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: D2.1_SecureGas Conceptual Model and CONOPS – intermediate version

ID: SecureGas_D2.1_FINAL

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

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

SecureGas
D2.1 – SECUREGAS CONCEPTUAL MODEL AND CONOPS – INTERMEDIATE VERSION

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

Document ID N°:	SecureGas_FINAL	**Version:**	Final
Deliverable:	D2.1	**Date:**	30/09/2019
		Status:	Approved

Document classification	PU Public

Approval Status	
Prepared by:	FHG
Approved by: (WP Leader)	RINA-C
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, Preliminary and Final Review
Martina Miro Andrea Basso Fabio Bolletta	RINA-C	WP2 Leader - Main contributions • Technical contributions regarding component definitions • Abstraction of the gas infrastructure system and component identification • Critical component identification
Ivo Häring Sebastian Ganter Jörg Finger	FHG	Deliverable Lead - Main contributions: • Deliverable draft structure • CM and CONOPS working definitions • Relation of D2.1 to other WPs • Introduction and conclusion chapters • Literature research • Dimensional CM and CONOPS approach ideas • Approaches to determine CONOPS
Ilias Gkotsis Anna Gazi Vanessa Papakosta	KEMEA	Main contributions: • Literature survey and definition of CONOPS
Keld Lund Nielson Giuseppe Gunta	ENI	Main contributions: • Coverage of security issues: monitoring technologies and related cyber tools • Industry experience on CONOPS
Algirdas Dominas Lina Rudzianskiene	AMBER	Main contributions: • Contributions on operation and maintenance • Input to templates for CM elements • Example issues and solutions
Aspa Skalidi	WINGS	Main contributions: IT Security threat coverage
Vytis Kopustinskas	JRC	Main contributions Risk assessment and simulation and related dimensions and metrics
Evita Agrafioti Dimitris Charalampakis	GAP	Main contributions: • Definition of requirement of a security management system (loop of activities that should be covered) • Inputs from related assessment processes (e.g. risk management, environmental compliance, etc.) • Completeness in terms of coverage of threats

REVISION TABLE

Version	Date	Comments
1.0	29/07/2019	Table of Content (ToC) of D2.1 by APRE
2.0	06/08/2019	First Draft Version by FHG
3.0	22/08/2019	Inputs from GAP, WINGS
4.0	30/08/2019	Inputs from AMBER, ENI, JRC, RINA-C
5.0	02/09/2019	Updated version by FHG
6.0	06/09/2019	Inputs from KEMEA
7.0	16/09/2019	Additional Inputs received
8.0	19/09/2019	First finalized draft circulated
9.0	20/09/2019	All inputs finalized. Draft ready for review
10.0	25/09/2019	Preliminary Review by RINA-C
11.0	27/09/2019	Final Draft Version by FHG
12.0	30/09/2019	Final review by RINA-C
FINAL	01/09/2019	Final Version

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 application 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 networks; 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 an 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

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

BC	Business Case
BOG	Boil-Off Gas
CBA	Cost-Benefit Analysis
CEP	Complex Event Processing
CI	Critical Infrastructure
CM	Conceptual Model
CONOPS	Concept of Operations
CROP	Common Relevant Operational Picture
DIAL	Differential Absorption Lidar
DRM	Disaster Risk Management
EGIG	European Gas pipeline Incident data Group
GIS	Geographic Information System
HLRA	High Level Reference Architecture
HMI	Human Machine Interface
HP	High Pressure
HS	Human Safety
ICT	Information Communication Technologies
IR	Infra-Red
IT	Information Technology
KO	Knock-Out (in context of KO drum)
KSI	Keyless Signature Infrastructure
LC	Life-Cycle
LDC	Local Distributer company
LIDAR	Light Detection and Ranging
LOC	Loss of Control
LP	Low Pressure
ML	Machine Learning
NG	Natural Gas
NGL	Natural Gas Liquide
RA	Risk Assessment
SAR	Satellite surveillance
SCADA	Supervisory Control and Data Acquisition
SeMS	Security Management System
S&S	Security & Safety
SSM	Soft Systems Methodology
TAP	Trans Adriatic Pipeline
TPI	Third Party Interference
UAV	Unmanned aerial vehicle
UMTs	Universal Mobile Telecommunication System
WP	Work Package

EXECUTIVE SUMMARY

The present document, Deliverable D2.1, is the interim version of the SecureGas Conceptual Model and CONOPS (Concept of Operations), delivered at Month 4 (M4) of the project

It represents the first and intermediate outcome of the work carried out in Task 2.1 "SecureGas Conceptual Model and Concept of Operations", started at Month 2 (M2) of the project, ending at Month 4 (M4) with the present document.

More in depth, this report provides a generic conceptual system modelling approach for the gas supply system and its technical security solutions (Conceptual Model, CM). It is also shown how the defined dimensional system analysis can be used to define concepts of operations of technical security solutions (CONOPS) in a concise way. This will support to ensure that the operator expectations regarding the technical security solutions can be better formulated for the application cases to be later designed and developed in the project.

D2.1 will also contribute to a more concise system specification, development, verification and validation in WorkPackage 2 "SecureGas Conceptual Model and High-Level Reference Architecture" and WorkPackage 3 "SecureGas extended components", that is about technical components. To this end working definitions are provided as well as abstract examples for CONOPS of the three business application cases of SecureGas. This showed that a level of CM and CONOPS modelling and development has been found that is appropriate for SecurGas regarding effort and resolution as well as understandability of CONOPS by operators and technology providers.

Finally, the report also shows how the intermediate CM and CONOPS will be used within WP2 for the development of the High Level Reference Architecture (HLRA) of the technical security system solutions, its interfaces and components.

D2.1 will be updated in a final version, constituting the Deliverable D2.2, at Month 21 (M21) of the project.

Both deliverables, D2.1 and D2.2 are of public nature. Therefore, it is worth nothing, that only publicly available information or information that can be shared with the public have been reported in D2.1. No sensitive or EU Classified information are contained.