INFRA SESSION - MODERATORS

Marina Martínez-Garcia
marina.cdti@sost.be

Marco Manso
marco@particle-summary.pt
marco.manso@imgs-eu.org

Katharina Friz
Katharina.Friz@vdi.de

INFRA Review Team:

Elodie Reuge | Katharina Friz | Marco Manso | Marina Martínez | Marta Kollarova

INFRA SESSION - PRESENTATIONS

INFRA-01-01	Adkinson, Lilian	ladkinson@gradiant.org
	Dubec, Branislav	branislav.dubec@unob.cz
	Quitanar Garcia, David	d.quintanar@cedrion.com
INFRA-01-02	Zacharias, Marios	mzacharias@space.gr
	Häring, Ivo	Ivo.Haering@emi.fraunhofer.de
	Kioumourtzis, George	gk@ianus-consulting.com
	Moulin, Thibault & Pons, Christophe	tmoulin@univ-catholyon.fr
(offline)	De Simone, Flavia	flavia.desimone@enide.com
	Felicioni, Licia	Licia.Felicioni@cvut.cz
	Stroińska, Kamila	kamila.stroinska@itti.com.pl
	Železná, Julie	Julie.Zelezna@cvut.cz
INFRA-01-03	Garrido, Sara Garcia	sgarcia@gradiant.org
	Häring, Ivo (Likert, Benjamin)	Benjamin.Lickert@emi.fraunhofer.de
	Faure, David	david.faure@thalesgroup.com
	Jírovec, Martin	jirovec@fit.vut.cz
	Giorgi, Graziano	graziano.giorgi@zanasi-alessandro.eu
	Herrera, Ivonne	Ivonne.Herrera@samforsk.no
(offline)	Dr Safak Dogan & Dr Xiyu Shi	S.Dogan@Lboro.ac.uk

INFRA-01-01

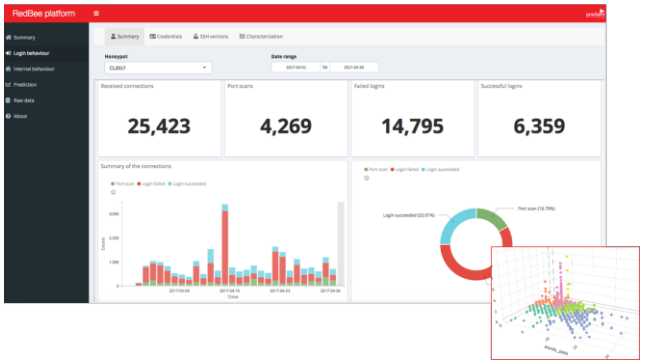
MERLIN: iMproving the protEction of cRiticaL INfrastructures across Europe

- *Lilian Adkinson*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*
- Role: *WP leader, S/T provider*

- Topic to be addressed: *HORIZON-CL3-2024-INFRA-01-01: Open Topic*

Proposal idea/content

- *System for increase the resilience to cyber and physical threats on European critical infrastructures.*
- *It will cover the risk assessment, monitoring, prevention, detection and mitigation of 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*
  - *Advanced **anomaly detection** techniques*
  - *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*
- *The proposal could take into account data from the CI, as well as other additional data such as the weather forecast, market predictions…*

gradiant
Connectivity · Intelligence · Security
for your business

Lilian Adkinson / ladkinson@gradiant.org

Project participants

- Existing consortium:
  - Proposed coordinator: *TBD*
  - Partners / Other participants:
    - *Gradiant (Spain): cyber protection (honeypots and anomaly detection)*
- Looking for partners with the following expertise/ technology/ application field:
  - *2 critical infrastructure operators*
  - *2 civil protection authorities*
  - *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*

gradiant
Connectivity · Intelligence · Security
for your business

Lilian Adkinson / ladkinson@gradiant.org

Critical infrastructure project

- *Branislav Dubec*
- *branislav.dubec@unob.cz*
- *University of Defence, Brno, Czech Republic*
- Role: *Proposal coordinator, WP leader*
- Topic to be addressed: HORIZON-CL3-2024-INFRA-01-01

Proposal idea/content

- **Goal:**
  - To contribute to Cluster 3 Horizon Europe Strategic Plan 2021-2024: Better Protect the EU and its Citizens Against Crime and Terrorism, Effective Management of EU External Borders, Resilient Infrastructure, Increased Cybersecurity, A Disaster-Resilient Society for Europe, Strengthened Security Research and Innovation.
- **By**:
  - **Identification of established and new threats,**
  - **Creating comprehensive infrastructure risk assessment tool,**
  - **Comprehensive cooperation of EU and EU`s partner countries.**

Branislav Dubec, branislav.dubec@unob.cz

Project participants - consortioum

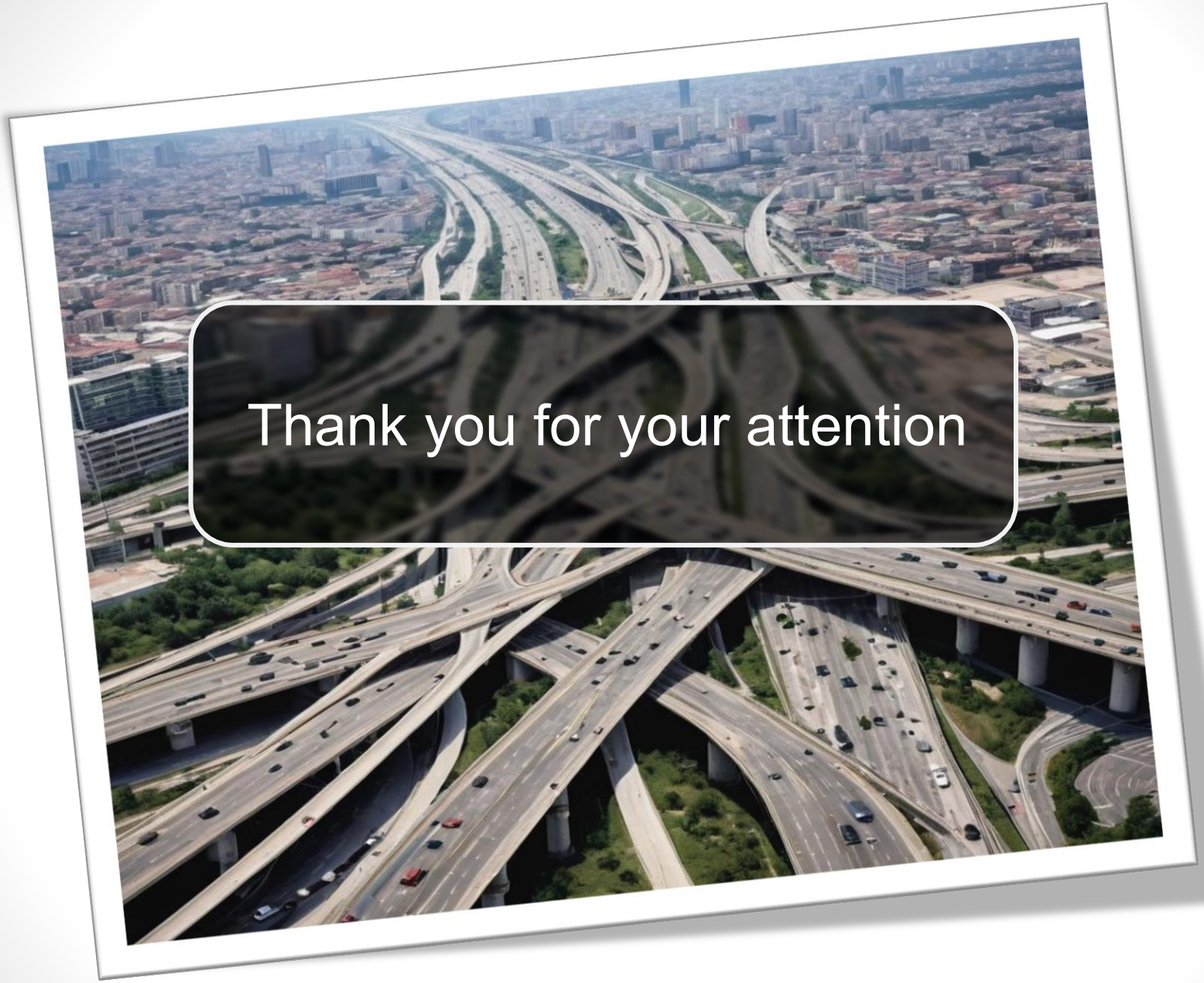
- Existing consortium:
  - Proposed coordinator: *University of Defence*
  - Partners / Other participants: *Established consortium of cooperationg partners from 5 different EU countries looking for new partners for cooperation on large scale project from the CL3-2024-INFRA call from EU and EU`s partner countries.*
  - *Consortium are participating in many similar research projects under other, both national and international science programs.*

Branislav Dubec, branislav.dubec@unob.cz

Project participants - partners

- Looking for partners with the following expertise/ technology/ application field:
  - *Access to data and/or national authorities and point of contacts in the field of critical infrastructure*
  - *Background in critical infrastructure protection, security, logistics data science and management, AI etc..*

Branislav Dubec, branislav.dubec@unob.cz



Branislav Dubec, branislav.dubec@unob.cz

Critical Infrastructures Biological Control

- *David Quintanar*
- *d.quintanar@cedrion.com*
- *CEDRION*
- Role: *WP leader*

- Topic to be addressed: *CL3-2023-INFRA-01-01 (Open topic)*

Proposal idea/content

- Ionic Wind (Kirion Technology) applied to get Critical infrastructure operators more resilient to Biological hazards.
- Developing an effective structure to prevent from health and biological hazards. Neutralizing microorganisms in infraestructures and people In shorter time and compatible with human presence and without chemical products.
- Kirion technology is capable to be integrated both in buildings, checkpoints and vehicles, providing an adequate security.
- Kirion technology is already proved against viruses and bacteria. We aim to be escalated other biological hazards and to be integrated into Critical Infrastructures. We are researching with activated water to be applied for: drinking water distribution networks, agricultural plantations and food logistics networks.

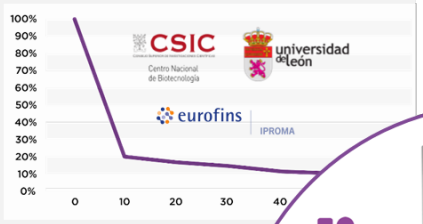
David Quintanar - d.quintanar@cedrion.com

Proposal idea/content

Efficient

The only proven solution efficacy with virus (including SARS-CoV-2) & bacteria in real conditions. **80% reduction in 10 min.**

*See paper published bellow**



Sustainable

Low energy consumption & **15% energy saving on HVAC**. No HEPA filters, meaning **no waste**. Minimum maintenance. 100% recyclable catalyst.

Singular

Patented technology to generate the most efficient **Ionic Wind** against microorganism, just with electricity.

ES2726228
Electro-hydro-Dynamic heat sink

WO/20227175572
Electrohydrodynamic ventilation device

Reliable

Create a safety healthy environment **that transmits trust and security** to employees and patients, generating a positive image in their spaces.

Silent

Totally silent **(0 dB)**. No movable parts.

CE EMI/EMC

Manufactured in Europe

System designed, developed and **manufactured in Spain.**

Food

Water

Transport

Health

EU already trusted In this technology

David Quintanar - d.quintanar@cedrion.com

Project participants

- Existing consortium:
  - Proposed coordinator: *??*
  - Partners / Other participants: Practitioner/Spanish/TBC. Practitioner/Türkiye/TBC.

- Looking for partners with the following expertise/ technology/ application field:
  - *Coordinators: Technological integrators of critical infrastructures solutions. Transportations solutions companies. Health companies. Agrufood companies.*
  - *Workpakage leaders: Vendors of technologies in each sector.*
  - *End users: Other public or private administrations interested.*

David Quintanar - d.quintanar@cedrion.com

INFRA-01-02

INFRA-01-01- Concept

- *Marios Zacharias*
- *mzacharias@space.gr*
- *Space Hellas SA*
- Role: *WPs leader, Technical Coordination*

- Topic to be addressed:

INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities

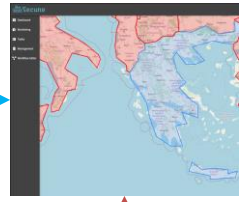
Offerings

- **Crowd-sourcing** capabilities for capturing urban security & resilience related data using BLE and other mobile & IoT technologies, and **operationally visualize** them in a SIEM. To be leveraged by predictive policing models.
  - Topic reference: "*…development of tools for recovery strategies and **proactive foresight** for urban and peri urban environments. The tactical tools should include **modelling** of urban centres and rural areas, **predictive tools,** improved global situational awareness…"*
- **Cybersecurity** safeguarding and cascading threat assessment at cyber-physical layers: CTI and mitigation on critical urban digital infrastructures.
  - Topic reference: "*provide solutions on cybersecurity issues and take on board new type of threats*"
- Lightweight and easily **deployable** tools for collaborative urban **security management**.
  - Topic reference: "*new tools that are designed in a simple manner and deployed in an effective way*".
- Replicability of **good practices** from relevant projects
  - Topic reference: "*Promotion of best practices…and spreading of effective tools and capabilities across entities in different EU territories despite their size and location*".

Offering Concept

Smart city infrastructure

SIEM
Cybersecurity safeguarding

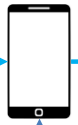


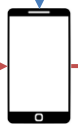
Urban risk management

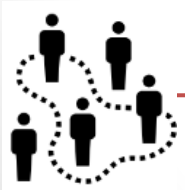
Urban authority

Practitioners' operations

Practitioners





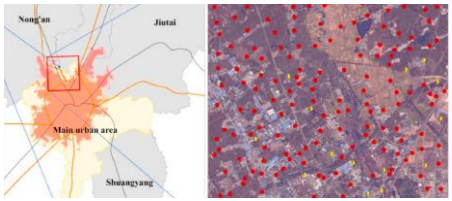


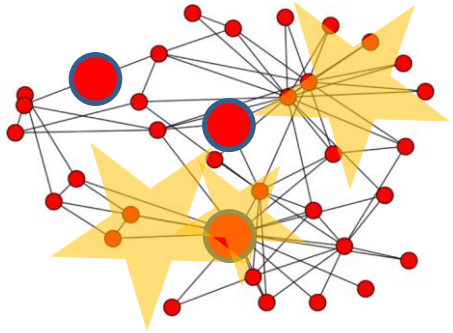
Citizens

Project participants

- Looking for **KEY** partners with the following expertise/ technology/ application field:
  - *Local Police for coordinator*
  - *Local Police with training simulation infrastructure*
  - *SSH with criminology background*
  - *Practitioners' training expert*
  - *Urban planning expert(s) - CPTED*

CauseResilience: Causality-driven operational resilience assessment, generation and management tools for operators and responders at community and territorial scale





- *Ivo Häring*
- *ivo.haering@emi.fraunhofer.de*
- *Fraunhofer EMI*

- Role: *Coordinator or Scientific/Technical coordinator under AYESA project coordination*
- Topic to be addressed: *HORIZON-CL3-2024-INFRA-01-02*

Type of approach	Resilience Cycle			Type of Activity, Tool results expected
	Before	During	After	
Analytical, Expert-based	Current / Future			Association, Seeing, What is? P(y|x)
				Intervention, Doing, What if? P(y|do(x), z)
				Counterfactuals; Retrospection, Imagining; Why? $P(y_x|x', y')$
Simulative, Engineering, Model-based	Current / Future			Association, Seeing, What is? P(y|x)
				Intervention, Doing, What if? P(y|do(x), z)
				Counterfactuals; Retrospection, Imagining; Why? $P(y_x|x', y')$
Data-driven, statistical, ML, A	Current / Future, Tools needed			Association, Seeing, What is? P(y|x)
				Intervention, Doing, What if? P(y|do(x), z)
				Counterfactuals; Retrospection, Imagining; Why? $P(y_x|x', y')$

Ivo Häring, ivo.haering@emi.fraunhofer.de

Advance, align and interface already successful resilience tools to TRL 8

- *Commercial tool providers and their customer basis know gaps*
- *Open source tool organizations know customers‘ needs*

- *Co-use of reslience tools for infrastructure health management, organizational managment and optimization of infrastructure and organizations*
- *Technologies to cover efficiently multiple threats, domino-effect assessment, allow for co-use of ressources, exchange of data, Open source online vizualization*
- *Demonstration of new best practices to strengthen business cases*

- *Starting tools available at Fraunhofer EMI including from EU projects covering Terrorism threats at urban and territorial scale (e.g. VITRUV, ENCOUNTER, EDEN), coupled infrastrucure at urban and territorial scale (e.g. SnowBall, RESISTO, SecureGas, Critical-Chains, Safety4Rail, SATIE, eFORT, dissocial event management at community scale (e.g. BESECURE, RESILIENS)*

Ivo Häring, ivo.haering@emi.fraunhofer.de

Project participants

- Existing consortium:
  - Proposed coordinator: *AYESA (General), Fraunhofer EMI (scientific/technical)*
  - Partners / Other participants:
  - SMEs with Infrastructure resilience assessment tools/approaches and platforms (tbc/examples), e.g., MSIG, FactorSocial, Sius-Consulting, Link11, …
  - as well as industry (tbc/examples), e.g., RINA and its RINACube platform, Leonardo platform, …
  - Organzations that provide open source resilience tools (tbc/examples), e.g., City Resilience Index, City Resilience Proofing Tool, Resilience Rising

Looking for partners with the following expertise/ technology/ application field:

- ***Infrastructure resilience commerical tool provider for operators and communities together with pilot customer*** *(e.g. operator, city, territorial authority, or responder) to provide an operational Use Case*
- ***Critical Infrastructure operator organization or authority*** *for city, community or territory/region*

Ivo Häring, ivo.haering@emi.fraunhofer.de

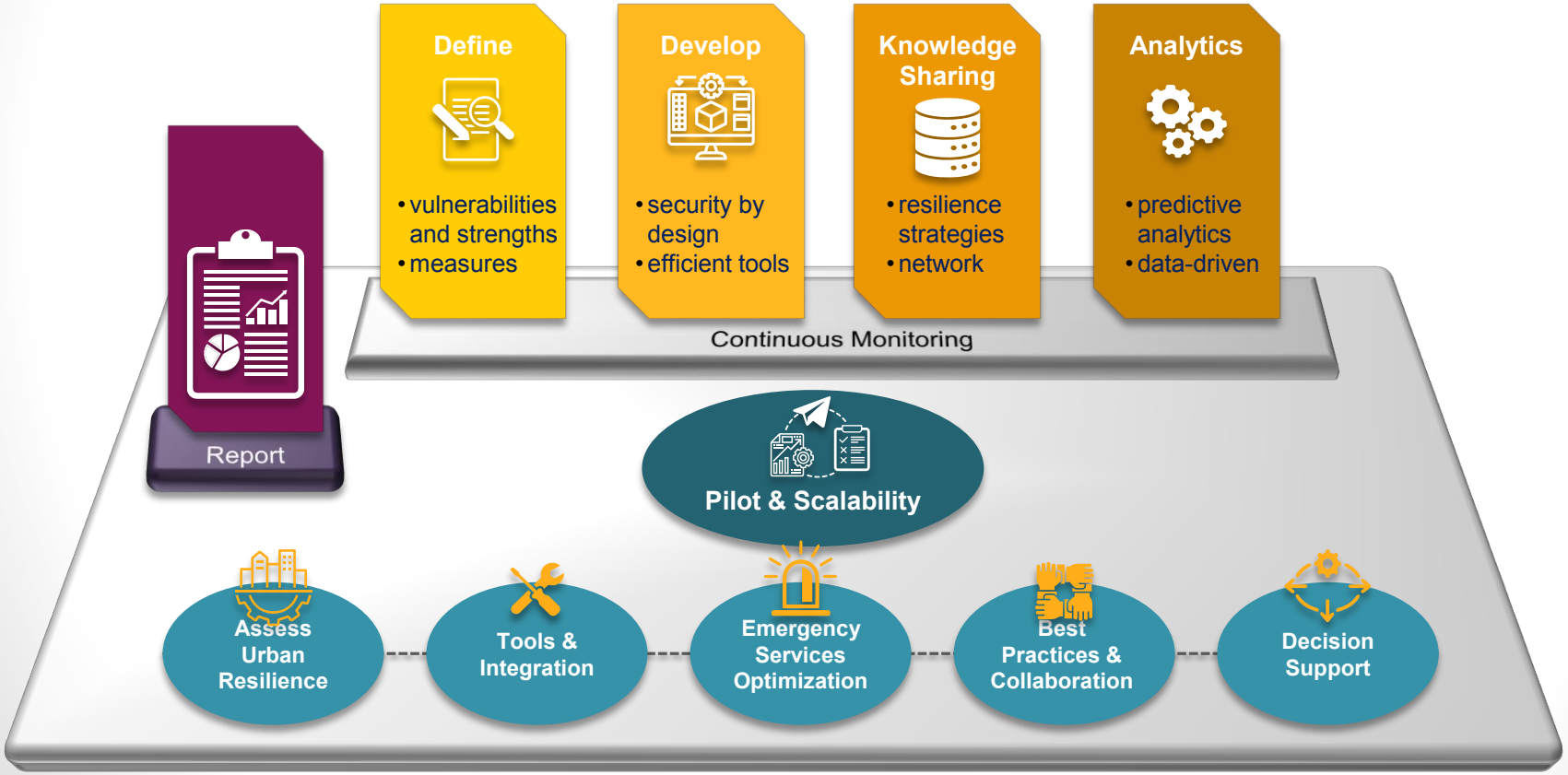
Secure **UR**ban **P**lanning **A**n d re**S**ilein**S**e (SURPASS)

- *George Kioumourtzis*
- *gk@ianus-consulting.com*
- *IANUS consulting Ltd*
- Role: *Proposal coordinator*

- Topic to be addressed: CL3-2024-INFRA-01-02

Proposal idea/content

- *Continuous threat and vulnerability assessment*
- *Integration of set of tools from previous EU funded actions*
- *Data fusion of various datasets*
- *Digital twins*
- *Simulation tools*
- *AI-based decision support*
- *Decision support for operational centres*



Georgios Kioumourtzis - gk@ianus-consulting.com

Project participants

- Existing consortium:
  - Proposed coordinator: *IANUS consulting Ltd*
  - Partners / Other participants:
    - *Urban planning and resilience (Italy) -University*
    - *Technology provider (TBC) –Planning tools*
    - *National Centre (Greece) -Threat assessment methods*
    - *Industry (France) -cybersecurity solutions*
    - *AI provider (Portugal)*
    - *Municipality in Greece*
    - *Municipality in Italy*
    - *Regional authority in Netherlands (tbc)*
    - *Regional authority in Finland*
    - *Municipality in Lithuania*
    - *Municipality in Cyprus*
- Looking for partners with the following expertise/ technology/ application field:
  - *Digital twins*
  - *Data fusion*
  - *Simulation platform*

Georgios Kioumourtzis - gk@ianus-consulting.com

A cutting-edge legal toolbox for smart city operators

- *Dr. Capt. (RC) Thibault MOULIN, Tenured Associate Professor of Law*
- *tmoulin@ucly.fr*
- *Lyon Catholic University (UCLy)*
- Role: *Task Leader or WP Leader*

- Topic : *HORIZON-CL3-2024-INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities*

Our proposal

Bringing our legal expertise to a high-level consortium

- ***Challenge**: Territorial entities are developing into more connected and complex systems: geolocalisation, level sensors, smart grids, etc. This is a huge challenge in terms of privacy & vulnerability.*
- ***Need**: designing compliant and safe infrastructures within legal boundaries.*
- ***Proposed tasks**:*
  - *Preliminary legal risks assessments of:*
    - *The tools and services that the CL3-2024-INFRA-01-02 consortium will develop*
    - *The use of such tools and services by the end users*
  - *Monitoring the lawfulness of the tools over their conception and testing*
  - *Drawing up 2 manuals (1 for developers, 1 for operators)*
    - *General recommendations*
    - *Fictitious case studies and scenarios*
  - *Producing a joint publication between partners to highlight challenges and solutions pertaining to the project.*

=> To be further discussed and completed with the project coordinator

Project participants

- We are looking for a Consortium Leader with an interest in legal expertise.

- The consortium: *in our opinion a successful consortium may consist of IT solution providers, engineering firms, local authorities (associate or partner), industrial, health and law enforcement actors, and other end users.*

Climate risk assessment framework for resilient buildings and surroundings

- *Licia Felicioni (licia.felicioni@cvut.cz)*

Czech Technical University in Prague
University Centre for Energy Efficient Buildings
Architecture and Environment Department

- Destination of interest: *CL3-INFRA*
- Proposal activity: *HORIZON-CL3-2024-INFRA-01-02*

Resilient and secure urban planning and new tools for EU territorial entities

- Role: *WP and/or task leader*

NBSINFRA website

*HORIZON-CL3-**2022**-INFRA-01-02*

Needs and interests

- Assess the influence of climate risks on different metrics, in alignment with the **EU taxonomy** and potential expenses incurred by damages.
- Summary of the management of all **relevant risks** for cities and municipalities.

- Looking for partners with the following expertise/technology/ application field:
  - Critical infrastructure operators/providers
  - Cities/municipalities where to perform pilot testing
  - Expertise in the field of economics, data management and sharing, and social sciences (SSH disciplines)
  - Technology developers/institutes to take into account upcoming developments in the critical infrastructure field

Arch. Licia Felicioni | licia.felicioni@cvut.cz

Contribution

- Our Department offer expertise in the **built environment and urban context**, we are currently working on several EU project (in particular, 2 about resilient built environment and municipality capacity in climate adaptation)
- **Risk assessment framework** co-design. Study of climate change adaptation indicators at the different spatial scales
- Support in the development of the in **the decision-making model** for cities and municipalities
- Definition of the methodology for **pilot activities design**.

Arch. Licia Felicioni | licia.felicioni@cvut.cz

CTdefender

- **Kamila Stroińska, Andrzej Adamczyk**
- kamila.stroinska@itti.com.pl, andrzej.adamczyk@itti.com.pl
- **ITTI** (SME, Poznań, Poland)
- Role: **WP leader, Technical leading partner, software developer**

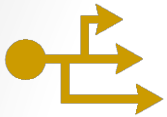
- Topic to be addressed: HORIZON-CL3-2024-**INFRA-01-02**: Resilient and secure urban planning and new tools for EU territorial entities

Scope

- **Evaluation of the resilience of an urban and peri-urban environment**, identification of weaknesses and recommendations for changes to organizational processes;
- **Creation of new tools and cost-efficient security upgrades of urban infrastructures** with possibilities of pooling and sharing of complex security systems, taking into account limited budgets of local authorities;
- Improved efficiency of the **security forces and emergency services** (police, firefighters, paramedics ...) for the benefit of the European citizens and residents;
- **Promotion of best practices**, creation of EU sovereign trusted decision support tool/solution and spreading of effective tools and capabilities across entities in different EU territories despite their size and location.

Kamila Stroińska email: kamila.stroinska@itti.com.pl

ITTI contribution

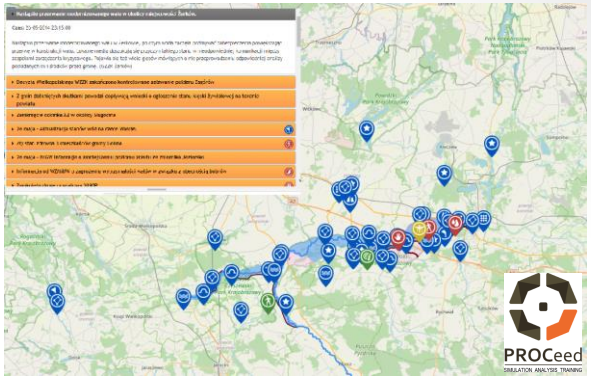


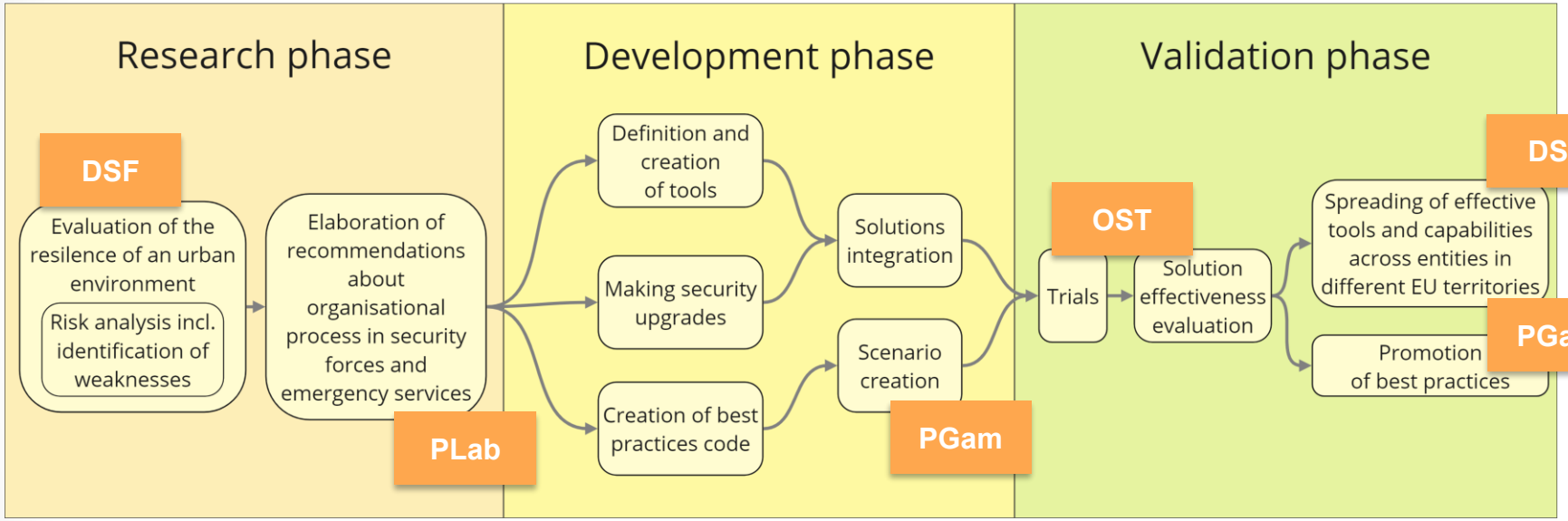
- **Decision Support Framework (DSF) -** *a software library for development of data-driven decision support and multi-criteria analysis tools*
  - *It may be used for the evaluation of the resilience of an urban and peri-urban environment after extension of DSF with the risk analysis algorithm (as a tool and a product)*

- **PROCeed Laboratory** - *an application for 'what-if' analysis using rule-based simulation*
  - *It may be used for modelling of urban infrastructure and identification of weaknesses and elaboration of recommendations*
- **PROCeed Serious Gaming –** *role-playing games*
  - *Promotion and excercise of best practices by:*
    - *improvement of situational awareness in simulated scenarios*
    - *training of tactical decision-making based on visualisation of consequences*

Kamila Stroińska email: kamila.stroinska@itti.com.pl

Concept of work





DSF - Decision Support Framework

PGam – PROCeed Serious Gaming

DSS – Decision Support System

OST – Observer Support Tool

PLab – PROCeed Laboratory

Kamila Stroińska email: kamila.stroinska@itti.com.pl

Project participants

- Existing consortium:
  - **ITTI (SME)**
  - Identified several partners (end users, RTOs) potentially interested in participating in the proposal

- Looking for partners with the following expertise/ technology/ application field:
  - **Practitioners**: security forces and emergency services; local authorities; organisations representing citizens and residents
  - **Software tool developers**
  - **Researchers** (risk assesments & security aspects in all kinds of incidents, eg. in physical, cyber- and procedural security)
  - **Urban infrastrucure experts and administrators**
  - **SSH**

Kamila Stroińska email: kamila.stroinska@itti.com.pl

Decision-making methodology for identifying optimal adaptation measures

- *Julie Železná (julie.zelezna@cvut.cz)*

Czech Technical University in Prague
University Centre for Energy Efficient Buildings
Architecture and Environment Department

- Destination of interest: *CL3-INFRA*
- Proposal activity: *HORIZON-CL3-2024-INFRA-01-02*

Resilient and secure urban planning and new tools for EU territorial entities

- Role: *WP and/or task leader*

NBSINFRA website

*HORIZON-CL3-**2022**-INFRA-01-02*

Needs and interests

- Develop an **integrated spatial decision framework** for identifying optimal adaptation measures at different planning levels (including district, neighborhood, and building levels), integrating resilience and sustainability principles (LCA)

- Elaborate a **summary of design solutions considering predicted future climate characteristics and environmental impacts.**

- Looking for partners with the following expertise/technology/ application field:
  - Expertise in the field of **GIS, IT, social** and **economical** sciences
  - **Critical infrastructure operators**/providers
  - **Demo sites** (real estates portfolios) at different scales to test the framework
  - **Technology developers/institutes** to take into account upcoming developments in the critical infrastructure field

Dr. Ing. Julie Železná | julie.zelezna@cvut.cz

Contribution

- Our Department provides:
  - **Specialized knowledge** in LCA, GHG for real estate portfolios, climate resilience assessment, and the development of rating systems methodologies, among other areas of expertise.
  - **Decision making framework** co-design. Study of climate change adaptation indicators at the different spatial scales and LCA indicators
  - Definition of the methodology for **pilot activities**.

Dr. Ing. Julie Železná | julie.zelezna@cvut.cz

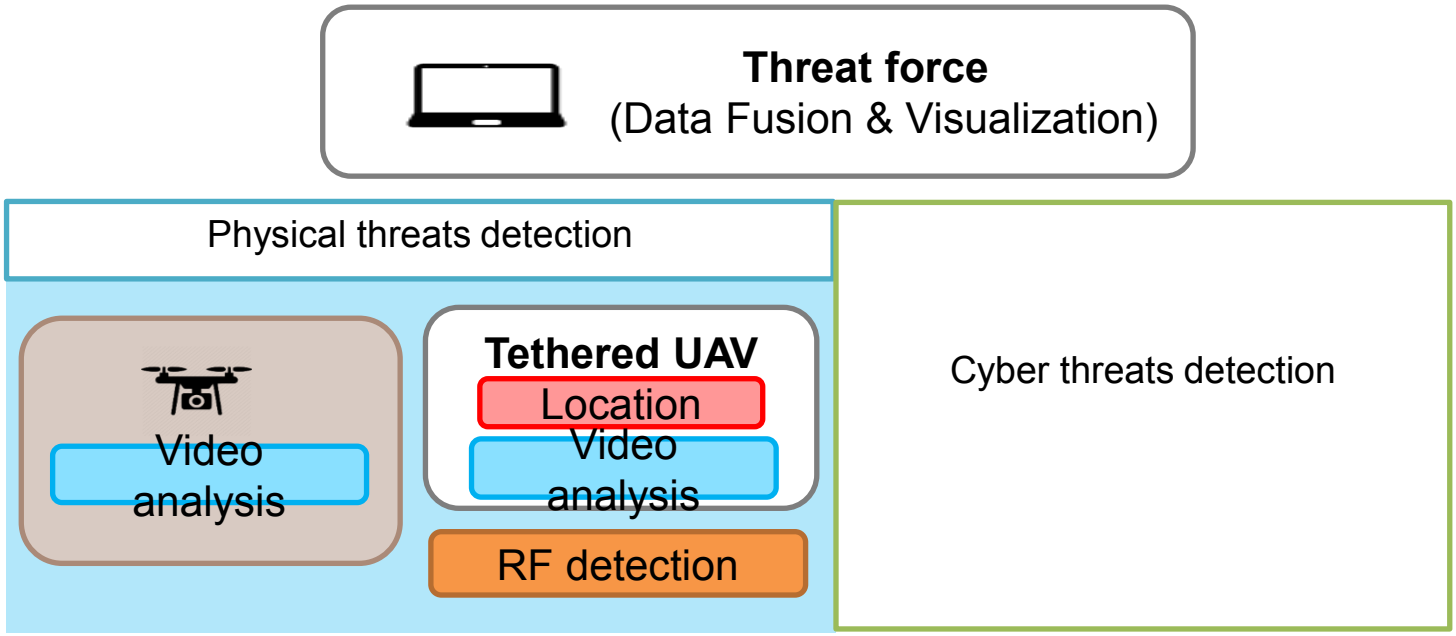
INFRA-01-03

Threat force

- *Sara García Garrido*
- *sgarcia@gradiant.org*
- *Gradiant (RTO, Spain)*
- Role: *Potential proposal coordinator. WP leader, S/T provider.*

- Proposal activity: *HORIZON-CL3-2024-INFRA-01-03:* Advanced real-time data analysis used for infrastructure resilience

Proposal idea/content



Sara García Garrido / sgarcia@gradiant.org

Proposal idea/content

Tethered UAV for perimeter surveillance

- ***Possible use cases:***
  - *Perimeter surveillance of water reservoirs, nuclear plants or other critical infrastructure, using RGB and IR cameras and IA video analysis for intrusion detection.*
  - *Use the tethered UAV for fast deployment of an emergency communication network in emergency situations (like fires in chemical plants or attacks to*

RF transmitters detector and locator

- ***Possible use cases:***
  - *Detect and locate interferences communication and location (like GPS and GALILEO) systems in critical infrastructures such as airports*
  - *Detection of unauthorized signal transmitters in critical infrastructures or government facilities*

Sara García Garrido / sgarcia@gradiant.org

Project participants

- Existing consortium: No
  - Gradiant: perimeter surveillance and RF detection
- Looking for partners with the following expertise/ technology/ application field:
  - *Law enforcement authorities*
  - *Critical infrastructure operators*
  - *Technology integrators*
  - *UAV operators*

Sara García Garrido / sgarcia@gradiant.org

Real-Time Resilience Monitoring

- *Ivo Häring, Benjamin Lickert*
- *Ivo.Haering@emi.fraunhofer.de, Benjamin.Lickert@emi.fraunhofer.de*
- *Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute, EMI*

- Role: *Proposal coordinator, WP leader, S/T provider*

- Topic to be addressed: *CL3-2024-Infra-01-03*

Experiences in EU projects:

Supply grids ICT systems Transport Airports

Proposal Idea: Real-Time Resilience Assessment of Power-Dependent Critical Infrastructure

Supply grids | ICT systems | Transport | Airports

Extend existing Key Performance Indicators for power grid by information of dependent infrastructure.

↓

Data collection and model construction for (real-time) quantification of the network's resilience, and evaluation of mitigation measures and vulnerabilities

↓

Development of resilience strategies, investigation of trade-offs as well as differences within Europe

Project inputs EMI can provide:

- Web-based **Resilience-Monitor** with **set of power system KPIs** for real-time resilience assessment,
- **Agent-based simulations** of **cascading effects** for **coupled infrastructures** in case of various threats,
- **Dynamic simulations** of **gas** and **power 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

[1] Ganter et al. *Towards Risk and Resilience Quantification of Gas Networks based on Numerical Simulation and Statistical Event Assessment,* Proceedings of the 29th European Safety and Reliability Conference (ESREL)
[2] Zalitis et al. *A Linearized Numerical Solution for Steady-State Simulations of Gas Networks,* Latvian Journal of Physics and Technical Science, VOLUME 58 (2021): ISSUE 3 (JUNE 2021), p. 137-153
[3] Ganter et al. *A highly robust gas network simulation approach through an inherently solvable problem formulation for network states far from intended design points*, Applied Mathematical Modelling, Volume 127, March 2024, p. 297-326
[4] Martini et al. *A robust transient gas network simulation for predicting the dynamics before, during, and after extensive disruptions*, Applied Mathematical Modelling, **(under review)**
[5] Schroven et al. *Initial Framework for a Generalized and Quantitative Resilience Evaluation of an Evolving Power Supply System*, Proceedings of the 33rd European Safety and Reliability Conference (ESREL)
[6] Lickert et al. *Modeling Impact Of Power Outages On Interdependent Critical Infrastructure*, Proceedings of the 34rd European Safety and Reliability Conference (ESREL) **(accepted)**

Benjamin Lickert Benjamin.Lickert@emi.fraunhofer.de

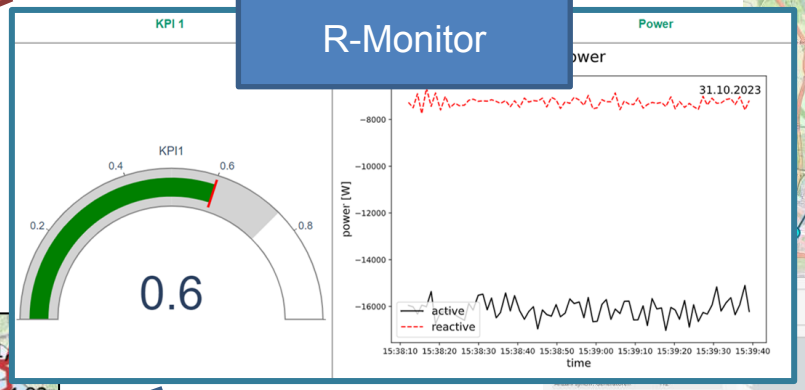
Proposal Idea: Real-Time Resilience Assessment of Power-Dependent Critical Infrastructure

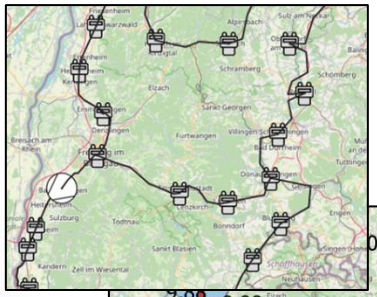
Additional input e.g.:
Telecommunication, transport, health, aviation, water, finance

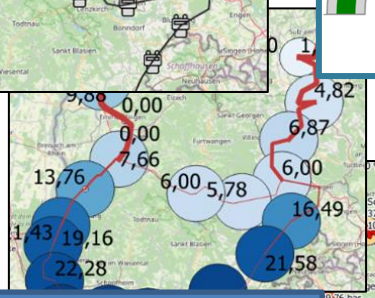
Resilience assessment + propose mitigation measure

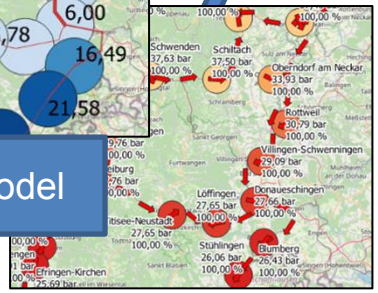
Cascade model

R-Monitor

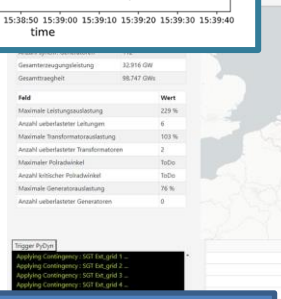


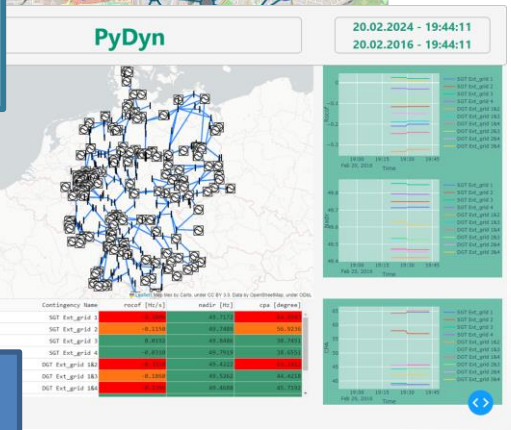






Gas grid model





Power grid model

Benjamin Lickert Benjamin.Lickert@emi.fraunhofer.de

Project participants

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***

- Existing consortium:
  - Proposed coordinator: *Open*
- Looking for partners with the following expertise/ technology/ application field:
  - *Critical infrastructure operators/ providers for shaping resilience assessment*
  - *Cities/ municipalities providing coupled infrastructure networks*
  - *Technology developers/ institutes to take into account upcoming developments in the critical infrastructure fields*
  - *Expertise in the field of socio-technical aspects of critical infrastructure (e.g. customers or operating staff)*

Benjamin Lickert Benjamin.Lickert@emi.fraunhofer.de

RDA & CRM

Realtime Data Analysis & Continuous Risk Monitoring

- *David FAURE, Souhail Youssefi*
- *David.Faure@thalesgroup.com, Souhail.Youssefi@thalesgroup.com*
- *Thales R&T France*

- Role: *Proposal coordinator, WP leader, algo provider*

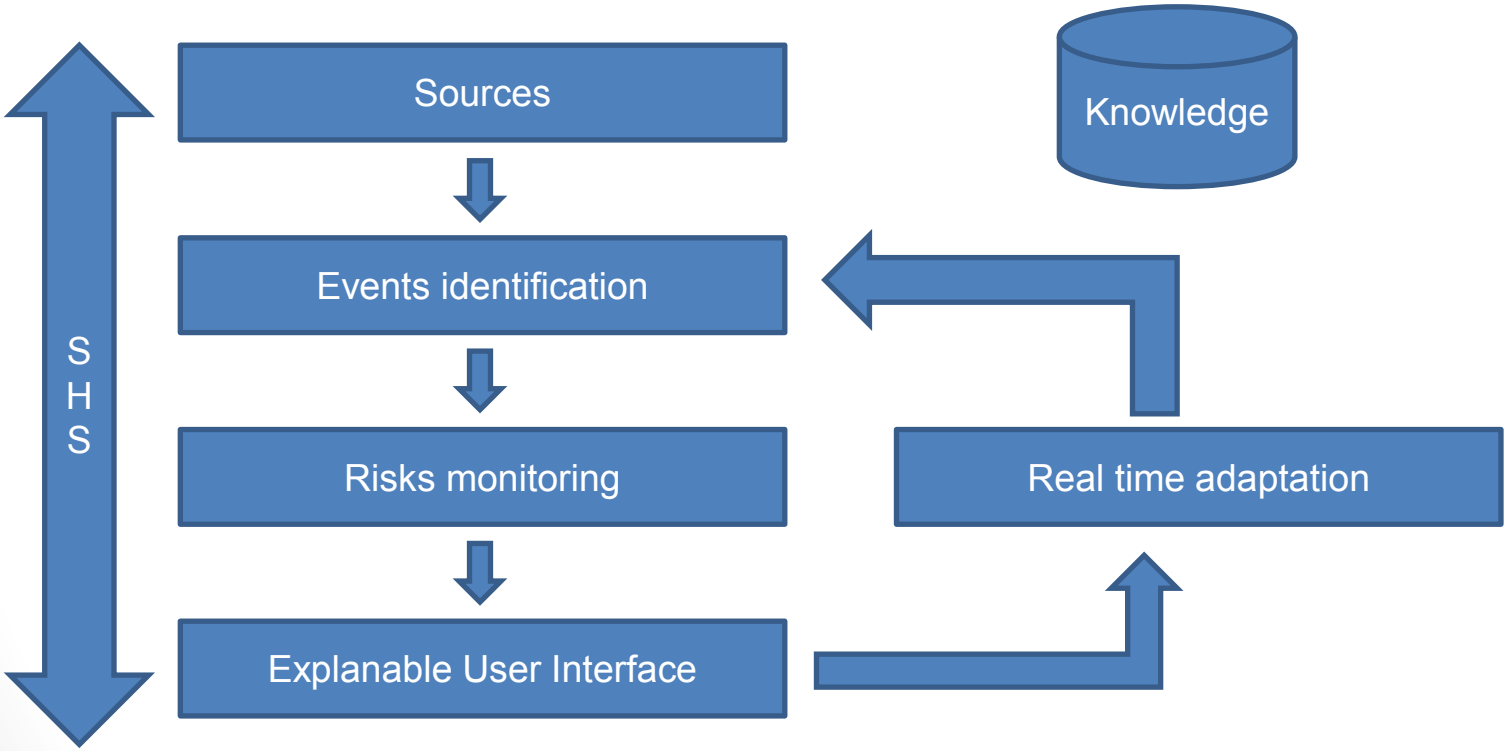
- Topic to be addressed: *HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience*

Proposal idea/content

- *Call: "Improved capabilities for risk and faulty events identification in infrastructure networks and smart cities through real-time analysis…"*
- *Key selling points:*
  - *From multiple sources extract risky events*
  - *Continuous risk monitoring and risk/event prediction*
  - *Learning loop to enhance risk detection*
- *Huge SHS need*
  - *Citizens as relevant information sources*
  - *Citizens behaviour prediction, risk acceptance analysis*
  - *Explicability for citizens and for "risk manager"*

David.Faure@thalesgroup.com / Souhail.Youssefi@thalesgroup.com

First very draft architecture



David.Faure@thalesgroup.com / Souhail.Youssefi@thalesgroup.com

Project participants

- Existing consortium:
  - Proposed coordinator: *Thales R&T France & INERIS (France)*

- Looking for partners with the following expertise/ technology/ application field:
  - *SHS*
    - *Citizen behaviour analysis/modeling, Citizen knowledge formalization, risk acceptance, risk decisions*
    - *Explicability*
  - *Technical*
    - *Multiple sources management*
    - *Event processing*
    - *Unexpected risk detection*
    - *Preparadness enhancement*
    - *Machine Learning*
    - *User Interfaces*
  - *Use case provider*

David.Faure@thalesgroup.com / Souhail.Youssefi@thalesgroup.com

Our Capabilities

- Situation Awareness
  - Intention Recognition
  - Knowledge Representation and Reasoning
  - Hybrid AI: Learning and Reasoning
  - Natural Language Understanding
  - New Learning Paradigms
- Problem modelling expertise
  - Mathematical formulation of operational needs
- Decision support
  - Multi-criteria / multi-objectives decisions
  - Collaborative & distributed decision
  - Interactive Decision Support
- Hybrid & Explanable AI (X AI)
  - Analytical, data-based and hybrid explanable AI, Explainable NN
  - Information fusion traceablity
- Optimisation
  - System Optimisation, Scheduling and planning
  - Constraint Optimisation
  - Constraints, Multi-Objectives Optimisation
  - Centralised and decentralised task allocation
- Autonomous multi-agent systems
  - UxV trajectory optimization
  - UxV and robot tasks coordination
- Trustable AI
  - Verification, Validation, Qualification of AI-based Systems

David.Faure@thalesgroup.com / Souhail.Youssefi@thalesgroup.com

TRICK: Twins for Resilient Infrastructures to Cyber attacKs

- *Martin Jirovec*
- *jirovec@vutbr.cz*
- *Brno University of Technology (HEI, Czech Republic)*
- Role: *WP leader, scientific lead (of proposal)*

- HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience

Proposal idea/content

- Immediate detection is critical for generating and updating Indicators of Compromise (IoCs)
- *Digital twin based platform with real-time analysis (*attackers' activities, *assessment, prevention, detection and response to threats)*
  - *A cyber-deception solution based on honeypots and*
  - *Advanced AI algorithms*
  - *Emulating specific vulnerabilities and characteristics*
- *OSINT sharing as early warning systems*
- *Training scenarios for capacities building*

Martin Jirovec, jirovec@vutbr.cz

Project participants

- Consortium:
  - Proposed coordinator: *TBD*
  - Partners / Other participants:
    - *Brno University of Technology (CZ) – AI-powered technologies - detection, analytics, response; digital twin; emulation; data mining; training scenarios and platform*
    - *SG – honeypots, AI-powered tech; data mining*
    - *TW - AI-powered cyber defence and detection*
- Looking for:
  - *Critical infrastructure operators/providers (incl. civil protection authorities) - e.g. power supply, hospitals, railway, etc.*
  - *Partners for the cyber protection of critical infrastructure*
  - *Social sciences and humanities (SSH) - Social scientists*
  - *Others:*
    - *Public authorities*
    - *Digital twin SMEs with expertise in cybersecurity*
    - *Automated exchange and Visualisation*
    - *Social and ethical aspects of IIoT, AI/ ML*

SMI2G
Security Mission Information & Innovation Group

ARCHER

(AI Real-time deteCtion of pHysical/cybEr Risks)

HORIZON-CL3-2024-INFRA-01-03

Zanasi & Partners
Security Research and Advisory

Graziano Giorgi
(graziano.giorgi@zanasi-alessandro.eu)
Proposal Coordinator / Scientific Coordinator

ARCHER 's idea

- **Objective:**
  - *Develop an **AI tool** for real-time monitoring of **infrastructures** and **smart cities** through a **multi-domain** (transports, health, energy, etc.) integrated modelling of **cyber & physical risks**.*

- **What we have:**
  1. ***Big Data Analysis** (30+ years in AI and Data/Text Mining),*
  2. ***Physical & cyber risk assessment*** ECHO Acting Advanced Cybersecurity Training SHIELD SECRET
  3. ***Source reliability & probability of falsehood ,*** SocialTruth
  4. ***Ethical & legal dimensions of AI applications for security,*** pop AI
  5. ***Security Research** (30+ projects in Security/Defence, end users involvement).*

Graziano GIORGI (graziano.giorgi@zanasi-alessandro.eu)

- **How we assemble it:**

Infrastructure network and/or smart city

Multi-domain data on cyber & physical threats

(Industrial) IoT & smart sensors

OSINT from Social and Web

Network traffic

…

Data Acquisition

1

AI Act

GDPR

4

AI Risk Radar

Identification

2

Prioritisation

3

Verification

Visualisation

5

SSH, training, SOPs with EU risk centers

Infrastructure/ Civil Protection operators

ARCHER

Graziano GIORGI (graziano.giorgi@zanasi-alessandro.eu)

ARCHER 's consortium

- **Proposal/Scientific Coordinator:**

  Zanasi & Partners
  Security Research and Advisory

- **Other consortium members (TBC):**
  - Italian municipality — IoT owner
  - HERMESBAY enhanced awareness — Crysis management expert
  - YUPPIES — Infrastructures and energy expert
  - Università Campus Bio-Medico di Roma — Infrastructures and health expert
  - DRI Defence Research Institute — Risk assessment expert

- **Looking for:**
  - *Infrastructures operators/owners,*
  - *Civil protection authorities,*
  - *Real-time analysis experts,*
  - *IoT, cloud and xG experts/owners.*

- **Z&P is also interested in:**
  - *HORIZON-CL3-2024*
    - *FCT-01-01*
    - *FCT-01-04*
    - *BM-01-02*
    - *BM-01-04*
  - *EDF-2024*
    - *DA-CYBER-NGCR-STEP*
    - *LS-RA-DIS-QUANT-STEP*
    - *LS-RA-CHALLENGE-SENS-RADNP*
  - *DIGITAL-2024*
    - *AI-ACT-06-TESTAI*

Graziano GIORGI (graziano.giorgi@zanasi-alessandro.eu)

Everyday

- *Dr. Ivonne Herrera & Dr. Rita Ugarelli*
- *ivonne.herrera@samforsk.no; rita.ugarelli@sintef.no*
- NTNU Social Research & SINTEF
- Role: *Proposal coordinator, WP leader*

- Topic to be addressed: CL3-2024-INFRA-01-03 Advanced real-time data analysis used for infrastructure resilience

**NSR has interest in joining efforts on other DRS topics*

Everyday - Proposal idea

The EVERYDAY project tackles critical infrastructure's adaptability by focusing on how resilient performance is manifested through everyday operations.

Activities include:

- *Build upon existing knowledge and experience from national and international initiatives and projects*
- *Co-develop tools and processes for early warning, management of interdependencies and decision making under uncertainty*
- *Co- develop methods and tools for improved capabilities for risk and faulty events identification in infrastructure networks and smart cities.*

Source: Hans Tilset, Ivonne Herrera

Ivonne Herrera, ivonne.herrera@samforsk.no; Rita Ugarelli, rita.ugarelly@sintef.no

Project participants

- Existing consortium:
  - Proposed coordinator, WPL confirmed
  - RTOs with strong track in risk and resilience research including SSH, confirmed
  - CI operators to be confirmed
  - Consolidating a core group

- Looking for partners with the following expertise/ technology/ application field:
  - *Partner – Data scientists*
  - *Partner – knowledge and technology provider Industrial Internett of Things for specific CIs*
  - *Partner – first responders*

Ivonne Herrera, ivonne.herrera@samforsk.no; Rita Ugarelli, rita.ugarelly@sintef.no

Offline Presentations

Resilient and secure urban planning

Speaker: Flavia De Simone
E-mail address: flavia.desimone@enide.com
Company: ENIDE: www.enide.com

Destination of interest: HORIZON-CL3-2024-INFRA-01: Resilient infrastructure

Topic of interest: HORIZON-CL3-2024-INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities

HORIZON-CL3-2024-INFRA-01-02: needs and interests

1. Assessing urban resilience, identifying weaknesses, and suggesting organizational process improvements.

2. Developing cost-effective security upgrades for urban infrastructures, enabling sharing of complex systems despite local budget constraints.

3. Enhancing efficiency of security and emergency services for the well-being of European citizens.

4. Promoting best practices, creating EU decision support tools, and facilitating their dissemination across diverse EU territories.

Flavia De Simone - flavia.desimone@enide.com

Contribution of ENIDE (1/2)

Who we are:
ENIDE is an SME located in Spain and focused on the application of digital solutions to various fields, including the security sector, and the development of business innovation actions.

Current situation:

EU territories face a shortage of dedicated, reliable tools to bolster coordination among local first responders and enhance security coverage, necessitating the development of new, user-friendly solutions tailored to the needs of local authorities.

Flavia De Simone - flavia.desimone@enide.com

Contribution of ENIDE (2/2)

ENIDE's suggested solutions:

1. **Integrated Monitoring System for Urban Areas:** through the use of sensor data, security cameras, and communication networks, the system offers real-time insights into urban environments, facilitating early detection of incidents like cyberattacks or natural disasters.
2. **Collaboration Platform for First Responders:** digital platform for efficient collaboration among first responders, incorporating communication, operational planning, and data sharing features to enhance coordination and response during incidents.
3. **Predictive Modelling for Urban Risks:** Utilize historical data and machine learning to predict urban risks and identify vulnerable areas like congestion points, flood zones, or high-crime areas. The final aim is to enable authorities to make informed decisions to enhance safety and resilience.
4. **Citizen Communication Platform:** Create a mobile/web platform enabling citizens to report incidents or risks, with features like emergency alerts, safe route information, and direct communication with authorities, promoting citizen participation to improve incident response.

Flavia De Simone - flavia.desimone@enide.com

Potential partners*

1. **UBIMET GmbH** (Austria):
   - Focus on reducing risks in inspecting and collecting data in civil engineering infrastructure, including worker health and safety.
2. **Mindearth Sarl** (Switzerland):
   - A consulting organization seeking partners for this topic. Experience in urban development and security.
3. **Imperial College London** (United Kingdom):
   - Renowned for research in data analytics, cybersecurity, and infrastructure resilience.
4. **IBM**:
   - Offers advanced analytics solutions, including real-time data analysis and cybersecurity.
5. **European Network for Cyber Security (ENCS)**:
   - Collaborates on cybersecurity research and resilience.
6. **Siemens**:
   - A leader in smart infrastructure solutions and data analytics, with expertise in urban planning, energy, and transportation infrastructure.
7. **Schneider Electric**:
   - Specialized in energy infrastructure resilience and real-time monitoring. Experience in developing secure and resilient urban systems.
8. **Network Rail (UK)**:
   - Manages critical rail infrastructure. Expertise in safety, security, and resilience of transportation networks.
9. **Mindearth Sarl** (Switzerland):
   - A consulting organization with expertise in urban development and security. Potential partner for innovative solutions in urban planning.

** Partners have not yet been contacted. Their interest in the call in not assured.*

Flavia De Simone - flavia.desimone@enide.com

Data analytics for infrastructure resilience

Speaker: Flavia De Simone
E-mail address: flavia.desimone@enide.com
Company: ENIDE: www.enide.com

Destination of interest: HORIZON-CL3-2024-INFRA-01: Resilient infrastructure

Topic of interest: HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience

HORIZON-CL3-2024-INFRA-01-03: needs and interests

1. Enhanced real-time risk identification in infrastructure networks and smart cities through secure public-private collaboration;
2. Tools for diverse data analysis and continuous risk monitoring;
3. Real-time tracking of hazardous agents in supply chains;
4. Improved interoperability for remote operations;
5. Increased cyber-resilience;
6. Real-time risk mapping with privacy considerations.

Flavia De Simone - flavia.desimone@enide.com

Contribution of ENIDE (1/2)

Who we are:
ENIDE is an SME located in Spain and focused on the application of digital solutions to various fields, including the security sector, and the development of business innovation actions.

Current situation:

The abundance of data sources presents an opportunity to enhance infrastructure risk identification, yet requires fast and resilient analytical tools. Filtering and prioritizing relevant data is crucial to address the diverse forms of cyber-attacks, necessitating contextual matching and source verification to prevent false results.

Flavia De Simone - flavia.desimone@enide.com

Contribution of ENIDE (2/2)

ENIDE's suggested solutions:

1. **Real-Time Data Analysis System for Infrastructure Resilience**: Develop a real-time data processing system to detect infrastructure risks like faults, cyberattacks, and incidents using machine learning and AI for improved accuracy and speed.
2. **Visualization and Alert Platform**: Create a platform for infrastructure managers to access real-time data with instant risk alerts and intuitive visualization tools for informed decision-making.
3. **Multisensor Data Integration**: Integrate sensor data (e.g., cameras, temperature sensors, accelerometers) for a holistic infrastructure view. Employ algorithms for anomaly detection. Enhance interoperability between infrastructure systems, risk centers, and first responder gear for remote operations and citizen input.
4. **Predictive Modeling for Faults**: Use historical data for predicting failures and future risks to aid preventive maintenance planning and minimize downtime. Factors such as material fatigue, usage intensity, and environmental changes should be taken into account.
5. **Data Security and Privacy**: Secure collected and analyzed data to comply with privacy regulations. Implement encryption, access control, and assess privacy impacts on individuals and society when processing personal data.

Flavia De Simone - flavia.desimone@enide.com

Potential partners*

1. **Universities and Research Centres**:
   - **Imperial College London**: Known for its research in data analytics, cybersecurity, and infrastructure resilience.
   - **Technical University of Munich (TUM)**: Expertise in smart cities, data science, and infrastructure management.
   - **University of California, Berkeley**: Renowned for its work in urban planning, data analytics, and resilience.
2. **Technology Companies and Consultants**:
   - **IBM**: Offers advanced analytics solutions, including real-time data analysis and cybersecurity.
   - **Accenture**: Provides consulting services for infrastructure resilience and data-driven solutions.
   - **Capgemini**: Expertise in digital transformation, data analytics, and cybersecurity.
3. **Government Agencies and Local Authorities**:
   - **European Union Agency for Cybersecurity (ENISA)**: Focuses on cybersecurity and risk management.
   - **National Institute of Standards and Technology (NIST)**: Provides guidelines for infrastructure resilience.
   - **Local city councils or regional authorities**: Engaged in urban planning and infrastructure management.
4. **Industry and Infrastructure Operators**:
   - **Siemens**: A leader in smart infrastructure solutions and data analytics.
   - **Schneider Electric**: Expertise in energy infrastructure resilience and real-time monitoring.
   - **Network Rail (UK)**: Experience in managing critical rail infrastructure.
5. **International Organizations and Networks**:
   - **European Network for Cyber Security (ENCS)**: Collaborates on cybersecurity research and resilience.
   - **European Association of Research and Technology Organizations (EARTO)**: Facilitates collaboration among research institutions.

** Partners have not yet been contacted. Their interest in the call in not assured.*

Flavia De Simone - flavia.desimone@enide.com

- *Dr Safak Dogan & Dr Xiyu Shi*
- *S.Dogan@lboro.ac.uk & X.Shi@lboro.ac.uk*
- *Institute for Digital Technologies, Loughborough University, UK*

- Destination of interest: CL3-CS & CL3-INFRA
- *Topics of interest:*
  - *CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment*
  - *CL3-2024-CS-01-02: Post-quantum cryptography transition*
  - *CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience*

Needs and interests

- *Destination - Increased Cybersecurity (CS)*
  - *Strengthened EU cybersecurity capacities & EU sovereignty in digital tech*
  - *More resilient digital infrastructures, systems & processes*
  - *Increased software, hardware & supply chain security*
  - *Secured disruptive technologies*
  - *Smart & quantifiable security assurance & certification shared across EU*
  - *Reinforced awareness & a common cyber security management & culture*
- *Destination - Resilient Infrastructure (INFRA)*
  - *Ensured resilience of large-scale interconnected systems infrastructures & entities that operate them in in case of complex attacks, pandemics, natural & human-made disasters, or the impacts of climate change*
  - *Upgraded systems for resilience of the operators & protection of critical infrastructure to enable rapid, effective, safe & secure response & without substantial human intervention to complex threats & challenges, and better assess risks ensuring resilience & open strategic autonomy of European infrastructures*
  - *Resilient & secure smart cities are protected using the knowledge derived from the protection of critical infrastructures & systems that are characterised by growing complexity*

Contribution

- What can you as practitioner organisation offer to a consortium?
  - Research & innovation with expertise in:
    - Generative AI and federated ML for cybersecurity/cyber-defence
    - Privacy enhancing technologies (e.g., Homomorphic encryption)
    - Applied cryptography
    - Information system security
    - Anomaly detection with complex signal processing & SNN
    - Future-proof secure technologies with post-quantum cryptography
  - Research dissemination as academic organisation

- Which role do you prefer in a consortium?
  - Preferably project beneficiary with technical coordination, WP lead as well as contributor to the dissemination activities notably, but can also lead if need be

Dr Safak Dogan (S.Dogan@Lboro.ac.uk)