N.3 NEWSLETTER

November 2020

SecureGas

Securing The European Gas Network

IN THIS ISSUE:

- Overview of the project – what happened and what is coming up
- SecureGas Extended Components

... ***and more!***

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

SUMMARY

SECUREGAS NEWSLETTER N.3

SecureGas
Securing the European Gas Network

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 – What happened and what is coming up

Clemente Fuggini (RINA)
Project Coordinator, on behalf of the SecureGas consortium

SecureGas has recently turned into its **2nd year**, corresponding to the **launching and execution of piloting activities at selected sites and installations**, where customized and adapted SecureGas solutions and services will be deployed, tested and validated.

In the last months, we have continued working despite the difficulties induced by the COVID-19 pandemics and the need for physical meeting at the installation sites and facilities. **We launched the Business Case 3 piloting activities at ENI selected infrastructure and installations and we have successfully installed the first set of components to be used for testing and validation**. A next run of installations and testing have been already planned and are foreseen in the months to come.

In addition, Business Case 1 and Business Case 2 at, respectively, EDAA, DEPA and AMBER facilities are progressing well and in line with the expectations and the contractual obligations. The identified scenarios for both Business Cases are now ready for the full implementation on site in physical and cyber installations and tests.

The last months have been also the occasion to successfully carry out **the first project review for the period June 2019 – August 2020**. During the review meeting, the achievements in this period have been reported, together with a clear and precise assessment on why and how they have met or not the project end-users' expectations. Beside this, **technology providers described the status of implementation of the solutions they are developing, thanks to a novel tool, the Extended Components Cards, to be used for promotion and exploitation of SecureGas technologies, solutions and outcomes**.

With now more than 1 year ahead, SecureGas is really entering into its crucial phase, where commitment, teamwork, dedication, patience and passion will play a key role. Indeed, it will be crucial to pass the winter time with all possible activities developed and with the less impacts that the COVID-19 pandemics will certainly cause.

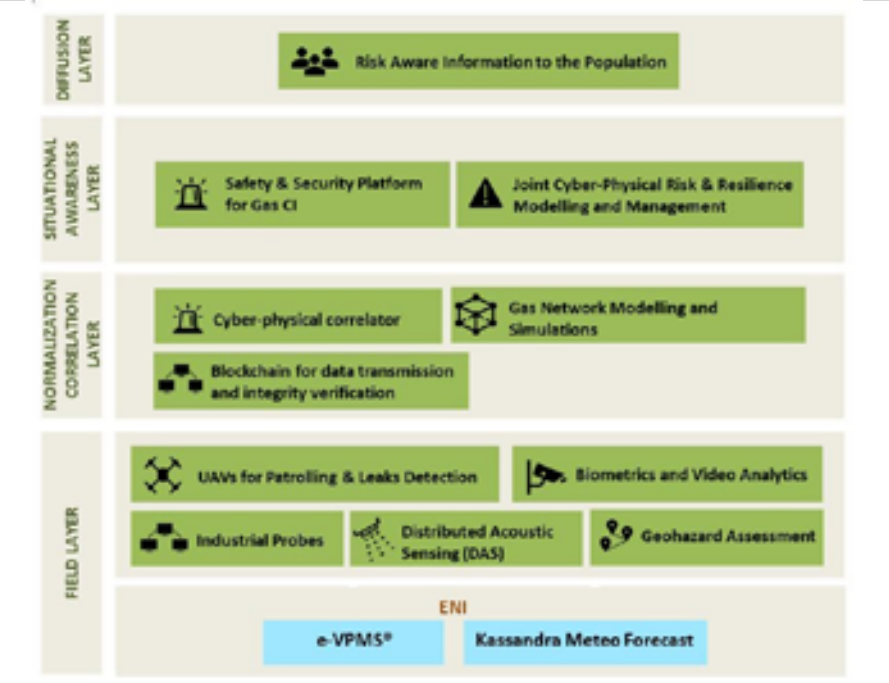
We, as consortium, **are committed**, despite all the external events and disturbances, to fully meet the EC, end-users and stakeholders expectation so that **to successfully complete the project and provide our contribution to the Security and Resilience of EU Energy (Gas) Critical Infrastructure and beyond.**

Stay tuned on SecureGas!
Stay safe and stay healthy!

SecureGas
Securing the European Gas Network

SecureGas Extendend Components

The components to be used by SecureGas are products and technologies brought into the project by qualified partners. These components have been "extended" - that is improved and integrated - to meet the needs of end users, addressing and solving the proposed business cases scenarios, adopting the most innovative technological solutions, without forgetting cost control and an easy and scalable deployment**.**



They have **to interoperate with each other to build an advanced and innovative solution aimed at improving the protection and resilience of the gas infrastructures**. **For each component**, which has technical specific features as designed by its provider, **the functionalities useful for Securegas objectives have been selected and extended** according to the architectural scheme shown in the figure, where:

FIELD LAYER

collets cyber-physical events through very different sophisticated components acting as detectors and sensors provided both by SecureGas technical providers and end users.

Vibroacoustic monitoring technology (e-vpms®) able to process pressure and acceleration signals for the continuous remote detection and identification of leaks and third-party interferences and **Kassandra Meteo Forecast** for the rainfall-induced landslides tailored to on-shore infrastructure are the systems made available by ENI.

Instead the *extended components* are: **Industrial Probes**: "Intelligent probes" monitors the OT network to identify suspicious or malicious activities aimed at performing unauthorized changes to commands on SCADA control system; **Distributed Acoustic Sensing (DAS)** technology able to convert a fibre optic cable, laid along the pipeline, into an array of virtual microphones to detect gas leaks on the pipeline; **Geohazard Assessment** provides geo-hazard maps and early warning based on the weather forecast system for rainfall-induced landslides tailored to on-shore infrastructure; **Biometrics and Video Analytics** component identifies, verifies and tracks objects and persons detecting potential intrusions through a combination of cameras and other instruments, such as accelerometer, vibrometer, door latch, etc; **UAV for Patrolling** provides advanced monitoring capabilities through drones operated by a Smart Docking/Recharging system, **UAV for Leaks Detection** is a UAV equipped with a special camera for detection, inspection and data processing on selected section of the infrastructure.

NORMALIZATION & CORRELATION LAYER

acquires the heterogeneous data coming from the field layer and performs an initial processing and correlation of them. In this Layer: **Cyber-physical Correlator** is a Machine Learning based tool for advanced event processing, aggregating information to detect threats and discover cyber, physical, or joint anomalies; **Gas Network Modelling and Simulations** that provides predictive simulation of the attack vectors impact on the pipeline and the corresponding optimized response vectors without harming the real infrastructure; **Blockchain for data transmission and integrity verifi-**

cation provides KSI (Keyless Signature Infrastructure) Blockchain functionalities used for integrity assurance of data transfer.

SITUATIONAL AWARENESS LAYER

provides to the operator the Decision Support, thanks to a deep analysis of the information elaborated, supported by risk analysis and scenarios simulations. In this layer: **Safety & Security Platform for Gas CI** SecureGas supports Users to determine the best outcome among various choices, potential decisions, the interactions between decisions and ultimately prescribes an optimal course of action to be taken; **Joint Cyber-Physical Risk & Resilience Modelling and Management** targets at the identification, assessment, and evaluation of potential risks and supports operators before, during and after an incident occurrence.

DIFFUSION LAYER

provides appropriate information to the public authorities within minimal time after an important security incident through the **Risk Aware Information to the Population component**.

The modularity and scalability of the SecureGas architecture allows you to selectively exploit only the functions and services you need, as demonstrated by the **3 Business Cases** where the extended components:

- have been customized, integrated and implemented on the infrastructure of the end users;
- cooperate with the numerous legacy protection systems already operating in the gas infrastructure by combining *as_is* and *to_be* technological solutions.

Business Case 1

Figure 1 - BC1 | Components

Business Case 1 - Risk-Based Security Asset Management through the Life-Cycle of Gas CI managed by DEPA and EDAA (Transportation and Distribution operator in Greece) aims to face the following threats scenarios: **(a) VBIED (explosives), (b) manual sabotage with cyberattack masking, (c) unauthorized physical access and (d) manual modification of valves configuration.**

SecureGas intends to prevent, detect and respond through the following integrated components:

- **Joint Cyber-Physical Risk & Resilience Modelling and Management** that aims at the identification, assessment, and evaluation of potential risks and supports operators before, during and after an incident occurrence;
- **Biometrics and Video Analytics** component that identifies, verifies and tracks objects and persons detecting potential intrusions through a combination of cameras and other instruments, such as accelerometer, vibrometer, door latch, etc.;
- **Cyber-physical Correlator** is a Machine Learning based tool for advanced event processing, aggregating information to detect threats and discover cyber, physical, or joint anomalies;
- When an incident occurs, **Risk Aware Information to the Population** provides the functionality to connect to the Public Warning Services managed by the competent public authorities in order to report incidents and events for the protection of the population.

Business Case 2

Figure 2 - BC2 | Components

Business Case 2 Impacts and cascading effects of cyber-physical attacks to Strategic Nodes of the Gas network, owned by AmberGrid (Transportation network operator in Lithuania) manages three use cases: **(a) Risk assessment of the strategic pipeline hub, 1 km area around Jauniunai Gas Compressor Station, (b) Methane leak detection by unmanned aerial vehicles and (c) Remote control deployment of valves.**

The extended components targeting the above use cases are:

- **the Gas Network Modelling and Simulations** that provides predictive simulation of the attack vectors impact on the strategic pipeline hub and the corresponding optimized response vectors without harming the real infrastructure;
- **UAV for Leaks Detection**, which is a UAV equipped with a special camera for detection, inspection and data processing on selected section of Amber Grid infrastructure;
- **Industrial Probes**, which are "Intelligent probes" monitoring the OT network in order to identify suspicious or malicious activities aimed at performing unauthorized changes to commands or alarm thresholds on SCADA control system;
- **Blockchain for data transmission and integrity verification** provides KSI (Keyless Signature Infrastructure) Blockchain functionalities used for integrity assurance of data transfer between UAV and the IT infrastructure of Amber Grid.

Business Case 3

Figure 3 - BC3 | Components

Business Case 3) Operationalizing Cyber-Physical Resilience for the Security and Integrity of Strategic Gas CI Installations owned by ENI (Energy integrated company from Upstream, Midstream to Downstream) intends **to address (a) Third Party Interference and Leak Detection, (b) Resilience of the OT/IT Network and the Forecast and (c) Early Warning of Landslides** thanks to the interoperability of the following SecureGas components and ENI's system:

- **Safety & Security Platform for Gas CI** supports Users to determine the best outcome among various choices, potential decisions, the interactions between decisions and ultimately prescribes an optimal course of action to be taken leveraging on the **Cyber-physical correlator outcomes**;
- **UAV for Patrolling** provides advanced monitoring capabilities through drones operated by a Smart Docking/Recharging system;
- **Distributed Acoustic Sensing (DAS)** is a technology able to convert a fibre optic cable, laid along the pipeline, into an array of virtual microphones to detect gas leaks on the pipeline;
- **Geohazard Assessment** provides geo-hazard maps and early warning based on the weather forecast system (**Eni – Kassandra Meteo Forecast**) for rainfall-induced landslides tailored to on-shore infrastructure;
- **Vibroacoustic monitoring technology (e-vpms®)** able to process pressure and acceleration signals for the continuous remote detection and identification of leaks and third-party interferences.

The following graph presents list the extended components and how they interact and contribute to the realisation of the SecureGas technical solution.

For more detailed information about each of the SecureGas extended component, visit a section on the SecureGas website dedicated solely to SecureGas extended components.

CLICK HERE

SecureGas publications

By November 2020, the following three **scientific papers** have been published by SecureGas:

M. Hromada, D. Rehak and N. Walker, "**Electricity Infrastructure Technical Security: Practical Application and Best Practices of Risk Assessment**" published IGI Global Disseminator of Knowledge, available at: https://www.igi-global.com/book/safety-security-issues-technical-infrastructures/239916

This publication presents the transition from general approaches to risk analysis, through risk identification methods and procedures and the assessment of major industrial and technological risks, to specific risk analysis methodologies for electricity infrastructures. An important part is also devoted to the introduction of practical approaches and methodologies that are accepted as "best practices" in connection with ensuring the technical security of electricity infrastructures.

S. Ganter, K. Srivastava, G. Vogelbacher, J.Finger, B. Vamanu, V. Kopustinskas, I. Häring and Alexander Stolz, **"Towards Risk and Resilience Quantification of Gas Networks based on Numerical Simulation"**, published in Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. Published by Research Publishing, Singapore, available at: https://www.rpsonline.com.sg/proceedings/esrel2020/html/3971.xml

This publication outlines the implementation of a zero-dimensional steady state gas network simulation code applying the momentum and mass conservation equation. The resulting non-linear system of equations is solved with a standard solver based on the Newton approach. As a result, pressure at the consumer ends are calculated for all disruption scenarios that include one single disrupted pipeline. Based on these calculated pressures a statistical evaluation of the importance of pipelines and the vulnerability of nodes is carried out. This approach is demonstrated using a small model of the Irish natural gas network including 14 pipelines and 13 nodes.

I. Häring, S. Ganter, J. Finger, K. Srivastava, E. Agrafioti, C. Fuggini and F. Bolletta, **"Panarchy Process for Risk Control and Resilience Quantification and Improvement"**, published in Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. Published by Research Publishing, Singapore, available at: https://www.rpsonline.com.sg/proceedings/esrel2020/html/4264.xml

This paper explores the options of combining a risk and resilience management cycle with a resilience cycle within a panarchy loop to achieve a holistic phased and iterative approach. Options are discussed and the best option is selected in terms of orthogonality of phases, merge and limitation of phases, well-defined core tasks of each phase and supporting methods. For the application domain critical infrastructure protection and the industry sector gas, it is shown how to support the phases of the joint risk and resilience management panarchy with the method quantitative gas grid simulation.

In Addition, a publication titled **"Validation Strategy as a Part of the European Gas Network Protection"** has been accepted for publication in the book under the working title "*Issues on Risk Analysis for Critical Infrastructure Protection*", ISBN 978-1-83962-621-0.
We will soon inform you about the website at which the publication will be available.

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

SecureGas is very active on its social media!

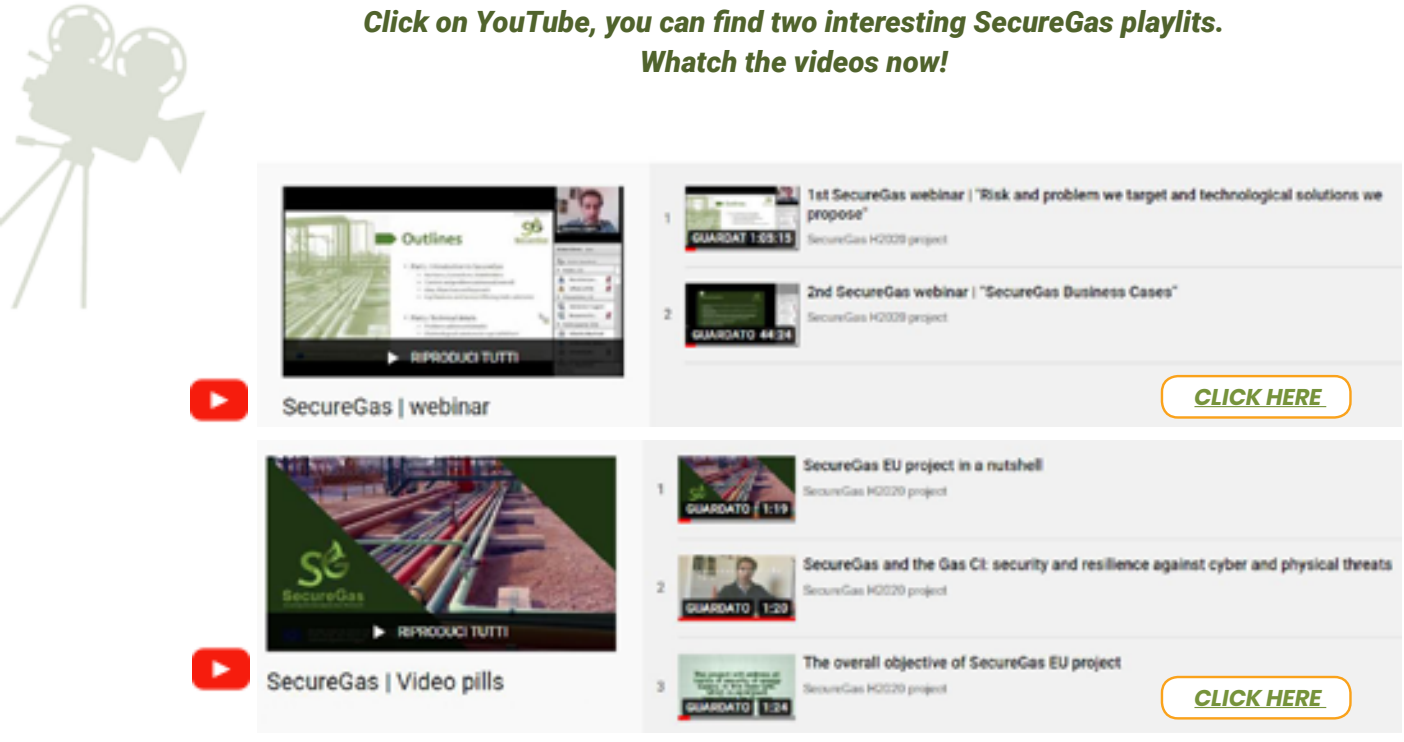
We regularly share most recent developments in the project and project results and show our activities like event participation, invitation to project events, etc.

If you want to be updated, FOLLOW US on:

TWITTER	LINKEDIN	YOUTUBE
@secure_gas	**@SecureGas**	**SecureGas H2020 project**

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

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



SECUREGAS COORDINATOR:

RINA
Clemente Fuggini
clemente.fuggini@rina.org

SECUREGAS PARTNERS:

Fraunhofer EMI
LEONARDO
KIMIA
ΔΕΠΑ
eni
guardtime
Amber Grid
Elbit Systems
WINGS ICT SOLUTIONS
IDEMIA
ADPM DRONES
RĪGAS TEHNISKĀ UNIVERSITĀTE
European Commission
EXUS
Analysis
Innov-acts
APRE
TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR
διανομή αερίου ΑΤΤΙΚΗΣ
D.MAST

Get in Touch!

www.securegas-project.eu