SecureGas

Securing the European Gas Network

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

SecureGas
Securing the European Gas Network

Project Title:	Securing the European Gas Network
Starting date	1 June 2019
Ending Date	30 November 2021
Budget info	9.194.410,60 € (funding around 7M€)
Partners	21 partners

SECUREGAS COORDINATOR:

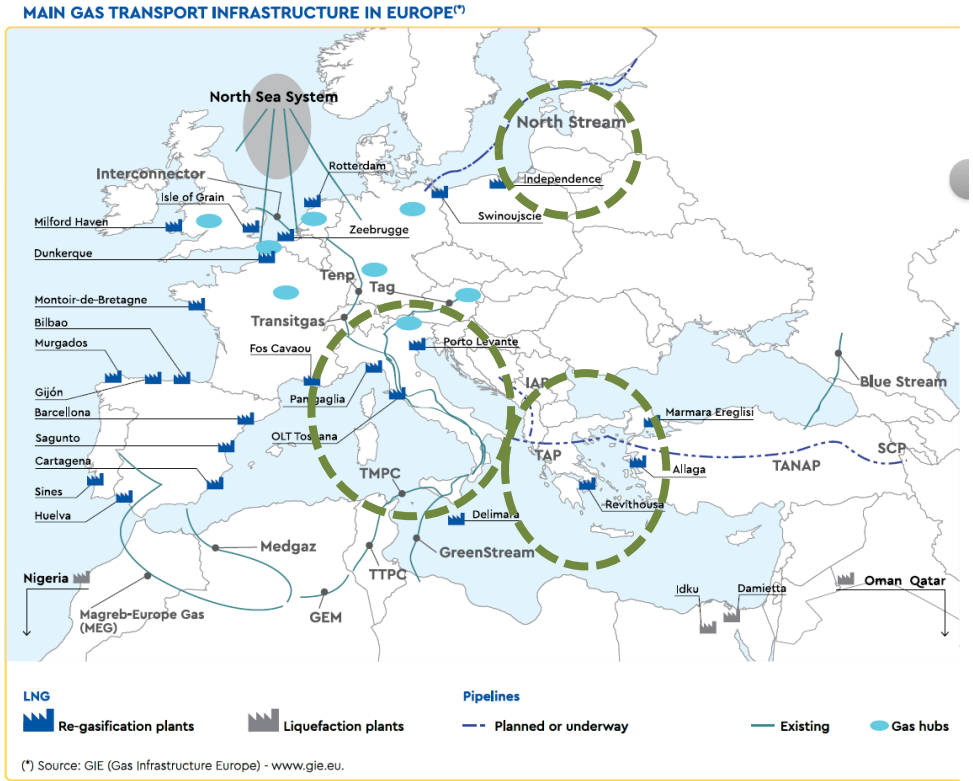
RINA

Clemente Fuggini
clemente.fuggini@rina.org

SECUREGAS PARTNERS:

Fraunhofer EMI · LEONARDO CYBER SECURITY · KEMEA · 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 · D.M.A.T

SecureGas Focus: EU Gas Network



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:

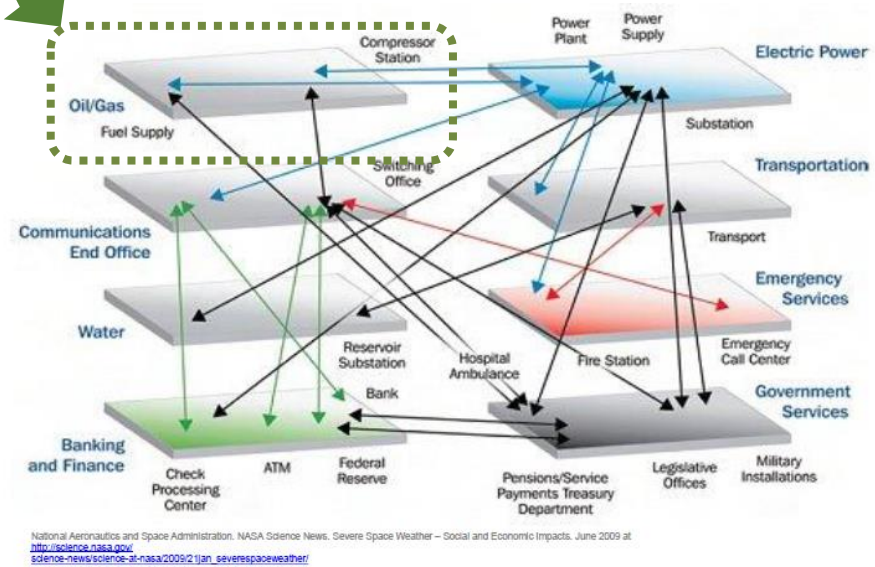
1) **Greece**
2) **Lithuania**
3) **Italy**

SecureGas project

SecureGas
Securing the European Gas Network

- **OVERALL OBJETIVE**: 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



National Aeronautics and Space Administration. NASA Science News. Severe Space Weather – Social and Economic Impacts. June 2009 at http://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather/

NATURAL EVENTS

MAN-MADE ACCIDENTS

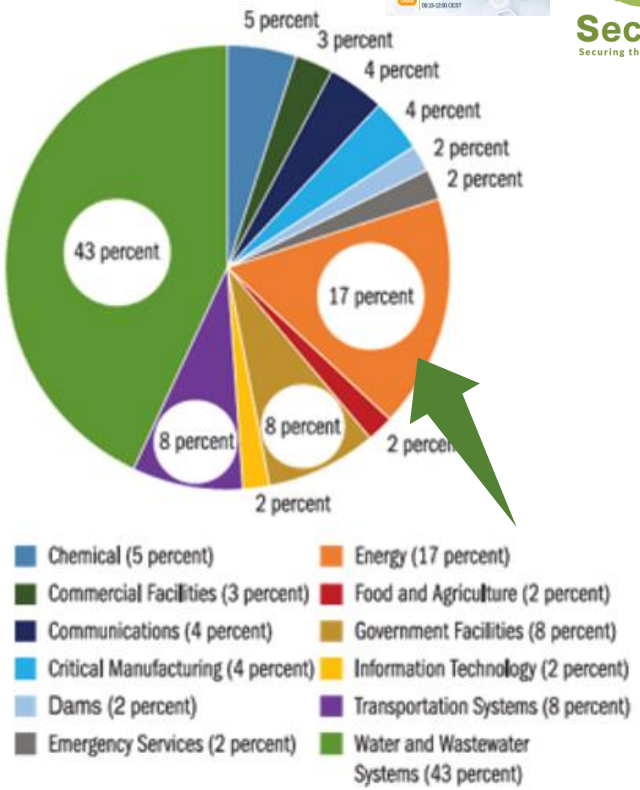
CYBER ATTACKS

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

Source: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3

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

Source: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

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

SecureGas
Securing the European Gas Network

Extended Components

SecureGas

TECHNOLOGIES FOR INFORMATION PROCESSING AND MANAGEMENT (B)

- Cyber physical correlator
- Blockchain for data transmission and integrity verification
- Cyber Security for IT and OT networks weakness
- Wings Platform

A — TECHNOLOGIES FOR SITUATIONAL AWARENESS AND DECISION SUPPORT FOR CYBER-PHYSICAL THREATS

- Safety and Security platform for Gas CI
- Autonomous docking station and UAV based asset management
- Onshore Landslide Susceptibility and Alert/Monitoring System

D — TECHNOLOGIES FOR JOINT CYBER-PHYSICAL SECURITY RISK MANAGEMENT AND RESILIENCE MODELLING

- Joint Cyber-Physical Risk and Resilience Management
- Gas Network Advanced Modelling and Fast-Dynamics Simulation
- Risk-Aware Information to the population
- Risk-Aware Information to the population (RAW component)

C — TECHNOLOGIES FOR DETECTION, IDENTIFICATION AND EARLY WARNING

- Distributed Acoustic Sensing (DAS) for monitoring of leakages and third party intrusion in Oil & Gas pipelines
- Combined analytics for biometrics and video analytics
- Cognitive framework for biometrics and video analytics
- Sensors for detection, identification and early warnings

https://youtu.be/vFa5qFTMzWI

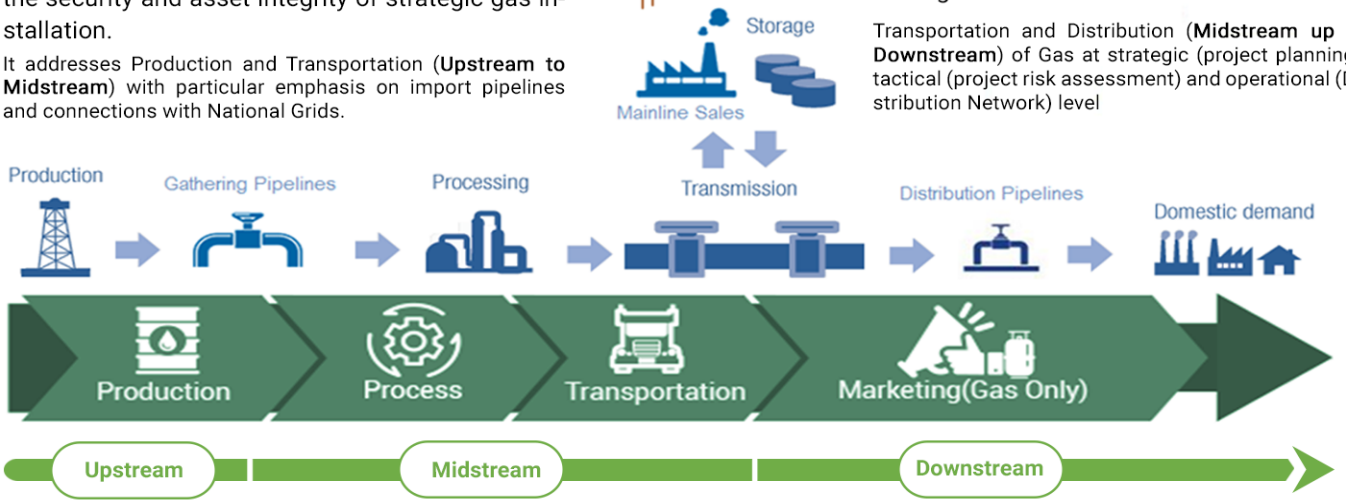
Validated in 3 Business Cases

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.

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



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

Business Case 1

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

SecureGas
Securing the European Gas Network

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.

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.

RISK AWARE INFORMATION TO THE POPULATION

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

BUSINESS CASE 1

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 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

SecureGas
Securing the European Gas Network

RESILIENCE OF THE IT/OT NETWORKS

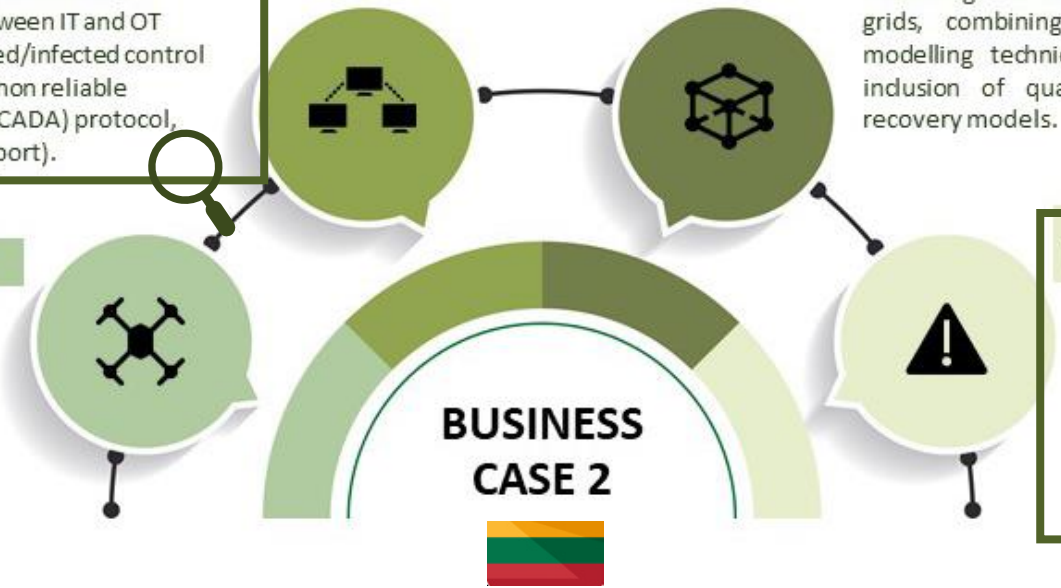
Improving security weaknesses in interface points between IT and OT networks (e.g. hacked/infected control server issuing fault/non reliable commands via OT (SCADA) protocol, fault information report).

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

SecureGas
Securing the European Gas Network

THIRD PARTY INTERFERENCE AND LEAKS DETECTION

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

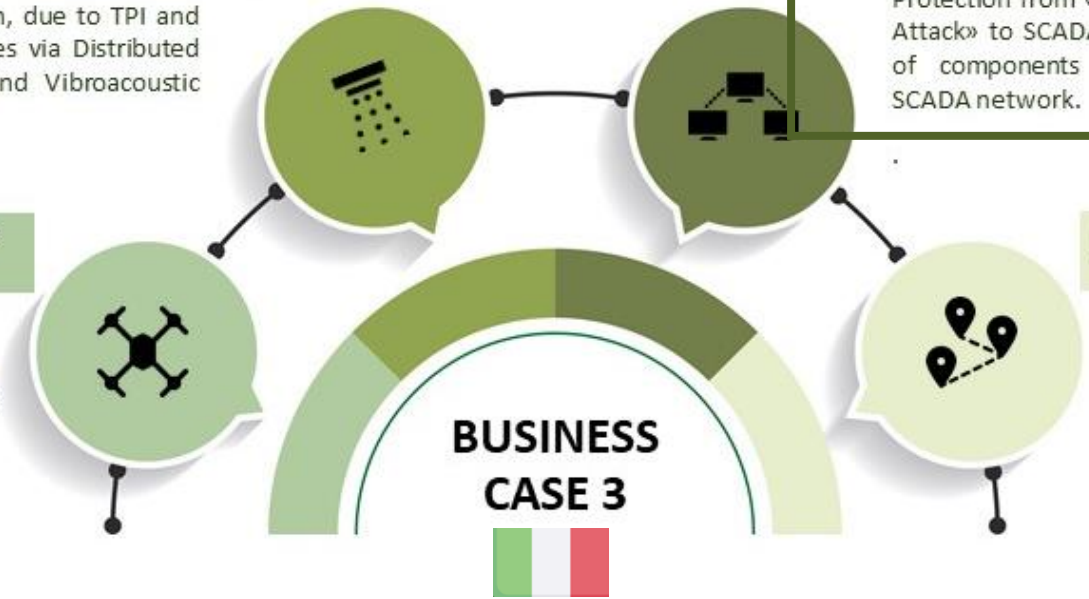
RESILIENCE OF THE OT/IT NETWORK

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

.

ACQUIRE AND GEO-REFERENCE ANY CHANGES

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



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

SecureGas
Securing the European Gas Network

- In a dynamically evolving context**, the challenges poses 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 a**t "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
Securing the European Gas Network

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