# Detection and response to drone overflight and crashes

- *Aldo Bonsignore*
- *A.bonsignore@idscorporation.com*
- *+390633217414*
- *IDS – Ingegneria Dei Sistemi S.p.A.*
  *Via Flaminia, 1068*
  *00189 Rome*
  *Italy*

- Role: *S/T provider*

- Proposal activity: ***SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe***

# IDS contribution

Radar Network

Detection

EO/IR + Jammers

Identification/Contrast

Console

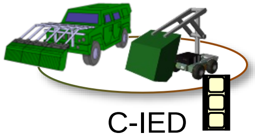
Command & Control

- *Drone detection, classification and tracking*
- *Jamming or spoofing*

# Project participants

Meteo Radar (volcanic ash)

Anti drone


C-IED

Hostile Fire Locator

Thru-Wall

IDS may play the role of partner providing the following expertise:

- 30 years of experience in radar based solutions. Design and provision of tailor-made radar products and services for detection of volcanic dusts, obstacle detection on the railway tracks, object detection behind walls, **detection of hostile drones for critical infrastructures protection**, IED (improvised explosive device) detection for route clearance operations, detection of bullets fired by snipers and mortars.

- Design and development of SW applications which aims to obtain rendering of information contained in signals and imagery acquired by radar, EO/IR, MS/HS sensors in the field of defense, security and environmental domain. Key technologies are Target Signature (DB) Management, Real-Time, Target Detection/Change Detection and Tracking, Automatic Target Recognition (ATR), Machine Learning, Multisensor Data Fusion Engine.

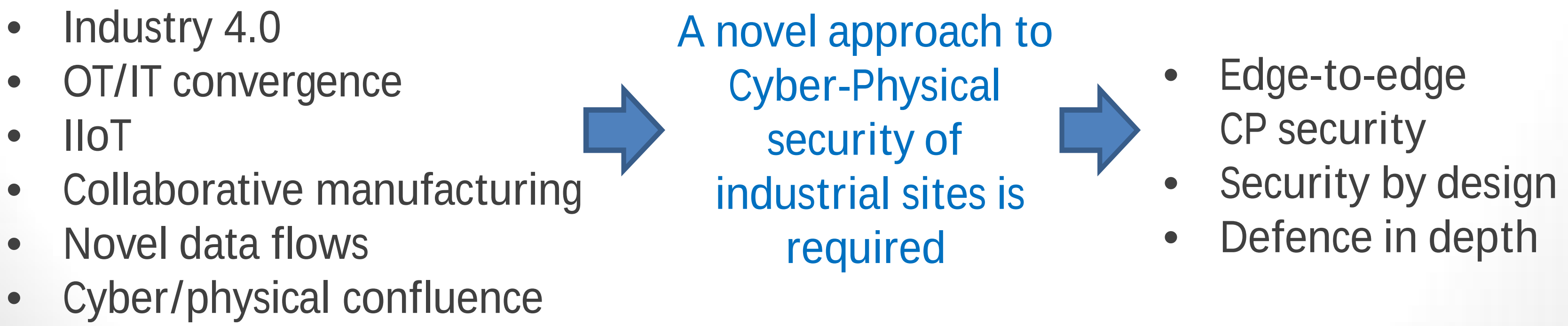
- Detection an localization of GNSS jammers by mans of IDS GNOME platform

- Advanced development stage of a GNSS spoofer as an a effector against drone threats

# SENSEI - SEcuriNg SEnsitive Industrial sites

- Charidimos Chaintoutis – *charidimos.chaintoutis@eulambia.com*
- EULAMBIA Advanced Technologies
- Role: *Proposal coordinator*

SU-INFRA01-2019 – *“Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe”* - Sensitive industrial sites

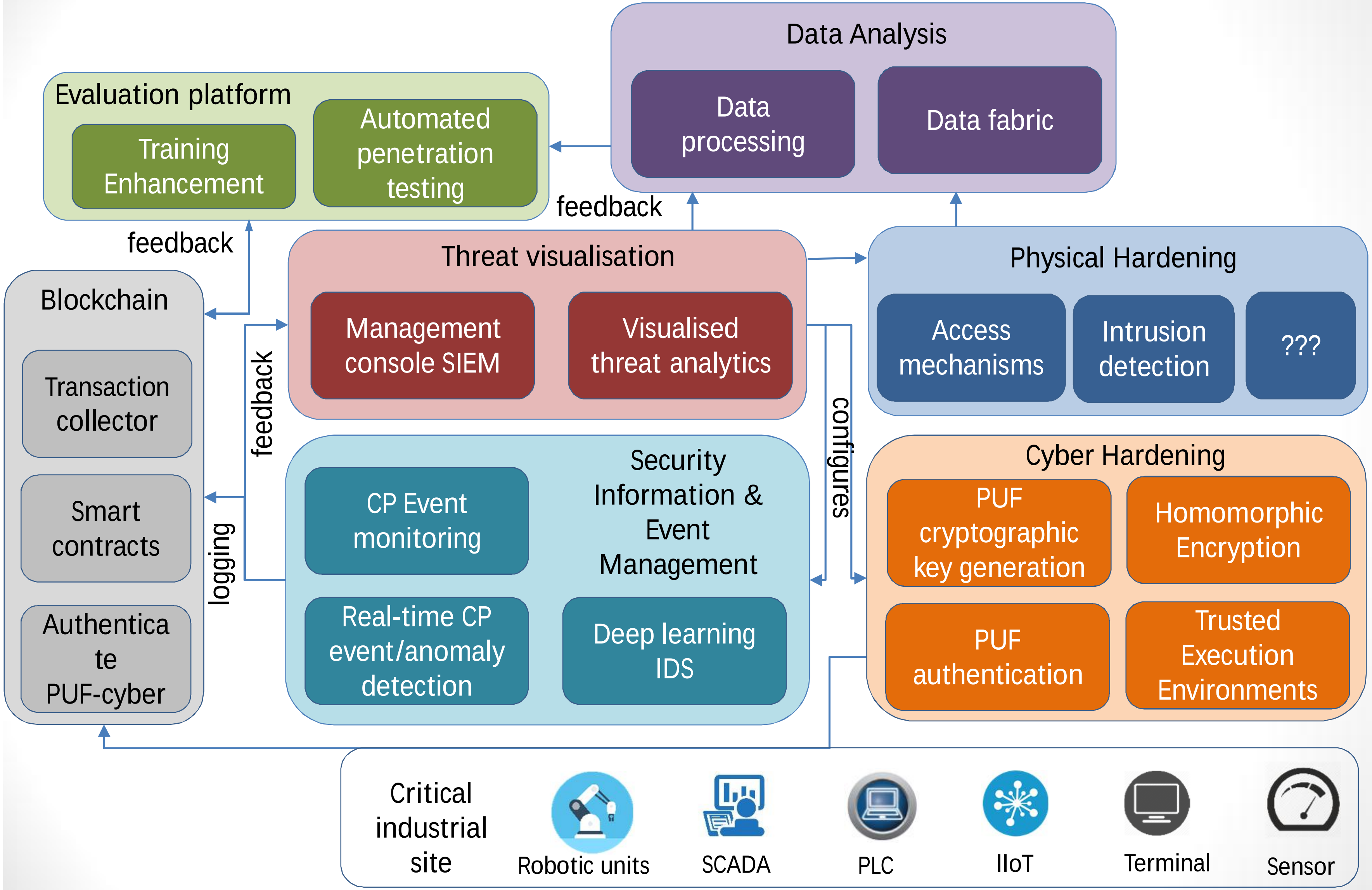


- Industry 4.0
- OT/IT convergence
- IIoT
- Collaborative manufacturing
- Novel data flows
- Cyber/physical confluence

A novel approach to Cyber-Physical security of industrial sites is required

- Edge-to-edge CP security
- Security by design
- Defence in depth

# SENSEI general concept



SMI2G 2019, 29-30 January 2019, Brussels

Charidimos Chaintoutis - charidimos.chaintoutis@eulambia.com

# SENSEI participants

- Existing partners cover cyber security aspects for IT
  - *PUFs, Blockchain, IDS/ADS, SIEM, TEE, HE*

- Looking for partners with the following expertise:
  - *Manufacturing/industrial systems*
    - *Security of legacy systems*
    - *OT/IT convergence*
    - *Industry 4.0*
  - *Novel physical security solutions (detection, response, mitigation)*
  - *Policy planning & engagement of the civil society*
  - *End User (Critical industrial facilities)*

# Integrated Model for Hospital Protection and Resilience

Gemelli

Fondazione Policlinico Universitario A. Gemelli
Università Cattolica del Sacro Cuore

- *Daniele Gui, MD, FACS, AAST*
- *daniele.gui@unicatt.it*
- *UCSC - Università Cattolica del Sacro Cuore (Medical School)*

- Role: *Scientific Coordinator*

- Proposal activity: SU-INFRA01-2018 *(Health Sector)*

# Proposal idea/content

- The proposed project wants to provide an integrated resilience approach and model to the Health Critical System

- We start from the identification of threats that specifically target health systems (with a 360 degrees approach, from cyber to physical) and with an eye open to the emergency functions of the Health System
- We move to the the identification of cost-effective technical solutions to be piloted and validated in the relevant Health environment
- Essential part of the idea, side-by-side with technical solutions, is a model for training of stakeholders and health structure staff and for building awarness
- Threats sometimes become true – therefore protection and prevention are crucial but it is necessary to have Plans B to restore situations to normality and control damage

# Project participants

- Proposed coordinator: *TBD*
- Scientific Coordinator: UCSC - *Università Cattolica del Sacro Cuore (expertise offered: University Hospital facility, simulation centre, wide experience in medical demos and validation on site, CBRNe response, Hospital testbed, ethical monitoring)*
- *Other partners: discussions ongoing with Engineering Company, Large Enterprise, Institutions and Authorities*
- Looking for <u>HIGHLY INNOVATIVE </u>partners with the following expertise/ technology/ application field:
  - *Blockchain (SME)*
  - *Threat intelligence (SME)*
  - *Cyber Security tools, including artificial intelligence (SME)*
  - *Social, societal and legal framework (SME)*
  - *Providers of tools for communication to the Health workers and to the population (SME)*
  - *Software and systems development, DSS, EMS, etc. specifically for Health applications (SME)*

# Joint physical-cyber resilience analytics, simulation and improvement process for renewable energy systems

- *Ivo Haering*
- *haering@emi.fraunhofer.de*
- *Fraunhofer EMI*
- Role: *Proposal coordinator or Technical WP leader*

- Proposal activity: *SU-INFRA-2019*
- *Open sector selected: Green energy supply (sub) systems and “local“ systems*

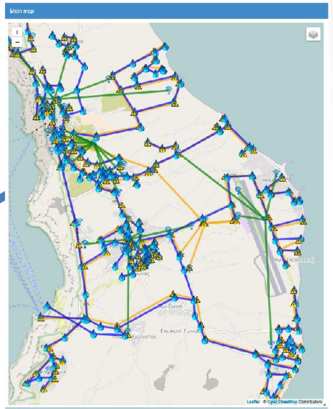
*Disclaimer: with the submission of this presentation the consent is given by its author for the organisers to distribute the presentation.*

Contact: haering@emi.fraunhofer.de, Fraunhofer EMI

# Proposal idea/content: Targeted innovations using resilience cycle; focus on key green energy grid elements and (local) (independent) subgrids;

physical

* Analytical and
* Engineering assessment
* Local energy grids, selected
entities



* Targeted Physical
robustness
and mitigation

Prevent cascades

by *operator actions post event

physical & cyber

disruption

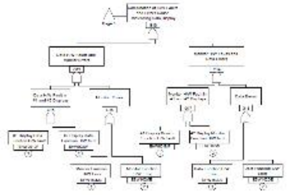
Mainly: Improved
response and recovery

Online monitoring
For *targeted response

Event analysis (EA)

cyber

Mainly: Detection,
prevention, protection



*cyber
fault tree analysis (FTA)

Fast grid simultion, up
to *real time resiliens analytics
and support to bounce forward/
learn

# Project participants

- Proposed coordinator/ End users wanted: European leading green grid operators and energy generators (e.g. offshore windmill energy operators and transmission grid operators like Tennet, EN-BW, local green high-tech supply companies or compontent providers, e.g. Sonnen, Tesla)
- Other participants: Academic experts in smart (local) energy grids, simulation models, Physical protection, ML/AI SME

- Looking for partners with the following expertise/ technology/ application field:
  - Companies with green solutions in the electricity grid domain, e.g. Large scale energy storgage systems, offshore installations, virtual green power plants, power-to-gas facilities,
  - Communities, urban quarters or cooperations with independent energy supply
  - *Effects on citizens and Human factors*
  - *Disaster management for utility networks*

Contact: haering@emi.fraunhofer.de, Fraunhofer EMI

# SU-INFRA01-2019: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

- *Prof. William Hynes*
- *William.hynes@futureanalytics.ie*
- *Future Analytics Consulting Ltd., Dublin, Ireland.*
- Role: *Work Package Lead*

- Proposal activity: SU-INFRA01-2019:
  Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

# A Cyclical Approach to the Development of Well Informed Tools and Technologies

- *Assess interdependent physical and cyber threats and incidents and cascading risks.*
- *Demonstrate accuracy of risk assessment approach using examples and scenarios of real life and compare results with other risk assessment methodologies.*
- *Develop improved real-time, evidence-based security management.*
- *Provide policy planning, engagement of civil society, and investment measures.*
- *FAC can deploy expertise gained from similar previous projects:*
  - *Reserach and analysis into resilence of CI.*
  - *Wide end-user / stakeholder consultation regarding the effecitveness of existing research, methods, and related technologies.*
  - *Brainstorming and analysis of the potential for combining best practice methods and approach.*
  - *Development of pilot methods / case studies to measure the impact of new proposals and pontential gaps – informed by consultation and analysis.*

# Project participants

- Proposed coordinator: *N/A*
- Partners / Other participants:
  Future Analytics Consulting – Work Package Lead
- Looking for partners with the following expertise/ technology/ application field:
  - EU wide academic researchers
  - Engineering
  - Risk Management Specialists
  - Energy and Infrastructure Specialists
  - Municipal/Local and Regional Authorities
  - Representatives from key citizen groups

# Technologies for Detection, Surveillance and Security in Critical Infrastructures

- *Dr Rodoula Makri*
- *rodia@iccs.gr*

- *Institute of Communications & Computer Systems - National Technical University of Athens (Microwaves & Fiber Optics Lab)*

- Role: *Scientific Coordinator / Technical coordinator - WP leader or S/T provider partner*

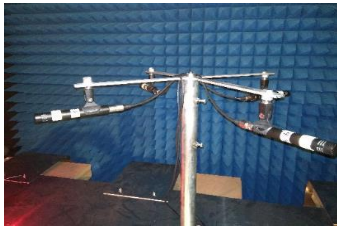
- Proposal activity:
- *SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*

# Experience of ICCS as S/T Provider

**Design and Development of Special Purpose Radars and relevant Signal Processing**

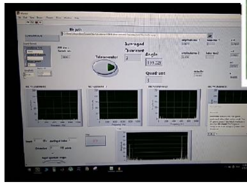
- ***Detection of small flying objects and airborne threats with low RCS (i.e. small UAVs or drones, unmanned devices) based on active and passive sensors***
  - monitoring and detection through combined small Doppler radars and acoustic devices
  - Potential intrusion events through signal processing and beamforming

- ***Electronic Surveillance Systems and anti-jamming techniques***
  - for the surveillance and management of the EM spectrum
  - for heavy loaded electromagnetic environments in VHF and UHF bands
  - Multistatic UHF Early warning radar and Data Fusion of multiple multistatic radars



- ***Computational EM scattering problems***
  - Inverse scattering problems - EM scattering problems by jet engine inlets
- ***Extensive experience in SAR image / signal processing***
  - Investigation of the feasibility of using radar signatures for targets classification and identification
  - 2D and 3D radio-coverage modeling in cellular wireless systems studies

- ***Detection of hidden alive beings within vehicles or containers***
  - With UWB radars and broadband acoustic sensors
- ***Life detector radars for people trapped in buildings***
  - i.e. in earthquakes - Various frequencies 433 MHz, 2,45GHz, 10GHz



# Potential Cooperations

Most recent H2020 Security projects that we are involved in:

- *RESISTO (2018-2021): RESIlience enhancement and risk control platform for communication infraSTructure Operators (CIP-01-2016-2017 – INFRA)*
- *iBorderCtrl (2016-2019): Intelligent Portable Border Control System (BES-5-2015) where we are Technical Coordinator*

- Seek to cooperate with:

- Administrative or Project Coordinator
- Looking for partners with the following expertise / application field:
  - data fusion topics, Decision Support Systems or Integrators
  - academic institutions/ research centers; wireless networks, radar and other sensors processing, satellite, data fusion
  - Providers / companies : offering surveillance platforms
  - SMEs and practitioners to incorporate user / application experience

Rodoula Makri, rodia@iccs.gr

# Drone swarms to improve security in critical infrastructures

- *Marcos Sacristán, Javier Gutiérrez, Clara Ayora:*
  - *marcos.sacristan@treetk.com*
  - *javier.gutierrez@treetk.com*
  - *clara.ayora@treetk.com*

- *Tree Technology - www.treetk.com (former Treelogic)*
  - *Spanish SME*
- Role: *Coordinator (possible)*

  *WP leader*

  *Technical provider (Computer Vision, AI techniques)*

- Proposal activity: *SU-INFRA01-2019*

# Proposal idea/content

- *Increase safety and security in transport infrastructures by exploiting the potential of drone swarms*
- *Efficient and effective coordination and simultaneous management of a number of different types of drones*
  - *Detection, identification and tracking of potential threats (objects, vehicles, humans or even animals of a certain size)*
  - *Monitoring of daily operations and infrastructure inspection*
- *Use of edge technologies to provide a faster response*
- *Integration with existing IT systems (security, control, management, etc.)*

Marcos Sacristán (TREE TECHNOLOGY) – marcos.sacristan@treetk.com

# Project participants

- Proposed coordinator: *TREE Technology (or Other)*
- Approach under discussion with*:*
  - *End users – IC operators*
  - *Swarm management experts*
  - *Standardisation bodies*
  - *Secure communications researchers*
  - *Legal & ethics*

- Looking for partners with the following expertise/ technology/ application field:
  - *Addtional IC operators*
  - *Experts in cyber-security*
  - *Technology providers/integrators*
  - *Drone manufacturers*

Marcos Sacristán (TREE TECHNOLOGY) – marcos.sacristan@treetk.com

# *System of Intelligent Sensors networks for critical infrastructures security*

- ***Nizar TOULEIMAT***
- ***nizar.touleimat@cea.fr***
- ***CEAtech – List Institute***
- Role: *Proposal coordinator / WP leader, to define later…*
- Proposal activity:
  - ***SU-INFRA01-2019****: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*

*(**SU-INFRA02-2019**: Security for smart and safe cities, including for public spaces)*

# *System of Intelligent Sensors networks for critical infrastructures security*

- *changing risks & emergence of new threats => not detected by video surveillance and other security systems*

- *necessity of new development & innovative products to guarantee the protection of critical infrastructures*

- ***multi-functional intelligent sensor network system, providing CBRN and Radio Frequency signal recording, intelligent data collection and processing for the purpose of reporting qualified alarms to an operator.***

# Project participants

- Proposed coordinator: ***CEAtech – List***
- Partners / Other participants:
    - **CEAtech (France)**: French largest application-oriented RTO. Specialist in Data Analysis and Systems Intelligence and in CBRN Sensors and Electronic Architectures
    - **Syrlinks (France)**: industrial, specialist of radio communications systems development, particularly in the space and military fields
- Looking for partners with the following expertise/ technology/ application field:
    - *Application sites and infrastructures*
    - *Legal & administrative*
    - *System integrator&operator*
    - <….>

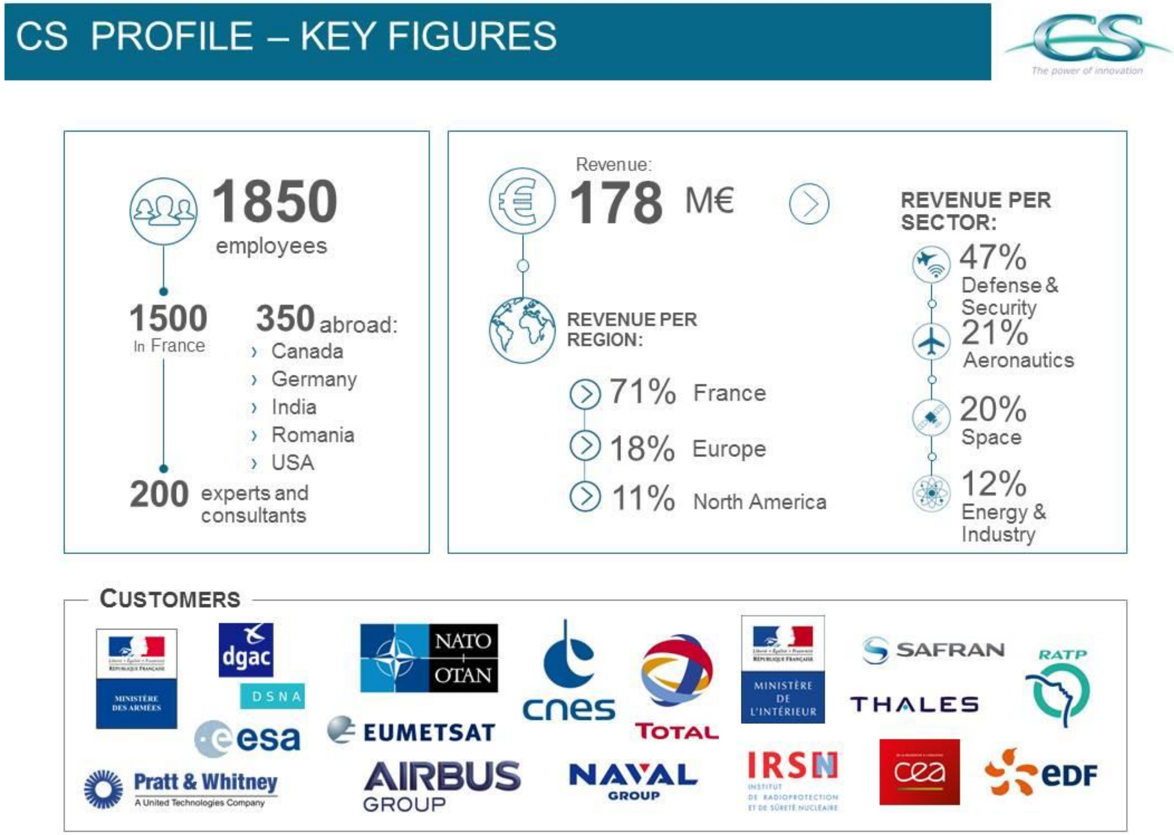
# UNITY 360

UNITY
Unify your Securities

- *Jean-Marie PILLOT*
- *jean-marie.pillot@c-s.fr*
- *CS Communication & Systems*
- *Proposal coordinator*

- Proposal activity: *SU-INFRA01-2018-2019-2020:*

  *Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*



CS PROFILE – KEY FIGURES

CS The power of innovation

1850 employees

1500 In France

350 abroad:
- Canada
- Germany
- India
- Romania
- USA

200 experts and consultants

Revenue: 178 M€

REVENUE PER REGION:

| | |
|---|---|
| 71% | France |
| 18% | Europe |
| 11% | North America |

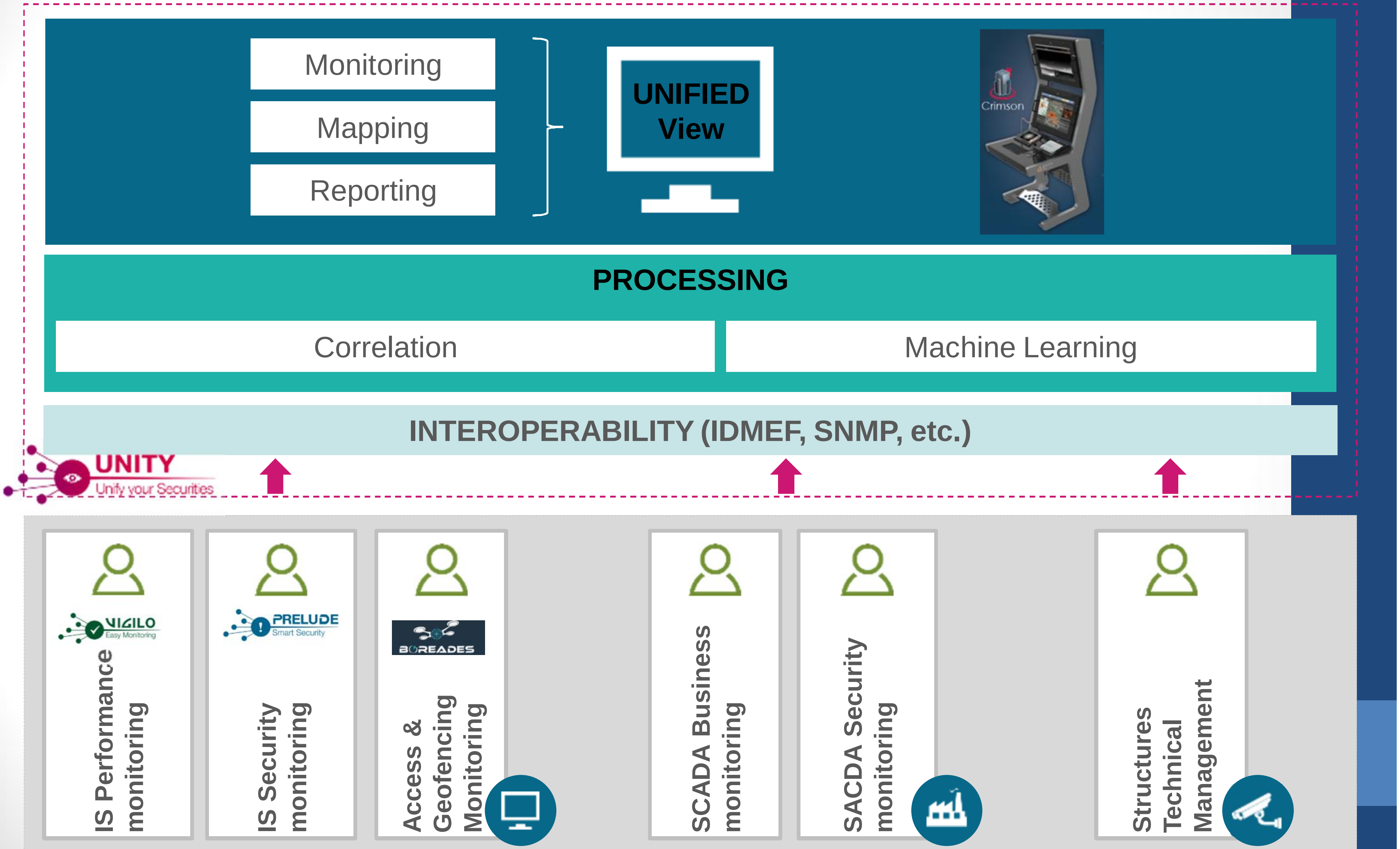
REVENUE PER SECTOR:

| | |
|---|---|
| 47% | Defense & Security |
| 21% | Aeronautics |
| 20% | Space |
| 12% | Energy & Industry |

CUSTOMERS

Jean-Marie PILLOT – VP BusDev CS: jean-marie.pillot@c-s.fr +33 673 862 933

# UNITY : *UNIFY YOUR SECURITY*



Monitoring

Mapping

Reporting

**UNIFIED View**

Crimson

**PROCESSING**

Correlation

Machine Learning

**INTEROPERABILITY (IDMEF, SNMP, etc.)**

UNITY
Unify your Securities

VIGILO Easy Monitoring
**IS Performance monitoring**

PRELUDE Smart Security
**IS Security monitoring**

BOREADES
**Access & Geofencing Monitoring**

**SCADA Business monitoring**

**SACDA Security monitoring**

**Structure Technical Management**

Jean-Marie PILLOT – VP BusDev CS: jean-marie.pillot@c-s.fr  +33 673 862 933

# Project participants

- Proposed coordinator: *CS SI*
- The Unity concept could be the SU-INFRA01 monitoring framework for :
  - Centralization, storage, indexation of security information,
  - Real-time, evidence-based security management of physical and cyber threats
  - Cyber threats and incidents correlation
  - Reporting, Analysis, Forensics
  - Response and mitigation
- CS expertise :
  - Editor of C2, SIEM and NMS products, open-source expertise
  - Expertise in international security standards (IDMEF/IODEF, STIX/TAXII)
  - H2020 track-record
- Looking for additional Partners:
  - *Infrastructure operators*
  - *AI Laboratory*
  - *SCADA specialist*
- www.prelude-siem.com, www.vigilo-nms.com , www.secef.net, http://boreades.fr/#news , https://aladdin2020.eu/

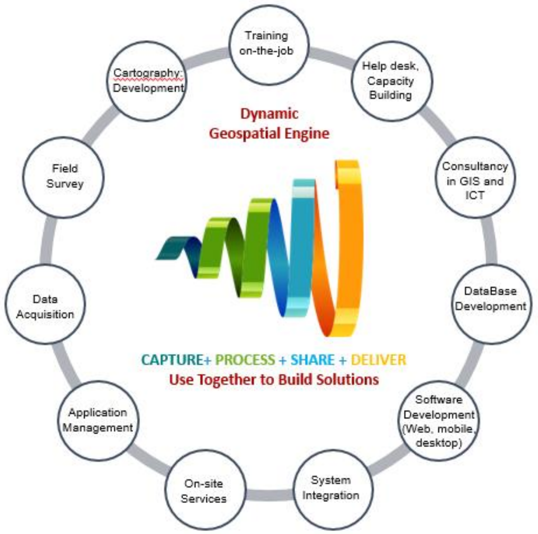
Jean-Marie PILLOT – VP BusDev CS: jean-marie.pillot@c-s.fr +33 673 862 933

# GENEGIS GI –SU-INFRA01-2019

- *Dott. Francesca Sapio*
- *Email:* f.sapio@genegis.net
- *Genegis GI srl* http://www.genegis.net/
- Role: *WP leader, Task lead*
- Proposal activity: SU-INFRA01-2019 *: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*

# GENEGIS GI –SU-INFRA01-2019

*GENEGIS GI* is an Italian SME providing software solutions, mainly in the Geo ICT area and covering the entire project life cycle with the appropriate technology, from the acquisition of raw data to its processing and integration, to the development of dedicated software applications.

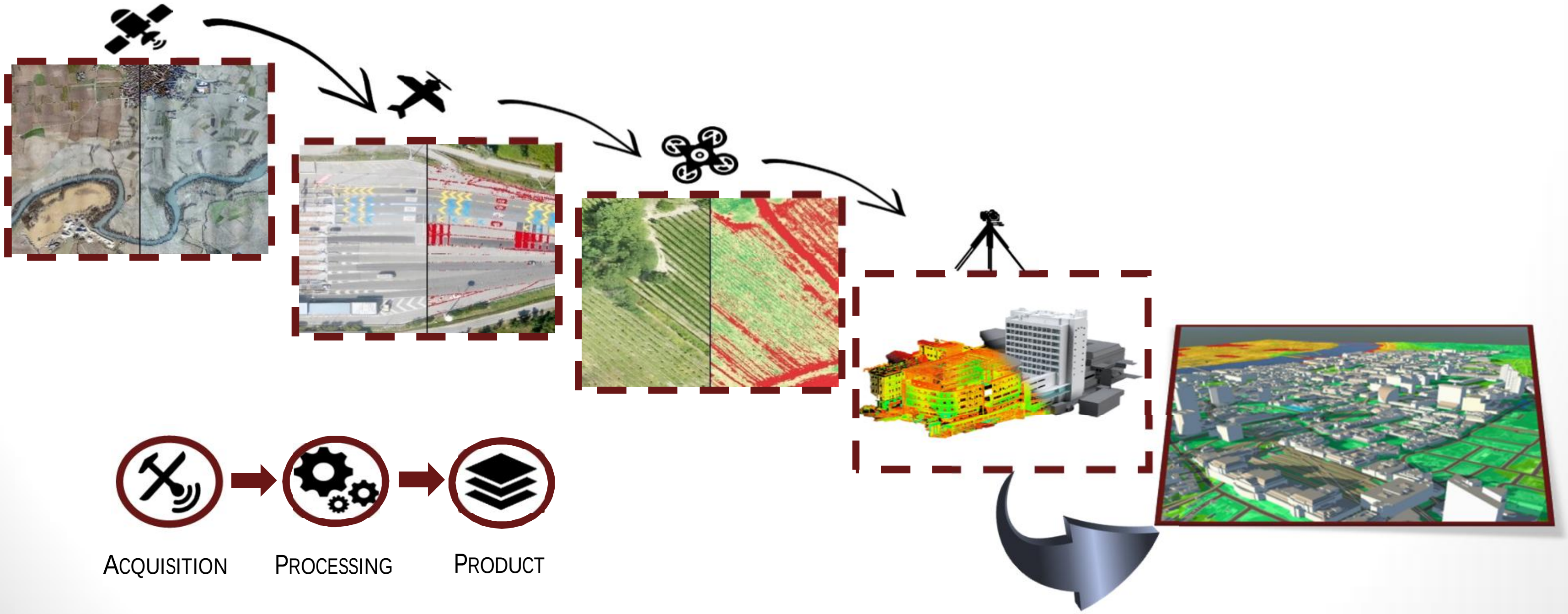

Training on-the-job
Help desk, Capacity Building
Consultancy in GIS and ICT
DataBase Development
Software Development (Web, mobile, desktop)
System Integration
On-site Services
Application Management
Data Acquisition
Field Survey
Cartography Development
Dynamic Geospatial Engine
CAPTURE+ PROCESS + SHARE + DELIVER
Use Together to Build Solutions

The research and innovation activity has led GeneGIS GI to collaborate with universities, main organizations and large companies, in Italy and all over the world, on many projects.
These are some of the most important ones:

- H2020 SME Instrument Phase 1: TRUST - TRUck Suistanable Transport - Innovative project for management of Contract Logistics
- H2020-SC1-2016 - Big Data supporting Public Health policies: PULSE Participatory Urban Living for Sustainable Environments.
- H2020-SC4-2016 - LOGISTAR - Enhanced data management techniques for real time logistics planning and scheduling.

# GENEGIS GI –SU-INFRA01-2019

- GENEGIS GI can offer their expertice:
  - *Vulnerability and resilience assesment tool for CI including DATA ACQUISITION using MULTI PLATFORM ( Satellite, Airbone, and Drone) and MULTI SENSORS (Multispectral, Thermal and Laser Scanning)*



ACQUISITION → PROCESSING → PRODUCT

# CISEC

- Marcos Álvarez
- malvarez@gradiant.org
- GRADIANT (RTO, Spain)
- Role: *Proposal coordinator; Technical coordinator; WP leader; S/T provider*

- Proposal activity: *SU-INFRA02-2019: Security for Smart Cities and "soft" targets in Smart Cities*

# Proposal idea/content

- *We propose a support system for improving the security in open and crowded areas based on multiple data sources with the following characteristics*
  - *Autonomous operation*
  - *Automatic alerts on suspicious objects and activities detection*
  - *Interconnection and integration with city smart systems*
- *Including Video analytics by Gradiant**
  - *Autonomous Surveillance video stations based on the combination of fixed and mobile (fixed cameras + drones, etc.)*
  - *Threat evaluation based on heterogenous and social media data source (video or otherwise)*

# Project participants

- Proposed coordinator: *GRADIANT*
- Looking for:
  - *City councils*
  - *Infrastructure operators*
  - *Smart City platform/system providers*
  - *Integrators*
  - *Security practitioners*
  - *Secure communication and data storage*
  - *Other technologies for detecting dangerous or toxic devices*
  - *IoT expert*

# < Attacks on Urban Rail Transport >

- *Recep AYDIN*
- *(recep.aydin@bursa.bel.tr )*
- *BURSA METROPOLITAN MUNICIPALITY*
- Role:
  - *Proposal coordinator and/or WP leader,*
- Proposal activity:
  - SU-INFRA02-2019 - *Security for smart and safe cities, including for public spaces*

# Proposal idea/content

- This proposal's objective is
- To develop an open&online platform that integrates already existing data bases (multi source video- visual, numeric, GIS) and
- to share, process, mine and manage the information among related stakeholders, such as;
  - National Police authorities
  - Metropolitan Municipalities
  - Security and Emergency Management Coordination Center
  - Other relevant stakeholders (in case of a need firefighters, ambulance centers, etc)

In order to

- Detect and monitor phsical and cyber threats
- to simulate the possible scenarios with AR applications,
- finally to provide useful information, in advence, to the related stakeholders

- One of the demonstration is planned to simulated in our city BURSA

We plan to generate a comphrenisive solutions to the possible attacks on urban rail transport systems

- Both phsical and cyber treats will be considered where these threats could be named as:
  - Cyber attacks to signaling systems, heating or lighting systems
  - Physical attacks (Drone threats, Bomb attacks like in Brussels)

# Project participants

Proposed coordinator:

*BURSA METROPOLITAN MUNICIPALITY*

- Partners / Other participants:
  - National Police authorities- TR
  - Metropolitan Municipalities- TR-Bursa
  - Security and Emergency Management Coordination Center-TR

- Looking for partners with the following expertise/ technology/ application field:
  - *Universities*
  - Augmented reality solution providers
  - Excellence in artificial intelligence with previous experience in emergency management issues.
  - Drone & unmanned air vehicle operators /controllers /experts
  - Metropolitan Municipalities

# Methods to detect weapons, and toxic substances

- *Aldo Bonsignore*
- *A.bonsignore@idscorporation.com*
- *+390633217414*
- *IDS – Ingegneria Dei Sistemi S.p.A.*
  *Via Flaminia, 1068*
  *00189 Rome*
  *Italy*

- Role: *S/T provider*

- Proposal activity: SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

# IDS contribution

Hostile Fire Locator

Drone mounted gamma rays and nerve gas sensors

- *Toxic substance detection*
- *Weapon detection*

# Project participants

IDS may play the role of partner providing the following expertise:

- 30 years of experience in radar based solutions. Design and provision of tailor-made radar products and services for detection of volcanic dusts, obstacle detection on the railway tracks, object detection behind walls, detection of hostile drones for critical infrastructures protection, IED (improvised explosive device) detection for route clearance operations, **detection of bullets fired by snipers and mortars.**

- Development of PAYLOADS for DRONES having the capability to:
  - Detect the presence of *gamma rays*
  - Detect the presence of *chemical aggressive substances*
  - Operate at *low and high temperature From* -20°C to +50°C
  - Provide information of the *GPS position of the detected threats*
  - Be waterproof

# SU-INFRA02 proposal idea

- *George Boultadakis: [george.boultadakis@eurodyn.com]*
- *Anna Malamou: [anna.malamou@eurodyn.com]*
- *European Dynamics*
- *Role:  WP leader*

- Proposal activity: *SU-INFRA02-2019: Security for smart and safe cities, including for public spaces*

# Proposal idea/content

**Sub-topic 4**

*Idea: An integrated platform of different components to offer a common cybersecurity management approach by solving interoperability issues, ensuring secure data exchange and storage in order to secure cities against a variety of threats.*

European Dynamics to participate as partner/ WP leader offering:

-as a major provider of IT solutions and services in the area of security/defense and Cyber Security (DSS/ C2 systems commercially and in H2020*);

-as a major provider of data management platform for different vertical applications (commercially):

- *Elastic / open **cloud architecture** capable of **storing and processing big datasets** coming from public service operators and security practitioners (i.e. ministries, law enforcements authorities, etc.) to support complex **data fusion and data-driven decision**.*
- ***Real-time big data handling techniques and data quality checking/cleansing** to improve data quality and **reduce the response time needed for detecting advanced security threats***
- *Necessary **know-how on EU interoperability strategies** & **technological infrastructure** to facilitate the legal and secure sharing of relevant information and intelligence owned among the different authorities to **ensure the interoperability of surveillance systems**, availability of information and also avoid duplication of efforts*
- *A **common cyber security framework (strategy)** which aims to improve, and enhance, the way smart cities protect themselves from threats including a **privacy-preserving framework and a set of privacy-by-design guidelines***
- *Protect personal data and sensitive information from unauthorized access, security attacks and hacking (**cyber security awareness**)*
- *Performing risk analysis and awareness through **cyber hygiene** and proposing specific training and awareness measurements on digital security*
- *Qlack Live **Integration** Environment that could potentially serve as a **suite for smart cities applications** with the following characteristics:*
  - *web-based dynamic platform that enables easy access from anywhere through a web-interface*
  - *for real-time collaboration between remote partners*
  - *supports virtual communities and*
  - *defines workspaces for members to use services/applications that facilitate interaction and processing of content.*
- *Software development, exploitation*

**H2020 SPEAR, H2020 FOLDOUT, H2020 SPACE-O*

George Boultadakis [george.boultadakis@eurodyn.com]

# Project participants

- Proposed coordinator: -
- Partners / Other participants: *End-users (cities, municipalities, network of cities), legal/ethical expert*

- Looking for partners with the following expertise/ technology/ application field:
  - *Novel monitoring methods/technologies provider*
  - *Innovative surveillance technologies provider*
  - *Experts in designing and planning simulation scenarios and case studies*
  - *Cyber experts*
  - *End users*

# Spiderweb

- Cristiano Fontana
- cristiano.fontana@pd.infn.it
- University of Padova (UniPD)
- Role: Proposal coordinator or WP leader

- Proposal activity:
  - *SU-INFRA02-2019: Security for smart and safe cities, including public spaces*

# Spiderweb

- Smart support for first intervention operators in case of detected radiological illegal item.
- Smart detection systems, grid located, to detect and track radiological threats.
- The algorithm will predict the final location helping to drive the person along a preferential path for further inspection.

# Project participants

- Proposed coordinator: *UniPD or other*

- Partners :
  - University of Padova (UniPD) – Italy
  - CAEN s.p.a. – Italy

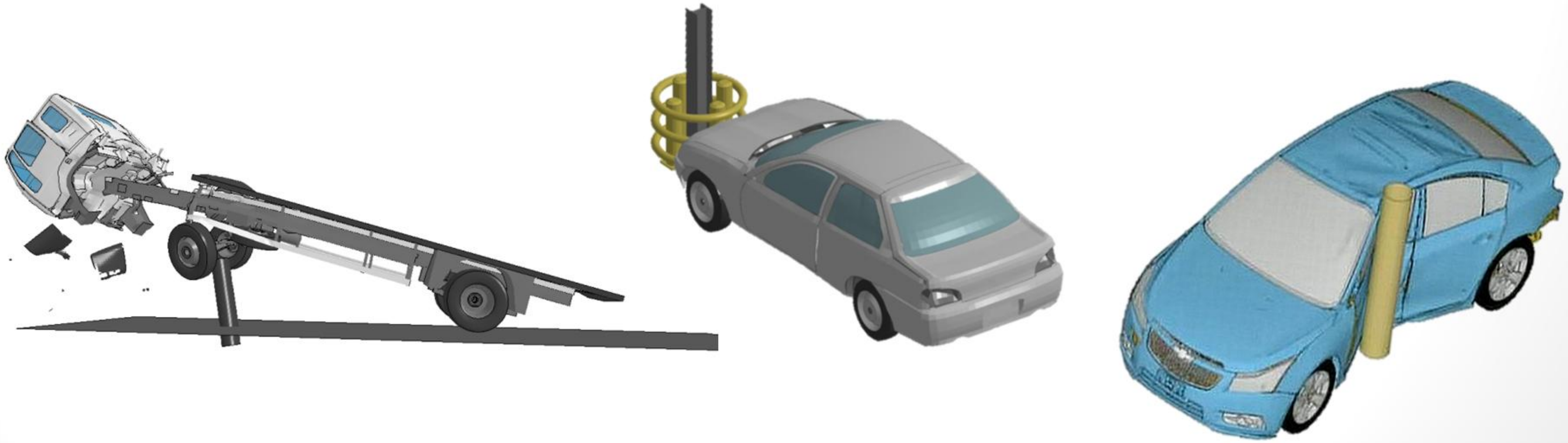
- Looking for partners with the following expertise/ technology/ application field:
  - *IoT partners*
  - *End-Users, practitioners*
  - *Augmented Reality*
  - *Other sensor technologies*

# Finite element simulations for assessing anti-intrusion product effectiveness

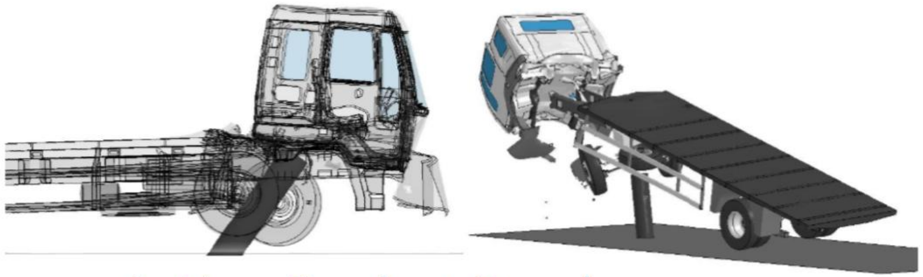
- *Rocco Frontera*
- *rocco.frontera@gdtech.eu*
- *GDTech*
- Role: *Possible partner*

GDTECH engineering

- Proposal activity: SU-INFRA02-2019



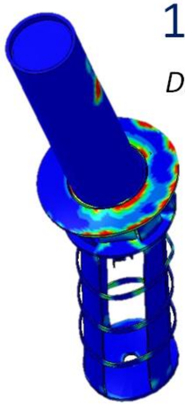
# Proposal idea/content



## 1. New Product Development

Drawings → Digital model → Simulation → Experimental tests

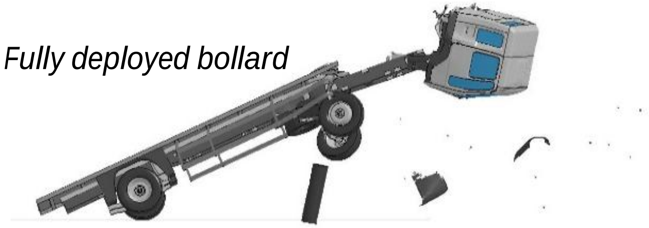
Optimisation



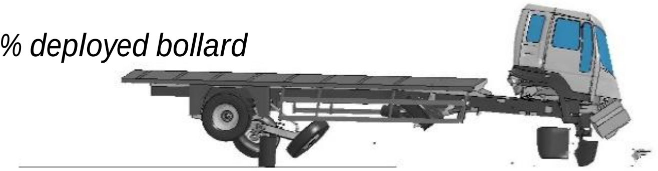
## 3. Adaptation to Site Conditions

*e.g. different kind of soil, concrete or rebars, bollard not completely deployed*

*Fully deployed bollard*



*50% deployed bollard*



## 2. Certification

*According to norms*

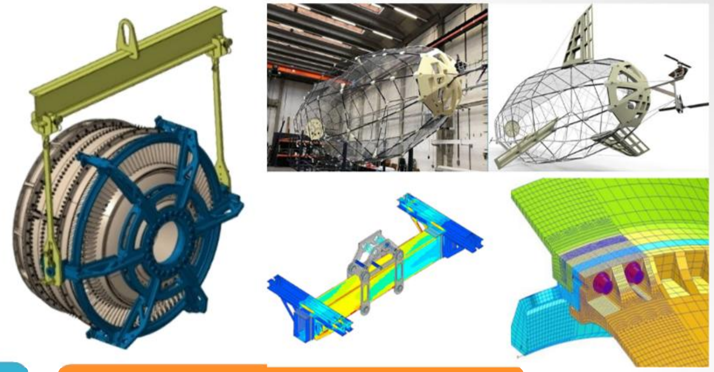
*New product*

*(Crash-tests)*

*Modified product*

PAS 68:2013 norm allows to assess modified products by FEA procedures

# Project participants



- *GDTech expertise*

Measurements & 3D Printing

Drawing & Design

Structural Analysis

Fluid Analysis

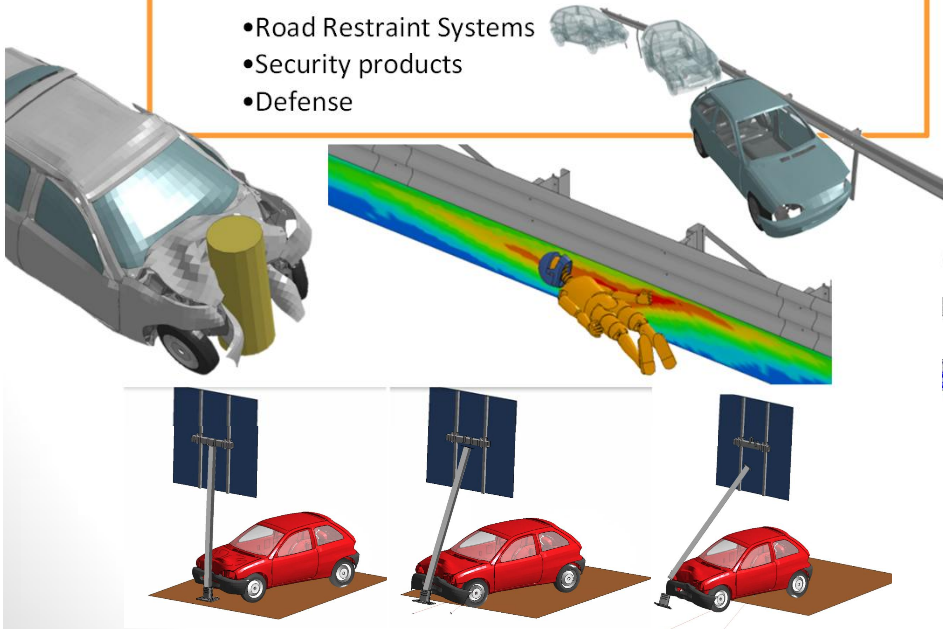
Acoustic Analysis

Other Services

- Accident reconstruction
- Emergency scenarios simulations

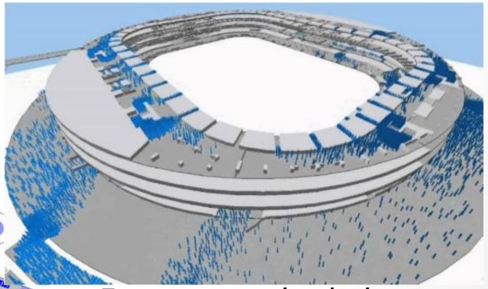
Structural Analysis

- Road Restraint Systems
- Security products
- Defense

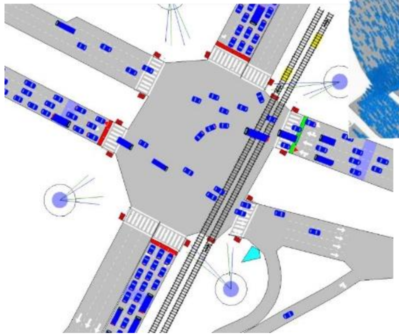


Emergency scenarios simulations

- Crowd simulations
- Traffic simulations



*Emergency exits design*



# SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

- *Prof. William Hynes*
- *William.hynes@futureanalytics.ie*
- *Future Analytics Consulting Ltd., Dublin, Ireland.*
- Role: *Work Package Lead*

- Proposal activity: SU-INFRA02-2019:
  Security for smart and safe cities, including for public spaces

# A Cyclical Approach to the Development of Well Informed Tools and Technologies

- *Ensure interconnectedness of complex and interdependent networks and systems – particularly through open platform development, solving interoperability issues.*
- *Ensure modelling and simulating of interdependence, securing communication and data storage, and address misuse.*
- *Develop novel monitoring methods, consider mitigation strategies to increase Resilience.*
- *FAC can deploy expertise gained from similar previous projects:*
  - *Development of open platform for sharing and managing information.*
  - *Application of Monitoring and Evaluation techniques.*
  - *Stakeholder, citizen engagment and collaboration.*
  - *Ability for relication and upscaling approaches and methods.*

# Project participants

- Proposed coordinator: *N/A*
- Partners / Other participants:
  Future Analytics Consulting Work Package Lead
- Looking for partners with the following expertise/ technology/ application field:
  - Technology experts
  - Transportation, Energy, Communication and Transactional Infrastructure Specialists/Owners/Operators.
  - Municipal cities and Regional Authorities
  - Risk Management Specialists
  - Representatives from key citizen groups

# Security for smart and safe cities, including for public spaces

- *Dimitris Kyriazanos*
- *dkyri@iit.demokritos.gr*
- *NCSR Demokritos*
- Role: *Coordinator/Technical Manager/WP leader*

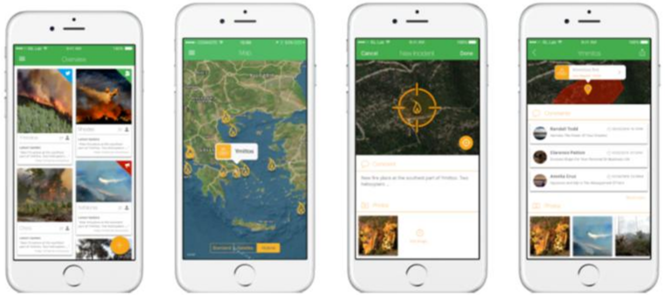
- Proposal activity: SU-INFRA02-2019

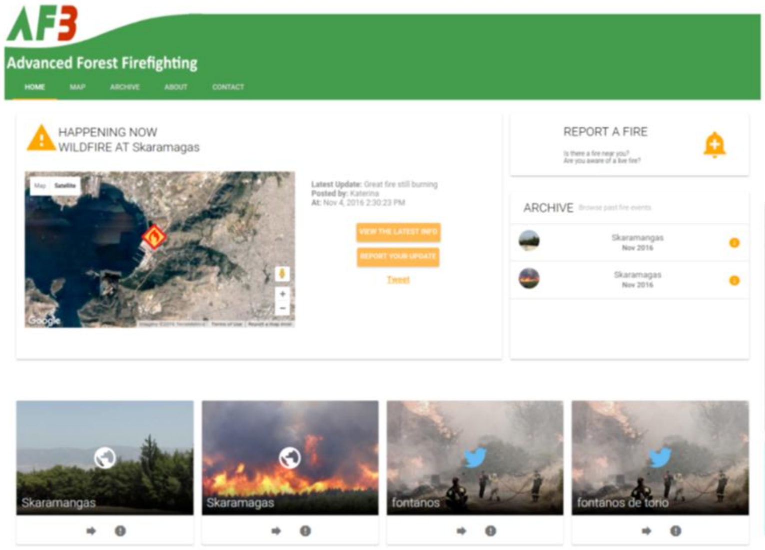
Dr. Dimitris M. Kyriazanos
Research Assistant Professor
Head of Security Unit - Integrated Systems Laboratory
Email: dkyri@iit.demokritos.gr
Phone number: (+30) 210 650 3150

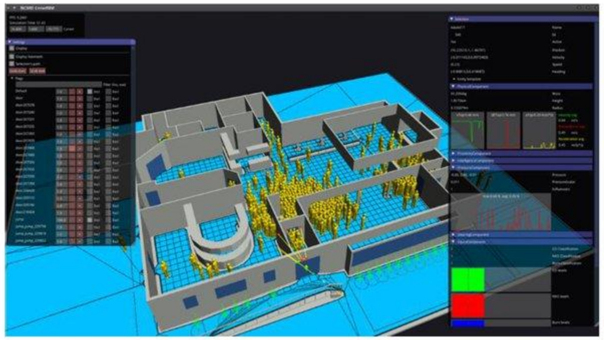
Dr. Stelios C.A. Thomopoulos
Head of Integrated Systems Laboratory
Email: scat@iit.demokritos.gr
Phone number: (+30) 210 650 3155
Mobile: (+30) 6944 98669

# Proposal idea/content

- *Evacuation simulation, crowd modelling and human factor impact assessment for public spaces like malls, events and hospitals*
- *Mobile/portable security portable apps and localisation, together with anomaly detection and machine learning for security early warnings*
- *Telecommunications during Emergency/Crisis – Athens 5G testbed, MCX*
- *Trial in Athens*







# Project participants

- Proposed coordinator: *NCSR Demokritos, Can be discussed*
- Partners / Other participants:
  - Greek Field Test Cluster of End Users and Assets/Infrastructure providers
  - Key RTOs

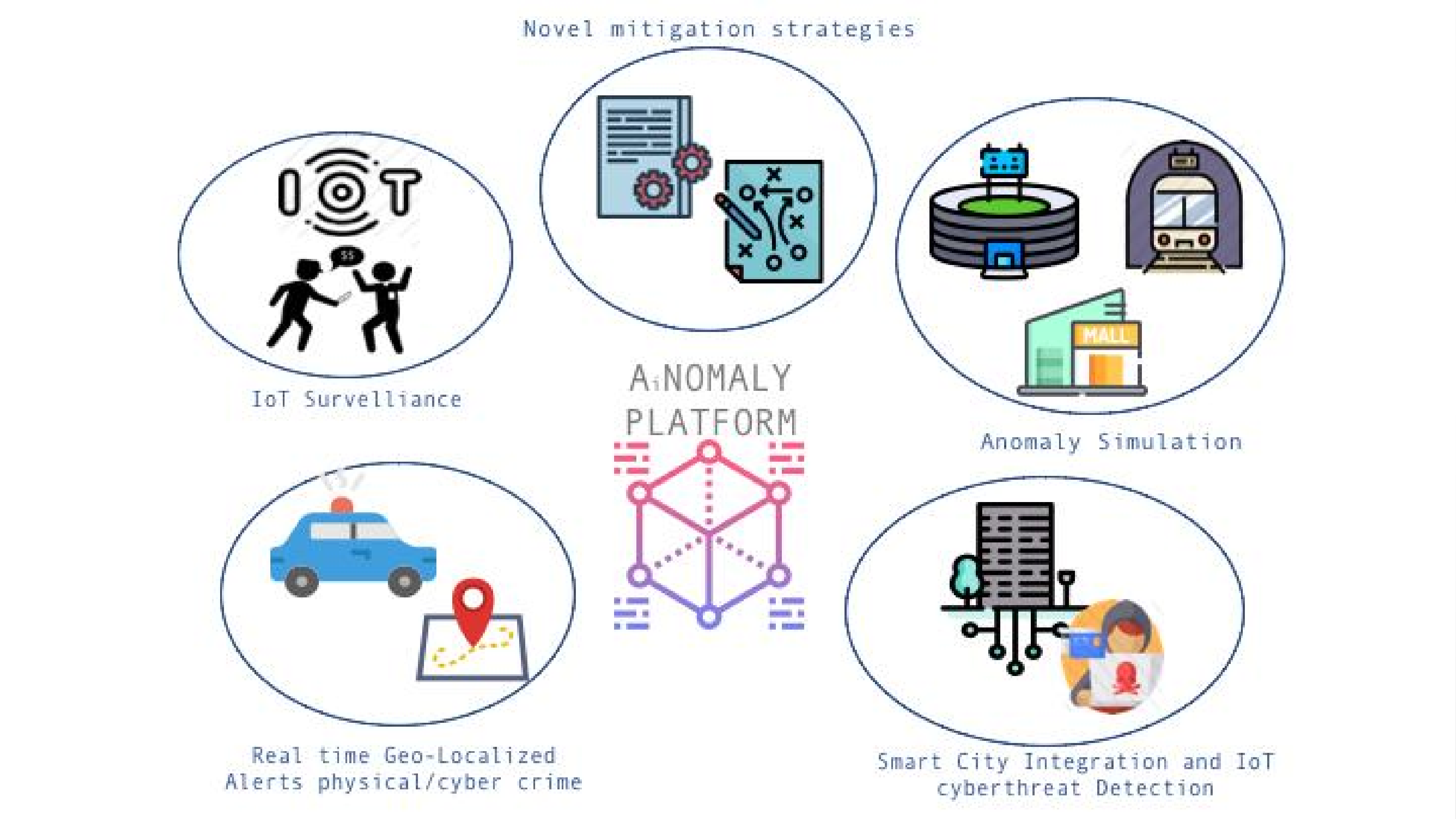
- Looking for partners with the following expertise/ technology/ application field:
  - *Technical Partners with a Smart/Safe City project portfolio including relevant IoT deployments*
  - *TRL 5-6*
  - *Pilot in other MS/AC and relevant urban planning and other stakeholders*

# AiNOMALY

- Iwona Maryla Maciejewska
- iwona.maryla@fib.upc.edu
- Universitat Politècnica de Catalunya - Barcelona Tech
- Role: *Proposal Coordinator*

- Proposal activity: *SU-INFRA02-2019*

# Proposal idea/content


Novel mitigation strategies
IoT Surveillance
AiNOMALY PLATFORM
Anomaly Simulation
Real time Geo-Localized Alerts physical/cyber crime
Smart City Integration and IoT cyberthreat Detection
IOT
$$
MALL

Iwona Maryla Maciejewska iwona.maryla@fib.upc.edu

# Project participants

- Proposed coordinator: Universitat Politècnica de Catalunya - Barcelona Tech (AI, IoT, cybersecurity, simulation & modelling)
- Partners / Other participants:
  - *ALTRAN (technical integrator)*
  - *RailGroup Cluster (pilot infraestructure)*
  - *Catalonia Mental Health Cluster (pilot infraestructure)*
  - *Mossos Esquadra/Dept Interior Catalonia (Catalonia regional law enforcement agency)*
  - *Technology providers: LBS & crowd monitoring, security network platform, access control*
- Looking for partners with the following expertise/ technology/ application field:
  - *Practioners*
  - *Local governments/ municipalities*
  - *Technologies providers: communications, detection of weapons, explosives and toxic*

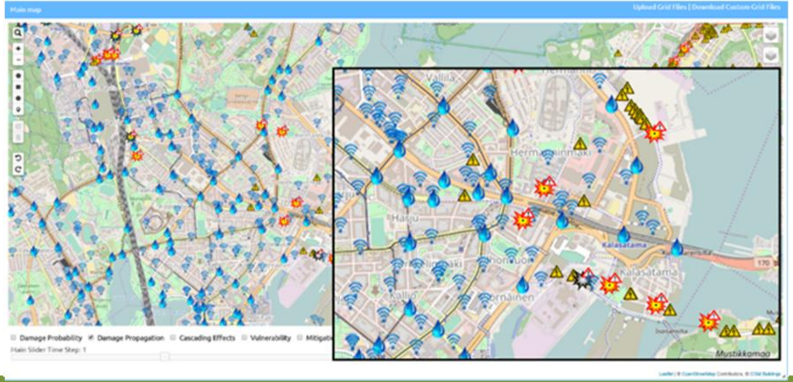
# Security concepts for smart and safe cities

- *Katharina Ross*
- *katharina.ross@emi.fraunhofer.de*
- *Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI; Germany*
- Role: *Proposal coordinator or WP leader*

- Proposal activity: *SU-INFRA-02-2019: Security for smart and safe cities, including for public spaces*

# Proposal idea/content

- *The aim of this proposal idea is the development of a simulation enviroment to improve the security for smart and safe cities by:*
    - Modelling critical infrastructure and safety aspects and their cyber and physical backbones
    - Running crisis scenario simulations to identify virtual and physical weak spots
    - Responding to attacks
    - Conducting table-top excercises to check existing concepts and measures



□ Damage Probability ☑ Damage Propagation □ Cascading Effects □ Vulnerability □ Mitigati

Main Slider Time Step: 1

# Project participants

- Proposed coordinator: *Fraunhofer EMI or other*
- Partners / Other participants: (strongly interested)
  - Laurea (Finland)
  - Leonardo (Italy)
  - UTT (France)
  - IBZ (Belgium)
  - Ministry of the Interior (Turkey)
  - Metro de Madrid (maybe case study)
  - Gemelli Hospital in Rome (maybe case study)

- Looking for partners with the following expertise/ technology/ application field:
  - Safety and security experts for building automation control systems in public buildings, hospitals, Christmas markets, soccer games in stadiums, etc.
  - Experts for video surveillance systems and other security systems
  - Big data analysts
  - Security experts
  - Experts for safe and smart cities and public spaces
  - First responders like policemen, medical staff, firefighters, etc.
  - Responsible persons of the cities for the two case studies

Burcu TÜRKÖVER

CBRN-IS Product Manager

HAVELSAN / TURKEY

bturkover@havelsan.com.tr

Partner (WP or Task Leader)

Interested Calls:

- SU-DRS04-2019-2020: Chemical, biological, radiological and nuclear (CBRN) cluster
- SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

# HAVELSAN – Business Areas

## COMMAND, CONTROL & COMBAT SYSTEMS

Command & Control Leader of Turkey

## TRAINING & SIMULATION TECHNOLOGIES

A Global Brand in Training & Simulation

## MANAGEMENT INFORMATION SYSTEMS

Leading E-Transformation Company of Turkey

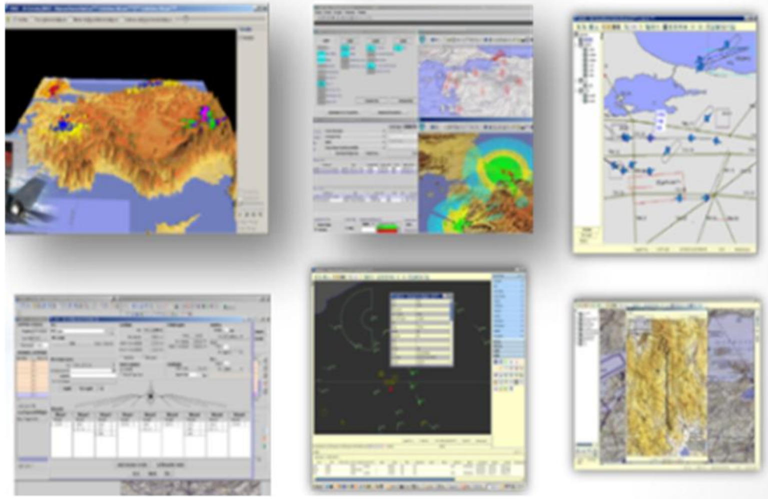
## HOMELAND & CYBER SECURITY

Center of Excellence in Security Solutions

# Chemical Biological Radiological Nuclear

HAVELSAN, provides Command, Control and Information Systems solutions to carry out the CBRN defense activities such as:

- Planning and Pre-Event Preparation
  - Defining Teams, Planning Intervention Processes, Identifying Threats
- Management of CBRN events
  - Warning and Reporting
  - Teams Assignment and Coordination
  - Monitoring and Control
- Risk Analysis
  - Capacity Analysis/ Contamination Analysis
  - Risk Assessment
- Decision Support
  - Calculation of Hazard Area
  - 3D Computation&Modelling of CBRN Dispersion
  - Route Planning
  - Identification of Chemical Agent Guidebook (IMER) / Emergency Response Guidebook (ERG)
  - Triage

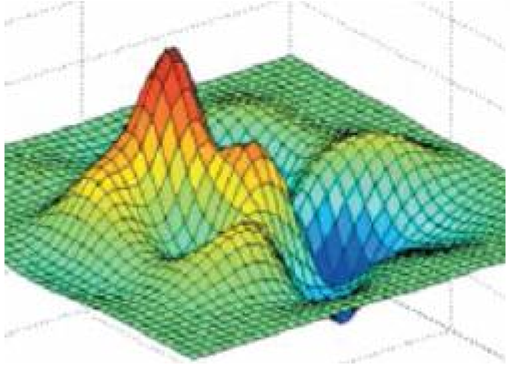


# Chemical Biological Radiological Nuclear

- Values Provided:
  - NATO Compatible Solutions
  - Solutions for both Military and Civilian Needs
  - Near Real Time Modelling with respect to Geographical and Meteorological Data
  - Rapid and Effective Planning and Decision Support Capabilities
  - Flexible integration of Detection and Identification Systems
  - Mobile solutions for Field Usage

# Chemical Biological Radiological Nuclear

- Calculation Models
  - NATO AEP - 45 (D)
  - NATO ATP - 45 (E)
  - Lagrangian Partical Dispersion Model
- Other Applied Standards
  - NATO ADatP-3
  - AEP 66
  - AJP 3.8
  - JC3IEDM



# RedBee

- *Lilian Adkinson Orellana*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*
- Role: *WP leader, S/T provider. Possibility of being Proposal coordinator.*

- Proposal activity: *SU-INFRA01-2019: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*

# Proposal idea/content

- *We propose a system for reacting dynamically to physical and cyber threats on sensitive industrial sites and plants. The proposal will cover the prediction, assessment, prevention, detection and response to these threats.*
- *The system will include RedBee, a cyber-deception solution with advanced analytic capabilities:*
  - *Platform for the management of different types of decoy services*
  - *It offers advanced analytics to characterize the cyber threats*
  - *It includes forecast and visualization of the attacks in real time*

Lilian Adkinson: ladkinson@gradiant.org

# Project participants

- Proposed coordinator: TBD
- Looking for:
  - *Industrial plants owners and operators*
  - *First responders*
  - *CERTs/CSIRTs*
  - *Industry, technologists and social scientists*
  - *ICS/SCADA honeypots developers*

Lilian Adkinson: ladkinson@gradiant.org