

N.4 NEWSLETTER

July 2021



Securing The European Gas Network

IN THIS ISSUE:

- Overview of the project – the second year and the last 6 project months
- Second SecureGas Stakeholders Workshop
- Demonstration and validation activities in SecureGas Business Cases

... and more!



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

SECUREGAS NEWSLETTER N.4

Overview of the project – the second year and the last 6 project months.....	PAG. 3
Second SecureGas Stakeholder Workshop	PAG. 4
Demonstration and validation activities in SecureGas Business Cases	PAG. 7
• Business Case 1: Greece	PAG. 7
• Business Case 2: Lithuania	PAG. 7
• Business Case 3: Italy	PAG. 8
SecureGas recent scientific publications	PAG. 11
SecureGas social media: <i>"Follow us and stay tuned!"</i>	PAG. 12



SecureGas Newsletter is the official, semi-annual newsletter from Horizon 2020 SecureGas Project. Each SecureGas Newsletter issue aims to disseminate project updates as well as news. It is developed and compiled with contributions from the SecureGas Consortium Partners and relevant Stakeholders.

Realised by APRE

Overview of the project – the second year and the last 6 project months

**Clemente Fuggini
(RINA)**

*Project Coordinator,
on behalf of the
SecureGas consortium*



”

SecureGas has now reached its second year and therefore it is **entering in the last 6 project months**.

In the last months (April 21st) SecureGas has organized a very successful **stakeholder workshop** with the involvement of 12 Stakeholders from 7 MS in representation of 10 organizations. The workshop focused on gathering feedbacks and expert opinions from the Stakeholders on the applicability of SecureGas Conceptual Model and High-Level Reference Architecture in real and operational Industrial environments. With this we wanted to understand how close or how far we are from real applications and what can be done in the last months of the project to close the gaps. Moreover, the **demonstration and validation activities** are now launched with the first encouraging results available. In particular, June 9th, exactly two years later the project physical kick-off meeting in Milan, was the day of the first DEMO event in the project, streamed only directly from the field, showcasing the ongoing tests at the ENI test-case in the project. The event saw the participation of 53 Stakeholders in the morning session (in Italian) and of 31 Stakeholders in the afternoon session (in English). In total 26 organizations attended the event (both remotely and in presence), including representative from the Italian Government and the European Commission.

Other tests are progressing as well in the other sites and infrastructure, owned and managed by DEPA, EDAA and AMBER, where we expect to showcase the results in dedicated demos by September 2021.

Therefore, we look forward to the end of the project, in **November 2021**, when a **final public conference** will be organized to share the project outcomes and pave the way to the next steps and opportunities. We are aware of the expectations in the project, of the challenges we must face in the demonstration activities as well as of the efforts we must put in these last, important, months. We know that only if we will work as a TEAM, where each and every person is fundamental, we will be able to achieve our objectives and to reach our goals, so that to provide our contributions to more secure and resilient European Critical Infrastructure.

*I would like to wish good luck to SecureGas
for the best conclusion possible.*



Second SecureGas Stakeholder Workshop

On 21 April 2021 SecureGas organized a second Stakeholder Workshop, which, due to the COVID-19 pandemic situation, took place online. It gathered 12 stakeholders from 7 Member States (Italy, Greece, Latvia, Poland, France, the Netherlands and Slovakia), external to the project consortium and active in the following fields: (i) Gas Critical Infrastructure owners and operators (ii) bodies implementing the CIP (Critical Infrastructure Protection) Directive at Member State level, (iii) technology and service providers active in the field of security. Besides the external stakeholders, the workshop was also attended by the project partners, resulting in **more than 50 participants**.

The **main objective** of the workshop was the **validation** of the final SecureGas Conceptual Model (CM), Concepts of Operations (CONOPS) and High-Level Reference Architecture (HLRA) as well as a discussion about their potential **exploitation** in industrially rele-

vant environments, taking as example three SecureGas Business Case scenarios.

In the morning session of the workshop, participants were divided in several small groups to discuss the **feasibility and operability of CONOPS, CM and HLRA**. Issues concerning the capturing of the current state of critical infrastructures and technological evolution as well as matching the existing technical systems' operations were debated, resulting in several ideas on how to improve the SecureGas solutions to better fit the existing and future needs of CI stakeholders. In order to ensure interactive approach and effective engagement of workshop participants, the MIRO Board was used. Below, some screenshots from the MIRO Board are presented to show the flow of discussions and suggested improvements concerning CONOPS, CM and HLRA.



Figure 1 - MIRO board | screenshots

The afternoon session of the workshop was focused on **testing the Conceptual Model and the High-Level Reference Architecture in three SecureGas Business Cases**. The session commenced with the presentation of 3 Business Cases scenarios, followed by scenarios deeper analysis in three parallel sessions, where external stakeholders together with project partners had the opportunity to discuss the potential use of SecureGas solutions in various industrial environments adapted

to SecureGas Business Cases. The results of the discussions are currently analysed by the Business Cases owners and the Coordinator, and will be reflected in the final exploitation strategy of the project. Also during the afternoon session, the MIRO Board was used, allowing for structured and lively exchanges between participants, as shown below.

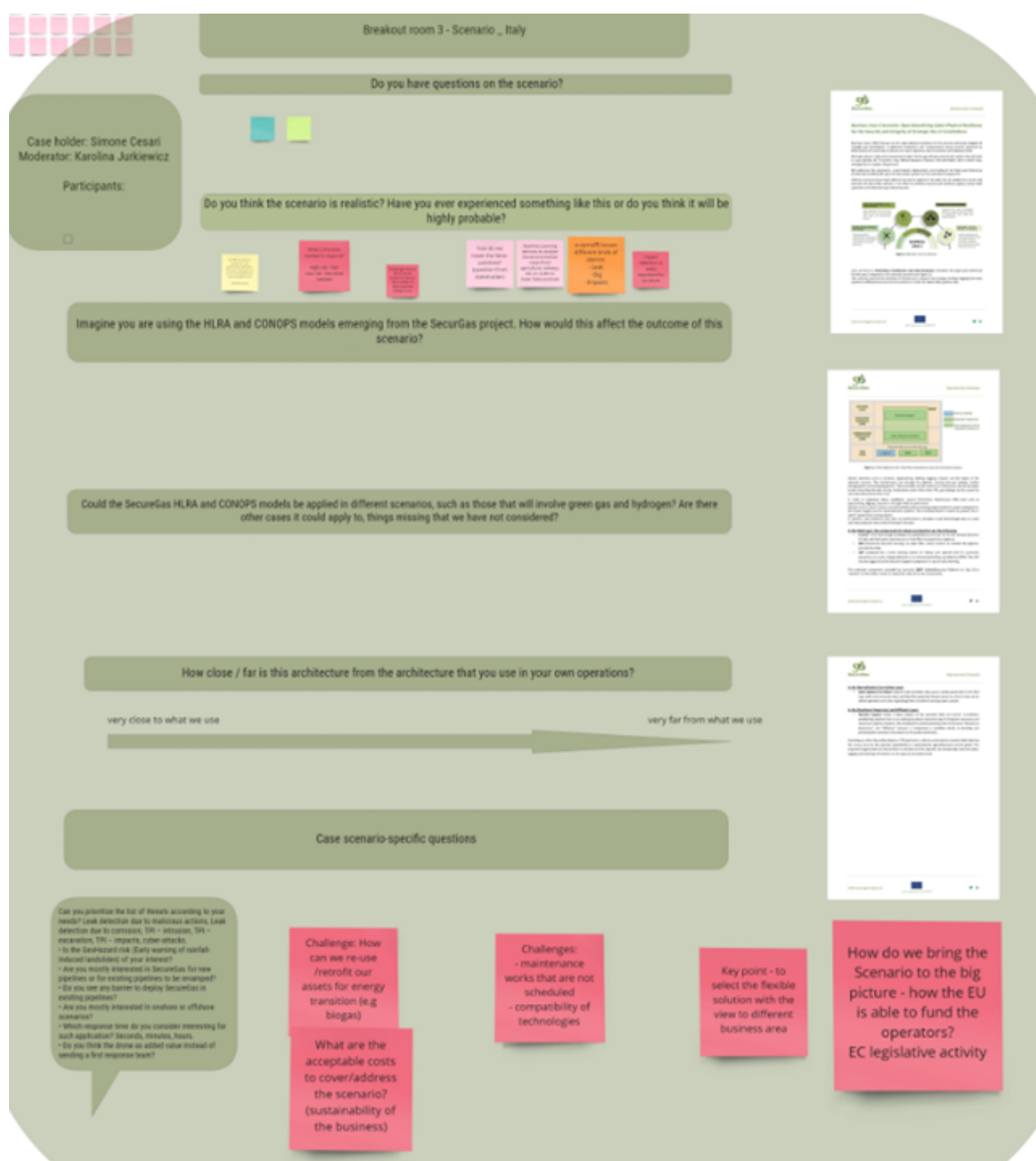


Figure 2 - MIRO board | screenshots [Breakout room 3 - Scenario Italy]



Demonstration and validation activities in SecureGas Business Cases

Business Case 1 - Greece



BC1 UPDATE

SecureGas follows a Business Case (BC) driven approach, with three main phases: Construction, Demonstration and Validation & Diffuse. In this direction each BC addresses the customization, deployment, and testing of the SecureGas high-level reference architecture (HLRA) and the extended components. This resulted in the deployment of a specific security solution (i.e. SecureGas service), integrated as far as possible into operations and currently on the process of being evaluated by the business case owner (i.e. DEPA, EDAA) during pilot activities.

BC1 conducted two OIPs for testing and validation purposes of the DEPA and EDAA implementations, respectively. The scope of the OIPs was to identify problems to address them before the final pilot in September.

DEPA VALIDATION AND TESTING (DEPA OIP)

At DEPA's OIP event we proceeded with the implementation of the scenarios UCD1 - UCD3 (D4.1) according to the designed intrusion paths. Execution of scenarios tested all relevant sensors under real-world situations and validated SecureGas's ability to detect and react to adverse events. We presented the path of the intruder with a live streaming video with the support of a mobile phone to all guests that participated remotely to this event. In parallel, we demonstrated the response of the Artemis Platform and the RAW component.

In this demonstration the scope was to present that the system responds as expected, during the designed intrusion paths of the scenarios. In this direction, we stucked on the designed paths and configured all sensors to respond as expected when an intruder follows similar paths. Demonstration took place on 28/05/21 at 11.00am EEST where the implementation of the UCD1-UCD3 scenarios was tested, based on the final intruder paths which successfully triggered the sensors and in parallel the response of Artemis and RAW. The overall process was fast and did not exceed a maximum of 30 - 40 minutes

EDAA VALIDATION AND TESTING (EDAA OIP)

At EDAA's OIP event on the 4th of June, we proceeded with the EDAA intrusion paths as depicted in SecureGas's scenario driven tests (D4.1). The EDAA OIP Rehearsal included three locations. Specifically, we tested the UC-E2 which includes an invader breaking the door with his car and activating the relevant sensors. The scenario also included tests on face recognition using a whitelisted person list in the EDAA scenario. For the validation tasks, we obtained the employee's consent to utilize the picture of his face with IDEMIA to configure the face recognition module in EDAA field location 3 (L3).

For the validation tasks, we obtained the employee's consent to utilize the picture of his face with IDEMIA to configure the face recognition module in EDAA field location 3 (L3).

All tech partners had representatives on both sites in all locations, so no personnel transportation from one site to the other was needed. Video streaming of the events and the enactment of the scenarios was successful. The tech partners solved pending technical problems from previous EDAA field tests and, thus, the event validation was correct along with its relevant alerts. Some technical issues emerged that are pending implementation to fulfill all desired check lists.

Business Case 2 - Lithuania



USE CASE 1: METHANE LEAK DETECTION BY UNMANNED AERIAL VEHICLE

Hard started, but now demonstrating fast pace use case has started to show tangible results. The UAV solution is currently in an advanced development phase. Most set up flights are performed. A new version "Mark II" is being used since it is more durable, has extended flight range. The solution introduces 5-motor configuration. Also a new flight control software was installed, as well as secure 4G LTE connection has been almost completed. New sensor for the methane leak detection was acquired with advanced data transfer protocols. In addition, KSI integration, JSON stream, CSV integration and GIS path planning development is being finalized.



It is planned that the first testing activities should begin in the end of July, together with basic training of

end users. AMBER has dedicated staff for the UAV operations and started UAV authorization procedures according EU and Lithuanian regulations.

USE CASE 2: RISK ASSESSMENT OF A PIPELINE HUB

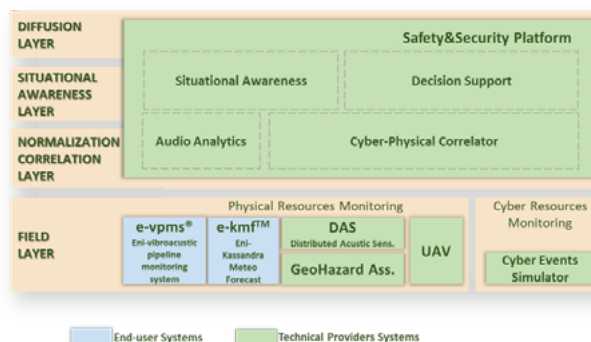
The kick off meeting of JCS risk assessment took place on 29th of June combining efforts from JRC, RINA, LDO and AMBER. Partners shared their insights on the matter, assigned tasks to identify threats in certain areas (natural, human, technological, procedures, cyber). It is agreed that full list of threats would be identified until the end of the summer and detail analysis using HAZOP methodology would be concluded during physical meeting in JCS in the beginning of September. It was also emphasized that outcomes of the SCADA-Shield component would be used for cyber risks identification and evaluation. It is foreseen that installation of SCADASHield would be performed by ELBIT on 12th – 15th of July.

USE CASE 3: REMOTE CONTROL DEPLOYMENT OF VALVES

There are left final adjustments to begin testing the solution, since AMBER infrastructure is completely set up. After the needed technical equipment from technological partner would be received, the testing activities will start. It is expected to begin testing in the mid of July. The results of this solution ought to be secure and reliable SCADA commands verified by Blockchain technology provided by technological partner Guardtime.

The whole SecureGas BC3 HLRA has been brought on field, fine-tuned and extensively tested during the one-week test campaign 17-21 May 2021.

The live demonstration of the Third-Party Interference and Leak Detection scenario has been performed and broadcast to the Partners and external stakeholders the 9th June 2021. The video recording will be published soon. *Stay tuned!*



Referring to the Third-Party Interference and Leak Detection scenario, three classes of events have been tested and demonstrated.

1) Third-Party Interference | Digging:

This class of events takes into account noisy activities prolonged over time, such as approaching with vehicles and machinery near the pipeline, mechanical excavation, manual excavation or even plowing the area around the pipeline with tractors. Since this kind of events are not in direct contact with the pipeline, they have been given a lower severity. When receiving TPI - *Digging* alarm, the operator in the control room could choose the proper way to patrol the area, either with human check or with the drone aid.



Business Case 3 - Italy

BC3 UPDATE

Business Case 3 “Operationalizing Cyber-Physical Resilience for the Security and Integrity of Strategic Gas CI Installations” owned by Eni (Energy integrated company in Upstream, Midstream and Downstream) reached the demonstration phase of the full-scale scenarios:

- Third Party Interference and Leak Detection scenario has been demonstrated on field.
- SCADA network monitoring scenario has been demonstrated in an in-house developed test bed.
- Geohazard scenario has been demonstrated on field simulating significant rainfalls in the area of interest.



2) Third-Party Interference | Impacts:

This class of events consists in impulsive activities made in direct contact with the pipeline shell. These tests simulate any voluntary or involuntary actions of a third-party that could cause a serious damage and even a severe incident.

Several instrumented equipment has been used: hammer, weight drop and pendulum.

Clearly, when a TPI – *Impact* alarm is triggered and received in the control room, the operator is suggested to call the governmental authorities, patrol the area with a drone and even close the valves of the interested section.



3) Leak Detection:

This class of events simulates any possible leakage in the pipeline due to corrosion or caused by a strong impact.

Controlled leaks into the atmosphere were possible in Eni site since the pipeline had been inertized with nitrogen. Several nipples (in dimensions and in shape) have been used to simulate the leakages.

A *Leak Detection* alarm is the most severe, therefore, in case of notification, the operator shall patrol the area with the drone, call the authorities, close the valves and depressurize the interested section.



The following scheme depicts the Business Case 3 Process: the field events detection and management and the role of the extended components.

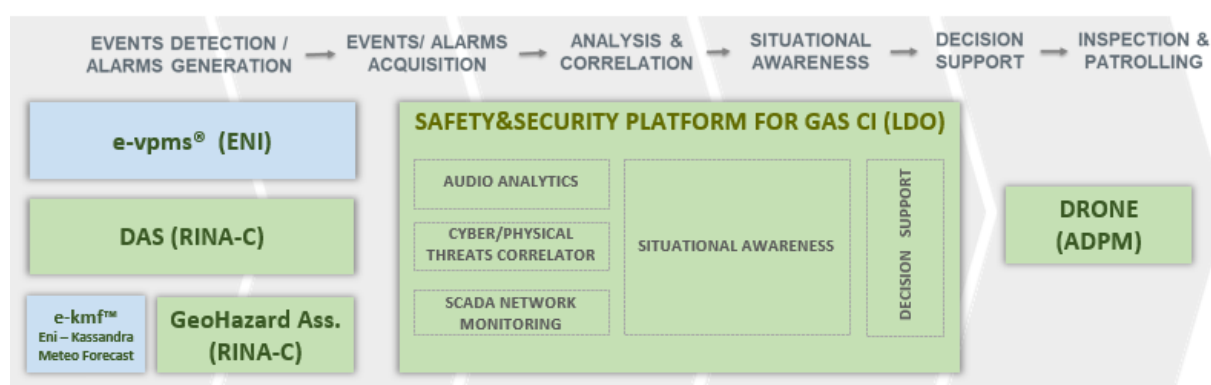
e-vpms® (by ENI) and DAS (by RINA) provide events and alarms such as TPI or Leaks detected in the pipeline.

e-kmf™ (Eni - Cassandra Meteo Forecast) is provided by ENI and exploited by the GeoHazard component (by RINA-C) to assess the risk of debris flows in the Pollein area and by UAV to monitor flight conditions.

The events/alarms generated during the execution of the scenarios described above, are acquired and correlated with environmental noises by the S&S Platform (by Leonardo) also in order to reduce the occurrence of false alarms.

The user interface provides fully situational awareness that allows the user to activate the appropriate course of action: the workflow involves the activation of human intervention and/or Systems such as Drone (by ADPM) with inspection tasks.

The HLRA of Business Case 3 demonstrated with success its robustness by detecting the above-mentioned events with a good geo-localization and time response, and also with a low false positive rate.



For more detailed information about the SecureGas Business Cases, visit a section on the SecureGas website dedicated solely to SecureGas BCs.

[CLICK HERE](#)

SecureGas recent scientific publications

Between November 2020 and June 2021, the following **scientific papers** have been published by SecureGas:

"Validation Strategy as a Part of the European Gas Network Protection"

Authors: D. Rehak, M., I. Gkotsis, A. Gazi, E. Agrafioti, A. Chalkidou, K. Jurkiewicz, F. Bolletta, C. Fuggini (2020) | Book title: Issues on Risk Analysis for Critical Infrastructure Protection. Vittorio Rosato and Antonio Di Pietro (Eds.) ISBN: 978-1-83962-621-0, available [HERE](#)

The European gas network currently includes approximately 200,000 km high pressure transmission and distribution pipelines. The needs and requirements of this network are focused on risk-based security asset management, impacts and cascading effects of cyber-physical attacks on interdependent and interconnected European Gas grids. The European SecureGas project tackles these issues by implementing, updating, and incrementally improving extended components, which are contextualized, customized, deployed, demonstrated and validated in three business cases, according to scenarios defined by the end-users. Just validation is considered to be a key end activity, the essence of which is the evaluation of the proposed solution to determine whether it satisfies specified requirements. Therefore, the chapter deals with the validation strategy that can be implemented for the verification of these objectives and evaluation of technological based solutions which aim to strengthen the resilience of the European gas network.

"Towards a Global CIs' Cyber-Physical Security Management and Joint Coordination Approach"

Authors: Vasiliki Mantzana, Eftichia Georgiou, Anna Gazi, Ilias Gkotsis, Ioannis Chasiotis, Georgios Eftychidis, published in Cyber-Physical Security for Critical Infrastructures Protection, pp. 155 - 170, First International Workshop, CPS4CIP 2020, Guildford, UK, September 18, 2020, Revised Selected Papers, available [HERE](#)

The aim of this paper is to describe three different CI types (airports, gas infrastructures, and hospitals); present the current physical and cyber security related regulations and standards adopted; identify their security operations, as well as the organisational and technical measures deployed by each CI; and finally describe a common, cyber-physical crisis management process encompassing the involved stakeholders. Moreover, gaps and best practices related to security issues are analysed and a global approach for CIs' cyber-physical security management and joint coordination is proposed.

"A performance-based tabular approach for joint systematic improvement of risk control and resilience applied to telecommunication grid, gas network, and ultrasound localization system"

Authors: Ivo Häring, Mirjam Fehling-Kaschek, Natalie Miller, Katja Faist, Sebastian Ganter, Kushal Srivastava, Aishvarya Kumar Jain, Georg Fischer, Kai Fischer, Jörg Finger, Alexander Stolz, Tobias Leismann, Stefan Hiermaier | Environ Syst Decis (2021), available [HERE](#)

This paper presents a framework for a resilience assessment and management process that builds on existing risk management practice before, during, and after potential and real events. It leverages tabular and matrix correlation methods similar as standardized in the field of risk analysis to fulfill the step-wise resilience assessment and management for critical functions of complex systems.

"ENERGY TRANSITION OF THE BALTIC STATES: PROBLEMS AND SOLUTIONS"

Authors: A. Sauhats, Z. Broka, K. Baltputnis | Published in Latvian Journal of Physics and Technical Sciences 2021, N.3, available [HERE](#)

The importance of the climate change problem is recognised by the governments of the overwhelming majority of the world's countries. To bring additional attention and enable more concrete action, in a number of countries and municipalities the issue has been declared a climate emergency. The need to solve this problem predetermines the task of replacing fossil energy sources with renewable alternatives. The process of the ongoing transformation is called energy transition. It includes transformation of all the energy-intensive sectors of economic activity: power generation, supply and consumption, heat generation and supply, electrification of transport, agriculture and household.



SecureGas social media: "Follow us and stay tuned!"

SecureGas is very active on its social media!

We regularly share most recent developments in the project and project results and show our activities like event participation, invitation to project events, etc.



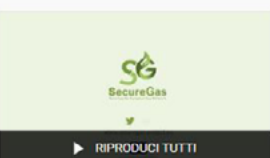
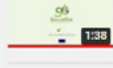
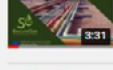
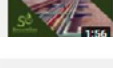
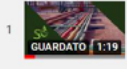
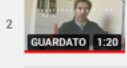
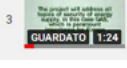
If you want to be updated, FOLLOW US on:



Find more about the SecureGas project, its main goals, Its business cases and its technological solutions.

Click on YouTube, you can find two interesting SecureGas playlits. Watch the videos now!



 SecureGas Extendend Components	SecureGas Extended Components collection SecureGas H2020 project  1:38  3:31  1:56 A1 - Safety and Security platform for Gas CI SecureGas H2020 project A2 - Autonomous docking station and UAV based asset management ADPM SecureGas H2020 project	CLICK HERE
 SecureGas webinar	 1:05:15  44:24 1st SecureGas webinar "Risk and problem we target and technological solutions we propose" SecureGas H2020 project 2nd SecureGas webinar "SecureGas Business Cases" SecureGas H2020 project	CLICK HERE
 SecureGas Video pills	 1:19  1:20  1:24 SecureGas EU project in a nutshell SecureGas H2020 project SecureGas and the Gas CI: security and resilience against cyber and physical threats SecureGas H2020 project The overall objective of SecureGas EU project SecureGas H2020 project	CLICK HERE

SECUREGAS COORDINATOR:



Clemente Fuggini
clemente.fuggini@rina.org

SECUREGAS PARTNERS:



Innov-acts



Get in Touch!

www.securegas-project.eu

