SecureGas project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 833017
SecureGas numbers and consortium

<table>
<thead>
<tr>
<th>Project Title:</th>
<th>Securing the European Gas Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting date</td>
<td>1 June 2019</td>
</tr>
<tr>
<td>Ending Date</td>
<td>30 November 2021</td>
</tr>
<tr>
<td>Budget info</td>
<td>9.194.410,60 € (funding around 7M€)</td>
</tr>
<tr>
<td>Partners</td>
<td>21 partners</td>
</tr>
</tbody>
</table>

SECUREGAS COORDINATOR:
Clemente Fuggini
clemente.fuggini@rina.org

SECUREGAS PARTNERS:
SecureGas focuses on key elements (e.g. installations, pipelines) of the +140.000 Km of the European Gas network from Production to Transmission up to Distribution.

... In 3 specific targeted areas:
1) Greece
2) Lithuania
3) Italy
SecureGas project

- **OVERALL OBJECTIVE**: To increase the **SECURITY & RESILIENCE** of the EU Gas Critical Infrastructure (e.g. network and installations), by taking into account both physical and cyber threats, as well as and their combination

- **APPROACH**: **Resilience-based** approach to tackle cyber-physical risks and threats to the Gas network and installations
Cyber Threats

- Energy systems and suppliers are target of ransomware and cyberattacks

- The number of incidents reported in the O&G sector is less if compared to physical incidents. Main ones:
  - Cyber attacks on OT network of SCADA systems
  - Ransomware attacks

- The impact (financial damage) is high
  - Global figures estimate that cybersecurity breaches in oil and gas and power cost operators $1.87 billion up to 2018

https://www.uscert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf
Reference Scenarios: Cyber

Cyber-Attack to the control networks of energy grid triggered by a gas grid operator

Cyberattack on gas pipeline data network
Source: https://www.thelocal.it/20171212/italy-state-of-emergency-austria-explosion-gas

Ransomware Impacting Pipeline Operations
Source: https://us-cert.cisa.gov/ncas/alerts/aa20-049a
Reference Scenarios: Cyber

Cyber-Attack to Colonial Pipeline

Hackers Breached Colonial Pipeline Using Compromised Password - The hack took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast.

It was the result of a single compromised password

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account

May 7th, an employee in Colonial's control room saw a ransom note ....

May 7th Colonial shuts down the pipeline

Colonial began resuming service on May 12th

No breach the more critical operational technology systems


It was the first time Colonial had shut down the entirety of its gasoline pipeline system in its 57-year history

Colonial paid the hackers a $4.4 million ransom
Solutions

https://youtu.be/vFa5qFTMzWI
Validated in 3 Business Cases

**BC3:** Operationalising cyber-physical resilience for the security and asset integrity of strategic gas installation.

It addresses Production and Transportation (Upstream to Midstream) with particular emphasis on import pipelines and connections with National Grids.

**BC2:** Impact and cascading effect of cyber-physical attack.

Transportation network (midstream) with particular emphasis to vital nodes of the network, that if damaged could cause significant disruptions and cascading effects to interconnected (energy) infrastructures.

**BC1:** Risk-based security asset life-cycle management.

Transportation and Distribution (Midstream up to Downstream) of Gas at strategic (project planning), tactical (project risk assessment) and operational (Distribution Network) level.
Business Case 1

Compliance with the “Common Risk Assessment Approach” as required by EU Regulation 2017/1938

COGNITIVE FRAMEWORK FOR BIOMETRICS AND VIDEO ANALYTICS

Identify malicious physical presence near critical gas infrastructures and suspicious objects detected from the cameras and input sensors within or near the CIs.

RISK AWARE INFORMATION TO THE POPULATION

Enable Gas CI operators to (efficiently) notify authorities (civil protection, first responders, other CI operators) on an emergency.

CYBER PHYSICAL CORRELATOR

A Machine Learning based tool for advanced event processing to monitor the resources of the SecureGas platform, as well as different components, aggregating the information in order to detect threats.

JOINT CYBER-PHYSICAL RISK & RESILIENCE MANAGEMENT

Enhance the security and resilience of gas CI networks, covering the main principles imposed by Resilience and Disaster Risk Management Cycle.

SU-INFRA01-2018 | Grant Agreement No. 833017

Securing the European Gas Network
Business Case 2

Compliance with the “‘running .. scenarios of disruption of gas supply (e.g. transmission infrastructure, storages) ... Assessing their likely consequences’,” of EU Regulation 2017/1938

RESILIENCE OF THE IT/OT NETWORKS
Improving security weaknesses in interface points between IT and OT networks (e.g. hacked/infected control server issuing fault/non reliable commands via OT (SCADA) protocol, fault information report).

GAS NETWORK MODELLING AND SIMULATIONS
Modelling and simulation of coupled gas grids, combining the already available modelling techniques with a thorough inclusion of quantitative response and recovery models.

UAVs FOR LEAKS DETECTION
Application of UAVs for leaks detection of buried pipelines and decision support to the operator.

JOINT CYBER-PHYSICAL RISK & RESILIENCE MANAGEMENT
Enhance the security and resilience of gas CI networks, covering the main principles imposed by Resilience and Disaster Risk Management Cycle.
Business Case 3

Compliance with the ""develop and agree on preventive and emergency measures"" as required by EU Regulation 2017/1938

THIRD PARTY INTERFERENCE AND LEAKS DETECTION

Leaks detection, due to TPI and external sources via Distributed Fiber Optics and Vibroacoustic sensors.

ACQUIRE AND GEO-REFERENCE ANY CHANGES

Patrolling via UAVs, programmable on demand by the operator and trigged by the leaks or intrusion detections.

RESILIENCE OF THE OT/IT NETWORK

Protection from «Man in the Middle Attack» to SCADA system by means of components that protect the SCADA network.

MONITORING AND EARLY WARNING OF LANDSLIDES

Hazard mapping and an early warning alert system for rainfall-induced landslides, specifically tailored to onshore linear infrastructures such.
Research & Innovation as an opportunity

- In a dynamically evolving context, the challenges posed by Cyber Threats are even more relevant.

- New and more complex type of attacks will cause severe consequences to the Energy (O&G) companies at both operational and financial level (see for instance the Colonial Pipeline).

- There is the need for more and new “solutions” to cope with these issues and for a “paradigm” shift that moves from PROTECTION TO RESILIENCE, aimed at preventing, promptly detecting, timely responding to and cost-effectively recovering from disruptions caused by cyber Threats.

- Research & Innovation in this field is therefore essential not only at “operational” level with new tools, solutions and applications to be developed but also at “strategic” level to enforce a Resilience approach into the management processes of the organizations.
SecureGas Project Coordinator
Clemente Fuggini (RINA)
clemente.fuggini@rina.org

www.securegas-project.eu

SecureGas project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 833017