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: D1.4 KPIs Inventory

ID: SecureGas_D1.4_FINAL

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

SecureGas
D1.4 – KPIS INVENTORY

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_D1.4_FINAL	**Version:**	FINAL
Deliverable:	D1.4	**Date:**	17/12/2019
		Status:	Approved

Document classification	PU Public

Approval Status	
Prepared by:	GAP
Approved by: **(WP Leader)**	FHG
Approved by: **(Coordinator)**	RINA-C
Scientific Coordinator	FHG
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	Scientific Coordinator, Internal Review
Sebastian Ganter	FHG	Work Package 1 Leader, Internal Review
Evita Agrafioti	GAP	Task 1.4 Leader, Editor
Anastasia Chalkidou	GAP	Task 1.4 Leader, Editor
George Papadakis	GAP	Task 1.4 Leader, Editor
Kushal Srivastava	FHG	Contributor
Anna Gazi	KEMEA	Contributor
Ilias Gkotsis	KEMEA	Contributor
Giuseppe Giunta	ENI	Contributor
Algirdas Dominus	AMBER	Contributor
Stella Tsiouma	DEPA	Contributor
George Stergiopoulos	DEPA	Contributor
Martina Miro	RINA-C	Contributor
Omar Zanoli	RINA-C	Contributor
Paolo Antonio Corvaglia	RINA-C	Contributor
Vit Striteckey	TPEB	Contributor
Dimitris Petrantonakis	EXUS	Contributor
Vassilios Vassiliou	EDAA	Contributor
Eugenia Koutiva	EDAA	Contributor
Antonio Zangrilli	ADPM	Contributor
Rosanna Crimaldi	LDO	Responsible for collecting the KPIs from technical partners and for Component KPIs

Aspa Skalidi	WINGS	Component KPIs
Priit Anton	GT	Component KPIs
Levi Tzahi	ELBIT	Component KPIs
Olga Galytska	IDMG	Component KPIs
Dirk Homberg	IDMG	Component KPIs
Dimitris Drakoulis	INNOV	Component KPIs
Filia Filippou	INNOV	Component KPIs

REVISION TABLE

Version	Date	Comments
V0.1	25/09/2019	First draft of D1.1 with ToC
V0.2	15/10/2019	Integration of end-users feedback
V0.3	6/11/2019	Integration of component KPIs and draft version of SecureGas – Cross Requirements
V0.4	18/11/2019	Update of KPIs based on additional feedback received (validated after the dedicated telco on the same day)
V0.5	22/10/2019	Final draft by GAP
V0.6	27/11/2019	Internal review by FGH (WP1-Lead)
V0.7	01.12.2019	Scientific Review (Scientific Coordinator, FHG)
FINAL	16/12/2019	Final review by RINA-C

SecureGas – PUBLISHABLE EXTENDED ABSTRACT

SecureGas focuses on the 140.000 km 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 to 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 in order to ensure that the delivery of the solutions and services are in line with the clear needs and requirements of the project.

These needs and requirements are focused on risk-based security asset management of gas transmission and distribution networks, impacts (economics, environmental and social) and cascading effects of cyber-physical attacks on European Gas grids (both cascading and interconnected). It is aimed to achieve better risk control and resilience through the operationalization of resilience guidelines and 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.

The present Deliverable 1.4 focuses on the identification of Key Performance Indicators (KPIs) for the SecureGas platform, its components and related services developed according to the operational and regulatory requirements as identified in Deliverable 1.1, the technical requirements as specified in Deliverable 1.2 and countering the potential threat landscape as described in Deliverable 1.3. The deliverable describes how the KPIs are developed along with the roles of the partners in this process. The structure of the rich KPI listing is explained based on the technical solution provision and the expectation of the end users. The main body of the deliverable are the listing of KPIs on solution component level and cross-sectorial KPIs. Finally the KPI list is discussed regarding its implications for the concept model and the high level reference architecture of Task 2.1 and its further versions as well as the technical solution specification of Task 2.2 and related interfacing tasks of WP2. It is shown how the KPIs are expected to be used for further development and testing in WP3, and more specifically within the business cases in WP4 to WP6.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AD	Active Directory
BC	Business Case
BCH	Blockchain for Data Transmission and Integrity Verification Mechanisms
CI	Critical Infrastructure
CM	Conceptual Model
CONOPS	Concept of Operations
CRS	Cross-Requirements
CROP	Common Relevant Operational Picture
DET	Biometrics and Video Analytics
DoA	Description of Action
DSS	Decision Support System
ECI	European Critical Infrastructure
GEO	Geohazards Assessment
GNS	Gas Network Advanced Modeling and Fast-Dynamics Simulations
HLRA	High Level Reference Architecture
IDD	Intrusion and Defects Detection
IDEA	Intrusion Detection Extensible Alert
IDMEF	Intrusion detection message exchange format
INT	Integration and Interoperability Layer
IPM	Data Analytics and Machine learning for cyber-physical security
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
KSI	Keyless Signature Infrastructure
LDAP	Lightweight Directory Access Protocol
LP	License Plate
MB	Megabyte
MM	Multi-mode
OCR	Optical Character Recognition
OSP	Operator Security Plan
OT	Operational Technology
OTS	Cyber Security for IT and OT network weaknesses
PIMS	Pipeline Integrity Management System
PTZ	Pan-Tilt-Zoom
RAW	Risk-Aware Information to the Population
RBAC	Role Based Access Control
RMG	Joint Cyber-Physical Risk and Resilience Management
SeMS	Security Management System
STIX	Structured Threat Information Expression
SM	Single-mode
SMS	Safety Management System
TRL	Technology Readiness Level
UAV	UAV-based Asset Management
UR	User Requirements
WP	Works Package

EXECUTIVE SUMMARY

The present deliverable D1.4 is the final deliverable of WP1 “SecureGas requirements, risks and threats identification” and the main outcome of task T1.4 “Key Performance Indicators (KPIs)”. Deliverable D1.4 targets the definition of the SecureGas KPIs, which are regarded as a measurable way to assess the SecureGas project’s efficiency in reaching its key objectives and also to track the progress of system development while evaluating its performance. Through the KPIs, the main areas to be tested, measured and validated are being defined.

The ultimate goal of D1.4 is to define two sets of KPIs, the *SecureGas component KPIs* and the *SecureGas Cross-KPIs*. Following a bottom-up rationale, the SecureGas component KPIs were firstly defined by the component providers (technical partners), reflecting the most important performance characteristics offered by each SecureGas component, and specifically by the eleven SecureGas extended components and the Integration and Interoperability layer (twelve components in total). The SecureGas component KPIs provided then the basis for the definition of the SecureGas Cross-KPIs, which reflect the expected key functionalities of the entire SecureGas solution (all components integrated into one system).

Considering that the KPIs depend, amongst others, on the end-users interested in the SecureGas system, their active engagement to the KPIs’ development activities enabled the definition of meaningful and tangible metrics. Indeed, the SecureGas end-users (AMBER, DEPA, EDAA, ENI) provided a list of KPIs they apply to assess the effectiveness of their management systems (such as Safety Management System, Security Management System, Pipeline Integrity Management System, Asset Management System) and to ensure the secure and safe operation of their Gas CI network. That list, along with the already defined User Requirements (URs), the Technical Requirements of each component and the Cross-Requirements (CRS), the Conceptual Model (CM) and Concept of Operations (CONOPS) as well as the High Level Reference Architecture (HLRA) were instrumental for development of the KPIs inventory. In addition, special emphasis was given on the feedback received by the external stakeholders, during the dedicated workshop held in Freiburg in M4.

The KPIs inventory developed within the present deliverable comprises 70 SecureGas component KPIs and eleven SecureGas Cross-KPIs. The KPIs are classified in distinct Dimensions and/or Fields, which reflect the general areas where the impacts are going to exert their effect, and are also linked to detailed descriptions and target values that set specific goals for the development and implementation phase. In addition, the SecureGas Cross-KPIs manage to address all the seven Risk and Resilience Phases, i.e. Prepare, Detect, Prevent, Absorb, Respond, Recover, Learn and Adapt, showcasing that the SecureGas solution do have the potential to add value and foster the implementation of all panarchy loop steps and thus to further enhance the security of the Gas CI network before, during and after an incident occurrence.

The KPIs of D1.4 will be further customized, at a later stage, to address the specific requirements and needs of each Business Case, formulating the so-called BC-KPIs. The BC-KPIs, will be extracted upon the definition of the Business Case scenarios and will be reported in D7.1. Those KPIs are the ones that will be finally measured at the three pilot demonstrations (WP4, WP5 and WP6).

The KPIs of D1.4 are envisaged to support the targeted development and realization of the SecureGas components towards well defined and tangible goals and to ensure that project objectives are being met throughout its entire lifespan.

1 INTRODUCTION

1.1 WP1 OBJECTIVES

WP1 is entitled "SecureGas requirements, risks and threats identification" and comprises four Tasks. Based on the information available in the Description of Action (DoA), the main objectives of WP1 are summarized as follows:

- Identification of SecureGas user requirements,
- Identification of SecureGas system requirements,
- Development of a thorough catalogue of physical and cyber threats targeting Gas Critical Infrastructure (CI), and
- Identification of KPIs that allow the evaluation of system performance, highlighting potential gaps and needs for improvement.

1.2 SCOPE AND OBJECTIVES

The current deliverable D1.4, entitled "KPIs inventory" is the main outcome of T1.4 and the last deliverable of WP1. Moreover, the delivery of D1.4 is linked to the second milestone of the SecureGas project, named MS2 "Availability of KPIs, definition of HLRA, Business Cases scenarios".

The main scope of D1.4 is the definition of KPIs, which constitute a means of assessing the quality and performance of the SecureGas solution and a way of evaluating the level of project goals and objectives fulfillment. D1.4 targets the definition of both low and high level KPIs: Adopting a bottom-up approach, a list of KPIs is defined for each SecureGas component (low level KPIs), providing then the basis for the definition of the SecureGas Cross-KPIs that refer to the features and functionalities offered by the entire SecureGas solution (i.e. all components integrated into one system) (high level KPIs).

The SecureGas User Requirements (D1.1)[1], the Technical Requirements (D1.2)[2], the Conceptual Model (CM) and Concept of Operations (CONOPS) (D2.1)[3] as well as the High Level Reference Architecture (HLRA) (D2.3)[4] served as valuable input to the definition of the KPIs. In addition, the feedback received during the stakeholders' workshop held in Freiburg in M4, was also instrumental.

The KPIs identified in the present deliverable aim at capturing all those characteristics of the components as well as of the entire SecureGas system that are key to performance success. The ultimate goal is the development of a thorough inventory of KPIs that will be, at a later stage, customized to address the distinct needs of each Business Case (BC). The KPIs customization to BCs (BC-KPIs) will be performed upon the definition of the BC scenarios and will be reported in WP7 (D7.1). Those BC-KPIs are the ones that will be finally measured at the three pilot demonstrations (WP4, WP5 and WP6) to evaluate the actual system performance.

Apart from setting the groundwork for the definition of the indicators to be tested in the piloting activities, D1.4 also aims at providing guidance for the targeted development and realization of the SecureGas components towards well defined and tangible goals. The development of those components is part of WP3 activities that have kicked-off in M5.

****

[1] SecureGas Deliverable - D1.1 "Organizational, Operational and Regulatory Requirements"

[2] SecureGas Deliverable - D1.2 "Technical Requirements"

[3] SecureGas Deliverable - D2.1 "SecureGas Conceptual Model and CONOPS – intermediate version"

[4] SecureGas Deliverable - D2.3 "SecureGas HLRA –intermediate version"

1.3 STRUCTURE OF THE DELIVERABLE

D1.4 comprises three core sections:

Section 2, entitled "Methodology for KPIs definition", outlines the methodological approach applied for defining the KPIs. Emphasis is given on the KPIs already applied by the SecureGas end-users (**Section 2.1**), as well as on the approach followed for the SecureGas component KPIs (**Section 2.2**) and the SecureGas Cross-KPIs definition.

Section 3, named "SecureGas component KPIs", provides the KPIs that have been defined for the eleven SecureGas extended components as well as for the Integration and Interoperability layers. Those KPIs are classified in various Dimensions and Fields and are presented in dedicated templates.

Section 4, entitled **"**SecureGas Cross-KPIs", is dedicated to the KPIs of the overall SecureGas solution outlining in particular its impact on the Risk and Resilience phases of the panarchy loop. The templates used are similar to the template of Section 3.

2 METHODOLOGY FOR KPIS DEFINITION

KPIs are deemed as a measurable way to assess the project's efficiency in reaching its key objectives. Also, as a means to evaluate the quality and measure the performance and impacts of the proposed technical solution(s). KPIs establish the main areas to be tested, measured and validated during the piloting activities, through a series of well defined and quantifiable indicators.

The KPIs defined in the current deliverable are classified along two main indicator types:

- *SecureGas component KPIs*, which reflect the key characteristics and functionalities offered by each SecureGas component and are applied for their performance evaluation;
- *SecureGas Cross-KPIs*, which reflect the key functionalities and the expected quality of the entire SecureGas solution, which constitutes a system of systems.

For the purposes of D1.4, the methodology adopted for the definition of the KPIs was built on a bottom-up rationale, i.e. the SecureGas component KPIs (low level KPIs) were initially defined, and then, drawing on that information, the SecureGas Cross-KPIs (high level KPIs) were derived.

The procedural pathway followed for the identification of KPIs is depicted in Figure 2.1.

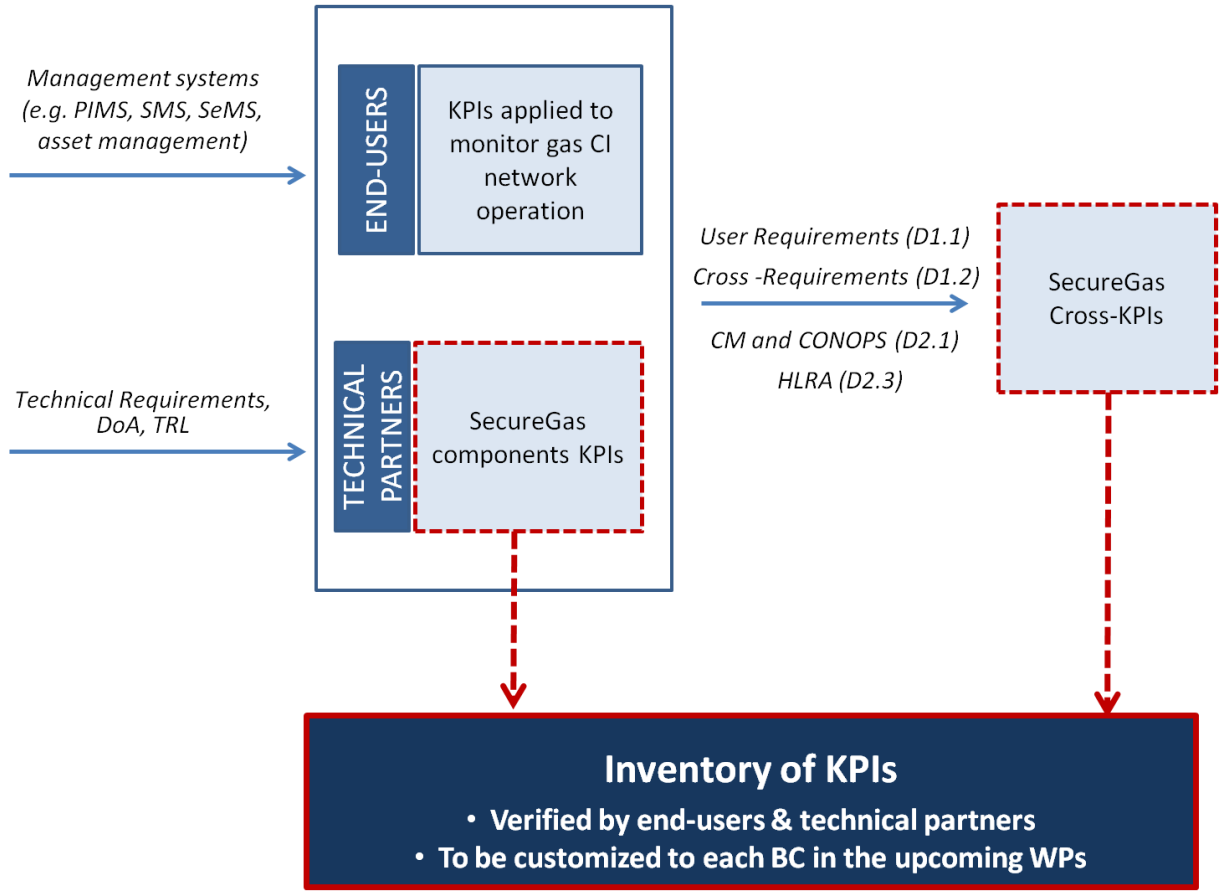

Figure 2.1: KPIs definition pathway

Considering that KPIs depend on the end-users and stakeholders interested in the SecureGas system, the first step of the adopted methodology regarded their active engagement to the KPIs definition activities. This initiative had already started taking place through the definition of the URs in M3 as well as through the dedicated stakeholders' workshop organized for the URs validation in M4 (in Freiburg, Germany). Indeed, the URs reported in D1.1, together with their external validation results, shed light to those characteristics of the system that are deemed important by the end-users.

Apart from the URs, and as part of the D1.4 activities, the SecureGas end-users were requested to provide indicative lists of KPIs that they apply to assess the performance of their network daily operations. The ultimate goal was not to capture specific metrics and targets for those KPIs, but to list the broad areas in which evaluations are performed for gas networks and to examine how the SecureGas solution could contribute and add value in that direction.

In parallel, a dedicated KPIs template was developed and distributed among SecureGas technical partners for the extraction of tangible and measurable KPIs that correspond to the key characteristics of their technical sub-systems (components). The SecureGas component KPIs were classified in distinct categories and were assigned detailed descriptions and values to enable their targeted realization in the upcoming WPs.

Drawing on the SecureGas component KPIs as well as on the KPIs provided by the end-users, and considering also the Cross-Requirements (CRS) already defined in D1.2, the SecureGas Cross-KPIs were formulated. Those KPIs refer to the SecureGas system as a whole, reflecting the most important features and characteristics of the integrated solution that are key to performance success.

Both the SecureGas component KPIs and SecureGas Cross-KPIs, upon being defined, were verified by the SecureGas technical partners and end-users participating in T1.4, forming an inventory of validated KPIs. Upon the definition of the BC scenarios, those KPIs will be customized to address the specific requirements of each BC. The three sets of the so-called BC-KPIs, which will be reported in D7.1, are the ones that will be finally measured during the three piloting activities to assess the actual performance of the SecureGas system.

The following sub-sections provide more detailed information on the KPIs applied to monitor gas CI network operation and outline the procedural steps followed for the definition of SecureGas component KPIs and the SecureGas Cross-KPIs.

2.1 KPIS RELATED TO GAS CI NETWORK OPERATION

Today most companies operate within the context of management systems that provide the basis for the successful fulfillment of their goals. Indeed, management systems constitute a set of policies, processes and procedures that are used by an organization to ensure that it can achieve its objectives. Those objectives may cover various aspects of organization's operations, thus, there are management systems dedicated to safe operations, quality of services, occupational health and safety, environmental performance, business continuity, etc.

The management systems that are related to the daily safe and secure operation of the Gas CI network, had been identified by the SecureGas end-users (AMBER, DEPA, EDAA, ENI) in D1.1, formulating the Organizational URs list. Those management systems are as follows (in parenthesis, in addition the code of the related UR is provided):

- Pipeline Integrity Management System (PIMS) (OR-SYST-01)
- Safety Management System (SMS) (OR-SYST-02)
- Security Management System (SeMS) (OR-SYST-03)
- Emergency/Disaster Management System (OR-SYST-04)
- Life Cycle Management System (OR-SYST-05)
- Operations Integrity Management System (OR-SYST-06)

In order to allow the monitoring and evaluation of the effective implementation of those systems and also the detection of potential inadequacies/failures in their performance, management systems are usually being accompanied by a set of KPIs. Through those KPIs, companies set specific and tangible metrics that reflect the exact goals they want to achieve in order to guarantee the successful performance of their management systems. In many cases those KPIs act proactively, as risk management measures, and are linked to unfavorable situations (e.g. number of serious incidents/accidents/near misses and number of injuries) which can be avoided if dedicated procedures take place.

Considering that the SecureGas system aims at adding value to the gas CI network with regard to its secure and safe operations and its protection against physical and cyber threats (all hazards approach), it was deemed rather important to take into consideration the KPIs that the SecureGas end-users already apply to monitor their network normal operation. To this end, the project end-users provided representative lists of KPIs that are linked to their companies' management systems and are related to SecureGas objectives. This action did not aim at capturing specific metrics and target values, but only to showcase the general areas of performance evaluation. The typically already used end-user KPIs are presented in Table 2.1.

Table 2.1: KPIs applied to monitor Gas CI network operation

KPIs for monitoring Gas CI network operation
Number of pipelines damage incidents
Number of pipelines near-miss incidents
Number of unauthorized interferences with the pipeline (excavation, construction, etc.)
Number of major leaks
Number of minor leaks
Number of failures that have not been localized
Number of cyber attacks directed to company's IT
Number of cyber attacks directed to company's IT systems
Number of cyber attacks directed to company's employees by using social engineering methods
Damage made due to human factor by IT system administrators
Loss of data from mobile data storages
Number of mobile IT devices infected by viruses or harmful software
Number of instances exceeding MAOP (maximum allowed operating pressure) Steady-State Conditions
Pipeline temperature
Number of alarms
Number of warnings
Validation of alarms
Validation of warnings
Number of reported security threats
Total Number of security incidents
Number of system errors
Number of technical failures
Average time to complete tasks
Average time per user to complete tasks
Average time between the occurrence of an incident and the first response
Time to resolve
Downtime (the percentage of the time service is available)
Availability (the total service time the system is available)
Time allocated for administration, management, training
Average time between the occurrence of an incident and the appearing in the system
Network packet delay
Number of unplanned stops
Number of inspections ratio (completed/ required) per predefined time
Number of safety critical /main equipment maintenance ratio (completed/ required)
Delayed work of maintenance by categories (repair, modification, prevention)
Delayed works for repair/ renovation
Spare parts and dispensable materials availability
Valves' availability for remote control during one-year period
Amount of valves' remote control cases during one-year period
Amount of valves' remote control failures during one-year period
Amount of failures of valves' hydraulic or of electric actuators during one year period
Cost benefit ratio for evaluation of mitigation measures
Risk reduction score for the evaluation of mitigation measures
Cost per incident
Operational cost

The KPIs provided by the SecureGas end users shed light on the most important parameters that are considered critical for the evaluation of the Gas network operation and enabled the identification of key areas where the SecureGas system needs to exert its impact and add value.

It needs to be highlighted that although all the end-users KPIs are deemed key elements for the system performance evaluation, nevertheless some of them did not contribute to the formulation of the SecureGas KPIs, mostly because they reflect attributes of an industrialized version of the SecureGas solution, and thus it was considered of low relevance to the task's and project's scope.

2.2 ELICITATION OF SECUREGAS COMPONENT KPIS

As it was aforementioned, one of the goals of D1.4 is the definition of SecureGas component KPIs. The components studied were the extended components of the SecureGas project, namely (in parenthesis, the abbreviation applied for each component, is provided):

1. Decision Support System (DSS)
2. UAV-based asset management (UAV)
3. Geohazards Assessment (GEO)
4. Data Analytics and Machine Learning for cyber-physical security (IPM)
5. Blockchain for data transmission and integrity verification mechanisms (BCH)
6. Cyber Security for IT and OT network weaknesses (OTS)
7. Intrusion and defects detection (IDD)
8. Biometrics and video analytics (DET)
9. Joint Cyber-Physical Risk and Resilience Management (RMG)
10. Gas Network Advanced Modeling and Fast-Dynamics Simulation (GNS)
11. Risk-aware information to the population (RAW)

Apart from the extended components, the following component was also considered:

12. Integration and interoperability layers (INT)

The SecureGas standard components were not taken into consideration within the current deliverable. Those components consist mainly of off-the-shelf HW and SW systems, and they are not considered a research development of the SecureGas project. Thus, the definition of the indicators to track their individual performance characteristics was deemed out of scope. Standard components will be defined and designed in Task 2.3, implemented in Task 3.5.

The SecureGas component KPIs were defined by technical solution/component providers (technical partners). The input information that allowed for KPIs definition was:

- *Components' technical requirements*. The technical requirements of the SecureGas components were defined in D1.2[5] and provide detailed information on all the capabilities, technical characteristics and functionalities offered by every technical subsystem. Those technical requirements were instrumental for the identification of the most important (key) performance characteristics of the SecureGas components. It is worth noticing that the technical requirements constitute a translation of user requirements into system specifications, reflecting thus the capabilities offered by the technical components to address users' needs. In that way end users' expectations are also, even indirectly, reflected through the SecureGas components' KPIs.
- *KPIs available in the DoA*. From the proposal stage, technical partners had identified for their components some preliminary indicators, along with their target values. Those KPIs are listed in Section 1.4 of the DoA and constitute the minimum required KPIs for the deployment phase.

****

[5] SecureGas Deliverable - D1.2 "Technical Requirements"

- *Technology Readiness Level (TRL)*. The expected components TRL upon the finalization of the SecureGas project, is a critical factor that was taken into consideration by the technical providers for the definition of KPIs that are indicative of the technological progress beyond the state of the art and the innovation potential.

In order to facilitate the identification and collection procedure, a dedicated template was developed and distributed among technical partners/component providers, see Table 2.2.

Table 2.2: Template used for KPIs identification and collection

Dimension	Field	Indicator	Description	Metric	Target value
Functional					
Interface					.
Security					
Operational					
Design					
Implementation					

The development of the template was based on the below rationale: The SecureGas component KPIs need to be classified into specific *Dimensions* that outline the general domains where the impacts are going to exert their effect. Those Dimensions drew on the categorization that had been used in D1.2[6] for the various features of the system and are as follows:

- ***Functional:*** this Dimension relates to a function that the component must be able to perform. It specifies what the specific component will be able to do. KPIs belonging to this dimension will be related to the services that the component provides, how the component should react to particular inputs and how the component should behave in particular situations.
- ***Interface:*** this Dimension is related to the data a component needs/provides. It relates to an external item with which the component must interact, or that sets forth constraints on formats, timing, or other factors caused by such an interaction.
- ***Security:*** this Dimension relates to security-related aspects, which is how the component secures itself (security functions that the system provides to users or other systems or infrastructures are to be considered in the functional dimension).
- ***Operational:*** this Dimension relates to the operational conditions or properties that are required for the component to operate or exist (e.g. availability, maintainability, reliability (non-functional characteristics).
- ***Design:*** this Dimension is related to the design of the component. It might be related to the limits on the options of a solution that are available to a designer; for example, to use a specific technology, product or the adoption of a specific technical standard.
- ***Implementation:*** this Dimension relates to the specifications or constraints of the coding or construction of a component.

****

[6] SecureGas Deliverable - D1.2 “Technical Requirements”

For all the aforementioned Dimensions, technical partners defined a set of more specific sub-areas, the so-called *Fields*, so as to further narrow down the KPIs impact sphere. Each Field was then linked to a set of *Indicators*, each one being assigned a *Description*, *Metric* and *Target Value*.

The SecureGas component KPIs are presented in Section 3. Those KPIs served as input for the definition of the SecureGas Cross-KPIs and will be also used as initial terms of reference for the targeted realization of the SecureGas components in WP3. In addition, those KPIs will be further customized in WP7 to address the specific requirements of each BC and thus to formulate the BC-KPIs that will be measured during the pilot demonstrations.

2.3 ELICITATION OF SECUREGAS CROSS-KPIS

Upon the definition of the SecureGas component KPIs, and considering end-users' feedback on the KPIs, they apply to monitor their Gas CI network operations. The next goal of D1.4 was the elicitation of the SecureGas Cross-KPIs. The SecureGas Cross-KPIs refer to those features and functionalities offered by the whole SecureGas system (i.e. all the components integrated into one system) which are key to its successful performance.

Apart from the SecureGas component KPIs and the general KPIs categories provided by the end-users partners, the elicitation of the SecureGas component KPIs drew also on the following:

- *SecureGas User Requirements*. As it was aforementioned, the KPIs need to be closely related to the end-users interested in the SecureGas system and to reflect how the SecureGas system can improve and add value to the existing procedures applied to monitor the safe and secure operation of the natural gas network. To this end, the URs defined in D1.1[7], as updated after the stakeholders' workshop in M4 in Freiburg, provided thorough information on the expected functionalities of the SecureGas system from the end-users perspective. Special emphasis was given on those requirements that are listed as "High Priority", meaning the requirements that have to be addressed by the means of technological development to support the core values of the SecureGas solution.
- *SecureGas Cross-Requirements*. The Cross-Requirements (CRS) are the technical requirements reported in D1.2 that refer to the functions, features and services provided by the whole SecureGas solution in order to address specific URs. Those CRS provided the baseline for the extraction of indicators that refer to the entire solution. Table 2.2, which is derived from D1.2[8], lists all the CRS of the SecureGas system along with the URs addressed by them. The criteria applied to assess how relevant a CRS is to formulate a KPI of the entire system were supported by the end-users feedback on the KPIs they respectively apply, the high priority URs of D1.1 which can be related to the KPIs and the feedback collected through the stakeholders' workshop.
- *SecureGas CM and CONOPS*. The SecureGas CM and CONOPS were defined in D2.1[9] and entail detailed information on the panarchy loop that links Resilience with the Disaster Risk Management Cycle. Considering the importance of developing a solution that adds value and fosters the implementation of all panarchy loop steps, the goal was to define KPIs that address all its Risk and Resilience phases as defined in D2.1, namely a) Prepare, b) Detect, c) Prevent, d) Absorb, e) Respond, f) Recover, g) Learn and Adapt.
- *SecureGas HLRA.* The SecureGas HLRA, which is part of the T2.2 activities, provided valuable information on the foreseen implementation of the integrated security services and enabled the definition of meaningful and tangible KPIs.

The SecureGas cross-KPIs are presented in Section 4.

****

[7] SecureGas Deliverable - D1.1 "Organizational, Operational and Regulatory Requirements"

[8] SecureGas Deliverable - D1.2 "Technical Requirements"

[9] SecureGas Deliverable - D2.1 "SecureGas Conceptual Model and CONOPS – intermediate version"

Table 2.3:Cross-Requirements (CRS) of D1.2 used to extract the SecureGas Cross-KPIs

Code	Req Title	Requirement Description	User Requirement
CRS_FUN_001	Legacy and new technologies	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	OP-INTER-01
CRS_FUN_002	HMI	The user interface of the SecureGas platform should give the operator a summary of all the alarms occurred in the system in a certain time window, with the possibility to drill down a particular alarm to access a more detailed description.	OP-USA-01
CRS_FUN_003	Event correlation	SecureGas shall correlate events from cyber and physical domains in order to generate, if it is the case, alarms stemming from apparently harmless events. Those events are generated both by legacy systems and by the extended-components provided by SecureGas platform itself.	OP-DSD-01
CRS_FUN_004	Physical threats	SecureGas shall provide detection of physical potential threats, such as leakages, intrusion, third party interference, geohazard-related issues	OP-DSD-02, OP-DSD-03, OP-DSD-04, OP-DSD-05
CRS_FUN_005	Cyber Threat	SecureGas shall provide detection of cyber potential threats, such as attacks on Scada and other control systems	OP-DSD-01
CRS_FUN_006	Decision support	SecureGas shall provide decision support and recommendation service to the operator in order to mitigate the effect of a cyber/physical attack	OP-DSD-13
CRS_FUN_008	Information Sharing	The platform shall address the task of sharing information with the public, as it is an integral part of the resilience and disaster risk management cycle	OP-DSD-14
CRS_IMP_001	Traceability	The logs must contain at least the following data: - 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); - IP address of the originator of the event; - description; - any errors produced by the event.	OP-INFOR-06
CRS_SEC_001	User Authentication	To access any functionality of the SecureGas platform, the user shall perform a login, by using a personal account. It is preferable to integrate the authentication process with external LDAP/AD systems, if available.	OP-CONF-03
CRS_SEC_002	Accountability	Each login/logout and login failure to SecureGas platform shall be logged.	REQUIREMENT NOT EXPRESSED[10]

****

[10] "REQUIREMENT NOT EXPRESSED" or "FREIBURG WORKSHOP" indicates if the Cross-requirement of D1.2 cannot be traced back to a user requirement of D1.1 or has been identified during the Freiburg workshop, respectively.

Code	Req Title	Requirement Description	User Requirement
CRS_SEC_003	Access Control	The SecureGas platform shall manage at least two profiles: Administrative and Operational. These profiles have different capabilities (according to separation of duties principle) and the users will be dynamically linked to one or another of them according to their responsibility (Role Based Access Control - RBAC paradigm)	OP-CONF-03
CRS_SEC_004	Device Authentication	The system shall adopt communication protocols/whitelisting mechanisms that perform the authentication of the authorized devices inside the system, in order to avoid spoofing attacks	REQUIREMENT NOT EXPRESSED
CRS_SEC_005	Communication Integrity	The system shall adopt communication protocols that assure the integrity of the relevant information sent by the sensors.	REQUIREMENT NOT EXPRESSED
CRS_DES_001	Data exchange	Wherever possible, data exchanges between all components shall take place in the form of JSON objects (JavaScript Object Notation)	REQUIREMENT NOT EXPRESSED
CRS_DES_002	Data exchange	In order to facilitate the sharing of information between all components, a standard language shall be identified among those emerged in the cyber security field (e.g. IDEA - Intrusion Detection Extensible Alert; IDMEF - Intrusion detection message exchange format; STIX 2.0 - Structured Threat Information eXpression)	OP-COND-03
CRS_FUN_007	User friendly GUI	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 (Pan-Tilt-Zoom) control, if allowed by the specific device). The 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.	OP-USA-01
CRS_SEC_006	Communication Confidentiality	The system shall adopt communication protocols that assure the confidentiality of the relevant information exchanged through the system	OP-CONF-04
CRS_DES_003	Modularity	The system while integrating different components (legacy systems already operating and new advanced technological solutions) should remain modular: the components may or may not be integrated in the deployed platform according to the end users' needs	OP-USA-04
CRS_DES_004	Resilience	SecureGas platform itself shall adopt fast recovery mechanisms/ procedures in order to be quickly available again in case of adverse events	OP-CONF-01

Code	Req Title	Requirement Description	User Requirement
CRS_DES_005	Financial sustainability	The costs of SecureGas related to both the provisioning of the platform and its maintenance, training and evolution must be competitive with respect to competing solutions (provided that the features offered are comparable)	FREIBURG WORKSHOP

3 SECUREGAS COMPONENT KPIS

The SecureGas component KPIs are listed in the following sub-sections. For all the twelve components, 70 KPIs were identified in total.

It needs to be highlighted that the majority of the SecureGas component KPIs cover the Functional and Operational Dimensions, while only few were provided for the Security and Implementation Dimensions. Although some of the components do have self-security mechanisms as well as implementation related features (see Technical Requirements – D1.2), it might be the case that those functionalities do not reflect a key characteristic for the evaluation of components' performance.

3.1 DECISION SUPPORT SYSTEM (DSS)

Table 3.1: DSS component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Operational	Decision Support	Cross Correlation	Percentage of right cross correlation raised by SecureGas system	% (Cross correlate / Total Alerts)	Greater than 50% of total of alerts
	Retention	Data Retention	The SecureGas platform should guarantee the retention of all data (event, alarm, video, logs) to allow a post-process analysis to the authorized operators	Time (dd)	Greater than a week
	Physical Cyber threats	False Positive	Percentage of false positive alerts raised by SecureGas system	% (False Positive / Total Alerts)	No more than 5% of total alarms generated should be false
Implementation	Heterogeneous System Integration	Integration	All cyber/physical security solutions defined in SecureGas are expected to be integrated in Trials	% (N° Subsystem integrated /N° Subsystem)	All subsystems must be integrated in a strong or weak way

3.2 UAV-BASED ASSET MANAGEMENT (UAV)

Table 3.2: UAV component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Pipeline inspection	Safe and continuous operations (24/7)	Operational time duration	Percentage %	80% of 24/7
		Survey efficiency	Number of cancelled missions	Percentage % (number of cancelled missions/ number of total missions)	<10%
		Short reaction time in case of incident	Time necessary for recovery actions Through this KPI the minimum reaction time to an accident (i.e. the time for the drone activation from hangar, take-off and alarm zone achievement) is measured.	Time	5-8 min
		No need for human intervention	Time of human intervention	Percentage % (time with no human intervention / total time)	80% of autonomy without human intervention
		Real time data sharing	Amount of data shared	Percentage % (MB shared / total MB collected)	100% data collected
		Cost-effectiveness of inspections	Cost reduction for inspection	Percentage %	At least 20% cost savings (to be confirmed by the project partners)

3.3 GEOHAZARDS ASSESSMENT (GEO)

Table 3.3: GEO component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Alert	Landslide hazard	Time to provide notification to the user in case of possible slope instabilities	hours	12h
Interface	Rain Measurements	Rain	Pluviometer rain measurements	number of pluviometer (nr) and rain measurement (mm/h)	1 pluviometer each hydrographic basin
	Rain Forecast (optional)	Rain	Rain forecast	mm/h	mm/h every 5x5km
	Digital Terrain Model	DTM	Topography along the route	DTM	cover slopes along pipeline route, 10x10m resolution
	Geotechnical/geological inputs	Geo properties	Geo properties/setting	coverage	cover critical slope area
Operational	Rain inputs (Measured or forecasted)	Near Real Time Availability	Rain data shall be available in near real time	minutes	every 30min

3.4 DATA ANALYTICS AND MACHINE LEARNING FOR CYBER-PHYSICAL SECURITY (IPM)

Table 3.4: IPM component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Scope	Types of events	Number of different types of events targeted by these components	Number	10
Operational	Reliability	Precision	Number of true positives divided by the sum of true and false positives	Percentage %	95%
	Reliability	Recall	Number of true positives divided by the sum of true positives and false negatives	Percentage %	95%
	Reliability	Time to detection	Time between the initiation of an event and its detection	Time (seconds)	5

3.5 BLOCKCHAIN FOR DATA TRANSMISSION AND INTEGRITY VERIFICATION MECHANISMS (BCH)

Table 3.5: BCH component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Data Integrity	Reliability	KSI blockchain issues KSI Signatures, that enable the properties of data to be verified	Time (sec)	<2
	Data Integrity	Reliability	Verifying data properties to assure data integrity	Time (sec)	<0.02
Security	Privacy	Monitoring KSI blockchain functionality	When using KSI blockchain the input data will never be exposed	0/1 (binary)	1
Interface	Availability	Access to service	When using KSI blockchain the service availability is 99,95%	Time (min) in years	< 264 min in 1 year

3.6 CYBER SECURITY FOR IT AND OT NETWORK WEAKNESSES (OTS)

Table 3.6: OTS component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	SCADA Protection	New Host detection	The system will alert if a new host connects to the network	0/1	1
	Alert sending via API	Alert received in management system	An alert will be sent to the management system. Through this KPI, the alerts received in the management system are measured	Percentage % (number of alerts received in management system / total number of alerts)	80%
Design	SCADA Protocols support	Protocol identification	The system will identify the protocols according to the protocol list in the REQs documents	0/1	1

3.7 INTRUSION AND DEFECTS DETECTION (IDD)

Table 3.7: IDD component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Leak alert	Leak Sensitivity	Minimum leak flow detectable within a certain period of time	% of the nominal gas flow	Can't be defined at this stage for two reasons: - Heavily depending on the fiber optic installation conditions - Literature values are typically related to pipelines in operating conditions (hence with gas pressure of about 50 bar) while the ENI installation that will be used as a pilot is not in service, with a reduced pressure (4 bar)
		Location accuracy	Accuracy at which the location of a leak along the pipeline can be determined	Distance (m)	< 10 m
	Intrusion alert	Intrusion sensitivity	Maximum distance from the fiber optic cable at which an event of a certain noise intensity is detectable	Distance (m)	5 - 25 m (depending on the noise intensity, hence on the event type)
Operational	Service reliability	Reliability	False alarm rate Recording of the quantity of detected events (intrusion and leakages) over a defined monitoring time window and comparison with the actual known quantity of events	% of total alarms	5-10% (depending whether in combination or not with other techniques)

Design	Monitoring domain	Monitored length	Distance along the pipeline (starting from the DAU) over which event detection is carried out	Length (km)	> 3 km (if MM fiber) > 25 km (if SM fiber)

3.8 BIOMETRICS AND VIDEO ANALYTICS (DET)

Table 3.8: DET component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Physical threats	Video surveillance 24/7 Processing	The system is able to analyze at day and low light conditions.	% of Time	96%
		Face recognition by day light	This is defined as a percentage of genuine face matches accepted by the system if the template quality over a threshold and the minimum inter eye distance is greater 20px.	% of Match	90%
		Face/person detection by day light	This is defined as a percentage of genuine faces and persons accepted by the system.	% detection	80%
		License plate (LP) OCR reading by day light	This is defined as a percentage of genuine license plate matches accepted by the system if the LP detection higher than 20px.	% reading	85%
		License plate detection by day light	This is defined as a percentage of genuine license plate accepted by the system.	% detection	80%
		Person detection under low light conditions	This is defined as a percentage of genuine persons accepted by the system by infrared images.	% detection	70%
		Face detection under low light conditions	This is defined as a percentage of genuine faces accepted by the system by infrared images.	% detection	60%

3.9 JOINT CYBER-PHYSICAL RISK AND RESILIENCE MANAGEMENT (RMG)

Table 3.9: RMG component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Effectiveness	Threat categories addressed	Number of different categories of threats (cyber, physical, cyber-physical, physical-cyber) addressed by the RMG	Number	4
		Coverage of alerts	Percentage of alerts that entail information about the risk level of the detected event	Percentage (%)	100%
		Automatic decision-support on mitigation actions	Percentage of alerts that will be automatically linked to recommendations on crisis management and mitigation actions	Percentage (%)	≥ 80%
		Impact metrics	Number of different types of consequences considered for risk evaluation. **Fatalities (public, employees, first responders)* *Injuries (public, employees, first responders)* *Cost of asset loss* *Out of service time* *Environmental impact* *Indirect cost (reputation, training, etc)*	Number	≥6
		Localization of risk	Percentage of risk level indicators that are location specific (i.e. percentage of risk level indicators that are referring/ linked to geo-localized assets)	Percentage (%)	≥ 60%

Interface	Interoperability	Access from various terminals	Number of different types of terminals that the RMG will be responsive	Number	3 (desktop, tablet, mobile)
Operational	Reliability	Local processing latency	Time elapsed between the moment an alert is received and alert risk level is calculated	Time (sec)	<3
	Regulation	Coverage of the requirements of the European Critical Infrastructure Operator Security Plan (ECI OSP) as imposed by the EU Directive 114/2008[11]	Number of OSP procedural steps the RMG component has impact on. ** The procedural steps of the ECI OSP are as follows:* *1. identification of important assets;* *2. conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact; and* *3. identification, selection and prioritization of counter-measures and procedures*	Number of steps covered	3
	Effectiveness	Enhancement of Panarchy Loop capabilities	Number of Risk and Resilience phases the RMG functionalities have impact on. ** The Risk and Resilience phases have been defined in the SecureGas CONOPS as follows:* *1) Preparation, Protection (before event)* *2) Detection* *3) Prevention* *4) Absorption, Protection (during and after event)* *5) Response* *6) Recovery (including system improvement)* *7) Learning and adaption*	Number	6

****

[11] Council Directive 114/2008/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Design	Usability / User friendly	Ease to use without S/W skills	Need of coding skills for data entry and/or forms configuration of Risk management tool	Percentage	0

3.10 GAS NETWORK ADVANCED MODELING AND FAST-DYNAMICS SIMULATIONS (GNS)

Table 3.10: GNS component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Transient Prediction	Spatial Resolution (transient)	Spatial resolution within the transient real-time prediction of the gas grid including 140000 km of pipeline regarding its state in terms of pressure and flow rates.	Length (Spatial Numerical Resolution) (km)	10 km
		Computing Time (transient)	Computing time within the transient real-time prediction of the gas grid including 140000 km of pipeline regarding its state in terms of pressure and flow rates at a spatial resolution of 10 km.	Ratio of computing time per physical time	< 1 (real-time)
		Domain Size (transient)	Domain Size within the transient real-time prediction of the gas grid regarding its state in terms of pressure and flow rates at a spatial resolution of 10 km.	Domain Size/ Total pipeline length (km)	140000 km
	Steady-State Prediction	Problem Size (steady-state)	Number of Elements (Nodes+Pipelines/ Edges) that can be accounted for during the identification of most critical elements based on steady-state gas grid simulation accounting pressure and flowrates.	Problem Size (Number of Elements)	1400 Elements

		Computing Time (steady-state, critical element)	Computing time needed for the Identification of most critical elements based on steady-state gas grid simulation accounting for pressure and flowrates including 1400 Elements (Nodes + Pipelines).	Computing time (days)	1 day
		Computing Time (steady-state, response pre-calculation)	Computing time needed for a pre-calculation of potential responses based on steady-state and transient gas grid simulation accounting for pressure and flowrates accounting for 1400 Elements (Nodes + Pipelines).	Computing time (days)	7 days
		Computing Time (response)	Computing time needed for the identification of 'best' response to a disruptive event (both, response and disruption may be a series of temporally distributed single events) based on correlation checks with precalculated and stored response simulation results.	Computing time (s)	60 s
Interface	I/O	Input	Input Gas Grid Topology (Input of Pipeline, Junctions, compressors, valves via file and manual user input)	logical	1
		Input	Input Gas Grid State (Input of Pipeline integrity, compressor performance, Valve position, pressures and flowrates via processed sensor data and via manual user input)	logical	1
		Output	Output (graphical visualization of the gas grid state, Indication of Warning and Decision advices)	logical	1
		Input/ Output	Use of standard input and output formats of open source (non-proprietary) and commercial (proprietary) interfaces	number	>1

3.11 RISK-AWARE INFORMATION TO THE POPULATION (RAW)

Table 3.11: RAW component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Reactivity	Latency	Time elapsed between the moment the operators decide that an incident needs to be communicated and the moment they send the notifying message to the concerned authorities.	Time (minutes)	< 3 minutes
	Content suggestion	Efficiency	Choice of messages to send in order to alert the rest of the supply chain	Number of suggested messages	3 types (for CI operators, civil protection or relevant authorities, first responders)
	Content suggestion	Precision	Set of parameters that assist the operator in accurately identifying the nature and the criticality	Number of parameters	At least 5 parameters
	Forensics	Completeness	Rich log history allowing to investigate if necessary	Completeness of the log record	3-year history
	Interface	Content localization	Number of available languages to make the tool accessible to all stakeholders	Number	4 (3 end users and English)
Operational	Stakeholders	Types of stakeholders	Number of different types of stakeholders that can be reached	Number	3 (CI operators, civil protection or relevant

					authorities, first responders)

3.12 INTEGRATION AND INTEROPERABILITY LAYER (INT)

Table 3.12: INT component KPIs

Dimension	Field	Indicator	Description	Metric	Target value
Functional	Alerting	Delay	Time to provide notification to the user in case of an alert	Time (msec)	< 200 msec
Interface	Connectivity	Compatibility	Ability of the INT component to integrate all the components (both SecureGas components and users' legacy systems) required by each Business Case	0/1 (binary)	1
	Standards definition	Flexibility	Ability of the INT component to address all the standards required by each Business Case	0/1 (binary)	1
Operational	Service continuity	Continuity	Time needed to restore the services	Time (min)	<120 min

4 SECUREGAS CROSS KPIS

The elaboration and analysis of the input information reported in Section 2.3 resulted in the identification of the following five main Fields of Cross-KPIs:

Reliability. This refers to the capability of the system to function in a correct manner within the given timeframe. This includes high accuracy of alert localization, avoidance of any delays in data provision, and a low rate of false alerts or errors.

Autonomy. It is regarded as the level of independence of the system. An autonomous system is capable to operate (detect and process incidents) without human supervision (but human in the loop, if deemed necessary).

Interoperability. It represents the ability of the system to work with new products (i.e. sensors or sub-systems) without special configurations. This characteristic makes it possible to exchange data with new components and establish communication and interpretation of the shared data without restrictions.

Usability. It is regarded as a set of attributes covering the effort needed for using a solution, and on the individual assessment of the use of the solution, by a stated or implied set of users.

Resilience. It reflects the ability to adapt from a disruption. This means that the system is able to identify potentially disruptive events and adapt to the evolving circumstances.

These Fields were assigned specific Indicators, resulting in a list of 11 SecureGas Cross-KPIs (Table 4.1).

Table 4.1: SecureGas Cross-KPIs

Field	Indicator	Description	Metric	Target value
Reliability	False alert rate	Percentage of false alerts (both positive and negative) raised by the SecureGas system.	% (False alerts / Total Alerts)	< 5%
	Cross correlation	Percentage of cross correlated alerts raised by the SecureGas system.	% (Cross correlated alerts / Total alerts)	> 50%
	Latency	Time elapsed between the moment an incident occurs and the moment the alert is displayed in the Operational Picture.	Time (sec)	< 10 sec

Field	Indicator	Description	Metric	Target value
	Mean time to notify	Time needed for the operator to create an incident notification and send it to competent authorities/ stakeholders (escalation of incident).	Time (min)	< 3 min
Autonomy	Threat categories addressed	Number of different threats categories addressed by the SecureGas system *Threat categories: cyber, physical, cyber-physical, physical-cyber*	Number	4
	Automatic detection of threats	Number of different threat types automatically detected by the SecureGas system. *Threat types based on the URs (D1.1):* *Intrusion detection, TPI, Leak, Landslide hazard, Cyber*	Number	≥5
	Automatic decision-support	Percentage of alerts automatically linked to recommendations on crisis management and mitigation actions	% (Alerts with decision support / Total Alerts)	≥ 80
Interoperability	Transparent integration of users' legacy systems	Number of users' legacy systems that can be easily and transparently integrated into the SecureGas system. *Through this KPI the system's ability to integrate at least one legacy sensor/system is estimated.*	Number	≥1
Usability	Multilingual Interface	Number of different languages that the SecureGas user interface will be available	Number	4 (English, Italian, Greek, Lithuanian)
Resilience	Self testing capabilities (system health check)	Percentage of components/sensors that provide information to the operator - through dedicated alerts - about their status (not functioning and/or no communication)	%	90-95%
	Accuracy degradation percentage of a measurement value	The maximum decrease of accuracy (due to concept drift), before the model is retrained to adapt to background changes	%	20%

The CRS that served as reference for the elicitation of the SecureGas Cross-KPIs are presented in Figure 4.1. Although all the CRS (Table 2.2) are important enough to guarantee a high level of performance for the SecureGas system, only the Functional ones were deemed instrumental to its performance success and they were thus linked to KPIs. In addition, apart from the Functional CRS, the only Design CRS that was also correlated to a KPI was the CRS_DES_004 "Resilience" which focuses on the recovery mechanisms of the SecureGas system.

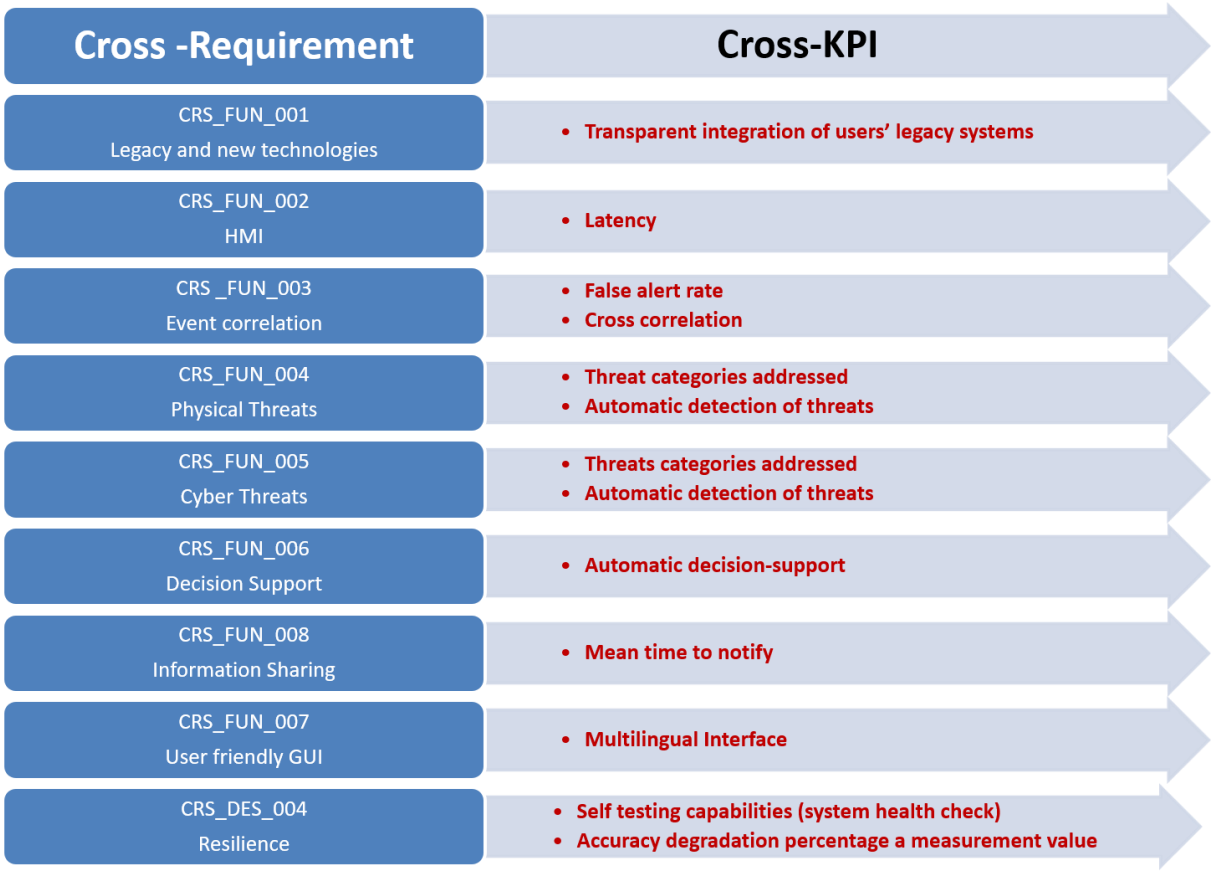

Figure 4.1: Cross-Requirements (CRS) link to Cross-KPIs

As mentioned in Section 2.3, the KPIs defined in the current deliverable were aimed at reflecting and having impact on all the Risk and Resilience phases of the panarchy loop (as being defined through the CM and CONOPS), so as to showcase how the core functionalities and performance indicators of the SecureGas system can add value to the enhancement of the resilience along the gas CI network.

Figure 4.2 presents the Risk and Resilience phases that are affected by each SecureGas-Cross KPI. Some of the Cross-KPIs are linked to one phase, some others to more, while the Cross-KPI "Multilingual Interface" is related to all the seven Risk and Resilience phases, since the enhancement of the usability parameters of a system has the potential to affect the entire security and resilience status of a CI network.

Figure 4.3 depicts the number of KPIs that have been identified for each Risk and Resilience phase, while Figure 4.4 shows the KPIs distribution to the activities taking place before, during and after an incident. Comparing the seven Risk and Resilience phases, the absorption phase (during the event), which encompasses the ability of a system to absorb shocks and continue operating, is the one that was linked to more KPIs (seven out of eleven KPIs). In general, as it can be observed through the

graphs, the SecureGas Cross-KPIs are mostly linked to the activities/phases taking place before the occurrence of an incident (prepare, detect, prevent) (approx. 47,1% of KPIs), although the SecureGas system do have performance parameters that are related to the post incident activities (response, recover, learn and adapt) (approx. 32.4%).

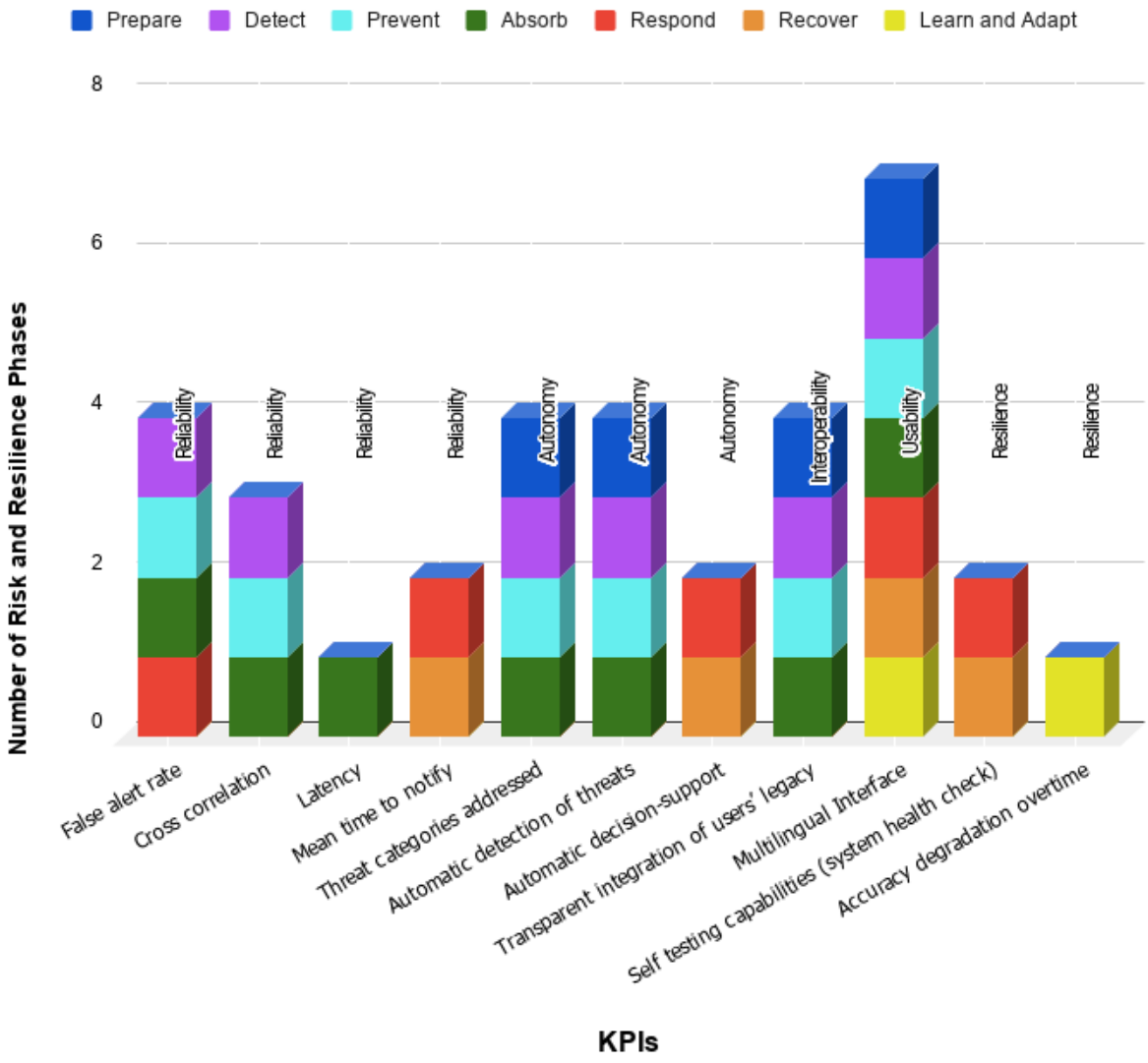

Figure 4.2: Risk and Resilience phases affected by each SecureGas Cross-KPI sorted according to the categories of Table 4.1

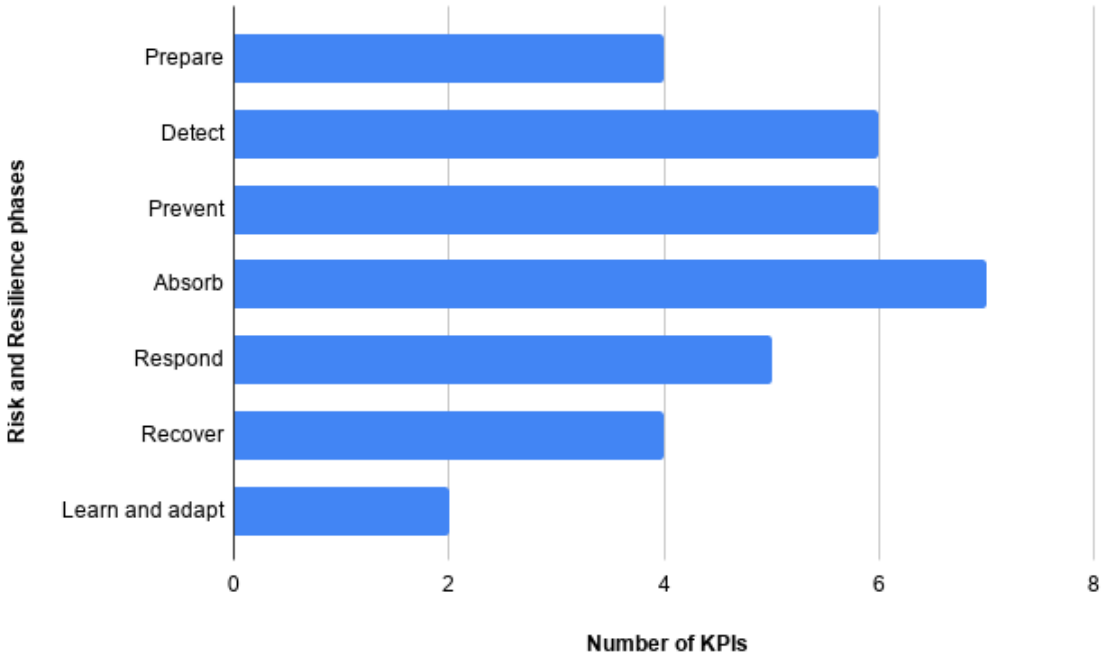

Figure 4.3: Number of SecureGas Cross-KPIs per Risk and Resilience phase

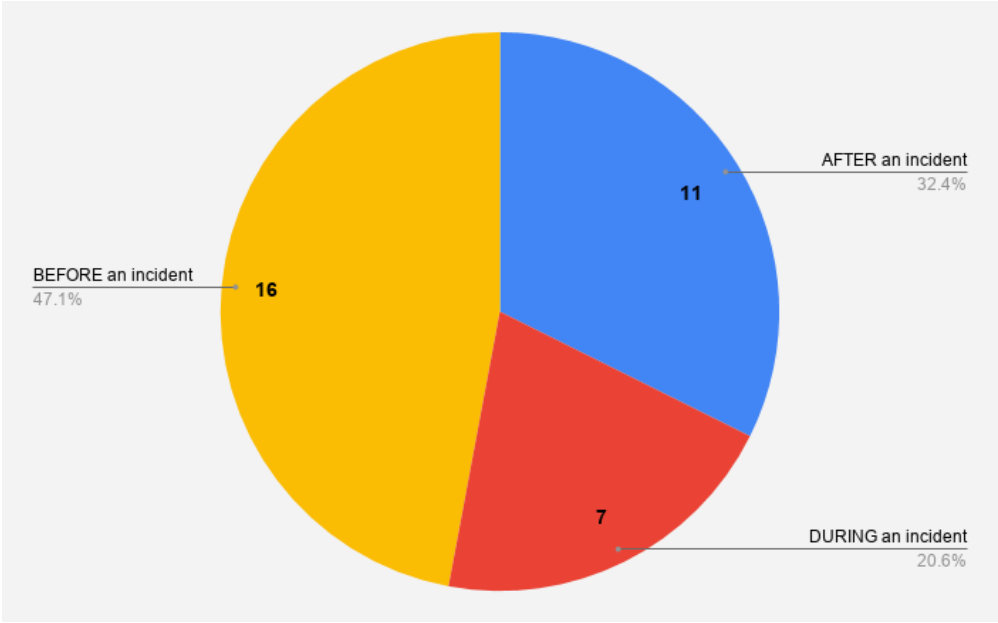

Figure 4.4: KPIs distribution to the activities taking place before, during and after an incident

5 CONCLUSIONS

The present deliverable D1.4 targeted the development of the SecureGas KPIs inventory. KPIs are considered as a measurable way to assess the SecureGas project's efficiency in reaching its key objectives and to evaluate the quality and performance of the proposed technical solution.

The KPIs identified in the current deliverable were classified into two categories: a) *the SecureGas component KPIs*, which reflect the key performance characteristics offered by each SecureGas component and b) the *SecureGas Cross-KPIs* that reflect the expected key functionalities of the entire SecureGas solution.

The methodological approach followed for KPIs definition was built on a bottom-up rational: a list of KPIs was firstly defined for each SecureGas component, and that list provided then the basis for the definition of the SecureGas Cross-KPIs of the entire system.

The SecureGas end-users (AMBER, DEPA, EDAA, ENI) provided a list of KPIs they are already applying to measure the effective implementation of their management systems and the secure and safe operation of their Gas CI network. That list, together with the already defined User Requirements of D1.1, the Technical Requirements of each component and the Cross-Requirements of D1.2, the Conceptual Model (CM) and Concept of Operations (CONOPS) of D2.1 as well as the High Level Reference Architecture (HLRA) of D2.2. served as input to the development of the KPIs inventory.

The KPIs inventory of D1.4 comprises 70 SecureGas component KPIs and eleven SecureGas Cross-KPIs, encompassing measurable and tangible metrics that are key to performance success. The SecureGas components cover mainly the Functional and Operational Dimensions, while only of them refer to the Security and Implementation Dimensions. With regard to the Cross-KPIs, they were classified into five Fields, namely Reliability, Autonomy, Interoperability, Usability and Resilience. In addition, the SecureGas Cross-KPIs managed to address all the Risk and Resilience Phases, namely a) Prepare, b) Detect, c) Prevent, d) Absorb, e) Respond, f) Recover, g) Learn and Adapt), showcasing that the envisaged SecureGas solution do have the potential to add value and foster the implementation of all panarchy loop steps and to further enhance the security of the Gas CI network before, during and after incidents occurrence.

The KPIs inventory developed in the current deliverable will be further customized, at a later stage, to address the specific requirements of each Business Case, formulating the so-called BC-KPIs. The BC-KPIs, which will be specified upon the definition of the Business Case scenarios, are the ones that will be finally measured at the three piloting activities (WP4, WP5 and WP6).

SecureGas

Securing the European Gas Network

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