EU-Funded project to increase the security and resilience of the European gas network

The European gas network forms an integral part of the EU's energy needs and its plans to meet the carbon reduction figures set out in the Paris Agreement. It already forms a significant role in the energy mix accounting for 22 percent of the energy usage, and with the growth of power-to-gas technologies initiatives, it is expected to grow.

The gas network is complex by nature and highly interconnected. It crosses borders, utilizes a variety of different transportation pipelines, and is served by numerous diverse storage arrangements. All this complexity makes it a relevant example of Critical Infrastructure (CI) vulnerable to disruption by natural disasters, accidents, cyber-attacks, malicious behaviour, criminal activity or terrorism. Moreover, any outages or shortage in supply can have an adverse effect on the security of the EU and the well-being of its citizens.

Therefore, providing security and resilience to this vital resource and its infrastructure is of paramount importance. However, given the interconnected nature of infrastructure and potential cascading effects, ensuring security requires a broader understanding of the ramifications of a disruption. Among CI, the gas network and infrastructure represent a challenging case to be made secure and resilient to both physical and cyber threats, and their combination in orchestrated pervasive and long-lasting threat vectors.

When it comes to physical threats, EGIG (European Gas pipeline Incident data Group) reported a total of 1366 incidents from 1970-2016, the leading causes being Third Party Interference (TPI), such as ground works, malicious acts and sabotages, and ground movements. When it comes to cyber threats, although the numbers of incidents reported so far is less, the results can be devastating as well. Attacks such as Night Dragon and Shamoon have caused considerable financial damage to oil and gas companies. Global figures estimate that cybersecurity breaches in oil and gas and power cost operators $1,87 billion up to 2018.

In this context, to ensure the security and resilience of the EU gas network, RINA is coordinating a major Research and Development EU collaborative project, SecureGas. In line with the European Energy Security Strategy, the European Programme for European Critical Infrastructure Protection (EPCIP), the EU's reliance on gas imports and the EU Regulation 2017/1938 on Security of Gas Supply, the project focuses on the 140.000km of the European gas network covering the entire value chain from production to distribution, providing methodologies, tools, and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats.

Over the course of the project, it will define a blueprint on how critical gas infrastructure should be planned, designed, built, operated, and maintained to cope with cyber-physical security threats. This will serve as baseline for defining a High-Level Reference Architecture (HLRA), that will be used as guideline for adapting, customizing, integrating technological components that will be finally demonstrated in a set of Business Cases. The resulting outcomes will be offered as services for the security and resilience of the EU gas network through a Platform as a Service (PaaS) model, that allows modularity, flexibility, cooperation, and third-party interoperability.

The project boasts a multidisciplinary consortium of 21 international partners. It is made up of integrated energy company (ENI S.p.A.), gas corporation (Public Gas Corporation of Greece S.A), TSO – Transmission system operator (AB Amber Grid), and DSO-Distribution system operator (Attiki Natural Gas Distribution Company S.A.), managing all together +15000km of pipelines; technology providers active in the field of Security and Critical Infrastructure (Leonardo S.p.A., Guardtime A.S., Elbit Systems Ltd., WINGS ICT Solutions, IDEMIA Identity & Security Germany AG, EXUS, GAP Analysis S.A., Innov-Acts Ltd., and Disaster Management, Advice and Training Consulting KG), research and academic institutions in Energy, Security and Resilience Engineering (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung, Kentro Meleton Asfaleias, Joint Research Centre Ispra, Riga Technical University, Technologická platforma Energetická bezpečnost ČR), to support the project implementation. Finally, the Stakeholder Platform (SP), led by Agenzia per la Promozione della Ricerca Europea, will provide advice to secure a long-lasting diffusion of the project outcomes, beyond the project perimeter as well.

This project receives funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 833017.