**1st SecureGas Workshop**

**10 September 2019**

## 1. Context and Approach

This event takes place in the context of the SecureGas project (GA No 833017), funded by the European Union, under the topic SU-INFRA01-2018 «Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe". The project, coordinated by RINA, started on 1 June 2019 and will last 24 months, aiming at **increasing the security and resilience of the European gas network**.

Indeed, among the Critical Infrastructure (CI) of Europe, **the Gas network** and infrastructure represents a **challenging example to made secure against both physical and cyber threats,** due to its complexity, the difference among transportation and distribution lines, supply-chain security issues, the various production and storage facilities.

When it comes to **physical threats**, EGIG (European Gas pipeline Incident data Group) reported a total of 1366 incidents from 1970-2016, the leading causes being Third Party Interference (TPI), such as ground works, malicious acts and sabotages, and ground movements. When it comes to **cyber threats**, although the numbers of incidents reported so far is less, the results can be devastating as well. Attacks such as Night Dragon and Shamoon have caused considerable financial damage to oil and gas companies. Global figures estimate that cybersecurity breaches in oil and gas and power cost operators $1,87 billion up to 2018.

In line with the European Energy Security Strategy, the European Programme for European Critical Infrastructure Protection (EPCIP), the EU's reliance on gas imports and the EU Regulation 2017/1938 on Security of Gas Supply, **SecureGas focuses on the +140.000km of the European gas network covering the entire value chain from production to distribution**, providing methodologies, tools, and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats.

Over the course of the project, it will define a blueprint on how critical gas infrastructure should be planned, designed, built, operated, and maintained to cope with cyber-physical security threats. This will serve as baseline for defining a **High-Level Reference Architecture** (HLRA), that will be used as guideline for adapting, customizing, integrating technological components that will be finally **demonstrated in a set of Business Cases**. The resulting outcomes will be offered as services through software services-based models, allowing modularity, flexibility, and third-party interoperability.

The project boasts a multidisciplinary **consortium of 21 international partners**. It is made up of integrated energy company (ENI S.p.A.), gas corporation (Public Gas Corporation of Greece S.A), TSO – Transmission system operator (AB Amber Grid), and DSO-Distribution system operator (Attiki Natural Gas Distribution Company S.A.), managing all together +15000km of pipelines; technology providers active in the field of Security and Critical Infrastructure (Leonardo S.p.A., Guardtime A.S., ADPM Drones Srl, Elbit Systems Ltd., WINGS ICT Solutions, IDEMIA Identity & Security Germany AG, EXUS, GAP Analysis S.A., Innov-Acts Ltd., and Disaster Management, Advice and Training Consulting KG), research and academic institutions in Energy, Security and Resilience Engineering (Fraunhofer-Gesellschaft zur

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833017

Förderung der angewandten Forschung, Kentro Meleton Asfaleias, Joint Research Centre Ispra, Riga Technical University, Technologická platforma Energetická bezpečnost ČR), to support the project implementation. Finally, the Stakeholder Platform (SP), led by Agenzia per la Promozione della Ricerca Europea, will provide advice to secure a long-lasting diffusion of the project outcomes, beyond the project perimeter as well.

## 2. Objectives

The workshop is one of two workshops foreseen in the project. It will gather around 10-12 stakeholders active in the following fields: (i) Gas Critical Infrastructure owners and operators and their associations (ii) bodies implementing the CIP (Critical Infrastructure Protection) Directive at Member State level, (iii) technology and service provides active in the field of security. Besides those stakeholders, the workshop will be also attended by the project partners, resulting in around 50 participants.

The main purpose of the workshop is to collect feedback of the stakeholders and the project partners on: (i) the User (operational, regulatory and organizational) requirements and the technical requirements for the Security of Gas Critical Infrastructure in Europe, and (ii) the definition of high-level scenarios for the three project business cases where the technological components will be tested and demonstrated.

Given the above, the objectives of the workshop can be summarized as follows:

- Objective 1 → Confirmation that the end-user requirements identified by the project reflect the most sensitive and shared requirements in the field & identification of missed user requirements
- Objective 2 → Validation of a list of pre-defined technical requirements to formulate detailed requirements for SecureGas components and their interoperability
- Objective 3 → Inputs for the definition of three business case scenarios to be developed by the project.

## 3. Methodology – overview

The workshop will use a variety of methods to harness individual insights, the unique technical expertise in the room, and collective brainstorming sessions to imagine a variety of known and unknown scenarios. In particular:

- Objective 1 → participants will be rotating around ten different flipchart papers around the room, each detailing a specific user requirement, and will be validating such requirements after informed conversations and add motivated questions. They will later brainstorm individually to add input on potentially missing user requirements, which will fit into a pre-existing taxonomy;
- Objective 2 → method to gather ideas on technical requirements will be like that of Objective 1;
- Objective 3 → a creative activity will be used for all participants to help all 3 Business Case owners to think through possible scenarios and potential risk factors and triggering events.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833017

**Agenda**

| 10 September 2019 – SecureGas Stakeholder Workshop | | |
|---|---|---|
| **TIME SCHEDULE** | **TOPIC** | **RESPONSIBLE** |
| 09.30 - 09.45 | ***Introduction to the workshop*** | |
| 09.30 – 09.35 | Welcome note | RINA |
| 09.35 – 09.45 | Overview of the workshop – steps, methodology | APRE |
| 09.45 – 11.00 | ***Objective 1*** | |
| 09.45 – 10.45 | Confirmation of end-user requirements identified by the project | APRE (facilitator) + all participants involved |
| 10.45 – 11.30 | Identification of missed end-user requirements | APRE (facilitator) + all participants involved |
| 11.30 - 12.00 | ***Coffee break*** | |
| 12.00 – 13.15 | ***Objective 2*** | |
| 12.00 – 13.15 | Validation of a list of pre-defined technical requirements | APRE (facilitator) + all participants involved |
| 13.15 – 14.15 | ***Lunch break*** | |
| 14.15 – 16.45 | ***Objective 3*** | |
| 14.15 – 15.30 | Inputs for the definition of thee business case scenarios (part 1) | APRE (facilitator) + all participants involved |
| 15.30 – 15.40 | ***Coffee break*** | |
| 15.40 – 17.00 | Inputs for the definition of thee business case scenarios (part 2) | APRE (facilitator) + all participants involved |
| 17.00 – 17.15 | ***Conclusions*** | RINA & APRE |

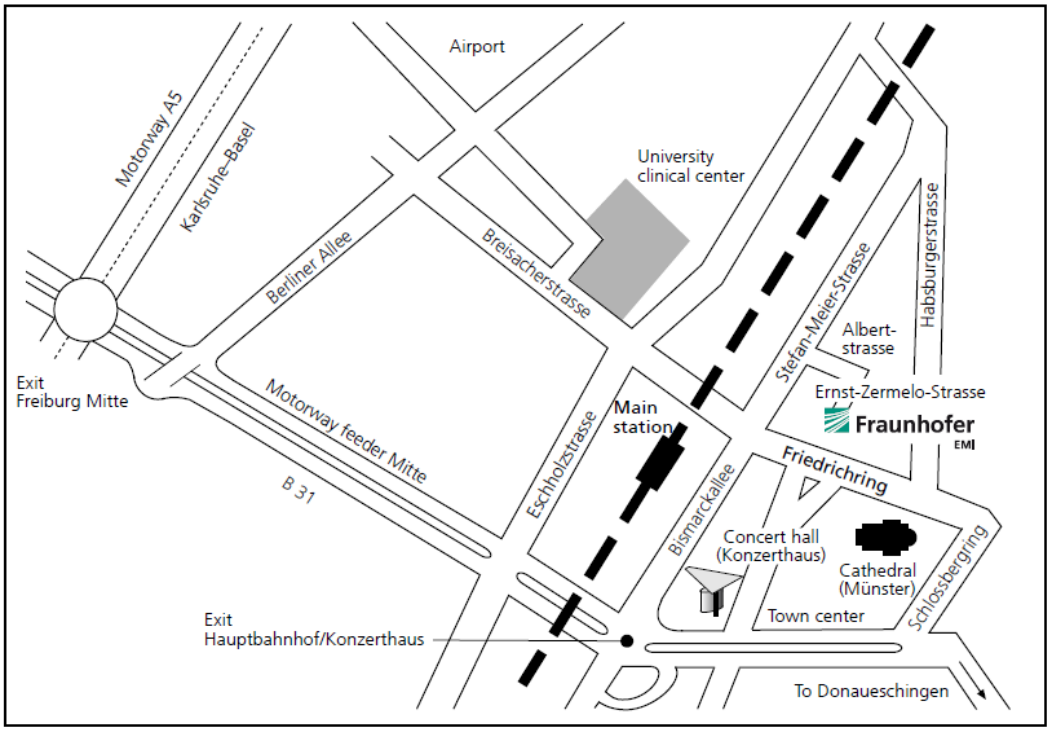
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833017

**Venue Adress:**

Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI
Ernst-Zermelo-Strasse 4
79104 Freiburg, Germany

https://www.google.com/maps/place/Ernst-Zermelo-Stra%C3%9Fe+4,+79104+Freiburg+im+Breisgau,+Germany/@47.9857346,7.8451292,13z/data=!4m5!3m4!1s0x47911c9d4e758f4b:0xe6a6f9ab3de5d3c8!8m2!3d48.0010296!4d7.8465689

MAP IMAGE




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833017