“Workshop on Vulnerability and Security of Critical Transport Infrastructure”

8 September 2015

Working Party on Transport Trends and Economics (WP.5)

Geneva – Palais de Nations

Towards an EU framework for the security of widezones: research project “ZONeSEC”

Dimitris Mandalozis

Strategic & Organisational Manager

Attikes Diadromes SA

ΑΤΤΙΚΗ ΟΔΟΣ

ΑΤΤΙΚΕΣ ΔΙΑΔΡΟΜΕΣ

Critical Infrastructure and Security Systems

- Critical infrastructure (e.g. highways, energy lines, pipelines) may spread over large areas/ large geographic zones.
- Depending on security systems used in critical infrastructure, illicit activities may be undetected, leading to large systemic failures and compromising financial stability, safety and security.

- Shortcomings of security systems:
  - Costs of the systems involved for the surveillance of large areas;
  - Complexity and diversity of the employed systems;
  - Efficiency, robustness and resilience;
  - Accuracy to detect illicit activity patterns;
  - Difficulty to coordinate surveillance and monitoring activities at national and transnational levels;
  - System compliance with EU policies and societal values with respect to privacy protection.

Zone Security - Highways

- Mechanisms already in place to deal with all sorts of events and illicit actions is to provide safe and easy access to the Users of the motorway.
- Threats that may escalate to crises as a result of illegal activities (in the case of a tolled motorway):
  - Demonstration, occupation, uproar
  - Sabotage
  - Vehicle hijacking
  - Terrorist act
- Sources of detection:
  - traffic intervention patrols that circulate constantly on the motorway,
  - network of cameras along the motorway,
  - telephone hotlines,
  - inductive loops under the surface of a motorway and
  - security subcontractors.

Wide Zone Security - Highways

- What about threats from infrastructure adjacent to a Highway?
  - not directly monitored by a motorway,
  - essential to include all systems in a wider, uniform approach.

- Attikes Diadromes, the operation and maintenance company of Attiki Odos, in Athens, Greece, joined the research project ZONeSEC, which is aimed at creating a multilayered digital security and surveillance platform that will operate as a Virtual Perimeter (virtual fence) around any wide-zone facility.

ZONeSEC at a glance

"Towards an EU framework for the security of Wide zones"

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

Grant agreement no: 607292

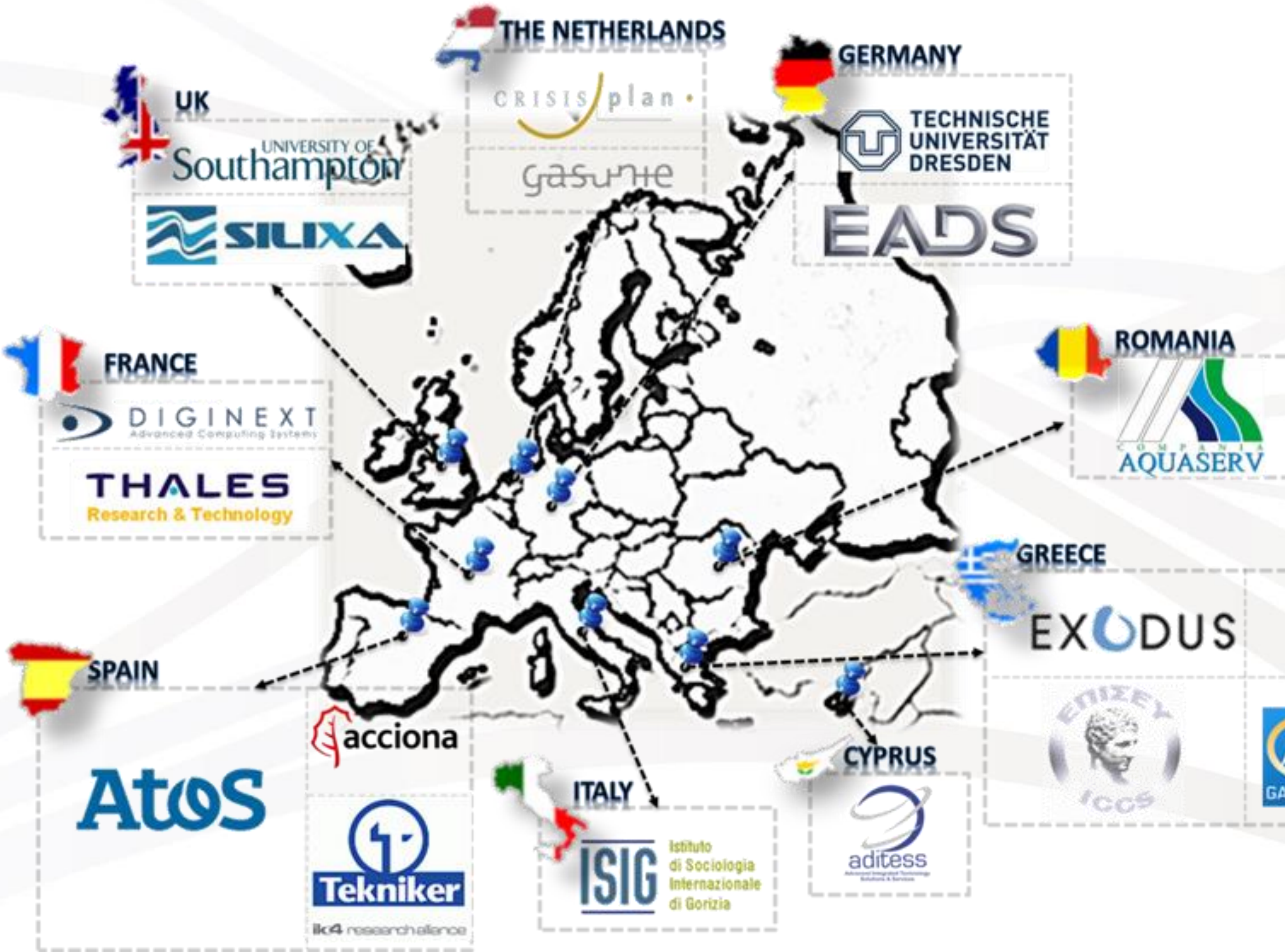
- Start date: 1 December 2014
- End date: 30 November 2018

- Total budget: 14,163,695 €
- Total funding: 9,262,732 €

ZONeSEC

ZONeSEC Partners

19 partners
9 countries
4 pilots
48 months



UK
University of Southampton
SILIXA

THE NETHERLANDS
CRISISplan
gasunie

GERMANY
TECHNISCHE UNIVERSITÄT DRESDEN
EADS

FRANCE
DIGINEXT Advanced Computing Systems
THALES Research & Technology

ROMANIA
COMPANIA AQUASERV

GREECE
EXODUS
Telesto Technologies
ΕΠΙΣΕΥ ICCS
Analysis GAP ANALYSIS S.A
ΑΤΤΙΚΕΣ ΔΙΑΔΡΟΜΕΣ

SPAIN
AtoS
acciona
Tekniker ik4 researchalliance

ITALY
ISIG Istituto di Sociologia Internazionale di Gorizia

CYPRUS
aditess

ZONeSEC description

- ZONeSEC aims at integrating affordable ground and airborne sensor observation technologies for the critical surveillance of large spatial areas of high economic value in Europe.
- A resilient and seamless communication platform will integrate all mechanisms that are already in place, to convey illicit events via multiple mechanisms such as audio, video, e-mail and other methods, over a common multilayer interface:
  - Secure and interoperable observation data and information management services using open standards with the aim of cost-effectively reusing them.
  - Knowledge Base (KB), focused on large-scale surveillance with high-performance detection of localized abnormal activities and alerts
  - high-level data fusion and reasoning with reduced uncertainties and false alerts, artificial Intelligence and proprietary algorithms.

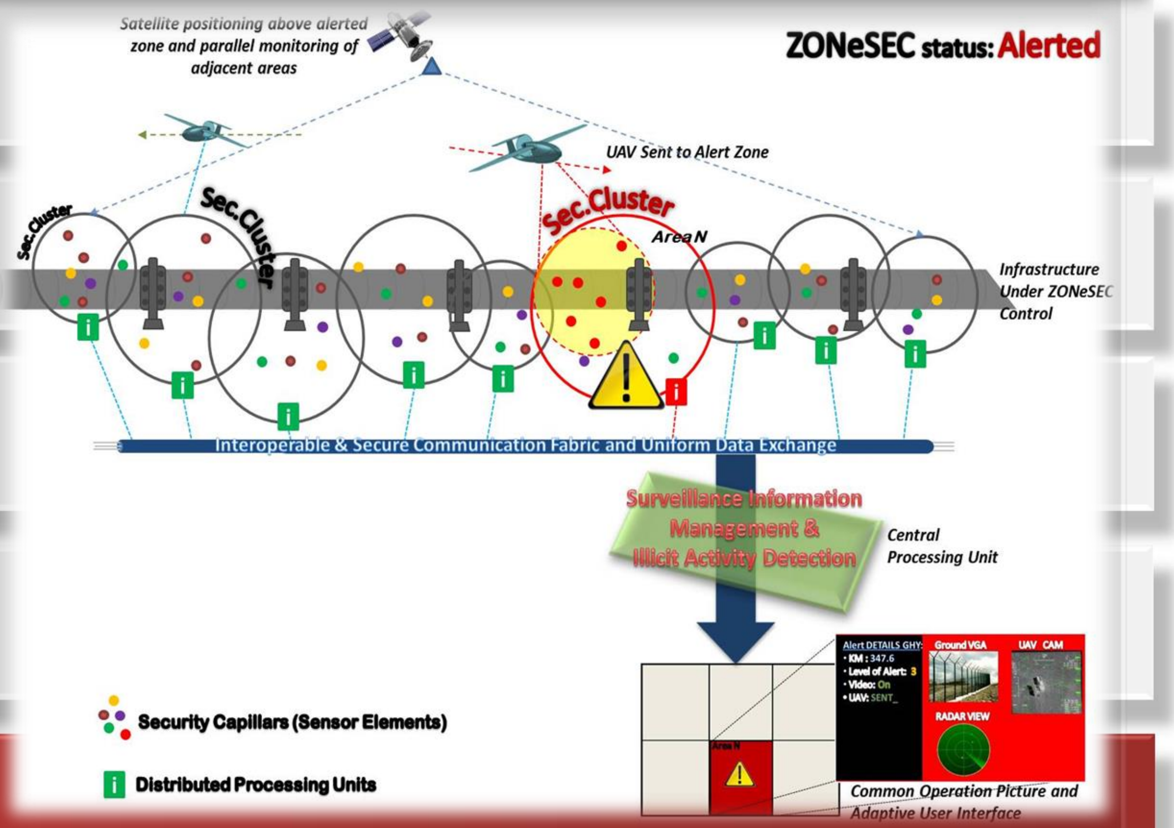
ZONeSEC Alerts

- Only actual events are processed (with low false alarm rate) into a user-friendly Graphical User Interface (GUI).
- The GUI will also:
  - define and modify zones of interest and sensitivities,
  - manage and review databases,
  - provide multilevel management tools: observing scenes from video cameras in real time, interaction with system security features such as intrusion alarms or real time and archived video and data forensics, complete system administration, etc.
- The platform will be tested in the detection of illegal unauthorized entrances/ trespassing, vandalism or deployment of harmful devices on installations.

ZONeSEC Operations

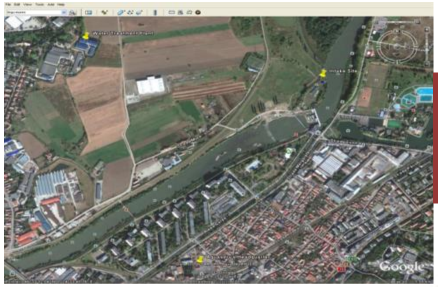
ZONeSEC System Elements (ALERTED Operation)

HIGHWAYS	ΑΤΤΙΚΕΣ ΔΙΑΔΡΟΜΕΣ acciona
RAILWAYS	ΑΤΤΙΚΕΣ ΔΙΑΔΡΟΜΕΣ acciona
GAS PIPELINES	Nord Stream nationalgrid Open Grid Europe The Gas Wheel gasunie
WATER	COMPANIA AQUASERV
OIL PIPELINES	ΑΤΤΙΚΕΣ ΔΙΑΔΡΟΜΕΣ

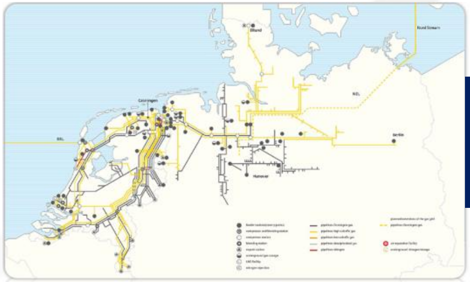

Satellite positioning above alerted zone and parallel monitoring of adjacent areas
ZONeSEC status: Alerted
UAV Sent to Alert Zone
Sec.Cluster
Sec.Cluster
Sec.Cluster
Area N
Infrastructure Under ZONeSEC Control
Interoperable & Secure Communication Fabric and Uniform Data Exchange
Surveillance Information Management & Illicit Activity Detection
Central Processing Unit
Security Capillars (Sensor Elements)
Distributed Processing Units
Area N
Alert DETAILS GHY:
• KM : 347.6
• Level of Alert: 3
• Video: On
• UAV: SENT_
Ground VGA
UAV CAM
RADAR VIEW
Common Operation Picture and Adaptive User Interface

Four Pilots

Pilot 1. Highway, Railtrack and Oil Pipeline - ATTIKES DIADROMES



Pilot 2. Water pipelines Surveillance - AQUASERV

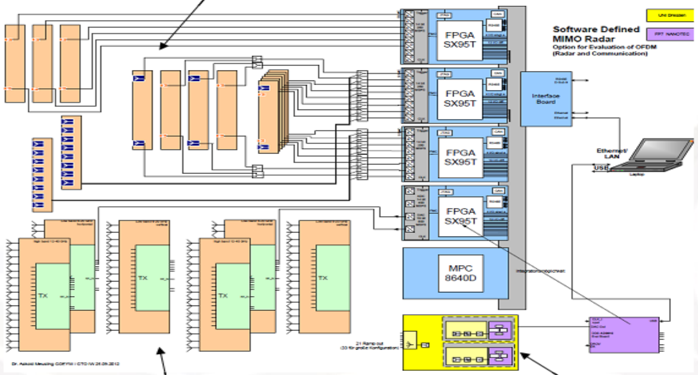


Pilot 3. Transnational Gas Pipeline Networks - GASUNIE

Pilot 4. Incident on a Highway with implications on neighboring Railtracks and Energy lines - ACCIONA

ZONeSEC Technologies (1/3)

- Software defined MIMO Radar



Ultra-broadband receivers (BiCMOS)

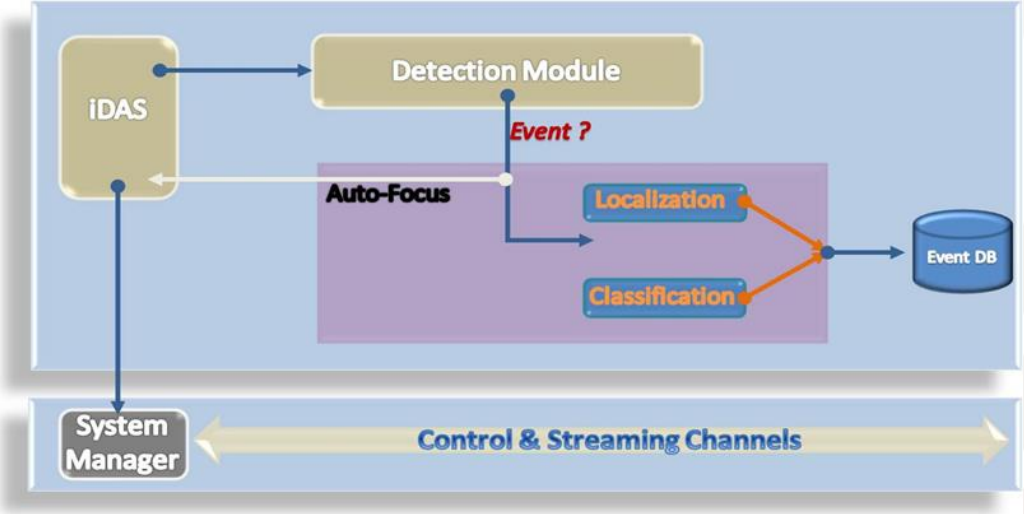
MIMO signal processing (FPGA)

Multiband antennas

Ultra-broadband transmitters (GaN, MEMS BiCMOS)

Ultra-broadband signal generation (BiCMOS)

- Optical Technology for Illicit Activity and Early Threat Detection (iDAS)



iDAS

Detection Module

Event ?

Auto-Focus

Localization

Classification

Event DB

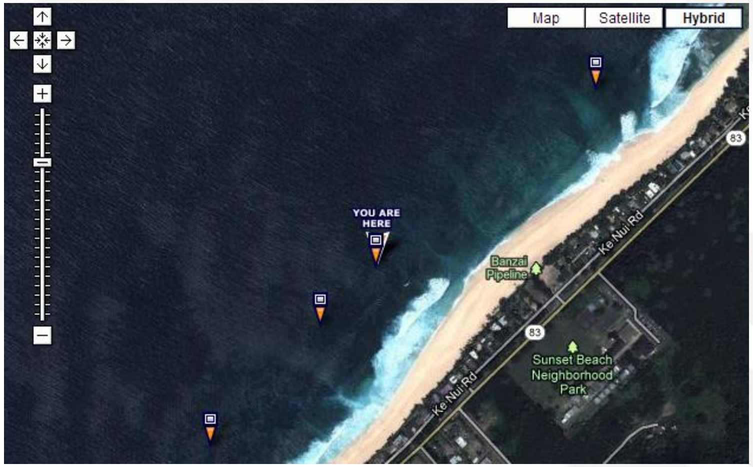
System Manager

Control & Streaming Channels

ZONeSEC Technologies (2/3)

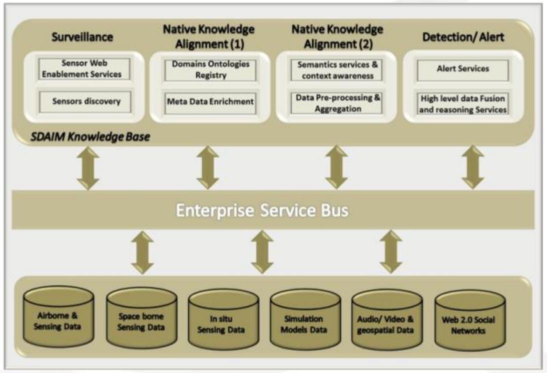
- Unmanned Aerial Vehicles (Multi-rotor mini-UAV)

- Satellite Imagery & Illicit Activity Pattern Detection and Early Identification of Potential Threats using Imaging (eg. Video-based state detection and monitoring, Hyper-spectral imaging)



ZONeSEC Technologies (3/3)

- Large Scale, Uniform and Secure Communications
  - Wired Sensors
  - Wireless Sensors
  - Cellular and Satellite Interfaced Sensors



Surveillance: Sensor Web Enablement Services; Sensors discovery

Native Knowledge Alignment (1): Domains Ontologies Registry; Meta Data Enrichment

Native Knowledge Alignment (2): Semantics services & context awareness; Data Pre-processing & Aggregation

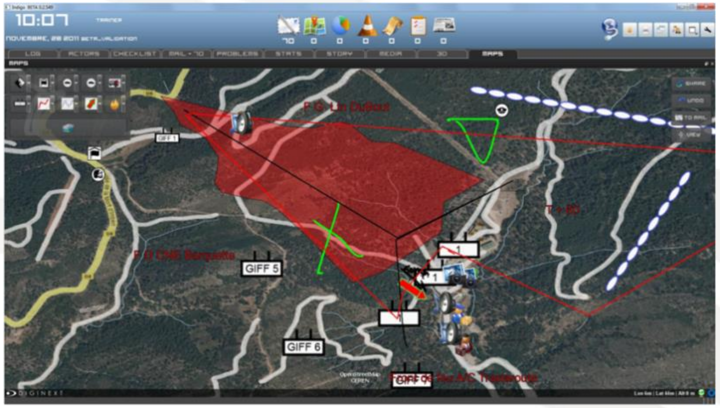
Detection/ Alert: Alert Services; High level data Fusion and reasoning Services

SDAIM Knowledge Base

Enterprise Service Bus

Airborne & Sensing Data; Space borne Sensing Data; In situ Sensing Data; Simulation Models Data; Audio/ Video & geospatial Data; Web 2.0 Social Networks

- iOC (intelligent Operations Centre)
  - SDAIM - Surveillance, Detection and Alerts Information Management, ZONeSEC Knowledge Base
  - Common Operational Picture and Adaptive User Interfaces



For more information about the project and the participants, please visit:

http://cordis.europa.eu/project/rcn/192560_en.html

http://www.zonesec.eu

Thank you!