1. CROSS –REQUIREMENTS

CROSS –REQUIREMENTS	
REQUIREMENT TITLE	CRS_FUN_001, | Legacy and New Technologies
REQUIREMENT DESCRIPTION	SecureGas will integrate the outcomes of cyber and physical protection systems already operating in the gas infrastructure (if any) with new advanced technological solutions for cyber/physical protection and detection
BUSINESS CASE AFFECTED	All
END USER REQUIREMENTS	OP-INTER-01 | Interoperability with existing systems| The SecureGas system should be interoperable with existing monitoring tools and systems of end-users

2. DECISION SUPPORT SYSTEM REQUIREMENTS

DECISION SUPPORT SYSTEM REQUIREMENTS	
REQUIREMENT TITLE	DSS_FUN_005, DSS_FUN_009| Decision support and Workflow Engine, Simulation Capabilities
REQUIREMENT DESCRIPTION	SecureGas supports Users to make proper decisions by using a Workflow Engine that reacts to each detected event by executing the associated automatic or semi-automatic processes, consisting of sequences of actions and reactions. Events can be the simple outcomes of cyber and physical protection systems or inferred events generated by performing (if it is the case) a correlation of apparently harmless events (from both cyber and physical domains). In order to assess the effectiveness of the countermeasures, SecureGas also provides simulation functions: based on both the attack simulations performed and the countermeasures chosen by the operators during the simulation, the system allows the identification of the most suitable countermeasures to intervene on the problem raised (avoiding the worst case in which countermeasures are more harmful than the threat to be countered)
BUSINESS CASE AFFECTED	All, BC-3
END USER REQUIREMENTS	OP-DSD-13 | Decision support | The SecureGas system should provide decision support and recommendation services to end-users targeted to priority security issues.

3. INFORMATION PROCESSING AND MANAGEMENT REQUIREMENTS

INFORMATION PROCESSING AND MANAGEMENT REQUIREMENTS	
REQUIREMENT TITLE	IPM_FUN_001, IPM_FUN_002, IPM_FUN_003, IPM_FUN_004, IPM_FUN_005 | Detection of physical and cyber anomalies, Correlation of cyber-physical data, Prediction of cyber-physical threats
REQUIREMENT DESCRIPTION	SecureGas will process physical parameter data to detect physical anomalies in operation and cyber activity data to detect cyber anomalies in operation. This functionality will be provided using unsupervised learning techniques and dynamically retrained models that will also identify background changes and adapt. Based on the physical and cyber anomalies identified (and potentially confirmation/rejection/alteration by the user), a pattern recognition algorithm will forecast threats that may appear in the future. Furthermore, a Cyber-Physical event correlator (rule and history based correlation) will combine heterogeneous data to detect/predict/ forecast potential cyber-physical threats, i.e. to enable the identification and prediction of threats that are not distinguishable using solely cyber or physical data
BUSINESS CASE AFFECTED	BC-1, BC-3
END USER REQUIREMENTS	OP-CONF-01 | Digitally secure and safe | The SecureGas system should be digitally secure and safe (protected against hackers and malware). OP-DSD-01 | Detection of cyber threats/attacks The SecureGas system should be able to detect cyber threats and attacks to end-users' IT and OT infrastructures.

4. OPERATIONAL NETWORK SECURITY REQUIREMENTS

OPERATIONAL NETWORK SECURITY REQUIREMENTS	
REQUIREMENT TITLE	OTS_FUN_03 | SCADA Network Protection |
REQUIREMENT DESCRIPTION	SecureGas monitors the end-user Operational Technology (OT) network in order to identify suspicious / malicious activity, Identify unauthorized devices and detect unexpected communications and actions. This is done in two steps: in the first step, a learning phase on the OT network (in order to build a baseline of authorized network traffic and mapping of the OT network devices) is performed; in the second step, all discrepancies detected against the authorized traffic are reported as anomalies or potential threats. In this way, the platform mitigates potential vulnerabilities of existing equipment or protocols, detects new/unauthorized devices on the OT network and notifies of suspicious communication between devices on the OT network
BUSINESS CASE AFFECTED	BC-2, BC-3
END USER REQUIREMENTS	OP-DSD-01 | Detection of cyber threats/attacks The SecureGas system should be able to detect cyber threats and attacks to end-users' IT and OT infrastructures.

5. UNMANNED AERIAL VEHICLE (UAV) REQUIREMENTS

UNMANNED AERIAL VEHICLE (UAV) REQUIREMENTS	
REQUIREMENT TITLE	UAV_FUN_06 | Smart Docking/Recharging system |
REQUIREMENT DESCRIPTION	The UAVs should be operated via the HANGAR. The HANGAR is the smart docking station, with enhanced air traffic management based on a distributed architecture and with extensive use of IoT technologies. HANGAR is the key for the diffusion of drones in DAY BY DAY applications (monitoring of large areas, critical infrastructures, pipelines, ...), without pilots or special authorizations. Thanks to the rapid charging system and to the integrated intelligence, HANGAR autonomously manage the entire flight process: weather monitoring, landing and take-off, programmed and ON-DEMAND MISSIONS. The smart docking station is a complex project with distinctive mechanical engineering and robotic solutions, machine to machine communications, autonomous flight, networking and predictive maintenance capabilities. The hardware is designed to be resilient and water-proof, ensuring the operational capability also in hostile environments. The Cloud connection allows remote data access in real time.
BUSINESS CASE AFFECTED	BC-2, BC-3
END USER REQUIREMENTS	OP-USA-05 Accurate Information The Securegas system should provide accurate information to the stakeholder. No more than 5% of total alarms generated should be false OP-DSD-08 Asset manipulation The SecureGas system should detect the illicit manipulation of end-users' assets/equipment (e.g. unauthorized manipulation of valve stations).

6. GEOHAZARDS ASSESSMENT FOR DECISION SUPPORT REQUIREMENTS

GEOHAZARDS ASSESSMENT FOR DECISION SUPPORT REQUIREMENTS	
REQUIREMENT TITLE	GEO_FUN_003| Modeling and results presentation
REQUIREMENT DESCRIPTION	SecureGas will operate a GIS based, near-real time model to assess slope stability and possible slope evolutions, based on three categories of data: • available "geo" related data (e.g. digital terrain model, slope, geology, geotechnics, etc.) along the pipeline route /network (in order to select risky areas) • prediction/real-time measurements of possible triggers for landslides • other monitored data. Results shall be made available to the end user in terms of potentially critical areas along the pipeline
BUSINESS CASE AFFECTED	BC-3
END USER REQUIREMENTS	OP-DSD-02 | Landslide hazard detection | The SecureGas system should detect landslide hazards

7. DETECTION, IDENTIFICATION AND EARLY WARNING REQUIREMENTS

DETECTION, IDENTIFICATION AND EARLY WARNING REQUIREMENTS	
REQUIREMENT TITLE	DET_FUN_003, DET_FUN_004, DET_FUN_007 | Video processing 24/7, Detection of different object types, Detection of unknown persons
REQUIREMENT DESCRIPTION	The video surveillance is aimed to gain high accuracy at both day light and night light conditions. This will be achieved by using infrared cameras. Algorithms based on convolutional neural networks are developed for low light and infrared illuminated conditions. The video analysis platform (MVI) shall detect different objects like face, person, motion, vehicle, vehicle license plates, and luggage. In particular, a functionlity of detection of unknown persons is provided. By using MVI's watchlist capability, known persons are stored in the database. Every person appearing in the video will get compared to the watchlist. Based on thresholds, it is automatically decided if this person was recognized. In case of the appearance of unknown persons, the operator will receive an alarm. The same mechanism can be used to raise an alarm when a person is positively identified, but encountered in an area closed to this person
BUSINESS CASE AFFECTED	BC-1
END USER REQUIREMENTS	OP-DSD-03 | Intrusion detection (including motion detection) | The SecureGas system should detect and identify suspicious persons (intruders) and objects.

8. GAS NETWORK SIMULATION REQUIREMENTS

GAS NETWORK SIMULATION REQUIREMENTS	
REQUIREMENT TITLE	Critical node identification, Fast graph and/or gas simulation
REQUIREMENT DESCRIPTION	Securegas will provide predictive simulation of the impact of attack vectors (a series of attacks that succeed each other) on the gas supply and corresponding optimized response vectors (a series of countermeasures that succeed each other). For the identification of the critical node this includes: 1) Generation of attack vectors 2) Simulation of the impact on the Gas Supply 3) Assessment of the impact using KPIs as metrics 4) Find maximum correlation between KPI drops and nodes involved within the attack vector. After having identified the critical nodes, the response vector will be optimized for the attack on the identified critical node/nodes. Hence the second step includes: 1) Generate response vectors 2) Simulate the impact of them on the Gas Supply 3) Assessment of the impact based on KPIs 4) Find the optimal response vector by comparing their simulated/estimated KPIs. Securegas will leverage the gas grid simulation results for improving prediction capability of graph methods. Implementation of the steady-state flow equation to enable the prediction of pressures and flow rates. The abstraction level thereby will remain at the graph level, however, using flow equation several physical effect can accounted for. E.g.: friction, gravity and inertia force. The simulation will still provide fast results.
BUSINESS CASE AFFECTED	BC-2, BC-3
END USER REQUIREMENTS	OP-DSD-15 | Simulation | The SecureGas System should provide simulation capabilities.

9. CROSS REQUIREMENT – USER INTERFACE

USER INTERFACE REQUIREMENTS	
REQUIREMENT TITLE	CRS_FUN_007 | User friendly GUI
REQUIREMENT DESCRIPTION	SecureGas Cockpit will be based entirely on web technologies and will use panels and cells to allow the display of multiple data on the screens, coming from different sources. The Operator layout can be visualized on one or more monitors. SecureGas Cockpit will give a high level of Situation Awareness through displaying a CROP (Common Relevant Operational Picture), which allows having in context all the necessary and sufficient information to understand what is happening and where. Three main features are envisaged: • Events Managements that will interoperate with field subsystem to receive events (either “informative” or “critical”) • Map Viewer that will display the geographical map on which are geo-referenced the systems, the assets, the devices, the events and the alarms handled by the platform in order to obtain a so-called CROP (Common Relevant Operational Picture). • Situation Viewer that will allow to handle live videos coming from cameras. (It is possible to operate on cameras with PTZ control, If allowed by the specific device). Situation Viewer also will allow to customize the monitor layout according to the user's preferences and to save this configuration so to use it at next access. It will be also possible to select the language to be used.
BUSINESS CASE AFFECTED	All
END USER REQUIREMENTS	OP-USA-01| User friendly | The SecureGas system should have a user friendly interface.

10. RESILIENCE AND RISK MODELING & MANAGEMENT REQUIREMENTS

RESILIENCE AND RISK MODELING & MANAGEMENT REQUIREMENTS	
REQUIREMENT TITLE	RMG-FUN-01 | Risk Management
REQUIREMENT DESCRIPTION	SecureGas will provide information to the operator on the risk level of the various physical and cyber threats that could affect the integrity of the Gas CI network. For the definition of the risk level of each threat, the following risk management procedures will be supported and deployed by SecureGas, namely: • Identifications of Gas CI assets • Definition of interdependencies among assets, systems, supply chain etc • Identification of threats per CI asset • Definition of security breach scenarios • Risk Analysis (qualitative or quantitative) - Threat, vulnerability and impact (including cascade effects) assessment • Risk evaluation based on predefined Risk Assessment Matrix (RAM) and risk acceptance criteria Risk reduction and resilience improvement will be addressed through recommendations on technical, organizational and managerial countermeasures. Risk reassessment is necessary per security scenario
BUSINESS CASE AFFECTED	BC1/All
END USER REQUIREMENTS	OP-DSD-12 | Risk level of events | The SecureGas system should provide information on the risk level of the various physical and cyber threats targeting end-users' network OP-DSD-13 | Decision support | The SecureGas system should provide decision support and recommendation services to end-users targeted to priority security issues

11. BLOCKCHAIN APPLICATION REQUIREMENTS

BLOCKCHAIN APPLICATION REQUIREMENTS	
REQUIREMENT TITLE	BCH_OPR_001 | Decision support BCH_OPR_002 | Data exchange BCH_OPR_003 | Cyber threat
REQUIREMENT DESCRIPTION	The gateway layer from KSI Blockchain Infrastructure must be hosted on-premise with Internet access to enable access to KSI Blockchain functionalities for data exchange. This is then used to ensure data integrity for long term data. Additionally, data integrity can also be verified offline and independently from blockchain provider. This allows to detect insider attacks and accidental modifications while being compatible with any file system and data format.
BUSINESS CASE AFFECTED	BC2/All
END USER REQUIREMENTS	OP-COND-02 Various kinds of threats |The SecureGas system should be versatile and adaptable to various kinds of threats (e.g. third party interference, explosion, fire, extreme weather, etc.). OP-INTER-01 Interoperability with existing systems | The SecureGas system should be interoperable with existing monitoring tools and systems of end-users.

12. IMPLEMENTATION OF STANDARD COMPONENTS REQUIREMENTS

<table>
<tr><th colspan="2">IMPLEMENTATION OF STANDARD COMPONENTS REQUIREMENTS</th></tr>
<tr><td>REQUIREMENT TITLE</td><td>IMP_OPR_003 | Plant Operations</td></tr>
<tr><td>REQUIREMENT DESCRIPTION</td><td>Decisions and actions shall be digitally logged on tamper proof ledger or database</td></tr>
<tr><td>BUSINESS CASE AFFECTED</td><td>All</td></tr>
<tr><td>END USER REQUIREMENTS</td><td>OP-INFOR-06 | Event register |
The SecureGas system shall allow the setup of an event register that will record and trace all SecureGas related actions that are carried out during the crisis.</td></tr>
</table>

13. RISK AWARE INFORMATION TO THE POPULATION REQUIREMENTS

RISK AWARE INFORMATION TO THE POPULATION REQUIREMENTS	
REQUIREMENT TITLE	RAW_FUN_001, RAW_FUN_002, RAW_FUN_003, RAW_FUN_004 | Connectivity with Public Warning Services (PWS), Current status information reporting, Forecasted (model-based) information reporting, Audio/Text Directions
REQUIREMENT DESCRIPTION	SecureGas will provide the functionality to connect to Public Warning Services (PWS – e.g. civil protection) managed by the competent public authorities in order to report incidents / events for the protection of the population. Two kind of information are envisaged: • Details of the reported incident/event, which should contain information such as: ○ date and time of the event; ○ type of event; ○ identifier of the user or the identifier of the process that triggered the event; ○ geo-location information (if available); ○ description • the forecasted spread of the incident and the area, population affected (if available) Furthermore, both audio and text notifications to operational authorities can be provided.
BUSINESS CASE AFFECTED	All
END USER REQUIREMENTS	OP-DSD-14 | Share information with the public | The SecureGas system should allow for sharing information with the public (predefined target groups) before, during and after a security incident.