FP7-607292

Towards an EU framework for the security of Wide zones

Table of Contents

1. Executive Summary

The challenges presented by the protection of critical infrastructures (CIs) represent a pressing issue for the European Union (EU). 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 that run across national borders. Furthermore, existing security measures has to be reused and integrated with any new sensors. The advancement of 24/7 surveillance systems for the security of Widezones with multiple assets at localised 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 prioritised. Critically the ethical and societal aspects have to be addressed from the beginning.

Included on the 7th Framework Program (FP7) projects, the project ZONeSEC (https://www.zonesec.eu/) proposes a complete and multidisciplinary solution based on the combination of already existing and novel sensors, taking into account the ethical&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.** 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.

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, use of simulation and the presentation of a common operational picture for the final user.

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 life Online Integration Pilots and three final demonstrations involving final users of different European countries (Greece, Romania, Spain).

2. Context and main objectives

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.

ZONeSEC will perform all needed research, development, integration and awareness raising work to yield a holistic system:

- By adopting a **Total Security Approach**, merging and balancing all relevant aspects in the design of an innovative Widezone surveillance system.
- To put in place **a scalable framework and congruent prototype** that will **guarantee the seamless and cost-efficient surveillance of Widezones – irrespective of their type –** enhancing to that effect the security of these broad areas beyond the mere surveillance of critical infrastructures.

- To support with its valuable functions a total **Early Detection and Situational Awareness** mechanism that will assist **authorities and operators in** the **prevention of illicit activities** even in the most complex, remote or demanding localized spaces.
- To dynamically assess how an activity might evolve into a threat for the well-being of the protected Widezone, **fusing different information data which** establishes an **active and dynamic surveillance framework** instead of the current passive and static one.
- To **improve the sensor base** and sensor intelligence for high quality input for the systems information fusion and processing framework, to detect various kinds of illicit pattern of activity, **reducing the rate of false alarms.**
- To provide a new **EU trendsetting benchmark** for Widezones surveillance systems, by delivering **a highly usable and on-line toolkit that will provide references, consultation and guidance services for the protection of infrastructure spreading across Widezones (EU-WSRT)**.
- To set a cornerstone for the **standardization of equipment, network architecture, processes and methodologies** for Widezones surveillance purposes on an EU level addressing the cross-cultural issues emerging from the diversity of normative frameworks, contexts of implementation etc. ZONeSEC aims at providing pre-normative standards through modern dual path standardization process: Standardization Organizations committees and workshop agreement/industrial specifications group.
- To provide **recommendations on policies** development aiming at harmonizing the European, National and Regional regulatory packages applicable to the protection of critical infrastructures in Widezones.
- To **safeguard the societal acceptance** of the proposed framework by adhering to the recommendations and expectations of the Societal Impact Expert Working Group.
- To set-up **visible demonstrations of an innovative and a Unique Reference Surveillance System** for the protection of Widezones in realistic situations.
- **To support civil protection authorities** in the formation and validation of proper safety procedures for the **mitigation of the effects of illicit activities** towards a Widezone. (esp. parts of the protected infrastructure that are close to metropolitan or urban, semi-urban areas)

The ZONeSEC methodology will bring the stakeholders in the spotlight of all envisaged systems development; from the **collection of user requirements**, to the iterative development and validation of the system's technical specifications & **the performance of pilot demonstrations and integrity tests**, the involved **user groups– infrastructure operators, citizens, first responders, crisis managers, resource/infrastructure managers**, and **public agencies** - will be integral cogs in the process.

3. Description of main S&T results/ foregrounds

3.1 Final results

3.1.1 Surveillance of Widezones *(Work Package 2)*

The preliminary work performed in this work package aimed at setting the groundwork for the initiation of the rest ZONeSEC project activities, focusing on defining the AS-IS situation of Widezones

surveillance and identifying requirements and needs in terms of technology and procedures applied for critical infrastructure protection. Towards that direction, a thorough literature survey was conducted on the existing critical infrastructure protection regulations, standards, guidelines and plans/programs applied worldwide as well as on the surveillance, detection and alert systems/sensors applied for Widezones security enhancement. Special emphasis was given on the Directive 2008/114/EC and the US Presidential Policy Directive-21 (PPD-21) (along with the subsequently issued National Infrastructure Protection Plan-NIPP), which are widely applied in the EU Member States and the US respectively, as well as on sector specific security plans applied for the protection of various critical infrastructure sectors such as highways, drinking water and natural gas networks.

The next action point targeted the engagement of the ZONeSEC end-users and the acquisition of their feedback with regard to the threats and hazards that might pose risks to their critical infrastructure security. An extended questionnaire was developed and distributed among consortium end-users that aimed at delineating their current security status and potential technological or procedural gaps as well as defining how the deployment of the ZONeSEC system could enhance their assets' and systems' integrity. Additionally, considering that WP2 was serving as the interface between ZONeSEC technical partners and end-users, the questionnaire also included questions from the technical partners' side that aimed at clarifying how their subsystems could be applied to each end-user case. More specifically, the Surveillance of Widezones questionnaire aimed at:

(i) identifying end-users' current situation and needs on standardization and regulations, legislation, ethics and societal issues;

(ii) identifying and analyzing the existing technologies applied for the surveillance of the end-users Widezones as well as the new ZONeSEC technologies that the end-users are interested in integrating;

(iii) assessing the priority use cases that the end-users are interested in addressing, and

(iv) assessing the adequacy of Security and Safety Management Systems (SeMS and SMS, respectively) applied by end-users' companies.

The feedback collected through the questionnaire, the information available in the DoW, an extensive literature review as well as the knowledge from previous related EU research projects were all instrumental towards the development of a thorough list of user requirements that described in detail the expectations the end-users have from the ZONeSEC system. Technical partners, then, defined the specifications their subsystems need to have to fulfill each user requirement, resulting thus to the development of the ZONeSEC "User and System Requirements" document. That was a living document, i.e. subject to modifications till the late project stage, which served as a traceability matrix and baseline tool for the concise development and realization of the ZONeSEC solution. In addition, considering that the ZONeSEC system was aimed to cover the needs not only of the consortium end-users but also of an extended end- users group, a dedicated workshop was held in Athens on October 2017 that was envisaged shedding light to potential additional user requirements that had not been identified so far. That action showcased that the ZONeSEC system was being developed considering every single user need.

The entire aforementioned information was integrated in the deliverable D2.1 entitled “Current and emerging needs of Widezones Surveillance”.

The next activity in this Work package, targeted the definition of the ZONeSEC use cases. For the purposes of the ZONeSEC project, two sets of uses cases were developed. The first one was regarded as a written procedure for capturing the sequence of interactions between users (e.g. the ZONeSEC Administrator and the WZ Technician) and the ZONeSEC system, i.e. describing what users are trying to achieve using the ZONeSEC system and what is the step-by-step process that the user follows to complete his goal using a particular ZONeSEC feature or component (e.g. how he/she logs into the ZONeSEC COP, how he/she deploys the UAV and how he/she acquires information on security clusters) . Those use cases were regarded as a means to identify, clarify and organize system requirements. Considering that the use cases were in place to ensure that all user requirements are addressed by the process of technological development, the use cases aimed and achieved to encompass all these user requirements. The second set of use cases aimed at providing an overview of the main processes that take place for the accomplishment of the ZONeSEC system functionalities. More specifically, through those use cases the detection capabilities of the ZONeSEC system were adequately described such as the detection of vehicle against traffic, the detection of fire, and the detection of perimeter approach by person or vehicle. For each detection category, detailed information on sensors’ and subsystems’ involvement, sensors installation, data flow, information displayed on the COP and sensors potential deployment limitations was provided.

Upon the development of the use cases, the following action regarded the definition of Key Performance Indicators (KPIs). KPIs constitute a way of performance measurement and objectives fulfillment evaluation and they are applied to measure progress towards project goals and the quality of a proposed/adopted solution. The KPIs identified for the purposes of the project focused on the evaluation of the ZONeSEC system (platform) performance as a technical solution, leaving aside the assessment of other methodologies and tools that were developed within the project (e.g. Risk Assessment, Standardization issues). Within WP2 the scope was to define high level KPIs that refer to measurable and comprehensible indicators for the performance of the ZONeSEC system as a whole, while low level KPIs were addressed by individual WPs which were related to sub-systems development. The approach adopted for the definition of the ZONeSEC KPIs, drew on the DoW and user requirements to derive specific indicators in order to follow progress on key aspects of system performance in a measurable and quantitative way. A set of five general performance categories was identified namely efficiency, autonomy, interoperability, reliability and robustness. Those general categories were correlated to relevant KPIs, for which a target value was set. For defining the target values emphasis was given on the desirable and targeted functionalities of the ZONeSEC system that also fulfill the end-user requirements and expectations. It should be highlighted that all the KPIs were quantitative and measurable indicators. The actual performance of the system, and thus the level of KPIs fulfillment, was tested at the three pilot demonstrations, allowing for the assessment of ZONeSEC effectiveness to achieve its key objectives and offer a beyond state-of-the-art solution.

The use cases together with the ZONeSEC KPIs formed the WP2 deliverable D2.2 “ZONeSEC Use Cases and target KPIs”.

One of the core tasks of this work package was the definition of a robust Security Management Framework that serves as a holistic approach for Widezone protection and resilience and aims at providing useful insights on the main elements that should be present in the security strategic plans

(e.g. the Operator Security Plans OSPs imposed by the Directive 2008/114/EC) developed and implemented by critical infrastructure owners and operators. The Security Management Framework encompassed all the provisions of an adequate Security Management System (SeMS) along with a Security Risk Management Framework that constitutes an integral part of it (figure below).

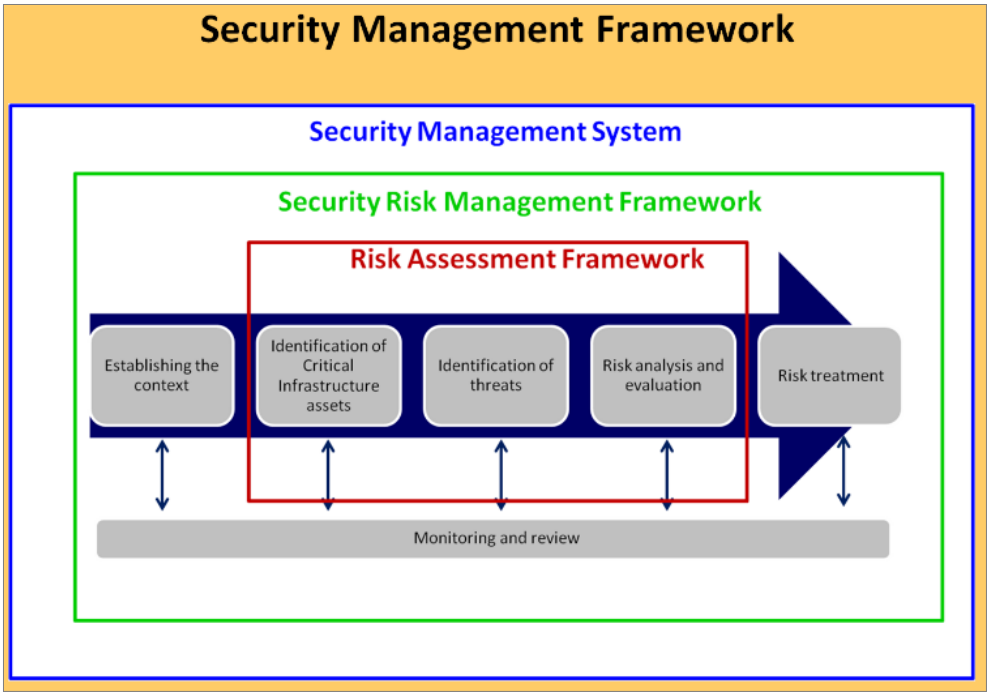


Figure 1 The ZONeSEC Security Management Framework

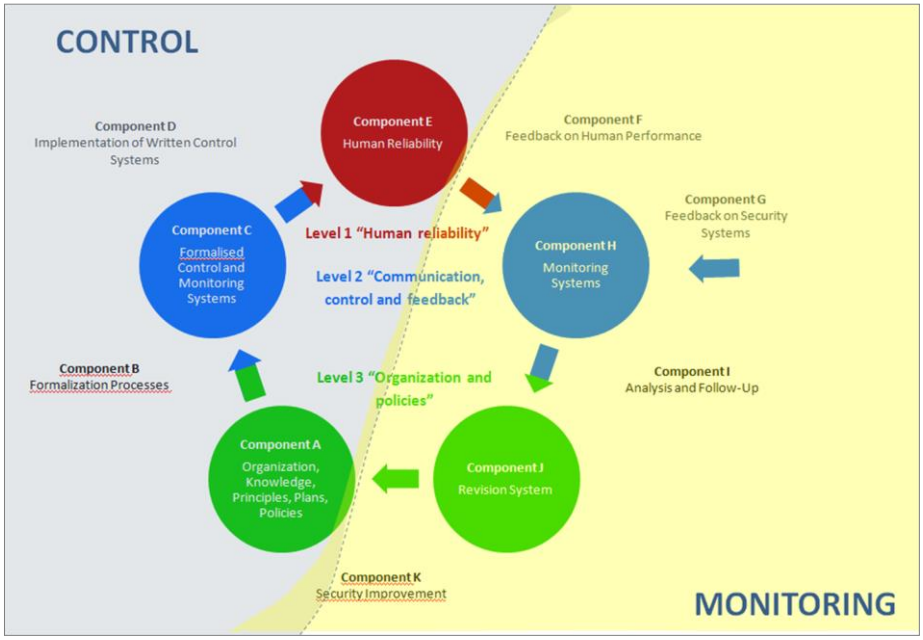


Figure 2 The SeMS presents as a Control and Monitoring loop of activities

As far as the SeMS is concerned, it constitutes as systematic approach applied to managing security, including all the necessary organizational structures, accountabilities, policies, procedures and resources. The developed SeMS was regarded as a Control and Monitoring loop of activities that need to take place for the protection against security threats (Figure 2). In brief, the proposed

framework for the SeMS, through its Components (boxes and links, A-K), provides all the necessary requirements for establishing, implementing, monitoring, reviewing and improving a company's security. Those requirements were analyzed in a questionnaire form, since the goal was not only to inform critical infrastructure owners/operators on the main provisions but also to provide them with a tool that enables them evaluate their company's SeMS maturity level. The SeMS questionnaire comprises approximately 500 questions that can be answered as Present, Weak, Absent, depending on whether the specific provision is addressed within company's SeMS or not.

A short version of the SeMS assessment questionnaire (approximately 100 questions), which covers only the main organizational and procedural requirements, was developed as a web based tool and integrated into the ZONeSEC European Widezones Reference Toolkit (EU-WSRT) (developed in WP12), serving as self-assessment rapid ranking tool. Navigating through the tool, the user is guided to answer a series of questions in order to get a score indicative of his company compliance level to the SeMS main provisions and requirements.

The Security Risk Management Framework, is an integral part of company's SeMS, in the sense that SeMS is considered inadequate and can function properly only if a formalized risk management procedure is integrated into it. The critical infrastructure security risk management framework supports a decision-making process that critical infrastructure partners collaboratively undertake to inform the selection of risk management actions. As shown in Figure 2, the main stages of the risk management process are:

a) Establishing the context
b) Identification of critical infrastructure assets
c) Identification of threats
d) Risk Analysis and Evaluation
e) Risk Treatment
f) Monitoring and review

For the scope of the ZONeSEC project, special emphasis was given on stages b, c, and d, which all together define the risk assessment procedure. Firstly, thorough lists of assets for various critical infrastructure sectors were developed, accompanied by detailed guidance on how the assessment of their criticality level can be performed. In addition, adopting the all-hazards approach, extensive lists of hazards and threats were developed including technological, accidental and natural hazards as well as terrorist and cyber attacks that can affect critical infrastructures and disrupt business continuity. However, considering the ZONeSEC project scope and objective, the developed risk analysis and evaluation methodology targeted mainly the manmade/intentional threats and acts of terrorism, such as explosion of man portable IEDs, CBRN threats and sabotage/vandalism. Through that methodology, the risk of a security breach scenario is estimated semi-quantitatively, considering among others how easy is the execution of the attack (from the attacker's perspective), how tempting the particular asset is, how vulnerable the asset might be in terms of available security systems and management procedures and what is the anticipated extent of consequences of the scenario under study.

Upon estimation of all risk assessment criteria, the ZONeSEC risk matrix with predefined likelihood and consequences scales is applied to locate each scenario within a specific "color –zone" (Figure 3). This color-coding risk ranking facilitates the identification of priorities and focus areas in which

additional measures should be applied to ensure assets' security and uninterrupted business continuity.

		Type of Consequences			LIKELIHOOD (1- 100)				
	Gravity Level	People	Enviro nment	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 3 The SeMS presents as a Control and Monitoring loop of activities

The aforementioned methodological procedure for risk analysis and evaluation was the backbone for the development of the CI Risk Assessment tool that was integrated into the EU-WSRT toolkit (developed in another Work package). Navigating through the tool, the user develops a series of scenarios, assesses the various feasibility, target attractiveness, vulnerability and consequences parameters and then gets informed on their risk level, in order to prioritize focus areas for further security investments.

In sight of the pilot demonstrations, the risk assessment methodology was applied for all ZONeSEC end-users cases, resulting to the definition of numerous worst case security breach scenarios as well as to the identification of weak points and gaps and the prioritization of additional security measures (technical, organizational, managerial) that need to be applied to reduce vulnerabilities and relevant risks. For those scenarios that involved dangerous substances (e.g. flammable, explosive and toxic substances), a specialized software was applied to simulate possible physical effects due to releases of those substances and thus to enable the estimation of consequence zones due to thermal radiation, overpressure and toxic cloud.

It needs to be highlighted that in Work package special emphasis was given on disseminating and spreading the concept of the ZONeSEC Security Management Framework. That was achieved through the organization of dedicated workshops, the participation in security related conferences and events (e.g. the OECD-JRC Workshop "System thinking for critical infrastructure resilience and security", the CAE Conference "Evolving Engineering Simulation: The age of Digital Twin") as well as through the establishment of clustering with the ERNCIP TG "Extended Warning Zones for Critical Infrastructure Protection (EWZ4CIP)". That extensive activity allowed for the validation of the SeMS and Risk Assessment approaches not only by the ZONeSEC end-users but also by numerous external critical infrastructure operators, stakeholders and experts at national and EU level.

The main elements and principles of the robust Security Management Framework were described in detail in the T2.5 internal report entitled “Common Risk Management among various Widezone Infrastructures”, which was shared among consortium partners.

3.1.1.1 Identified innovations:

The greater challenges and achievements of this work package could be summarized as follows:

- Definition of the main principles of a robust Security Management Framework that is applicable to multiple Widezone Critical Infrastructure sectors. The proposed and adopted framework reflects the main requirements imposed by the Directive 114/2008/EC with regard to the development of Operator Security Plans (OSPs) by the European Critical Infrastructure operators. The establishment of a holistic Security Management Framework by critical infrastructure owners/operators is deemed as a fundamental prerequisite that has to be present prior to the deployment of any security countermeasures, since it is the only means to guarantee measures’ efficient application and thus an in depth enhancement of critical infrastructure protection.
- With regard to Widezone critical infrastructures, there is no standardized methodology applied for the development of holistic and robust Security Management Framework (including SeMS and Risk Assessment): A novel methodology was developed incorporating the main principles of internationally acknowledged guidelines, standards and good practices. An extended group of end-users, including a technical advisory group of representatives from the oil and gas sector, validated the developed methodological framework and highlighted its applicability in energy CIs.
- The developed holistic Security Management Framework adopts the all-hazards approach towards critical infrastructure protection, encompassing additionally natural and technological hazards as well as hybrid threats that could affect the integrity of critical infrastructures and disrupt business continuity. The concepts of assets’ and systems’ internal and external interdependencies and their interconnectedness with the upstream and downstream supply chain were introduced in the proposed framework and constitute an integral part of it. That approach provides a systematic framework for the communication between policy makers, authorities and operators, enabling coordinated response planning, raising stakeholders’ awareness level and fostering effective CI protection. That framework was the backbone for the development of the CI Risk Assessment tool that was integrated into the EU-WSRT toolkit (WP12).
- The requirements of a comprehensive Security Management System (SeMS) were defined and developed in a questionnaire form, which serves as a self assessment tool for companies’ maturity level in terms of organizational issues, procedures, accountabilities and resources dedicated to security. The SeMS assessment questionnaire has been integrated as a distinct module in the EU-WSRT toolkit (WP12).
- Development of a holistic Security Management Framework that applies to all Widezone sectors and CIs: The implementation of ZONeSEC SeMS, Risk Management and Risk Assessment approaches in a series of pilot cases demonstrated its ability for consistent applicability, validity and credibility to a wide range of CIs (e.g. water, road and rail transport, oil and gas, electricity etc).
- Preliminary Risk Assessment was performed for all 7 OIPs and pilot demonstration cases (ACCI, AQS, ATTD, DESFA). Numerous representative security breach scenarios have been studied and their risk level was estimated. That analysis enabled the identification of

vulnerabilities in the critical infrastructure networks under study, showcasing and prioritizing the focus areas where additional measures, such as ZONeSEC subsystems, can be applied. Moreover, the Preliminary Risk Assessment was the groundwork for an another novelty introduced by the ZONeSEC project: All alerts appearing on COP were assigned a criticality level, which is estimated as a function of the risk of all possible security breach scenarios related to that alert. In this regard, operator's early warning and increased awareness on potential anticipating threats is achieved.

- Clustering with the ERNCIP Thematic Group "Early Warning Zones for Critical Infrastructure Protection (EWZ4CIP)" that enables sharing of common priorities on fostering the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities. That action enabled the identification of further needs related to technological developments, promotion of standardization activities on systems' interoperability, policy enforcement and training practices as well as dissemination of ZONeSEC project achievements, the validation of the adopted ZONeSEC Security Management Framework and the establishment of a collaboration framework that could serve as a means of possible exploitation of ZONeSEC project results.
- Promotion of the ZONeSEC Security Management Framework and engagement of critical infrastructure operators, stakeholders and third parties in the concept of the holistic security management framework as well as in the technological developments of the ZONeSEC project: Through the organization of dedicated workshops, the participation in security related events and dedicated technical meetings, key "players" were successfully introduced to the field of critical infrastructure security, spreading the concept and goals the ZONeSEC project serves, increasing their awareness on security issues, and showcasing the need of collaborative efforts from both public and private entities towards the development of security plans that reflect the needs of national critical infrastructure owners.

3.1.2 Modular Sensing Platforms – Ground Systems *(Work Package 3)*

As a general conclusion of the work performed in this work package, several different contributions have been delivered to the whole ZONeSEC solution that have been fully tested and demonstrated in the final pilot activities.

Starting from an **initial survey** and evaluation of technologies and solutions applicable to Widezone surveillance and following with the identification, specification and **development of** several **novel Ground sensing solutions**, a set of novel detection technologies have been successfully brought to the final ZONeSEC solution. In parallel, a more **conceptual approach** by means of the definition and modelling **as Security Capillaries of every interfaced sensing system** has been proposed and implemented, targeting not only the novel systems (ground and airborne) but also commercial solutions (COTS) and the existing legacy systems at end users' premises.

Furthermore, the definition, specification and **development of the Security Clusters** has been also led from WP3, giving the whole ZONeSEC solutions the means **to dynamically scale the system** considering geographical, communication or processing aspects, while keeping the whole process of adding or removing Capillaries inside a Cluster transparent and easy for the operator. This activity has required very close and strong collaboration between several technical WPs (mainly WP3, WP5, WP6, W7 and WP8), indirectly helping in the overall integration process for the different components developed by partners.

Finally, and supporting the rest of activities previously mentioned, the last task of WP3 about **Plug-Play and Forget** has focused on the definition and development of **solutions for an easier, more efficient installation, deployment, operation and maintenance** of components at different levels,

from a more specific approach for the Wireless Sensor Networks up to the more generic about Security Capillaries and Clusters.

3.1.2.1 Identified innovations:

The innovations provided by *Modular Sensing Platforms – Ground Systems Work package* of ZONeSEC can be summarized as follows:

- **Novel ground sensing solutions**

A set of innovative ground sensing solutions using different technologies have been developed and successfully tested:

- **optic fiber based** distributed acoustic (iDAS) and temperature (ULTIMA) **sensing platforms**, being able to cover several kms with a single processing unit, that is able to detect, classify and locate different events along and around the fiber.
- A **spectral sensing system** combining detection and processing in several visible and non-visible ranges, such as hyper (400-700nm), SWIR (900–1700nm), Thermal (8-13um) and supporting not only an enhanced detection under harsh conditions but also advanced features like virtual fence/perimeter placement
- **Plug, Play& Forget wireless** acceleration **sensors**, offering a low cost, easy to deploy and maintain solution that can be also extended with optional features like motion detection (to reduce false positives) and energy harvesting capabilities (to extend the battery lifetime).

- '**Capillaries' concept → common interface and model for any subsystem**

The concept of Security Capillaries proposed by ZONeSEC is an abstraction of the different sensor systems within ZONeSEC platform, a way to describe in a common format the features and information of the very wide and heterogeneous catalogue of sensing platforms, new, commercial or legacy, that can be found in every specific WideZone where ZONeSEC might be deployed.

The concept of Capillaries has been defined to act as the front-end for the (raw) data acquisition, and a common abstract metamodel based on **OGC standards** has been provided to describe all those potentially 'to-be-interfaced' heterogenous systems:

- Sensor data observations, based on **O&M** standard
- Metadata modelling using **SensorML**
- **Tasking** profile for "incoming commands"

Further reading: Deliverable D3.3 entitled as "Security Capilaries and Clusters Data Models and Ontology".

- **The 'ZONeSEC Cluster' as enabler for scalable and distributed surveillance**

From the perspective of the physical architecture of ZONeSEC, Security Clusters can be considered as processes running onto a certain machine (specific one or belonging to an existing Sensing system).

Regarding the logical operation of a cluster, it can be considered as an element placed in the middle of the logical communication channel between the Security Capillaries and the ZONeSEC Core. On both sides, the CLusters use the Uniform Communications of WP6.

Conceptually, the Cluster itself can be essentially assumed as a special Capillary that is able to aggregate other Capillaries according to a specific configuration (configurable following tasking model of OGC) and run some local detection algorithms and rules. The results of these local processings will become the set of observations that the Cluster provides.

The main functionalities that ZONeSEC Clusters offer are:

- **Virtual aggregation** of capillaries
- Embedded intelligence towards **distributed** illicit activity **detection**.
- Configurable and **autonomous**

- **Plug&Play&Forget (PPF)** paradigm applied to ZONeSEC

Main goal: 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.

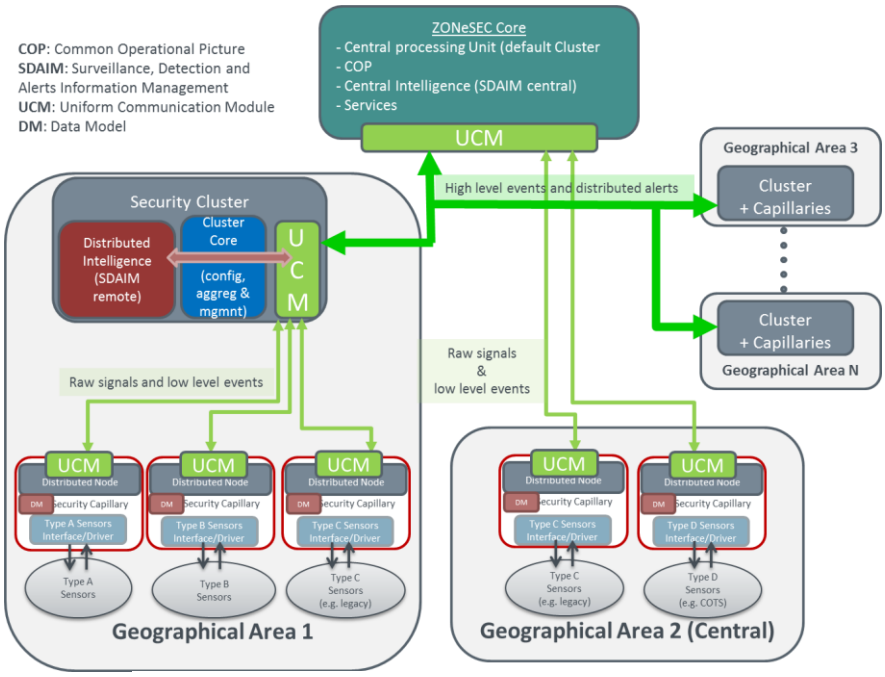


Figure 4: Zonesec Clusters architecture

Some of the PPF features adopted in ZONeSEC system:

- 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 cost calculations and decisions relate to a deployment of Wireless Sensor Networks (WSNs).

Further reading: Deliverable D3.4 entitled as "Plug& Play& Forget Technology".

3.1.3 Modular Sensing Platforms – Airborne and Radar Systems (*Work Package* 4)

ADITESS participation in the ZONeSEC project is mainly related with the provision of Mini-UAV Systems. The work done by ADITESS is divided in two main parts: (a) the integration of Mini-UAV systems, and (b) the development of relevant software to support the operations of Mini-UAVs in surveillance applications. During research, ADITESS identified the appropriate payload, communication equipment and UAV platforms to fulfill end-users requirements. In particular, two Mini-UAV platforms, one multi-rotor and one helicopter type, equipped with dual sensors (day and thermal) as well as state-of-the-art digital data links have been developed and used during the ZONeSEC pilots. Additionally, the preparation of Mini-UAV Ground Control Stations to support the manual and

automated flight, control of payload and the integration with ZONeSEC Core have been achieved throughout the project's lifetime. Beyond the provision of Mini-UAV Systems, ADITESS developed the Task-Based Guidance (TBG) system, an intelligence web-based component for the coordination of UAV teams, platforms and sensor configuration. In particular, TBG can be considered as a decision support system for the selection of the appropriate Mini-UAV platform (platform, payload, communication) and ground control station (GCS), based on several criteria, including the mission analysis (path, time, covered distance, range), GCS locations, risk metrics and specifications of the equipment. The result of the TBG component on a mission request is the generation of the mission plan. Considering the developments in ZONeSEC project, ADITESS manages to provide Mini-UAV services where the management of the fleet and the transmission of real-time image from remote locations (thousand miles away from the control center of Critical Infrastructures) is achieved.

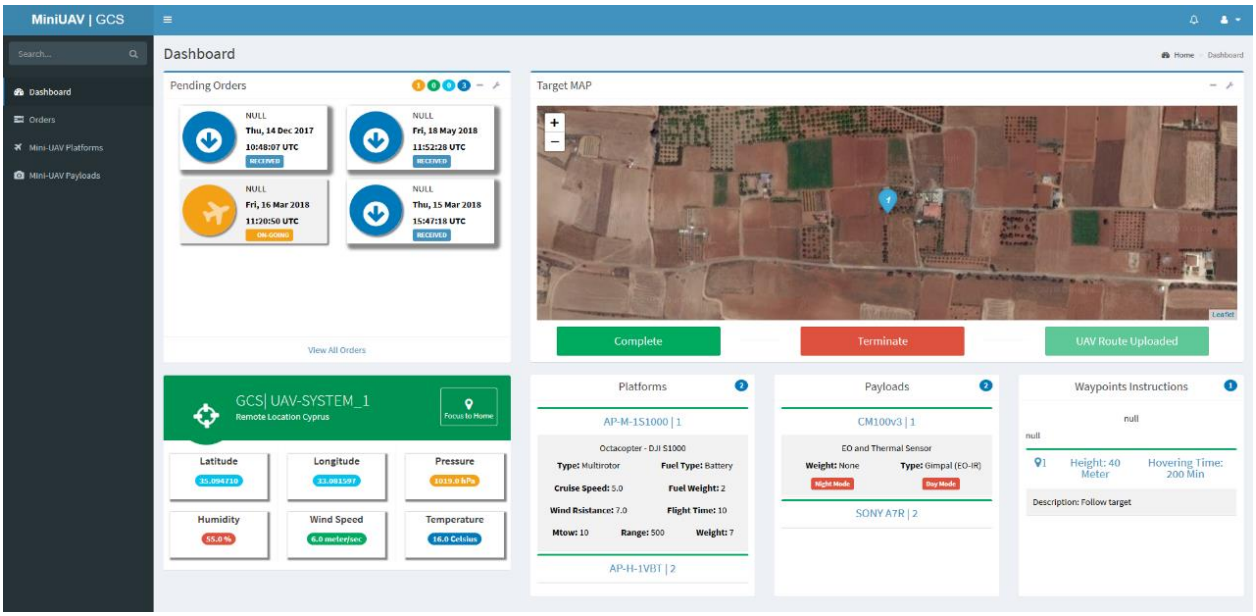


Figure 5 Ground Control Station

Airbus developed a software-defined Multiple-Input-Multiple-Output (MIMO) radar system, capable of estimating target position (range and azimuth) and velocity. Radars are especially relevant for zone security because of their inherent all-weather detection capability. Additionally, radar systems which capture also angular information are usually mechanically steered, in sophisticated radar systems the steering can also be done electronically. The MIMO concept is a new approach to obtain angular information. Here, the transmit antennas illuminate the whole scene and beamforming is applied at the receive array. This makes it possible to obtain angular information in a low size, weight, power and cost (SWAPC) manner. The system was built in a modular way. This allows to adapt the system to the scenario at hand. For example, the field of view (detection area) can be modified by exchanging the antennas, focused high-gain antennas increase the detection range but narrow the field of view, in contrast, not-directed antennas with low-gain have a wide field of view but limited range. Furthermore, the system was designed for a very high frequency agility. This means that the operating frequency can be easily changed within a very wide frequency band in order to comply with international governmental regulations. The system development was divided in two parts. First, a prototype with reduced functionality and afterwards a full-scale system demonstrator were built and tested.

Figure 6 MIMO radar deployed at ATTD pilot, Athens, Greece

A novel frequency synthesizer, which acts as a signal generator within the primary FMCW MIMO radar system, has been designed by the TU Dresden. This frequency synthesizer uses a novel architecture and combines multiple voltage-controlled-oscillators in order to create an ultra-wideband frequency ramp. Even though the wide output frequency tuning range of 3 GHz to 22 GHz, the system features still low phase noise and is cheap and small at the same time.

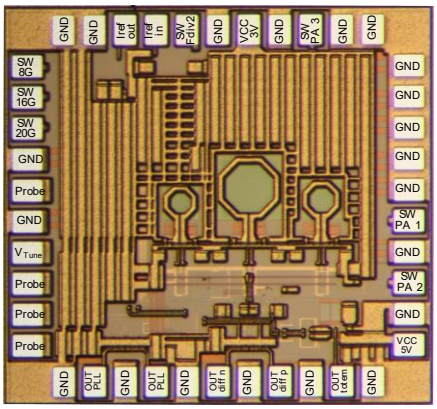


Figure 7 130 nm SiGe ASIC micrograph, area 1.4x1.3 mm²

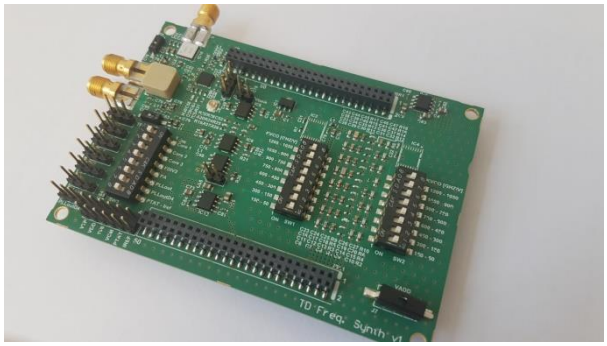


Figure 8 Ultra-broadband frequency synthesizer for frequency ramp generation

Ultra-wideband, high dynamic range Receiver (RX) and Transmitter (TX) FMCW MIMO radar Front-Ends have been designed, fabricated and tested (Figure 9 and Figure 10). The designed RX and TX ASICs comply with the given specifications and outperform the State of the Art in orders of magnitude.

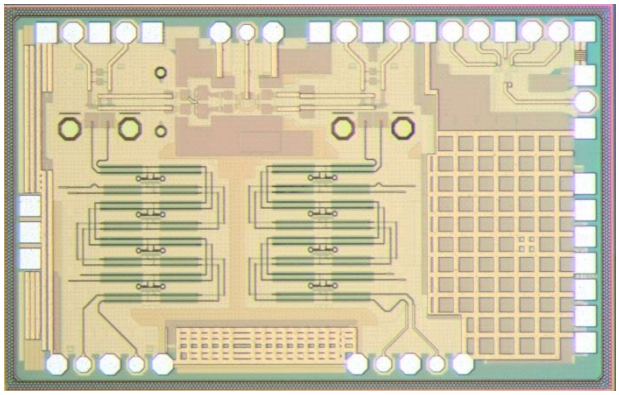


Figure 9 130 nm SiGe RX Front-End, area 2.2 × 1.4 mm² 130 nm SiGe TX Front-End, area 3.2 × 1.2 mm²

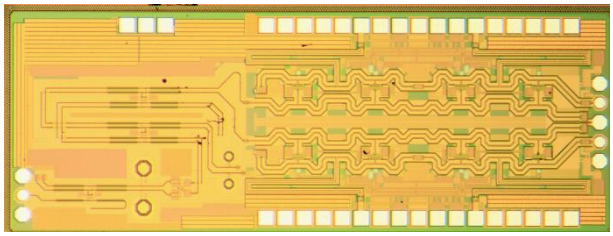


Figure 10 130 nm SiGe TX Front-End, area 3.2 × 1.2 mm²

3.1.3.1 Identified innovations:

Main achievements of the technical development were the software-designed real-time MIMO signal-processing algorithms, the target tracking and the setup of a complete hardware demonstrator, starting from chip-level.

The demonstrator has two transmit and eight receive antennas and achieves an angular resolution of about 5° in azimuth. The output power of the system is comparable to a mobile phone. In the most advanced configuration, the radar was capable of detecting person up to 150 meter in a field of view of 100° in azimuth.

The full-scale demonstrator was successfully deployed two times, in Targu Mures, Romania, June 2018 and Athens, Greece, October 2018. There the system was able to detect persons entering a forbidden zone, showed the track of the person on the COP and finally raised an alarm when the person crossed a virtual fence.

3.1.4 Large Scale Surveillance, Detection and Alerts Information Management (*Work Package* 5)

The SDAIM (Surveillance, Detection, and Alerts Information Management) system software is a result of the joint R&D work of the 13 WP5 partners, led by the IT Innovation Centre at the University of Southampton, in close collaboration with the rest of the ZONeSEC WPs and especially with the end-users and technical experts in these WPs.

The SDAIM is a self-sufficient federated system for geo-distributed surveillance, critical events detection and alerts generation and management for the security of large critical infrastructures (Widezones). Within ZONeSEC the SDAIM is responsible for the (soft-real-time) detection of illicit activities to support timely decision making by the Widezone's security operatives. This is achieved by the utilisation of state-of-the-art technologies, techniques and algorithms for distributed computations, scalability, fault-tolerance and multi-modal multi-sensor data and information fusion. The SDAIM implements the JDL/DFIG multi-level data and information fusion model for holistic Widezone surveillance, detection of critical events and generation of security related alerts (figure below).

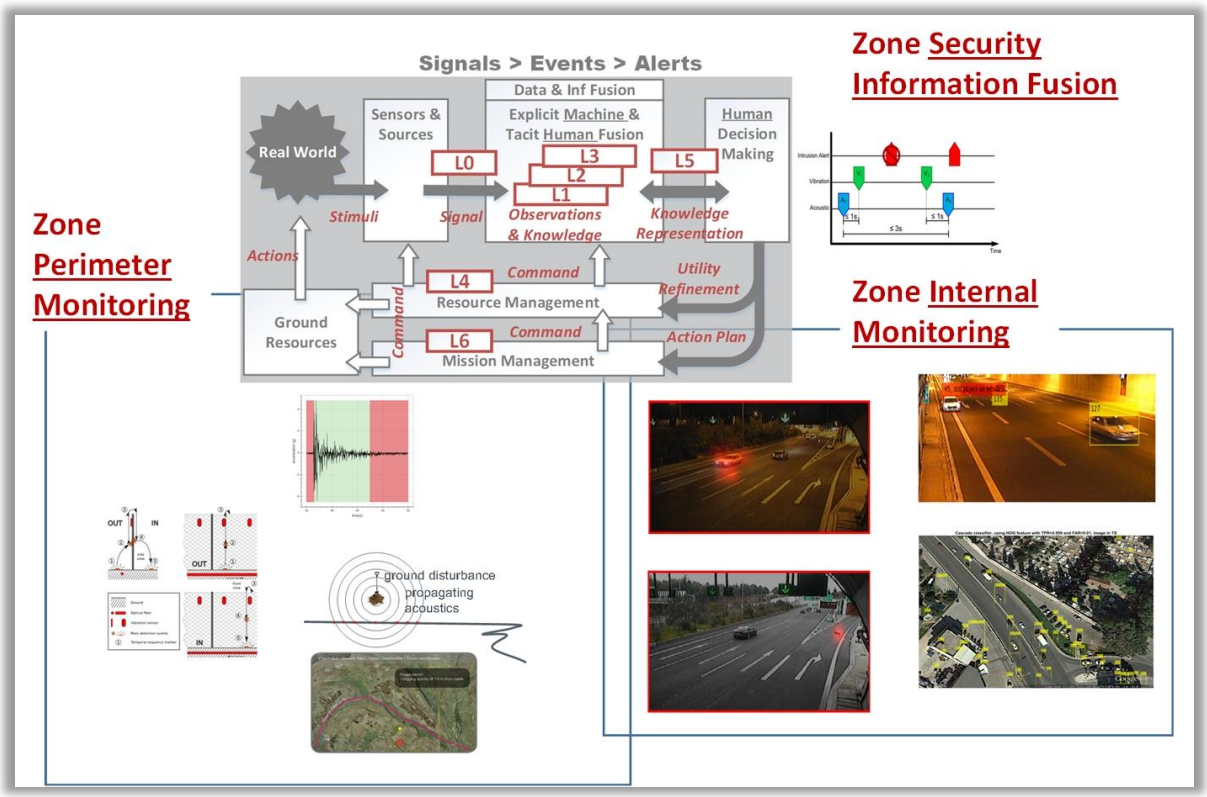


Figure 11. The SDAIM implements the JDL multi-level data and information fusion model for holistic Widezone surveillance, detection of critical events and generation of security related alerts.

The SDAIM enables the intelligent data and information processing and reasoning from heterogeneous observation data sources. These are generated from a high variety of sensor observation platforms. Currently, the SDAIM considers observation data sources from 3D accelerometers, underground acoustic sensors, CCTV cameras, thermal and hyperspectral cameras, radars and cameras mounted on UAVs. This is achieved by undertaking sources', data and information modelling through the creation of metadata, in order to automate the system and data

processing configurations and the information management. The aim is to achieve sensors "plug-and-play" and the automatic on-demand access to fusion processes, their configuration and processing. We achieve this by employing OCC SWE SensorML inspired metadata exchange sensor plug-and-play protocol and Docker based algorithms virtualization and provisioning middleware. The Docker based middleware (including Docker Compose, Docker Swarm and custom built components), termed Elastic Fusion Controller, also provides for automated SDAIM scaling, fault tolerance and runtime diagnostics and monitoring. The virtualized algorithms deployed on demand as Docker containers communicate with each other, depending on their place in the multilevel fusion process, via a high performance communication middleware based on the RabbitMQ broker. RabbitMQ implements an extremely rich functional set to do with the ability to dynamically accept new message sources, to configure the message exchange patterns and the quality-of-service of message exchanges, and to rout messages depending on metadata. RabbitMQ also supports broker federation and implements an advanced security model based on sandboxing of users in virtual hosts, fine grain roles specification, and versatile user authentication and authorization models. For a high level components view of the SDAIM please see figure below.

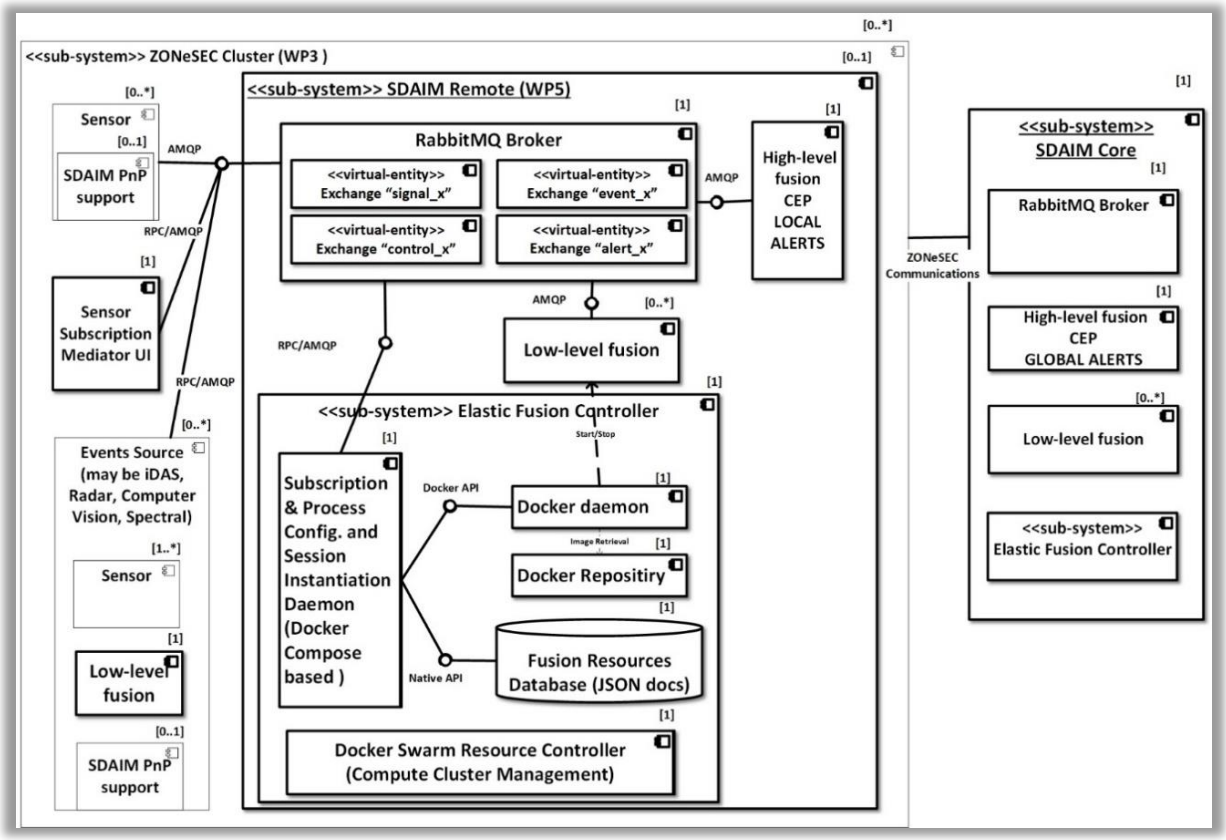


Figure 12. SDAIM high-level components UML diagram.

In terms of detection and alerts generation functionality, currently the SDAIM provides the following capabilities:

1. **High intensity vibration events detection from acceleration sensors on perimeter fences;**

The algorithm used for event detection is based on Median Absolute Deviation (MAD) and Confidence Interval method. The algorithm detects onset and end of a high intensity fence vibration event (see Figure 13 below). A feature based threshold is used to prevent FP due to noise. The algorithm is highly accurate with minimal computational resources required.

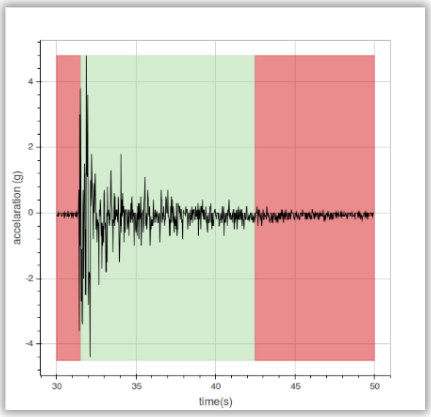


Figure 13. Sample high intensity fence vibration events detection.

2. Unimodal multi-sensor fusion and motion events detection in iDAS ground acoustics;

In this algorithm, classification is performed on the sequence of spectrograms, derived from the acoustic data and acoustic events are identified and classified by a Deep Convolutional Neural Network, which assigns percentage scores corresponding to predetermined event classes. There are 3 distinct types of events (walking, moving vehicle and digging). The classification scheme is trained offline after a pre-processing step. After classification, an adaptive thresholding scheme provides the final decision on the class of the detected event. The figure below depicts the corresponding spectrograms for a walking and a digging detection.

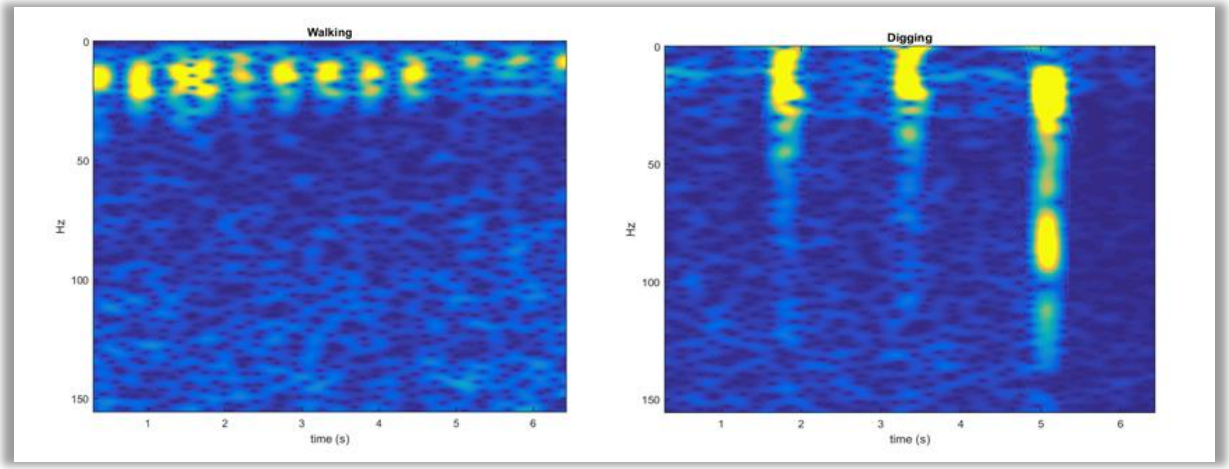


Figure 14. Spectrograms depicting a walking (left) and digging (right) detections.

3. Unusual flow and stationary vehicles events detection from CCTV cameras observing roads;

Two algorithms were developed for use depending on the availability of training data. For cases with sufficient amount and quality of training data, the algorithm used is based on Robust Real-Time Unusual Event Detection Using Multiple Fixed-Location Monitors where the image frame is tilled with local monitors each modelling the usual flows which are expected in the neighbourhood of that monitor. Given two consecutive frames, optical flow (a measure of motion between two images) is calculated and used to calculate the motion at each monitor. The detected motion is evaluated against the learned model at each monitor and a decision is made as to the usualness of the detected motion. Usualness in the video is detected using a voting scheme over spatial and temporal windows that accumulate and fuse the low-level alerts from the local monitors. The operation of this algorithm is depicted on Figure 15.

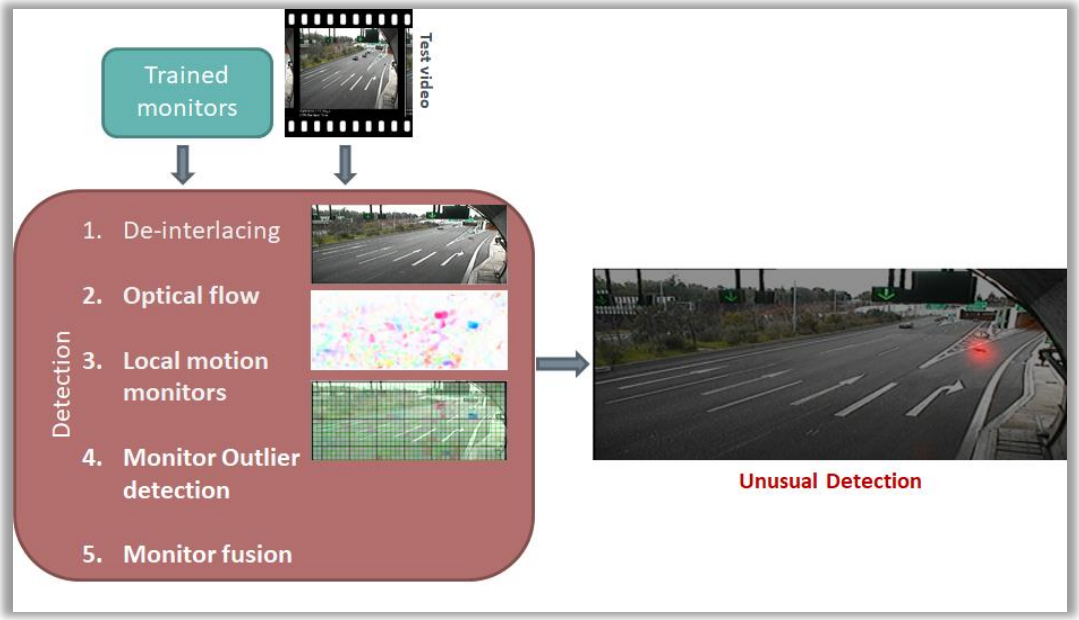


Figure 15. Unusual Traffic flow detection algorithm depiction.

In the cases where insufficient training data is available we use algorithm based on two background subtraction methods. One is the temporal variance-based method introduced by Joo and Zheng and the other is the median background method. These two methods are used to combine the robustness of temporal variance with the capability of median model to detect objects – stationary vehicles in the current case. Further, a blob tracking approach is used which matches the detected blobs based on their size and motion. Here a Kalman filter is used to predict the next location of the object based on its previous motion. Example output of this algorithm is depicted on Figure 16.

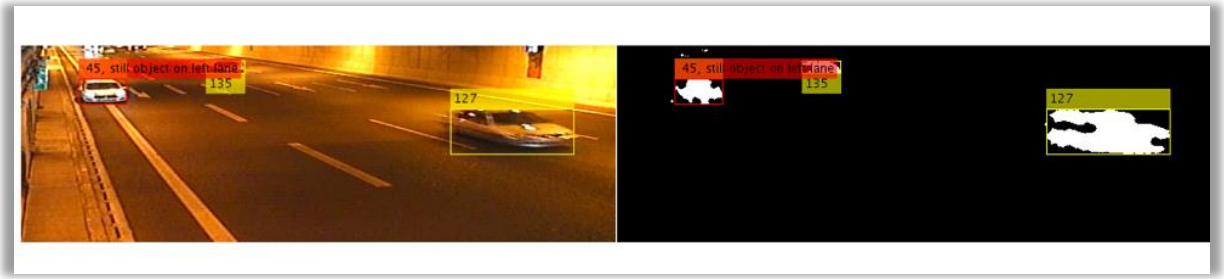


Figure 16. Example output of the Stationary Car detection algorithm.

4. Illicit equipment manipulation events detection from CCTV cameras, observing inner building's spaces and open work-grounds;

In this algorithm, a trained convolutional neural network is used to detect different parts of the body such as neck, shoulders, elbows, wrists, knees, etc.. Another convolution neural network is responsible for associating each part of the body detected by the first one, thus forming the skeleton of all the people who appear in the image. Once each part of the body has been detected

and a statistically viable association has been achieved, the 2D coordinates of each part are obtained. Knowing the intrinsic and extrinsic characteristics of the video camera we can obtain the 3D coordinates of each part of the body. By means of examples of the actions that we want to identify, a classification algorithm (SVN Support Vector Machine) is trained, which is subsequently responsible for identifying the action.

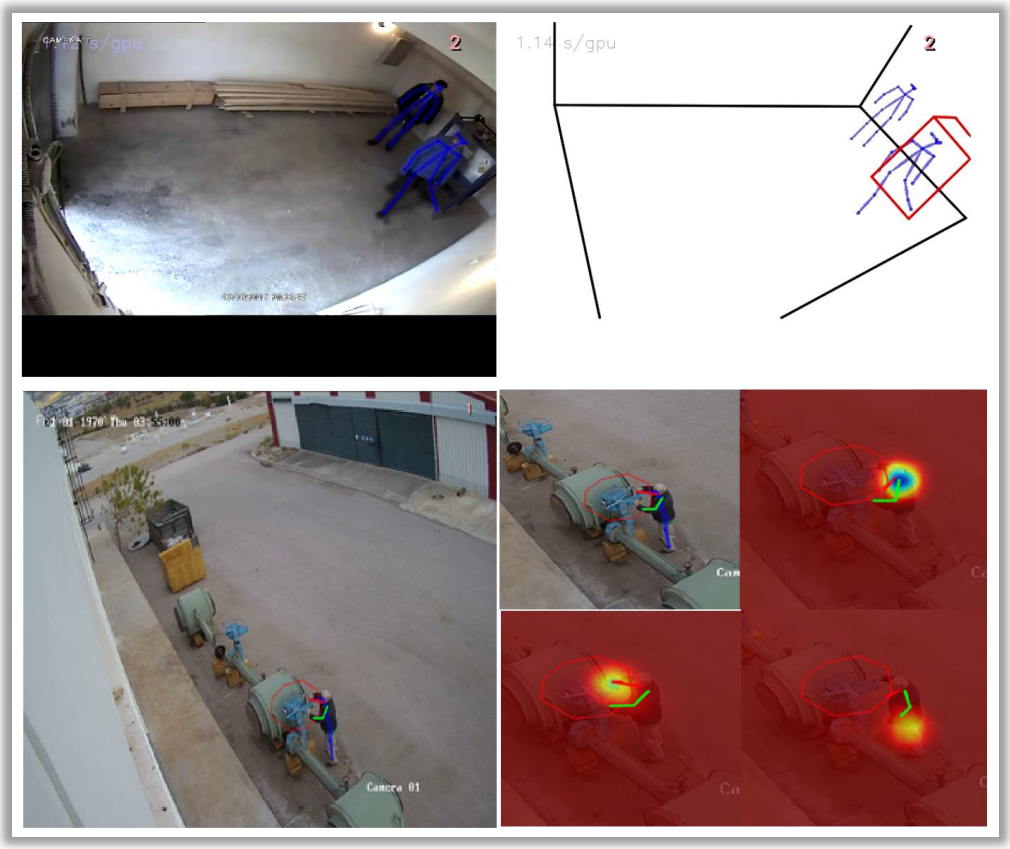


Figure 17. Illicit equipment manipulation detection algorithm output depiction: container tampering (top) & valve manipulation (bottom).

5. Approach and trespassing events detection by thermal and spectral cameras observing open spaces, by object detection, tracking and registration, in different environmental conditions;

Image streams from four different sensors (SWIR, Thermal, Hyperspectral, UV) are fused and processed based on learning frameworks. A background subtraction module utilies mixtures of Gaussians to dynamically recalculate the background in a near-real time fashion. For the calculation of motion flows, Farneback's Dense Motion Flow algorithm is utilised. Then, the detected people are projected on a local coordinate system. The final detected targets are extracted after their spectral verification and recognition based on data association learning modules that exploit their temporal spectral signatures, from all available datasets. For each iteration of the online algorithm, a decision system provides alerts to the system, if the proximity, velocity and direction of the detected people are above certain thresholds. Figure below depicts the operation of this algorithm.

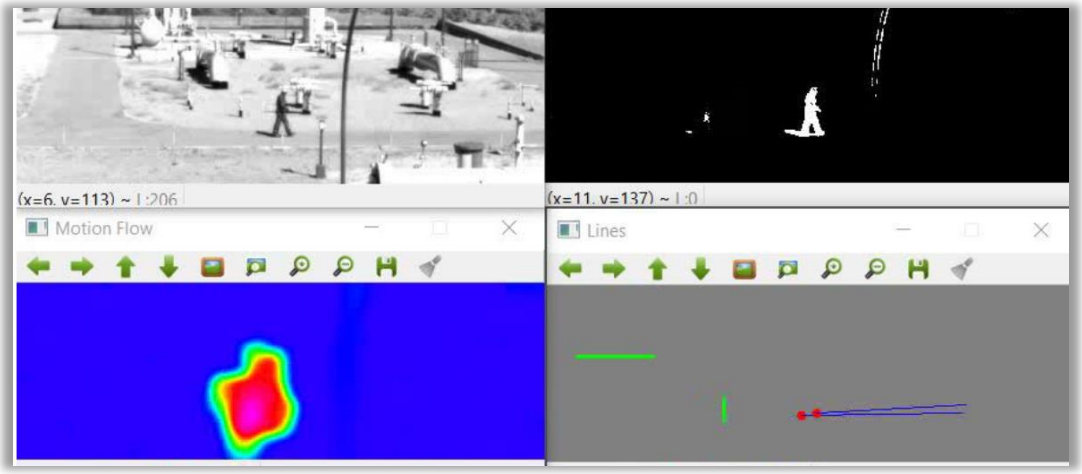


Figure 18. Approach and trespassing events detection from spectral cameras data - algorithm operation depiction.

6. Approach and trespassing events detection by MIMO radar observing open spaces, by object detection and tracking, in different environmental conditions;

Object detection and tracking is performed on data from a MIMO radar which is actively being developed by Airbus. A pipeline of processing steps is used to extract moving objects, track them and estimate their speed. This pipeline involves Background subtraction, Gabor filtering, size and ratio restricted blob tracking and Kalman filtering.

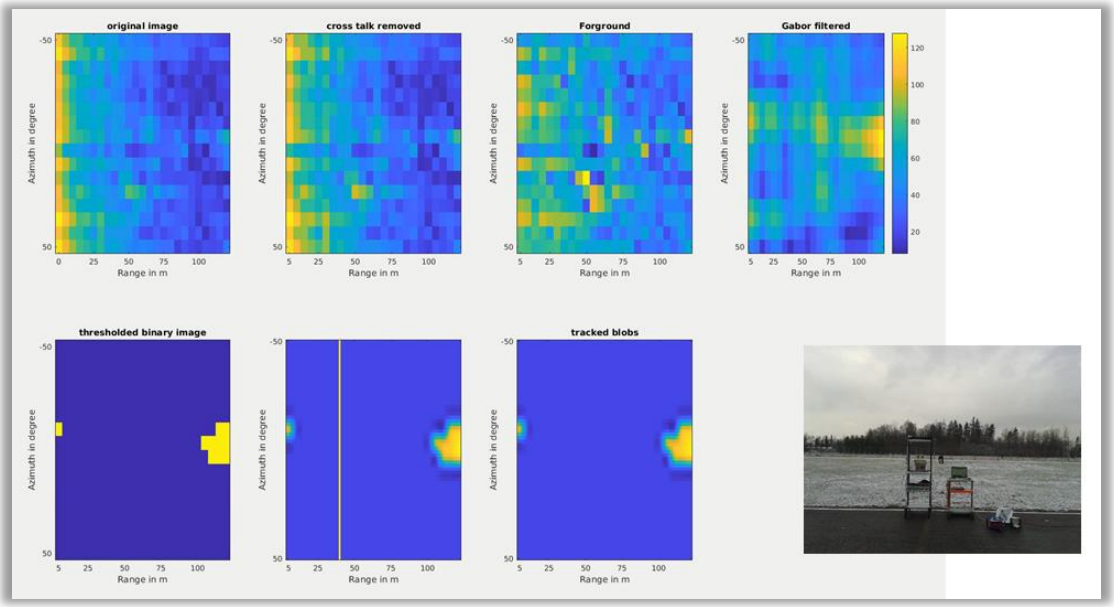


Figure 19. MIMO radar approach and trespassing events detection algorithm pipeline.

7. Detection and localisation of cars and humans from UAV mounted visible spectrum cameras;

This algorithm detects and classifies objects in aerial images and estimates their geo-position. To achieve this, a convolutional neuronal network has been trained, with special emphasis on the use of this type of images for training. A module for decoding the metadata acquired by the UAV in KLV format has also been developed. The neural network is able to identify objects of the following classes: cars, people, trucks or motorcycles. The algorithm used combines a convolutional neuronal network architecture of the MobileNet type and the Single Shot Detectors (SSDs) detection methodology. A Caffe implementation of MobileNet-SSD detection network, with pre-trained weights is used as a pre-trained network. This network is refined by training it with several public datasets such as: KITTY, DLR 3K Munich Vehicle Aerial Image Dataset, and images acquired in the test flights using the WP4 UAVs. The detection of objects by the algorithm is depicted in figure belowFigure 20.

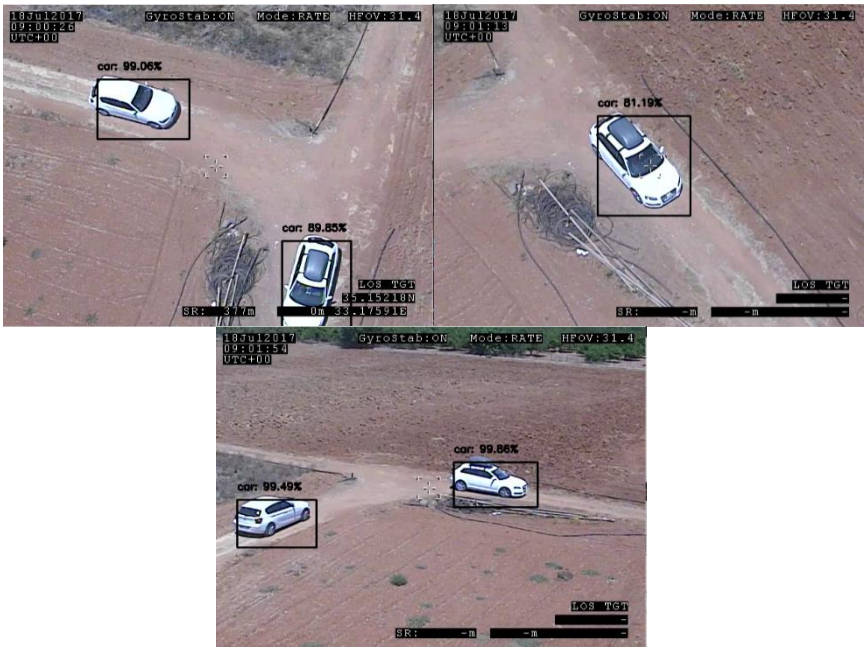


Figure 20. Detection of objects in areal images, labeled with their class ('Car') and classification probability.

8. High Level Information Fusion and Alerts Generation through Event Stream Processing and Situation Criticality Assessment.

The SDAIM implements a rich set of generated alerts (see the paragraph below) by a complex event processor (CEP) in the high level information fusion layer. Based on inference and semantic pattern matching the CEP transforms the sensors' detections into alerts that make sense to the security operative. Taxonomy of the generated alerts is depicted on Figure 21.

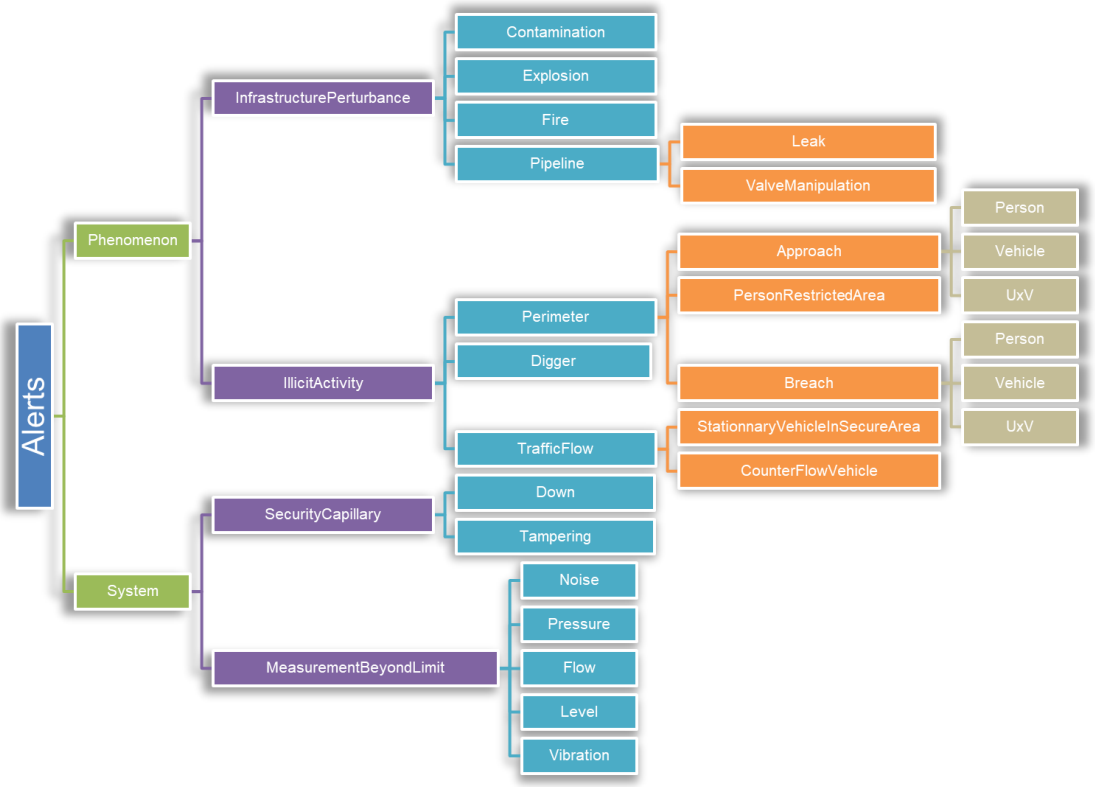


Figure 21. Taxonomy of the alerts generated by the Event Stream Processing.

To aid improved operator awareness, the CEP features automated generation of documents that explain the computation of the particular alerts. These documents are generated directly from the ruleset used by the CEP.

In addition to the core CEP functionality a framework for assigning criticality levels to alerts is implemented – see Figure 22. The criticality of each alert is estimated based on prior assessment of the impact level of particular illicit behaviour.

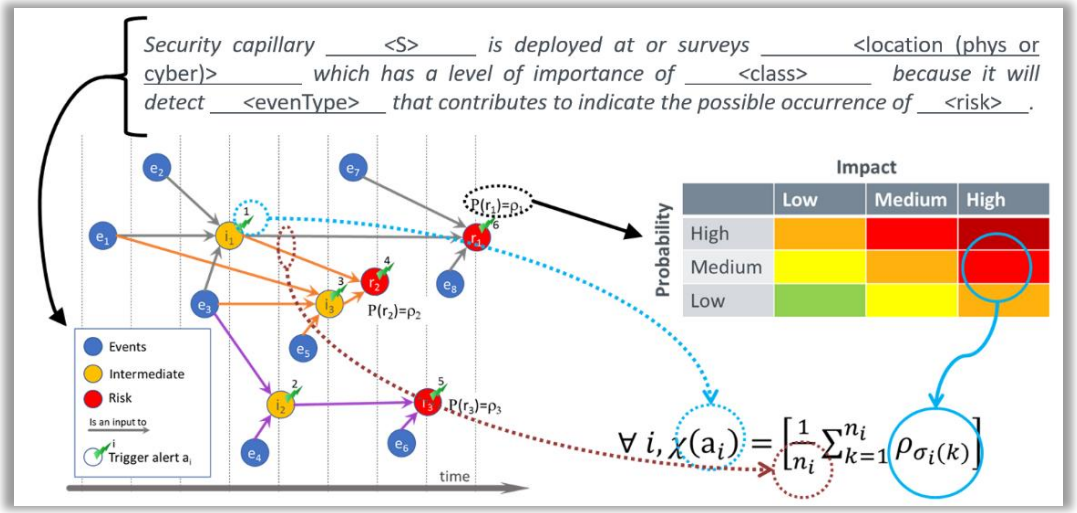


Figure 22. Schematic outline of the Impact/Criticality assessment framework for alerts.

The SDAIM was successfully integrated deployed and demonstrated as part of the full ZONeSEC system during a number of on-site integration pilots and also full scale pilots involving external end-users. At its final version, in terms of high-level end-user observable outcomes (alerts), the SDAIM provided the following (actionable) information for improved situation awareness and aiding the decision making of the security operatives:

- Generated Alerts for:
    1. Perimeter Approach (Person/Vehicle)
    2. Perimeter Breach (Person/Vehicle)
    3. Person in Restricted Area
    4. Stationary Vehicle in Secure Area
    5. Counter-flowing Vehicle
    6. Pipeline Leak
    7. Pipeline Valve Manipulation
    8. Digger Detection
    9. Contamination
    10. Fire
    11. Explosion
    12. Security Capillary Down
    13. Security Capillary Tampering
    14. Measurement Exceeding Limit (for Noise, Pressure, Flow, Level, Vibration)
- Estimated and assigned Levels of Criticality to the generated alerts (as per base model of risks and impacts on a particular critical infrastructure)

3.1.4.1 Identified innovations:

The SDAIM (prototype) sub-system, designed, delivered and piloted in the ZONeSEC project is, according to our knowledge, the only system addressing in a holistic way the needs for multi-modal multi-sensor data and information fusion for improved situation awareness for the Widezone's security operatives. For the security of Widezones, it uniquely combines state-of-the-art Big Data technologies, data processing techniques, machine learning algorithms and information fusion frameworks. The SDAIM functions as a geo-distributed, federated, secure, soft-real-time, scalable, fault tolerant sub-system with sensor and sources plug-and-play capabilities. The fusion algorithms use state-of-the art machine learning approaches specifically applied to the ZONeSEC target domain of Widezone surveillance and security. The selection and implementation of the individual algorithms is based on the specific requirements of the target domain including soft-real-time operation, available computational capacities, optimal true-positive vs. false-positive rates, ease of training data acquisition, amongst other. A high level information fusion layer abstracts the numerous low-level critical events detections by aggregating them into illicit behavior detections, estimates the impact of the detected illicit behavior and generates alerts with associated criticality level. In this way the cognitive burden placed on the human security operative is reduced, while if needed, the individual low-level event detections can still be exposed to the security operative. In our view the SDAIM as a (prototype) system is beyond the state-of-the-art in the Widezone security domain (see the full spectrum of SDAIM capabilities in the discussion above).

3.1.5 Interoperable communications fabric and uniform data exchanges (*Work Package 6*)

Critical infrastructures that span across large areas (wide zones) phase many challenges related to data distribution and cybersecurity. The Uniform Communication Fabric, developed in the content of work package 6, addresses these challenges and ensures a) the fast, reliable and secure delivery of data captured by the various sensorial systems to the data aggregation/processing modules, b) the timely distribution of configuration tasks to the sensorial systems and aggregation nodes, c) the deployment of the most effective networking technologies, taking into account the specific characteristics of each wide zone section, and c) the protection against various cybersecurity attacks. The Uniform Communication Fabric comprises of a set of modules that address the aforementioned challenges: the data adaptation module, the communication module and cybersecurity module.

The data adaptation module is responsible for collecting the heterogeneous data generated by the sensorial systems (ZONeSEC security capillaries, end-user's legacy systems and COTS sensors), transforming them to a uniform data format and forwarding them to the communication module. It also facilitates the integration with the sensorial systems and legacy systems, according to the interface (-s) each system supports (e.g. web services, web sockets, direct connection to databases or file servers etc.). In respect to the uniform data representation, observations generated by the sensorial systems are transformed to the well-established OGC® Observation & Measurement standard, while the OpenGIS® Sensor Planning Service Interface Standard (SPS) is utilized for representing configuration tasks (e.g. UAV flying instructions). As a result of the aforementioned approach a data abstraction layer is created.

The implementation of the communication module is based on the Data Distribution Service (DDS™), a middleware protocol and API standard for data-centric connectivity from the Object Management Group® (OMG®). By following the data centricity paradigm, the communication module understands what data it stores and controls how to share that data, which ensures that the ever-increasing amounts of sensorial data are provided to the users reliably, securely and in real-time, qualities that are necessary for mission-critical applications. The communication module basic characteristics are: a) it follows the publish-subscribe approach, which efficiently connects information producers to matching consumers, b) it is distributed, allowing the system to be scalable, avoiding bottlenecks at central nodes and providing multiple levels of redundancy, c) it has a configurable cryptographic mechanism and an authentication scheme, that safeguards the system against threats such as unauthorized subscription, unauthorized publication, tampering and replay and unauthorized data access.

ZONeSEC also provides a monitoring cyber-security solution based on multi-agents. The cyber-security agents are the components in charge of the cyber defense, by monitoring the internal and incoming traffic and generating cyber-domain alerts, which complement the physical-domain ones. Each cyber-security agent integrates a set of cyber-sensors, a cyber-sentinel agent and a cyber-monitor. The cyber-sensors analyze the traffic and generate events related to intrusion detection and can be: a) Network Intrusion Detection System (NIDS) that analyze the traffic and detect known attack patterns (e.g. brute force login attempts, denial of service attempts, web attacks, etc.), suspicious behaviors and malware signatures, b) Deep-Flow Inspection (DFI) Anomaly Detectors that can detect potential intrusions by running machine learning algorithms trained using the normal network traffic, c) Honeypots that can identify potential intruders or attackers. The cyber-sentinel agent is responsible for collecting, normalizing and transferring the data generated by cyber-sensors to a cyber-monitor. The cyber-monitor filters, aggregates and correlates the events generated by the cyber-sentinel sensors, triggers cyber-alarms and publish them using the communication module.

The set of modules consisting the ZONeSEC Uniform Communication Fabric enables the seamless integration of novel sensors and sensor systems installed on a widezone infrastructure, as well as the interconnection with existing legacy systems, in a scalable, distributed, secure, uniform, efficient and reliable way.

3.1.5.1 Identified innovations:

A competitive advantage of the ZONeSEC communication gateway platform is the alleviation of the overwhelming resource heterogeneity which governs the ZONeSEC systems' sensors, actuator and devices. The communication gateway adapters' primary aim is, thus, exactly to drift away from proprietary protocols and data formats with respect to field devices and publish the resources in a uniform, harmonized format so that they may be integrated with minimal effort and time to any decision support system following the communication gateway data model.

The data model of the communication gateway uses of widely adopted standards in order to enable real-time communication in an interoperable and seamless way. The adaptation and harmonization of these standards have led to the definition and development of a semantic interoperability layer. The disseminated information has been semantically annotated, enabling fast deployment, extensibility and easy adaptation.

3.1.6 Simulation framework for prototyping and improving situational awareness (*Work Package* 7)

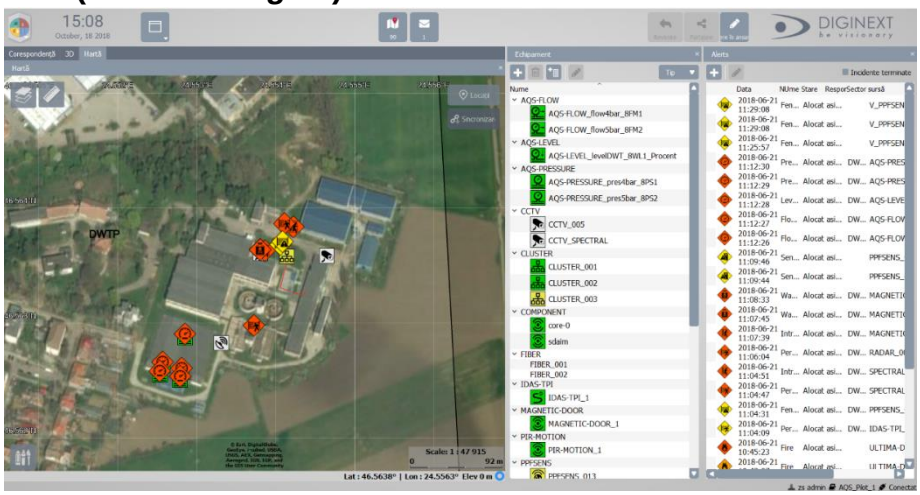


Figure 23: Screenshot of COP in Romanian Use case

This Work package had three primary goals. The first objective was to provide the operator with an interactive **Common Operational Picture** (COP) system, entailing a clear, synchronized and interactive view (with 2D maps and 3D view of geospatial data) of a controlled area enriched with alerts and information transmitted from sensors. The second objective was to provide the ZONeSEC system with a simulation platform in order to host simulated sensors than can replace any signal (including video) and can provide the ZONeSEC platform with the same input as the real sensors. The last objective was to provide an authoring tool, the scenario editor (SE), with a 3D geographical environment and representation of the Critical Infrastructure (CI) to help the operator configure and run the simulation

by defining complex situations (that are otherwise difficult to produce in an operational context), or by replacing missing subsystems with virtual counterparts (see figures below).

Indeed, there are major limitations in reproducing threats and dangerous situations over a Widezone, such as the cost of deploying temporary systems along kilometres of infrastructure (for instance along highway or gas pipeline) or situations breaking health and safety requirements (like a vehicle driving counter flow). Therefore, as an alternative solution, Within this work package, we researched and developed simulation techniques as an answer to the missing information required to enable large scale validation of the system and to provide the means to conduct training sessions.

3.1.6.1 Identified innovations:

Within this work package, we succeeded in delivering these 3 components. Derived from the user and system requirements, the COP has become an intuitive system to navigate between different 3D Infrastructure mock-ups deployed over a Widezone; gathered data from dynamic sources (deployed sensors and legacy data, raised alerts, UAV positions…) are displayed in a legible way in real-time. In addition, command by distance have been developed in order to facilitate the operations such as configuring an UAV mission or disabling systems for schedule maintenance. All these features provide the operator with an overall multi-site situational awareness and complete picture of the ongoing infrastructure situation.

Figure 24: Screenshot of 3D representation of COP in Romanian Use case

With the help of the Simulation modules, WP7 created dynamic scenarios intuitively and provided the ability to include simulation data from any type of sub-systems to feed the platform and train the algorithms / gateways during development. It also gave the possibility to create richer training sessions with more immersive data displayed into the COP.

The main challenges faced during the development of simulation modules were twofold:

- To create a system that requires non-trivial computer tasks to be performed, tailored for non-computer scientist. WP7

Figure 25: Simulation Tool with a path

had to abstract simulation configuration and provide interactive means to deploy multiple virtual systems at specific geographical position or along critical infrastructures.

- To provide a generic simulation framework to store and replay ZONeSEC sub-systems data in a same fashion as real ones.

3.1.7 ZONeSEC Framework Design, Development and Integration *(Work Package 8)*

ZONeSEC Framework Design, Development and Integration work package's objectives were dual. On one hand it had the responsibility of describing, creating and implementing the architecture of the entire system. This architectural work had also the natural extension of coordination and taking the leadership of the integration of all the system components during the phases of i) construction of the code and, ii) during the integration and testing phases prior to the Pilots and OIPs (there were 7 of them).

On the other hand, this WP was responsible of the design and implementation of the central data hub and the microservices associated to it. These elements acted as the central hub and common service elements for the entire framework.

3.1.7.1 Identified innovations:

Finally, the platform was adapted and oriented, using the new breakthroughs to make it gather and process huge amounts of real-time data. The implementation in each of the 3 venues (Attikes diadromes, Aquaserv and Acciona) had many specific differences that required customized approaches, which were handled in a case-by-case basis. The ZONESEC solution became a platform that can manage the surveillance of different critical infrastructures, and the same components can be applied to other products and services for further exploitation, in any domain.

Integration was a real success due to the use of:

- A proved communication layer: DDS
- A common data model based on SOS standard
- A modular architecture with the use of micro-services

3.1.8 Pilot Demonstrations and System Validation Campaigns *(Work Package 9)*

In the ZONeSEC project, a total of **seven demonstration activities** were scheduled: four On-site Integration Pilots (hosted by each end-user at their premises) and three pilot demonstrations (hosted by three of the project's four end-users). The system was developed partly through integration tests performed during the four **On-Site Integration Pilots** (OIPs). In these pre-pilot exercises, partners worked together to test the developed ZONeSEC components, integrate the available technologies, acquire real-life data, and identify eventual bottlenecks as well as possibilities for improvement. The OIPs were unique opportunities to gather feedback from end-users on the performance of the system in its current development stage, but also on the planned technical work. They also come after an intense period of technical development.

After the OIPs, the system was demonstrated to end-users through a series of three **pilot demonstrations** held in Spain, Romania, and Greece in the last year of the project. Although the three pilot demonstrations shared the same main objective (to demonstrate the system to stakeholders and validate it with end-users), the focus of the pilots differed depending on the critical infrastructure that the host end-user operated and the associated threats. This translates into different functionalities and detection capabilities. Both OIPs´ and pilot demonstrations´ outcomes facilitated the delivery of an optimal product that responds to the real needs of critical infrastructure operators.

The schedule followed by the project in terms of the demonstration campaign can be seen in the table below.

Table 1: ZONeSEC demonstration Campaigns

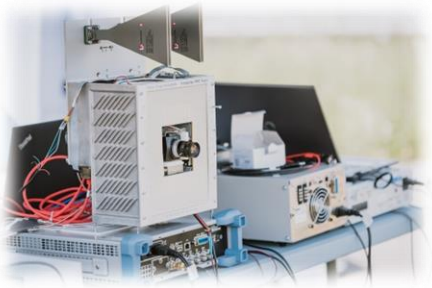
Type of activity	Date (project month)	End-user host (type of infrastructure)	Location
On-site integration pilot	November 2015 (M12)	Acciona (highway operator)	Torja, Spain
On-site integration pilot	December 2016 (M25)	Attikes Diadromes (highway operator)	Athens, Greece
On-site integration pilot	June 2017 (M31)	Aquaserv (public water system operator)	Târgu Mures, Romania
On-site integration pilot	December 2017 (M37)	DESFA (natural gas transmission system operator)	Athens, Greece
Pilot demonstration	March 2018 (M40)	Acciona (highway operator)	Torja, Spain
Pilot demonstration	June 2018 (M43)	Aquaserv (public water system operator)	Târgu Mures, Romania
Pilot demonstration	October 2018 (M47)	Attikes Diadromes (highway operator)	Athens, Greece

A **tailor-made scenario** was developed for each OIP, according to the results of the risk assessment of the pilot locations and the security concerns of the infrastructure operators. For the pilot demonstrations, given that they were hosted by the same end-users as the OIPs, the scenarios were updated in light of the technology readiness level and a more advanced understanding of the system's capabilities. Improvements emerging from testing activities (OIPs) were used to refine the scenarios that had been employed in the OIPs.

Overall, the following **tools/technologies** were demonstrated to the end-users attending the seven activities:

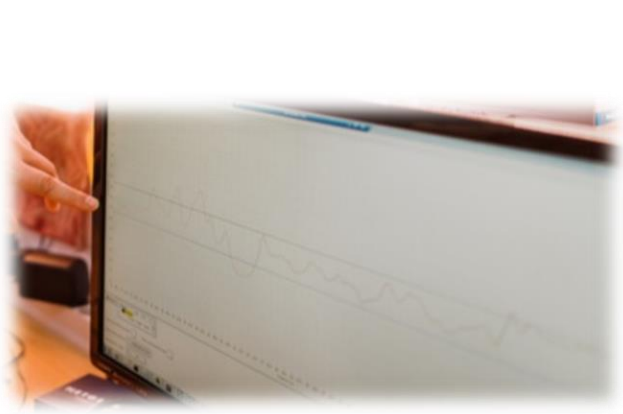
- Sensors:
  - Ground-based: novel (e.g. spectral imaging system, acceleration sensors, acoustic and temperature sensors, video analytics, MIMO-radar), as well as legacy systems (e.g. CCTV);
  - Airborne: a mini-UAV sub-system that allows for rapid, semi-automatic deployment of UAVs (with different detection capabilities) to remote areas;

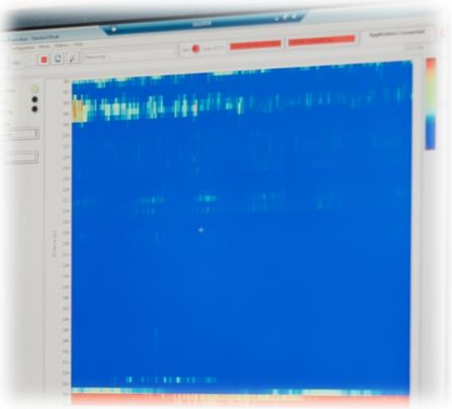
MIMO-radar (EADS, THALES, TUD)



Acceleration sensors (TEK)

ULTIMA and iDAS (output)





UAV sub-system and COP

Spectral system

Figure 26: ZONeSEC sensors

- Surveillance, Detection and Alerts Information Management (SDAIM), which analyses data and automatically fuses the events detected so as to send meaningful alerts to the Control Centre.
- Common Operational Picture (COP), the sole user interface that displays data from other components, including alerts once illicit activities are detected;
- EU-WSRT, a software tool allowing critical infrastructure operators to assess the risks of their widezone, and issuing recommendations for improving surveillance.

The ZONeSEC system was built primarily to detect, classify, localize and alert on illicit activities directed at the infrastructure's assets, thus to improve situational awareness of extensive areas. Overall, the **detection types** demonstrated to end-users include:

- system manipulation (sensor tampering);
- sensor unavailability (sensor down);
- operation/process disturbance (fire, vehicle driving against traffic, stationary vehicle, legacy systems' parameters beyond limits [integration of SCADA]);
- cyber activity;
- approach to physical or virtual perimeters;
- intrusion into physical or virtual perimeters;
- asset manipulation (equipment manipulation [pipeline valves]; digging; water contamination)

The goal of the demonstration campaign was primarily to test and improve the capabilities of the ZONeSEC system. Four methods were used to collect feedback from end-users at the pilot activities: pilot/OIP handbook, carousel stations, evaluation forms and open discussion.

The **pilot handbook** served two purposes: informing end-users on the proceedings of the pilot activity and validation. In terms of validation, it was designed to provide end-users with a platform for individually evaluating the multiple functionalities and overall performance of the ZONeSEC system, and easily registering that feedback. Complementary to the quick training session on the user interface (the COP), the system's actual performance, the carousel stations and the dedicated Q&A session following the demonstration, the handbook provided end-users with sufficient means for a fair assessment of the ZONeSEC system. To that end, it included sections that asked for end-users" written input: the expected performance of the system (in a checklist format), the comments section at the end of each demonstration case, and the evaluation form. End-users were required to return the filled out handbook to the pilot coordinator at the end of the pilot.

Figure 27: Pilot handbook

The **carousel stations** were themed discussions on the different ZONeSEC components. End-users attending the pilot activities were invited to break into small groups and attend each of the carousel stations. Carousel stations were run by technical partners, who presented their developments multiple times but to different audiences. Carousel stations ran simultaneously (in sessions of 20-30 minutes) as many times as to equal the number of groups formed. The aim was to offer participants the opportunity to find out more about the system, thus fostering the acquisition of feedback from end-users and project partners. Whenever carousel stations could not be run simultaneously due to the limited number of participants (the case of the OIPs, where no external guests were invited), end-users went on-site, where the technical partners had installed their equipment, and discussed in turn with each of them.

Figure 28: Critical infrastructure professionals attending the carousel stations at the ZONeSEC final pilot

The **evaluation forms** were more detailed for the first pilot activities (one form per component). Towards the end of the project, they were condensed into one evaluation form that focused on the overall system.

At the end of each pilot activity, the consortium engaged in an **open discussion** with the end-users, reflecting on the technical performance of the system and organisational aspects. The aim of these discussions was to reach agreement on the issues faced, the solutions to be adopted and how they will be implemented. In addition, end-users had the chance to provide their point of view on ZONeSEC developments and how they could fit their current infrastructure, while indicating either for the whole platform or for specific subsystems the level of importance of those systems in terms of further strengthening their security measures.

3.1.8.1 *Lessons learnt from field test activities*:

First On-Site Integration Pilot (OIP) at ACCIONA's Highway: The OIP at Acciona was a small-scale test initiated by the technical partners, as a result of the need to begin integration work as soon as possible. Not foreseen in the original plan, this activity amounted to a proof-of-concept for which

no official evaluation had been planned and carried out. However, the invaluable lesson of this event was that the pilot activities should not be left for the last year of the project (as originally planned), but that similar integration tests should be carried out at regular intervals until the system can be demonstrated to an interested audience (final project year). With the support of the project's dedicated end-users, who have constantly evaluated the system based on their needs and experience, the capabilities of the ZONeSEC system were improved greatly through the four integration tests.

Second On-Site Integration Pilot (OIP) at ATTIKES Diadromes Highway: The second OIP at the Greek tollway operated by Attikes Diadromes was instrumental in realizing the ZONeSEC system's potential of addressing the main challenges widezone operators deal with. By identifying (and solving) a lack of understanding amongst end-users and technical partners of how the detection technologies work and how they communicate with each other, the consortium was able to study the complementarity of the different ZONeSEC technologies and exploit it to make the system adaptable to different user needs and locations.

Third On-Site Integration Pilot (OIP) at AQUASERV water treatment plant: Aquaserv, a water treatment plant in Romania, hosted the third integration test of ZONeSEC. Although in terms of functionality no major challenges ensued, this pilot event constituted a milestone in the way alerts were conceptualized at the system level. The multiple alerts received on the COP for individual detections coming from different sensors were positive evaluation results, yet not all were considered relevant for the Control Room staff (certainly not the duplication of alerts coming from individual detection events and from the fusion thereof). Renewed effort was dedicated after this pilot activity to better make use of the results of the risk assessment as well as information about the detection capabilities of the ZONeSEC sensors in the way alerts are created (and brought to the attention of the Control Room staff).

Fourth On-Site Integration Pilot (OIP) at DESFA natural Gas distribution premises: The final on-site integration event took place near Athens, at one of the valve stations of DESFA (the Greek national natural gas transmission system). The consortium's good progress in terms of demonstrating improved functionalities was challenged by network issues. A crucial lesson identified with this testing opportunity was that more attention needed to be paid to network arrangements. The solution conceived in the aftermath of the event included the decisions to create a dedicated subnet for ZONeSEC (separated from the end-users' other subnets), to have a dedicated IT specialist to support the ZONeSEC technical team, and the team to arrive at the pilot site the week before the event.

First pilot demonstration at ACCIONA highway:



The first pilot demonstration of the ZONeSEC system (hosted by Acciona, the highway operator in Spain) refocused the consortium's attention on the network. Even though most of the tests executed on-site rendered positive results during the pilot week, the system's performance was hampered on the day of the pilot by the network quality. It became clear that the measures taken after the DESFA OIP (as a solution to the local network problem) proved insufficient. The consortium concluded that, in fact, more effort to enable proper local network conditions for system operation was necessary to

be invested from both sides (the ZONeSEC technical team and the end-user hosting the pilot). Two new roles were formally created and adopted into the pilot preparation process:

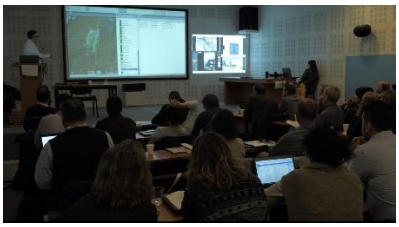
- a system administrator responsible for producing a clear network map (informed by the network requirements of all system components) and being the point of contact between the ZONeSEC technical team and the local network expert;
- a local network expert (of the end-user hosting the pilot event) who had to be appropriately equipped to diagnose and resolve potential network issues.

Second pilot demonstration at AQUASERV water treatment plant:



The second pilot took the consortium back to the water treatment plant in Romania (Aquaserv). The end-users attending the event characterized the system as a useful and efficient tool for wide-zone security, having the ability to combine many complex surveillance sensors and systems (both new and legacy) and to present their operations in a simple, intuitive, appealing, user-friendly and mobile interface. The project's end-users noted the improved integration, stability, and accuracy since the last pilot and appreciated that the main issue affecting the previous pilot was resolved.

Third final demonstration at ATTIKES DIADROMES Highway:


Attikes Diadromes, the Greek toll way operator, hosted the final demonstration of the project. ZONeSEC left an overall positive impression on the participant end-users. They described it as a system-of-systems key to the surveillance of wide zones, with great potential if customized to the needs of each critical infrastructure sector. End-users recognized the system's ability to enhance situational awareness and provide a comprehensive overview of the physical security system to the operator of a widezone. It encompasses the necessary tools to understand safety/security issues, identify existing gaps and foster improvement.

End-users shared many compliments with regard to the outcome of the ZONeSEC project. The different technologies (sensing modalities) are interesting in so far as they respond to particular challenges, which vary with the type of critical infrastructure (e.g. iDAS and ULTIMA are appealing to the water and oil sector for leak detection, but less to highway operators). Notwithstanding, end-users highlighted that the ability of the system to integrate different new and legacy systems is what makes it a product that should be marketed. One of the biggest achievements of the ZONeSEC project, announced during the plenary discussion after the final pilot demonstration, is that one of the project's end-users is willing to buy the ZONeSEC system.

3.1.9 Acceptance of Surveillance, Adaptive Ethics and Privacy model *(Work Package 10)*

During the ZONeSEC project, several activities were performed in terms of research on the acceptance and potential adaptability of new technologies to ethical concerns and privacy and data protection issues. The activities focused on:

a. Analysis of ethical issues and privacy requirements;
b. Analysis of perception and acceptance of monitoring/control technologies;
c. Development of an Internal self-assessment tool for project partners;
d. Development of a Self-assessment tool for operators;
e. Identification of ethical and legal issues concerning protection of citizen's rights in the EU legal regulation of privacy.

a) Ethical issues 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.

The **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 its development. The use of new technologies had to be accompanied by activities that implied, for willing volunteers (i.e. no one has to be forced) to sign Informed Consent Forms or authorization forms for the use of private information for dissemination purposes. Citizens' personal information was protected, and physical, social and psychological well-being was ensured as well as respect of individual rights, interests, sensitivities and privacy. Another principle in strict relation with the protection of citizens is the principle of ensuring prevention of any harm that could derive from the use of deployed technologies. Proper precaution measures in order to minimise disturbance were taken. Confidentiality and anonymity are 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. From a legal and ethical point of view, the collection of data is only the first step in the processing of personal data. Processing of collected data was carried out with caution, with respect to the regulations concerning privacy and data protection.

During the project, from a *public (societal) perspective*, several issues and measures have been implemented in order to respect both regulations applied at European Union level and national legislation. Of far most importance were the notification forms which were submitted to the National Data Protection Authorities - NDPAs in Romania, Greece, Cyprus and Spain, where pilots where undertaken. Since the project tackles an involvement of wide critical infrastructure subject to public use, the necessity to inform the NDPAs was crucial in order to gain validation of project activities and to ensure respect of regulations.

ZONeSEC Ethical management framework had the main aim to ensure full compliance with the ethical and privacy principles established by the project. The framework of the ethical management of the project was included in the work of the WP10, the Ethical Board (ETB) and the Independent Ethics and Data Protection Expert (IEDPE).

During the project's lifetime the ETB, composed of five members, met periodically depending on project's needs. The frequency of interaction between the leader of the WP10 and the Ethical Board was conditional to the overall project activities within the work packages (WPs). The assignment of the IEDPE was performed in the last year of the project and allowed for intermediate consultation sessions both with the WP10 and the ETB.

The main task of the Independent Ethics and Data Protection Expert was to assess whether:

- the Consortium Partners did respect the fundamental rights embedded in European and national legislations with emphasis on the right to privacy and data protection;

- the Consortium Partners did comply with their substantial and procedural obligations as well as with data security requirements;
- the abovementioned requirements were met within the research activities of the project.

The Independent Ethics and Data Protection Expert supplied legal and practical advice to the project manager and other project partners regarding the precautions to be taken and procedures to be followed in respect of national and EU legislation for the protection of privacy and ethical principles.

Special attention was given to the issues concerning the protection of personal data, since this was the main ethical risk associated with the activities of the project. This was also the approach adopted by the Consortium Partners who have identified the following issues that may have arose with regard to the project:

- use of (personal) location data and possible infringement of location privacy;
- implications of persons' profiling (monitoring, analysing habits etc.);
- challenges regarding lawful and fair (personal) data processing, especially concerning purpose of the processing, potential transfers to third countries;
- data security issues.

Moreover, for precaution and demonstration that the process of data collection, use and storage within ZONeSEC has not caused any high risk to individuals, a **Data Protection Impact Assessment** (further in the text: DPIA) has been performed.

The DPIA is one of the specific processes mandated by the General Data Protection Regulation (GDPR). The GDPR states that organisations must carry out a DPIA where a planned or existing processing operation "is likely to result in a high risk to the rights and freedoms of individuals". DPIAs are particularly relevant to ensure a privacy-by-design approach when introducing new data processing systems or technologies. Within ZONeSEC there was no evidence showing that there might have been a high risk to infringe rights and freedoms of individuals. Nevertheless, a DPIA has been performed in order to verify this hypothesis.

The process of DPIA within the project implied the following implementation steps:

1. **Identification of the need for the DPIA** – the need for a DPIA was identified as in the context of accountability it is key to be always aware of any potential high risk and be in the position to mitigate such risk. In this perspective, this process was also recommended by the ZONeSEC Independent Ethics Expert.
2. **Description of the information flow** – the undertaken DPIA within the project was able to describe how information was collected, stored, used and deleted. This particular stage was performed during the lifetime of the project, in order to be updated and to evaluate any potential risks (i.e. adaptive strategy). A specific questionnaire for data collection was elaborated for this purpose, which was addressed to technical partners.
3. **Identification of privacy and related risks** – the DPIA also catalogues the range of threats/risk as follows: low risk; medium risk; and high risk.
4. **Identification and evaluation of ethical values** – the DPIA not only identifies privacy and related risks. The approach adopted by article 29 "Data Protection Working Partner" of the Guidelines on Data protection Impact Assessment was considered when choosing to evaluate also potentially high risks to individuals' fundamentals rights and freedoms (based on Charter of Fundamental Rights of the European Union; and European Convention for the Protection of Human Rights and Fundamental Freedoms).
5. **Record the DPIA outcomes and integrate the DPIA outcomes into the project** – a record of the outcomes of the DPIA (steps 1-4) is made in a form of a report.

b) Analysis of perception and acceptance of monitoring/control technologies

A survey was aimed at investigating: 1) citizens' perception and acceptance in regards to the monitoring activities in general; 2) the level of citizens' acceptance in regards to specific monitoring tools and systems for surveillance and maintenance of public assets (large-scale infrastructures).

Research structure

The questionnaire used for the purposes of the research was composed of four main sections:

I. Socio-demographic data;
II. Perception;
III. Acceptance;
IV. Use of monitoring technologies.

Distribution of the questionnaire

The survey was distributed among project partners for them to "snowball" in their own countries, through their own social media, newsletters, websites etc. Although originally drafted in English, for dissemination purposes the questionnaire was also translated into six languages (i.e. English, French, Greek, Italian, Romanian, and Spanish), so as to reach a more diversified audience (i.e. a set of responders being able to answer to a questionnaire in English represents already a very specific target).

Main research results

Responses to the questionnaire were received from 353 respondents in total from France, Greece, Italy, Macedonia, Romania, Spain. Respondents were almost equally distributed among male and female, with a slight predominance of male respondents (53,6 % of the total). Most of the respondents of the questionnaire (39,4%) belong to an age group between 31 and 40 years of age.

The second section of the questionnaire was aimed at investigating **citizens' perception in regard to monitoring activities** in general. According to the responses, the life areas/domains perceived by respondents as more subject to control are:

- Their Internet browsing activity;
- Their use of credits cards for payments;
- Being filmed by cameras in airports;
- Their Internet purchase activity;
- The content of their bags while travelling through airports.

The third section of the questionnaire was dedicated to revealing the **acceptance of the respondents in regard to monitoring activities** in general. The respondents were specifically asked to express their agreement on several given statements. Respondents expressed their agreement, in particular, with the following statements:

- My privacy is very important to me; I cannot stand any infringement of my right to have its protection guaranteed;
- I wonder if all surveillance really contributes to the common good;
- I wonder if all this surveillance means increased security;
- I accept to be monitored and to share my personal data only after being properly informed and signing a consent form.

Respondents thus showed to value their privacy highly and to agree to give it up for security/safety purposes only if properly informed: generally, the idea that more surveillance increases the common good is seen with distrust.

Another question was aimed at identifying the places that respondents deem important to be equipped with surveillance cameras. Critical infrastructures (i.e. airports, bank counters/ITMs; subway/railway platforms; gas pipelines; oil pipelines; water production and distribution systems; warehouses for the storage of chemicals) received a high ranking in terms of perceived importance and thus need of protection.

The aim of the fourth section was to investigate the **level of citizens' acceptance** in regard to few identified monitoring tools and systems for surveillance and maintenance of public assets (large-scale infrastructures).

Analysing the main purpose of monitoring technologies, according to respondents, the main purpose is to: ensure public security (28.3%) and act as a risk mitigation measure (22.7%).

While the main achievement of monitoring technologies, according to respondents, is to: make citizens feel safer (24.6%), make crime detection more efficient (22.9%) and make management of wide areas more efficient (22.1%).

Another question was aimed at identifying the more sensitive critical infrastructure that, according to respondents, should be more subject to protective measures. According to respondents, the critical infrastructures that should be more subject to protective measures are chemicals' warehouses, water production and distribution systems, gas pipelines and oil pipelines.

In this section of the questionnaire, also a set of hypothetical scenarios (mainly related to the fact of being monitored during daily activities) have been proposed to respondents. Respondents were asked to express how well a series of statements related to each scenario represented their feelings.

In general, respondents showed to have a positive approach to monitoring tools and systems in their daily life, mainly referring to a:

- **Safety/security profile** - referring to a person which accepts/rejects acts of monitoring if they are related to safety and security;
- **Ethical profile** - referring to a person which accepts/rejects monitoring as an ethical concern, related to a set of ethical values generally adopted in his/her daily life.

Another question was aimed at identifying the measures that, according to respondents, could protect public security better. A high percentage of respondents (28.6%) report that all the proposed measures are necessary to protect public security better.

c) Internal Self-assessment

An internal self-assessment tool for project partners was developed and distributed in order to assist them in the evaluation and monitoring process within their institutions in regard to the respect of data protection norms. A questionnaire was developed in order to provide all project partners with a first instrument of self-assessment, at the beginning of the project, to allow for monitoring and analysis and adjustment of its operating procedures and protocols with respect to the current regulations regarding the protection of privacy and protection of sensitive data. The main normative references which were followed in order to verify and assess the full correspondence of each project activity to the current legal requirements regarding the protection of confidentiality of personal data are:

- Charter of Fundamental Rights of the European Union (2010/C 83/02);
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- other EU directives and measures; and
- legal instruments, regulations and guidelines of the countries where data processing will be conducted.

In order to prevent misinterpretations of the meaning of the most frequent terms on the protection of privacy, the definition of the terms used in the questionnaire (principal keywords) was provided in the introduction to the questionnaire, in line the European legal framework (Art. 2 of the Directive 95/46 EC).

The work was intended to provide useful guidance to project partners to identify possible problems and adjustment needs of the required standards within the project, in regard to the protection of privacy and personal data. Some partners might, in fact, have had to apply certain procedures for the first time for specific activities to be carried out during the project. Individual project partners were

requested to complete the questionnaire with the greatest serenity, sincerity and willingness, without being influenced by the natural propensity to respond positively when asked about information or opinions on the structure of their affiliation (psychological process called “fallacy of optimistic bias”). The information provided by project partners was analysed with the aim to highlight aspects useful for optimizing operational procedures and control of activities within ZONeSEC, in compliance with domestic and international legal framework for privacy protection.

d) Self-assessment tool for operators

Development of the questionnaire and testing

The development and testing of the self-assessment tool were performed with the assistance from the end-users. The formulation of the potential end-users involved in the end-users’ board was performed, in consultation with all project partners. This board was the main instrument used for selection of participants in the end-user workshop, with the objective of engaging end-users in an interactive process for collecting feedback and comments on a draft Self-Assessment Questionnaire. For this purpose, the Workshop entitled "Data Protection and Privacy” (Athens – 18/19 October 2017) was organized in order for end-users to participative review the first version of the questionnaire prepared to assess the capabilities of end users for protection of personal data/information in their everyday work.

The main aim of this tool is to assist end-users in verifying the level of implementation of specific data protection procedures, directing their attention where major breaches seem to be occurring. If these are highlighted by the tool, after an expert in depth review, the institution/organisation could consider taking reasonable steps to safeguard the personal information in their custody or prevent from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

After the performed workshop, the tool was prepared in a form of excel document, containing scores for each question.

Self-assessment tool as a product

The self-assessment tool is designed to assist end-users/operators (organisations, companies etc. dealing with collection, processing and storage of data) in doing a first check on their level of compliance with the legal framework in force (GDPR) concerning 5 different dimensions: 1) Adoption of relevant data security policies; 2) Personal information management; 3) Personal information protection standards; 4) Technological protection measures; 5) Access to databases containing personal information.

The assessment results should let each respondent (organisation/company) visualise for each specific dimension (see above) if it:

- does NOT meet Minimum Requirements;
- MEETS Minimum Requirements;
- MEETS Minimum Requirements and is also implementing extra measures that are not compulsory by law (i.e. implements more stringent measures than what required as compulsory by law).

It should be stressed that this tool is not aiming at providing a “GDPR compliance guarantee” check-list for operators. It serves as a support and awareness raising tool to be used by end-users/operators to understand their overall positioning within the complex legal corpus presented by the GDPR. Moreover, end-users/operators should be aware that national by-laws need to be considered as well in order to guarantee their compliance with the new legal framework on data protection.

The final version of the self-assessment tool is integrated, as a distinct module, in the European Widezones Surveillance Reference Toolkit (EU-WSRT).

e) Identification of ethical and legal issues concerning protection of citizen's rights in the EU legal regulation of privacy

A specific part of the research was dedicated to the evolution of the European Union legal regulation of privacy and data protection, focusing on:

- The novelties introduced by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - **GDPR**), repealing Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (further in the text: Data Protection Directive).
- The Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (further in the text: **PCJA Directive**).

3.1.9.1 Identified innovations:

The project dealt with many activities concerning the collection and use of data. The effort performed by WP10 was that of a constant update with normative EU standards and monitoring of evolutions also in national regulations, so to ensure an adaptive approach of all activities concerning data management.

The evidence collected from the general public shows a high degree of concern about privacy protection, while a widespread awareness on the need of monitoring and protecting CIs was also found among respondents.

The example of the ethical and data management process performed within ZONeSEC could be usefully applied also to other domains of action where technological development is so intertwined with the need to protect society as a whole, not only from attacks to its safety and security, but also from the misuse of data of the citizens.

3.1.10 Standardization and Regulatory Activities *(Work Package 11)*

Standardization activities and development of CWA: Standards provide the means to facilitate compatibility of various components, products and services and enable the collaboration of businesses and consumers in terms of cost reduction, performance enhancing and safety improvement. Standardization is a time-consuming process that requires the interaction of various expert stakeholders in order to reach consensus and set out specifications on all-kinds of processes, products, and services.

The ZONeSEC project took the opportunity of this new environment and launched the development of pre-normative standards on "Interoperability of security systems for the surveillance of widezones", through the standardization concept of the CEN/CENELEC Workshop Agreement (CWA) procedure. The CWA is a light, not time-consuming procedure that is designed to meet the market needs, where an innovative technology has not reached a sufficient degree of maturity and reflects the consensus of identified individuals and organizations responsible for the content[1]. The basic objective of the ZONeSEC's CWA was to disseminate the research results and embed them within the EU standardization landscape in the secure technologies domain. The produced CWA is a guide that can

[1] More information about the CWA procedure can be found in the official site of the CEN/CENELEC: https://boss.cen.eu/developingdeliverables/CWA/Pages/default.aspx

later be developed and adopted by operational stakeholders as standards and/or can be included in regulatory provisions.

Following the approval of the Project Plan submitted to CEN/CENELEC, the procedure officially started with the Kick-off meeting that took place on 11 December 2017 in Athens. The participation to the kick-off meeting was open to anyone and the opportunity to contribute was widely advertised in advance by its proposers and by CEN/CENELEC member bodies. Twenty six (26) stakeholders actively participated and during the meeting the workshop chair (Dr. Diimitris Drakoulis) and secretariat (BSI – British Standards Institution)[2] was approved, along with the workshop project plan that described the scope and the desired results of the CWA. Three drafting cycles began after the kick-off meeting, leading after 12 months to the final CWA document, which has reached the consensus required from all the registered participants. During this drafting period the 20 registered participants closely collaborated through physical and virtual meetings, in order to provide a guide on interoperable security systems for widezone environments that was submitted for publication in CEN/CENELEC on November 2018. The basic chapters of the CWA have to do with the: a) Proposed architecture, b) Interoperability recommendations, c) Operational needs and d) Security requirements (figure below), providing a pro-active approach towards identifying a guide to a total solution for the protection of widezone infrastructures.

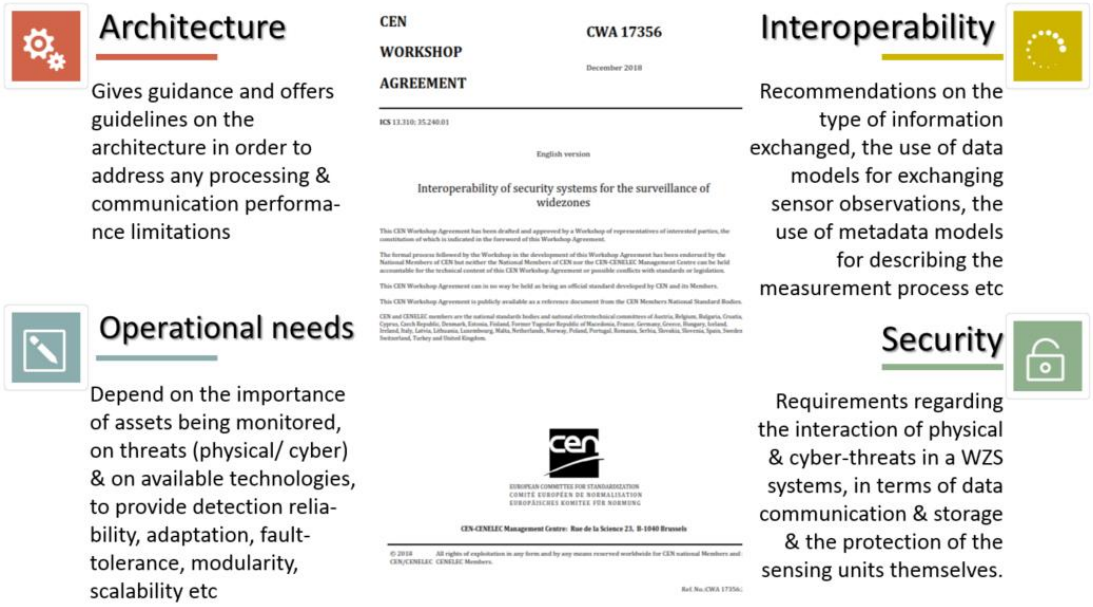


Figure 29: CWA thematic areas

The final CWA 17356:2018 has been published at CEN/CENELEC official website and it is now available for download by any interested party:

https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:68549,2341530&cs=1C3DCED093484F2A7DC3F880C6D920FD1

[2] The Secretariat provided a professional management support in the form of administrative, operational and technical services to the Workshop.

According to the CWA procedure established in CEN/CENELEC Guide 29[3], the CWA will stay valid for 3 years, after which the Workshop Secretariat (BSI) shall consult the ZONeSEC Workshop registered participants & the relevant CEN/CENELEC technical bodies (e.g. TC 391 Societal & Citizen security), to determine whether the CWA 17356:2018 shall be confirmed for another three (3) years, revised, transformed into another deliverable, or withdrawn.

Exploit Pre-commercial Procurement (PCP) approaches: Innovative Innovation procurement can be used as an effective instrument to influence technological development, innovation and as an additional tool, to increase the R&D public expenditures. In the next years, procurement of innovation is likely to become a key element of a balanced innovation policy strategy in European countries, as demand-driven policy instruments will be bringing companies and government together to cooperate on developing innovative solutions for major societal challenges, such as ageing, mobility, heath care, transport and environment.

A separate section concerning the innovation procurement initiatives was also reviewed under the WP11 of the ZONeSEC project, with extended analysis on Pre-commercial Procurement (PCP) approach. Particularly, the PCP essentially refers to the purchase of R&D services by the public sector. It is triggered by procurers identifying the need to solve a socio-economic problem or challenge of public interest for which there is no solution available on the market yet. Accordingly, the PCP is not concerned with the procurement of existing products or services already in the market (common termed to as Commercial-Off-the-Shelf of COTS) but with the R&D phase, which involves the solution exploration and design, prototyping, up to the development of a limited volume of first products or services.

The provided analysis provided information on the evaluation and presentation of the PCP procedure, aiming to elaborate a "cookbook" of best practices for the adaptation of the PCP approach towards the exploitation of secure technologies for surveillance in wide zones. The basic objective was that after the completion of the ZONeSEC project, particularly the end-user organisations of the consortium will be familiarized with the PCP process/ tools and put them into use to meet their security needs in their countries and in the EU environment. Additionally to the PCP procedure and for reasons of completeness, the PPI (Public Procurement of Innovation) procedure was described, which is the next step after the completion of the PCP procedure, offering solutions that are more mature and thus closer to the market. In the PPI approach, the public sector provides a seal of approval for innovative solutions by acting as a launching customer/ early adopter.

Further reading: Del 11.9 – "Recommendations on the best practices to exploit Pre-commercial Procurement approaches toward the exploitation of secure technologies for surveillance of Widezones".

"White Book" on good regulatory practices: The importance of Critical Infrastructures (CI) in the EU environment is undeniable. Malfunctions or damages, to critical points (functions, equipment and controls) may lead to large systemic failures of the processes operating in widezones, while economic stability, safety and security in Europe could be potentially compromised.

For the proper function and security of CIs a set of technological, operational and regulatory measures apply to protect CIs against incidents that may escalate to crises. With this concept in mind, a "white book" on good practices was developed under the WP11, regarding the protection (operational, technological) of widezone CIs and the enhancement of their resilience.

Particularly, six (6) independent thematic axes were reviewed and presented, all equally important for the proper operation of CIs and all relevant to the project's results:

[3] "CEN/CENELEC Workshop Agreement", CEN/CENELEC Guide 29, Edition 1, November 2014 (ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/29_CENCLCGuide29.pdf

Technological approach

- Thematic axis #1: General overview of the Remotely Piloted Aircraft Systems (RPAS), their use as well as restrictions and general recommendations about their application for surveillance purposes in CIs environment.
- Thematic axis #2: General description of the regulations and good practices on the design and development of novel radar systems (MIMO radars) for the 24/7 surveillance of CIs

Regulatory approach

- Thematic axis #3: Analysis of the legal framework concerning CIs and how it can be further updated and exploited to provide robust and unconditional critical services to citizens.
- Thematic axis #4: Analysis of the new GDPR regulation framework about personal data protection and its impact on CIs. A list of recommendations was provided to align CI practices with the new requirements of the regulation (e.g. privacy-by-design for the surveillance equipment, assignment of a data protection officer etc).
- Thematic axis #5: General review of "The NIS Directive", concerning cyber security issues and how they can be implemented in CIs operations. A set of recommendation were also presented, applicable to CI stakeholders in order to increase their resilience again cyber-attacks.

Operational approach

- Thematic axis #6: Detailed insights on the ZONeSEC Security Management Framework, which constitutes the baseline for the development of Operator Security Plans (OSPs) by critical infrastructure owners/operators, as imposed by the Directive 2008/114/EC.

Further reading: Del 11.7 – "Recommendations for enhancement of the European regulatory landscape aiming at accommodating the results of the ZONeSEC"

3.1.10.1 Identified innovations:

No innovations identified.

3.1.11 The European Widezones Surveillance Reference Toolkit (EU-WSRT) *(Work Package 12)*

Within this Work Package the European Widezones Surveillance Reference Toolkit was designed and developed (**http://wsrt-app.exus.co.uk/**). The European Widezones Surveillance Reference Toolkit (EU-WSRT) is a web application consisting of different supportive functionalities for everyday tasks of Widezone owners and operators. These functionalities are divided into the following major sections:

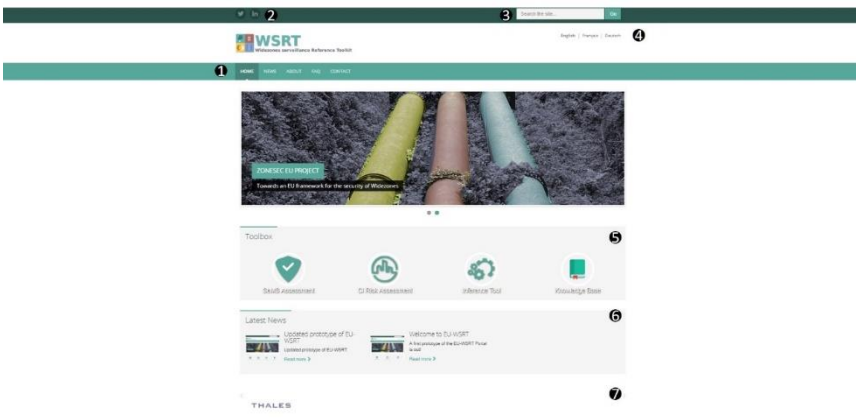


Figure 30: EU-WSRT Toolkit screenshot

Supportive content: this section includes all functionalities that are related to the management of content, i.e. a typical **Content Management System** (CMS). The content added onto the section is related to Critical Infrastructures security and surveillance and provides a common reference framework, becoming a knowledge base maintained and evolved by the relevant stakeholders (EU Bodies and authorities, National authorities, other research projects, etc.) for the interest of the security community and society as a whole.

Specific EU-WSRT functionalities: in this section of the toolkit the focus was to support organizations that operate a Critical Infrastructure (CI) and intent either to perform an evaluation of their security status or to deploy a new surveillance solution. EU-WSRT is a decision support tool, promoting a security by design approach and aiming at providing documented recommendations for CIP. The core system structure is based on the following sub systems:

1. **A knowledge based library Tool:** Knowledge Base is the repository for sharing documentation throughout the platform or within a team inside the same company. The documents can be categorized according to their relevance or user's will.
2. **The Security Management System (SeMS) Assessment Tool:** This module provides a questionnaire that covers all the main requirements of a comprehensive SeMS, used by users who are interested in assessing the SeMS provisions and procedures within their Widezones. The results of the SeMS assessment procedure provides useful information to be used as input for the risk evaluation process offered by the CI Risk Assessment module.
3. **The Data protection Self-Assessment Tool:** it is a self-assessment tool for organisations/companies in order to enable them to evaluate their compliance with EU standards and regulations in terms of data management and protection and privacy. The self-assessment tool is highlighting gaps between the existing compulsory EU regulations in terms of data management and protection (i.e. GDPR) and actually implemented standards in the organisation/company utilising the tool.
4. **The CI Risk Assessment Tool:** This module aims at supporting Widezone owners, operators, managers and decision makers in identifying, assessing and evaluating risks related to their Widezone security. The CI Risk Assessment module was developed according to ZONeSEC comprehensive security risk assessment methodology which incorporates the main principles of national and international regulatory frameworks and standards applied towards risk management and critical infrastructure protection.
5. **The Inference engine Tool**: The Inference engine is one of the core parts of the EU-WSRT. The role of this module is to provide the user with suggestions with regards to CI, based on data held at the system (preconfigured and maintained by the owners of EU-WSRT). The inference engine is approached through a Business Rules Management System (BRMS) where knowledge is modeled (business rules) and will provide a way to the users to give input to the system and extract some very specific quantitative results with regards to their tasks of interest.

3.1.11.1 Identified innovations:

Effective risk assessment methodologies are vital for any CI Protection programme. The extensive number of risk assessment methodologies for critical infrastructures clearly supports this argument. Risk assessment is indispensable to identify threats, assess vulnerabilities, and evaluate the impact on assets, infrastructures or systems taking into account the probability of the occurrence of these threats. There is a significant number of risk assessment methodologies for CI consisting of some main elements: Identification and classification of threats, identification of vulnerabilities, and evaluation of impact. However, there is a huge differentiation of risk assessment methodologies based on the scope of the methodology, the audience to which it is addressed (policy makers, decision makers, research institutes) and their domain of applicability (asset level,infrastructure/system level, system of systems level). These attributes are not mutually exclusive, in the sense that the domain of applicability defines to a certain extent the target group of the methodology mostly addressed to policy makers and relevant authorities and less to operators or to asset managers at local level. To fulfil this gap/vision, ZONeSEC built on the existing state-of-the-art in Total Security Evaluation, by introducing a new set of tools that contributed in advancing current common best practices in several aspects such as:

- improvement, extension, and harmonisation of evaluation indicators for security applications and services;
- focusing on characteristics and needs in European countries, although taking into account the different situations in different parts of Europe (e.g. national values weighted for user context);
- increased awareness among decision makers of the positive potential of Widezones critical infrastructure applications and services.
- Provision of accessibility, comparability and transferability of existing knowledge in national and international level.
- Provision of an easy-to-use decision support instrument to identify suitable and mature security applications/services,
- Provision of an easy-to-use system for decision makers to compare different options of security systems' implementation towards the formulation of their final decisions.

Further reading: Deliverable D12.2 entitled as "EU-WSRT Administrator's manual".

4. Potential impact and main dissemination events

4.1 ZONESEC mission and vision

ZONeSEC Need: A potential failure of critical infrastructures such as, pipelines, energy lines, transportation routes, etc., can occur at any point and at any unexpected moment across their extended grid spread over wide geographic areas. These Wide-zones aim primarily to the strengthening of the infrastructure's robustness by extending in a trans- boundary fashion for the transport of materials necessary on a daily basis. Failures at critical points (functions, equipment, and controls) can compromise the integrity of the involved installations and the security of energy and resources supply, with adverse socio-economic effects to citizens, customers and the environment (major accidents). Shortcomings in the control of hazards inherent to the safe performance of the infrastructures are strongly linked with the effective implementation and functioning of a Safety Management System (SMS) including appropriate safety and security provisions, emergency planning and other proactive measures such as surveillance, from detection to alert.

The current shortcomings in a total security approach become apparent when one considers:

1. the costs of the systems involved for the surveillance of large areas,
2. the complexity and diversity of the employed systems,
3. their efficiency, robustness and resilience,
4. their accuracy to detect illicit activity patterns,
5. difficulty to coordinate surveillance and monitoring activities at national and transnational levels,
6. their compliance with EU policies and societal values with respect to privacy protection.

An opportunity exists for a system to deal with the issue of Widezones and large area security in a holistic and systemic manner, which provides in that sense a solid solution to the above-mentioned issues.

ZONeSEC Vision / Mission: ZONeSEC defines Widezones as the extensions of infrastructure that is critical for the support of the citizens' daily activities and their normal operation impacts directly the security and safety of civilians.

Illicit/Illegal is the activity that is incurred to a Widezone (part of large infrastructure such as a highway, pipeline, high voltage electricity network, etc.) by a malicious third party either **accidentally or deliberately**). ZONeSEC is **not interested** in detecting phenomena such as a **leakage due to**

corrosion in a pipeline as this is an issue of maintenance and not of **detection of illegal or threatening activities** with direct or indirect **impact on the security of citizens**. Nevertheless, ZONeSEC will make the necessary provisions to collaborate with health monitoring systems or other legacy systems for Widezones surveillance and operations management.

It goes without saying that ZONeSEC will make all the necessary provisions for its components to be integrated and made compatible and interoperable with existing monitoring tools and systems, which are used for the surveillance and maintenance of large-scale infrastructure.

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.

At the same time, ZONeSEC guarantees technological excellence by leveraging best of breed activity pattern recognition and state models, based on data from advanced low cost sensors, state of the art simulation techniques, robust, resilient, and flexible and cutting edge IT and Communication infrastructure, expert systems and reasoning for decision support and seamless large volume of data and information sharing to multiple channels.

The Global Objective of ZONeSEC is to support the security of citizens by providing a total solution for the protection of Widezone infrastructure.

4.2 ZONESEC Anticipated Impact

4.2.1 Impact on interoperability of data and information exchange among stakeholders (advanced situation awareness)

ZONeSEC improves interoperability by providing:

1. *Interoperable and Cooperative ZONeSEC solutions* to facilitate the coordination of Widezones surveillance activities. The scalability of the system guaranteed by a strong backbone service infrastructure with an advanced knowledge base enables the expansion system's management of large volumes and heterogeneity of observation data and streams.

2. *Interoperability of the ZONeSEC platform at a national level.* For nationally-contained crisis events the ZONeSEC platform provides a solution that is able to liaise seamlessly with the existing surveillance systems and infrastructure that are already in place; ZONeSEC is adapted according to the existing national standards and processes, while at the same time keeps an outlook for a pan-European uniform approach.

3. *Interoperability at a cross-border level.* ZONeSEC provides a system of systems with choreographed services for best performance across the whole geospace of the Widezones surveillance operations.Multi-national teams and first responders participated through shared access to monitoring resources, detection and alerts. This increase in efficiency of operations along with the security of the involved personnel assures the security of the citizens through advanced means of large scale disseminations of alerts.

4.2.2 Impact on wide zones surveillance procedures

Based on E.C. a number of major limitations (potential shortcomings in the normal operation of Widezones, and requirements have been identified at three key levels. :

1. **Legislative.** There is no EU legislation aimed at controlling third party interference (need for improving regulatory controls in this respect);

2. **Self-regulatory.** There are new and not yet implemented technologies and R&D that can provide new ways to improve pipeline integrity, safety and security against third party interference (development of standards and participation of oil & gas sector in R&D as an important part of self-regulation, is in the interest of all stakeholders); and

3. **Technical.** There are important limitations and gaps in the existing surveillance programs and procedures of Widezones (need for more reliable, technologically upgraded, efficient and cost –effective surveillance techniques). It has already been mentioned that any legislation or regulation aimed at improving pipeline safety should build on the sector's achievements and on the mechanisms of self-regulation that are in place and have proven their worth. Failing to recognize this might render the measures counterproductive. Accordingly legislation and regulation should focus on goal setting and facilitate, for those who can demonstrate competence, a high degree of self-regulation.

Moreover, technical limitations and gaps encountered in the common surveillance practices can solely be tackled with improvements in the effectiveness of a tailor-made and appropriately implemented Safety Management System (SMS) (for pipelines PIMS).

The ZONeSEC common technological backbone, satisfies all needs (legislative, self-regulatory and technical) in the control of third party interference caused by non-authorized and malicious acts and provides improved data fusion, interconnection and interoperability between diverse actors and Widezones stakeholders.

The information processing required for an unauthorized operation disturbance to become an emergency plan activation is routed through the assessment of risks to the health and safety of people involved, the equipment and structures concerned, the energy / resources / services supply chain and the invested capital.

The following stages are crucial for the information and decision making processing as required for detection through alert:

a. definition of abnormal conditions and situations for each and every system under systematic monitoring for potential threats
b. detection and identification of excursions from normal operation
c. assessment of risks involved based on consultation of the existing informed knowledge assets
d. expert support to decision making in triggering the appropriate alert mechanism, and
e. provision of alternative response plans when emergency measures are insufficient or crisis management exhibits shortcomings.

The difficulties become massive if one considers the range and diversity of systems (utilities, information, and actors) involved in the above stages across Widezones. A single attempt to outline the rationale for an advanced collective surveillance approach will produce a long list of requirements addressing as a minimum the following:

a. what constitutes a major threat (sources of hazard)
b. systematic monitoring (minimizing hazard at the source)
c. what constitutes an abnormal condition (safety critical and vulnerable points)
d. detection mechanisms and systems (tracing the initiating events of a failings sequence)
e. what constitutes an excursion from normality (controls against set thresholds)

f. risk assessment procedures and criteria (top events: hazards analysis and consequence assessment of accident scenarios)
g. informed databases (background information systems through and on which risk assessment outputs are quantified, positioned and communicated)
h. initiators (individual or in clusters) of emergency levels and alert (emergency response criteria)
i. "equivalent risk" management response plans (activating prevention, controlling and mitigation measures, resources and systems)

The architecture of ZONeSEC approach takes on board all above mentioned requirements aiming at minimizing the vulnerability of critical ends such as:

a. interpretation and communication tools for processed data,
b. data standardization with universal references,
c. extent of operators involvement (human actors),
d. organizational factors shortcomings, and
e. Completeness and adequacy of knowledge assets.

The systems employed by ZONeSEC provides reliable and informed answers on each and every requirement by proposing among others:

a. common sets of criteria applicable by Widezones stakeholders
b. reference top events scenarios and gap analyses oriented to target threads
c. comprehensive contents of safety procedures and response plans
d. best available techniques and mechanisms adaptable and applicable uniformly across Widezones
e. advanced technology sensors and hardware compatible to existing utilities
f. widely used information systems and data processing certified for quality and user-friendliness
g. efficient communication means and channels between systems and operators
h. functional specifications and training protocols for systems adaptation to integral functioning.

Last but not least, a concrete risk management approach has been adopted addressing:

a. Operational Controls,
b. Inspection and Surveillance techniques,
c. Hazard Analysis and Risk Assessment methodologies,
d. Management of Change, and
e. Response and Emergency Planning prerequisites.

All these elements of the ZONeSEC Safety Management System (SMS) have been addressed under a common safety culture as being implemented from a single safety management board with common safety commitments, provisions and procedures at a single safety critical site. ZONeSEC thus acted as a common ground and common risk communication language interconnecting systems and system elements reducing data and decisions ambiguity to a minimum.

4.2.3 Impact on socio-economic benefits of the project

ZONeSEC and the Citizens

ZONeSEC is in principle a framework-oriented project. Its approach is holistic and systemic in the sense that it covers activities that extend beyond technical progress and relevant achievements. In this light, ZONeSEC properly assessed the issues relevant to making it acceptable by the society and citizens and aligning its nature to the ethical constraints established. ZONeSEC is an overall

framework and a supporting system of systems that provides support in view of enhancing the security of citizens. Therefore, ZONeSEC takes into consideration specific aspects of its potential societal acceptance in order to ensure its success and to minimize the possibilities for resilience against its nature and applications. **A Societal Impact Checklist** from the Guide for Applicants has been used for the definition of the ZONeSEC impact on society.

4.2.4 Economic benefits

The European economy relies heavily on the smooth and uninterrupted operation of Widezones. Gas and oil are being transported internationally and even intercontinentally in many cases. The huge highway networks bridge distances between countries while rail tracks transfer goods and people 24x7. Electricity lines run millions of kilometers all over Europe, supporting a growing economy and water pipelines support a sustainable living model. ZONeSEC took a major step towards ensuring the security and normal operations of these (and other types) Widezones that support the backbone of the European economy.

ZONeSEC delivers value in a clearly monetizable manner as well. This is mainly achieved in two fashions: 1) **savings on damages avoided** from the early detection of illicit activities and 2) cost savings and **economies of scale** on infrastructure by defining a **common base line** for the surveillance of Widezones in the European Union.

Firstly, ZONeSEC is able to detect illicit activities that might lead to threatening circumstances, thus minimizing their impact on the economy. Accidents such as that of **Natural gas pipeline, Ghislenghien (Belgium) 2004** or **LPG pipeline near Ufa (USSR) 1989,** can be reasonably expected to be prevented saving both human lives and avoiding disruptions in the local and national economies.

Furthermore, ZONeSEC enables cost savings at a greater scale since the surveillance needs of Widezones will be homogenized across EU-27. This can be seen in a four-fold manner:

i. ZONeSEC's robust, modular and extensible architecture will allow all potential end-users to easily accommodate the required components, irrespective of the sophistication, size and complexity of their existing systems.
ii. The introduction of the DirectSIM framework from the military domain into civilian applications will provide an unprecedented ability to decision makers, to simulate available systems against different illicit activities and threats in view of assessing their suitability and performance before the any actual procurement.
iii. The harmonization of surveillance procedures and the establishment of a supporting interoperable framework will further promote cost savings especially in a cross-border and transnational perspective.
iv. Alignment of ZONeSEC's design to the European societal values and code of ethics that reduces the vandalisation of its components as a result of non-conformance or non-acceptance.

4.2.5 Contribution to Regulatory

ZONeSEC establishes a new way in which the surveillance of Widezones will be handled in a holistic approach and not per scenario or application domain manner. For this to happen, ZONeSEC extends its effort to tackle the delicate issues that underlie any attempt to enhance the security of citizens. Ultimately, the goal is to ensure the adoption of the modern technologies in an interoperable manner. Consequently, policies and regulation has to be aligned with the needs and capabilities of the new technologies. Recommendations on the best way to implement the results of the ZONeSEC bearing in mind the plethora of regulatory authorities in Europe at European, National and Regional levels, will be produced.

Surveillance is not exclusively aimed at conformity with certain legal requirements. Surveillance by the authorities is often the starting point of a process that leads to tracking down offenders and prosecution.
To assess the coverage of European, National and Regional regulatory provisions, a Regulatory benchmark has been developed. The benchmark is based on a combination of the safety provisions applied to fixed installations and an assessment of the accident history and major accident hazard potential of onshore pipeline transport. The legislative benchmark includes, among others, the following general safety provisions:

- **Prevention of threats coming from illicit activities**
  - Safety management systems
  - Risk assessment
  - Technical safety management measures
  - Prevention of third part interference
- **Mitigation of impact of threats;**
  - Emergency plans (authority's onus)
- **Efficient communications of risks and protecting actions:**
  - Information to the public
  - Exploitation of broadcast networks to convey relevant safety messages.

The assessment of the coverage of national legislation has included more detailed requirements within each of the main general safety provisions. Interviews with key regulatory authorities in the several planes (European, National, and Regional) were carried out aiming at ensuring that the ZONeSEC Recommendations for further enhancement of the Regulatory landscape can be effectively impacted and thus implemented in the revision of the applicable regulation

4.2.6 Added value at the European level

a. <u>Creating A Level Playing Field For The European Industry</u>

As mentioned, ZONeSEC sets the cornerstone for the definition of a European-wide framework regarding the surveillance of Widezones. In the current market of EU-27, as fragmented as it is, there are no apparent best practices built on solid foundations that will foster competitiveness and growth for the European Industries. On one side, technologically advanced countries and respective operators are highly accustomed to the latest systems and are able to spend considerable amounts of their annual budgets to secure wide area infrastructures. New member states with similar infrastructure at hand still have a considerable way ahead to bridge the gap with their neighbors. Considering that many of the newly planned large-scale projects on the setup of trans-European networks are heavily dependent on the new member states, one can see the importance of the successful implementation of ZONeSEC.
To that effect, ZONeSEC creates a level playing field for the European Industry by means of building on:

- The accumulated knowledge and delivered results of numerous Research and Development projects.
- The deep understanding of the shortcomings and inefficiencies of currently employed systems.
- The mapping and ultimately bridging of the significant differentiating factors in the tackling of the Widezones surveillance issue among different countries and industries.
- The creation of the EU-WSRT that is a major deliverable of the proposed work.
- The strong participation of key Industrial players from the European Market (ATOS, EADS, THALES).
- The involvement of a representative set of end-users that bring to ZONeSEC the much needed diversity both in terms of technology, geography, culture and domain of application.
- The setup of a strong Advisory Board that already has important members, committed to consulting the consortium with the overall steering of the project to achieve maximum impact.
- The capacity of leading research institutions from different European countries.

- The strong links with the standardizations bodies to ensure the creation of consistent and coherent approaches.
- The heavy investment in driving societal, ethical and regulatory research that will guarantee:
  - The acceptance of the proposed framework by the society.
  - Its alignment with the European agenda for the Security of the Citizens.

Therefore, ZONeSEC opens a new "arena" for conducting business related to Widezone surveillance and security, which will be under the auspices of the European Commission and the blessing of the involved stakeholders. ZONeSEC also creates a business sense that will be governed by uniformity, homogeneity and common understanding/tackling of current and emerging needs for the surveillance of Widezones.
In ZONeSEC **the European Industry was at the core of driving this evolution and one can expect a major transformation in the coming years.**

a. Contribution to Standards

The regulation framework and the standardization issues of operational procedures (including the certification of Widezone surveillance systems) as well as the societal and procurement implications so as to generate an initial framework for the design and development of suitable Widezone surveillance systems' approach in Europe, constituted a major goal of ZONeSEC. Among other important technology research activities, the ultimate goal was to contribute to achieve interoperability among devices, networks, processes and methodologies linked to the implementation of safety mechanisms to monitor and protect Widezones.

Therefore, Standardization was a major goal of ZONeSEC.. ZONeSEC makes use of the modern approaches in the standardization framework by following a double path aiming at pushing the adoption of new standards accommodating the results of ZONeSEC outcome: the conventional process through the Technical Committees of the European Standardization Organizations, namely CEN/CENELEC and ETSI, as well as the industrial-driven approach through the CEN/CENELEC Workshop Agreement and/or ETSI Industrial specifications. Through this process, ZONeSEC contributes to the creation of EU wide standards for interoperability aspects related to surveillance of Widezones.

4.3 Awareness Raising/ Main dissemination events

4.3.1 Organization of workshops

There have been three major workshops during project lifetime:

- Athens end users conference (2017): During the 18th and 19th of October 2017 ZONeSEC held its *End User workshop in Athens*, Greece. The event was a great success with more than 20 people from many relevant European companies. The event included a dissemination and exploitation dedicated section. This event marked the first step in **creating a final users community** to be exploited for dissemination & exploitation.
- Chania meeting (8 March 2018): Workshop about **"***Endorsement of White Book: Good Practices for Critical Infrastructure Protection"*. The workshop was dedicated to Oil & Gas Sector. It was hosted by Gap Analysis S.A in Chania, Crete, Greece. Between the participants we can highlight; DESFA, AVIN, CORAL (ex. Shell), NATO (Souda Bay Fuel Depot), JRC-ERNCIP, EXUS, TELESTO, GAP. The workshop covered the following **key thematic areas**; Operator Security Plans (OSP), Integrating new technologies for CI protection, Security Management framework for the Oil & Gas sector, ZONeSEC methodology for assessing security risks, Security Management System requirements and Operators Experience.

- Final workshop: According to the DoW "A major Conference is planned for the end of the project in order to provide all the potential stakeholders of the ZONeSEC foreground knowledge with a comprehensive presentation of the results of the project." [T13.1.4 Workshops and Conferences]. Preparation of meeting started in Sept 2017 with a part-time responsible. In order to improve impact, the idea was to add a "*ZONeSEC event day*" to one of the biggest European conferences in CIP: CRITIS 2018.
  Event was held at Vytauto Didžiojo universiteta in Kaunas, the 27th of September 2018.

Figure 31: ZONeSEC final workshop at Vytauto Didžiojo universiteta in Kaunas, the 27th of September 2018

4.3.2 Participation to exhibitions

First period of ZONeSEC project (2015):

- CPLAN participated in a *conference about H2020 projects* on April 28th, 2015 in Netherlands. In that conference CPLAN had the opportunity to present to an approximately 50 people audience a brief introduction about ZONeSEC project together with some other FP/ & H2020 projects they are involve in.
- *Civil Protection FORUM*: EXO attended the Civil Protection FORUM held in Brussels on the 6th and 7th of May 2015. In this event, EXO had the opportunity to disseminate information about ZONeSEC project, through EXO's dedicated booth.
- Participation of Attikes Diadromes to the "*UNECE Workshop on Vulnerability and Security of Critical Transport Infrastructure*", 8 September 2015, Geneva

Second period of ZONeSEC project (2016):

- ATOS presented *ZONeSEC to the Spanish Ministry of Defence* in March 2016.
- ATOS participated in the *CIRAS final conference* (8th of June 2016 at Katowize, Poland) making a presentation about ZONeSEC and its possible synergies with of CIRAS.
- ADITESS made dissemination of the ZONeSEC project during RSCy2016 (IEEE Compound Semiconductor Integrated Circuit Symposium) conference: "*Fourth International Conference on Remote Sensing and Geoinformation of Environment*" 4-8 April, 2016 – Cyprus.
  - The presentation "Towards a Framework for the Security of Widezones (ZONeSEC)" was given by Mr. Nikolaos Koutras during the Workshop "*Defense and Security Geo Intelligence*" on the second day of the conference. Furthermore, graphical material, the banner and the UAVs were present on ADIT´s booth.
- In December 2016, ADITESS participated in the International Conference "*Safety and Health in Facilities Management*" organized in Cyprus from the local Safety and Health Association.

  - The presentation "*Advanced Technologies for CI Protection from CBRN Hazards*" was given by Mr. Nikolaos Koutras. ZONeSEC project was presented focusing on the outcomes of the project and how they can be used in cases of CBRN hazards.
- GAP disseminated project results to:
  - Companies involved in the design of European projects of common interest – Trans Adriatic Pipeline (TAP) and Eastern Mediterranean (EastMed) pipeline.
  - Competent authorities that regulate critical infrastructures (CI) in Malta.
- ADITESS disseminated the ZONeSEC project during the International Conference "*Safety and Health in Facilities Management*" organized in Cyprus on the 3rd of Dec 2016 through a presentation related with the protection of critical infrastructures and Mini-UAV Systems. For the event, ADITESS added also a post to its own website where photos were presented. Also, during the event tweets by ADITESS were also posted mentioning ZONeSEC project.
- ITINNOV: Exploitation meeting with security professionals and participation at the *UK Security Expo Conference 2016 - Safety at Critical Infrastructure* – London, Nov-Dec 2016
- ITINNOV: Exploitation meeting at *Thales Pitstop, Digital Catapult, surveillance of critical infrastructure (railways)* - London, Dec 2016
- ISIG participated at the Workshop "*21st Century strategic foresight*", organized by the European Fund for the Balkans on 14-15 May 2016 in Becici, Montenegro.
- ISIG participated at the *Regional Policy Academy*, organized by the European Fund for the Balkans on 13-15 September 2016 in Belgrade, Serbia.
- ISIG participated at the International Conference "*Social change in the global world*" organized by the Goce Delcev University in Shtip, Faculty of Law, Center for Legal and Political Research, on 1-2 September 2016 in Shtip, FYROM
- ISIG participated at a seminar organized at the University Ss. Cyril and Methodius – Skopje on 22 December 2016 in Skopje, FYROM

Third period of ZONeSEC project (2017):

- ZONeSEC presentation at *ARES 2017:* Atos has presenting ZONeSEC in ARES [https://www.ares-conference.eu/] held in Reggio Calabria, Italy from August 29 to September 1, 2017
- ZONeSEC in *CRITIS 2017 International Conference*: ZONeSEC was represent in CRITIS 2017 by EXODUS S.A (October 8-13, 2017)
- ZONeSEC in "*Smart Cities and Mobility as a Service*" International Conference: ATTD participated in the International Conference "Smart Cities and Mobility as a Service", University of Patras – 7-8 December 2017
- *European Researchers' Night*: ZONeSEC was presented through the ICCS booth at the European Researchers' Night, in Athens, on the 29th of September, 2017
- Atos disseminate ZONeSEC in *Conference of Security, Democracy & Cities* in Barcelona (16 and 17 of Nov 2017)
- ZONeSEC was disseminated during *Milipol Paris 2017* from 21 to 24 of November: Both in Atos and Diginex booths (in separate initiatives)
- ZONeSEC in CNSP in Corsica: Diginext was present in the *124th National Congress of Firefighters* that took place in France from 11th to 14th October 2017

- ZONeSEC was present by DXT at the *14th International Conference on Systems for Crisis Response And Management (ISCRAM)* organised from the 21st of May to the 24th in Albi, France
- ZONeSEC was present by DXT at the *Technos Days of VALABRE*, centred on surveillance and crisis management, which took place in France from May the 22nd to May the 24th.
- ITINNOV: Poster presentation at *Computational Challengers in Image Processing*, University of Cambridge, Sep 2017
- ITINNOV: Poster presentation at *Standardisation & Ethical & User Requirements Workshop* – Athens, Oct 2017
- EXO & GAP: *2nd Greek Conference for Critical Infrastructure Protection*. KEMEA- Greek Center for Security Studies 2nd Greek Conference for Critical Infrastructure Protection. 19 & 20 Dec. 2017, Athens, Greece
- ATTD presented a paper at *the 8th International Conference for the Research in Transportation*, ICTR – 27-29 September 2017 Thermi, Thessaloniki
-

Fourth period of ZONeSEC project (2018):

- ATOS presented ZONeSEC during *CRITIS2018 conference*.
- ATOS presented ZONeSEC in *ERNCIP* thematic group meeting about "Early warning group" (Leganes, Madrid)
- ZONeSEC at the international conference "*Efficient Use and Management of Water 2018*"
- Tekniker disseminated ZONeSEC in *Conference IOT week* bilbao
- Workshop on "*Endorsement of White Book: Good Practices for Critical Infrastructure Protection*". 8 March 2018, Chania, Crete, Greece (organized under ZONeSEC project)
- ERNCIP Thematic Group (TG) "*Extended Warning Zones for Critical Infrastructure Protection (EWZ4CIP)*" meeting. ZONeSEC presentations describing advances in the project during ERNCIP meetings:
  - 30 May 2018, Ispra, Italy
  - 19 September 2018, Leganes, Madrid, Spain
  - 13th of Nov 2018. London UK
- Joint OECD-EU JRC Woskshop "*System thinking for critical infrastructure resilience and security*". 24-25 September 2018, Paris, France.
- ZONeSEC event "*Widezone Surveillance for Critical Infrastructure Protection*" (co-located with CRITIS 2018 conference at Vytauto Didžiojo universitetas), 27 September 2018, Kaunas, Lithuania.
- 34th International CAE Conference and exhibition "*Evolving Engineering Simulation: The age of Digital Twin*". 8-9 October 2018, Vicenza, Italy
- *GAP: CHEREE Chemicals Regulations Enforcement & Inspections – Building Authority Capacity for REACH/CLP and SEVESO III Compliance Workshop*, 12-13 September, 2018. Chania Greece
- GAP participated and disseminated ZONeSEC in 34th International *CAE Conference and exhibition* "*Evolving Engineering Simulation: The age of Digital Twin*". 8-9 October 2018, Vicenza, Italy

4.3.3 Videos and Photos

Many hundreds of photos were made during the 4 On-Site pilots and 3 final Pilots. These photos are included in ZONeSEC repository and has been used extensively in dissemination material, project webpage and social media groups.

During the last year of the project and specifically after each official pilot, you-tube like videos were prepared from the consortium in order to record the action performed during the pilots and promote through demonstration the systems developed from different partners operating in real environments as well as the overall ZONESEC concept. Some screenshots from the videos and their corresponding links are shown below:

Figure 32: Screenshots from videos prepared during Pilots

ACCIONA 1st official pilot:

https://www.youtube.com/watch?v=dP8_Faak4Ls

AQUASERV 2nd official pilot:

https://www.youtube.com/watch?v=j7bVqL64W1k (short version)

https://www.youtube.com/watch?v=6UR4sB3Cbgw&feature=youtu.be (long version)

ATTIKES Diadromes 3rd official pilot:

https://youtu.be/OR6JGsYz_ik (short version)

https://youtu.be/KpdtQLOT6e8 (long version)

4.3.4 Newspapers and interviews

- Radio interview by Atos: Atos has disseminated ZONeSEC in the radio using the website RFID-Latino.com
- Attikes Diadromes wrote an article about ZONeSEC in its own magazine

http://media.interactive.netuse.gr/pegasus/Multimedia/pdf/ntao_50_id5942352.pdf (page 8)

- ADIT submitted an article to Cyprus Safety and Health Association annual magazine.

During the life of the project we tried repeatedly to interest local TV stations (Alcarria TV in the Pilot of Torija, Spain) and with Euronews TV station. There was no success in the issue.

4.3.5 Brochures, posters, flyers and Newsletters

In the first year of the project, a common brochure, a common poster and official fliers were created. These materials were updated during project lifetime to reflect the changes in coordination and the new partner of DESFA. All these materials can be found in the ZONeSEC website (www.zonesec.eu).

- *Dissemination of the OIPs*:
  - Newsletter (number 1 to 4)
  - Press releases (1 to 4); sent through Atos
  - Sway presentation and slideshow (3 and 4 OIPs)
  - Video of first OIP (non-professional)
- Dissemination for Pilots:
  - Newsletter (number 5 to 7)
  - Press release (5 to 7); sent through Atos
  - Video dissemination

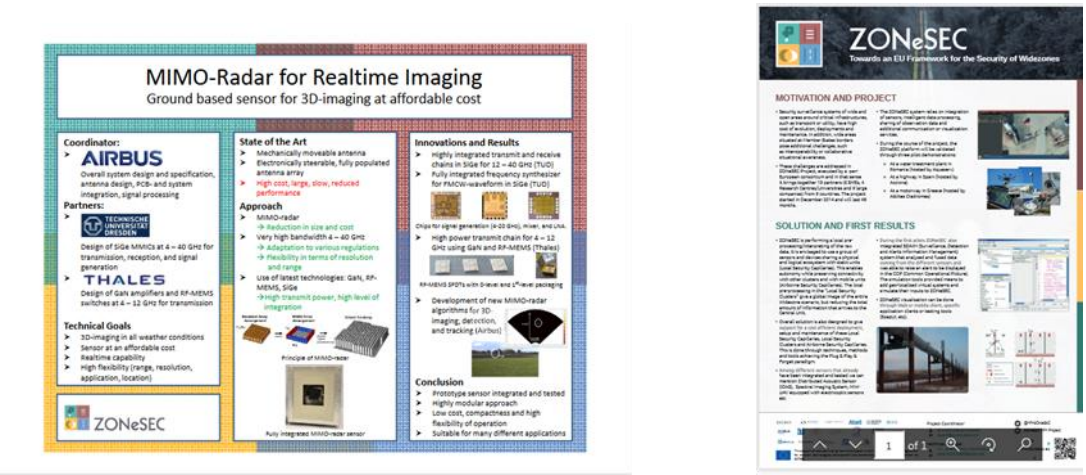


Figure 33: Screenshot from ZONESEC posters

Figure 34: ZONeSEC newsletter example

4.3.6 Presentations and scientific publications

First period of ZONeSEC project (2015):

- *WORLD HIGHWAYS: ATTD prepared an article titled "Towards an EU framework for the security of wide zones: research project "ZONeSEC", which was published in the May 2015 issue of the magazine "World Highways".*

Second period of ZONeSEC project (2016):

- *EADS presented a research paper describing the actual achievements with respect to the MIMO radar IEEE Transactions on Microwave Theory and Techniques*.

- *TUD presented a paper in CSICS2016 Conference (23-26 Oct) in Austin, Texas*.

Third period of ZONeSEC project (2017):

- *Conference paper written by ADITESS "Ubiquitous UAVs: a cloud based framework for storing, accessing and processing huge amount of video footage in an efficient way" has been submitted and presented in the international conference on Remote Sensing in Cyprus (RSCy 2017), Paphos, Cyprus, March 2017*

- *Institute of Communications and Computer Systems (ICCS) of the School of Electrical and Computer Engineering (ECE) of the National Technical University of Athens (NTUA) has presented paper to conference ISPRS SPEC3D*
- *ISIG presented a paper during "Challenges of Contemporary Society II", Skopje, FYRM, 17. November, 2017 with the title "Perception and acceptance of monitoring/control technologies: evidence from European project ZONeSEC". Atos was coauthor of the paper.*

- *EADS: A paper was submitted and accepted for publication at IEEE Transactions on Geoscience and remote sensing in the Dec. 2017 issue. It describes the concept, the hardware realisation as well as the signal processing of the MIMO radar. A. Ganis, E. Miralles, et.al. "A portable 3D imaging FMCW MIMO radar demonstrator with a 24x24 antenna array for medium range applications".*

- *Publication to ISESS Conference, Zadar, Croatia, May 2017, Sabeur Z. et al., Large scale surveillance, detection and alerts information management system for critical infrastructure. International Symposium on Environmental Software Systems. (2017). – 10 p*

- *Publication to ISPRS - SPEC3D conference. Frontiers in Spectral imaging and 3D Technologies for Geospatial Solutions October 25-27, 2017, Mattilanniemi 2, Agora, Jyväskylä, MULTIMODAL DATA FUSION FOR EFFECTIVE SURVEILLANCE OF CRITICAL INFRASTRUCTURE Z. Kandylakis, K. Karantzalos, A. Doulamis, and L. Karagiannidis, Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., XLII-3-W3, 87-93, https://doi.org/10.5194/isprs-archives-XLII-3-W3-87-2017, 2017*

Fourth period of ZONeSEC project (2018):

- *Articles presented in the Conference "Efficient Use and Management of Water 2018" in the next number (06/2018) of Romanian Water Association Journal, ROMAQUA*

- *Paper in San Diego: presented in BCITCS 2018, October 14-17 in San Diego and later on published in BCITCS (https://bcicts.org/).*

- *Paper called "Protecting water infrastructures: ZONeSEC research project – pilot demonstration for water companies" composed by many members of ZONeSEC consortium and lead by AQUASERV has been finally sent and accepted for the International Conference Efficient Use and Management of Water 2018.*

- *M. Sakalas, N. Joram, and F. Ellinger, "1.5-54 GHz High Dynamic Range LNA and Mixer Combination for a MIMO Radar Application," in 2018 IEEE BiCMOS and Compound Semiconductor Integrated Circuits and Technology Symposium (BCICTS), 2018, pp. 118–121.*

- *M. Sakalas, S. Preis, D. Gruner, and G. Boeck, "Iterative design of a harmonically tuned multi-octave broadband power amplifier," in 2014 IEEE MTT-S International Microwave Symposium (IMS2014), 2014, pp. 1–4.*

- *M. Sakalas, N. Joram, and F. Ellinger, "A fully balanced ultra-wide band mixer MMIC with multi-tanh triplet input for high dynamic range radar receiver systems," in 2017 International Conference on Noise and Fluctuations (ICNF), 2017, pp. 1–4.*

- *M. Sakalas, P. Sakalas, N. Joram, and F. Ellinger, "Fully differential high input power handling ultra-wideband low noise amplifier for MIMO radar application," in 2017 IEEE Compound Semiconductor Integrated Circuit Symposium (CSICS), 2017, pp. 1–4.*

- *M. Sakalas, P. Sakalas, and F. Ellinger, "Low Power Ultra-Wide Band LNA Based on Active Impedance Matching Technique for UWB Wireless Communication," in 2016 IEEE Compound Semiconductor Integrated Circuit Symposium (CSICS), 2016, pp. 1–4.*

- *M. Sakalas, N. Joram, and F. Ellinger, extension on: "Low Power Ultra-Wide Band LNA based on Active Impedance Matching Technique for UWB Wireless Communication," Solid State Circuits, Journal. Pending.*
- *M. Sakalas, N. Joram, and F. Ellinger, "Highly Robust 130 nm SiGe BiCMOS Power Limiter, LNA and Mixer IC for a Wideband 1.5 – 18 GHz MIMO Radar Receiver", 2019 IEEE International Microwave Symposium, June 2019, Boston.*
- *M. Sakalas, S. Li, N. Joram, P. Sakalas and F. Ellinger, "Ultra-Wideband 8-45 GHz Transmitter Front-End for a Reconfigurable FMCW MIMO Radar", 2019 IEEE Radio Frequency Integrated Circuits Conference, June 2019, Boston.*
- *K. Koncz, L. Kajcsa*, G, Inglese **, E. Agrafioti, A.G. Papadakis, A. Chalkidou***, M. Andeva**** , J. R. Martinez ***** and D. Petrantonakis. Protecting water infrastructures: ZONeSEC research project – pilot demonstration for water companies. International Conference Efficient Use and Management of Water 2018*

For more information about ZONeSEC dissemination activities, please visit: www.zonesec.eu

5. Consortium and Contact Point

The ZONeSEC consortium consists of the following industrial, academic and research partners:

EXODUS S.A. (EXO) www.exus.co.uk	Greece
DIGINEXT (DXT) www.diginext.fr	France
IK4-TEKNIKER (TEK) www.tekniker.es	Spain
ATOS (ATOS) www.atos.net	Spain
TECHNISCHE UNIVERSITÄT DRESDEN (TUD) www.ccn.et.tu-dresden.de	Germany
INSITITUTO DI SOCIOLOGIA INTERNAZIONALE DI GORIZIA (ISIG) www.isig.it	Italy
EADS INNOVATION WORKS (EADS) https://www.airbus.com/	Germany

UNIVERSITY OF SOUTHAMPTON www.it-innovation.soton.ac.uk	United Kingdom
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS) www.iccs.gr	Greece
CRISISPLAN BV (CPLAN) www.crisisplan.nl	The Netherlands
ADITESS LTD. www.aditess.com	Cyprus
GAP ANALYSIS SA (GAP) www.gapanalysis.gr/	Greece
SILIXA (SIL) https://silixa.com/	United Kingdom
THALES RESEARCH & TECHNOLOGY (THALES) www.thalesgroup.com	France
TELESTO TECHNOLOGIES PLIROFORIKIS KAI EPIKOINONION EPE (TEL) www.telesto.gr	Greece
ATTIKES DIADROMES (ATTD) https://www.aodos.gr/	Greece
AQUASERV (AQS) https://aquaserv.ro/	Romania
ACCIONA Infraestructuras S.A. (ACC) https://www.acciona.com/	Spain
HELLENIC GAS TRANSMISSION SYSTEM OPERATOR (DESFA) http://www.desfa.gr/	Greece

For more information on the project, please contact Dr. Dimitris Petrantonakis (dpetr@exodussa.com), or visit the project's web site www.zonesec.eu