N.1 NEWSLETTER

December 2019

SecureGas

Securing The European Gas Network

IN THIS ISSUE:

- SecureGas project in a nutshell
- SecureGas: acheivements so far

... ***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.1

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

SecureGas project in a nutshell

1

PROJECT ACRONYM:	SecureGas
PROJECT TITLE:	Securing the European Gas Network
GA NUMBER:	833017
CALL:	SU-INFRA01-2018-2019-2020 | Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe
ACTION TYPE:	Innovation Action (IA)
STARTING DATE:	1° June 2019
ENDING DATE:	31 May 2021
DURATION:	24 Months
BUDGET INFO:	9.194.410,60 € (cost); 6.993.400,75 € (funding)
PARTNERS:	21 partners

SecureGas

The challenge

Existing and new Gas infrastructure will have to resist to hazards and absorb their impacts more efficiently and more effectively; accommodate and recover the effects of a hazard more timely and safely; and be designed/restored to coordinate more efficiently across the various phases of a disaster risk management cycle.

Project Objectives

To increase Security and Resilience of the EU Gas Critical Infrastructure (e.g. network and installations) from production to transmission up to domestic distribution, by taking into account both physical and cyber threats, as well as and the combination of them.

Concept and approach

Towards a Resilience-Based Management of Gas Assets and Infrastructures: a systemic (multi-hazards, multi-threats) security risk and resilience management approaches, including the combination of physical and cyber threats, their interconnections, cascading effects and emergent behavior (unexpected systemic behavior).

Expected Results

- SecureGas Conceptual Model (CM): blue print on how to design, build, operate and maintain the EU gas network to make it secure and resilient against cyber-physical threats.
- SecureGas High-Level Reference Architecture (HLRA): a reference framework for the implementation, integration and interoperability of SecureGas components.
- A set of advanced components (covering Situational Awarness, Decision Support, Information Management, Risk and Resilience Management), customized, integrated to the extent needed and according to the HLRA, afterwards deployed, demonstrated and validated in the three project business cases, designed according to policy-relevant scenarios.
- A Cost Benefit Analysis (CBA) to asset the benefits and impact of SecureGas in the three Business Cases to SecureGas.
- White paper *"Lessons learnt and recommendations for cyber-physical resilience of European Gas Critical Infrastructure"*.

Target end users

Gas Critical Infrastructure Managers and Operators, Gas and Energy companies, Associations and Agencies in Gas Sector in EU and at National Level, Bodies implementing the CI Directive at National level.

Main project events

> Mediterranean Security Event | 29-31 October 2019, Crete, Greece

> SecureGas 2nd End-user Workshop | November 2020, Athens, Greece

> SecureGas Final Conference | May 2021, JRC - Ispra, Italy

EU Policies

- SecureGas frames the regulatory context in D1.1 "Organisational, Operational and Regulatory requirements".
- SecureGas Business Cases have been designed to address specific issues of EU Regulation 2017/1938 on Security of Gas Supply.
- SecureGas delivers a White Paper acknowledging The European Energy Security Strategy, The European Directive 2008/114/EC, The European Programme for European Critical Infrastructure Protection (EPCIP).

SecureGas: acheivements so far

2

In November 2019, SecureGas has entered Month 6 of its timeline, out of 24 months foreseen in total.
From the project kick-off in June 2019 up to November 2019, the project has already complemented several activities and has reached some important achievements that are turning soon into tangible outcomes.

First at all, both **end-users and technical requirements have been delivered**.
They have been iterated and validated during the 1st stakeholder workshop in Freiburg, September 10, 2019.

They availability of end-users and technical requirements, allows us moving to the next phase of the project, corresponding to the delivery of the **SecureGas Conceptual Model** (CM) and, based on this, of the **SecureGas High-Level Reference Architecture** (HLRA).
The CM is intended as a blue print on how to design, build, operate and maintain the EU gas network and its installations to make them secure and resilient against cyber-physical threats.

Furthermore, it has to be seen as an extension of the classical Disaster Risk Management (DRM) cycle in terms of pre-hazards and post-hazard phases, as depicted in the **figure 1**.
In addition, how the "panarchy loop" is integrated within the various phases of an Asset Management process (Evaluation and Planning, Design, Construction, Operation & Maintenance), is depicted in the **figure 2.**

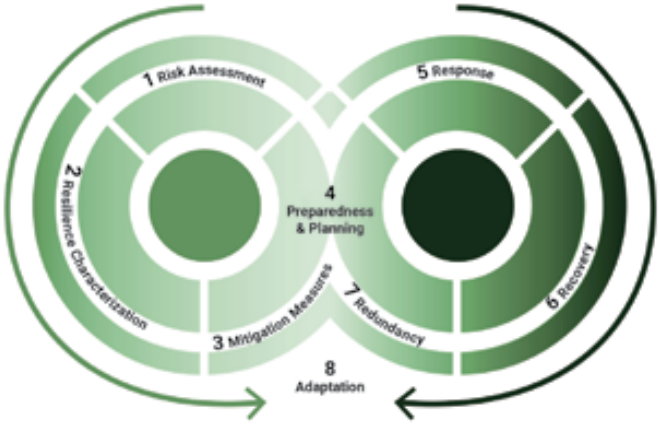


Figure 1 - SecureGas Conceptual Model: linking Resilience and the DRM cycle in a "panarchy loop" (Source RINA)

On the other side, the HLRA is intended to provide a reference architectural framework for the implementation, integration and interoperability of SecureGas components, being agnostic from the specific installation, and thus comprehensive of main installation and infrastructure typologies in the Gas network.

SecureGas components design is starting soon, banking on the technical requirements and HLRA definition. The components cover a variety of technologies and applications ranging from Situational Awarness, Decision Support, Information Management, Risk and Resilience Management.

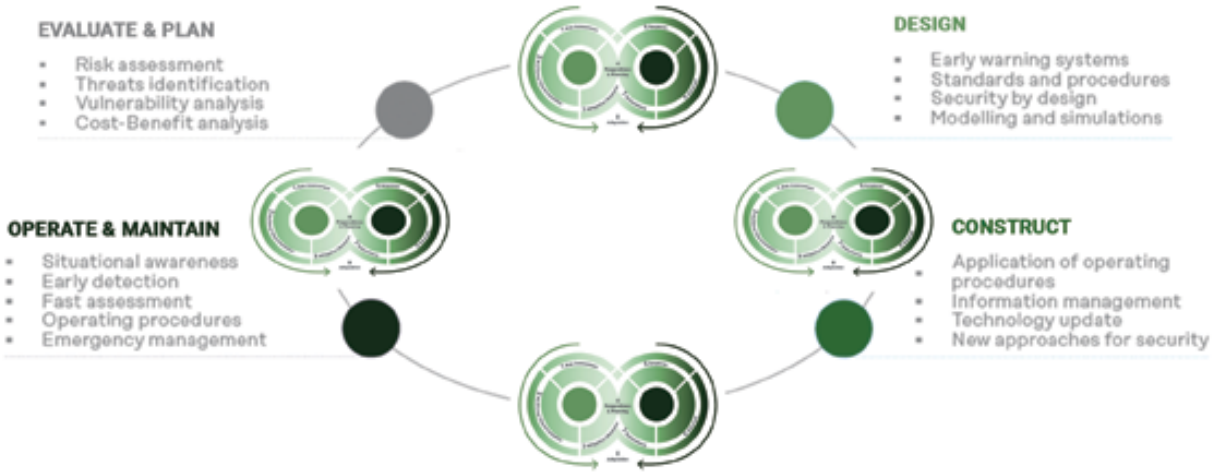


Figure 2 - Integration of the Panarchy loop into an Asset Management process across the Life-Cycle of an infrastructure (source RINA)

The components will be later on customized, deployed, demonstrated and validated in **three project Business Cases**, according to their scenarios.

Indeed, in parallel to the implementation of the components, the design of the project Business Case scenarios is ongoing. They will reflect specific issues that are relevant for the project and the stakeholders in the gas sector as well as they will try to provide tangible contributions to EU directives and policy including the European Directive on Critical Infrastructure, and the EU regulation on Security of Gas Supply.

In parallel to the technical work, SecureGas is seriously monitoring any ethics and security issue arising in and from the project, through a process of continuous supervision of ethics and security, in line with the H2020 guiding principles and in compliance with the main regulations and directives in scope.

Last but not least, SecureGas **communication and dissemination activities** haven been launched from the very beginning of the project and are constantly ongoing to ensure wide visibility of the project and its results on timely basis.
In this context, **SecureGas social media accounts** have been established:

Also the **SecureGas website**

https://www.securegas-project.eu/

is now fully operational. Besides the latest news about the project, it also contains a **Stakeholder Platform**, where security-related stakeholders are registered and have the possibility to access all relevant project documentation and to exchange information between themselves and with the consortium partners. If you are interested to join the platform, write directly to the *Platform Manager* at: magni@apre.it.

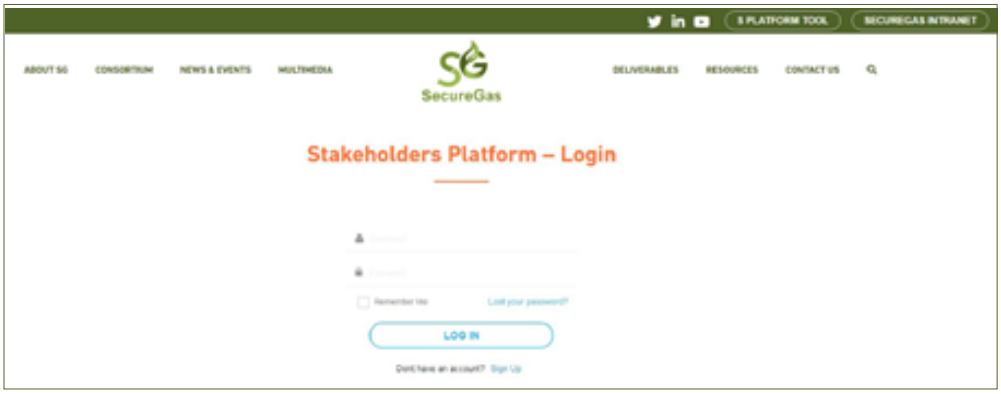


Figure 3 - SP tool | HOME PAGE

Figure 4 - SecureGas website | HOME PAGE

1st SecureGas Stakeholder workshop. Main outcomes

3

The workshop, that took place on 11 September 2019 in Freiburg (Germany) at the premises of a SecureGas partner – Fraunhofer-Gesellschaft, was one of two workshops foreseen in the project. It gathered 15 stakeholders, external to the project consortium and 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 was also attended by the project partners, resulting in **more than 50 participants**.

The **main purpose of the workshop** was to collect feedback of the stakeholders and the project partners on: (i) the End-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.

- SecureGas should be digitally secure and safe (protected against hackers and malware) as well as resilient so as to easily recover from potential adverse events.
- Installed hardware components of the SecureGas system should be secure and safe to prevent loss, damage or harm of the system and resilient so as the system to recover fast in case of potential adverse events.
- SecureGas should be designed considering organizational interoperability aspects that enable seamless interaction and collaboration of different organizations, authorities and entities to achieve their mutual goals.
- SecureGas should be designed and deployed taking into consideration the training needs of future users.
- SecureGas should enable the report of security incidents affecting the normal operation of the Gas CI network.
- SecureGas should be cost-efficient and financially sustainable, taking into account market trends and commercial prices of the competition.
- SecureGas business offering should be designed taking into consideration the maintenance cost of the system's infrastructure as well as any auxiliary and consulting services to be provided to the end-users.

Regarding the **first Business Case (BC1) led by DEPA (Greece)**, the workshop participants provided diverse comments on the business case potential pilot scenarios. Most information concerned the realization of threats and potential triggering events on the proposed generic scenarios. Participants focused on explaining how multiple threats and simultaneous events can influence the impact of malicious attacks on gas pipes and stations. One interesting scenario that was introduced by stakeholders involved a situation with two simultaneous threats: intentional or unintentional wildfires and malicious attacks that leverage them to attack vulnerable stations and pipes and cover their tracks.
Stakeholders' and consortium partners' feedback provided essential information that is being used for the development of BC1 scenarios, by pinpointing potential sensitive issues during modeling and by listing critical threats and worst-case impact according to their knowledge and expertise.

Regarding **the second Business Case (BC2) led by AMBER (Latvia)**, three business case scenarios were introduced to the external stakeholders to collect know-how and experience:

a) Application of drone for gas leak detection,
b) Analysis and modelling of gas network resilience with respect to location of SCADA remotely controlled valves,
c) All-hazard and all-threats case study of compressor station and nearby pipeline area.

The summary of the feedback collected is provided below:

a) Investigate available alternative solutions, including fibre optic technology, satellite images, surveillance from helicopters and manual inspection of leaks. Combination of different alternatives for leak detection can be applied to be sure on data accuracy.
b) Analysis may include checking of SCADA communication credibility using simulation, consequences to remote SCADA control if there is no electricity or mobile coverage as well as in case of an unauthorized software update or single node compromised.
c) The analysis may include risk assessment, identification of critical nodes and strategy for replacement, options / threats for remote operation, community-watch programs, "Intelligent probes" to monitor the OT network in order to detect suspect activities.

Feedback received from the stakeholders is valuable in terms of broader perspective and possible additional

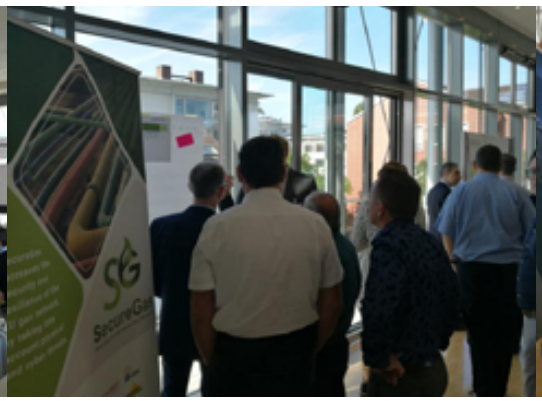
solutions of the BC2. Such inputs like: combination of different alternatives, community-watch programs, "Intelligent probes" to monitor the network, are the most important. All relevant aspects will be evaluated during the course of the work within business case.

Regarding **the third Business Case (BC3) led by ENI (Italy)**, the workshop was very useful in aligning the key requirements and critical points of the Business Case context (e.g. gas production and transportation to the national grids).

Indeed, the participation of stakeholders that share the same role and view of BC3 and of BC3 owner, ENI, was beneficial. In particular, a representative from the stakeholders provided a number of points that are largely shared by BC3 and acknowledge the perspective of company/organizations, such as ENI; whose role in the Gas Value Chain is focused on import/export of natural gas from production and extraction to the national grids.

Moreover, the stakeholders clearly identified triggering points and helped understanding weakness in the foreseen generic scenario description with respect to critical assets that should be protected.

As such, all points raised have been helpful in better aligning the scope of BC3 to common needs and requirements as well as to policy concerning gas supply in EU and have confirmed that the direction BC3 was looking for is the correct one.



Watch the video: "*SecureGas H2020 project | First Workshop*"

SecureGas: "*We have been there!*"

4th Meeting of the Community of Users on Secure, Safe, Resilient Societies

16 – 19 September 2019, Brussels, Belgium

SecureGas presented its goals to increase the security and resilience of the EU gas network.

7th Pipeline Maintenance & Integrity Management for Oil & Gas Industry

16-18 October 2019, Amsterdam, the Netherlands

ENI, on behalf of SecureGas, discussed '*Future Developments in Gas Transportation Smart Grids*' and provided a comprehensive overview of SecureGas project, its objectives and achievements so far.

Mediterranean Security Event 2019

29-31 October, 2019, Heraklion, Greece

The event organised by SecureGas partner - the Center for Security Studies (KEMEA) – aimed to facilitate interaction and synergy among security R&D activity and the networks of practitioners. SecureGas latest advancements were showen at the project booth and presented both: (i) in a dedicated session during the first day of the project, (ii) as well as in the framework of the CIP projects clustering, at a workshop aiming at working towards capacity building in the domain of R&D for Critical Infrastructure Protection in context of the DG HOME EPCIP and the coming Horizon Europe (HEU) Program.

MEDITERRANEAN SECURITY EVENT 2019

SecureGas
Securing the European Gas Network

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.MAST

Get in Touch!

www.securegas-project.eu