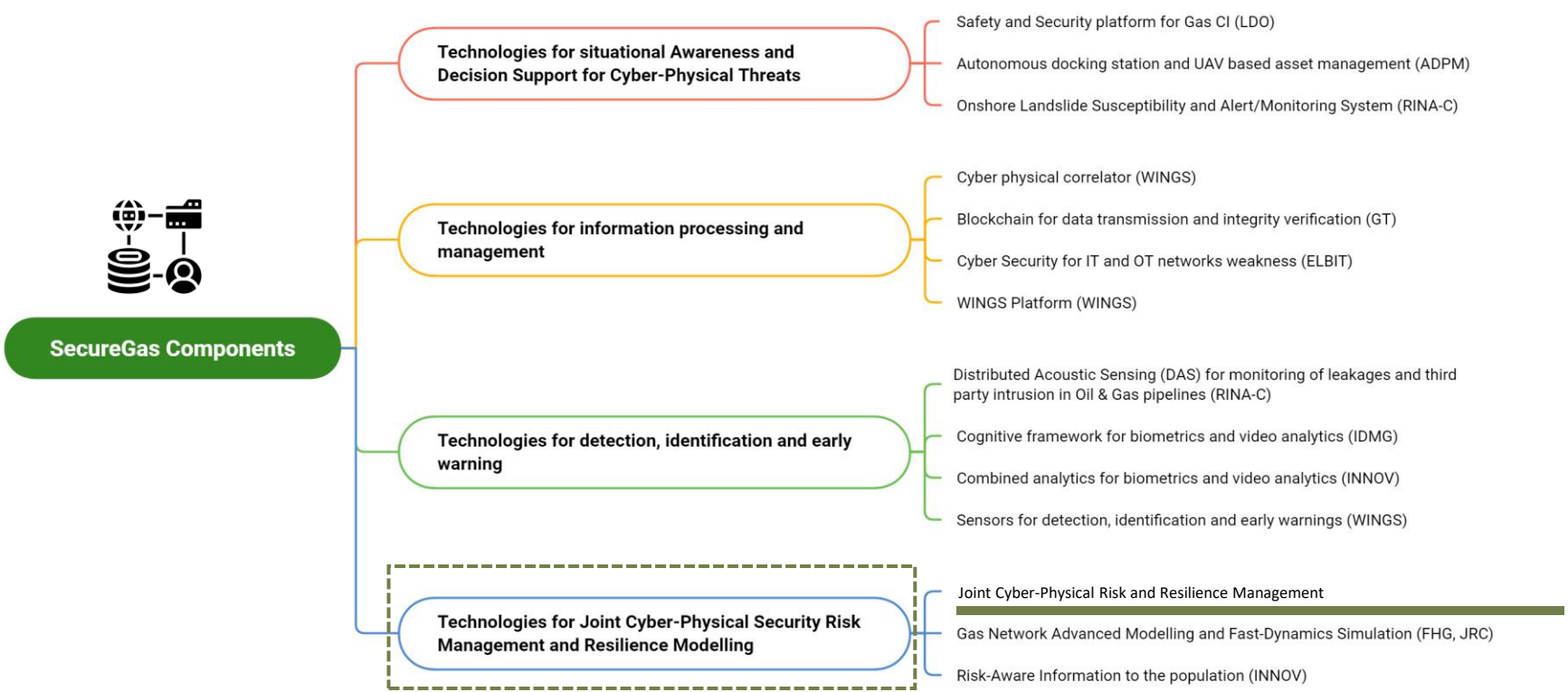
SecureGas

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 extended components



Joint Cyber-Physical Risk and Resilience Management

DESCRIPTION

The Joint cyber-physical risk and resilience management component (RMG) aims at enhancing the security and resilience of the Gas CI network, covering the principles imposed by the SecureGas panarchy loop. Indeed, the RMG component aims at providing support to the operators before, during and after an incident occurrence.

There are **two possible functionalities** of the risk assessment component:

a) The first one (standalone version) foresees a tool which is not connected to other systems and provides the software environment for applying the RMG model and assess risk and resilience for multiple security breach scenarios.

b) The second one (real time one), which interconnects to other systems/sensors, receives real time data allowing the dynamic evaluation of the risk level of the detected incidents, providing also resilience estimates and recommendations to the operators.

c) Both the above provide capabilities of risk and resilience assessment and therefore support decision making offering advanced situational awareness during security breach incidents.

Joint Cyber-Physical Risk and Resilience Management

SecureGas
Securing the European Gas Network

BENEFITS

The **MAIN BENEFITS** are:

(a) A tool for systematic and consistent risk analysis and assessment of security breach scenarios, addressing all assets and systems that are established within the boundaries of the CI under study.

(b) Provide support to the operators before, during and after an incident occurrence, aiming at adding values to the main risk and resilience phases.

(c) Supports real time risk and resilience assessment capabilities, enabling the dynamic risk level estimation of the security incidents detected by the SecureGas system.

(d) Provides the operator real time recommendations on the actions that need to be performed for the absorption of an event, the efficient response to it and the fast recovery in case of disruption.

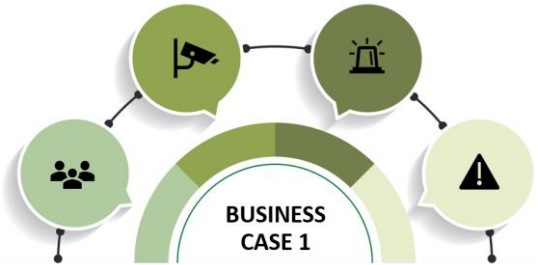
(e) Risk and resilience assessment regarding security threats and emerging risks for new Gas CI projects (design phase) shall support the implementation of a comprehensive all-hazards approach considering ssecurity, safety, technical and environmental aspects

Joint Cyber-Physical Risk and Resilience Management

SecureGas
Securing the European Gas Network

APPLICATION CASE

- **Business Case 1**



TARGETS

- **Target End Users:**
  1) HSSE Managers
  2) CI National Competent Authorities
  3) IT experts
  4) Other security services and software providers

- **Target Assets:**
  1) Oil & Gas CI operators (onshore/offshore)
  2) Other CI operators (e.g. energy and transport, water, health)
  3) Security Systems providers and Consultants in CIP
  4) European Research Projects

SecureGas

Securing the European Gas Network

SecureGas partner:

EXUS | GAP

g.diles@exus.co.uk - g.lazarou@exus.co.uk - d.katsaros@exus.co.uk | agrafioti@gapanalysis.gr

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