SecureGas
Securing the European Gas Network

Securing The European Gas Network

H2020-SU-INFRA-2018
SU-INFRA01-2018-2019-2020
Grant Agreement No. 833017

SecureGas: D1.1 Organisational, Operational and Regulatory Requirements

Secureas_D1.1_FINAL

This is only the executive summary.
The full deliverable will be available once approved by the EC/REA

This project has receveid funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833017

SecureGas
D1.1 – ORGANIZATIONAL, OPERATIONAL AND REGULATORY REQUIREMENTS

Project Title:	Securing The European Gas Network
Project Acronym:	SecureGas
Contract Number:	833017
Project Coordinator:	Rina Consulting S.p.A.
WP Leader:	FHG

Document ID N°:	SecureGas_D1.1_FINAL	**Version:**	FINAL
Deliverable:	D1.1	**Date:**	31/08/2019
		Status:	Approved

Document classification	PU Public

Approval Status	
Prepared by:	ENI
Approved by: **(WP Leader)**	FHG
Approved by: **(Coordinator)**	RINA-C
Security Approval **(Security Advisory Board Leader)**	RINA-C

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Clemente Fuggini	RINA-C	Project Coordinator, Final Review
Ivo Häring	FHG	WP1 Lead
Giuseppe Giunta	ENI	Task 1.1 Lead, Deliverable Lead, Editor
Evita Agrafioti	GAP	Co-editor
George Papadakis	GAP	Contributor
Anastasia Chalkidou	GAP	Contributor
Dimitris Charalampakis	GAP	Contributor
Keld Lund Nielsen	ENI	Contributor
Dimitris Gritzalis	DEPA	Contributor
George Stergiopoulos	DEPA	Contributor
Panagiotis Dedousis	DEPA	Contributor
Stella Tsiouma	DEPA	Contributor
Vassilios Vassiliou	EDAA	Contributor
Eugenia Koutiva	EDAA	Contributor
Algirdas Dominus	AMBER	Contributor
Monika Hirschmugl-Fuchs	DMAT	Contributor
Vit Stritecky	TPEB	Contributor
Martin Hromada	TPEB	Contributor

REVISION TABLE

Version	Date	Comments
1.0	10/07/2019	Draft report definition by FHG
2.0	29/07/2019	Draft version, Introduction, Objectives and Scope by ENI
3.1	30/07/2019	Draft version including a detailed ToC

3.2	08/08/2019	Partners contributions TPEB, DMAT
3.3	20/08/2019	All partners feedback consolidated
3.4	21/08/2019	Final draft by GAP
3.5	22/08/2019	Contribution update by DMAT
4.0	23/08/2019	Reviews and final inputs by FHG and ENI
5.0	27/08/2019	Final review by RINA-C
6.0	28/08/2019	Additional inputs by contributors
FINAL	29/08/2019	Final Version

Disclaimer
The work described in this document has been conducted within the SecureGas project.
The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

SecureGas – PUBLISHABLE EXTENDED ABSTRACT

SecureGas focuses on the 140.000Km of the European Gas network covering the entire value chain from Production to Distribution to the users, providing methodologies, tools and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats. Three business cases, addressing relevant issues for the Gas sector and beyond (e.g. oil), have been identified so that to ensure the delivery of solutions and services in line with clear needs and requirements, focused on: risk-based security asset management of gas transmission and distribution networks; impacts (economic, environmental and social) and cascading effects of cyber-physical attacks on interdependent and interconnected European Gas grids; integrity and security, through the operationalization of resilience guidelines, of strategic installations across the EU Gas network.
SecureGas tackles these issues by implementing, updating, and incrementally improving extended components, integrated and federated according to a High-Level Reference Architecture built upon the SecureGas Conceptual Model, a blue print on how to design, build, operate and maintain the EU gas network to make it secure and resilient against cyber-physical threats. The components are contextualized, customized, deployed, demonstrated and validated in each business case, according to the scenarios defined by the end-users. Related services provided by SecureGas will be offered to the end-users via a Platform as a Service (PaaS) that allows modularity, flexibility, cooperation and third-party interoperability, thus securing a long-lasting impact, supporting the project exploitation strategy. A multidisciplinary consortium (Gas operators, technology providers, research institutions, sector-related associations), supports the project implementation across Construction, Demonstration and Validation phases, as well as a Stakeholder Platform ensures inputs, advise, and a wider Diffusion of the project outcomes.

The present report focuses on the identification of gas Critical Infrastructure (CI) operators/managers requirements as identified by the End-Users in the consortium, namely ENI, AMBER, DEPA, EDAA. The report shows how the requirements were collected, systematically presented as well as which main observations can be drawn based on the final user requirements. The report also draws on end-user requirements of similar critical infrastructure projects and published literature.
The report structures end-user requirements with respect to organizational, operational and regulatory requirements using a rich tabular structure (see Annex A for the complete list). The involvement of the operators is documented (see Annex B for more details). Finally, it is shown how the user requirements will be further used throughout the project to show the high relevancy of the take-up of the end user expectations.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

GCG	Gas Coordination Group
CI	Critical Infrastructure
CM	Conceptual Model
CONOPs	Concept of Operations
DoA	Description of Action
ECI	European Critical Infrastructures
ENTSOG	European Network of Transmission System Operators for Gas
KPIs	Key Performance Indicators
MFA	Multi-Factor-Authorization
OSP	Operator Security Plan
PIMS	Pipeline Integrity Management System
SMS	Safety Management System
SeMS	Security Management System
SLO	Security Liaison Officers
TPI	Third Party Interference
WP	Work Package

EXECUTIVE SUMMARY

The present deliverable D1.1 is the first deliverable of WP1 "SecureGas requirements, risks and threats identification" and the main outcome of T1.1 "Organizational, Operational and Regulatory Requirements". Deliverable D1.1 targets the definition of the SecureGas end-user requirements, highlighting end-users needs with regard to Gas Critical Infrastructure (CI) security and emphasizing on their demands and expectations regarding integrated security solutions, such as the SecureGas system. The ultimate goal of deliverable D1.1 is to capture and elaborate all the desired features and characteristics of the SecureGas system from the End-Users' perspectives.

In sight of defining the SecureGas end-user requirements, the first step of the adopted methodological approach included a thorough literature review on recent academic publications and EU co-funded R&D projects. The review focused on the European and national regulatory framework around Gas CI security and operation, the security-oriented organizational practices and procedures, the attributes, capabilities and characteristics the technical solutions should have so as, when deployed, to foster the security and resilience of Gas CI networks. The literature review enabled the identification of current and emerging needs and practices regarding Gas CI security aspects.

Upon the delineation of the current status around regulatory, organizational and operational aspects of Gas CI security, the next step included a series of consultation remote and physical meetings with the SecureGas End-Users, namely ENI, AMBER, DEPA, EDAA, for collecting their specific expectations and needs (Details available in ANNEX B). A Requirement Collection Questionnaire, which drew on the literature survey findings and on the information available in the Description of Action (DoA), served as guidance and facilitation document during the requirements consultation phase.

Based on the end-users inputs, the information available in the DoA and the literature survey outcomes, a set of 76 SecureGas end-user requirements was extracted (Complete list and details available in ANNEX A). Those requirements were classified into 3 types, namely regulatory, organizational and operational, and subsequently further grouped into various categories. The operators also reviewed and provided input to the end-users requirements as documented in a rich matrix structure. A priority level, i.e. high, medium or low, was assigned to each requirement, which is indicative of how instrumental the requirement is in order to support and achieve the core values of the SecureGas solution.

An extended user community, the SecureGas Stakeholder Platform (SP), will validate the SecureGas end-user requirements defined in the current deliverable, during a dedicated workshop planned for M4 (organized in WP8), so as to ensure that the requirements do reflect the needs and industrial policies of an Europe-wide target group.

Within the upcoming project tasks, the SecureGas end-user requirements will be addressed by the process of technological development, serving thus as the baseline for the design, development and realization of the SecureGas solution. Towards that direction, user requirements will be correlated to technical specifications, allowing for the development of a traceability matrix that will monitor the level of requirements fulfillment. The end-user requirements will serve as an input for the development of Key Performance Indicators (KPIs). End-user requirements either address the need to control the risk and improve resilience with respect to potential threats or need to be fulfilled even in the advent of potential risk events. Additionally, the SecureGas user requirements will constitute the baseline for developing the SecureGas Conceptual Model (CM) and Concept of Operations (CONOPS), the reference high-level architecture as well as for defining the business case scenarios that will validate the SecureGas solution.