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 in numbers

Project Acronym	SecureGas
Project Title:	Securing the European Gas Network
GA number:	833017
H2020 Call	SU-INFRA01-2018 «Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe"
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

Consortium

SecureGas

SECUREGAS COORDINATOR:

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 lightweight efficiency
1862 RĪGAS TEHNISKĀ UNIVERSITĀTE
European Commission
EXUS
Analysis GAP ANALYSIS S.A.
Innov-acts
APRE Agenzia per la Promozione della Ricerca Europea
TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR
διανομή αερίου ΕΤΑΙΡΕΙΑ ΔΙΑΝΟΜΗΣ ΑΕΡΙΟΥ ΑΤΤΙΚΗΣ Α.Ε.
D.M.A.T

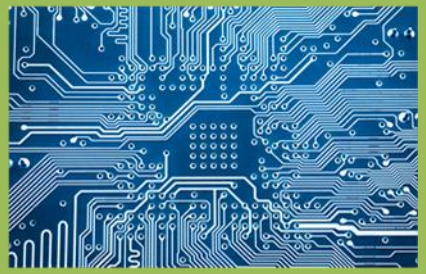
Overall Objective

To increase 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 the combination of them

NATURAL EVENTS

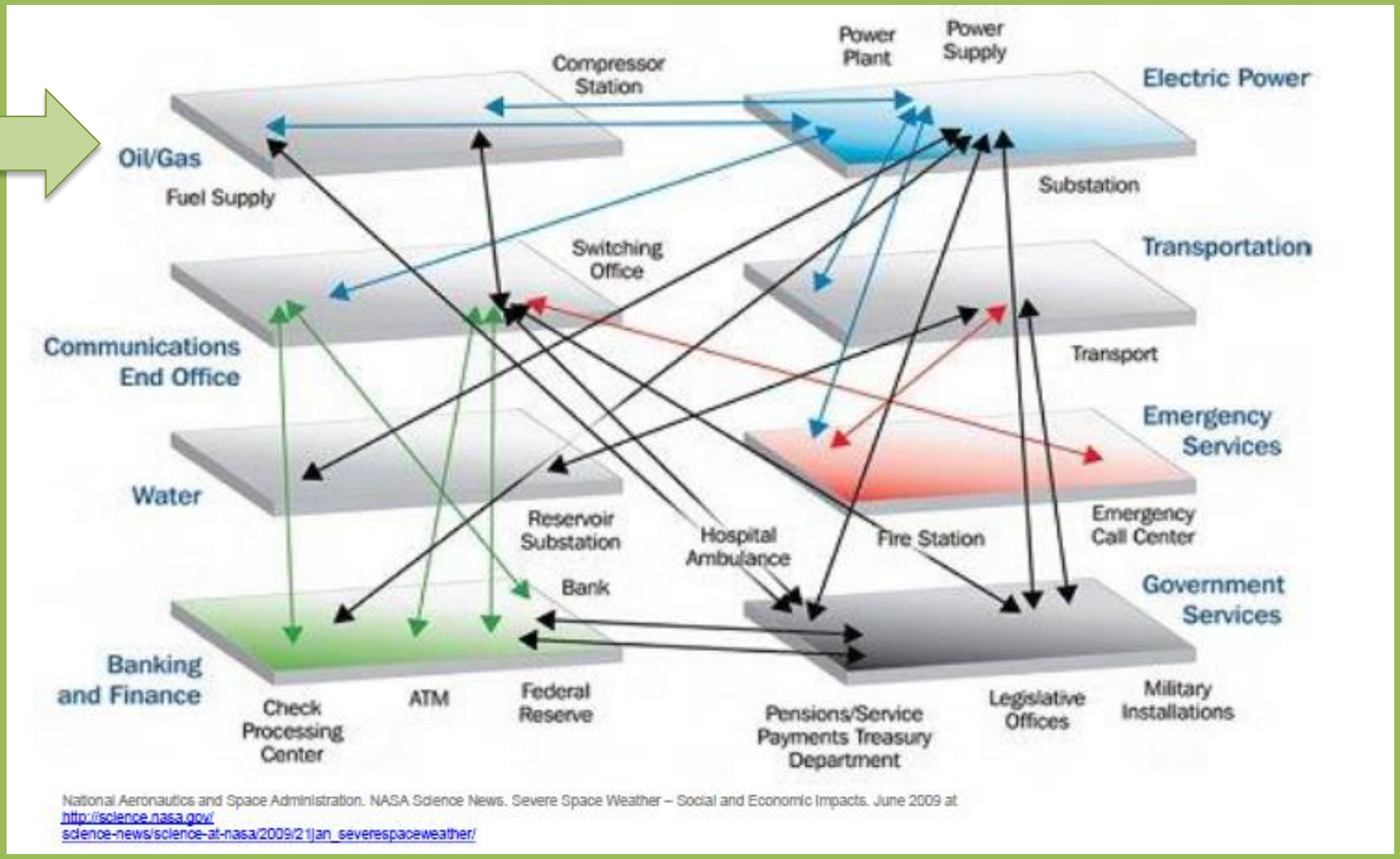
MAN-MADE ACCIDENTS

CYBER ATTACKS



Target - Critical Infrastructure (CI)

SecureGas



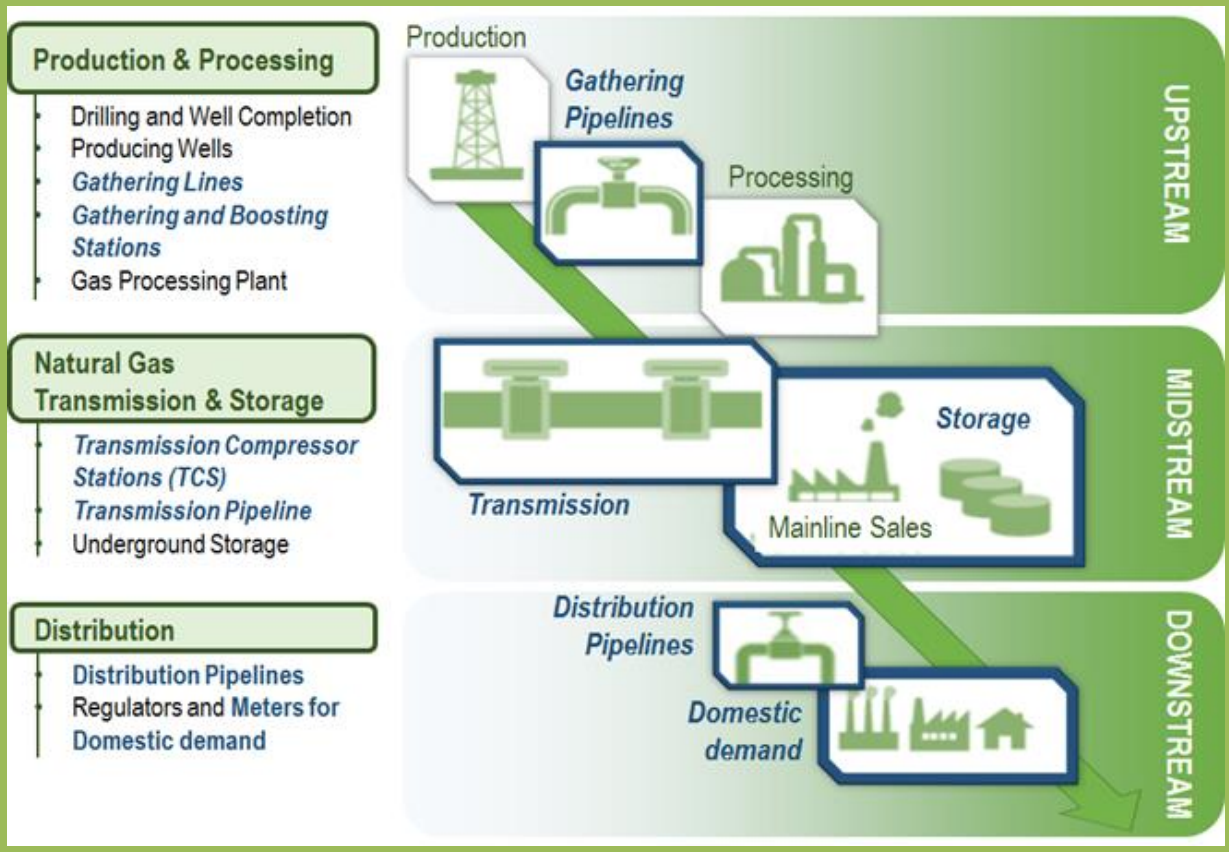
National Aeronautics and Space Administration. NASA Science News. Severe Space Weather – Social and Economic Impacts. June 2009 at http://science.nasa.gov/science-news/science-at-nasa/2009/21jan_severespaceweather/

Focus - EU Gas Network

SecureGas

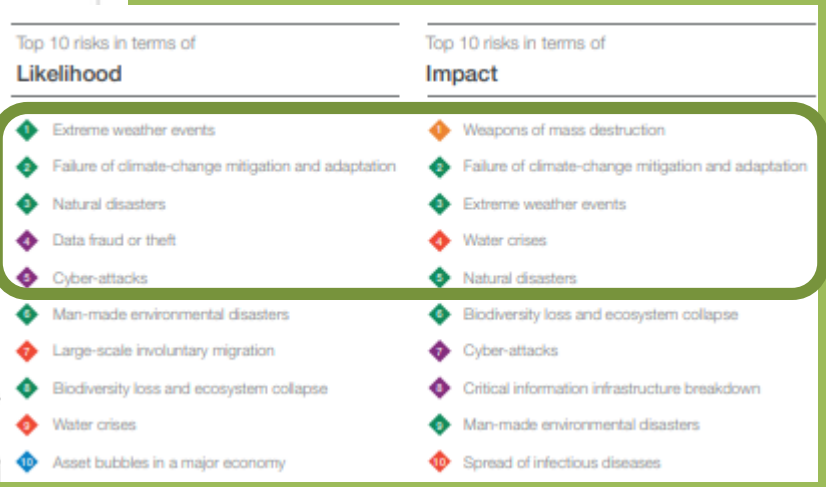
Focus – More in depth

SecureGas focuses on key elements of the +140.000Km of **the European Gas network** covering the **entire value chain** from Production to Transmission up to Distribution



SecureGas FOCUS in BOLD BLUE

Risk Landscape



WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

The Global Risks Report 2019
14th Edition

Physical Incidents

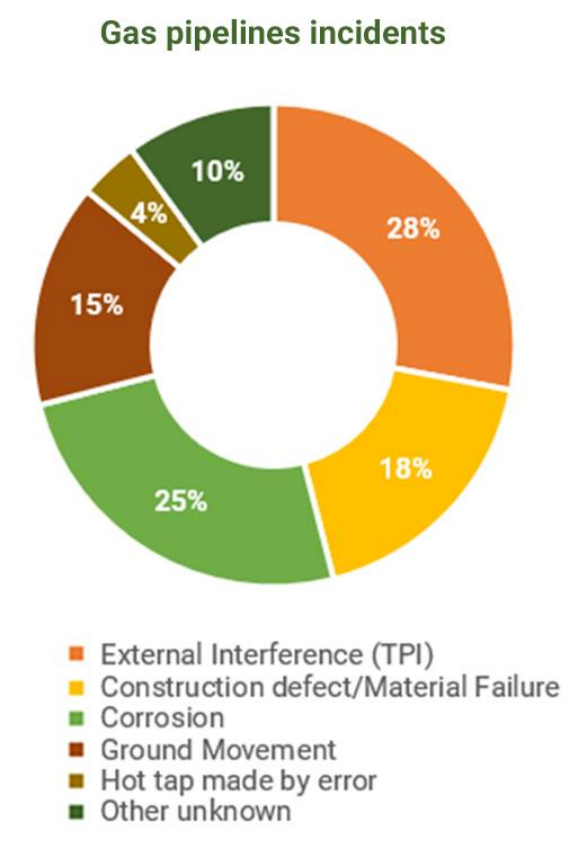
A total of 1366 incidents to gas network reported from **1970-2016**

Main causes:

A. **External interference (TPI)** (e.g. digging, piling or ground works by heavy machinery)

B. **Corrosion**

C. **Ground movement** (e.g. dike break, mining)



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

Cyber Threats

SecureGas

- The **number of incidents** reported so far **is less** if compared to the physical ones
- The **results can be devastating** as well
- Attacks cause **considerable financial damage**


Forbes

Night Dragon Attacks Target Technology in Energy Industry

William Pentland Contributor
Feb 19, 2011, 01:02am • 4,025 views

The Guardian, Published on 26.10.2016,
https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Cascading Events

SecureGas

Gas Networks and infrastructure are highly dependent and interconnected by nature

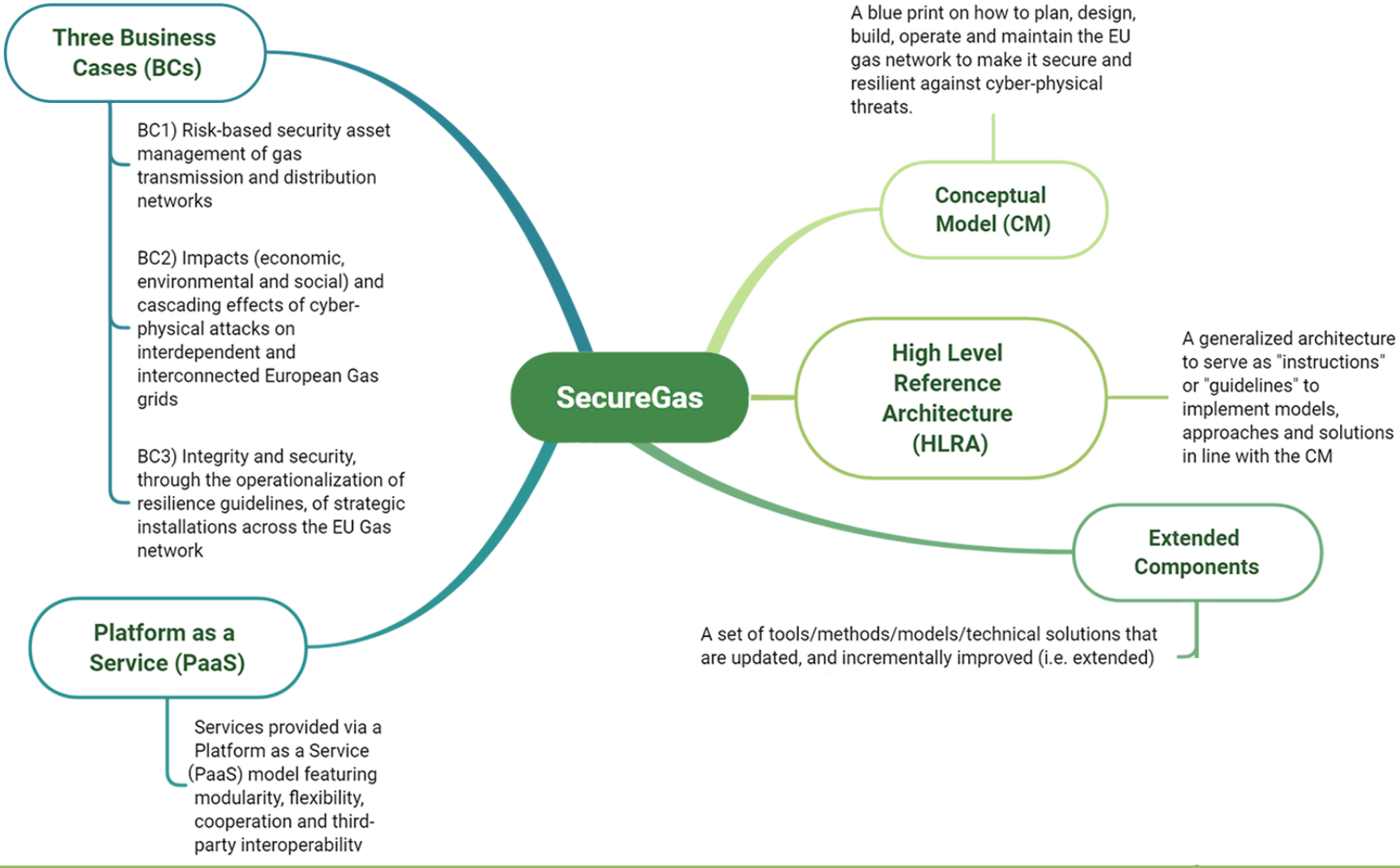
Providing "resilience" means **not only to secure the specific infrastructure in scope** but also **to understand and estimate the potential cascading effects** induced by the loss of functionalities of one infrastructure on the others

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

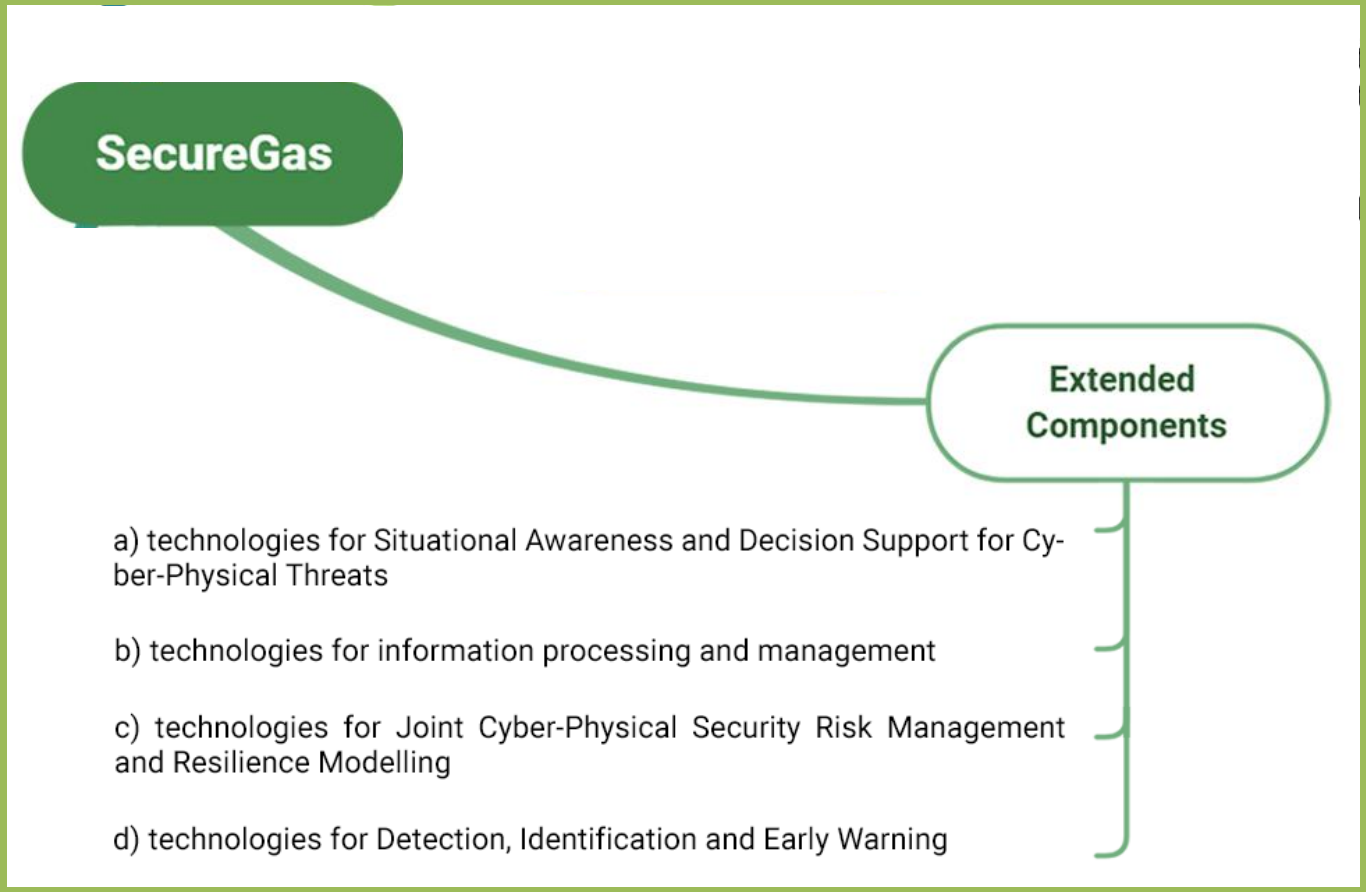
https://www.thelocal.it/20171212/italy-state-of-emergency-austria-explosion-gas

Key Features

SecureGas



Key Features



A value chain approach

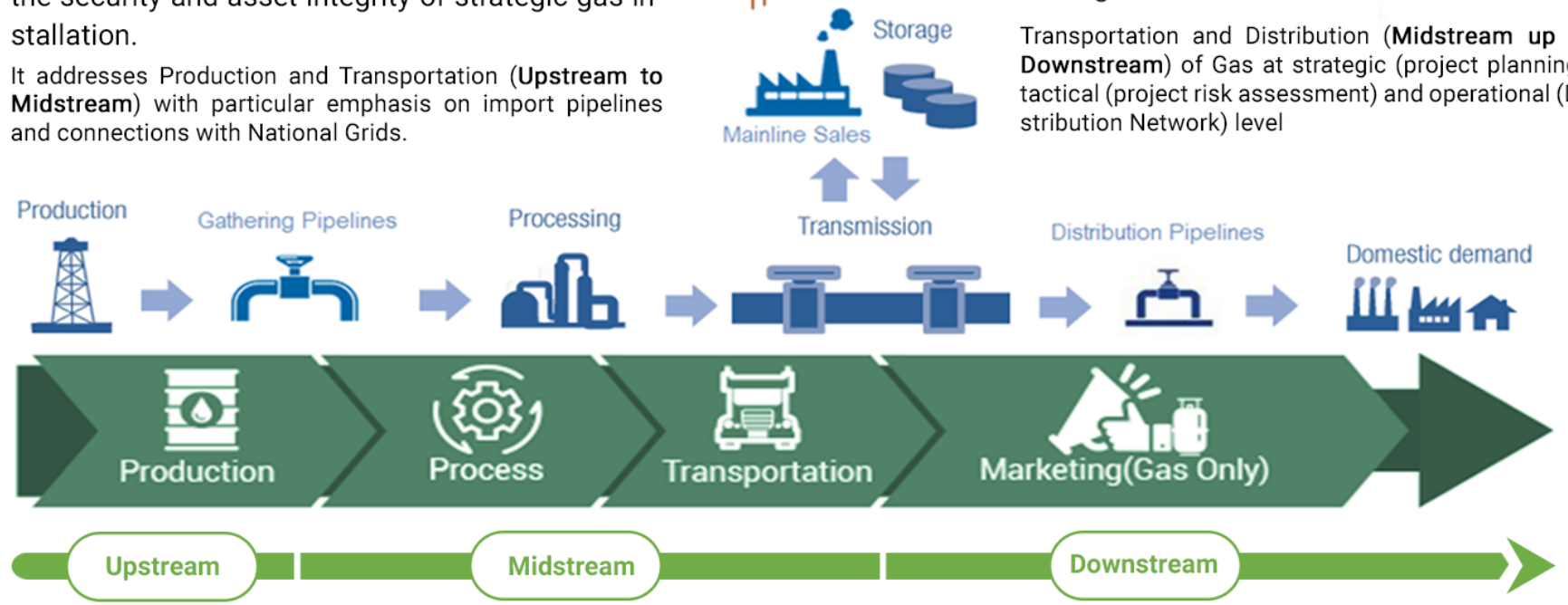
SecureGas

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 Stakeholders

- *Gas Critical Infrastructure (CI) managers and operators (at any point within the supply chain)*
- *Regulatory & Implementing Bodies at National and EU Level*
- *Associations in the Gas Sector and Beyond (e.g. GIE, ENTSOG, etc.)*
- *Technology and Service providers in the field of Security*
- *The wider Scientific Community of Security, Risk and Resilience*

SecureGas

Securing the European Gas Network

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