CAMPUS CYBER

SMI2G PITCHES EDITION 2023

This presentation gathers all the pitches submitted to the Security Mission Information and Innovation Group (SMI2G), assembling actors looking for consortia around innovative topics at European level for the 2023 calls of the Horizon Europe Civil Security for Society Call.

00. SUMMARY.

01. FIGHTHING CRIME AND TERRORISM.

- CL3-2023-FCT-01-01: Processing of large, complex and unstructured datasets resulting from criminal investigations, while reconciling big data analysis and data protection
- CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis
- CL3-2023-FCT-01-05: Crime as a service
- CL3-2023-FCT-01-06: Enhancing tools and capabilities to fight advanced forms of cyber threats and cyberdependent crimes

01. FCT-01-01: Processing of large, complex and unstructured datasets.

+ **NAME :** Thb-cise using social-related data and common information sharing (cise) in the fight against trafficking in human beings (thb) in the western Balkans for an improved european cooperation

+ **COMPANY :** LAUREA University of Applied Sciences, Finland + **CONTACT :** Johanna.Karvonen@laurea.fi

+ **BRIEF :** The Western Balkans is one of the most significant areas of departure for irregular migration and human trafficking to the EU. (https://prd.frontex.europa.eu/document/risk-analysis-for-2022-2023/)

Objectives :

- **Improve the cooperation** and information sharing between European and Western Balkan (Police) Authorities focusing on illegal trafficking and its embodiment in societies
- Within the framework of the project, **export European values** and good practices to the countries of the Western Balkans. (Establishing an EU mechanism on democracy, the rule of law, and fundamental rights)
- By integrating existing (Big) data platforms and their services, the project will **provide an enhanced awareness picture** to support decision making
- **Explore ways how to tackle THB**, taking advantage of existing (BIG) data (social media, 3rd sector, open-source intelligence (OSINT), and how to involve different social, 3rd sector stakeholder's data
- **Develop** a cross-sectoral training curriculum LEA, social and 3rd sector

+ **NEEDS :**

- EU Police Authorities/public authorities explicitly designated for the prevention, detection, and/or investigation of THB or other criminal offenses
- Organizations with experience in crime research and/or Big data analysis
- Technical partners providing Big data service solutions
- Stakeholders from both Western Balkans and EU member states targeted by THB (3rd sector, social, correctional services)

FCT-01-01: Processing of large, complex and unstructured datasets.

+ NAME : PRESERVE - PRIVACY PRESERVING BIG DATA PLATFORM FOR CRIMINAL INVESTIGATIONS

+ **COMPANY :** Gradiant (RTO, Spain)

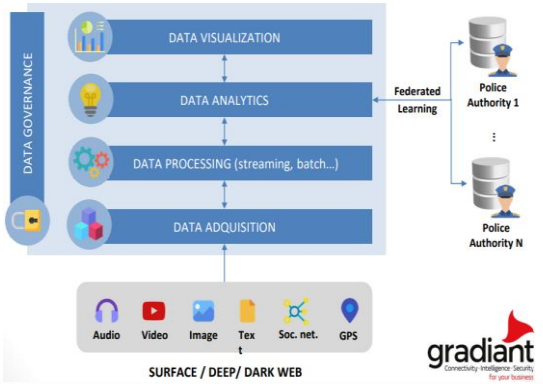
+ **CONTACT :** ladkinson@gradiant.org

+ **BRIEF :** Development of an IMS platform for European Police Authorities with advanced AI capabilities for detecting and countering emerging threats.
The Big Data platform will allow to handle large, complex and unstructured datasets, including audio, video, image, text and social network data.

The platform will include the use of :

- Social network analysis (SNA) and UEBA techniques to identify communities and determine suspicious behaviors.
- Privacy preserving techniques, such as the combination of Federated Learning + differential privacy + multikey homomorphic encryption + TEE, to enable the training of privacy preserving ML models while ensuring the quality of data.
- Secure integration of untrusted IoT in trusted environments (trusted execution environments)
- Specific location privacy algorithms.
- Detection of deep fakes, OCR, speech recognition…

+ **NEEDS :**
- 3 Police Authorities (from different EU Member States)
- Big Data and AI experts
- Deep/dark web data crawling
- PETs experts
- Others



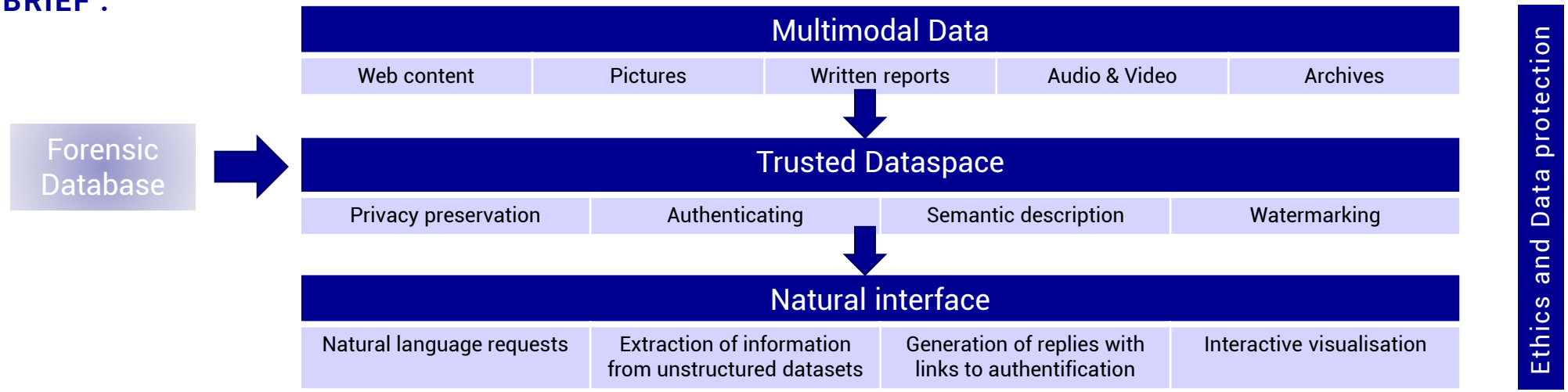
01. FCT-01-01: Processing of large, complex and unstructured datasets.

+ **NAME :** FORENSIC NATURAL INTERACTION ASSISTANT

+ **COMPANY :** Thales SIX France

+ **CONTACT :** edward.brodie@thalesgroup.com

+ **BRIEF :**



+ **NEEDS :**
- Complimentary Biometry
- Interactive data visualisation
- Legal & ethical partner
- LEA

01. FCT-01-01: Processing of large, complex and unstructured datasets.

+ **NAME :** CRIMINALYS

+ **COMPANY :** TREE Technology

+ **CONTACT :** javier.gutierrez@treetk.com

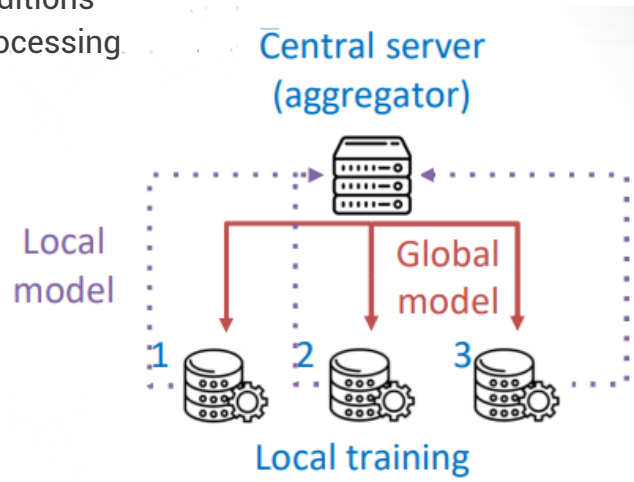
+ **BRIEF :** **Two-fold approach**

Big Data and Federated Learning

- Whole data lifecycle
  - Heterogeneous data/sources
  - Real-time/batch processing
  - Storage, access, exploitation, visualisation
- Federated ML to build collaborative models without sharing data
- GDPR-compliant approach

Computer Vision capabilities

- Deepfake detection – connected with identity management
- Detection of logos, people, entities, relevant objects / environments
- OCR in adverse conditions
- Image and video processing



+ **NEEDS :**

- Audio processing (AI-based) – University, company
- Interoperability – Large company
- End users – Police authorities

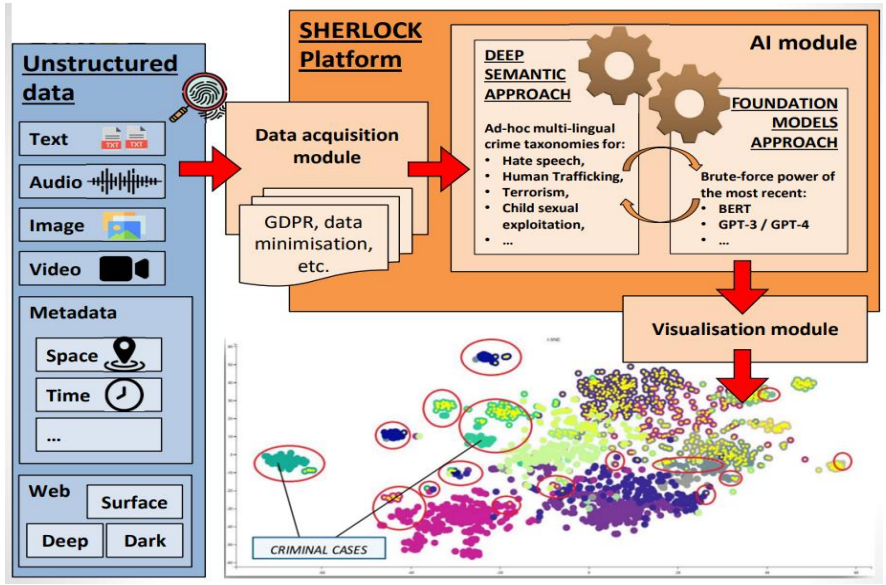
01. FCT-01-01: Processing of large, complex and unstructured datasets.

+ **NAME :** SHERLOCK - **SH**ared criminal **E**vidence gathe**R**ing and ana**L**ysis s**O**lution

+ **COMPANY :** Zanasi & Partners

+ **CONTACT :** graziano.giorgi@zanasi-alessandro.eu

+ **BRIEF :** Detect or anticipate crimes by analysing unstructured, heterogeneous and multi-lingual data by developping an **AI-based multi-lingual platform**, leveraging on partners with a strong expertise in:
  - **Unstructured Big Data Analysis** (IBM researchers and «Gartner Magic Quadrant» organisations);
  - **Security Research** (members of ESRAB/ESRIF, 30+ projects in Security/Defence, Scientific & Technical Coordinator of NOTIONES);
  - **Law Enforcement** (former Carabinieri officers, experts in LEAs involvement);
  - **Advisory on AI and Security** (several clients in Europe -EUROPOL, LEAs, …- and in MENA).



+ **NEEDS :**
- Artificial Intelligence developers
- Forensics and Intelligence experts
- Deep and dark web experts
- System integrators
- Europol Innovation Lab members

FCT-01-02: A harmonized European forensics approach on drugs analysis.

+ **NAME :** Nosum 2

+ **COMPANY :** University of Valencia

+ **CONTACT :** josesaez@uv.es

+ **BRIEF :** Based on a previous project called NOSUM that created a GHB detection kit and achieved TRL5.
A chemical method brings substantial advantages (in terms of reliability, readiness, instrumentation required and cost) when compared to bio-chemical and electro-chemical systems.

Topic requirements	Going beyond these requirements
↗ Detection on urine; ↗ End-users (forensic institutes, police) to remain at the centre of the process; ↗ Obtaining legally enforceable evidence in chemical submissive crimes.	↗ Detection on saliva; ↗ Increased usability by making reactivity directly available on solid (instead of a liquid solution); ↗ Insertion in a multidrugs test; ↗ Simple kit ready to be used by citizens (for their personal protection) and by entertainment centers.

+ **NEEDS :**
- Forensic
- Institutes
- Police authorities
- European associations.

01. FCT-01-02: A harmonized European forensics approach on drugs analysis.

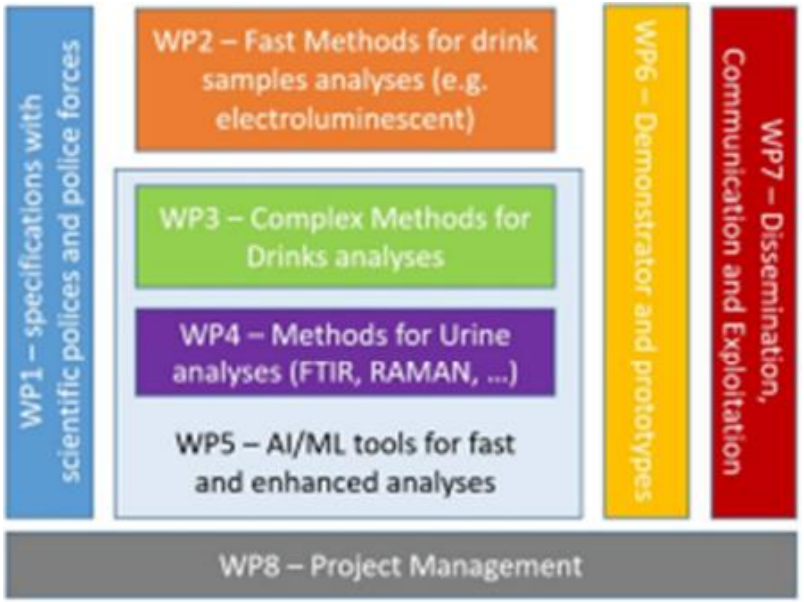
+ **NAME :** ADDRICT - **A**ccurate illicit **D**rug **D**etection sensors and methods for fast **R**eliable, **I**ntelligent and automated **C**hemical substances **T**ests

+ **COMPANY :** CEA

+ **CONTACT :** Emmanuel.Scorsone@cea.fr, Antonin.Galtier@cea.fr

+ **BRIEF :**

- **Focus on fast innovative sensors and reliable equipment for drug detection**
- **Alignment on the needs** for scientific and operational police forces and forensics validation
- **Fast methods** (e.g. electroluminescent solution for detection in glass, optical measurements and colorimetric strips)
- More **complex methods** for drink and urine analyses
- **AI/ML tools** for fast and enhanced analyses
- **Demonstrations and sensors**
- **Strategies for dissemination and exploitation**



+ **NEEDS :**

- Partners: technology provider for innovative solutions.
- LEAs: scientific, forensic, or operational forces.

+ **NAME :** GHB portable sensor

+ **COMPANY :** Military Institute of Chemistry and Radiometry

+ **CONTACT :** t.sikora@wichir.waw.pl

+ **BRIEF :** **We would like to develop portable sensor that gives easyto-inetrpret results and can be used in the field by Police Authorities.**

- ↗ Standarized methodology for optymizing the GHB evidence colection;
- ↗ Analytical technologies for in-situ sample screening;
- ↗ Communication and positioning modules for localizing the information and transporting it further;
- ↗ Transmission of obtained results in real time;
- ↗ Generating reports and building a database (possibility of quick communication and reporting).

Our experience in development of detection devices:
We developed an instrument allowing for the simultaneous **detection of TATP and HMTD**. The developed system uses differential ion mobility spectrometry (DMS) in combination with a specially designed gas sample injection system.

- ↗ **Mobile device for detection of biological threat**
- ↗ **A Mobile Device for Monitoring the Biological Purity of Air and Liquid Samples**

+ **NEEDS :**

- Forensic experts or Institutes with experience in determination of GHB and/or analogs
- Police Authority - to determine the procedural requirements that the evidence must comply
- First responders – policeman, on-site sample security personnel

01. FCT-01-02: A harmonized European forensics approach on drugs analysis.

+ **NAME :** Unveiling Criminal Networks through Innovative Drug Analysis Methods

+ **COMPANY :** Police Presidium of the Czech Republic

+ **CONTACT :** martin.kutra@pcr.cz

+ **BRIEF :** The Czech Republic Police has extensive experience in project management and **cooperation with EUROPOL/INTERPOL**. Among our greatest successes is the creation of the global collection of drug seizures called RELIEF Database, which is currently operated by the INTERPOL General Secretariat. The Police of the Czech Republic is continually working to improve the functionalities of the RELIEF Database by **adding new software utilities** which compare drug seizure not only from toolmark(s) perspective but also from the chemical composition of drug.

+ **NEEDS :**
- Project coordinator
- LEAs worldwide

FCT-01-05: Crime as a service.

+ **NAME :** NO SERVICE!

+ **COMPANY :** LAUREA

+ **CONTACT :** tuomas.tammilehto@laurea.fi

+ **BRIEF :**

Who is going & doing online ?
Includes all human activity: criminal too !
When services become online:

- ↗ Accessibility increases
- ↗ Scalability increases
- ↗ Efficiency improves
- ↗ User experience enhances, e.g., 24/7 availability
- ↗ Data collection improves, e.g., enables personalizing the user experience

Great benefit for organised crime, huge challenge to LEAs!
All the elements of market economy and business is present in illegal activities.

We need to study them to **understand contemporary criminal operations**.
Understanding is the key to prevention:

- ↗ Organised Crime
- ↗ Entrepreneurial criminals
- ↗ Dark web
- ↗ Business logic / value chains
- ↗ Money and supply flows
- ↗ And more

Most pivotal: **recognise and detect legitimate business from illegal!**
And build prevention for that

+ **NEEDS :**

- Expertise on illegal (and legal) online markets
- Data analysts, number crashers
- AI knowhow
- LEAs!
- And those who can asks the right questions!

01. FCT-01-06: Fight advanced cyber threats and cyberdependent crimes.

+ **NAME :** CRY-CIDER

+ **COMPANY :** Université de Loraine, BETA lab & LORIA lab

+ **CONTACT :** p.labic@unistra.fr

+ **BRIEF :** **A non-dogmatic, adaptive and close to the field approach.The search for innovative actions built on state-of-the-art expertise**

CRY-CIDER Platform
- ↗ Crypto-assets crime detection, classification and diffusion

Best practices
- ↗ IT and regulation tools to track, protect and fight crypto crime

Train and adapt
- ↗ Dedicated and targeted training programs

+ **NEEDS :**

End users
- Regulatory authorities
- Anti cyber-crime units
- Financial services, banking sector

Academics

Expertise (at least 1 needed): Work package leaders will be a team decision!
- IT, blockchain, malware, data and privacy protection;
- White collar crime models, transaction models (legal and illegals), intermediaries
- Cybercrime, fraud, laundering, racketeering, ransom, (field and research)
- MiCA, law and regulation, financial regulation, data protection, sovereignty.

FCT-01-06: Fight advanced cyber threats and cyberdependent crimes.

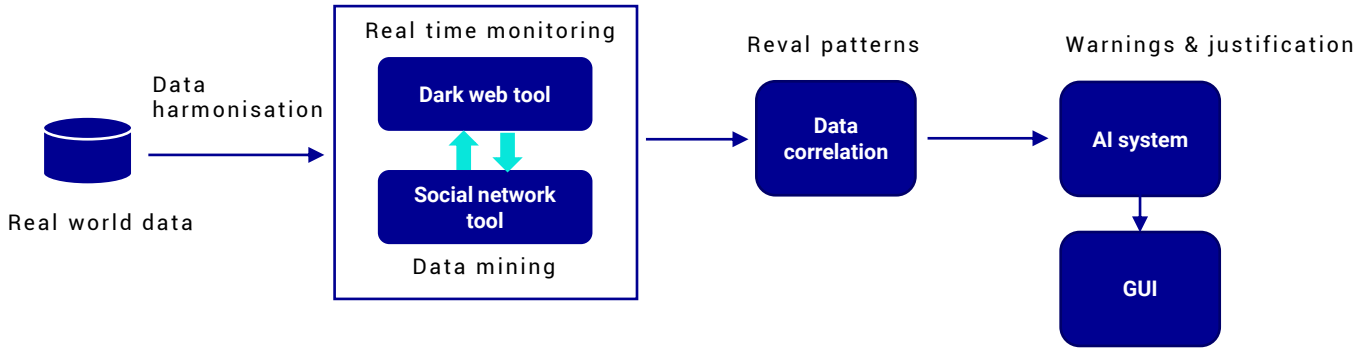
+ **NAME :** Enhanced investigation of web-based communication and dark-web related cyber crimes

+ **COMPANY :** Diadikasia Business Consulting - DBC

+ **CONTACT :** navgerinos@diadikasia.gr

+ **BRIEF :** **Platform that enables investigators to :**

- Extract, store, process and analyze useful information from unstructured chat sessions and the dark web
- Receive alerts with regards to crime-related topics and data
- Find correlations between criminal tools discovered by investigators in different places/countries



+ **NEEDS :**

- Additional LEAs
- Training expert for prosecutors & judicial authorities
- International judicial network

FCT-01-06: Fight advanced cyber threats and cyberdependent crimes.

+ **NAME :** FORSETI - **F**ighting **O**rganised c**R**ime using **S**peech, cryptocurr**E**ncy and darkne**T** **I**ntelligence

+ **COMPANY :** Brno University of Technology

+ **CONTACT :** ipluskal@vut.cz

+ **BRIEF :**

Area :

- Dark Market Places (DM), Social Media, OSINT, Digital Forensic Investigation, Law Enforcement (LEA).

Idea :

- Use periodical web scraping of **Dark Market Places** to gather evidence such as:
  - products / goods, quantity / sales count, prices, photos, country of Origin, …
- Cross corelate observed purchases with data available on public blockchain
- Using standard evidence sources like wiretapping of voice and social networks of suspects to mine metadata with:
  - speaker recognition, background noise artefact extraction, metadata extraction by other voice and image processing.

Cross correlate DM, Blockchain, Vision and Voice evidence. We want to work on implementation of tools that would help law enforcement agencies to make Europe safer!

+ **NEEDS :**

- A consortium partners, who are aligned with the project idea
- LEA organizations with interest in the project.

FCT-01-06: Fight advanced cyber threats and cyberdependent crimes.

+ **NAME :** Belgian Local Police

+ **COMPANY :** Brussels - Antwerp Police

+ **CONTACT :** Pierre.Vanbeveren@police.belgium.eu
Doris.Verreyken@police.belgium.eu

+ **BRIEF :**

Potential role : Task leader

- ↗ Operational / pilot scenarios definition, capability/functionality specification
- ↗ Validation and demonstration in operational scenarios
- ↗ Co-innovation and product co-development, etc...

Info : Belgian local police forces have all competences in all areas – Two biggest local police forces in Belgium.
Areas : Given our locations, specific infrastructures, mission statements, metropolitan issues, international institutions, numerous mass crowd events.

We also have a **large international network** and **partnerships** with other Law Enforcement Agencies (LEAs) , which guarantees dissemination and promotes further training.

+ **NEEDS :**

- Innovative safety & security,
- Security by design,
- Protecting public spaces,
- Counter drone measures,
- New ways of
- Protesting, alternative mobility,... . But also topics such as
- Inclusion, diversity, equal rights, xenophobia, racism (ISF –
- HORIZON – CERV - …)

01. FCT-01-06: Fight advanced cyber threats and cyberdependent crimes.

+ **NAME :** Multiple Interests by End-Users

+ **COMPANY:** Valencia Local Police, Spain

+ **CONTACT:** proyectosplv@valencia.es

+ **BRIEF :**

Horizon Europe – Work Programme 23-24 Civil Security for Society; preferred Topics:

↗ DESTINATION: BETTER PROTECT THE EU
↗ AND ITS CITIZENS AGAINST CRIME AND TERRORISM

CALL – FIGHTING CRIME AND TERRORISM 2023

- FCT-01-02 – Forensics on drugs analysis (option B)
- FCT-01-03 – Community Policing
- FCT-01-04 – Security in public spaces
- FCT-01-06 – Tools to fight cyber-threats and Cybercrimes

Horizon Europe – Work Programme 23-24 Civil Security for Society; preferred Topics:

↗ DESTINATION: RESILIENT INFRASTRUCTURE

CALL – RESILIENT INFRASTRUCTURE 2023

- INFRA 01-02 – Resilience of critical infrastructures

Horizon Europe – Work Programme 2023-2024 Civil Security for Society; preferred Topics:

↗ DESTINATION: DISASTER-RESILIENT SOCIETY FOR EUROPE

CALL – DISASTER RESILIENT SOCIETY 2023

- DRS 01-04 – Robotics in hazardous environments

+ **NEEDS :**

- N/A

02. BORDER MANAGEMENT.

- CL3-2023-BM-01-01:Capabilities for border surveillance and situational Awareness
- CL3-2023-BM-01-02:Identify, inspect, neutralize Unexploded Ordnance (UXO) at sea
- CL3-2023-BM-01-04:Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials

BM-01-01:Capabilities for border surveillance and situational Awareness.

+ **NAME :** Collaborative situational awareness from drones, towers and sensor meshes for autonomous border surveillance

+ **COMPANY :** Finnish Geospatial Research Institute(FGI)

+ **CONTACT :** tuomo.malkamaki@nls.fi

+ **BRIEF :** **Situational awareness center with multimodal geospatial**, satellite and historical monitoring data combined with continuous data stream from a monitorir sensor platform, AI based analytics and data fusion.

Sensor platform for autonomous situational awareness, comprising :

- ↗ Towers with monitoring sensors capable of semi-autonomous surveillance, network connection, processing unit and drone battery charge (docker)
- ↗ Ground/mobile docker stations/boxes
- ↗ Ground sensor meshes
- ↗ Swarm of drones with sensors and edge processing capacity
- ↗ Drone sensors for collaborative positioning, monitoring, and target detection

Human-Machine-interface designed for monitoring both inside and outside the border crossing points in land and sea borders.

+ **NEEDS :**

- Mesh connectivity/data transfer, CBRN knowledge
- API and UI with VR/AR for c2 systems
- We are open for discussions with other relevant partners

+ **NAME :** HAPS4BORDER

+ **COMPANY :** Aratos Systems BV

+ **CONTACT :** info@aratos-systems.com

+ **BRIEF :** **Human trafficking** remains a major global problem with devastating social, economic, and security consequences. **Maritime routes** are commonly used f illegal human trafficking, and detecting and preventing such activities remains a significant challenge.

High Altitude Platform Systems (HAPS) offer a potential solution for monitoring and preventing illegal human trafficking in sea borders.

In **HAPS4BORDER** we aim to develop and deploy a HAPS-based monitoring system for detecting and preventing illegal human trafficking in sea borders.

HAPS4BORDER project will adopt **a multi-disciplinary approach** involving experts from different fields such as aerospace engineering, data analytics, ar law enforcement agencies.The proposed project system will use **Artificial Intelligence** to:

- ↗ Enhance the system's performance
- ↗ Improve the accuracy and efficiency of data analysis
- ↗ Enable predictive analytics

Leading to better situational awareness and more effective prevention of illegal human trafficking activities.

+ **NEEDS :**

- Multidisciplinary Researchers
- Aerospace engineers,
- Software Engineers
- Data engineers
- Coastguards
- AI experts
- etc.

02. BM-01-01:Capabilities for border surveillance and situational Awareness.

+ **NAME :** Kemea

+ **COMPANY :** GeoBorder

+ **CONTACT :** g.dimitrakopoulou@kemea-research.gr

+ **BRIEF :** **Increase border surveillance capabilities** by developing technologies with better performance and cost-efficiency, ensuring compliance with legal ar ethical regulations and norms.
Development and deployment of land & maritime efficient, flexible, and interoperable technologies integrated with legacy systems, existing infrastructure EUROSUR and CISE.
Organise operational trials in different countries from Mediterranean to Baltic/Scandinavia with cross-community and cross-authority synergies.
Link with results and lessons learnt from ANDROMEDA, EFFECTOR, NESTOR, PROMENADE, BorderUAS, FOLDOUT etc.
BMVI, exploit
Technologies planned to be covered :

- ↗ Wide area surveillance with advanced detection & tracking capabilities
- ↗ Deployment of mobile, semi-autonomous surveillance towers
- ↗ IoT and advanced mesh connectivity
- ↗ Enhanced C2 and situational awareness with virtual and AR capabilities
- ↗ RPAS systems and autonomous vehicles
- ↗ Advanced sensors for geolocalisation
- ↗ Passive, low-energy systems
- ↗ Artificial intelligence

+ **NEEDS :**

- Border & Coast Guard Authorities from Mediterranean and Nordic Countries
- Networked deployable, mobile, semi-autonomous surveillance towers
- Passive, low-energy systems for border surveillance and situational awareness
- Interoperability of sensing, analysis, and C2 systems with VR/AR
- Experience in interoperability with EUROSUR and CISE

+ **NAME :** BOSENPRO - **BO**rder **SEN**sor **PRO**tector

+ **COMPANY :** Visionware

+ **CONTACT :** fcustodio@visionware.pt

+ **BRIEF :** **Deployable sensor system with integrated AI that detects critical events – the system works deployed in the field and only needs to communicate when the AI detects events.**

- ↗ Events may be : person or vehicle crossing restricted area; boat approaching beach; wi-fi/SIM systems tries to connect, and others
- ↗ Images or other evidences are sent to a central system

Multiple deployment possibilities (tower, drone, treetop, sea buoy).

Sensors work autonomously and process on the edge; evidence can be stored if **connectivity is impaired.**

Privacy by design with **automatic blurring** of images - **unblurring on request of authorities** after need is established.

+ **NEEDS :**

- Border/Coast Guard Authorities
- UAV/UMV developer
- Researcher in the field of border protection/migration et. al.

BM-01-01:Capabilities for border surveillance and situational Awareness.

+ **NAME :** UNIFRONT - **UN**iversal A**I**-plat**F**orm for Mediterranean f**RON**tier pa**T**rol

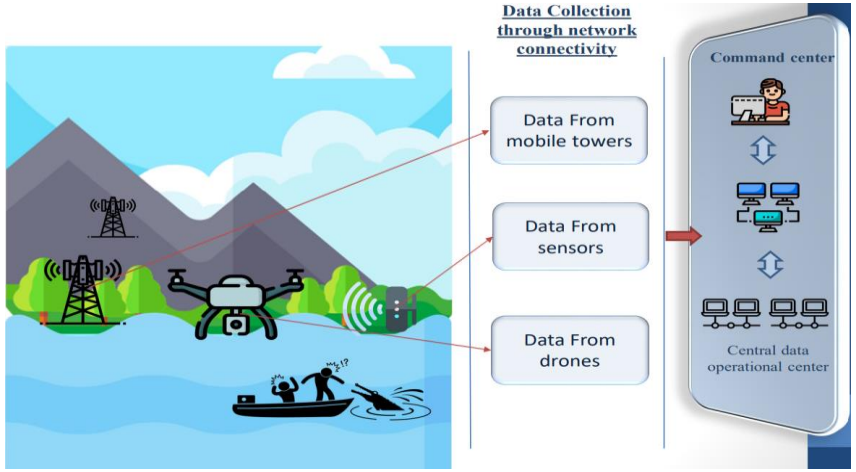
+ **COMPANY :** Zanasi & Partners

+ **CONTACT :** maria.ustenko@zanasi-alessandro.eu

+ **BRIEF :** Design a shared border surveillance **AI-driven solution** in order to improve border security in the Mediterranean area, cost and sea, made of :

  - **Onboard sensors** and **signal processing** [COFDM, IP-based, MESH, etc, channels, RINICOM, Havelsan] – sensors for geolocalisation, drones, adapted for marine environment [wing-in-ground drones, e.g. SEAWINGS project], IoT, VR and AR for enhanced C2 and situational awareness

  - **Ground AI-based platform** for visualizing and analysis of the collected data [unstructured Big Data analysis] **used by** Board/Coast guard authorities



+ **NEEDS :**
  - AI developers
  - System integrators
  - Border & Cost guard authorities

BM-01-01:Capabilities for border surveillance and situational Awareness.

+ **NAME :** Border threat detection

+ **COMPANY :** Gradiant (RTO, Spain)

+ **CONTACT :** ajimenez@gradiant.org

+ **BRIEF :** The proposal consists of combining both types of surveillance modalities (UAVbased and fixed station-based) in order to take advantage of each modality's strengths and alleviate their respective weaknesses. It would consist to (but not limited to) the following :

Automatic surveillance from ground-based fixed IR cameras

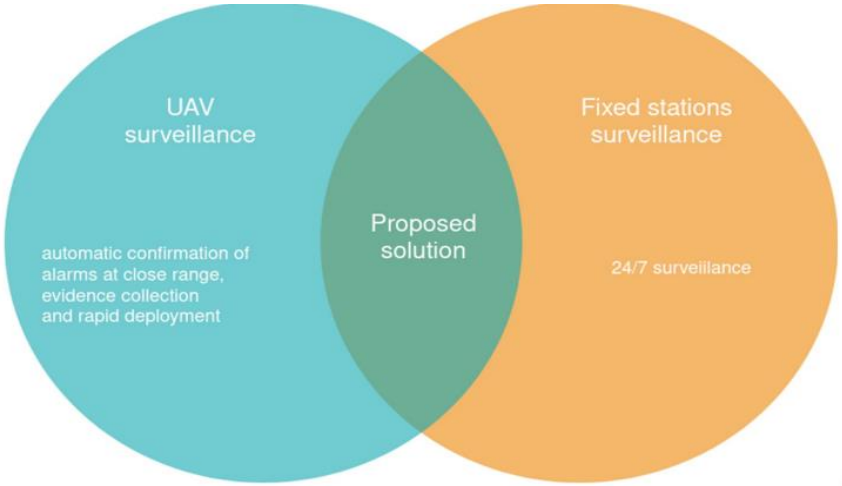
- ↗ Video Surveillance for the detection of drones or UAVs, ground or maritime vehicles.
- ↗ Multi-spectral video processing for improving detection/tracking capabilities with respect to separate spectral bands.
- ↗ Efficient video processing in low SwaP devices for flexible deployment in remote locations.
- ↗ Automatic generation of pre-alarms in real time.

Automatic and rapid deployment of UAV for target detection and tracking

- ↗ Video processing for detection/tracking of people, vehicles and objects (land and maritime scenarios).
- ↗ Efficient video processing in low SwaP devices for flexible deployment on board UAVs.
- ↗ Automatic confirmation of evidence in real time.

+ **NEEDS :**

- Law enforcement authorities, border control agencies
- Technology integrators
- Unmanned vehicles manufacturers
- Partners from previous BM- 2021-01-01



+ **NAME :** Collaborative situational awareness from drones, towers and sensor meshes for autonomous border surveillance

+ **COMPANY :** Onera

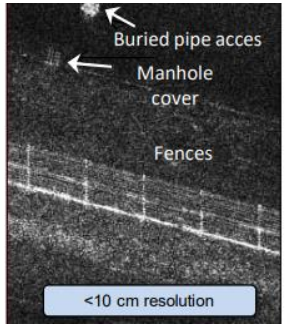
+ **CONTACT :** remi.baque@onera.fr

+ **BRIEF :**

Concept : Continuously day/night and all weather radar imagery and moving target detection on ground/sea and under forest used for detection of people and vehicles crossing borders.

Activities : Theoretical study, requirements, real environment demonstration (sensor and platform management,measurement and signal/image processing) and recommendations.

Radar sensors onboard small aircraft and UAV (small and high altitude).



+ **NEEDS :**

- Lead
- End users
- Electronic Warfare sensors for smartphone detection
- Optronic / LIDAR / thermal IR sensors
- Other platform/sensors

02. BM-01-01:Capabilities for border surveillance and situational Awareness.

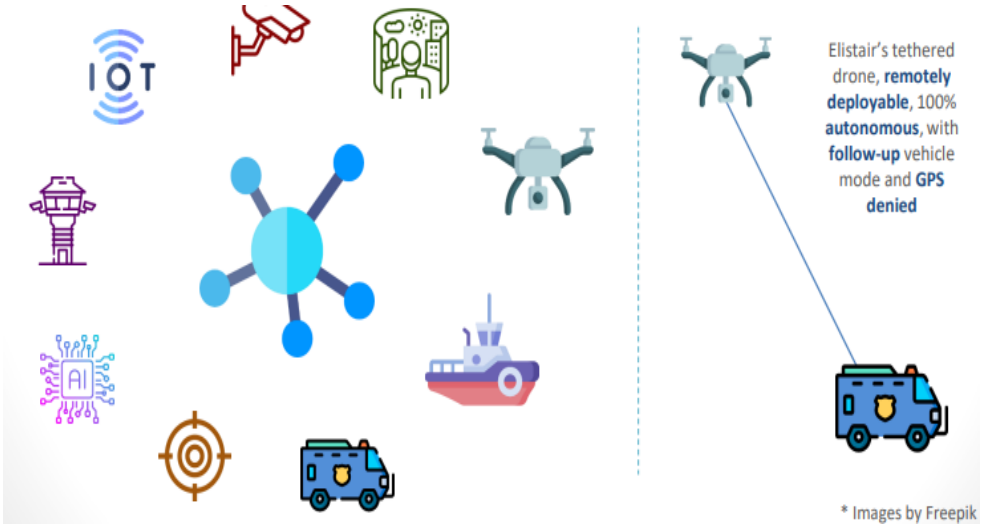
+ **NAME :** Border surveillance

+ **COMPANY :** Elistair

+ **CONTACT :** s.tardi@elistair.com

+ **BRIEF :** An **integrated system composed of new technologies and legacy systems**, integrated in a Command&Control system to facilitate decision making of operators and providing a 24/24h monitoring/surveillance of the border.

Technologies could be integrated on a patrol vehicle (land or maritime) to enhance situational awareness and help end-users take quicker decisions/be aware sooner.



+ **NEEDS :**
- Command & control system expert
- Technologies : cameras, RF systems, radars, unmanned systems…
- Social media analysis technology
- Augmented Reality

02. BM-01-01:Capabilities for border surveillance and situational Awareness.

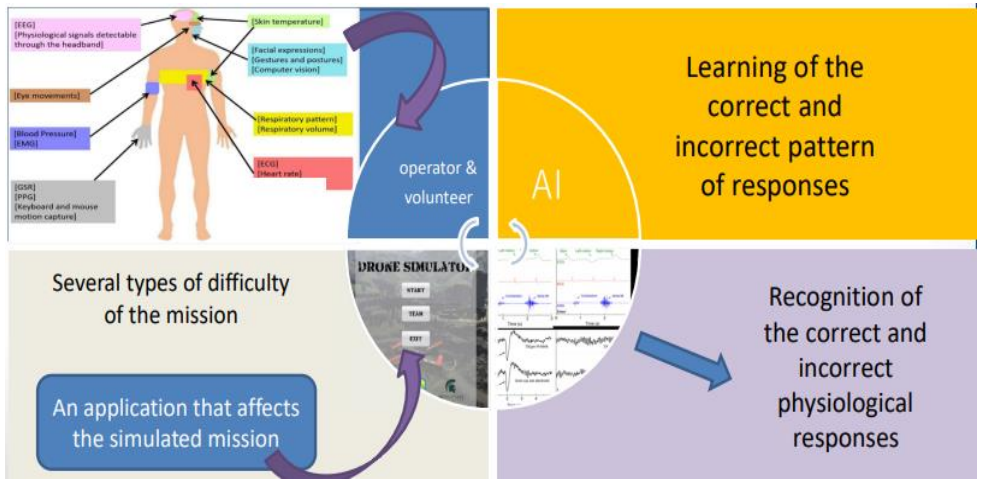
+ **NAME :** Biometric Border Guard – biobGAI

+ **COMPANY :** Military University of Technology

+ **CONTACT :** konrad.wojtowicz@wat.edu.pl

+ **BRIEF :** **Border guard vehicle simulation environment for data acquisition and operator evaluation**

- ↗ Vehicle data processing for AI driven mission management system
- ↗ Biometric data processing for AI driven mission customization and operator evaluation



+ **NEEDS :**
- Coordinator: industry partner
- Industry partners: UAV, AI, VR, simulation, biometric
- End Users: Border Guard, Military, Security Service

+ **NAME :** Turkish Coast Guard Command

+ **COMPANY :** Turkish Coast Guard Command

+ **CONTACT :** diab@sg.gov.tr/iilgar@sg.gov.tr

+ **BRIEF :**

Related Content (Main Missions)

- Search and Rescue
- Struggling against Irregular Migration
- Ensuring Maritime Security

Coast Guard Management System Project

- Includes detection and identification of tracks,
- With radar and day/night visual systems,
- In the coastal and offshore areas,
- With 95% coverage in territorial waters.

A Semi-Autonomous Sea Vehicle Development Project

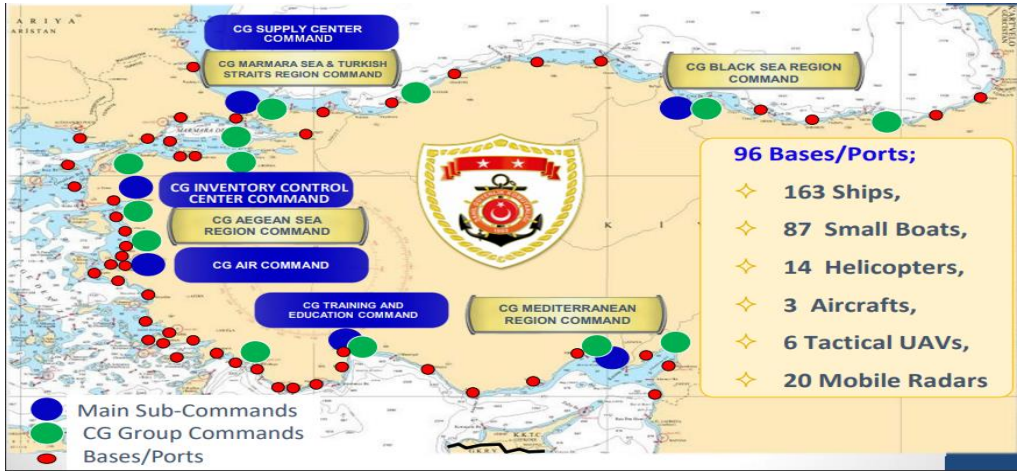
- Aims to enhance the interception capability.

The Procurement of the Remotely Operated Underwater Vehicles (ROV)

- Increases the underwater search, scanning, detection and identification capabilities.

+ **NEEDS :**

- Mesh connectivity/data transfer, CBRN knowledge
- API and UI with VR/AR for c2 systems
- We are open for discussions with other relevant partners



BM-01-02:Identify, inspect, neutralize Unexploded Ordnance (UXO) at sea.

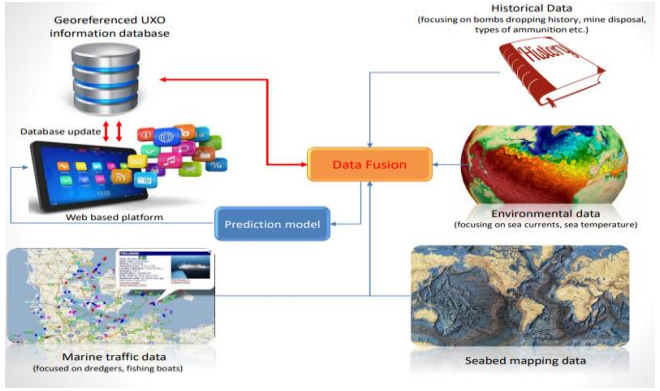
+ **NAME :** ROBFIDES

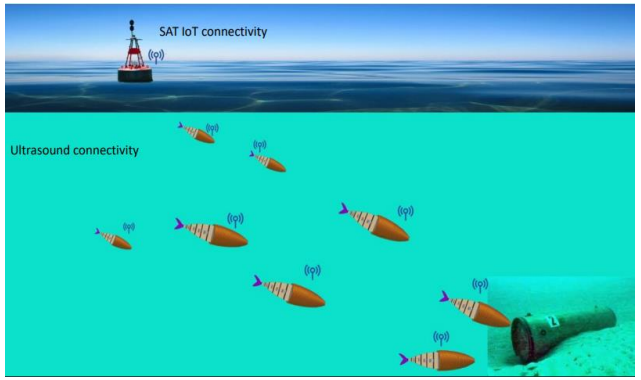
+ **COMPANY :** ForceApp BV

+ **CONTACT :** info@forceapp.eu

+ **BRIEF :** **Robotic Fishes of modular type (sensors carried in accordance with the mission)**

- UXO Detection [close distance images transmission – positive recognition – geo UXO database update]
- UXO identification [image processing process]
- UXO classification [comparative analysis through historical data database]
- UXO assessment [Subsea dynamic laser scanners – acoustic & ultrasound sensors]





+ **NEEDS :**

- At least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated countries
- Municipalities / regional authorities in other EU Member states
- Relevant academic partners
- Industry partners (maritime operations)
- International organizations (e.g., International Maritime Organization (IMO),UN)

02. BM-01-02:Identify, inspect, neutralize Unexploded Ordnance (UXO) at sea.

+ **NAME :** Preliminary proposal name - UXO SMART-DETECT

+ **COMPANY :** Hologarde, Groupe ADP

+ **CONTACT :** Marie.Kolago@adp.fr

+ **BRIEF :** Description of the proposed project: **increasing automatization of UXO detection process & its reliability :**

- ↗ Operational environment of the solution will focus on a **depth up to 600 meters** (so as to include submarines in the security risk)
- ↗ **The solution will incorporate IA to allow** (i.) data processing in real-time & (ii.) increased detection capacity
- ↗ Possibility to use the existing **UHV MANTA** (unmanned hybrid vehicle, designed by Marine Tech) as part of use-cases:
  - Initially designed for bathymetry
  - Now, dual-use UHV (both for civil, security & military purposes)
  - Agnosticity: capacity to incorporate a variety of sensors.

Increasing UHV decision-making autonomy :

- ↗ Current status: no possibility of live-time communication with UHVs due to depth constraint, therefore **autonomy is required** to achieve **UXO detection missions with improved capacities** ;
- ↗ Incorporation of IA (SLAM) in the solution aims at **allowing UHV decision-making capacity regarding mission outcomes** (continue / avoiding obstacle / autopilot / selection of appropriate actions to identify, discriminate & mapping the target,…).

+ **NEEDS :**

- UXO threat & risk assessment expertise,
- Underwater UXO depollution operations (private company or Navies),
- Sensors' providers: mostly photogrammetric measuring cameras with SLAM.

+ **NAME :** Intelligent pan-European customs dataspace (C-SPACE)

+ **COMPANY :** Diadikasia Business Consulting - DBC

+ **CONTACT :** navgerinos@diadikasia.gr

+ **BRIEF :** **Introducing an integrated European approach to customs risk and ecommerce management** that promotes compliance and introduces an "acting as one" customs authorities setup.

Harmonised exchange of information on the basis of internally accepted data models and message formats.

Reengineering of customs and customs related processes to enhance their efficiency, effectiveness and uniform application.

Offer to **operators services to be able to interact in the same way with the customs authorities** of any Member State.

Enhance cooperation between customs and security and border management authorities and synergies between their information systems.

Development of security policies which demand more personal data to be provided, customs, like other authorities, will have to deal with that and with issues such as privacy.

+ **NEEDS :**
- Standardization
- Spectroscopy
- Custom equipment suppliers
- Additional customs, border authorities to offer pilots

03. RESILIENT INFRASTRUCTURE.

- CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services
- CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

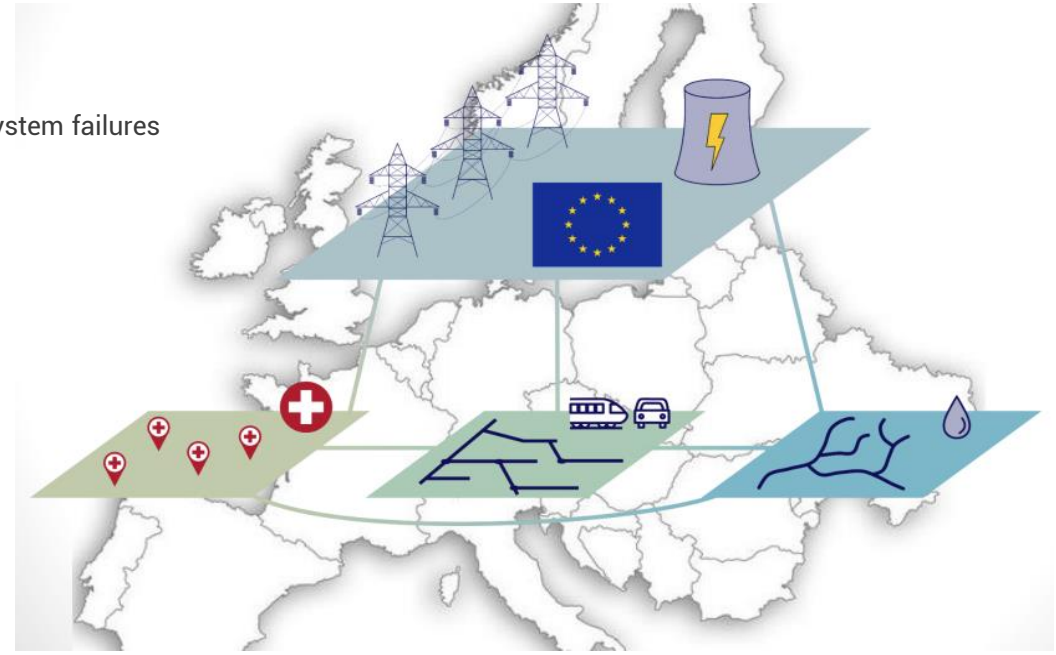
03. INFRA-01-01: Facilitating strategic cooperation for essential services.

+ **NAME :** Enhanced preparedness of interdependent critical entities by framework-based assessing and monitoring cross-border risk and resilience – CRITMON

+ **COMPANY :** University of Wuppertal

+ **CONTACT :** sbach@uni-wuppertal.de
daniel.Lichte@dlr.de

+ **BRIEF :** **Cross-border risk and resilience monitoring framework**
- ↗ (Standardised) indicator set for CEs
- ↗ Cross-/trans-border risk network connecting different layers of Ces
- ↗ Exemplary features
- ↗ Simulation of consequences of (local) disruptive events and component or sub-system failures
  - Situation picture and map (risk monitoring



+ **NEEDS :**
- Tandems of research partner with a national (regulatory) agency, covering a specific (set of) CEs
- (European) Associations representing CEs

INFRA-01-01: Facilitating strategic cooperation for essential services.

+ **NAME :** Resilience of $N \pm \{m\}$ redundant CI/IT systems against multi-threats $\{t\}$ through large-scale extreme value simulation

+ **COMPANY :** Fraunhofer EMI

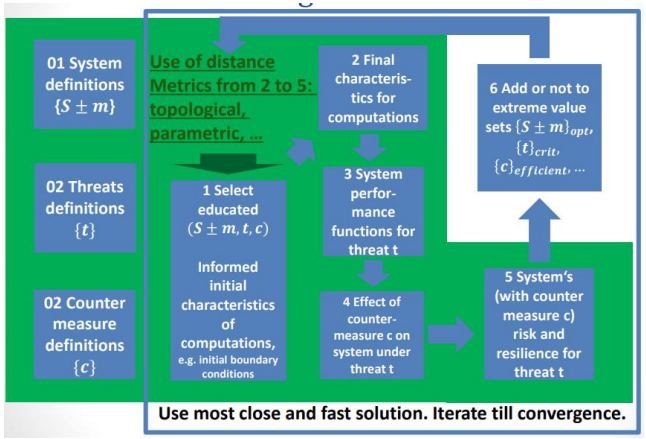
+ **CONTACT :** haering@emi.fraunhofer.de

+ **BRIEF :** Myriads of possible multiple threat events t affecting 1, 2, … of N system elements.

- ↗ Approach to identify most critical ones
- ↗ Approach to identify most efficient counter strategy c
- ↗ Takes redundancy design $N \pm \{m\}$ of system S into account
- ↗ Approach to overall extreme value problem of finding efficiently set of most critical multi threats of cardinality l = 1,2, …

$$\underset{computation\ ressources}{min} = \left\{ \begin{matrix} \max\limits_{t \in \{t\}} Risk\ of\ t \text{ on } S \text{ (with } c) \\ |t| = l \end{matrix} \right\}$$

- ↗ Approach to **determine most efficient overall set of countermeasures** $\{c\}$ by comparing sets of critical threats and resulting risk and resilience measures



+ **NEEDS :**

- Commercial companies providing large scale commercial simulation tools for operators of single CI or Cyber domain systems.

E.g.: Commercial Electricity, gas, water, waste water, railways, national/international roads, inland navigation, bank transfer system…

- Open source organizations for CI or Cyber network simulation tools
- Large scale CI or Cyber grid European operators, e.g. transnational wind or solar farm health monitoring system operators

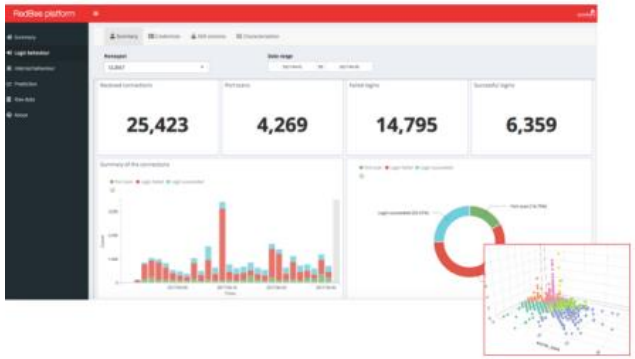
INFRA-01-02: Reinforce the resilience of critical infrastructures.

+ **NAME :** REACT - Enhancing the protection of European Critical Infrastructures

+ **COMPANY :** Gradiant (RTO, Spain)

+ **CONTACT :** Ladkinson@gradiant.org

+ **BRIEF :** System for reacting dynamically to physical and cyber threats on European critical infrastructures. It will cover the prediction, assessment, prevention, detection and response to these threats.



The **cyber protection** of the CI will be enabled through:

- A cyber-deception solution based on **honeypots** and supported by advanced AI algorithms, that allows to characterize and predict cyber attacks
- The **modeling of the behaviour** of CI operators, in order to detect insider threats
- Other prevention and mitigation strategies (TBD)

The proposal will also consider the **physical protection** of the CI, taking into account natural hazards, accidents, terrorism, among others.
It will consider possible **cascading effects** of a disruption on the CI.
The proposal could take into account data from the CI, as well as other additional data such as the weather forecast, market predictions…

+ **NEEDS :**

- 3 infrastructure owners and operators (include civil protection authorities) from different EU Member States,
- Partners for the physical protection of the critical infrastructure
- Partners for the cyber protection of critical infrastructure focused on : Prevention • Response
- Others : ICS/SCADA honeypots developers • Public authorities • Social scientists

INFRA-01-02: Reinforce the resilience of critical infrastructures.

+ **NAME :** Cyber and non-cyber holistic support toolbox and integrated system for resilient infrastructures

+ **COMPANY :** SIMAVI

+ **CONTACT :** monica.florea@simavi.ro

+ **BRIEF :** Strengthening **cross-sector resilience of interconnected and interdependent critical infrastructures** by implementing a cyber and non-cyber holistic support toolbox and integrated system aiming at providing **improved situational awareness, preparedness/mitigation, response and recovery types of intervention**.

- ↗ Development of digital twin-driven simulations with a focus on specific critical infrastructure sector operators (OECD, July 2019) selected for each piloting
- ↗ country that has the potential to generate cascading effects between them;
- ↗ "Swarm leaning" approach to employ an ensemble learning feature for increasing the robustness of the AI algorithms;
- ↗ Real-time multimodal data fusion tools & techniques for enhanced detection and prediction;
- ↗ Cyber and non-cyber Vulnerability Assessment and Anomaly Detection tools in networked critical infrastructures;
- ↗ Advanced operators systems integration & interoperability for protection, seamless recovery and operational continuity;
- ↗ Pilot validation and demonstration activities in Romania and other EU countries with critical operators testing against cyber and non-cyber threats in specific sectors such as: Utility companies, Hydropower plants, DSOs/TSOs, Hospitals, Airports & Ports, etc.

+ **NEEDS :**

- R&D organizations / other technology providers specialized in cybersecurity for critical infrastructures, integrated process and testing in cybersecurity
- Other critical infrastructure pilots

+ **NAME :** Vigilant maritime surveillance

+ **COMPANY :** Laurea University of Applied Sciences, Finland

+ **CONTACT :** johanna.karvonen@laurea.fi

+ **BRIEF :** **The vigilant maritime surveillance project aims to :**

- ↗ Provide support to the resilience of Critical Infrastructure operators against threats to the European subsea critical infrastructure
- ↗ Strengthen the surveillance of European maritime EEZ and beyond with an automated anomaly service recognition service to significantly reduce the risks and exposures to anomalies or deliberate events
- ↗ Strengthen cable protection through improved ndustry cooperation (between cable owners, telenetwork operators, etc.) and cooperation between the industry, the member states, and the EU
- ↗ Improve the information sharing of systematic data on regulatory agencies, regulatory regimes concerning the laying and repair of cables, current protection measures, national surveillance capabilities and operations, cable ownership, and damage incidents as well as suspicious activity

+ **NEEDS :**

- Infrastructure operators for subsea cables (Industry)
- Civil protection authorities
- Expert on cyber cryptic solutions
- Public authorities interested in CER directive implementation requirements (ministries, EU actors, national organizations)

INFRA-01-02: Reinforce the resilience of critical infrastructures.

+ **NAME :** SitAw societal resilience

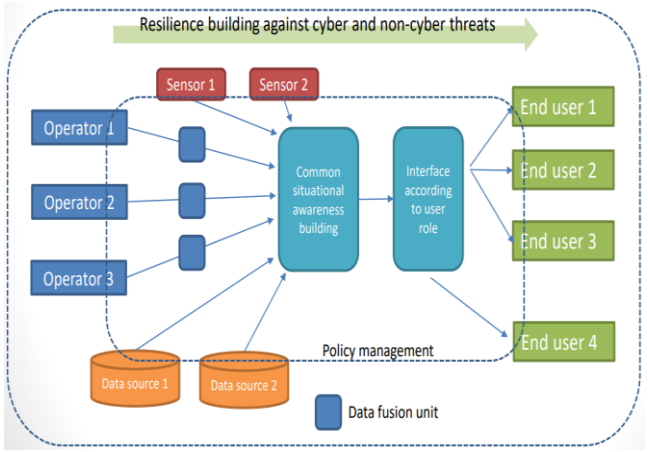
+ **COMPANY :** VTT Technical Research Centre of Finland Ltd.

+ **CONTACT :** jaana.keranen@vtt.fi

+ **BRIEF :**

- **Modelling the systemic network of operators and stakeholders in complex crisis** to improve coordination of multiple actors, clarify areas of responsibility, and support decision-making and priorisation of activities;
- Developing **reliable** and **dynamic situational awareness**, **preparedness** and **governance** by integration of multitude data sources and mobile applications to enable timely coordination of measures;
- Developing **resilience plan conception method** to increase combined **cyber** and **physical resilience** considering both rapidly evolving changes and long-lasting exceptional situations;
- **Building visual** and **easy-to-understand** presentation of processed information for diverse end users as part of situational awareness;
- **Implementing simulation of crisis situations** as part of training of operators and citizen guidance planning.

Situational awareness for societal resilience



+ **NEEDS :**

- Practitioners/beneficiaries such as infrastructure operators, civil protection/ public authorities
- Technology providers, e.g., in the field of situational awareness, security, data platform for coordination and communication, data visualization

INFRA-01-02: Reinforce the resilience of critical infrastructures.

+ **NAME :** Resilience Assessment of Interlinked Critical Infrastructure

+ **COMPANY :** Fraunhofer EMI

+ **CONTACT :** Kris.Schroven@emi.fraunhofer.de

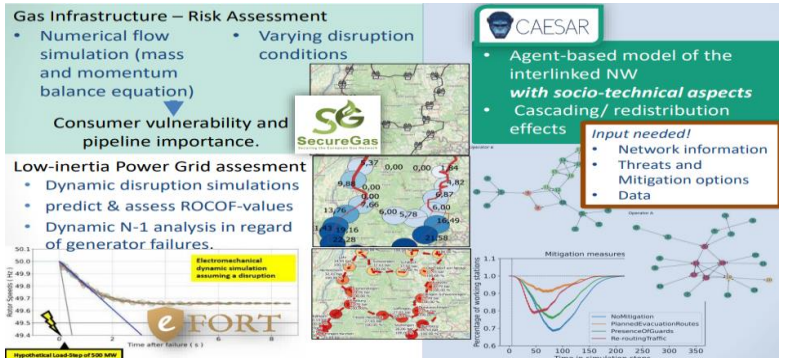
+ **BRIEF :**

Assesment tools EMI provides :

- ↗ **Agent-based simulations** of **cascading effects** for **coupled infrastructures** in case of various threats,
- ↗ **Dynamic simulations** of **gas** and **energy grids** at a well-balanced level of detail accounting for most important grid components
  - Hydraulic-gas-network-modelling accounting for e.g., pipelines, compressor-stations, pressure-regulators, flow-regulators
  - RMS-power-grid-modelling accounting for e.g. lines, synchronous-machines, AVRs, speed-governors, loads

We are looking for :

- ↗ **Information/ data** of interlinked critical infrastructure networks
- ↗ Relevant **threats and mitigation options**
- ↗ New or upcoming, **game-changing technologies** in the critical infrastructure field
- ↗ Ways to consider **socio-technical aspects**



Our tools for System Analysis

+ **NEEDS :**

- Critical infrastructure operators/ providers
(e.g. power supply, gas, railway, water supply, air traffic, logistics)
- Cities/ municipalities providing coupled infrastructure networks to perform resilience assessment
- Technology developers/ institutes to take into account upcoming developments in the critical infrastructure field
- Expertise in the field of socio-technical aspects of critical infrastructure (e.g. customers or operating staff)

04. INCREASED CYBERSECURITY.

- CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)
- CL3-2023-CS-01-02: Privacy-preserving and identity management technologies
- CL3-2023-CS-01-03: Security of robust AI systemsa

CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces).

+ **NAME :** ARIES - **AI** based technologies for the p**R**otection of **IoT** Eco**S**ystems

+ **COMPANY :** Gradiant (RTO, Spain)

+ **CONTACT :** ladkinson@gradiant.org

+ **BRIEF :** The focus of **ARIES** is to secure advanced IoT infrastructures, such as smart cities, covering the communication of the devices, their data collection and
processing, and the integration of new untrusted devices in the infrastructure.
The platform will include a set of technological modules to enable the automated **detection, analysis, and mitigation of cybersecurity attacks** on the cloud and edge.

The proposal will include the following :

- **AI based tools** for cyber threat intelligence, including the use of **anomaly detection** (AD) techniques and the analysis of **honeypots** data
- **Reinforcement Learning** (RL) techniques to improve the resilience of IoT devices against cyber attacks
- **Confidential and verifiable computing** (CVC) in the edge
- Securizing communications and device identity

+ **NEEDS :**

- Software technology providers
- Industry partners
- Use cases

CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces).

+ **NAME :** New tools for Cyber threat intelligence

+ **COMPANY :** Amadeus

+ **CONTACT :** vincent.rigal@amadeus.com

+ **BRIEF :** Build a project that will gather **several cybersecurity use cases** around the web protection :

- ↗ Advanced **anti-bot detection** and mitigation for e-commerce websites: new methods for scrapers identification behind Residential IP Proxies (RESIP) that use **IoT devices**
- ↗ Automated **cyber threat intelligence** to better protect IT environment
- ↗ **AI attacks** management

Amadeus will develop above three listed solutions for the travel industry sector

Other consortium's partners expertise already identified :

- ↗ Federated machine learning
- ↗ User behaviour data analysis capabilities

+ **NEEDS :**

- Partners that provide OT (operational technology) systems
- IoT / OT systems with exposure to Internet, directly or indirectly, or physical security systems also
- Multi-cloud technology providers

04. CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces).

+ NAME : CLEARANCE - Communication soLution for a sEcure And interoperable computiNg Continuum Environment

+ **COMPANY :** Citypassenger

+ **CONTACT :** ycornilliere@citypassenger.com

+ **BRIEF :** **CLEARANCE** aims to secure the transformation of our digital society from a legacy network of interconnected components to a complex, connection-persistent, massive and highly heterogeneous Computing Continuum ecosystem.

- **Demonstrate robust and interoperable** network implementations for IoT/Edge/Cloud Computing Continuum towards a new paradigm for wider adoption.
- **Zero-Trust architectures & lifecycle management** and obsolescence for IoT to address IoT being the weakest part of the Computing Continuum.
- **Fine granular management of the different levels of privileges**, especially in a mutli-entities context, to guarantee a secure usability of resources augmenting user-centric privacy.

+ **NEEDS :**

- Additional End Users to provide use cases for the validation
- IoT environment industrial
- Zero-trust technology provider
- Expert in AI for cyber threat
- Academics labs are welcome

04. CS-01-02: Privacy-preserving and identity management technologies.

+ **NAME : PERSONA** - **P**rivacy-pr**E**serving compr**E**hensive **SO**lutions forbetter health a**N**d rese**A**rch

+ **COMPANY :** Defence Research Institute

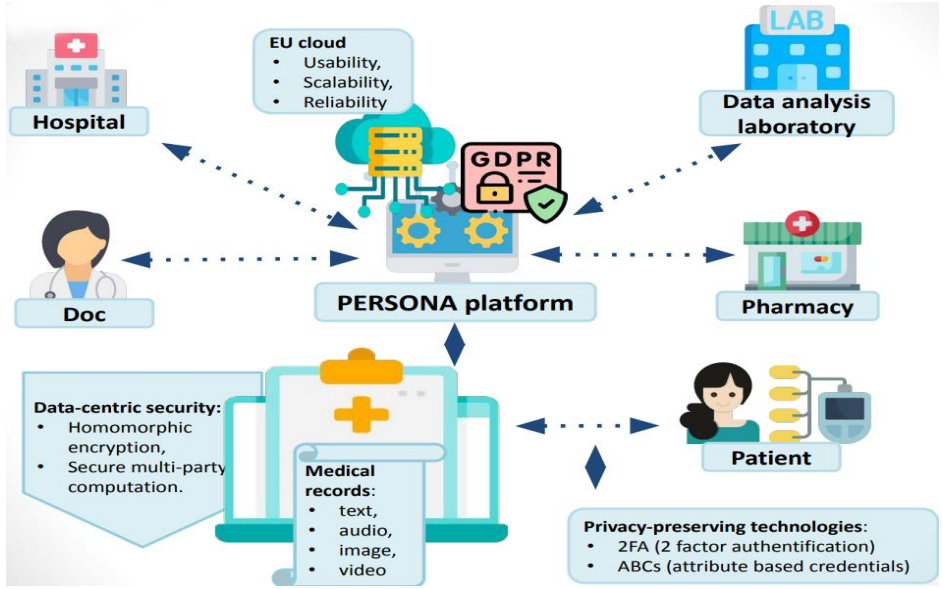
+ **CONTACT :**
alessandro.marani@defenceresearchinstitute.eu

+ **BRIEF :**

OBJECTIVE : making the exchange of healthcare information more secure, privacy-oriented for the benefit of users.

SOLUTION : an integrated and interoperable platform for data sharing while fully respecting users' privacy.

DRI has already involved **2 large hospitals** in this proposal !



+ **NEEDS :**

- Healthcare) system integrators and developers
- IoT experts
- Cyber threats and Cryptography experts
- Experts in digital identity
- Cloud and data-storage providers
- SMEs in the field of healthcare

CS-01-02: Privacy-preserving and identity management technologies.

+ NAME : The eID Wallet

+ COMPANY : Locknest

+ CONTACT : Pierre.LeRoy@locknest.fr

+ BRIEF :

The **eID Wallet** project will design, create and commercialize an ecosystem centered around a **reliable** and **easy** to **use physical device** for **small and medium enterprises**. It will store, protect and distribute the user's **digital identity.**

This project will:

- ↗ Offer a **physical,** state of the art, secure **digital identity wallet.**
- ↗ **Increase** the **security** by drastically reducing the attack surface.
- ↗ Be compliant with all **existing authentication infrastructures** and operating systems.
- ↗ Provide **privacy by design**, data are only available to the data owners who has a **complete control** over their **personal data**.

+ NEEDS :

- Design and production of enclosure.
- Hardware and software pentesting.
- Legal expertise on GDPR and data privacy issues.
- SaaS/Cloud infrastructure partner.

- ↗ Be **Open Source** and **Open Hardware**.
- ↗ Be **scalable** by design in a complete ecosystem (Hardware, Cloud, Software solution).
- ↗ Enforce **GDPR**.
- ↗ Use **Self-Sovereign Identity** management technology.

The eID Wallet: Ecosystem

CS-01-02: Privacy-preserving and identity management technologies.

+ **NAME :** Enhanced cyber threat intelligence on a privacy preserving and federated computation

+ **COMPANY :** Gradiant (RTO, Spain)

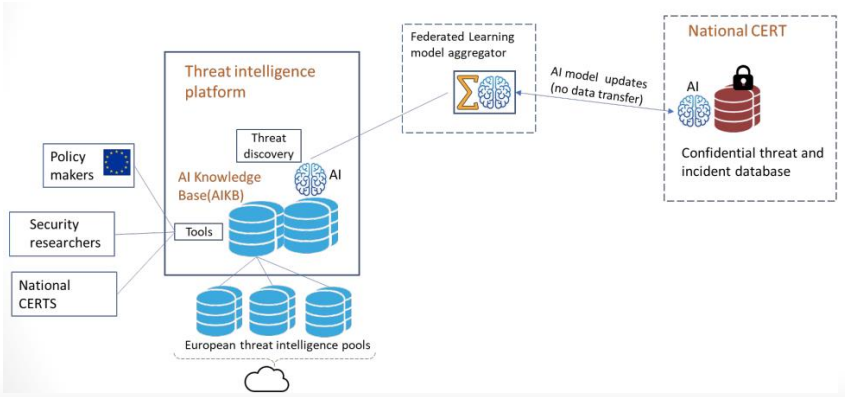
+ **CONTACT :** ladkinson@gradiant.org

+ **BRIEF :** The aim of the proposal is to **create a reliable privacy preserving federated platform** for sharing and improving cyber threat intelligence.
Platform for predicting zero day attacks based on AI analysis of pooled national threat and incident data.
Privacy of data contributors (attack victims) and CERTs is 100% preserved.
Validation or piloting of privacy-preserving computation in realistic federated data infrastructures.

The platform will include the use of:

- ↗ Improved scalable and reliable privacy-preserving technologies for federated processing of cyber threat intelligence and their integration in real-world systems: Differential Privacy, Secure Multi-Party Computation, Multi Key homomorphic encryption and trusted Execution Environments
- ↗ Privacy by design and privacy metrics
- ↗ Effective FL algorithms and aggregator methods

+ **NEEDS :**
- Federated learning algorithms experts
- Cyber Threat Intelligence experts
- Policy makers and GDPR experts
- CERTs



CS-01-02: Privacy-preserving and identity management technologies.

+ **NAME :** Scalable and reliable privacy-preserving technologies for self-sovereign identity solutions

+ **COMPANY :** TREE Technology

+ **CONTACT :** Santiago.macho@treetk.com

+ **BRIEF :** The aim of the proposal is to **create a novel platform to generate, validate and custodian the citizens' digital identity in an agile, secure and privacy preserving way.** This proposal will be based on **IMPULSE**, an ongoing H2020 project which consists of a novel eID management system that can be integrated as a new option into online public services.

The platform will include the use of :

- The European self sovereign identity framework on top of European Blockchain service Infrastructure (issuer, verifier and holder)
- Support for new selective disclose verifiable credentials in order to attest specific user's identity attributes in a privacy-preserving way
- Zero knowledge proofs for blind users' identity attribute checking
- AI-based algorithms for document verification and fraud detection, including Manipulation Attack Detection (MAD) and Presentation

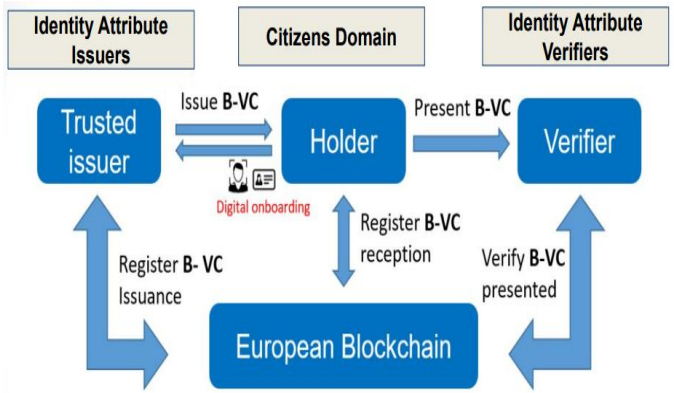


Figure 1: Entities or organizations involved in the SSI scheme

B-VC : Blind verifiable credential

+ **NEEDS :**

- Trust Service Providers
- Multi-Biometric techs experts
- Policy makers: GDPR and eIDAS experts
- Use cases (verifiers and issuers)

+ NAME : MAP - Multimodal Authentication Platform

+ COMPANY : SESTEK

+ CONTACT : tuba.arslan@sestek.com

+ BRIEF :

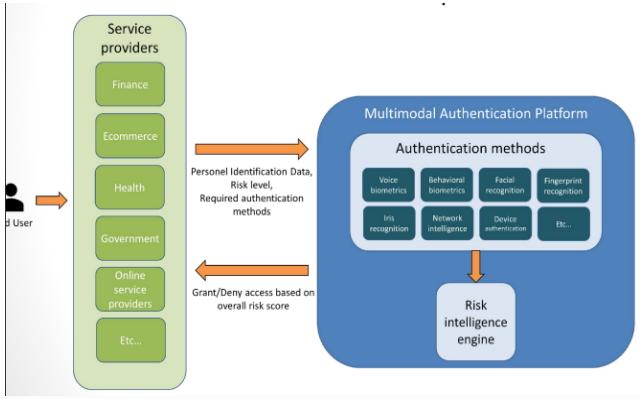
Deliver an intelligent & modular multimodal authentication platform.
Expand intelligent authentication concept **beyond authentication of a single modal.**
Support real-time (often passive) use of **multiple biometric factors**, informed **by other modalities**.
Orchestrate with **AI-infused decision engines**.
Secure and reliable **identity management** and **privacy protection**, enabling **federated sharing** and processing of both personal and industrial data.
Enhancing security-sustaining tools for **cyber threats.**

+ NEEDS :

- Coordinator
- Technology providers: authentication of different modalities, federated learning, identity protection
- Standardization
- Use case providers willing to test and use final platform

MAP Project aims to deliver an intelligent authentication platform & 3rd party services in line with the Commission's "European Digital Identity Architecture and Reference Framework" concept to be enabled by;

- Contribution to promotion of **GDPR compliant** European data spaces
- **Self-sovereign** identity management technologies and solutions
- Authentication of different modalities
- Diverse of authentication methods
- AI-infused risk intelligence engine
- End-to-end value chain
- **Modular structure**
- Serve different verticals



04. CS-01-03: Security of robust AI systemsa.

+ NAME : Security of robust AI systems (no title available yet)

+ **COMPANY :** KEMEA

+ **CONTACT :** g.kokkinis@kemea-research.gr

+ **BRIEF :** Design and develop a **Security-by-Design AI framework**.

Include **SOTA context awareness in ML** in this framework.

Pilot this framework against selected areas of adversarial attacks.

Benchmark resiliency of the developed FW against existing solutions

Consider proposed Artificial Intelligence Act and

- ↗ Submit policy recommendations
- ↗ Produce best practices for implementation
- ↗ Context awareness
- ↗ Resilience
- ↗ RobustnessConfidential and verifiable computing (CVC) in the edge

+ **NEEDS :**

- End user needs
- Pilot design and evaluation
- Dissemination, Communication, outreaching (Lead / Support)
- Ethical and Legal (Lead Support)
- Policy recommendations

+ **NAME :** Sec-AI - **Sec**urity technologies for a verifiable and resilient **AI**

+ **COMPANY :** Gradiant (RTO, Spain)

+ **CONTACT :** ladkinson@gradiant.org

+ **BRIEF :** The aim of **Sec-AI** is to **create a reliable platform** involving a set of coordinated security technologies to build reliable, verifiable and resilient AI models.The project will research the state-of-the art of novel attacks against AI models and data.
Sec-AI will explore the **impact of an attack on different types of AI models**, such as Federated Learning (e.g., assuming a malicious participant on the network, poisoning the exchanged parameters during the training process) or Deep Learning (e.g., reducing the accuracy of a class, weight poisoning), among others.

The project will explore **possible defenses**, such as the use of :

- ↗ Interpretable Machine Learning (IML) techniques for increasing robustness and tackling **adversarial attacks** against central and federated learning models.
- ↗ Verifiable and confidential technologies for **computing AI on the edge** (Trusted Execution Environments and Zero Knowledge proofs)

Sec-AI will include **the validation of the developed mechanisms and the definition of metrics** to assess the impact of the attacks.

+ **NEEDS :**
- Machine and Deep learning experts
- Security by design experts
- AI regulatory and certification schemes experts
- Use cases

04. CS-01-03: Security of robust AI systemsa.

+ **NAME :** DETECT-AI

+ **COMPANY :** TREE Technology

+ **CONTACT :** Santiago.macho@treetk.com

+ **BRIEF :**

Motivation :

- The collection of data from different sources is becoming increasingly (health, industry and computer security).
- This poses several challenges: biased, erroneous or event fraudulent/poisoned data.

Consequence :

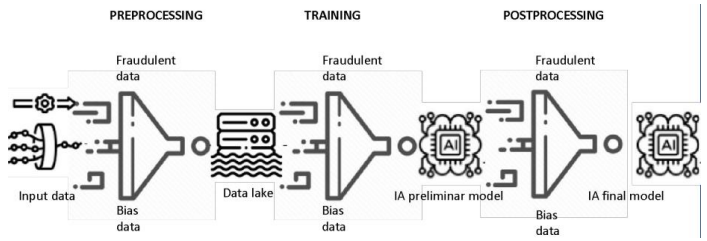
- Negative impact on the quality of the extract information

Non accurate decision-making

+ **NEEDS :**

- Cybersecurity
- Machine Learning
- Platform developer
- Data providers (health, industry, computer security, ….)

We propose **the development of a new platform** that enable users to automatically detect and **correct attacks targeting ML models**, biased, erroneous or fraudulent/poisoned data.



This platform will be based on **Machine Learning and data analytics techniques** to identify anomalous patterns in the data and flag them for further review and correction and/or discard them.

04. CS-01-03: Security of robust AI systemsa.

+ **NAME :** New Generation AI Systems for Security

+ **COMPANY :** ZEUS consulting

+ **CONTACT :** info@zeusconsulting.com

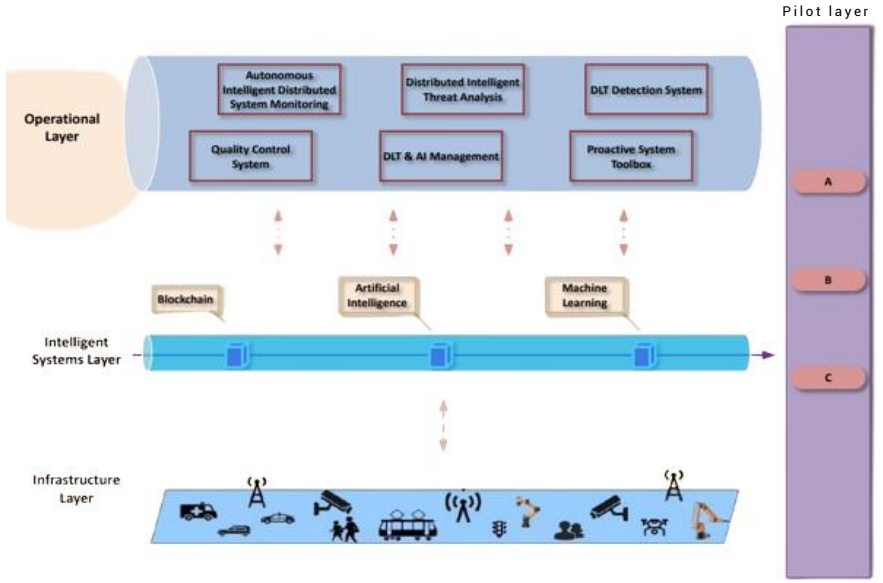
+ **BRIEF :**

Digital AI-Infrastructure for cyber-attack and hybrid-threat preventions;

Increased software, hardware and supply chain mitigation measures against cyberattacks in AI Systems;

Security of cross-border knowledge and data sharing;

Establishing a **reinforcement of awareness** and a common cybersecurity management and culture.



+ **NEEDS :**

- Technical AI/ML Expert
- Big Data Analytics
- System Integrator
- Pilot Cases

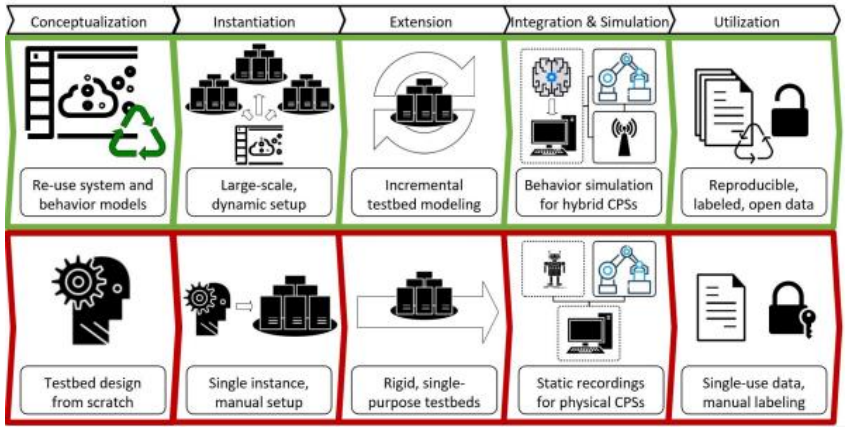
04. CS-01-03: Security of robust AI systemsa.

+ **NAME :** HORIZON-CL3-2023-CS-01-03

+ **COMPANY :** AIT

+ **CONTACT :** markus.wurzenberger@ait.ac.at

+ **BRIEF :** **Development of AI algorithms for intrusion and attack detection in system logs** (e.g., syslog, syscalls/audit logs, application logs, web logs) and network traffic;
Model-driven testbed approach to generate large and realistic labelled log data sets to evaluate and test AI algorithms;
Study and enable certification of AI algorithms within AIT's testbed;
Apply the concept of digital twins to simulate attacks against CPS and OT to improve AI algorithms;
Detect and mitigate effects of adversarial ML;
Application of reinforcement learning to improve robustness and resilience of AI intrusion detection algorithms.



+ **NEEDS :**
- Looking for an appropriate consortium

04. CS-01-03: Security of robust AI systemsa.

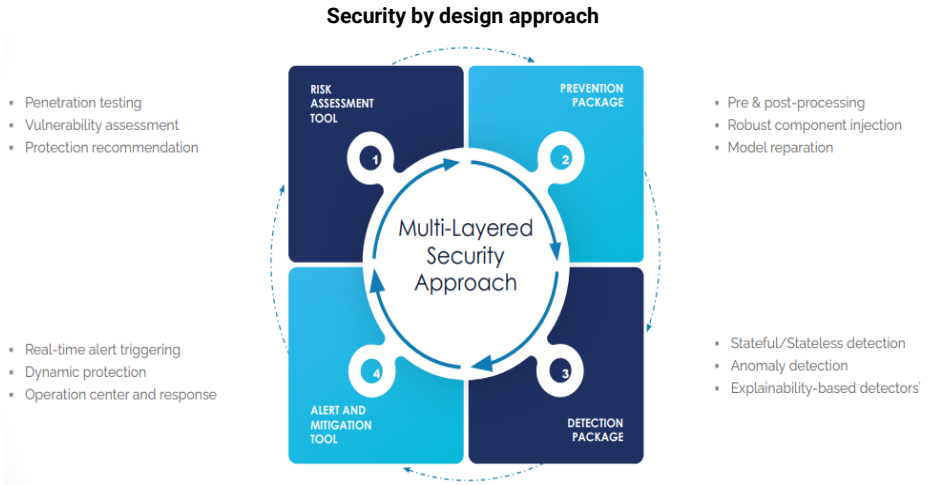
+ **NAME :** Security of robust AI systems

+ **COMPANY :** DeepKeep

+ **CONTACT :** rony@deepkeep.ai

+ **BRIEF :** **Create an automated software platform that will provide the following layers of AI security:**

- **Risk analysis:** run multiple tests and attacks on AI models & datasets and uncover risks and vulnerabilities. The tool will also generate a risk assessment report.
- **Prevention layer:** fortification and prevention functions against adversarial attacks
- **Real-Time attacks detection & mitigation:**
  - Detection layer: deploy a variety of detectors on AI models to detect adversarial attacks in real-time
  - Mitigation tool: concrete tools for tracking and mitigating attacks in real time



+ **NEEDS :** **Use cases : Large Enterprises from the BFSI/Automotive/Government sectors**
R&D : Enterprises and Academic institutions with expertise in:

- Adversarial AI (Evasion, Stealing, poisoning, etc.)
- Trustworthy AI (weak spots, OOD, XAI, confidence, etc.)
- AI ethics and regulation (AI ACT)
- ML context awareness

04. CS-01-03: Security of robust AI systemsa.

+ **NAME :** AI-AutoSec - AI Privacy, Security, Reliability and Accountability by Design

+ **COMPANY :** University of Reading

+ **CONTACT :** atta.badii@reading.ac.uk

+ **BRIEF :** AI-AutoSec will develop **ML Pipelines** to support Anomaly Detection for at least three application domains deployed as benchmarking testbeds. These will **deploy a number of already optimised top performing ML algorithms** applied to research datasets including synthetically generated datasets and evaluated using a range of metrics.

The following approaches will **inform the Countermeasures Prioritisation** within the AI-AutoSec approach to Integrated **Privacy**, **Security**, **Reliability** and **Accountability** by Design of AI Solutions:

- ↗ Context-Aware Risk-Based Model-Driven Threats Ranking and Vulnerabilities Analysis including against Adversarial Attacks
- ↗ Interpretability, Systemic Bias and Reliability Analysis
- ↗ Ethical Compliance Analysis

Privacy, Security, Reliability and Accountability by Design will be informed by the relative efficacy of a range of Countermeasures including retraining, gradient masking, recycling and AI-enabled synthesis techniques to ensure Accountability, Reliability and Robustness to Adversarial Attacks by Design.

+ **NEEDS :**

- Use-Case Partners in Health, Security, Multi-modal Mobility
- Use-Case Partners in Other Domains
- Partners for Solution Integration and Evaluation
- SSH Partner

05. DISASTER-RESILIENT SOCIETY FOR EUROPE.

- CL3-2023-DRS-01-01: Improving social and societal preparedness for disaster response and health emergencies
- CL3-2023-DRS-01-02: Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)
- CL3-2023-DRS-01-05: Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments
- CL3-2023-DRS-01-06: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery

DRS-01-01: Preparedness for disaster response and health emergencies.

+ **NAME :** Disastrous Communications (DISCO)

+ **COMPANY :** VTT Technical Research Centre of Finland

+ **CONTACT :** ville.ollikainen@vtt.fi

+ **BRIEF :**

Addressing Disaster-Resilient Society 2023

- Project proposal: Disasterous Communications (DISCO)

The BASIC idea is to focus on communications

- Make official communications transparent (proven authenticity) and prevailing over fake/disinformation
- Target communications to vulnerable people; focus on basics, helping also others to understand
- Create a fast lane to online advertising and digital signage platforms, etc.

+ **NEEDS :**

- Media industry, content producers
- Fake news analysis
- Healthcare, pandemics, diagnostics,…
- Steganography
- Social / social media / social graph experts
- Digital signage, online advertising, …
- AI / ML
- NLP
- Everyone who feels having something relevant to the call

DRS-01-01: Preparedness for disaster response and health emergencies.

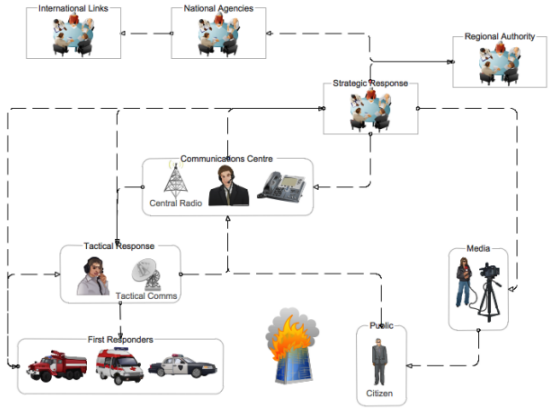
+ **NAME :** Societal Enhanced Framework for Emergency Resilience (SAFER)

+ **COMPANY :** Trinity College Dublin

+ **CONTACT :** Derek.Ross@tcd.ie

+ **BRIEF :** **Resilience Framework** and **Solutions** across society actors that fosters inclusive pro-active risk management capacity building.

This will accommodate **pluralism, diversity** and **equality** through innovative socio-technical systems analysis.



Spontaneous unAffiliated Volunteers in Emergency Response Systems
SAVERS

SMS4EMS

+ **NEEDS :**
- Gender, Diversity, Inclusion
- Resilience tools and solutions
- AI and ML

DRS-01-01: Preparedness for disaster response and health emergencies.

+ NAME : Cross Culture Disaster Response for All

+ **COMPANY :** AAHD

+ **CONTACT :** ismailumitbal@gmail.com

+ **BRIEF :**

Health illiteracy and inequalities are barriers for effective disaster response. **Crisis communication** (4 all) for acute situations so gain resilience to use Crisis time. Considering all languages, gender, etc…

Community Based DRR training, (Living Lab and APPs);

Surveillance (app?) for **early detection of emerging zoonosis** (Syndromic Surveillance, severity, geographic distribution, host, transmission routes, etc.).

Thermal drone, Crowdsourcing, monitoring + Public Health;

Preparation of mobile Living Labs to use the most vulnerable areas;

AAHD has been responding to **all kinds Disasters** and **unexpected incidents**;

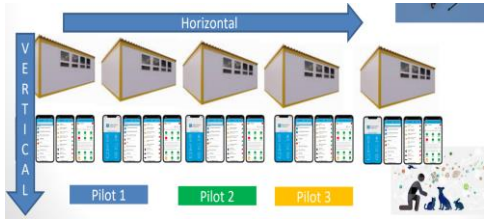
AAHD can provide; **KPIs, User requirements, Use Cases, Tailor-made scenarios;**

Next Generation Technologies for Emergency and Disaster Response Contributing with the experience from the successfully concluded or ongoing **H2020 Projects;**

Large demonstration capabilities (field testing) for the utilization of largely existing capabilities and combining them into a single, user-friendly platform.

+ **NEEDS :**

- University (Infectional dis. clinic / Law)
- Children/elder care NGOs
- SME -(positioning, AI, ChatGPT)
- Large Industry (Crowdsourcing, app, drone-termal)
- CSO (SSH- Gender)
- FRs



DRS-01-02: Design of crisis prevention and preparedness actions.

+ **NAME :** Future Imaginaries

+ **COMPANY :** NTNU Social Research (NSR)

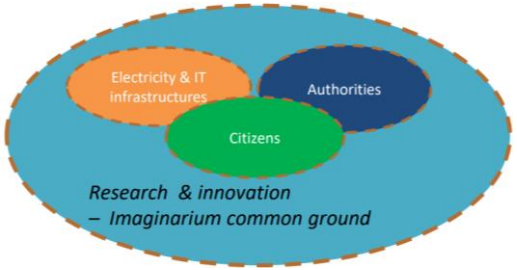
+ **CONTACT :** susanne.hansen@samforsk.no
ivonne.herrera@samforsk.no

+ **BRIEF :** Through co-creation and context-sensitive approaches, the overall objective of **FutureImaginaries** is twofold:

- To co-create knowledge and increase capacity to deal with digital breakdown crises at different levels (local, regional and supranational) and together with relevant energy stakeholders (communities, civil protection, national security, regional and local authorities, private sector responsible for critical infrastructures).
- Contribute with co-created knowledge and systematized experience on strategies dealing with surprising events at community, regional and supranational levels.
- Develop an arena for citizens and authorities to catalyze dialogue and trust.
- To provide policy recommendations to the EU based on the cocreated knowledge; and provide socio-technical solutions for handling interdependencies and cascade effects when dealing with digital breakdown crisis in the energy delivery value chain.
- Capacity building development in action labs where researchers, citizens and stakeholders co-create future scenarios and sociotechnical solution.

+ **NEEDS :**

- Looking for partners to create a consortium or to join a matching one



DRS-01-02: Design of crisis prevention and preparedness actions.

+ NAME : COSIB - **C**risis c**O**mmunication **S**ystems **I**n digital **B**reakdowns

+ COMPANY : ITTI

+ CONTACT : kamila.stroinska@itti.com.pl
andrzej.adamczyk@itti.com.pl

+ BRIEF :

Scope :

- Identification of **interdependencies** among **critical infrastructures** (big metropolises, vulnerable industries & public services) and **services**
- Electricity outage and digital breakdown situations

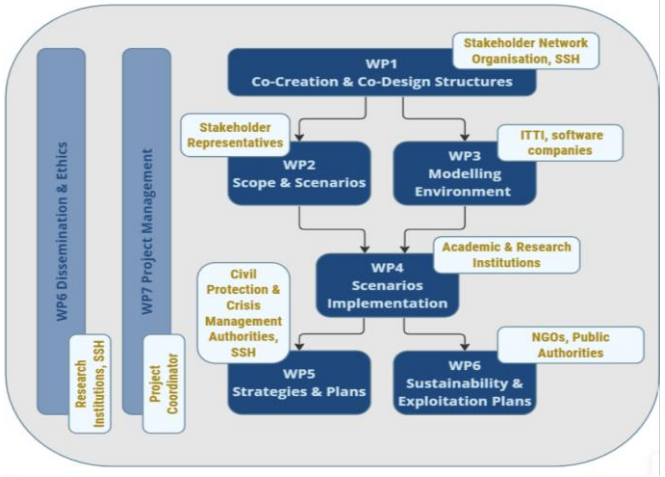
Aim/Goal :

- Development of **citizen-friendly tool**
- **Optimisation of communication systems (including crisis communication) and architectures**

Methodology : **Scenario-based analysis** (cascading effects modelling & simulation, evaluation & optimisation)

Expected results : plans of **prevention and preparedness actions** (including civil protection plans)

Project participants & WP structure



+ NEEDS :

- Proposal coordinator
- Critical infrastructure managers in large metropolitan centers, crisis management/civil protection authorities, private sector and actors responsible for critical infrastructures
- Institutes for applied research in the areas of security, SSH
- Citizen organizations (e.g. organizations with experience in civil contingency planning and training)

DRS-01-05: Robotics systems for use in hazardous environments.

+ **NAME :** UGV4TRIAGE

+ **COMPANY :** AAHD

+ **CONTACT :** turhans112@gmail.com

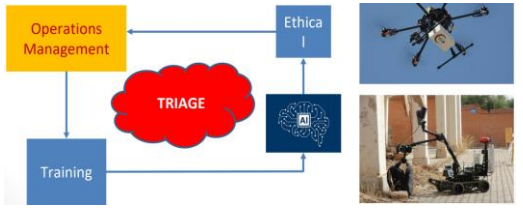
+ **BRIEF :**

- Triage is a life-saving practice in disasters.
- UGV and UAV supported first responders will be able to do more work in less time, with less personnel and more safely
- Triage of the causalities in the hazardous zone could be possible
- More human lives could be saved.
- 'False negative cases identified by AAHD from 2023 Turkiye Earthquakes' will be used
- AAHD can provide; KPIs, User requirements, Used Cases, Tailor-made scenarios, Next Generation Technologies for Emergency and Disaster Response

- Autonomous vehicles are an important area where artificial intelligence is used. We aim for a fast and accurate triage with artificial intelligence supported autonomous vehicles and drones with less people
- Identifying the dangers in the environment, determining the number of casualties to be triaged, remote management of the operation, training of the first responders, and providing a social gain with an ethical and legal practice are among the objectives of the project.

+ **NEEDS :**

- FRs (LEA, Civil defense)
- Technology Provider SME
- Communication Provider Industry/SME
- UGV SME/industry
- SSH CSO-RTO-University



05. DRS-01-05: Robotics systems for use in hazardous environments.

+ **NAME :** CONCORDIA - Enhan**C**ed situati**O**nal aware**N**ess and resilien**C**e Of fi**R**st respon**D**ers in r**I**sky situ**A**tions

+ **COMPANY :** Tree Technology

+ **CONTACT :** javier.gutierrez@treetk.com
rita.Nogueira@treetk.com

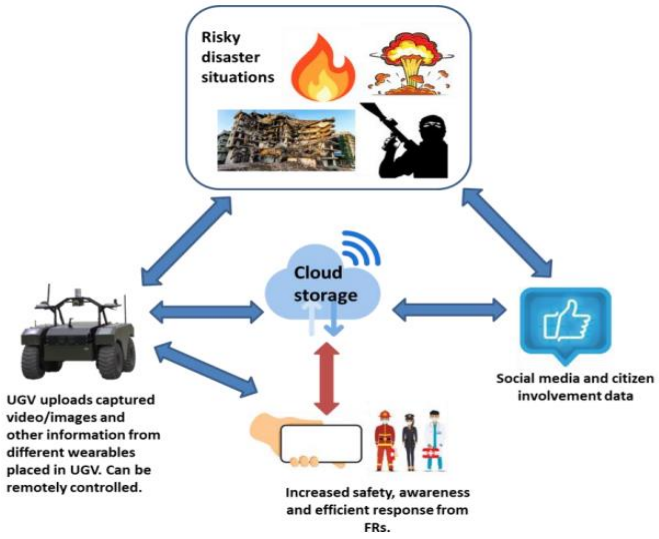
+ **BRIEF :**

Motivation :

- First Responders (FRs) need to be protected, connected and fully aware in disaster situations, to perform their jobs without exposing their lives
- In disasters, the surrounding environment could be risky for FRs

Solution :

- Robotics and automated systems can help increase productivity and efficiency to prevent, prepare, and/or respond disasters situations
- Fusion of information from several types of sources
- Enhances reaction capability/time, flexibility and crisis management,without endanger FRs, through autonomous systems



+ **NEEDS :**

- Human Machine Interface
- Robotic/wearables systems
- Mobile interfaces

DRS-01-05: Robotics systems for use in hazardous environments.

+ **NAME :** NextGen Rovers

+ **COMPANY :** Gradiant (RTO, Spain)

+ **CONTACT :** ajimenez@gradiant.org

+ **BRIEF :** **NextGen Rovers objective is to improve the situational awareness and communications of UGVs.**

- ↗ Improved positioning accuracy through the use of GALILEO, sensor fusion and the possibility of integrating high-precision local positioning based on UWB
- ↗ Redundant communication system based on datalink (LoS) and cellular communications (3G, 4G & 5G), possibility of integrating satellite communication
- ↗ Image and video processing via AI onboard hardware or via 5G edge computing
- ↗ Route planning and replanning in real time ("provides the vehicle with intelligence to make decisions autonomously")

+ **NEEDS :**

- Law enforcement authorities
- UGV manufacturers, integrators and/or operators
- Sensor manufacturers
- AI experts for decision making
- Legal & ethical partner
- End users experience monitoring and impact

03. DRS-01-05: Robotics systems for use in hazardous environments.

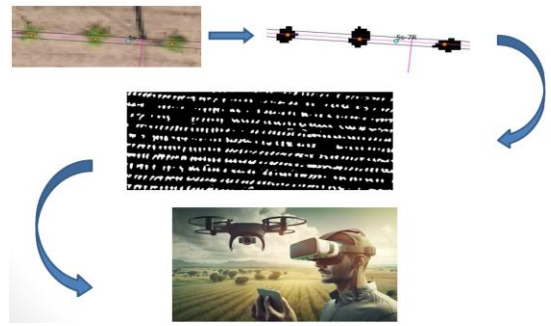
+ **NAME :** Drones for Disaster-Resilient Society

+ **COMPANY :** Czech University of Life Sciences in Prague

+ **CONTACT :** kumhala@tf.czu.cz

+ **BRIEF :**

- Using AI in drones for searching lost people; autonomous search, the operator is contacted upon identification, with the use of VR/AR glasses will decide on the next course of action. The operator can then send a rescue ground drone.
- Participation principle: air drone for mapping, data processing, ground drone performs the intervention according to the data of the air drone.
- Using AI in ground drone for mine detection (war in Ukraine). Autonomous search, the operator is contacted upon identification, with the use of VR/AR glasses will decide on the next course of action.
- Proof-of-concept Research. The use of AR/VR glasses as human-machine interaction technology.



+ **NEEDS :**

- Communication, Dissemination & Exploitation
- Ethics, Legal and Societal area
- Expertise in robotics systems, security, civil protection, strategic planning, etc.
- Pilot sites to test the technology (fire brigade, emergency medical services, etc.)

05. DRS-01-06: Increased decision-support systems for first responders of last-kilometer emergency service delivery.

+ **NAME :** ISLA-FED

+ **COMPANY :** Blockchain2050 BV

+ **CONTACT :** koutsiara@blockchain2050.io

+ **BRIEF :** A Satellite IoT system integrated with smartphones to leverage existing technologies such as(drones, AI, and sensors) and communication technologies to support first and second responders in their immediate response to natural disasters. **Development of a secure and tamper-proof system** for tracking and managing the data generated by the IoT devices and sensors using blockchain technology, to ensure data privacy and security, creating immutable records and automating the management of emergency response workflows.

Expected outcomes

- Identification and evaluation of existing technologies supporting first and second responders in their immediate response to natural disasters, highlighting strengths and weaknesses, through continuous monitoring with accuracy and availability of near real-time data using Satellite IoT devices
- Testing and implementation of promising technologies in real-world conditions with reliable coverage while consuming low power (satellite networks provide coverage where traditional networks will struggle or fail)
- Accurate prediction and rapid assessment of disaster locations and extent of damage to prevent massive devastation

+ **NEEDS :**

- First responders' vehicles – logistics
- Drone-providers
- Authorities of disaster response from at least 3 different EU Member States
- Standardization organizations
- SSH partners
- Other?

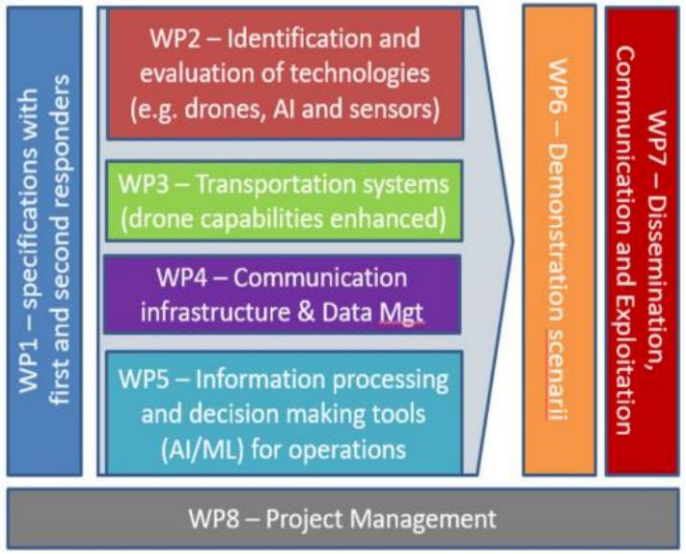
05. DRS-01-06: Increased decision-support systems for first responders of last-kilometer emergency service delivery.

+ **NAME :** TECH4RESPONDERS

+ **COMPANY :** CEA

+ **CONTACT :** jean-philippe.poli@cea.fr
antonin.galtier@cea.fr

+ **BRIEF :** First focus on the needs of first responders for **different typical scenario** in collaboration with **firefighting, medical emergency** and **police forces**.
Technologies : Identify and evaluate the different necessary technologies
Transportation systems : Increase drone capabilities and interfaces for piloting and operations.
Communication : data sharing, security, reliability.
Decision making tools :
↗ Information processing
↗ Sharing for operation enhancement
Demonstration according to scenarii.



+ **NEEDS :**
- First and second responders' organizations or agencies
- Drones and Sensors

05. DRS-01-06: Increased decision-support systems for first responders of last-kilometer emergency service delivery.

+ **NAME :** RESCUED - **R**emote **E**mergency **S**ensor-Based **C**ontrol, **U**nmanned **E**xploration and **D**elivery

+ **COMPANY :** German Federal Agency For Technical Relief

+ **CONTACT :** Nils.Krippner@thw.de

+ **BRIEF :** The RESCUED-project aims to **improve the operational strengths of disaster relief organizations through the use of new technologies such as drones, AI and sensors. It involves identifying and evaluating existing technologies** and testing promising user-oriented solutions in real-life conditions to improve operations in smoky environments, such as forest fires. **Key information will be made available** to first and second responders remotely, enabling effective operations on the ground without endangering their lives. In this context, **last-mile logistical problems** that hinder the delivery of relief supplies to disaster-prone areas are also overcome.

+ **NEEDS :**
- ≥ 3 first responders` organizations
- Representatives of local or IDRM regional authorities from ≥ 3 EU countries or associated countries

05. DRS-01-06: Increased decision-support systems for first responders of last-kilometer emergency service delivery.

+ **NAME : TECHSupport4NDRr** (Natural Disaster Response and Recovery)

+ **COMPANY :** Enide Solutions (Barcelona, Spain)

+ **CONTACT :** radivoj.malic@enide.com

+ **BRIEF :** Supporting first (and second) responders for enhanced response to natural disasters.
Development, testing and implementation of **Decision Support Systems** technologies to support FRs, based on :
- ↗ Telecom data
- ↗ AI for forecasting
- ↗ Surveillance cameras data analyses
- ↗ **Alternative data source very welcome (additional use case or addition to existing)**

Improving Disaster Resilience.
More details available on request to potential candidates.

+ **NEEDS :**
- Additional First/Second Responders : Fire fighters, medical teams; search and rescue (ideally from countries other then Italy, Spain and Turkey from those countries
- Additional Research/Academic Partners (preferably from countries not already involved; but not restricted)
- Drones experts (able to navigate in low visibility: e.g. smoky environments)
- Last-kilometer emergency service delivery experts (emergency logistics)
- Wildfires response experts (from EU)

05. DRS-01-06: Increased decision-support systems for first responders of last-kilometer emergency service delivery.

+ **NAME :** Automated search and rescue concept for buried people after heavy building damage or building collapse

+ **COMPANY :** Fraunhofer EMI

+ **CONTACT :** julia.rosin@emi.fraunhofer.de

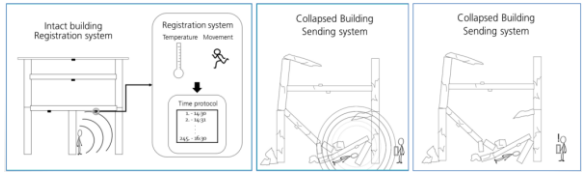
+ **BRIEF :**

↗ Development of country-specific building catalogs with representative buildings and their typical collapse damages

↗ Drone-based scan of damaged area → exact overview of the affected area with number and type of heavy damaged or collapsed buildings

↗ Multifunctional sensor unit for automated and fast detection of buried people → location and number of buried people

↗ Provides information for immediate activity of first responder



↗ Combination of (1), (2), (3) provides the basis for the ad-hoc set-up of a site-specific but also disaster area-wide SAR operation

- Fast reaction since information of (1) and (3) is available immediately after disaster, (2) will be available very quickly
- Overarching operational organization according to demand

↗ Building collapse simulation of representative buildings

↗ Multifunctional sensor unit for automated and fast detection of buried persons under building debris (see figure)

- If a building collapse is registered, information about the presence of persons is sent to the outside
- With a smartphone this information can be evaluated to locate the persons buried under the building debris
- Patent: US20220246016A1, EP4036885A1

+ **NEEDS :**

- Technical engineering company or research institute with ambition to manage consortium
- Companies that are interested in developing the multi-sensor unit (sensor-based building security, manufacturers of smoke and fire detectors or surveillance technology, sensor technology)
- Drone scan of buildings and post-processing of scans
- First responder
- Disaster management authorities, (municipal) administration
- Construction companies with experience in simulating building collapses of country-specific building types

06. STRENGHENING SECURITY RESEARCH INNOVATION.

- CL3-2023-SSRI-01-02: Accelerating uptake through open proposals and advanced SME Innovation

SSRI-01-02: Accelerating uptake through SME Innovation.

+ **NAME :** Secured Social Network

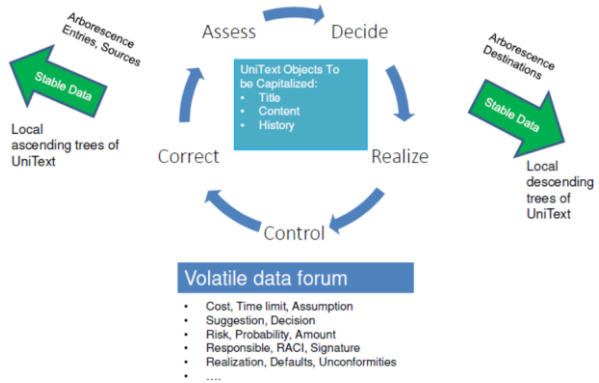
+ **COMPANY :** UniText SAS

+ **CONTACT :** Philippe.Jarrin@UniText.fr

+ **BRIEF :** **The Secured Social Network** concept exists at TRL 5/6 with the UniText concept to be enriched and adapted with existing technological bricks and partnerships agreements

↗ The Goal is to Introduce Lean, Agile, Risk management at the root of a WORM (Write Once, Read Many) DataBase at the root of

- Market place, Calls and Offers in Project Mode/Negotiation
- **Trusted circle of users** where access rights/missions are delegated and mutually watched
- Trusted centralized servers per LEI that securely communicate with each other on high level defined access rights
- Key Information and **Key Characteristics** managed with agility, within virtual or implicit comprehensive documentation (See Agilemanifesto.org)
- Risk Management from design inspired by Aerospace Methodology



+ **NEEDS :**

- Capacity in Web Development to reach TRL 6/8
- Adaptable technological know how in Social Network, Digital Work Place, Collaborative environment
- API Security to manage data Exchange between Secured Servers containing WORM Data Bases
- Cyber Security of WORM Data Bases, where the ransomware vulnerability is far buried within the root system
- Risk management, Lean and Agile methodologies to be included at design level of the Secured Social Network
- End User in Option A, B, C, D of HORIZON-CL3-2023-SSRI-01-02 HORIZON-CL3-2024-SSRI-01-02

CAMPUS CYBER