources accordingly.

CI Risk Assessment tool

The CI Risk Assessment module aims at supporting Widezone owners, operators, managers and decision makers in identifying, assessing and evaluating risks related to their Widezone security. For the development of the CI Risk Assessment module, the main principles of national and international regulatory frameworks and standards applied towards risk management and critical infrastructure protection were adopted [11,12,13]. As depicted in Figure 3 the CI Risk Assessment procedure comprises three main steps namely: i) Identification of critical infrastructure assets, ii) Identification of threats and iii) Risk analysis and evaluation.

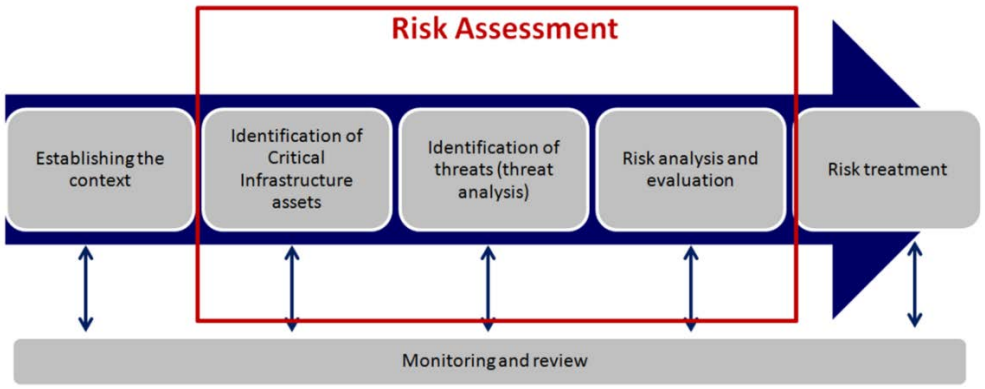

Figure 3. Main steps of Risk Assessment procedure

Regarding the identification of critical infrastructure assets, after having selected the CI sector of interest (e.g. water network, electricity, highway), the user is provided with an indicative list of assets and systems (relevant to his Widezone) that might be considered necessary for the production and the delivery of good services. For instance, for the drinking water sector, the given assets list includes, among others, the groundwater and surface water sources, pipelines, open canals, pumping stations, reservoirs, artificial lakes, water physicochemical treatment, tanks, pumps, valves and SCADA.

Upon assets selection, the user is guided to identify the possible threats each of those assets could be exposed to. A predefined list of security related threats, including explosion, contamination, theft, sabotage, cyber-attacks etc. is available by the tool, thought the user has the option to define additional threat categories he might be interested in investigating.

Having defined the security breach scenario (asset and threat), the last step regards the analysis and evaluation of its risk level. The CI Risk Assessment module is based on a semi-quantitative risk assessment procedure, through which the risk level of each security breach scenario is calculated as the likelihood of its occurrence multiplied by its anticipated consequences. Since security threats are not probabilistic and they do not have a statistical basis for determining likelihood, this is qualitatively calculated through the assessment of the following parameters:

- Feasibility, which relates to the ease of execution of the specific attack from the attacker's point of view;
- Target attractiveness, which is related to the features of a particular asset that make it more or less likely to be attacked for a particular type of attack;
- Vulnerability, which is regarded as the probability of the successful completion of the attack and is closely related to the security systems deployed in the critical infrastructure as well as to the existing security procedures.

The consequences of each scenario are assessed through the evaluation of impact related criteria. More specifically, the user is guided to provide a gravity scale with regard to the number of casualties, number of fatalities, cost of asset loss, environmental impact, out of service time, etc.

For the evaluation of risk analysis results, a risk matrix, with predefined scales for overall likelihood and combined consequences, has been introduced to the tool in order to enable user to have a better understanding of whether the risk level of each scenario is unacceptable, within tolerable limits or broadly acceptable (Figure 4). In that way, the outcomes of the CI risk assessment module enable companies/organizations to identify their security gaps and thus to better prioritize focus areas and security corrective measures.

		Type of Consequences			LIKELIHOOD (1- 100)				
	Gravity Level	People	Environment	Assets	A (4)	B (8)	C (16)	D (32)	E (64)
CONSEQUENCES	G6	Massive Fatalities to Public, Rescuers or Employees	A ≥ 200 ha	C ≥ 200 MEuros				Scenario	
	G5	Multiple Fatalities to Public, Rescuers or Employees	50 ≤ A < 200 ha	50 ≤ C <200 MEuros					
	G4	Single Fatality to Public or Multiple Fatalities to Rescuers or Employees	10 ≤ A < 50 ha	10 ≤ C < 50 MEuros					
	G3	Single Fatality to Rescuers or Fatalities to Employees	2 ≤ A < 10 ha	2 ≤ C < 10 MEuros					
	G2	Single Fatality or Injuries to Employees	0.5 ≤ A < 2 ha	0.5 ≤ C < 2 MEuros					
	G1	Single Injury to Employ	0.1 ≤ A < 0.5 ha	0.1 ≤ C <0.5 MEuros					

Figure 4. Risk Matrix applied for risk ranking

Inference Engine

The Inference Engine is envisaged supporting companies'/organizations' decision making with regard to CI protection. Its ultimate goal is to provide suggestions for enhancing the security status of a Widezone and/or an asset by finding the best match with security "concepts" (device, measures) which correlate best in terms of threat addressing, properties and constraints.

Navigating through the Inference Engine, the user is guided to provide input data related to his Widezone. For instance, those data may refer to the type CI sector, length of the asset that needs to be protected, its geographical location, available budget to be allocated for Widezone/assets surveillance, weather conditions in the area where the asset is located, etc.

Utilizing a set of data held in its knowledge base, the inference engine provides then the user with recommendations on assets protection and Widezone security enhancement. Such suggestions regard, for example, the type of security systems that need to be applied, the estimated cost, relevant regulatory issues pertinent to the recommended surveillance systems, etc.

5. PARTS OF SOLUTION: ZONeSEC TECHNOLOGIES CANVAS

Main technical components of ZONeSEC are presented in Table 1.

Table 1. The ZONeSEC technology canvas

ZONeSEC component	Description	Functionality
iDAS (sensing platform)	Silixa's intelligent Distributed Acoustic Sensor (iDAS) is an optoelectronic system which records the true acoustic signal continuously along the path of sensing fibre 10s of kilometres long with a frequency range of less than 1mHz to over 100kHz and a spatial resolution down to 1 metre.	iDAS offers the flexibility to operate on single mode or multimode fibre without the introduction of any external or additional apparatus, with no loss of signal quality and while preserving the true acoustic nature of the measurement. Enable detection of intrusion in secured area or detection of leaks.
ULTIMA (sensing platform)	Silixa's ULTIMA DTS range is the world's highest performing family of Distributed Temperature Sensors.	ULTIMA offers the finest temperature and spatial resolutions, from 0.01˚C and 35cm. Enable detection of fire or detection of explosion in secured area.
Acceleration sensors	Wireless Vibration-Acceleration Sensors developed by IK4-TEKNIKER	Detection of abnormal movements Low cost Plug&Play&Forget sensors
Spectral imaging system	Novel multisensory system with thermal, hyperspectral and SWIR cameras provided by ICCS	Enable virtual area fencing Detection of intrusion in secured area in bad weather conditions (rain, fog or dust) or at night.
Mini-UAV with onboard camera	Two mini-UAV provided by ADITESS (a multirotor and a helicopter type) equipped with electro-optic sensors including daylight and thermal cameras provided by ADITESS	Detection and tracking of selected targets such as people, cars. Enable live video streaming or photos from the inspected area.
MIMO-radar	MIMO Radar provided by Airbus in cooperation with TUD and Thales.	Detection of moving targets even in bad weather conditions (rain, fog or dust) or at night. The system can cover an area up to 200m and detect e.g. intruding persons in a secure area.
Cyber-agent	Provided by ICCS	Detection of cyber attacks
ZONeSEC Core	ZONESEC core is the integration component produced by ATOS and EXUS	Enable interconnection and interoperability of ZONeSEC components
UCM	Uniform Communication Module developed by ICCS	Enable interoperable and real-time communication from heterogeneous sources including legacy systems such as CCTV, Intruder Detection System, Vehicle Detection System, SCADA system, METEO System etc.
SDAIM	Surveillance, Detection and Alerts Information Management developed by IT-INNOVATION and THALES	Analyses and fuses data coming from the different sensors and is able to raise alerts on the COP
SIMISAW components: COP, SE and SP)	Common Operational Picture (COP) - Novel visualisation system developed by DIGINEXT. In addition, several COPs can connect to the same situation and share common information	Enable users to have a clear, synchronized, and interactive view of a controlled area enriched with alerts and updated information transmitted from security capillaries and enhanced with video stream from CCTV or mini-UAV cameras.
	Scenario Editor (SE) developed by DIGINEXT intuitive authoring tool to configure and run the simulation from a 3D geo-localized environment populated with a virtual representation of CI and virtual entities.	Provide means to create complex situations by deploying virtual sensors, characters, vehicles, and define interactions between them. Moreover, added sensors populate the ZONeSEC Core database allowing virtual sensors to be displayed on COP. These simulation tools can also be used for training operators and testing alert procedures
	Simulation Platform (SP) by ATOS and DIGINEXT intuitive simulation tool to enable a large-scale test and validation without having access to real systems.	Aid in designing and assessing a vast security system in a Widezone taking into account issues such as different coverage areas, sensor types, or threats.

6. PARTS OF SOLUTION: ETHICS AND SOCIETAL

The development of the ZONeSEC platform including several of steps in order to respect both ethical and privacy requirements. Issues related to legal and ethical implications have been addressed for the final purpose of establishing a solution which covers the current societal challenges when it comes to the protection of privacy.

Privacy is a complex topic. Its perception in a new monitoring technology world is a broad subject. Mechanisms and instruments reducing people's privacy, whether they are state or commercial actors, prefer that such instruments are not to be reduced nor put in question as a problem. The increasing impact of technology on privacy is obvious. Since the first famous incident with privacy intrusion owing to a ''mobile camera'', eloquently described by Warren and Brandeis (1890)[2], the emergence of ever more intrusive technologies has altered the discourse on privacy fundamentally.

ZONeSEC ethical management framework for citizens' protection took into consideration some elementary and crucial principles. From an *individual person perspective*, the far most important principle is *integrity*, which comprises ensuring honest, fair, and respectful treatment of persons involved in the project and subject to is development. The use of new technologies must be accompanied by activities which did not force citizens (volunteers, citizens) to sign Informed Consent Forms or authorization forms for the use of private information for dissemination purposes. Citizens' personal information must be protected thus physical, social and psychological well-being should be ensured and respect of their rights, interests, sensitivities and privacy. Another principle in strict relation with the protection of citizens is the principle of ensuring any harm, and these anticipating harms that can be caused during the use of such technologies. Proper precaution measures in order to minimise disturbance should be made. It is also very important to avoiding undue intrusion and to ensure the technology will not in any way harm citizens and became a disturbing experience. Confidentiality and anonymity is very important and it is mandatory to ensure the right to the citizens to remain anonymous and to have their rights to privacy and confidentiality respected.

During the project, from a *public (societal) perspective*, several issues and measures have been addressed and undertaken in order to respect both national legislation as well as legal regulations applied at European Union level. Of far most importance were the notification forms which were sent to the respective national data protection agencies (in Romania, Greece, Cyprus and Spain). Since the project tackles an involvement of wide critical infrastructure subject to public use, the necessity to inform the respective agencies is crucial in order to gain validity of the project and respect of regulations. However, by mere notification to the relevant authorities, the public is not informed. From legal and ethical point of view, the collection of data is only the first step of the processing of personal data. Processing collected data was carried out with caution. Most discussions of the ethics of computer surveillance are informed by the principles of fair information practice that received widespread public notice. Thus, the project also involved procedures to ensure that the public present at all project activities is informed by posting adequate and understandable signs and notices.

Data gathering and protection efforts imply ethical assumptions that are often unstated.

Thus, a distinction was made between (1) the means (instrument) of data collection, (2) the context and conditions under which the data are gathered, and (3) the uses/goals to which the data

[2]Warren, S. D., and L. D. Brandeis. 1890. ''The Right to Privacy.'' Harvard Law Review 4 (5): 193-220

are put. There is a temporal sequence here, as we start with the means and then move to collection and use. Since the project is challenging the notion of security and privacy at the same time, a specific and privacy-by-design approach was used. There is always the question on whether privacy and security can be reconciled. There is abundant evidence that many technologies aimed at enhancing security by subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. This was seriously taken into account and while developing the solutions offered by ZONeSEC, technology played a crucial role in the conciliation between privacy and security, by giving always priority to the former. The Table 2 below shows one of the main dimensions of privacy and security concerns which were addressed and respected during the project.

Table 2. Dimensions of Privacy Concern and Security Concern

Privacy Concern Dimensions	**Security Concern Dimensions**
Collection: collecting too much information on the user and storing it in the database	*Authentication*: the need to verify the authenticity of the user and the online platform
Unauthorised secondary use: usage of personal information for other purposed, without users' prior approval	*Non-repudiation*: the need to ensure that the transaction is genuine and not disputable
Improper access: access to personal information by unauthorized individuals	*Confidentiality*: the need for protecting the information from unauthorized access
Errors: Accidental and deliberate errors in the handling of personal information	*Integrity*: the need for preventing the information from getting altered or corrupted

The so-called privacy-enhancing technologies and identity management systems are expected to replace human oversight in many cases. The technology and its use have a major impact on the gathering, storage, retrieval and dissemination of information and its mail ethical impact relates to accessibility/inaccessibility and the manipulation of information. With the help of technology is it easier to access a person's private information by more people. Many scholars and experts pointed out that the use of technology in the processing of information cannot be seen as ethically neutral.[3] There are number of challenges in regards to privacy issues in 21st century and the most important could be said that it is the assurance that the technology which is used incorporates strict privacy requirements in the software, architecture, infrastructure, and work processes in a way that makes privacy violations unlikely to occur.

[3]Christians, C.G. (1991). Information ethics in a complicated age. In Ethics and the Librarian. Proceedings of the Allerton Park Institute, 29-31 October 1989, University of Illinois, Graduate School of Library, edited by F.W. Lancaster. Vol. 31. Also In Cochrane, J. (1991). Hell hound on my trail. Ethics and librarianship. New Zealand Libraries, 46 (11): 2 6-31. Kluge, E.H.W. (1994). Health information, the fair information principles and ethics. Methods of Information in Medicine, 33: 336-345.

7. USE CASES: AQUASERV ON SITE INTEGRATION PILOT (AQS OIP)

The ZONeSEC system has been deployed in three different types of critical infrastructure, namely highway, drinking water supply system, and natural gas distribution system, in three European countries. The purpose of these deployments was, first, to test ZONeSEC at different stages of its development process so as to allow for improvement, and, second, to demonstrate its performance to stakeholders. A total of seven pilot activities had been planned: four On-Site Integration Pilots and three Pilot demonstrations.

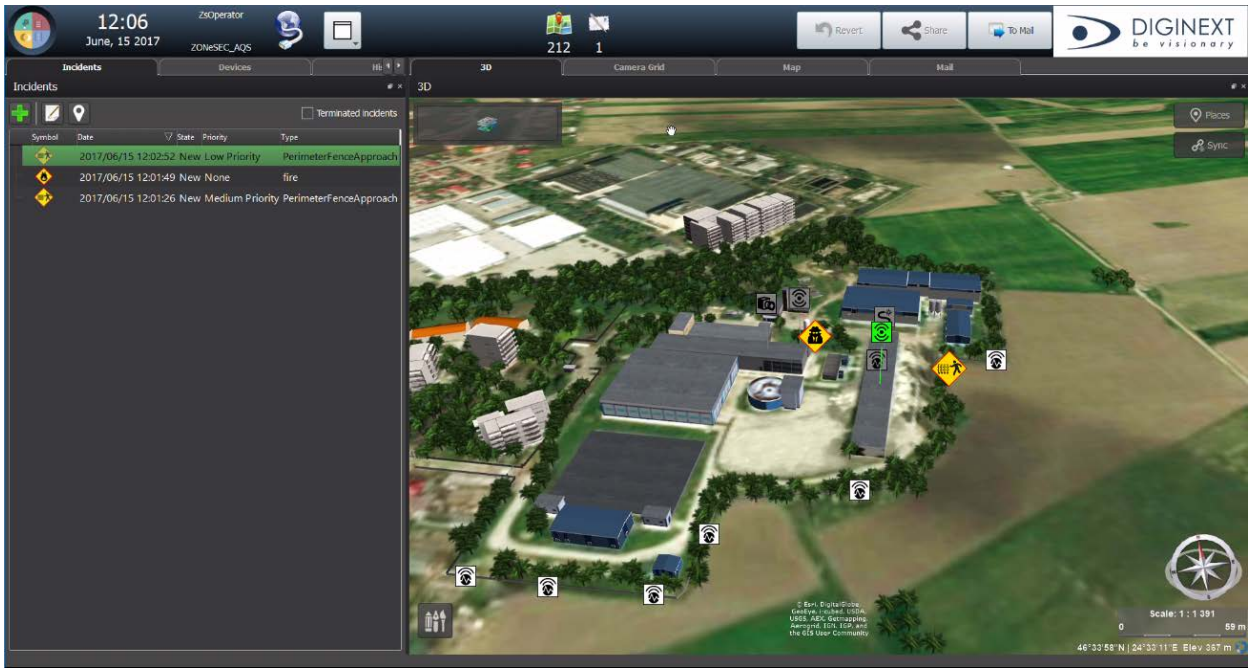

Figure 5. Screenshot of COP prepared for Aquaserv Pilot

Amongst the pilot activities carried out so far, Aquaserv hosted one On-Site Integration Pilot at its premises in Tirgu Mures, Romania, between 14th and 16th June 2017. Based on the needs and security concerns of the critical infrastructure at hand, a scenario of simulated threats was employed to show the benefits of ZONeSEC for water utilities and to test the system in near-real-life conditions. More specifically, the scenario involved a series of connected illicit activities (including a water contamination attempt), at four locations: Raw Water Intake Site, Drinking Water Treatment Plant (approximately 1 km away from the previous), Operations Centre of Aquaserv, and an airfield in Cyprus (used by the UAV sub-system). Using different technologies, the ZONeSEC system was capable to perform the following:

- 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.

Figure 6. Screenshot of the Scenario editor prepared for Aquaserv Pilot

In terms of the technology deployed, the detection capabilities were provided by the following sensing modalities and components:

- Plug&Play&Forget Wireless Acceleration sensors provided by IK4-TEKNIKER. These sensors were installed attached to different fence both at Raw Water Intake Site and Drinking Water Treatment Plant and identified abnormal movement of the fence;
- Distributed Acoustic Sensor (IDAS) provided by Silixa. IDAS is an optoelectronic system monitoring the acoustic field along an optical fibre cable. In this OIP, the IDAS was successful in detecting movement near a set perimeter;
- ULTIMA provided by Silixa. The ULTIMA DTS range is the world's highest performing family of Distributed Temperature Sensors. The ULTIMA family offers the finest temperature and spatial resolutions, from 0.01˚C and 35 cm. It is a standalone unit with an on-board PC and user-friendly software interface;
- Spectral Imaging System provided by ICCS. This is a novel multi-sensor system with thermal, hyperspectral and SWIR cameras. The processing of the huge amount of spectral video data was locally performed. The system successfully detected and disseminated approaching and intrusion alerts near AQS technical building;
- Mini-UAV sub-system, provided by ADITESS. This event tested the UAV sub-system's ability to receive missions or orders from the COP, and, through the Task-Based Guidance component, to prepare the flight plan for a mission. The UAV deployed was equipped with electro-optic sensors including daylight and thermal cameras, and provided real-time video stream including metadata (i.e. position, target);
- CCTV (legacy): The AQS premises included pre-existing video surveillance cameras. Due to security restrictions, direct access to this equipment could not be acquired, yet for testing purposes, a similar IP camera was used to connect to its live footage;
- Video analytics, provided by Atos. A special algorithm was developed to detect water contamination attempts. Due to security restrictions, a pre-recorded video (as opposed to live

footage) from the AQS CCTV camera in the water treatment room was streamed using the simulation module of ZONeSEC to test the video analytics;

- Magnetic contact switch (legacy), provided by ICCS. A magnetic contact switch similar to the commercial product that Aquaserv has in place was integrated into ZONeSEC to test detection of intrusion into secure room;
- SDAIM (Surveillance, Detection and Alerts Information Management) provided by IT INNOVATION and THALES, analyzed and fused data coming from the different sensors and was able to raise alerts to be displayed on the COP;
- COP (Common Operational Picture) provided by DIGINEXT and the simulation tools provided by ATOS and DIGINEXT. The COP displayed a 3D cartographic view of deployed sensors and raised alerts from subsystems. The simulation tools provided means to add geo-localized virtual systems and simulate their inputs to ZONeSEC;
- Uniform Communication Module (UCM) designed by ICCS, has been successfully integrated into ZONeSEC security capillaries and legacy systems enabling interoperable and real-time communications from heterogeneous sensor systems, following a distributed communication architecture;
- Security Clusters provided by IK4-TEKNIKER in collaboration with ICCS and IT INNOVATION, have been tested for the first time. A preliminary setup was proven, allowing the operator (COP) to aggregate a set of acceleration sensors of a certain area to be managed by a Cluster, which then raised distributed vibration alerts;
- CORE: All the different sub-systems were interconnected by the ZONeSEC Core and its supporting services. ZONeSEC Core is the integration component produced by ATOS in collaboration with EXUS.

8. FUTURE STEPS

The ZONeSEC system will be further refined in terms of improving the speed and accuracy of detection to enhance early warning, as well as in terms of adapting the system to best fit the requirements of the project's end-users. The latter is related mostly to the event fusion rules that determine the (combination of) events sufficiently dangerous to the infrastructure to automatically become alerts in the Operations Centre.

With the latest improvements, the fully integrated ZONeSEC system will be demonstrated for water utilities at Aquaserv in June 2018.

9. CONCLUSIONS

ZONeSEC aims to address the needs of Widezones surveillance by defining a new European-wide framework, which will extend beyond a sole technical proposition. Driven by the need to yield a holistic and uniform approach, ZONeSEC redefines the issue of security of widezones by taking into consideration issues pertaining to costs, complexity, vulnerability, societal acceptance and ethics.

10. ACKNOWLEDGEMENT

The authors would like to thank the project ZONeSEC. This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607292. For more information about the project and participants please visit https://www.zonesec.eu/.

11. REFERENCES

[1] Directive on European Critical Infrastructures: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF;
[2] European Programme for Critical Infrastructure Protection (EPCIP): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF;
[3] The new approach to EPCIP can be found in https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf;
[4] http://cordis.europa.eu/programme/rcn/19074_en.html;
[5] Critical Infrastructure in: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en;
[6] CCTV in public space in countries of the EU| Research and Documentation Centre (WODC). 2000;
[7] Stephen Ranford ; The picture is not clear: How many CCTV surveillance cameras in the UK?| British Security Industry Association, 21 August 2015 in https://www.bsia.co.uk/publications/publications-search-results/195-the-picture-is-not-clear-how-many-cctv-surveillance-cameras-in-the-uk.aspx;
[8] Juwet Griet, Cameras in public space, attitudes towards video surveillance in Belgium & Italy, http://www.academia.edu/7363692/Cameras_in_public_space_attitudes_towards_video_surveillance_in_Belgium_and_Italy;
[9] Mitrou, L., Drogkaris, P., & Leventakis, G. (2014). Legal and Social Aspects of Surveillance Technologies: CCTV in Greece?. *Perspectives on Surveillance*, 39;
[10] A definition of these objectives can be found in: https://www.zonesec.eu/project;
[11] Council Directive 2008/114/EC, of 8 December 2008, on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. Official Journal of the European Union. L 345, 75-82;
[12] US Department of Homeland Security (2013). National Infrastructure Protection Plan. Partnering for Critical Infrastructure Security and Resilience. Washington, DC, US;
[13] ISO 31000:2009. Risk management-principles and guidelines. International Organization for Standardization. Geneva, Switzerland.