ECSCI Workshop

25th of June 2020

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

Project Title:	Securing the European Gas Network
GA number	833017
Starting date	1 June 2019 (M1)
Ending Date	30 Nov 2021 (M30)
Budget info	9.194.410,60 € (cost) 6.993.400,75 € (funding)
Partners	21 partners

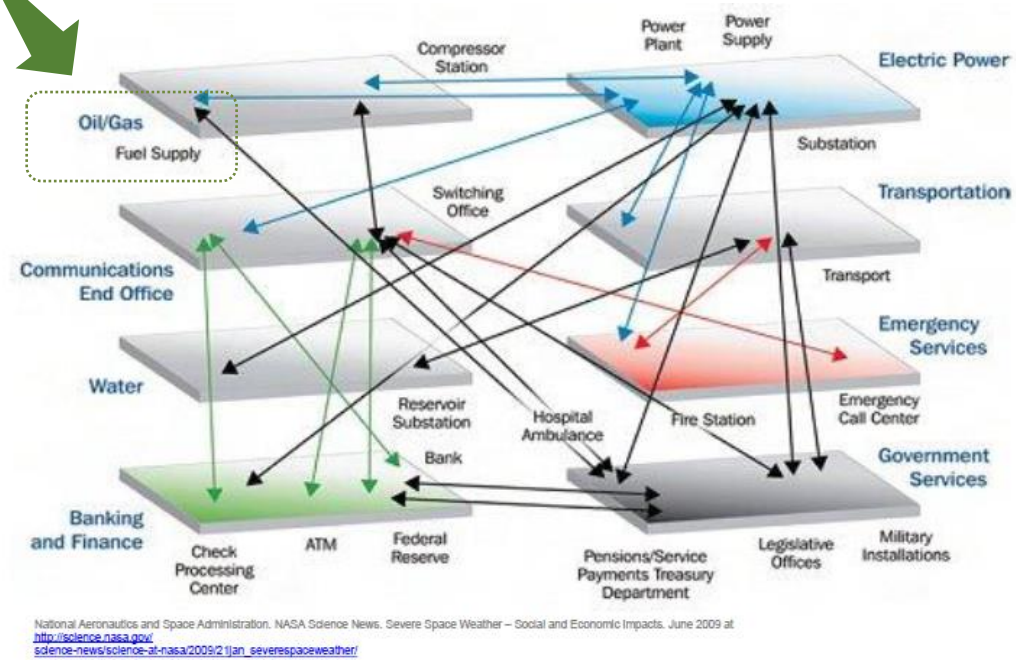
SECUREGAS COORDINATOR:

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

Context: Critical Infrastructure



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/

Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions.

The damage to a critical infrastructure, its destruction …. may have a significant negative impact for the security of the EU and the well-being of its citizens. [EU COM 114/2008]

Context: Physical Incidents

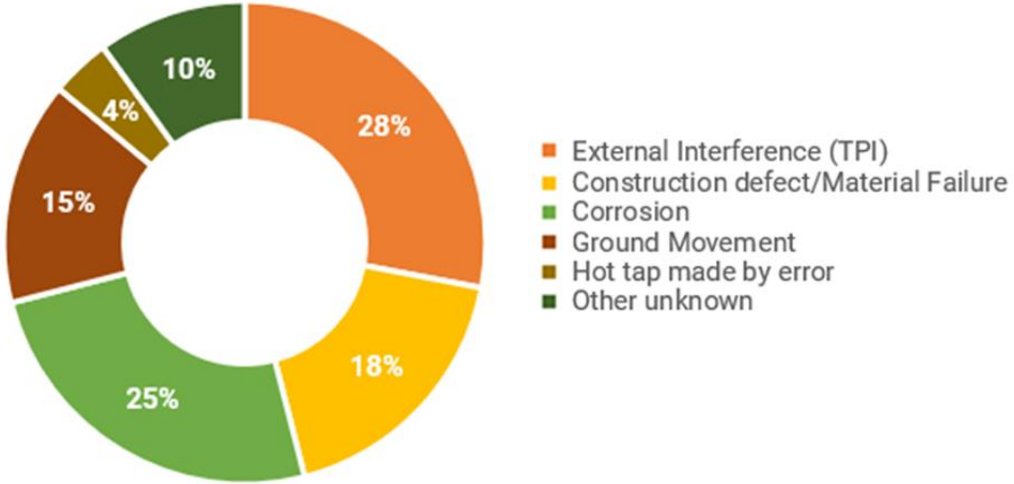
A total of 1366 incidents to gas network reported from **1970-2016**

Main causes:

A. **External interference (TPI)** (e.g. digging, piling or ground works by heavy machinery)
B. **Corrosion**
C. **Ground movement** (dike break, mining)

SecureGas addresses A) and C) as well as man-made/terrorist threats

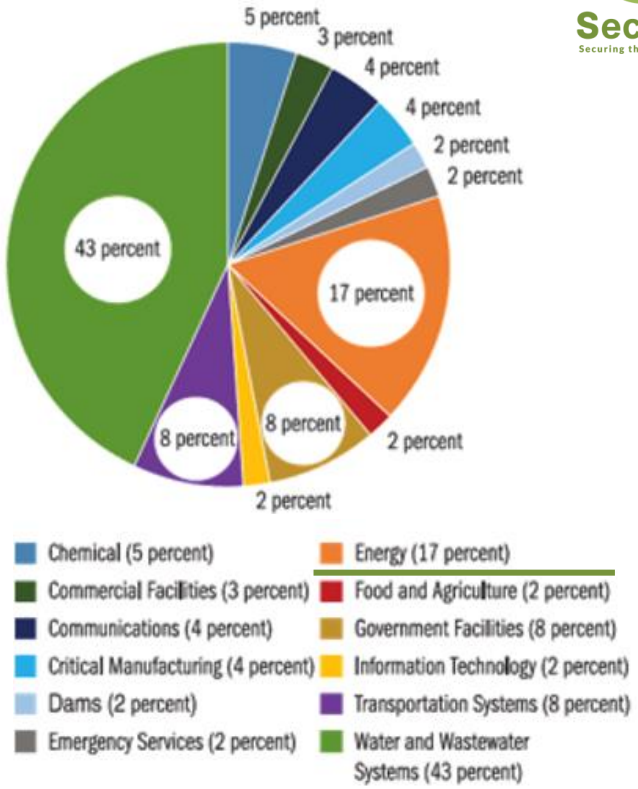
Gas pipelines incidents



Gas pipeline incidents, 10-th report of the European Gas Pipeline Incident Data Group (EGIG) https://www.egig.eu/reports; https://www.egig.eu/overview

Context: Cyber Threats

- The **number of incidents** reported so far **is less** if compared to the physical ones ….
- Whilst 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
- The main cyber issues addressed by SecureGas are cyber attacks on OT network of SCADA systems
- ***The protection of ICS/SCADA networks is a cross sectorial solution for any critical infrastructure***



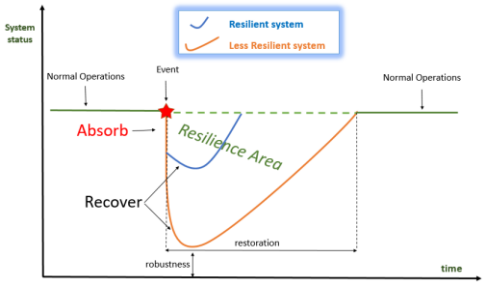
https://www.uscert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

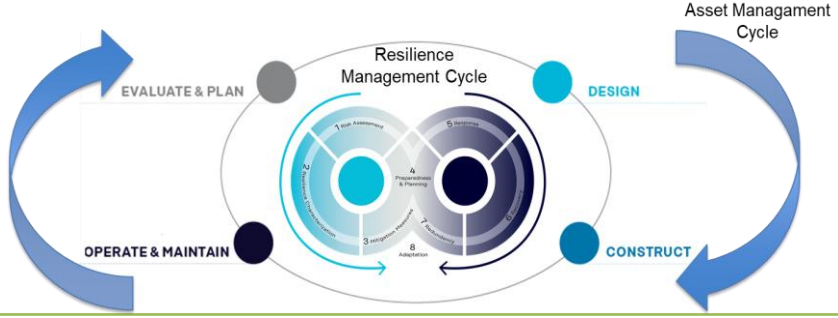
SecureGas idea: from Resilience of CI… to «Resilience Management» of CI… incorporating cascading effects

Providing "**resilience**" for Critical Infrastructure means to estimate the impact of loss of functionalities on the business and service continuity

Linking **Resilience Capabilities** (Plan/Prepare, Detect, Absorb, Recover, Adapt) to the **Disaster Management Cycle** (Prevention, Preparedness, Response, Recovery) and then embedding them into an **Asset Management Process**.

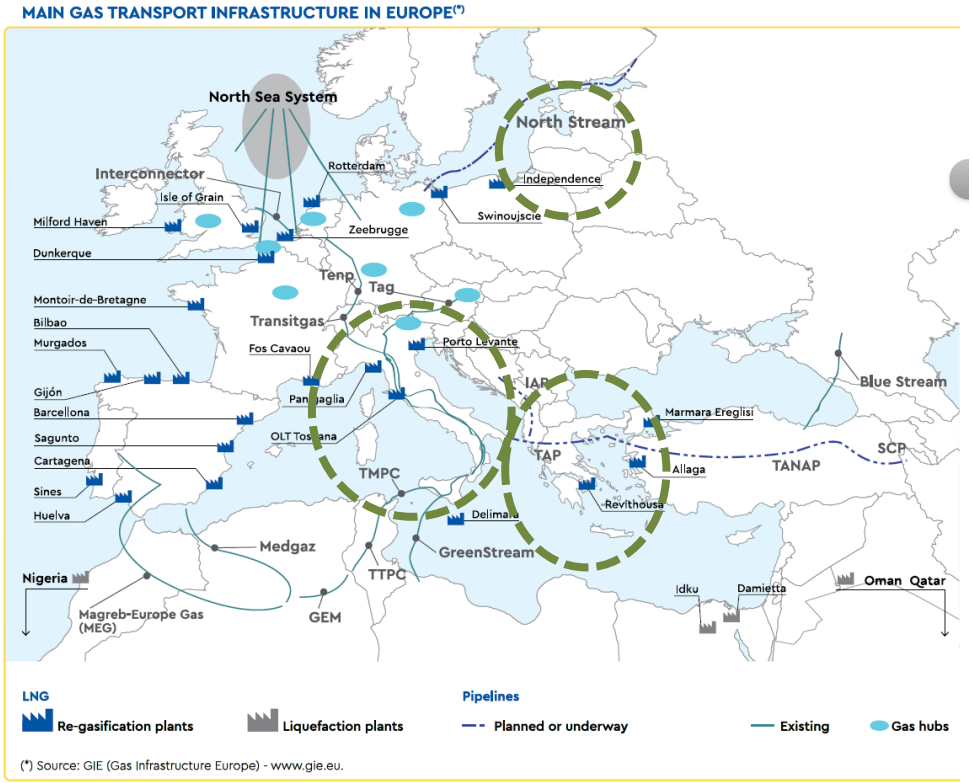
Providing "resilience" means **not only to secure the specific infrastructure but also to understand and estimate the potential cascading effects** induced by the loss of functionalities of one infrastructure on the others





Italy's Gas supply limited by explosion at gas plant in Austria 2017

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 (Baltic states)**
3) **Italy**

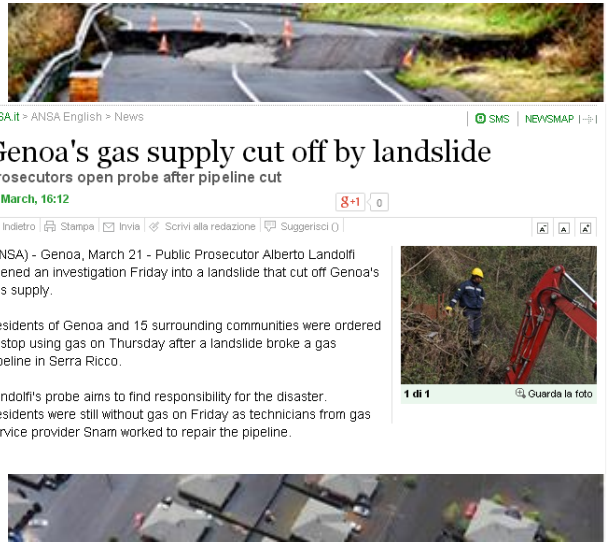
End Users:

ΔΕΠΑ · διανομή αερίου attikis · Amber Grid · eni

SecureGas Overall Objective

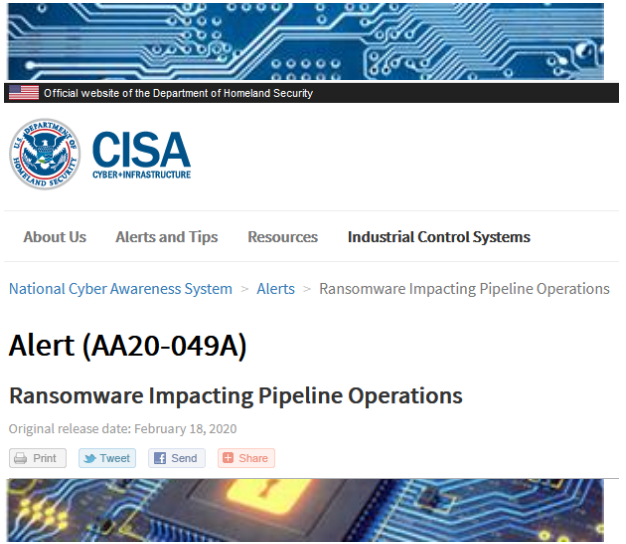
To increase the **SECURITY** & **RESILIENCE** of the EU Gas Critical Infrastructure (e.g. network and installations), by taking into account both physical and cyber threats, as well as and their combination.

NATURAL EVENTS



MAN-MADE ACCIDENTS

CYBER ATTACKS



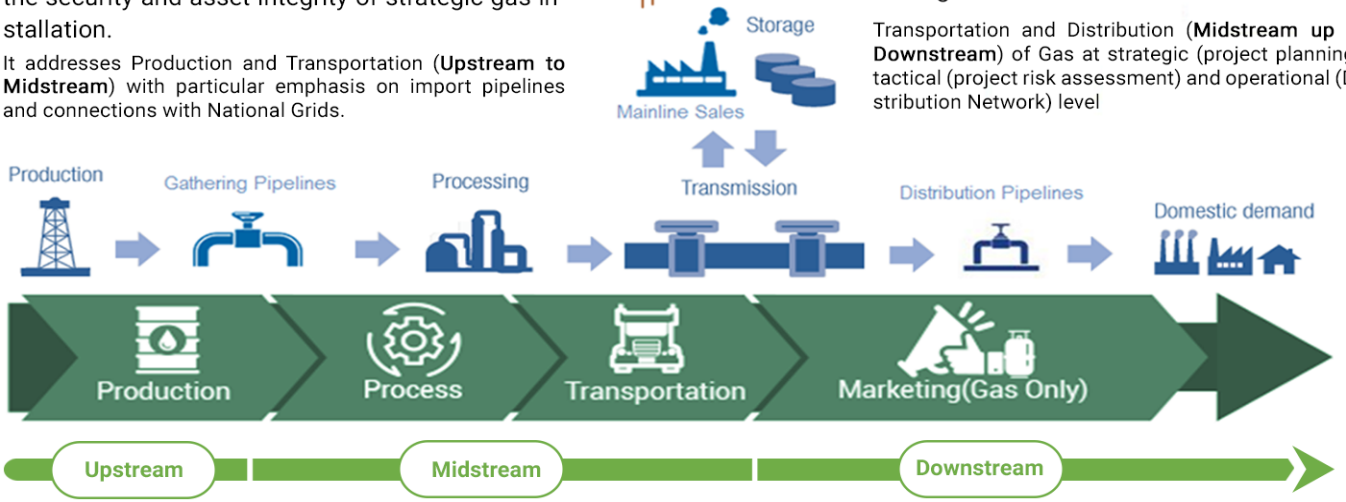
Validated in 3 Business Cases

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

SecureGas adopts a Business Case driven approach across the whole Gas supply chain from Production to Marketing, from Upstream to Downstream

Key features & Service Offering

SecureGas
Securing the European Gas Network

SecureGas

Conceptual Model (CM)

A blue print on how to plan, design, build, operate and maintain the EU gas network to make it secure and resilient against cyber-physical threats.

Three Business Cases (BCs)

- BC1
- BC2
- BC3

High Level Reference Architecture (HLRA)

A generalized architecture to serve as "instructions" or " guidelines" to implement models, approaches and solutions in line with the CM.

Extended Components

A set of tools/methods/models/technical solutions that are updated, and incrementally improved (i.e. extended) integrated and federated according to the HLRA

Extendend Components details:

a) technologies for Situational Awareness and Decision Support for Cyber-Physical Threats

b) technologies for information processing and management

c) technologies for Joint Cyber-Physical Security Risk Management and Resilience Modelling

d) technologies for Detection, Identification and Early Warning

Platform as a Service (PaaS)

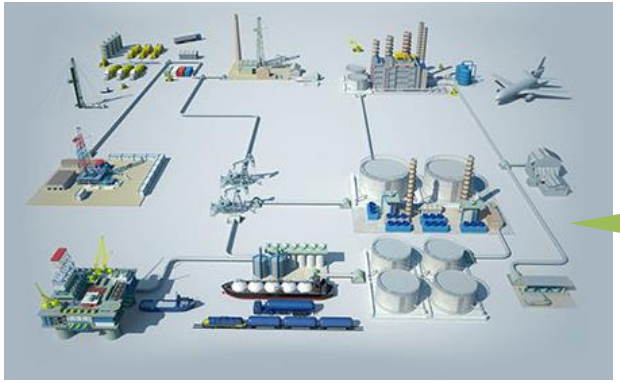
Services provided via a Platform as a Service (PaaS) model featuring modularity, flexibility, cooperation and third-party interoperability.

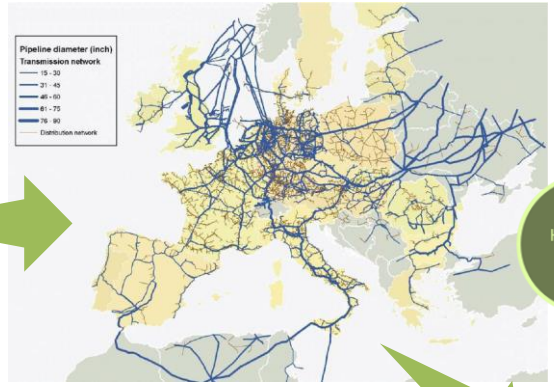
SecureGas extended components

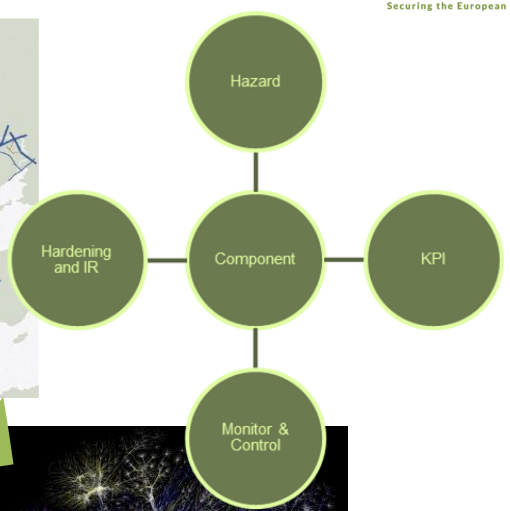
SecureGas Components

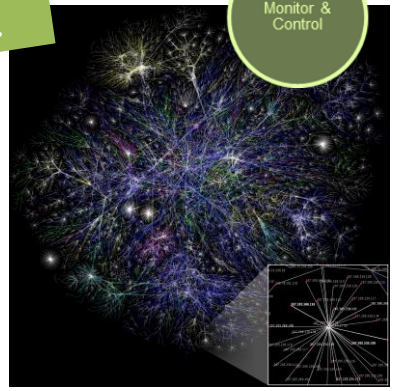
- **Technologies for situational Awareness and Decision Support for Cyber-Physical Threats**
  - Safety and Security platform for Gas CI (LDO)
  - Autonomous docking station and UAV based asset management (ADPM)
  - Onshore Landslide Susceptibility and Alert/ Monitoring System (RINA-C)
- **Technologies for information processing and management**
  - Cyber physical correlator (WINGS, LDO)
  - Blockchain for data transmission and integrity verification (GT, LDO)
  - Cyber Security for IT and OT networks weakness (ELBIT)
  - WINGS Platform (WINGS)
- **Technologies for detection, identification and early warning**
  - Distributed Acoustic Sensing (DAS) for monitoring of leakages and third party intrusion in Oil & Gas pipelines (RINA-C)
  - Cognitive framework for biometrics and video analytics (IDMG, INNOV)
- **Technologies for Joint Cyber-Physical Security Risk Management and Resilience Modelling**
  - Cyber-Physical Security Risk and Resilience Modelling and management (GAP, JRC, EXUS, FHG, RTU)
  - Gas Network Advanced Modelling and Fast-Dynamics Simulation (FHG, JRC)
  - Risk-Aware Information to the population (INNOV, GAP)

Conceptual Model



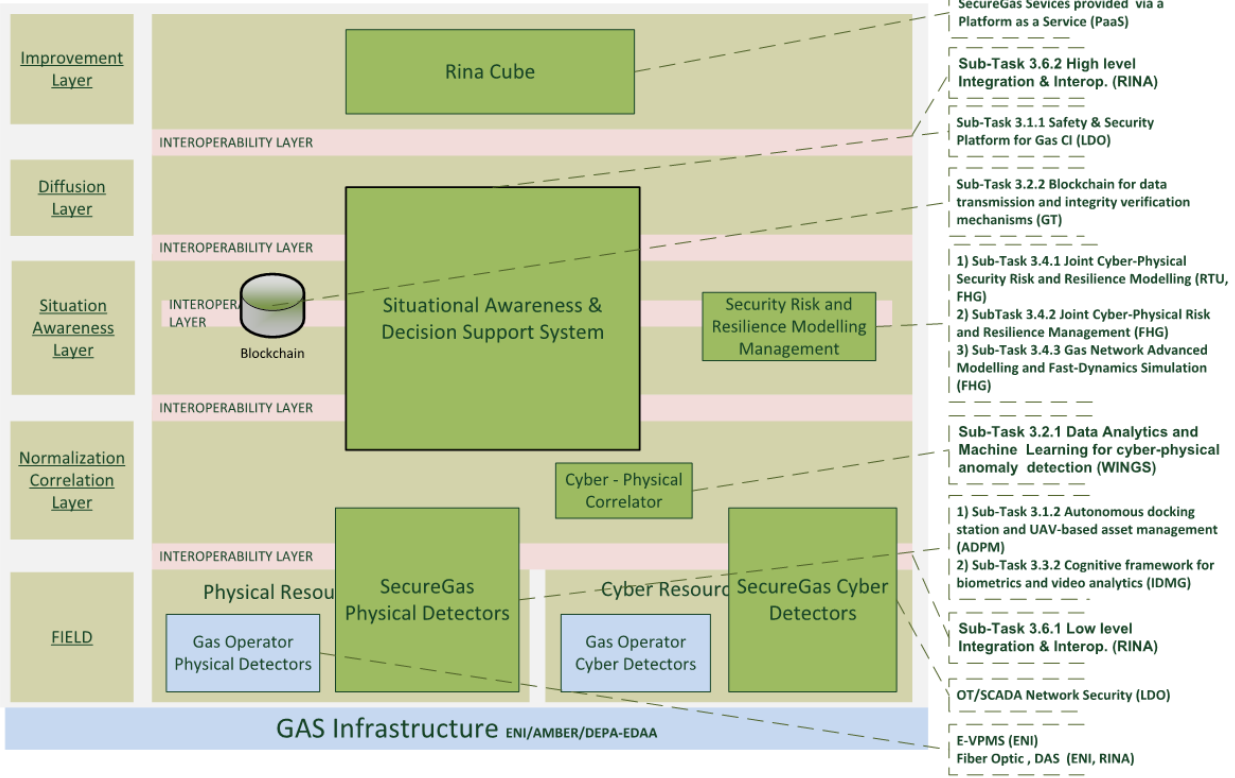






- Gas Infrastructure abstracted as networks where resources flow from one node to the other
- For each node and link main risks assessed and KPIs assigned
- KPIs constantly monitored to determine the global performance of the network and adjust its response on events

High-Level Reference Architecture



A **reference framework** for the implementation, integration and interoperability of SecureGas components

Platform as a Service (PaaS)

- The service is aimed at providing the means for the overall management of Oil&Gas infrastructures.
- It exploits the SecureGas High Level Reference Architecture (HLRA).
- RINA CUBE can encompass the top layer of the HLRA and collect all of its feedback and correlate its different feature and highlight threat patterns.
- This allows End-Users to find causality relationships where there might not be an apparent one and help in the definition and implementation of remedial security and safety measures.
- Furthermore RINA CUBE will facilitate the communication with the authorities and provide the means for the correct management of security and safety related matters both in the planning and the aftermath of an event.

Digital platform of platforms CUBE Digital platform of platforms





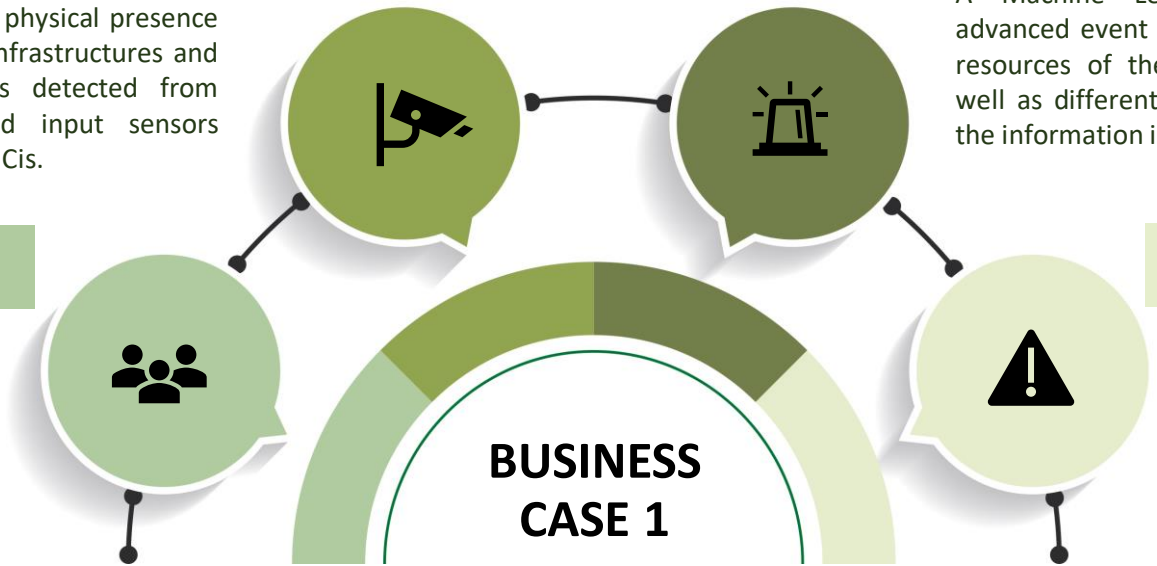
Business Case 1 Components

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.

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.

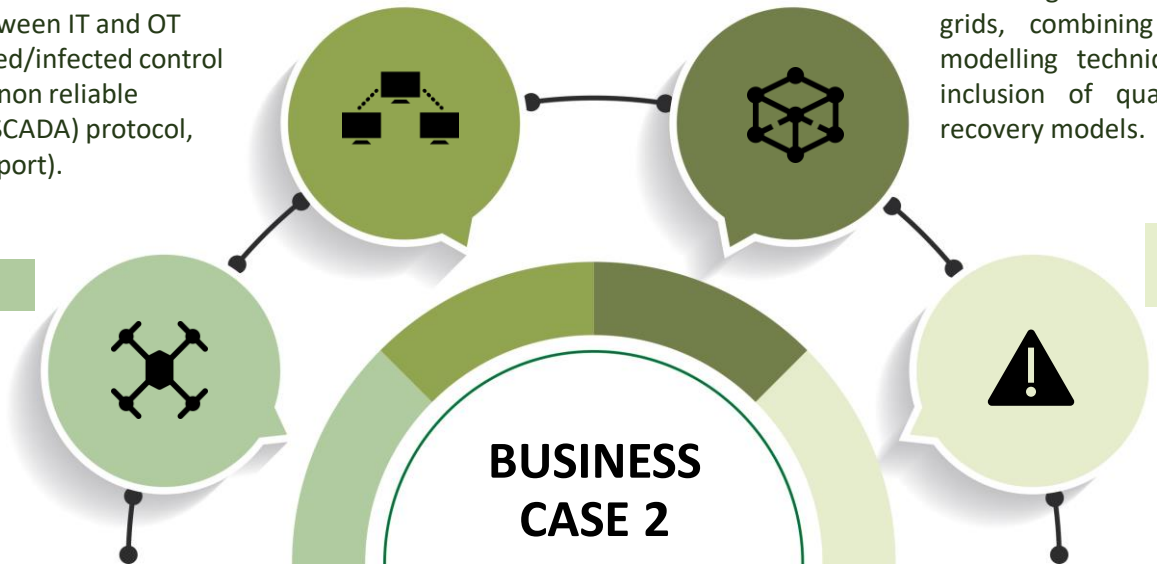
Business Case 2 Components

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 Components

THIRD PARTY INTERFERENCE AND LEAKS DETECTION

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

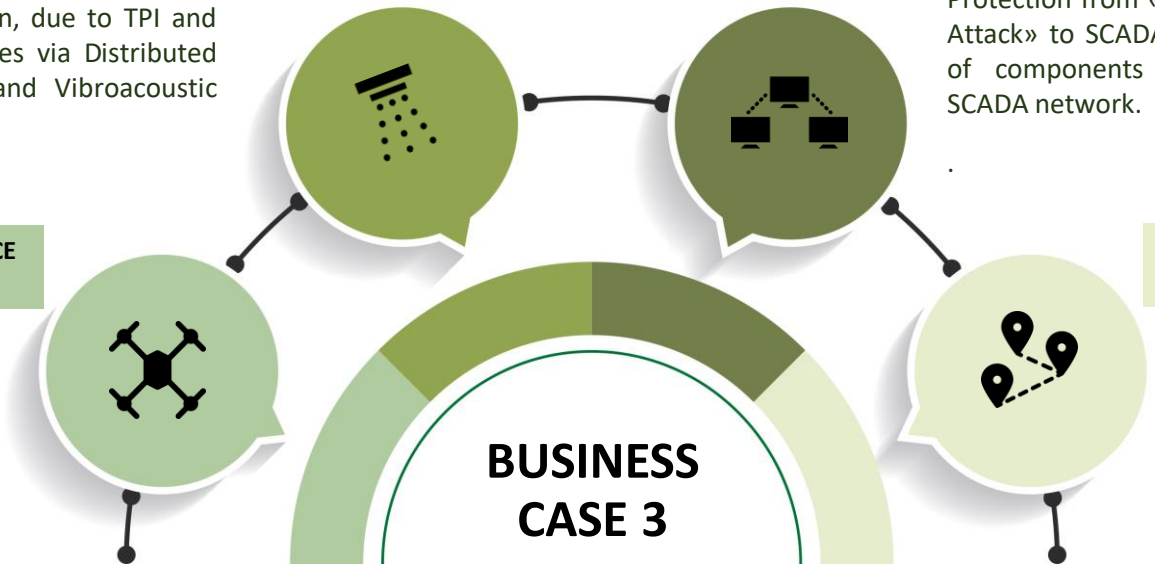
RESILIENCE OF THE OT/IT NETWORK

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.

SecureGas stakeholders

- **GAS CRITICAL INFRASTRUCTURE (CI) OWNERS AND OPERATORS**
  - Transmission System Operators (TSOs)
  - Distributor System Operators (DSOs)
- **ENERGY COMPANIES**
  - Any company in the sector that needs to protect and made resilience its assets (e.g. refineries, platforms) against cyber and physical threats, natural events.
- **ASSOCIATIONS IN THE GAS SECTOR AND BEYOND** (e.g. GIE, ENTSOG, GCG, ReCO system for Gas)
- **PUBLIC AUTHORITIES** (e.g. Ministries of Interior / Infrastructure / Development, Police, FireBrigade, Civil Protection, Energy Regulatory Authorities, etc.)
- **EUROPEAN DIRECTORATE GENERALS** (DG-HOME, DG-ENER, DG-ECHO, DG-CONNECT)

SecureGas opportunities for replication

- **SECUREGAS IS BUSINESS CASE DRIVEN**
  - Business Cases have been designed by the O&G companies in the consortium. This ensures that requirements, specifications, architecture and components are highly applicable and replicable in the O&G sector domain for Security & Resilience purposes.
- SecureGas has been conceived as a modular solution that can fit needs of small and very large (Oil &) Gas operators (from O&G corporations and Energy company, to local distributors) across the whole supply chain (from upstream to downstream).
- All SecureGas components address a wide range of cyber-physical threats.
- A subset of SecureGas components addresses specific issues identified in the 3 business cases and it is validated against SotA solutions and KPIs defined by the Business Cases Owners (e.g. the O&G companies in the consortium).

SecureGas contribution to the policy context

A. SecureGas frames the "**regulatory context**" of Security & Resilience for Gas CI in Deliverable **D1.1 Organisational, Operational and Regulatory requirements**"

B. SecureGas **Business Cases** have been **designed to address** specific issues highlighted in the **EU Regulation 2017/1938 on Security of Gas Supply as well as the EU Directive on Critical Infrastructure Protection** (Council Directive 2008/114/EC of 8 December 2008)

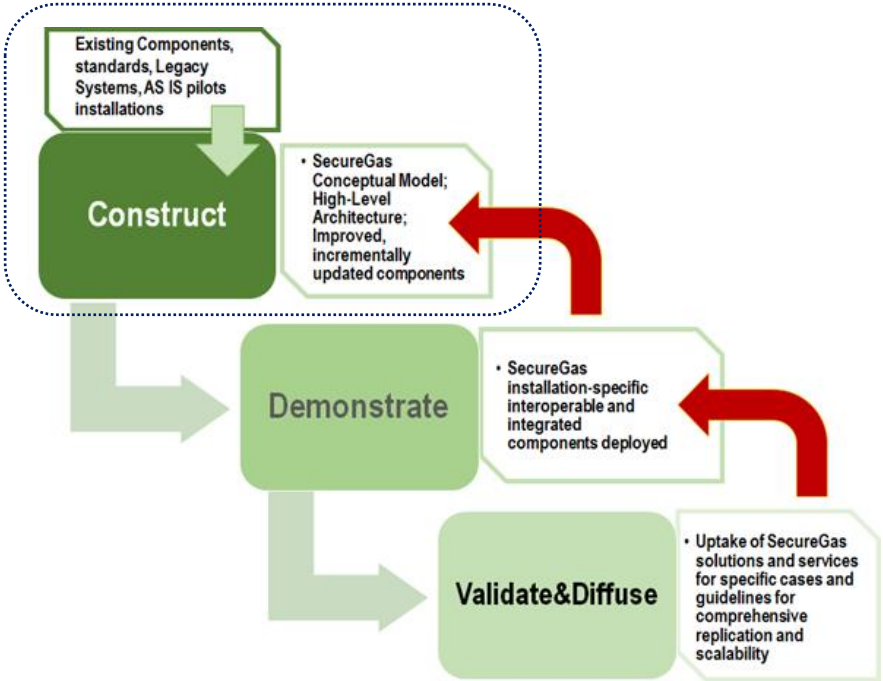
C. SecureGas will deliver a **White paper "Lessons learnt and recommendations for cyber-physical resilience of European Gas Critical Infrastructure"**

D. SecureGas will deliver **guidelines for standards addressing convergence of Safety and Security** approaches as well as improved certification mechanisms surrounding the future standards proposals

Implementation status

User, Operational and Legislative Requirements	D1.1	PU
Technical and Standard related Requirements	D1.2	CO
Risks, Threats and Vulnerabilities	D1.3	EU-RES
KPIs Inventory	D1.4	PU
First Release of the Conceptual Model (CM)	D2.1	PU
A set of Concepts of Operations (CONOPS) for the implementation of the CM	D2.1	PU
First Release of the SecureGas High-Level Reference Architecture	D2.3	PU
Ethical & Legal Monitoring Plan Data Management Plan	D9.1 D9.3	PU
Communication and dissemination strategy	D8.3	PU
A set of scenarios and related uses cases for the 3 Business Cases	D4.1 D5.1 D6.1	EU-RES

Until May (M12), **the project has delivered**:



User and technical requirements

1

Past EC-funded projects
Academic Publications

2

Focus Groups
Semi-structured interviews
Questionnaires

3

Requirements

Operational
- Confidentiality, data protection and safety
- Conditions
- Interoperability
- Detection, situational awareness and decision support
- Usability
- Information management
- Cost

Regulatory
- EU legislation
- National legislation

Organisational
- International Standards
- Management Systems

Technical
- Cross – Requirements
- Component specific

4

External End-Users & Stakeholders Validation Workshop September 2019

Risks, Threats and Vulnerabilities for Gas CI

SecureGas
Securing the European Gas Network

Political
Geo-political
Social
(War/Civil War, Protests , Invasion)

Cyber Threats
(DoS, Physical manipulation, SCADA)

Operational
(Material Failures, Installation, Maintenance)

Explosion
(Man, Vehicle, Kamikazes)

Critical Utilities Failures
(Power, cooling/heating, emergency)

Technical
(Corrosion, Mechanical Impacts, Design/ Planning error)

Chemical / Biological Radiological / Nuclear

Ground Works
(External contractors machinery, excavation, digging)

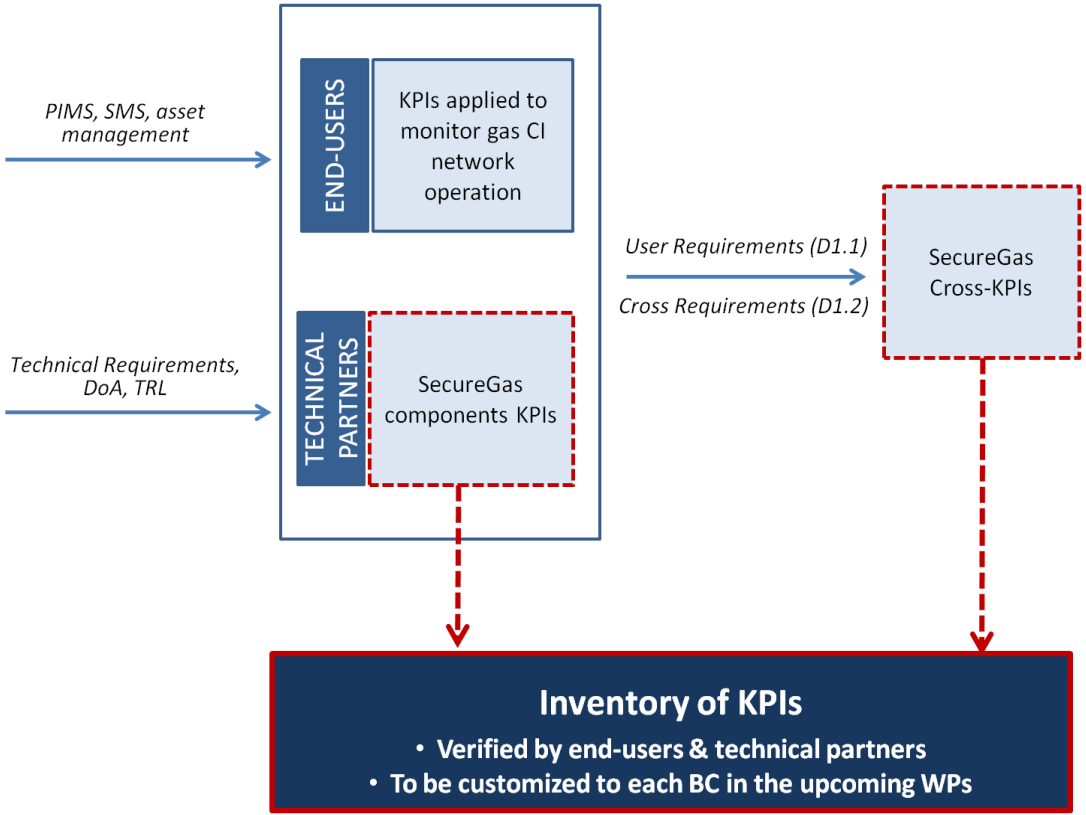
Indirect threats
(Aviation / Maritime / Vehicle / Rail accidents)

Criminal
(Vandalism, Personnel attack, Thefts)

Natural
(Land slide, Fire, Lighting)

Hardware Vulnerabilities
(Equipment failure / Vulnerability / Misuse)

Key Performance Indicators

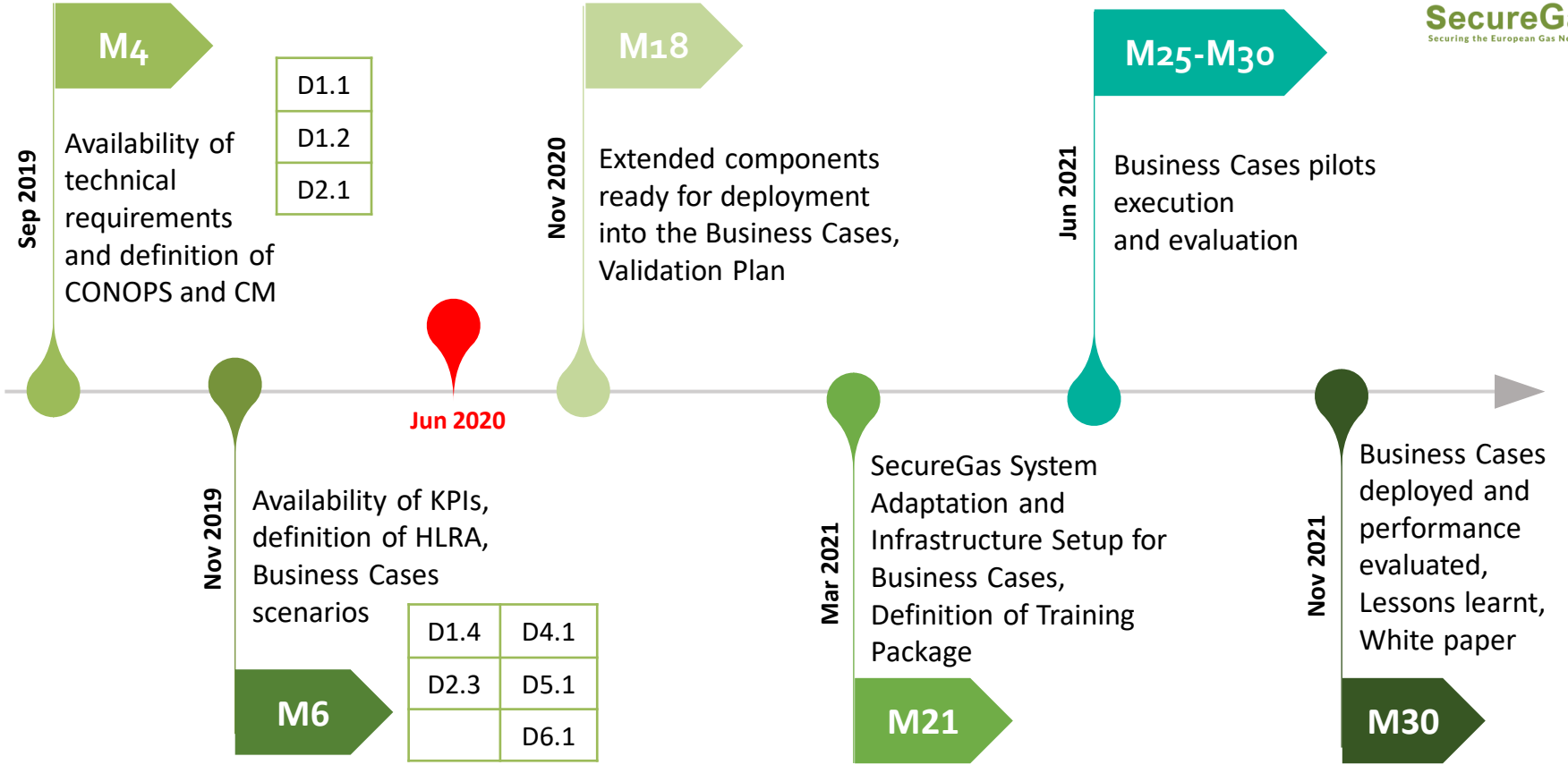


SecureGas Cross-KPIs	
Field	**Indicator**
Reliability	False alert rate
	Cross correlation
	Latency
	Mean time to report
Autonomy	Threat categories addressed
	Automatic detection of threats
	Automatic decision-support
	Alert criticality
Interoperability	Transparent integration of users' legacy systems
Usability	Multilingual Interface
Resilience	Self testing capabilities (system health check)

Scenarios and related uses cases

- Unauthorized physical access
- Intrusion and Manual modification of valves configuration
- (Vehicle) explosive device
- Remote control deployment of valves
- Manual sabotage with cyberattack masking (signal tampering)
- Physical-cyber-physical/ «Man-in-the-Middle» attack to the SCADA system
- Methane leak detection by Unmanned Aerial Vehicle (UAV)
- Third Party Interference enhancement

Implementation status



SecureGas

Securing the European Gas Network

SecureGas Project BC Manager

Ilias Gkotsis (KEMEA)

i.gkotsis@kemea-research.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