

SecureGas: D2.3_SecureGas HLRA– intermediate version

ID: SecureGas_WP2_Deliverable_D2.3_FINAL

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



SecureGas

D2.3 – SECUREGAS HIGH LEVEL REFERENCE ARCHITECTURE – 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_WP2_Deliverable_D2.3_FINAL	Version:	FINAL
Deliverable:	D2.3_SecureGas HLRA– intermediate version	Date:	20/11/2019
		Status:	Approved

Document classification	PU Public
--------------------------------	-----------

Approval Status	
Prepared by:	RINA-C
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
Andrea Basso Martina Miro	RINA-C	WP2 Leader, Task 2.2 Leader and Main Editor of Deliverable D2.3 Main contributions included: <ul style="list-style-type: none"> • Technical contributions regarding component definitions • Abstraction of the gas infrastructure system and component identification • Critical component identification • Definition of the HLRA structure
Omar Zanoli Giuseppe Cevasco Aldo Gallerini Giorgio Gentile Paolo Corvaglia	RINA-C	Contribution on the descriptions of specific components and their interaction in the HLRA
Rosanna Crimaldi Federico Scottoni Paolo Bonanno Giovanni Basile	LDO	Jointly definition with RINA-C of the High-Level Reference Architecture structure. Contribution on the description of specific components and their interactions.
Dimitris Drakoulis Anastasia Eleftheriou	INNOV	Contribution on the descriptions of specific components and their interaction in the HLRA
Evita Agrafioti Anastasia Chalkidou George Papadakis	GAP	Contribution on the descriptions of specific components and their interaction in the HLRA
Dimitris Petrantonakis	EXUS	Contribution on the descriptions of specific components and their interaction in the HLRA
Vytis Kopustinskaskas	JRC	Contribution on the descriptions of specific components and their interaction in the HLRA
Sebastian Ganter Kushal Srivastava	FHG	Contribution on the descriptions of specific components and their interaction in the HLRA
Ilias Gkotsis	KEMEA	Contribution on the descriptions of specific components and their interaction in the HLRA
Luca Brizzi	ADPM	Contribution on the descriptions of specific components and their interaction in the HLRA
Priit Anton	GT	Contribution on the descriptions of specific components and their interaction in the HLRA
Olga Galytska	IDMG	Technical contributions regarding Cognitive Framework for Biometrics and Video Analytics
Giuseppe Giunta	ENI	Contribution to technologies for leak detection in particular to ENI-Vibroacoustic Pipeline Monitoring System: e-vpms@

REVISION TABLE

Version	Date	Comments
0.0	02/09/2019	First Draft Version of the High-Level Reference Architecture for discussion and analysis
1.0	16/10/2019	Table of Content (ToC) of D2.3 by RINA-C
2.0	03/11/2019	Updated ToC by RINAC
3.0	18/11/2019	Comments and contributions by INNOV
4.0	25/11/2019	Integration of LDO proposal, review after discussion during teleconference
5.0	29/11/2019	Comments and contributions by GAP, JRC, FHG, IDEMIA, ELBIT, ADPM, ENI
6.0	02/12/2019	Integration of comments made by KEMEA Contributions by all partners
7.0	10/12/2019	Integration of contributions and feedbacks coming from all partners involved
8.0	16/12/2019	Revision and integration by LDO
9.0	17/12/2019	Revision and integration by RINAC
FINAL	19/12/2019	Final review by RINA-C

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 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.

A graphical representation of the main features and outcomes of SecureGas is provided below.

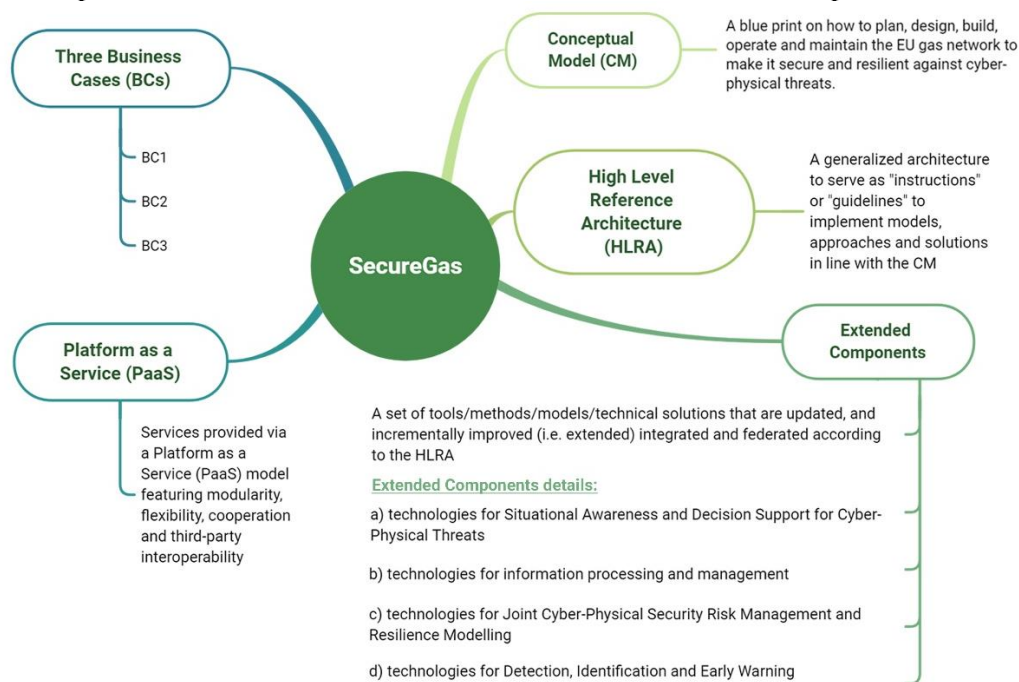


TABLE OF CONTENTS

	Page
LIST OF TABLES	7
LIST OF FIGURES	7
ABBREVIATIONS AND ACRONYMS	9
EXECUTIVE SUMMARY	11
1 INTRODUCTION	13
1.1 SCOPE OF THE DOCUMENT	13
1.2 STRUCTURE OF THE DOCUMENT	13
1.3 INTERACTION WITH OTHER PROJECT TASKS	13
2 GENERIC GAS INFRASTRUCTURE COMPONENTS AND ARCHITECTURE	15
2.1 EXTRACTION	15
2.1.1 Blow Out Preventer (BOP)	15
2.1.2 Christmas Tree	15
2.1.3 Corrosion Inhibitors Injection	15
2.1.4 Gas Lift System	16
2.2 TREATMENT	16
2.2.1 Separator	16
2.2.2 Sweetening	16
2.2.3 Liquefied Natural gas	17
2.2.3.1 Liquefaction	17
2.2.3.2 Regasification	19
2.2.3.3 Storage	20
2.3 TRANSPORT AND DISTRIBUTION	20
2.3.1 Pipelines	20
2.3.1.1 TPI	22
2.3.1.2 Gas Leaks	22
2.3.2 Pumping Stations	22
2.3.3 Metering Station	22
2.3.4 Pressure Reduction	22
2.3.5 Odourising Box	22
2.4 AUTOMATION, CONTROL AND SAFETY SYSTEMS	23
2.4.1 Generalities	23
2.4.2 Supervisory Control and Data Acquisition	24
2.4.3 Pipeline management, control and safety	25
2.4.4 Process control systems	28
2.4.5 Safety systems	29
2.4.6 Integrated Control and Safety System (ICSS)	30
2.4.7 Telecom and Security/Surveillance Systems	32
2.4.7.1 Data Transmission Systems	33
2.4.8 Asset optimization and maintenance support	33
2.4.9 Information management systems (IMS)	35

3	LINK BETWEEN THE GENERIC ARCHITECTURE AND SECUREGAS HLRA	36
4	SECURE GAS HIGH LEVEL REFERENCE ARCHITECTURE	38
4.1	INTERACTIONS AMONG COMPONENTS	40
4.2	FIELD LAYER	40
4.2.1	Physical Resources Monitoring	41
4.2.1.1	Technologies for Leak Detection and Third Party Interference (RINA-C, ENI)	41
4.2.1.2	ENI-Vibroacoustic Pipeline Monitoring System: e-vpms®	41
4.2.1.3	UAV based Asset Management (ADPM)	46
4.2.1.4	Geo-Hazard Assessment (RINA-C)	47
4.2.1.5	Intrusion and Defects Detection (RINA-C)	48
4.2.1.6	Cognitive Framework for Biometrics and Video Analytics (IDMG, INNOV)	49
4.2.2	Cyber Resources Monitoring	50
4.2.2.1	Cyber Security for IT and OT networks weakness (ELBIT)	50
4.3	NORMALISATION AND CORRELATION LAYER	51
4.3.1	Cyber Physical Correlator	52
4.3.1.1	Cyber Physical Correlator (WINGS)	52
4.4	SITUATIONAL AWARENESS LAYER	52
4.4.1	Decision Support System – Safety and Security Platform for Gas Critical Infrastructure (LDO)	53
4.4.2	Blockchain for Data Integrity, Validation and Forensics (GT)	54
4.4.3	Risk and Resilience Modelling/Management	55
4.4.3.1	Joint Cyber and Physical Security Risk and Resilience Modelling and Management (GAP, JRC, RTU, FHG)	55
4.4.3.2	Gas Network Advanced Modelling and Fast-Dynamics Simulation (FHG, JRC)	56
4.5	DIFFUSION LAYER	58
4.5.1	Risk aware information to the population (INNOV)	58
4.6	IMPROVEMENT LAYER (RINA-C)	59
4.7	INTEROPERABILITY LAYERS (RINA-C)	62
5	CONCLUSIONS	64
	REFERENCES	66

LIST OF TABLES

No table of figures entries found.

LIST OF FIGURES

Figure 1-1	Representation of proposed interim version of SecureGas HLRA	12
Figure 1-1	Diagram of interdependencies among D2.3 and other Tasks	14
Figure 2-1:	High level representation of a gas treatment facility	17
Figure 2-2:	T vs. Q in a liquefaction cascade cascade	18
Figure 2-3:	Overview of the liquefaction process up to export facilities	19
Figure 2-4:	Disruptions caused by landslides	21

Figure 2-5:	Stages of the oil and gas process	23
Figure 2-6:	SCADA system topology (typical)	24
Figure 2-7:	Wellhead automation system (typical)	25
Figure 2-8:	Gas Pipeline	25
Figure 2-9:	Typical Architecture of a Pipeline Automation System	26
Figure 2-10:	HIPPS Typical Architecture	27
Figure 2-11:	Leak Detection Methods	27
Figure 2-12:	Example of a Leak Detection System Architecture (Acoustic Technology)	28
Figure 2-13:	Typical Architecture of a PCS	28
Figure 2-14:	ICSS Typical Architecture	31
Figure 2-15:	Computerised Maintenance Management System	34
Figure 2-16:	Information management system topology	35
Figure 3-1:	SecureGas Components	37
Figure 4-1:	SecureGas High Level Reference Architecture – Interim Version	39
Figure 4-2:	Info/Data Exchange among SecureGas extended components	40
Figure 4-3:	SecureGas HLRA: Zoom on FIELD Layer	40
Figure 4-4:	e-vpms® Technology Scheme for Leak Detection and Third Party Interference Alarms	42
Figure 4-5:	e-vpms® Sensing Group and Typical Installation on Pipeline	43
Figure 4-6:	E-vpms® software suite including maps and pipeline schematic representation	43
Figure 4-7:	e-vpms® System Performance and Operability Conditions	44
Figure 4-8:	SecureGas HLRA: Zoom on NORMALIZATION & CORRELATION Layer	51
Figure 4-9:	SecureGas HLRA: Zoom on SITUATIONAL AWARENESS Layer	53
Figure 4-10:	Gas Network Simulation	57
Figure 4-11:	SecureGas HLRA: Zoom on DIFFUSION Layer	58
Figure 4-12:	SecureGas HLRA: Zoom on IMPROVEMENT Layer	59
Figure 4-13:	RINA CUBE services options in SecureGas	61
Figure 4-14:	RINA CUBE: Potential Stakeholders involvement and roles in SecureGas	62
Figure 5-1:	Example of instantiation of the HLRA to a generic SecureGas Business Case	65

ABBREVIATIONS AND ACRONYMS

BC	Business Case
BOG	Boil-Off Gas
BOP	Blow-Out Preventer
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
DPI	Deep Packet Inspection
DRM	Disaster Risk Management
DSS	Decision Support Tool
EGIG	European Gas pipeline Incident data Group
GIS	Geographic Information System
HIPPS	High Integrity Pressure Protection 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
LNG	Liquified Natural Gas
LOC	Loss of Control
LP	Low Pressure
ML	Machine Learning
NG	Natural Gas
OT	Operation Technology
PCS	Process Control System
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
XT	Christmas Tree

EXECUTIVE SUMMARY

SecureGas Project aims at protecting and making resilience gas networks from cyber-physical attacks and threats through the implementation of a resilient security infrastructure.

In particular, the purpose of SecureGas is not just to provide solutions for existing assets in the gas industry, but also to define the way forward, with relevant best practices, to a more resilient infrastructure.

For this reason, a High Level Reference Architecture (HLRA) has been defined and described in detail in this document, in order to provide the structuring principles of the security system, to be declined on the different business cases, not limiting them to the ones taken into account in the context of this project but also in further and future applications.

The first part of the present document outlines the main components of the gas production system, that are identified under the mechanical and architectural perspective; the different components are then put together to define the baseline state of the art in industry. This is important to understand that any generic gas infrastructure could potentially be addressed by the solution implemented in the SecureGas project.

Secondly, the definition of the HLRA is herewith addressed in its different layers and components. The purpose of the HLRA is to increase the resilience to physical and cyber (and the combination of them) threats of the gas networks: this is achieved by means of a multilayer system which components monitor the existing gas infrastructure to determine the relationship between physical and cyber events. The correlated events are then used for decision making and dissemination purposes in order to maintain an appropriate level of safety for all of the stakeholders.

The structure of the proposed HLRA is, as mentioned above, made of layers following a bottom-up approach, that are organized as follows:

- Field layer – needed to detect events related to cyber-physical threats;
- Normalization & Correlation layer – acquiring data coming from the layer below and performing their first elaboration and correlation;
- Situational Awareness layer – providing the operator the decision support by analysing the processed information and being supported by risk analysis and scenario simulation;
- Diffusion layer – needed to warn the operators about the occurrence of an incident and provide the related information;
- Improvement layer – providing the services implemented in SecureGas project “as-a-Service”.

Figure 1-1 depicts the architecture in accordance to the aforementioned structure.

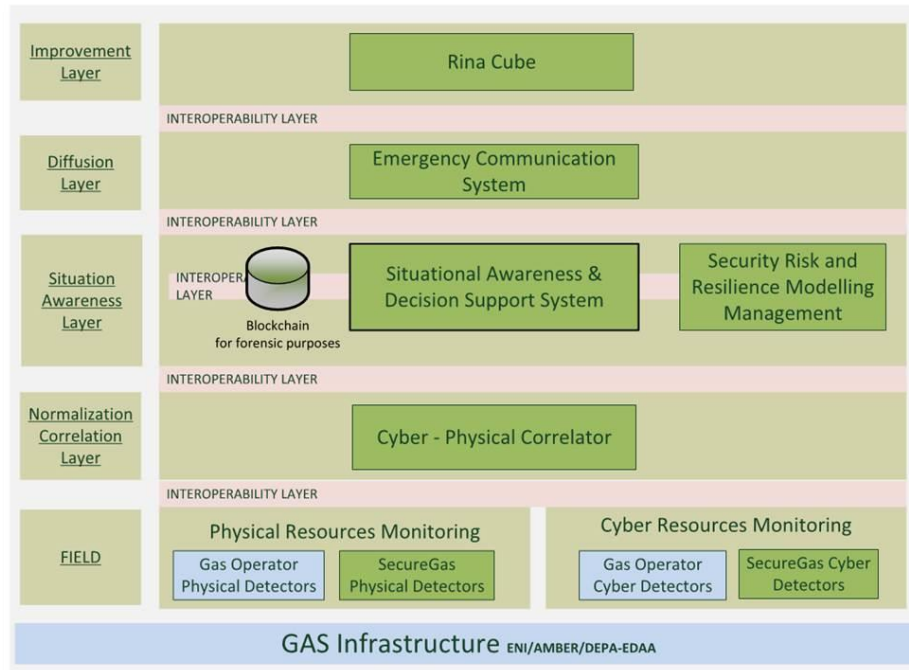


Figure 1-1 Representation of proposed interim version of SecureGas HLRA