CYBERSECURITY ROMANIA
- BUCHAREST TALKS -

Beia
CONSULT INTERNATIONAL

Challenges and opportunities for IoT security

GEORGE SUCIU

R&D AND INNOVATION MANAGER,
BEIA CONSULT INTERNATIONAL

Content

- Biography
- About BEIA Consult
- Introduction
- IoT
  - Security
  - Challenges
  - Opportunities
- Projects
- Conclusions

Biography

- George Suciu Jr. :
  - graduated from the Faculty of Electronics, Telecommunications and Information Technology (ETTI) at the University “Politehnica” of Bucharest (UPB), Romania(www.upb.ro)
  - MBA in Informatics Project Management and IPR from the Faculty of Cybernetics, Statistics and Economic Informatics of the Academy of Economic Studies Bucharest(www.ase.ro)
  - Ph.D. / Researcher at Aalborg University
  - R&D and Innovation Manager and Co-owner of BEIA Consult International (Romania), a research performing SME (www.beiaro.eu)
  - Experience in coordinating, participating and evaluating R&D projects
  - Founders of several start-ups

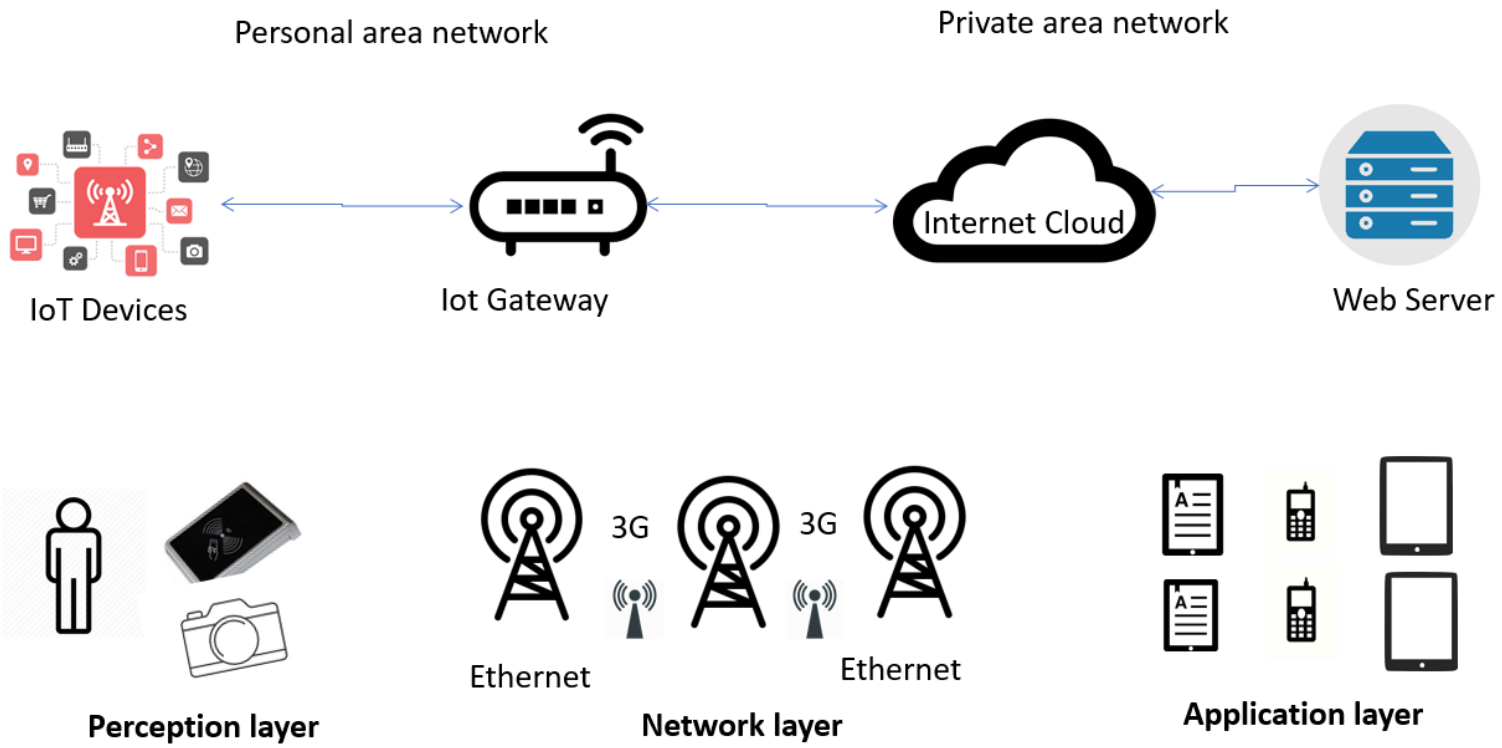
BEIA Consult

- BEIA has an experience since 1991 in over 5,000 turnkey projects for ICT and IoT solutions.
- Over 40 R&D projects: Horizon 2020 is the EU's largest research and innovation program with nearly € 80 billion available over 7 years (2014-2020)
  - **SWITCH**: Software Workbench for Interactive, Time Critical and Highly self-adaptive Cloud applications (ICT-9)SoMeDi: Social Media and Digital interaction intelligence
  - **ESTABLISH**: Environmental Sensing To Act for a Better quality of LIfe: Smart Health
  - **SeaForest**: Intelligent forest protection monitoring system based on wireless sensor network
  - **SoMeDi**: Social media and digital interaction intelligence
  - **CitiSim**: Smart City 3D simulation and monitoring platform
  - **VIRTUOSE**: Virtualized Video Services
  - **WINS@HI**: Wereable IoT Network Solution for Work Safety in hazardous Industrial Environments
  - **VLC/IR-RF**: Hybrid VLC/IR-RF Communication for Smart Space Based on Multi-Functional Thermal Image Sensor Module
  - **A-WEAR**: A network for dynamic wearable applications with privacy constraints
  - **SCRATCh**: SeCuRe and Agile Connected Things
  - **DEFRAUDify**: Detecting Fraudulent activities on the internet
  - **I-DELTA**: Interoperable Distributed Ledger Technology
  - **TIPS** : Trust, Isolation & ProofS
  - **COSIBAS**: Cognitive services for IoT-based scenarios

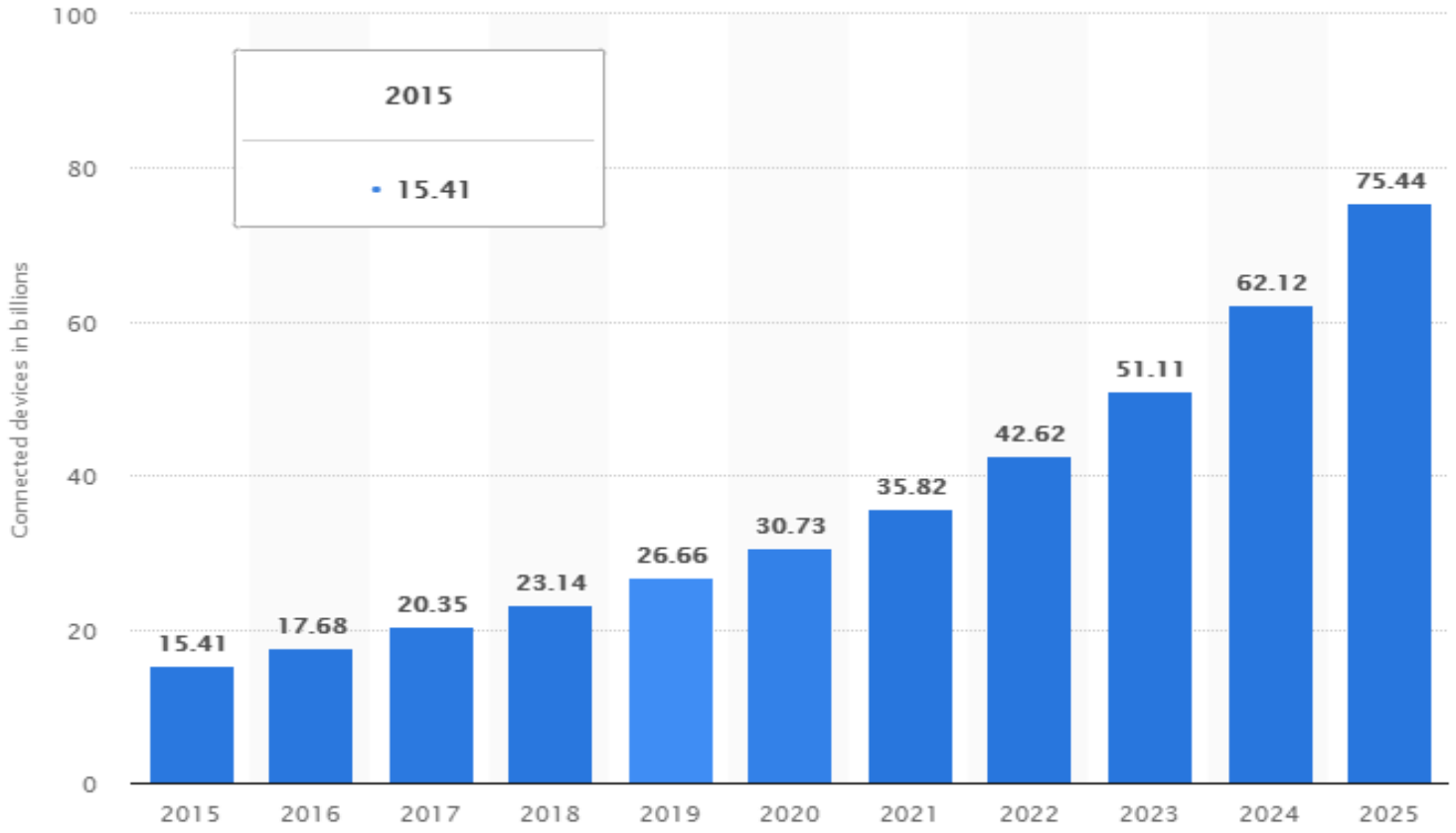
Partnerships

- Partners in Romanian R&D:
  - University “Politehnica” of Bucharest (www.upb.ro)
  - Research Institute for Artificial Intelligence (www.racai.ro)
  - Romanian Space Agency (www.rosa.ro)
  - National Institute for Research and Development in Electrical Engineering (www.icpe-ca.ro)
  - National Institute of Aerospace Research “ELIE CARAFOLI” (www.incas.ro)
  - National Institute for Research and Development in Informatics (www.ici.ro)
  - Research and Development Institute for Industrializing and Marketing Horticulture Products “HORTING” (www.horting.ro)
  - National Institute for Research and Development in Microbiology and Immunology for the Military (www.cantacuzino.ro)
- Member in the Directory Council of the German-Romanian Chamber of Industry and Commerce (AHK-Deutsch-Rumaenische Industrie- und Handelskammer) and other Chambers of Commerce and Clusters:
  - Leader of NEM Romanian Mirror Group (www.nem-pt.ro) and ARTEMIS
  - Member of Romanian Association for Electronic and Software Industry (ARIES), Electronic Innovation Cluster (ELINCLUS)

IoT architecture



IoT device trends and anticipated growth



The Security Features of IoT

- **Technological challenges**
  - result of the heterogeneous and ubiquitous character of IoT devices
  - associated with **wireless technologies**, **scalability, energy**, and **distributed nature**
- **Security challenges**
  - associated with the **systems** and **functionalities** that should be implemented to produce a secure network
  - concerned with the lack of the ability to ensure security by **authentication**, **confidentiality**, **integrity** and **end-to-end security**
  - Security implemented in IoT throughout the improvement and operational lifecycle of all IoT devices and hubs
- IoT devices software
  - paramount to be authorized
    - when an IoT device is turned on, it should authenticate itself into the network, and afterwards to start collecting or transmitting any kind of data
- **Firewalling**
  - important factor for the IoT network to **filter packets** addressed to the devices
- **Automation**
  - **autoconfigure**, **auto-repair** and **auto-coordinate**
  - rise in the vulnerability of the systems (manual interaction is extensively reduced)

Challenges with Security Principles

- Balancing the **end-user satisfaction**, the **costs** and the **implementation efforts** with **security**
- Level of safety ⇔ level of comfort provided by any solution
- Levels of confidentiality, integrity, availability and authentication
  - consistently determined using a **sliding scale**, having in mind the application, use case or environment -> imperative to hit the precise balance between the expected security levels, and cost or even the practicability of implementation. (**e.g.** a group of IoT devices like particular sensors, might require more processing power for advanced cryptographic transactions)
- Obtaining an architecture that is regulated by various devices, applications and networks =>
  - higher product quality
  - faster innovation and integration
  - broader community

} better response to undesired intrusions when or if they arise

Opportunities

- Increased **market size ($$$)**
- New **AI** technologies
  - More number of inter-connected devices => more data
  - applying analytics on all aspects of the business => opportunity to **improve** strategy and the customer experience
  - Semantic IoT (natural language interaction with things) including biometry
- **Blockchain**
  - audit trails, accountability, smart contracts, speed
  - **Build trust**
    - between parties and devices
    - reduce risks of collision and tampering
  - **Reduce costs**
    - remove overhead associated with intermediaries and middlemen
  - **Accelerate transactions**
    - reduce settlement time from days to almost instantneous
- **5G**
  - Smart doorbells & surveillance systems => help identify & recognize people => boost of security

Projects

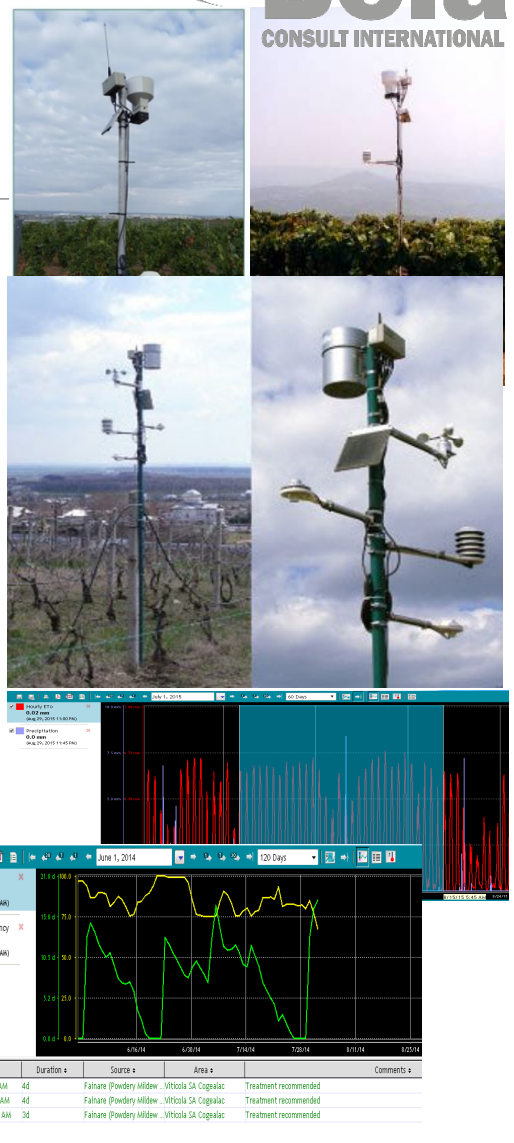
- **SA-TERRA**: Energy Efficient System for Automation and Telemetry for Resource Management in Precision Farming & **SmartAgro**: Telemetry system for intelligent agriculture

---

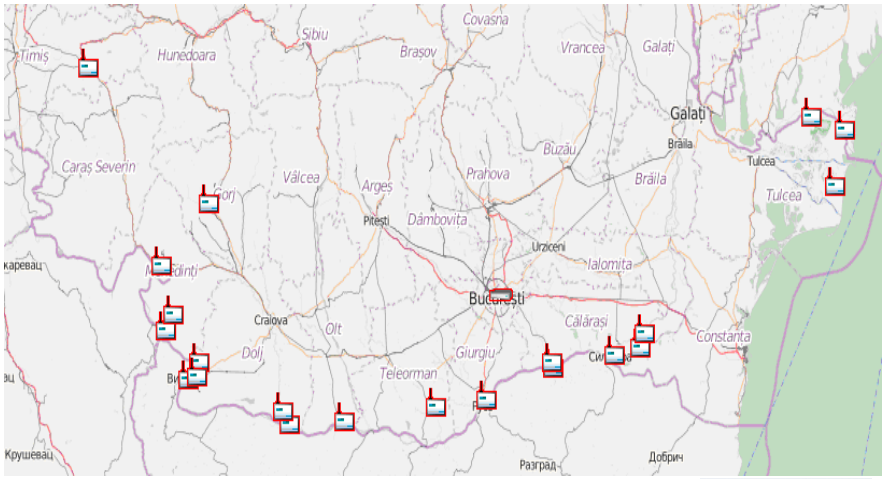
- **WATER-M**: Unified Intelligent WATER Management
- **TELEGREEN**: Telemonitoring system, equipment, installations and facilities for the production of clean energy
- **TERRA-RO**: Informatics system for real time analysis of risk factors for environment and public health
- **3DSafeguard**: Global Situational Awareness in Rescue, Calamity and Inspection Operations,
- **ASUA:** Advanced Sensing for Urban Automation
- **ALADIN** : Airports Landside and Air-land Side Attacks' Detection and Prevention
- **CitiSim**: Smart City 3D simulation and monitoring platform
- **ODSI**: On Demand Secure Isolation
- **PARFAIT**: Personal dAta pRotection FrAmework for IoT
- **SealedGRID**: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID
- **SAFECARE**: Integrated cyber-physical security for health services - SAFEguard of Critical health infrastructure
- **ToR-SIM**: Integrated Software Platform for Mobile Malware Analysis

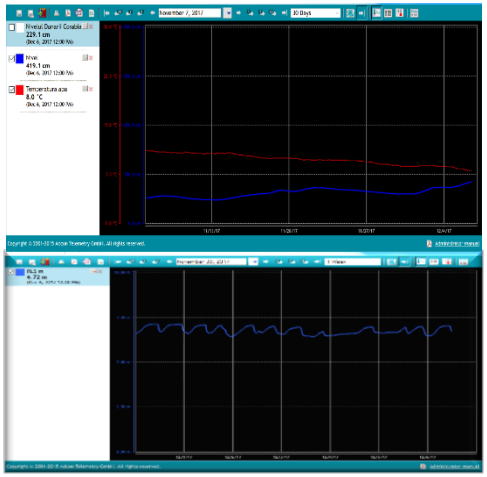
SA-TERRA and SmartAgro

- development of an integrated telemetry solution for automated resource management in precision agriculture
- modern cloud computing frameworks (IaaS, PaaS, SaaS)
- modeling and simulation software: MATLAB, LabVIEW
- programmable logic controller and HMI devices
- complex monitoring and control system: hardware-software project, SCADA applications for resource management, increased autonomy by power supply from photovoltaic panels on the field equipment.
- low energy consumption, low administration costs, scalability, forecasting functionality, diagnosis, potential for extension
- cooperation with universities / research institutes
  - development of the entrepreneurship skills of researchers, master and PhD students
  - development and testing activities of energy efficient industrial systems.
  - organizing of joint workshops for adapting the go-to-market tools and methodologies to the university profile.
  - Live data : www.beia-telemetrie.ro
  - Crop Science Division of Bayer Romania
  - AgroExpert: Telemetry stations for National Phytosanitary Authority



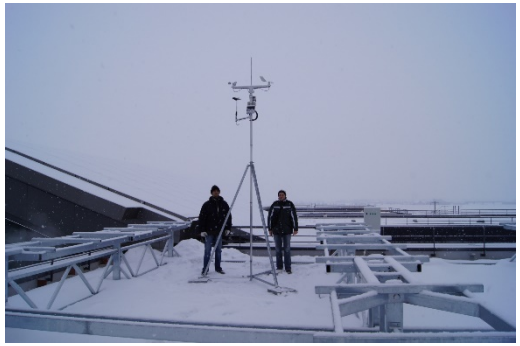
- finding solutions to the interoperability, real-time, big data and heterogeneous data challenges to being able to guarantee water supply and quality along with the stability and reliability of a smart water network



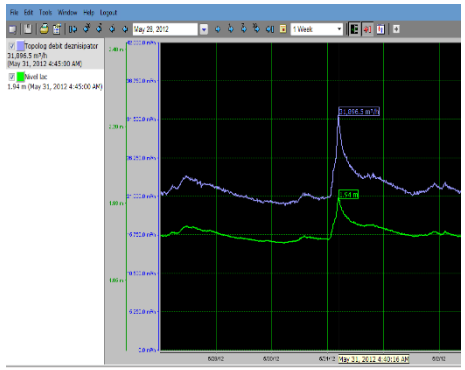


TELEGREEN - Telemonitoring of clean energy sources: hydro, solar, wind

- Monitoring of primary energy sources
- Monitoring of installations: output, efficiency, status of batteries & consumables, security

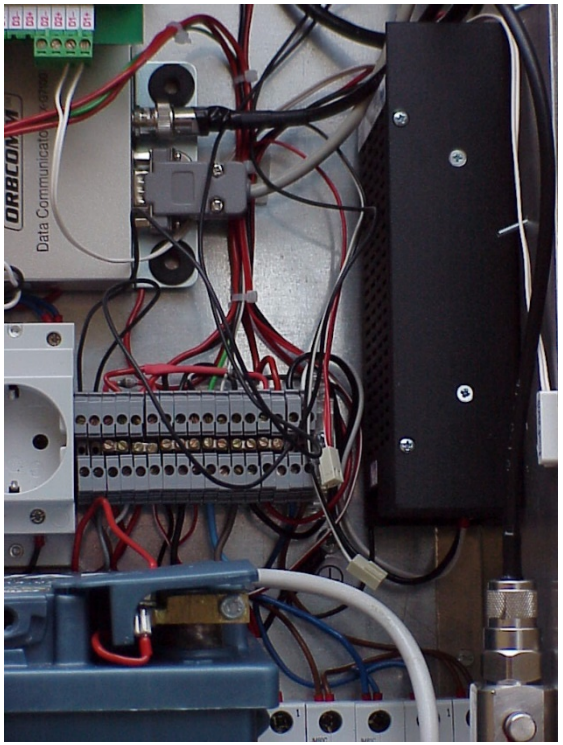





TERRA-RO

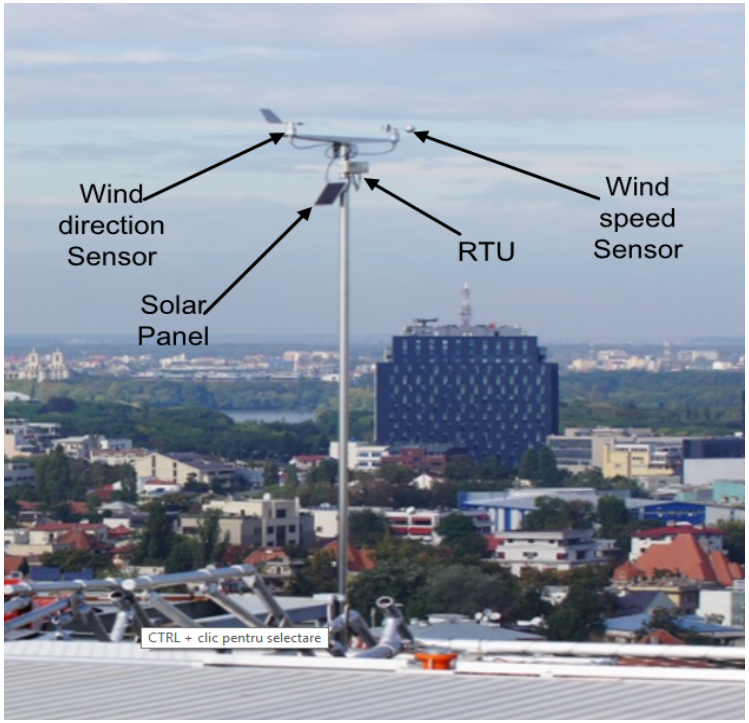
Radiations monitoring system and early warning based on ORBCOM LEO network to provide adequate local radioactivity monitoring networks around the nuclear plant of Cernavoda



ASUA
Advanced Sensing for Urban Automation

Beia
CONSULT INTERNATIONAL

- solutions for managing constrained devices in challenging environments, while enabling them to get connected by becoming parts of an advanced sensing system.
- addition of new sensors to existing systems will be facilitated by designing flexible interfaces for enhanced interoperability



3DSafeguard proposes a solution enabling the situational awareness by introducing an integrated operation workflow, which deploys the following technological innovations:

- multi-modal heat, depth, toxicity, acoustic and video sensors mounted on acting officers or UAVs,
- sensor data fusion, resulting in reconstructed 3D map of unknown premises as actors propagate though and in tracking of the actor positions;
- situational analysis and decision support providing automated guidance and alerts to the officers,
- multi-layered visualization of the sensors, analysis- and 3D-map data onto coordinator displays and onto HMD displays of acting officers.

Airports Landside and Air-land Side Attacks' Detection and Prevention

The project will offer an optimally scalable solution that will integrate several security fields, tools, and services so that we will take into account all the requirements and limitations and adaptation of the ALADIN solution to different specific companies, air traffic administrations or other end users.

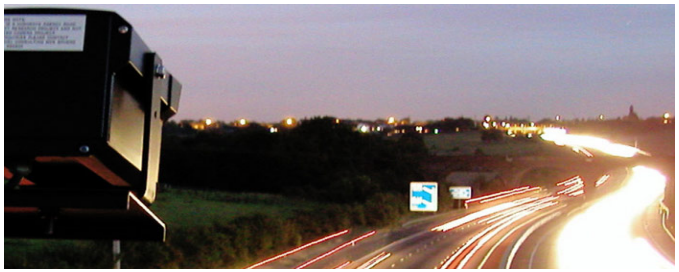
The ALADIN Platform will improve the Safety management functions of providing air navigation services that make sure that all safety risks will be identified, assessed and reduced to an acceptable level since, within the recent applications, there are not integrated Cyber Security tools for Airports Communications.

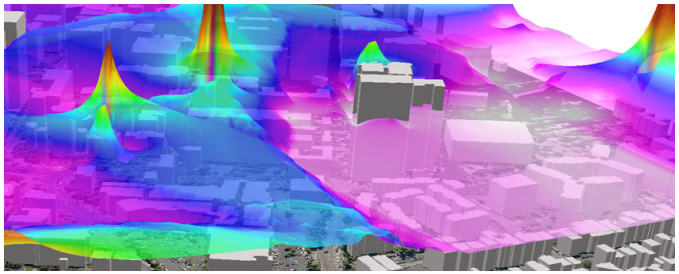
The motivation behind ALADIN project derives from the current political and economic situation: the attack occurred in USA 9/11, caused a significant number of changes to national and international aviation security regulations. Confidence in the sector dramatically affected the proclivity to travel, and the public is only recently returning to pre-9/11 numbers and the industry returning to profitability.

https://aladin.beia-consult.ro/

Smart City 3D simulation and monitoring platform

- design and implementation of a new generation platform for the Smart City ecosystem
- provide a powerful 3D simulation, monitoring and control infrastructure to enable planners to make critical management decisions on tactical and strategic levels based on the knowledge provided by the specific platform developed.
- for a natural interaction and better understanding of the events that happen in the city, 3D visualization techniques as augmented virtuality and augmented reality will be explored.





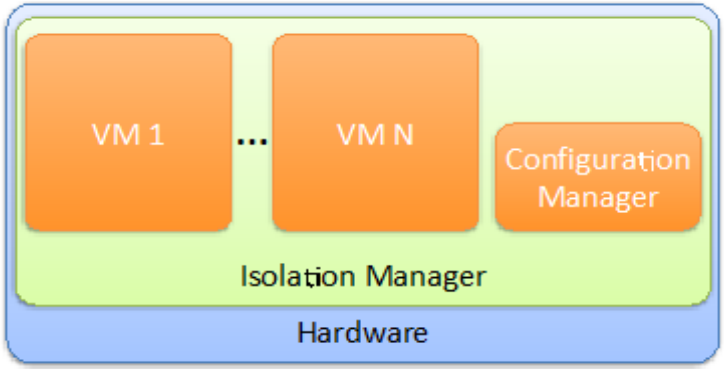
On Demand Secure Isolation

- Delivers new security models with the properties and the benefits of both hardware and software approaches
  - minimal properties for isolation, with the goal of being used in mass production (low-cost and constrained CPU) in all approaches that require context isolation: M2M, IoT, network infrastructure sharing, etc.

- TCB (Trusted Computing Base)[1] level: Proven hypervisor ("reducing complexity to build proven TCB")
  - build and formally prove that the ODSI Hypervisor supports the security requirements with lower manpower, thanks to an innovative software development methodology and tool chain enabling the rapid and cost-effective development of flexible and maintainable trusted systems
  - show that the MesoVisor can implement the isolation model with small TCB
  - demonstrate that both solutions (MesoVisor and ODSI Hypervisor) have performance close to systems without it

- Software Level: Applicability of the isolation model for the application
  - proposes several uses cases to validate the API offered by the isolation kernel, including a BYOD application
  - show that routing-dedicated hardware with isolation properties offers good performance and are compatible with the isolation kernel
  - propose software architectures and implementations for partition management and secure communication between components implementing ODSI approach

- Assurance Level: The Lego Methodology
  - composition of certification: enable certification as a Lego construction
  - easier the certification by reducing dependencies between applications running
  - adapt the existing risk analysis and certification methodology to the specific needs of ODSI
  - identify the security requirements for each component of the project
  - promote the work in standardization organizations



Personal dAta pRotection FrAmework for IoT interoperability

- Security & privacy of personal data => limitations for the growth of the Internet of Things (IoT) market. Interoperability increases the complexity of service production processes and the cost of production. Lack of security and trust for the protection of privacy put a barrier between service providers and consumers

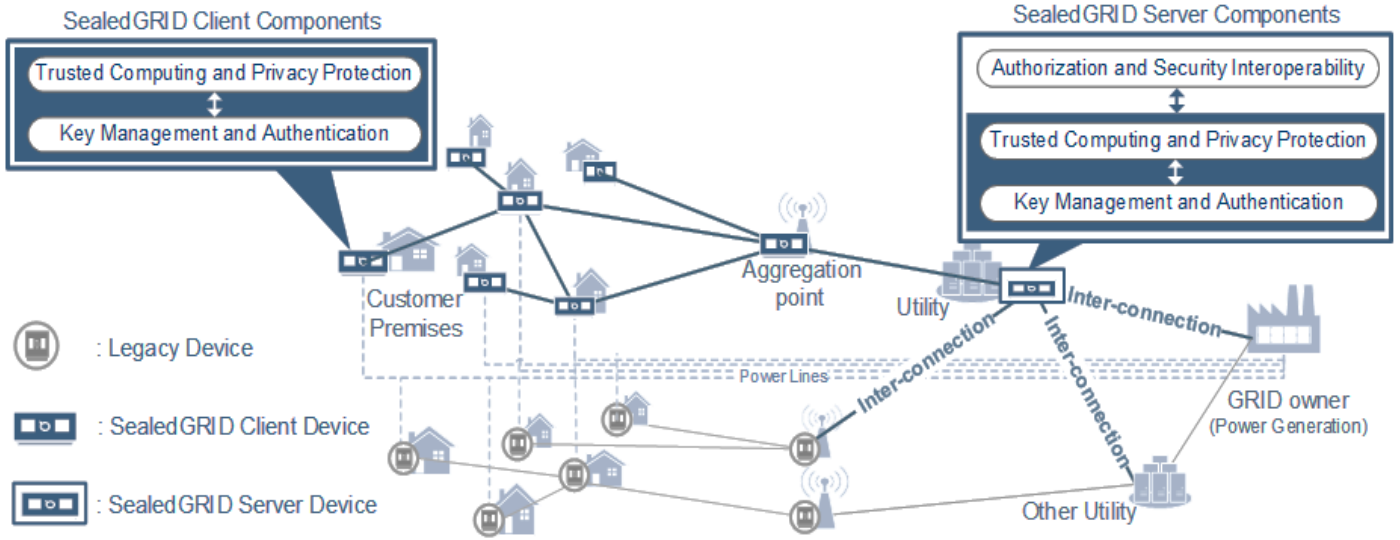
- **Objectives**
  - develop a platform for protecting personal data in IoT applications => reduce the complexity of integrating and deploying services in today's IoT technology by providing interoperable software libraries, tools, and SDK elements
  - generate huge business potential
    - integrated, scalable and extendable privacy and security framework -> will be demonstrated by 2 use cases (Personal Information Management & Smart Home Services) leaded by industrial partners of the project consortium
  - define interoperability and security/privacy methodologies, rules and guidelines to make recommendations for the policy makers

- Consortium
  - 11 partners from 3 countries (France, Turkey and Romania)

Sealed GRID

Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID

- Aims at bringing together experts from industry and academia from cross-sectorial research areas having complementary background with the long-term goal to design, analyze, and implement a ***scalable, highly trusted and interoperable Smart Grid security platform***
  - builds on a realistic architectural image of industrial installations considering the special characteristics of energy infrastructures, their cyber and physical requirements
- **Objectives**
  - efficient operation of critical infrastructure, while preserving quality of service, for the ultimate benefit of customers
  - providing an integrated solution that will be applicable to existing systems
  - providing advanced security features in legacy equipment upgrading their capabilities for operation in modern computing environments
  - limiting the security risks for the expansion of remote energy distribution network management, towards the evolution of Smart Grid



SAFECARE

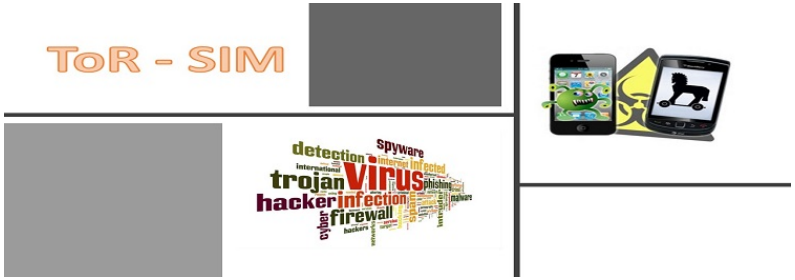
Integrated cyber-physical security for health services

- Aims to provide solutions that will improve physical and cyber security in a seamless and cost-effective way
  - promotes new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts

1: Sharing best practices between security and health actors, industrialists and university scientists.
2: Analysis and learning: by focusing on health services infrastructure, Safecare works towards creating a protection system, which covers threat prevention, response and mitigation of impacts across infrastructures.
3: Decision Support: Since threats cannot be analyzed solely as physical or cyber => develop an integrated approach to fight such combination of threats. Safecare will deliver high quality & innovative solutions in system security to support healthcare stakeholders take decisions.
4: Collect information on the heterogeneous sources of new threats.
5: Raising awareness => create a protection system which covers threat detection and mitigation of impacts across infrastructures and populations.
6: Disseminate the results and best practices throughout the health user communities to enhance awareness on how to handle multi-faced threats.

ToR – SIM

- develop a software platform that integrates, in a unitary manner, the malware analysis procedures for most of the existing mobile terminals, with the purpose of strengthening the security of mobile terminals and networks.
- identifying the operational requirements and capabilities necessary for developing and securing solutions for mobile applications and terminals
- increase of cyberprotection solutions efficiency by a partnership between government, academia and industry.



Conclusions

- Increase in the number of IoT devices => more and more **automation** will be needed for both **individual users** and **industrial environments**
  - Automation levels rise within IoT systems => **hardware** and **software vulnerabilities** will increase
- In the close future, information from IoT devices is going to be handled by **proxy network servers**, because end devices used nowadays practically have few, if no security features => more work should be spent on **designing IoT devices**
- Before **better standards** concerning **privacy** protection of individual data and better **security rules** on transmission procedures and cloud/ information storage, security of sensors and wearables will stay poor
- The variety of the software and hardware in the IoT area gives solid market competition, but it also provides a security issue since there is no general “system”.
  - dynamically characterized by the request of the customer and the response from the vendors.
- The capacity to design secure IoT devices relies on the meaning of security standards and agreements between vendors.
  - Providers will handle the access to devices in the cloud, but they cannot grant 100% security against unapproved access => is fundamental to exist **cooperation between vendors** in order to develop a **secured IoT world**.

CYBERSECURITY ROMANIA
- BUCHAREST TALKS -

Beia
CONSULT INTERNATIONAL

Thank you!

GEORGE@BEIA.RO