# Horizon Europe | *Civil Security for Society*

## 1. Destination – Better protect the EU and its citizens against Crime and Terrorism

## Call – Resilient Infrastructure 2023

*Session Chairs:*

- *Angeliki Tsanta (EOS)*
- *Alberto Bianchi (Leonardo/IMG-S)*

# Resilient Infrastructure

| # | Organisation | Presenter |
|---|---|---|
| **CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services** | | |
| 1 | University of Wuppertal | Sylvia Bach |
| 2 | Fraunhofer EMI | Ivo Häring |
| **CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures** | | |
| 3 | Gradiant | Lilian Adkinson |
| 4 | SIMAVI | Monica Florea |
| 5 | Laurea University of Applied Sciences | Johanna Karvonen |
| 6 | VTT Technical Research Centre of Finland Ltd. | Jaana Keränen |
| 7 | Fraunhofer EMI | Kris Schroven |

# INFRA-01-01

Facilitating strategic cooperation to ensure the provision of essential services

| # | Organisation | Presenter |
|---|---|---|
| 1 | University of Wuppertal | Sylvia Bach |

# Enhanced preparedness of interdependent critical entities by framework-based assessing and monitoring cross-border risk and resilience – CRITMON


- *Dr.-Ing. Sylvia Bach*
- *sbach@uni-wuppertal.de*
- *Department of Public Safety and Emergency Management, University of Wuppertal*

- *Dr.-Ing. Daniel Lichte*
- *Daniel.Lichte@dlr.de*
- *DLR PI Institute for the Protection of Terrestrial Infrastructures*


- Role: *WP leader, scientific lead of proposal*
- Proposal activity: *CL3-2023-INFRA-01-01*

# Proposal idea/content

- 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)



Dr.-Ing. Sylvia Bach, sbach@uni-wuppertal.de

SMI2G
Security Mission Information & Innovation Group

# Proposal idea/content



Dr.-Ing. Sylvia Bach, sbach@uni-wuppertal.de

SMI2G
Security Mission Information & Innovation Group

# Project participants

- Existing consortium:
  - Proposed coordinator: *to be determined*
  - Partners / Other participants:
    - *University of Wuppertal, Germany, confirmed*
    - *DLR PI, Germany, confirmed*
    - *(HighSolutions GmbH, Germany)*
    - *(Federal Office for Information Security (BSI), Germany (LoI))*

- Looking for partners with the following expertise/technology/ application field:
  - *Tandems of research partner with a national (regulatory) agency, covering a specific (set of) CEs*
  - *(European) Associations representing CEs*



Dr.-Ing. Sylvia Bach, sbach@uni-wuppertal.de

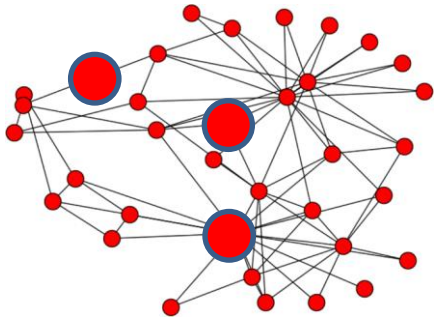
# INFRA-01-01

Facilitating strategic cooperation to ensure the provision of essential services

| # | Organisation | Presenter |
|---|---|---|
| 2 | Fraunhofer EMI | Ivo Häring |

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


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

https://link.springer.com/article/10.1007/s13538-020-00772-9

- Role: *Proposal coordinator*
- Proposal activity HORIZON-CL3-2023-INFRA-01-01, Facilitating strategic cooperation to ensure the provision of essential services
- $N$ Number of system elements or functions
- $m$ Number of redundant additional subsystems
- $m$ Number of systems that can be removed without effect on (key) system functions
- $\{t\}$ threat events considered

# Large-scale network-based multi-threat events and mitigation simulation

- 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** $l = 1,2, \ldots$

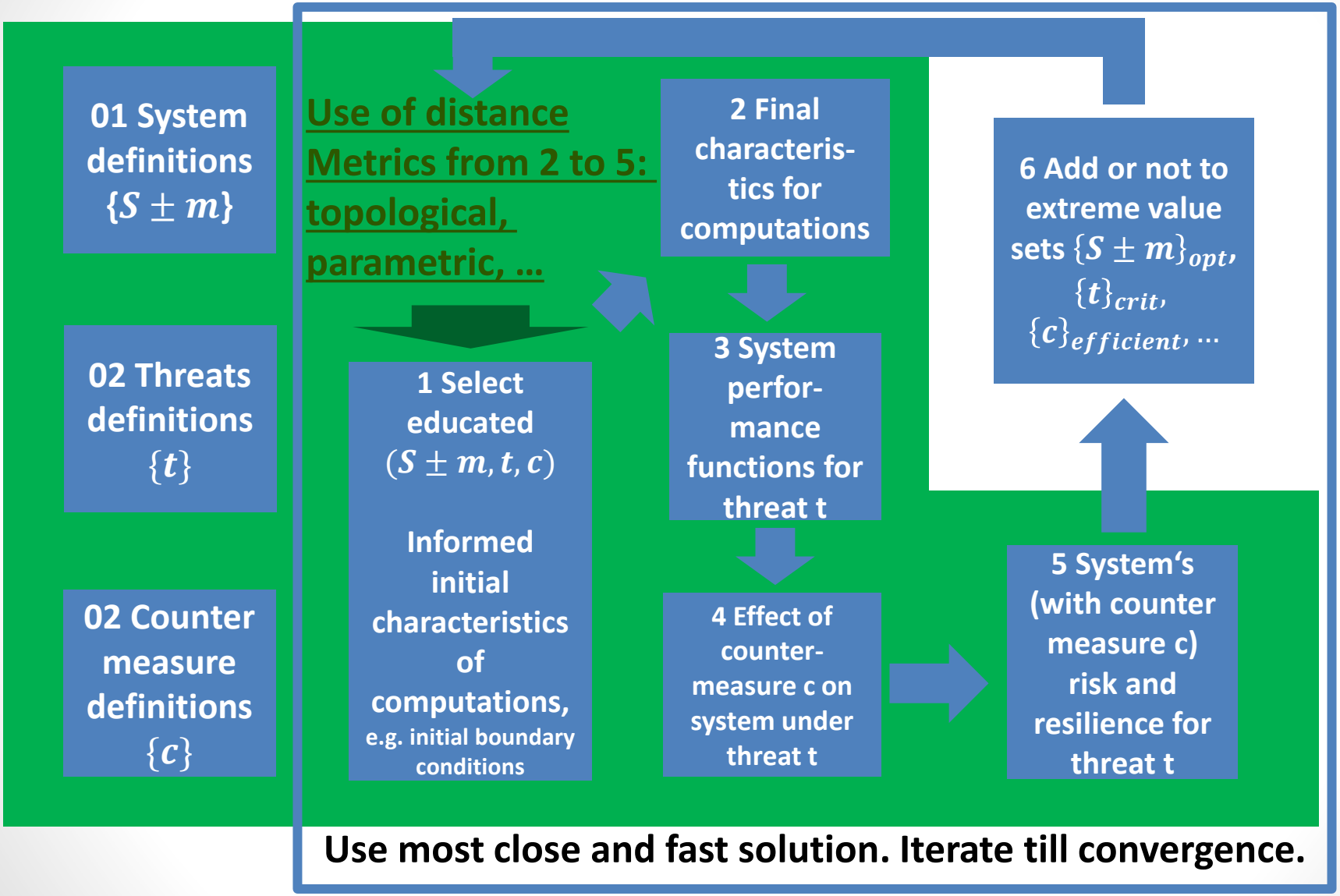
$$\min_{\substack{computation \\ ressources}} = \left\{ \max_{\substack{t \in \{t\} \\ |t|=l}} \text{Risk of } t \text{ on } S \text{ (with } c) \right\}$$

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



Ivo Häring, haering@emi.fraunhofer.de, +49 7628 9050 638

# Large-scale network-based multi-threat events and mitigation simulation






Ivo Häring, haering@emi.fraunhofer.de, +49 7628 9050 638

# Project participants

- Existing consortium:
  - Proposed coordinator: *Fraunhofer EMI*
  - Partners / Other participants: *University Freiburg (tbc)*
  - *(Simulation domain academic experts, tbc)*

- Looking for partners with the following expertise/ technology/ application field:
  - ***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 network simulation tools*
  - ***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*



Ivo Häring, haering@emi.fraunhofer.de, +49 7628 9050 638

# INFRA-01-02

Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

| # | Organisation | Presenter |
|---|---|---|
| 3 | Gradiant | Lilian Adkinson |

# REACT: Enhancing the protection of European Critical Infrastructures

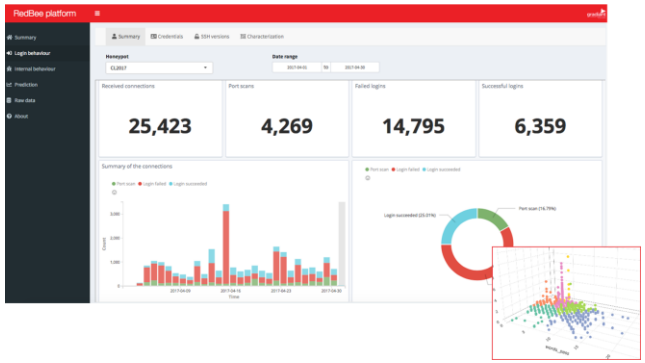
- *Lilian Adkinson*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*
- *Role:  WP leader, S/T provider*

- Proposal activity: *HORIZON-CL3-2023-INFRA-01-02 Supporting critical infrastructures against cyber and non-cyber threats to reinforce the EU resilience of critical entities*

SMI2G
Security Mission Information & Innovation Group

# Proposal idea/content

- *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…*




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 UEBA)*
- Looking for partners with the following expertise/ technology/ application field:
  - *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*



Lilian Adkinson, ladkinson@gradiant.org

# INFRA-01-02

Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

| # | Organisation | Presenter |
|---|---|---|
| 4 | SIMAVI | Monica Florea |

# Cyber and non-cyber holistic support toolbox and integrated system for resilient infrastructures

- ***Dr. Monica Florea**, Head of Unit European Projects*
- *monica.florea@simavi.ro*
- ***Software Imagination & Vision (SIMAVI), Romania***
  - *SME with strong experience in software development (in fields as Security & Cybersecurity, Energy, Industry 4.0, eHealth, Smart Cities), integration & pilot implementation*
  - *Over 45 H2020 & 15 Horizon Europe projects*
  - *Coordinator role for 5 security Horizon projects*
- **Role**:
  - *WP-leader, Technical provider/leader, Integrator, Coordinator*
- **Proposal activity**:
  - **HORIZON-CL3-2023-INFRA-01-02**

# Proposal idea

*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.



**Monica FLOREA, monica.florea@simavi.ro**

# Project participants

- Existing consortium:
  - Proposed coordinator:
    - *SIMAVI (Security & Cybersecurity R&D References: https://www.simavi.ro/en/rd-projects);*
    - *Open for other coordinator collaboration.*
  - Partners / Other participants:
    - *Critical infrastructure pilots (from Romania and EU countries);*
    - *Security & Cybersecurity SMEs;*
    - *Universities.*

- Looking for partners with the following expertise/ technology/ application field:
  - *R&D organizations / other technology providers specialized in cybersecurity for critical infrastructures, integrated process and testing in cybersecurity*
  - *Other critical infrastructure pilots*



Monica FLOREA, monica.florea@simavi.ro

# INFRA-01-02

Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

| # | Organisation | Presenter |
|---|---|---|
| 5 | Laurea University of Applied Sciences | Johanna Karvonen |

# VIGILANT MARITIME SURVEILLANCE

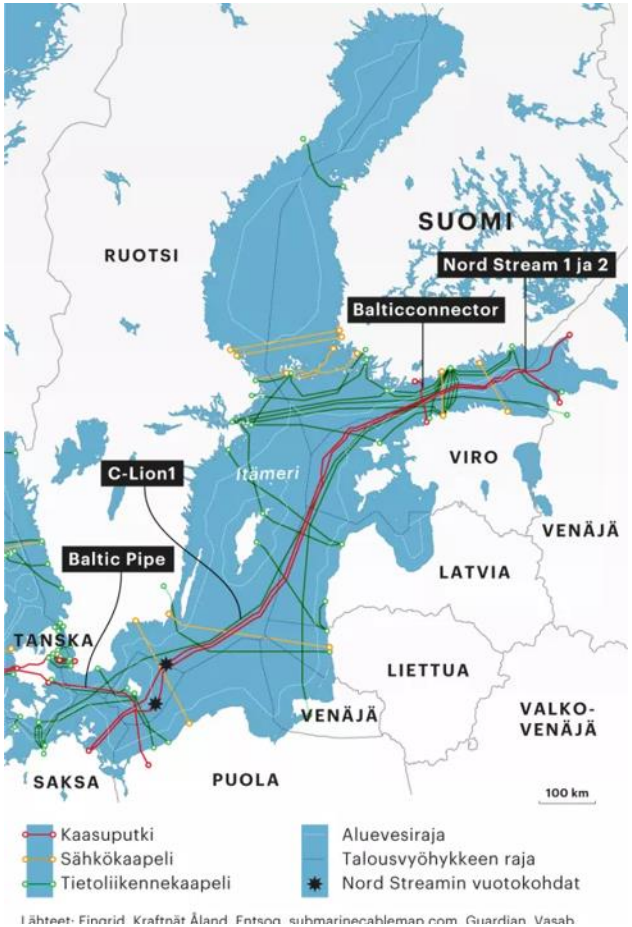
- Johanna Karvonen
- johanna.karvonen@laurea.fi
- Laurea University of Applied Sciences, Finland
- Role:  Proposal Coordinator

- Proposal activity: *HORIZON-CL3-2023-INFRA-01-02*

*Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures*

# 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 industry cooperation (between cable owners, tele network 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






Johanna Karvonen, johanna.karvonen@laurea.fi

# Project participants

- Existing consortium:
  - Proposed coordinator: *Laurea University of Applied Sciences*
  - Partners
    - Academia: GER, PL, FI
    - SMEs: FI
- Looking for partners with the following expertise/ technology/ application field:
  - 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)



Johanna Karvonen, johanna.karvonen@laurea.fi

# INFRA-01-02

Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

| # | Organisation | Presenter |
|---|---|---|
| 6 | VTT Technical Research Centre of Finland Ltd. | Jaana Keränen |

# SitAw societal resilience

- *Jaana Keränen*
- *jaana.keranen@vtt.fi*
- *VTT Technical Research Centre of Finland Ltd.*
- Role: *WP leader/partner*

- Proposal activity: *CL3-INFRA-01-02, Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructure*

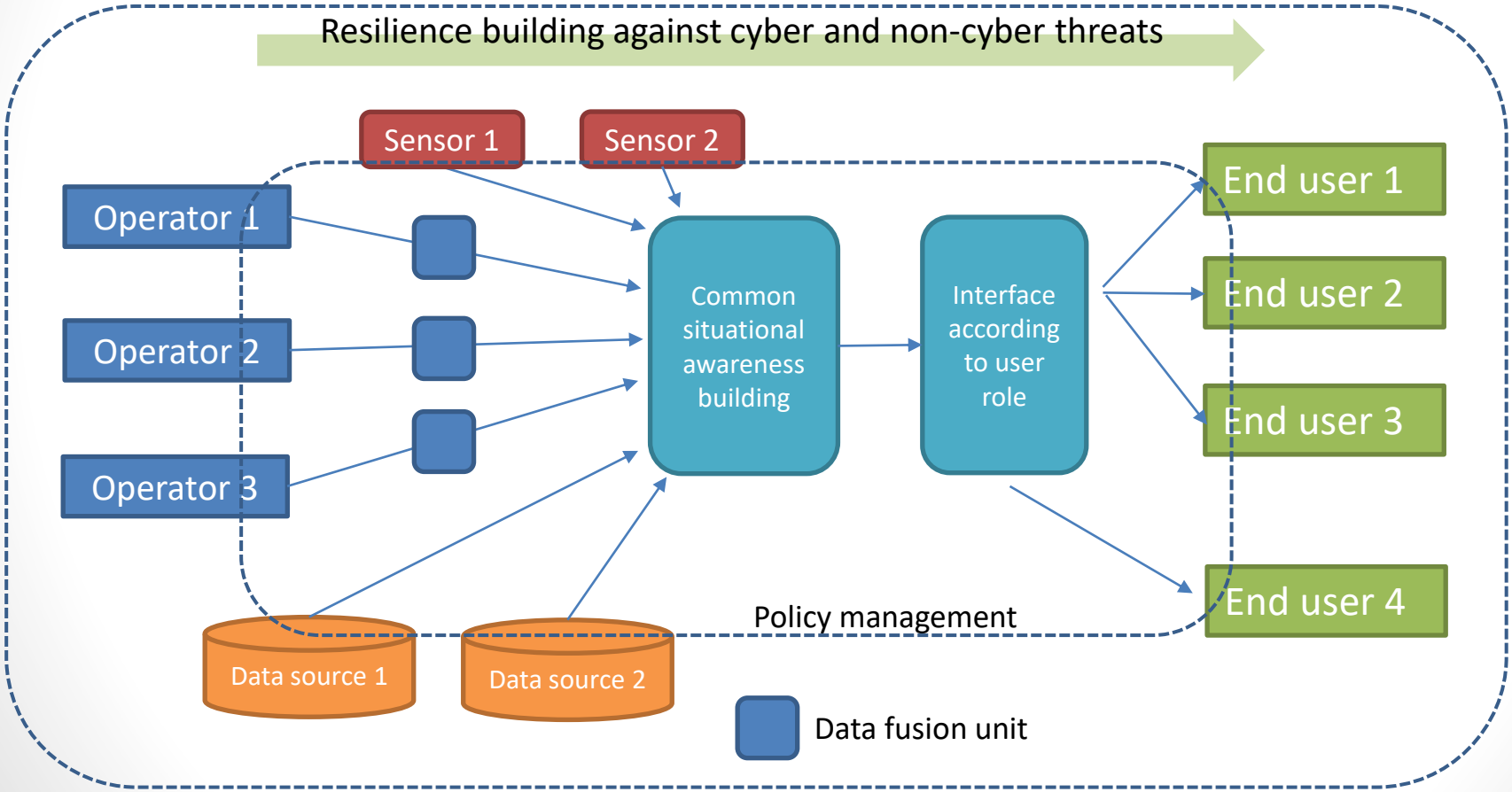
# Proposal idea/content

- *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*



Jaana Keränen, jaana.keranen@vtt.fi

# Situational awareness for societal resilience






Jaana Keränen, jaana.keranen@vtt.fi

# Project participants

- Existing consortium:
  - Proposed coordinator: *we are looking for a good coordinator*
  - Partners / Other participants: *we are currently discussing with Business Tampere (economic development agency of the Tampere region) to find suitable Finnish practitioners/beneficiaries*

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



Jaana Keränen, jaana.keranen@vtt.fi

# INFRA-01-02

Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

| # | Organisation | Presenter |
|---|---|---|
| 7 | Fraunhofer EMI | Kris Schroven |

# Resilience Assessment of Critical Infrastructure


- *Kris Schroven*
- *Kris.Schroven@emi.fraunhofer.de*

- *Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI*


- Role: *WP leader, S/T provider*
- Proposal activity: HORIZON-CL3-2023-INFRA-01-02

- Supply grids
- ICT systems
- Transport
- Airports

# Proposal Idea: Resilience Assessment of Interlinked Critical Infrastructure

- Supply grids
- ICT systems
- Transport
- Airports

***System analysis***

↓

***(Real-time) quantification of the network's resilience, and evaluation of mitigation measures and vulnerabilities***

↓

***Development of a resilience strategy***

*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***



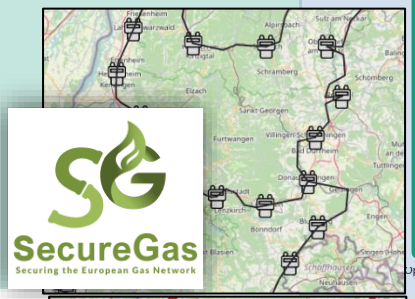
Kris Schroven, kris.schroven@emi.fraunhofer.de

# Our Tools for a System Analysis

Gas Infrastructure – Risk Assessment

- Numerical flow simulation (mass and momentum balance equation)
- Varying disruption conditions

Consumer vulnerability and pipeline importance.



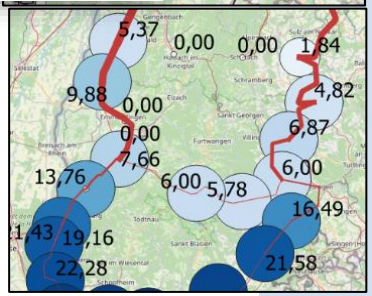
SecureGas
Securing the European Gas Network

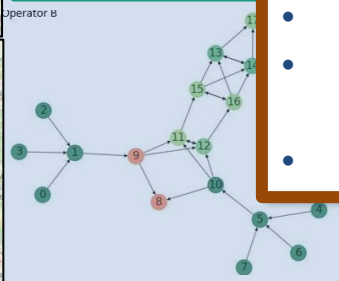
CAESAR

- Agent-based model of the interlinked NW ***with socio-technical aspects***
- Cascading/ redistribution effects

*Input needed!*

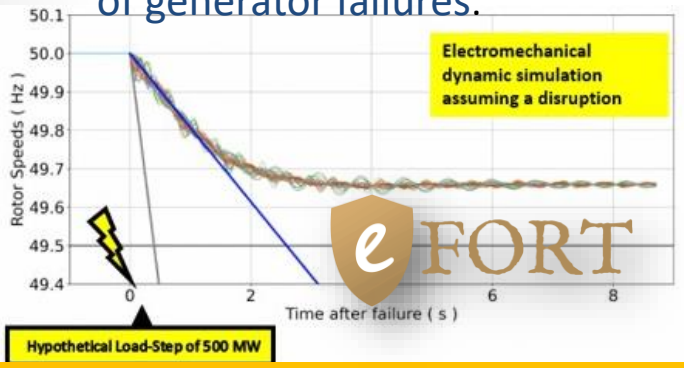
- Network information
- Threats and Mitigation options
- Data

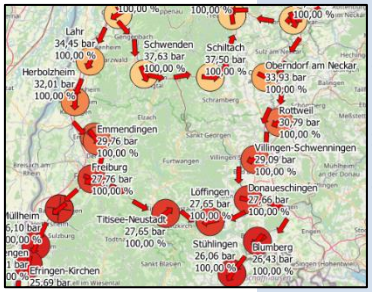


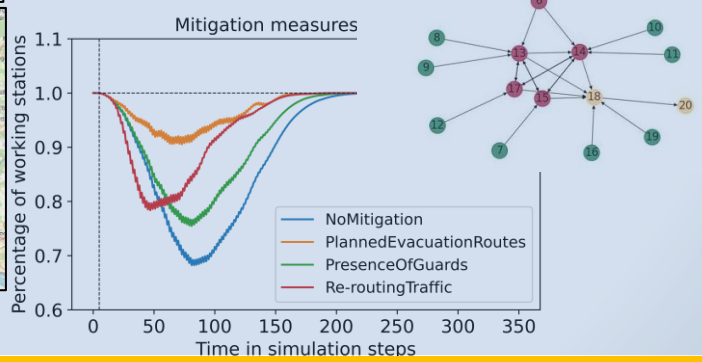




Low-inertia Power Grid assesment

- Dynamic disruption simulations
- predict & assess ROCOF-values
- Dynamic N-1 analysis in regard of generator failures.






Kris Schroven, kris.schroven@emi.fraunhofer.de

SMI2G
Security Mission Information & Innovation Group

# Project participants

- Existing consortium:
  - Proposed coordinator: *Open*
- Looking for partners with the following expertise/ technology/ application field:
  - *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)*



Kris Schroven, kris.schroven@emi.fraunhofer.de