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 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.

1 INTRODUCTION

After the introduction given in the current chapter including key working definitions, in chapter 2 the development of the Conceptual Modell is described. This involves the definition of system dimensions and their assembly resulting in the SecureGas conceptual model. Bases on this the focus of chapter 3 is then shifted towards the generation of Concept of Operations using the CM-framework. This chapter also include two CONOPS-examples using two application cases. Finally, the last chapter provides a conclusion in regard to the CM and the CONOPS respectively.

1.1 GENERAL BACKGROUND AND CONTEXT

Modern societies are becoming increasingly dependent on Critical Infrastructure (CI) systems to provide essential services that support economic prosperity, governance, and quality of life. Such systems are generally not alone but interdependent at multiple levels to enhance their overall performance. In the past couple of decades series of events have shown that this interdependency can cause cascading failures leading to catastrophic disaster and widespread human, environmental and economic losses.

Examples include electric line failures leading to wildfires in California simultaneously causing power outages, loss of lives and properties and spiraling into economic failures (a branch of PG&E filing for bankruptcy) [1]. Another example is the very recent attacks on the pipelines in Saudi Arabia which is causing not only disruption of supply but might also lead to armed conflicts between associated countries with impacts propagating up to United States of America.

There have been multiple events causing disruptions in the EU gas pipelines as well. As gas availability is critical to so many other CIs, a disruption in distribution can lead to series of failures or disruptions causing cascading disasters. The overall objective of the industry and the governments is to avoid such events and in case it occurs, to minimize the impact of such events. To achieve this a detailed knowledge of such events, state of the art of technological installments and operational readiness is needed. With this as a premise, the project SecureGas is intended to create an integrated environment of Gas CI and elements of the solutions as a foundation that will make the EU Gas CI more secure and resilient to threats and disruptions.

As a part of the project SecureGas, Work Package 2 (WP2) “SecureGas Conceptual Model and High-Level Reference Architecture” is designed to create an abstract conceptual model (CM) that encompasses all the components of the Gas CI and technical security solutions being provided. Furthermore, to ensure a proper understanding of the working of the entire model, a description of concepts of operations (CONOPS) of technical security solutions in the form of a template are defined.

There are three defined application cases for the project out of which two cases are used as examples to explain the model and associated working descriptions. The results of this modeling methodology are then used to create a High-Level Reference Architecture (HLRA) for the project which is intended to support the integration of SecureGas components, reuse of SecureGas results, use of SecureGas components in different contexts or in different design patterns. The modeling is delivered in this report while the HLRA is delivered in next reports.

As a result of Task 2.1 “SecureGas Conceptual Model and Concept of Operations” this first deliverable, as intermediate report, delivers a basic abstract model based on the current user and technical requirements as fixed in WP1 “SecureGas requirements, risks and threats identification”.

These inputs work as a guidance to navigate this project towards designing a model directly addressing end-user’s concerns thereby providing a targeted ready to use solution at the end of the project. The following section clearly introduces the task in hand and its scope.

1.2 AIM AND SCOPE OF DOCUMENT

1.2.1 Aim

The objective of the document is to define and implement a first version of the SecureGas Conceptual Model (CM) on how European (EU) Gas Critical Infrastructure (CI) has to be planned, designed, constructed, operated and maintained to be secure and resilient against the various threats (cyber, physical and a combination of cyber-physical). The CM constitutes a blueprint for secure and resilient Gas CI in EU.

At this point it is also very import to note that this document presents the current understanding of the project based on the user and technical requirements which were used as prime input for this work already delivered in WP1 via the Deliverable D1.1 "Organisational, Operational and Regulatory requirements" as well as via the Deliverable D1.2 " Technical requirements". The CM in itself is a continuous and iterative process. This document presents, at Month 4 of the project, an intermediate version of the CM and associated CONOPS. As the project transitions into the implementation phases, many aspects of this document will be further elaborated, clarified and changed to provide a comprehensive report on the CM and CONOPS as final deliverable D2.2 due at Month 21 of the project.

1.2.2 Scope

The document introduces two key technical terms, Conceptual Model (CM) and Concept of Operations (CONOPS). A small literature survey on both CM and CONOPS is provided thereby explaining the relevancy of them for Critical Infrastructure modeling and implementation of secure and resilient CI, in particular gas pipeline network. The document starts with introducing the CM for gas CI and then shifts to CONOPS. Towards the end it uses two application cases to explain the implementation of this modeling methodology in SecureGas CI.

1.3 KEY WORKING DEFINTIONS

In the following subsections working definitions are provided. They are ordered starting with more basic definitions and advancing to higher level concepts. Later definitions refer to earlier ones only.

1.3.1 Working definition natural gas supply system

System is defined as a set of known elements with known deterministic interactions and states. At least the system behavior should be accessible by (advanced) simulation.

Critical infrastructure (CI) is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disaster, terrorism, criminal activity or malicious behavior, may have a significant negative impact for the security of the EU and the well-being of its citizens [2].

The gas supply system comprises of all system elements that are needed to provide natural gas to the end user, including organizational and economic dedicated units. Thus defined gas supply systems are critical infrastructures (CI) systems.

1.3.2 Working definition gas infrastructure security system

The gas infrastructure cyber-physical security system comprises of all elements of the natural gas supply system that are dedicated to analyze and control the overall risk and to improve resilience regarding potential physical, cyber and/or cyber-physical risk events.

1.3.3 Working definition Conceptual Model (CM) and CM development

The Conceptual Model (CM) of the gas supply system is an abstract description model. Each system component and behavior can be characterized using a set of dimensions. The abstract description comprises a dimensional analysis of key aspects of the system regarding its static and dynamic (behavioral) properties.

Dimensions of description include:

1. System layers, e.g. physical, technical, cyber, organizational, policies

2. System elements considered, e.g. pipeline tube
3. Value chain phases, e.g. production, cleaning, storage, transmission, distribution
4. Persons involved or responsible, e.g. worker, team lead, command and control, operator, third party, decision maker, company board members, representative of certificate bodies, policy maker
5. Threats addressed, e.g. seismic, flooding, sabotage, terroristic explosion, cyber-attack on SCADA system
6. Risk and/or crisis management phases covered, e.g. context analysis (know context, objectives identification, knowing stakeholders), system understanding and modelling, risk identification, risk computation, resilience computation, risk evaluation, resilience evaluation, mitigation and improvement measure selection, mitigation and improvement measure implementation, event detection, event absorption, response, recovery, system adoption, system improvement
7. Live cycle phases of gas supply system addressed, e.g. design, construction, operation, maintenance, improvement, dismantling

Example for the description of a system element using the abstract system dimensions where relevant: A gas infrastructure tube belongs to the physical layer, e.g. to the transmission system, mainly workers are directly interacting with it, and it is mainly affected by physical threats.

Example for the description of a security system property using the abstract system dimensions where relevant: UAVs have the capability to detect gas leakages of gas transmission infrastructures. The conceptual model development describes an approach to define for a given gas supply sub-system, e.g. parts of a transmission infrastructure, a valid conceptual model sufficient for CONOPS generation.

1.3.4 Working definition Concept of Operation (CONOPS) and CONCOPS development

A concept of operations is a document describing the characteristics of a proposed system from the viewpoint of an end-user, who will use that system in his daily work activities or who will operate or interact directly with the system. It is used to communicate the system characteristics to all stakeholders. CONOPS are widely used in the military, governmental services and other fields.

The value of CONOPS to system development is multi-faceted wherein the CONOPS plays a role across the entire life-cycle, from need identification, to system inception and development, to system disposition and disposal. The CONOPS provides an analysis that bridges the main gaps between the users' operational needs and the developer's technical specifications, without scrutinizing technical issues.

Moreover, the CONOPS documents integrates system's characteristics and users' operational needs in a manner that can be confirmed by the user without requiring any technical knowledge.

A CONOPS should also define the roles of the stakeholders involved throughout the process and include the following [3]:

- Statement of the goals and objectives of the system;
- Strategies, tactics, policies and constraints affecting the system;
- Organizations, activities and interactions among participants and stakeholders;
- Clear statement of responsibilities and delegation of authorities;
- Specific operational processes for fielding the system and
- Processes for initiating, developing, maintaining and retiring the system.

The following reference documents are of importance

- The first standard was 1362 -1998 - IEEE Guide for Information Technology - System Definition - Concept of Operations (CONOPS) Document [4]
- It was superseded by the document 29148-2011 - ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes --Requirements engineering [5].
- Following, the 2012 AIAA revision proposal Guide: Guide to the Preparation of Operational Concept Documents (ANSI/AIAA G-043A-2012) (Revision of G-043-1992) [6] .
- Currently, the last version IEEE 29148-2018 - ISO/IEC/IEEE International Standard Systems and software engineering -- Life cycle processes -- Requirements engineering [7]

In a nutshell, the CONOPS may use the conceptual model (CM), also through several use case/scenarios definition, to describe in detail application options of the gas supply security system to ensure overall acceptable risk control and resilience of a gas supply system or subsystem. CONOPS describe how to use technical solutions in the intended way most efficiently. They should be understandable by users as well as developers.

An example is the detection of physical disruptions: The capability to detect physical disruptions in pipelines using optical fibers monitors the physical system layer. The capability itself also resorts to the technical and cyber layer for implementation. It is mainly relevant for operational centers and repair teams. The capability is relevant for the detection phase and supports fast response, it mainly belongs to the sensing capabilities and is most relevant for daily maintenance.

1.4 RELATION TO OTHER WORKPACKAGES AND TASKS

The inputs of the current task, Task 2.1, are the organizational and operational requirements that were provided as output from Task 1.1 (reported in D1.1 – public deliverable) as well as abstract information on first versions of the output of Task 1.2 regarding technical requirements. Further inputs for the current task are reference conceptual models that can be taken from literature as well as the above listed general understanding on CONPOS.

The output that is provided from the current task Task 2.1 is the conceptual model (CM) to be used as blue print on how conceptually Gas CI have to be designed, built, operated and maintained to be secure and resilient using graphical models as well as guidelines for its implementation.

The current task will also define the CONOPS approach and examples that serve together with the CM as input for Task 2.2, which includes the development of the SecureGas High-Level Reference Architecture (HLRA).

2 CONCEPTUAL MODEL

A Conceptual Modeling (CM) often is perceived as a way of introducing the process of modeling a system, by concentrating on a reduced abstract appreciation of that system, with a necessary reduction in the number of affecting variables and relations contributing to the model. The definition of CM is highly dependent on the context it is being used in.

The following section presents a literature survey performed to provide an understanding of the various ways CMs are used. The section 2.2 defines CM for present context of SecureGas. This section provides the dimensions used in the present CM for gas critical infrastructure. To provide a complete context, gas life cycle phases (section 2.3), gas system elements (section 2.4), gas value chain dimensions (section 2.5) have been explained briefly. With this as contextual information, a brief detail of threat events encountered is presented motived from the EGIG report. This chapter then proceeds to introduce resilience management. Finally this chapter details the risk and resilience capabilities addressed by SecureGas (section 2.8) and concludes with detailing the persons affected in the entire end-to-end infrastructure (section 2.9) and recommended gas infrastructure CM (section 2.10).

2.1 LITERATURE REVIEW ON CONCEPTUAL MODEL IN THE CONTEXT OF CONOPS FOR CRITICAL INFRASTRUCTURE

In general conceptual modelling can be seen as the process of abstracting a model from the real world. Based on the problem situation, the modeler decides which aspects of the real world to include and which not. In this process, decisions have to be made regarding the scope and level of detail of the model. This further translates into making assumptions and consequently simplifications to be made to the model.

In simply terms, a conceptual model (CM) captures the basic elements of a system, and the interaction of those elements, which provides an overview of the system being modeled. The "conceptual modeling" as a term is an abstraction that materializes based on the context it is being used in.

Following are some cases where Conceptual Modeling was used for Critical Infrastructure (CI) or systems involving CI.

1. Sokolowski [8] describes CM from 2 different perspectives, one is the description function that is representative of something that already exists while the second is the prescription function which is representative of something that, if it did exist, should follow a prescribed theory, or set of defining axioms. The perspective model also represents some phenomena or data, but rather than being based on some empirically observable part of the world, it is based on a theory. In this way, an abstracted representation is made of what should exist, if the theory were to be followed. For both the approaches, the paper concluded that taking these approaches ensured highlighting patterns for development leading to component reuse, identification of crucial checkpoints for validations and eventually generation of a model that ensured the implementations specifically follow the intended use of the modeled system.
2. Ouyang [9] reviews the conceptual and qualitative studies about CI systems and their interdependencies as well as their modeling and simulation approaches in the literature. Existing approaches were broadly grouped into six types as empirical, agent-based system based, network based and others. The comparisons were based on the following criteria:
    a. Quantity of input data
    b. Accessibility of input data
    c. Types of interdependencies
    d. Computational complexity
    e. Maturity

    The implementation of all the methods mentioned needed a huge amount of input data. The agent based models needed a large variance of data types, for example policy decision variables, human behavior variables. Flow-based methods needed detailed information about component characteristics which are usually related to the privacy and security issues and are difficult to obtain. System based and network-based approaches needed much higher computational time. The

most important conclusion forms the perspective of modern modeling techniques was that none of these techniques incorporated the concept of resilience, hence none of the models could be directly used for CM of SecureGas.

3. Kotiadis [10] discuss about the processes involved in conceptual modelling. The paper uses an example of Health and Social care system design to explain the different processes. It focuses on two conceptual modeling processes: knowledge acquisition and model abstraction. It further introduces Soft Systems Methodology (SSM) as a problem structuring approach. As per the research there are three steps involved in creating a CM:

    a. System description

    b. Conceptual model

    c. Computer model

    The paper divides the CM into 2 distinct elements namely problem domain and model domain. Knowledge acquisition involves study of the problem domain to acquire knowledge about the real world and to derive a system description which leads to making assumptions and documenting them. Within the model domain one needs to abstract a CM from the system description. The case study provides a good starting point for understanding the CM from an implementation point of view. This would be particularly useful in the next phase of the project.

To summarize this section, existing research involving CM for CI, types of modeling for CI and methodologies within CM were studied. This is considered as background information for the present approach.

The type of modeling introduced in the present report for Gas CI is unique in the perspective that it tries to perform the knowledge acquisition in the problem domain using a dimensional analysis of the CI and solution. The present approach for instance covers static and dynamic system aspects. It also covers different types of (simulative) modelling on the level of description. It covers in addition existing systems and systems that should be developed.

Furthermore, the unique coupling of CM and CONOPS in the beginning of the product development phases provides a unique methodology that ensures not only directed implementation of the solutions but also a clean description of work of these solutions to enhance effectiveness of these solutions.

2.2 CONCEPTUAL MODEL AS DIMENSIONAL ANALYSIS

The CM is supposed to capture the entire gas system including the corresponding security system. It is intended to achieve the CM by analyzing all dimensions of the system to identify the complete domain of action/influence. Spanning this domain using dimensions enables a systematic structuring such that a certain degree of completeness can be guaranteed.

The dimensional analysis also enables functional decomposition of the CI. This decomposition is essential to identify the functional components of the CI. The advantage of this activity is that it breaks up the complexity of the system into elements that can then be covered by different technical security solutions.

The guiding principles of selecting dimensions for this dimensional analysis are:

- Coverage of all system aspects;
- Orthogonality, i.e. the overlap of a pair of Dimensions should be as small as possible to ensure that there are no Attributes that appear along several Dimensions;
- It can be decided whether Dimension and Attributes are relevant and when not;
- Accepted by users and science.

2.3 LIVE CYCLE PHASES OF GAS SYSTEM INCLUDING THEIR RELATION TO RISK AND RESILIENCE MANAGEMENT

In the present section an attempt is made to demonstrate the main dimensions that should be considered during the implementation of a "Panarchy Loop" in all Life Cycle phases of a Gas system.

As defined in description of action (DoA), inter alia the "panarchy loop" is assumed to be the basis for the Conceptual Model (CM) of SecureGas project. The panarchy loop is intended to link Resilience and Disaster Risk Management (DRM). This covers risk control and resilience assessment and improvement. The implementation of a full Disaster Risk Management Cycle would thus certainly necessitate implementing all the Pre-Hazard (left part in the figure below) and Post-Hazard phases (right part of the figure below) or activities of risk management. **Error! Reference source not found.** illustrates this proposed approach.

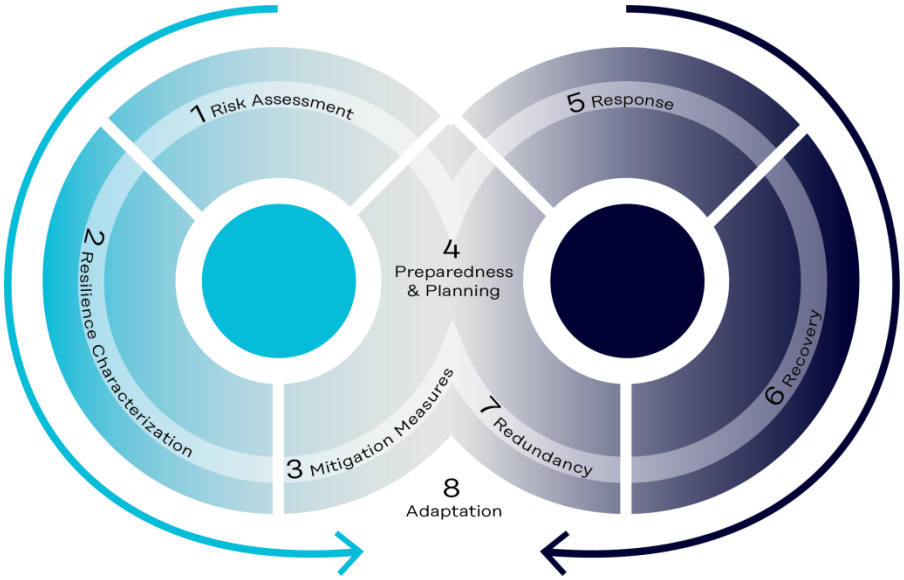

Figure 2.1: SecureGas Conceptual Model linking Resilience and DRM in a panarchy loop (Source RINA)

Resilience can be seen as the link or even the capability to link the Pre-hazard activities with the relevant Post-Hazard activities or phases. In the present framework of analysis, the "Pre-hazard" activities are meant to be all appropriate measures and provisions that take place before an incident occurs, while the "Post-hazard" activities are meant to be those following an incident. In other words, Pre-hazard" activities can be seen as "Pre-security incident" actions and provisions while "Post-hazard" activities as "Post-security incident" actions. Such provisions, measures or actions are necessary and should be taken in order to prevent and manage in a complete and appropriate manner any relevant security threat, security event or incident.

When a security threat or hazard has not been identified or sufficiently prevented and controlled, there is always the risk of an incident to occur with adverse effects and potentially considerable impact to the public, the capital or the environment. The extent and severity of the incident impact or consequences depend on the threat importance (its potential to create harm) and the vulnerability of the CI to which the threat is targeted.

In those cases where sufficient and effective preventative measures and provisions (technical, organizational, managerial) can be implemented, are in place and are in turn kept available and operational, the risk of an incident with adverse effects can be reduced to tolerable levels. Such measures can be considered within the "Pre-security incident" provisions and actions.

Moreover, in those cases where further controlling measures, mitigation of effects and emergency measures are identified, can be implemented, and are in place available and functional, the extent of consequences of a potential incident can be reduced to minimum possible. Such measures can be considered within the "Post-security incident" provisions and actions.

All above mentioned provisions, measures or actions are largely identified in security/safety management methodological approaches and in fact indicate the phases of a standard Security Management System (SeMS) with groups of security provisions and procedures.

The relevant phases of the Pre-Hazard and Post-Hazard loops make an integral part of the overall "panarchy loop". This "panarchy loop" as a whole has been postulated to be mandatory for the full implementation of the Disaster RISK Management Cycle (DRM) adopted by SecureGas project.

The relevant phases of the Pre-Hazard and Post-Hazard loops (8 in total) are bound to include the following elements (in sequence) of an overall risk management cycle and to apply the principles of an inclusive Conceptual Model (CM) for Resilience and Security in the SecureGas project:

Pre-Hazard ("Pre-security incident") loop phases

(1) Risk Assessment
(2) Resilience Characterization
(3) Mitigation measures
(4) Preparedness and Planning

Post -Hazard ("Post-security incident") loop phases

(5) Response
(6) Recovery
(7) Redundancy
(8) Adaptation.

In SecureGas the standard Life Cycle (LC) phases of any asset in a CI are set out to be compliant to Asset Management standards, namely ISO 55000:2014. As such the life of an asset begins with the conception and the initial stages of the asset design and ends with the decommission of the asset itself, moving across construction, operation and maintenance as visualized in the Infrastructure Governance cycle. To summarize the following 4 phases in the LC of a gas CI are considered by SecureGas:

a) Evaluation and Planning
b) Design
c) Construction
d) Operation & Maintenance

Any Asset Management processes of a CI should thus be seen within those phases and involved procedures, see

, where the different dimensions and forms (from circular to oval) assumed by the phanarcy loop depends on the relevance and effectiveness of its phases according to the phase of the LC of the asset.

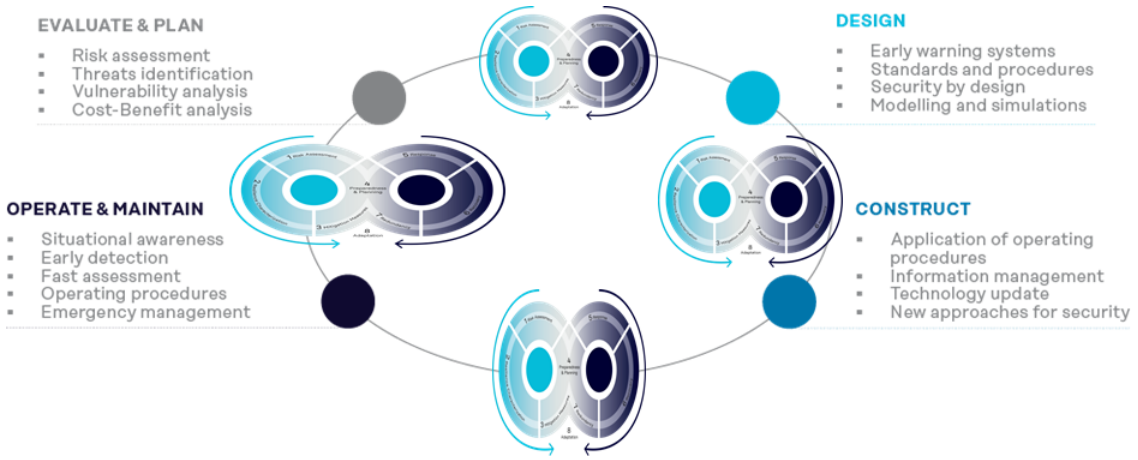

Figure 2.2: Integration of the Panarchy loop into an Asset Management process across the Life-Cycle of an infrastructure (source RINA)

Security breaches can cause deviations that are organized in one or more of the above LC phases of a CI. Deviations can be seen as deviations from either normal design, or construction, or operations or maintenance.

The provisions and measures included within a standard SeMS, being either preventative, controlling, correction, mitigation or emergency, are bound to address all possible deviations that can occur within a DRM cycle.

The standard Life Cycle (LC) phases of any asset in a CI (how a CI is governed) are used as distinct domains (time-oriented sets of actions) in which the CM of SecureGas should seek to discover all possible underlying causes of the conceived security breaches. To this end, the following question should be posed in order to identify which are the relevant LC phases for the examined CI asset:

"May a security breach have as underlying cause an error (or shortcoming/failing) in the asset's:

- Design?
  or
- Construction?
  or
- Operation?
  or
- Maintenance?

An additional LC phase, "Evaluation and Planning", can be considered before the Design phase. LC phases can also be analyzed further or grouped as necessary according to the needs of the user. Options include for instance phases like Extension of gas supply system or Dismantling.

After we conclude with the CI's relevant domains for seeking errors/failings and underlying causes of security breaches, the next step is to systematize the ways in which we should proceed with the analysis to identify and prevent such errors. Four main "reviewing procedural sequences" are distinguished and used to group prevention and recovery measures in key areas, such as,

A. Hazard review,
B. Checking and supervision of tasks,
C. Human factors review, and
D. Routine inspections and testing (including surveillance)

To this end, the following question should be posed in order to identify which are the ways or "reviewing procedural sequences" to follow per case of examined CI.

"Can an error, shortcoming or failing of the CI be prevented by:

- Hazard review?
  or by
- Checking and supervision of tasks?
  or by
- Routine inspections and testing?
  or by
- Human factors review?

By answering the above questions, the areas of importance for the CM can be delineated.

Prevention and recovery measures can then be grouped in key areas (or areas of importance) per asset ot CI.

A methodological and systemized approach is proposed (based on a standard inspection management system), to identify the ways to proceed in reviewing the underlying causes of security breaches and preventing them from occurring. In this approach, all relevant LC stages of an asset of a CI system are taken on board and are strongly linked with the overall risk management phases or the main Pre-hazard phases (Pre-security incident phases) of the "Panarchy Loop".

Possible sources of shortcomings leading to LOC (Loss of Containment) or failure of the CI are depicted in the relevant cross sections in the matrix of the above key-areas vs. the Gas Life Cycle Stages of a relevant CI.

In Table 2.1 below as example by answering the above questions and by assuming that all Gas LC phases of an asset are relevant to be examined. The root symbol "√" stands for potential causes.

Table 2.1: Areas of importance for the CM identified after assessment of Life-Cycle (LC) phases of a Gas CI

	(Evaluation and Planning) PLAN	Design DESG	Construction CONSTR	Operation OPER	Maintenance MAINT
Hazards review RA (Risk Assessment)	√ RA-PLAN	√ RA-DESG	√ ReAssess-RA-CONSTR	√ ReAssess-RA-OPER	√ ReAssess RA-MAINT
Checking and Supervision of tasks		?	√ SuperVis SPRV-CONSTR	√ SuperVis SPRV-OPER	√ SuperVis SPRV-MAINT
Human Factors Review	?	?	?	√ HFR-OPER	√ HFR-MAINT
Routine Inspections and Testing including Surveillance			?	? INSP-OPER (SURV)	√ Routine Inspect INSP-MAINT

The above example demonstrates that Hazard reviews and Risk Assessment is more likely to support identification and prevention of Gas CI failings during the whole life cycle of the CI. On the other hand, Human Factors reviews and Routine Inspections and Testing (including Surveillance) are rather more focused in identifying and preventing Gas CI failings during the Operation and Maintenance LC phases of the CI. It can thus be concluded that Hazard reviews and Risk Assessment are more important during Planning and Design LC phases of a Gas CI.

It follows the mapping of the areas of importance based on end user's needs:

Key areas of importance for the CM of SecureGas are further applied to identify important Threats per type of CI asset e.g. Pipeline body, valve stations, etc. and per LC phase.

Possible sources of threats leading to a security breach in a CI asset are depicted in the cells of the matrix below (**Error! Reference source not found.**) per life cycle phase of the CI and per type of asset. Similar questions such as the above should be posed, i.e.:

"Can a threat to a CI asset be identified, foreseen or prevented by:

- Hazard review?
  or by
- Checking and supervision of tasks?
  or by
- Routine inspections and testing?
  or by
- Human factors review?

In Table 2.2 below a number of important threats have been identified as example, by answering the above questions and by assuming that only selected Gas LC phases of an asset are relevant to be examined. The identification of Threats per type of CI asset and asset LC phase, can be further supported by specific incident statistics. For instance, Third Party Interference (TPI) as a Threat to the main Gas Pipeline body of HP Transmission networks can be rather foreseen and prevented by **Routine inspections and testing (Surveillance)** of the Pipeline. Similarly, since numerous past incidents in O&G pipelines occurred due to Design shortcomings, relevant Threats can be identified and prevented by appropriate **HAZARD reviews and Risk Assessment.** Past incidents in O&G pipelines can also indicate Threats during Operation and Maintenance phases identifiable through **Human Factors Reviews or Routine inspections and testing (Surveillance).**

Table 2.2: Important Threats for a CI asset identified per LC phase and per type of Gas asset (example)

	Planning	Design	Construction	Operation	Maintenance
HAZARD REVIEW - RA					
Key Areas of Importance	RA-PLAN	RA-DESG	RA-CONSTR	RA-OPER	RA-MAINT
CI asset					
PIPE BODY high pressure (HP) natural gas (NG) Transmission Infrastructure	Routing alternatives	Threat 1 Threat 2			
PIPE BODY low pressure (LP) NG Distribution Infrastructure		Threat 3 Threat 4			
VALVE Stations					
PUMP Stations					
Other Stations/Installations					
Checking and Supervision of tasks SPRV					
Key Areas of Importance	SPRV-PLAN	SPRV-DESG	SPRV-CONSTR	SPRV-OPER	SPRV-MAINT
CI asset					
PIPE BODY HP NG Transmission Infrastructure					
PIPE BODY LP NG Distribution Infrastructure					
VALVE Stations					
PUMP Stations					
Other Stations/Installations					
Human Factors Review HFR					
Key Areas of Importance	HFR-PLAN	HFR DESG	HFR -CONST	HFR- OPER	HFR- MAINT
CI asset					
PIPE BODY HP NG Transmission				Threat 5	Threat 7

Infrastructure					
PIPE BODY LP NG Distribution Infrastructure					
VALVE Stations				Threat 6	
PUMP Stations					Threat 8
Other Stations/Installations					
Routine inspections and testing (Surveillance)					
Key Areas of Importance	INSP-PLAN	INSP-DESG	INSP-CONST	INSP-OPER (SURV)	INSP-MAINT
CI asset					
PIPE BODY HP NG Transmission Infrastructure				Third Party Interference (TPI)	Threat 9
PIPE BODY LP NG Distribution Infrastructure					Threat 10
VALVE Stations					
PUMP Stations					
Other Stations/Installations					

Through the above considerations, it can be demonstrated that the "Panarchy Loop" including Pre-Hazard and Post-Hazard phases, being the basis for the Conceptual Model (CM) of SecureGas project linking Resilience and Disaster Risk Management (DRM), can be implemented in all Life Cycle phases of a Gas system and for all types of CI assets. When a "Panarchy Loop" is systematically implemented, useful results can be extracted concerning identification of important Threats and ways to prevent them.

In summary, the examples shows that the flowing system life cycle phases can be distinguished and used with advantage for overall secure gas system assessment pre and post hazards:

1. Evaluation and planning, including extension planning
2. Design
3. Construction
4. Operation
5. Maintenance
6. Dismantling

It was also shown that the panarchy approach is suitable to combine risk control and resilience assessment and improvement processes.

2.4 ELEMENTS OF A GAS CI

Gas CI consists of a series of elements involved in transportation, treatment (sweetening) and conditioning of gas over the entire gas infrastructure. This includes a system of pipes, compressor stations, meter stations, storage, distribution infrastructures and other installations.

Natural gas are pressurized into liquids known as Natural Gas Liquids (NGLs) and then transported over the pipelines. The pipelines involved in transmission are constructed out of carbon steel. In order to maintain and regulate pressure in these pipelines, multiple compressor stations are involved in the distribution infrastructures. To enable the distributors to keep track of the volume transferred, metering stations are placed at suitable intervals. Gas storage is an important and critical part of the system.

The following subsections list some of the important components of the gas CI and provide a brief overview, respectively.

2.4.1 Trasmission infrastructure

Transmission of natural gas is transportation of natural gas via gas transmission system mostly comprised of high-pressure pipelines, except for the production process pipeline network and part of the high-pressure gas pipelines mainly used for the local distribution of natural gas, designed for the delivery of natural gas to consumers, except for gas supply.

The transmission system is comprised of gas transmission pipelines, gas compressor stations, gas metering and distribution stations, cathodic protection systems installed to prevent corrosion of the pipeline, remote data transmission and telecommunication systems.

With a view to ensuring the reliability, efficiency and safety of the gas transmission system operation, the scheduled repair and maintenance works are implemented on an ongoing basis. The gas transmission pipeline engineering design, construction as well as operation and maintenance works are performed according to detailed rules and regulations. Depending on the operational factors, technological layout, results of the regular maintenance operations, additional attention is being paid to the riskiest gas transmission pipelines. Gas pipeline intelligent pigging (internal diagnostics) works are carried out periodically.

2.4.2 Distribution infrastructure

According to Zanjirani Farahani [11] the distribution infrastructures enable the transportation of gas to the end user. Local distribution companies (LDCs) receive the gas in city gates, transfer points from transmission pipes to LDCs, and deliver it to individual customers. This delivery is done with the help of an extensive network of small-diameter distribution pipes throughout municipal and suburban areas. End users of natural gas from LDCs are residential, commercial, and industrial sectors and power-generation customers. Note, however, that some large commercial and industrial customers receive natural gas directly from the high-pressure pipelines.

2.4.3 Pipeline

The pipeline is one of the main means of transportation and consists of a tubular duct having the purpose of safely bringing the gas from one facility to another; these can operate in high, medium or low pressure. In general, the higher the pressure the greater the pipe section and the flow transit and therefore it is reasonable to say that from a supply chain perspective the importance of a section or segment decreases with pressure. In fact, major disruption to large pipelines can leave entire areas without supply for hours or even for days.

The most critical outcome of a failure is rupture with subsequent leakage of hydrocarbons; causes can be:

1. Third Party Interference (TPI) – i.e. sabotage and theft;
2. Leaks due to lose flanges (connections and T-Sections) or internal/external corrosion;
3. Impact of natural events (e.g. landslides).

Possible impact of landslides is typically faced during the design of the pipeline. Geological and geotechnical data are collected in order to evaluate slope stability along the pipeline route. Although pipeline route aims at minimizing landslide risk, landslide impacts may still be present during the operation phase. For areas where the landslide risk is known to be present, mitigation actions (e.g. slope stabilization intervention) are typically undertaken if feasible from a technical and economical point of view.

Where interventions are not achievable, slope monitoring remains the sole countermeasure to reduce consequences on the asset, community and environment. The monitoring system will vary depending on the soil/rock conditions, expected failure mode, triggering mechanism, pipeline route, etc. Standard monitoring system includes soil pore pressure measurements (piezometers) and soil displacement measurements (inclinometers). More advance monitoring systems may include evaluations of other soil properties (e.g. moisture content) or monitoring/predictions on triggering events (e.g. rainfall).

However, even small discontinuities in the surface within pipes as caused by TPI are critical since internal corrosion massively increases at such exposed bulge areas.

2.4.4 Pumping station

The pumping station is the heart of the distribution system at all levels (midstream and downstream); they can be of different types, but the most common ones make use of several centrifugal compressors in series as the required pressure often cannot be achieved with a single compression cycle.

Knock-out (KO) drums are used between different compression stages to cool down the gas and collect the resulting mixture of heavier hydrocarbon and water. The transported gas is dehumidified by means of demisters that prevent the moisture reaching the compressors. Should the process be compromised in any of them, the compressor might experience cavitation and break with disruptive effects; moreover, chemically aggressive agents might initiate corrosion inside the pump.

2.4.5 Comand and control station

The metering station calculates the heating power of the provided gas by means of a pair of parallel gas chromatographs. The quality of the gas is measured by the difference in composition of the two samples provided; if compromised the process could yield unreliable results with subsequent economic damage.

2.4.6 Storage system

Cryogenic storage is necessary for loading/unloading operations and work as peak shaving facilities. The storage tanks must maintain the LNG at a temperature of -164°C. The outer shell can be made of cryogenic steel or pre-stressed concrete that must be capable of dealing with operation at very low temperatures. A vapor barrier is fitted between the external cladding and the perlite insulation.

The critical issue is to maintain the temperature as low and regular as possible in order to avoid overstress induced by thermal deformation and overpressure. Compromising the temperature control can thus cause major disruption from the structural and process perspective – especially Boil-off Gas (BOG) handling.

Faults and attacks on thermal control devices or insulation can require extraordinary maintenance that can only be initiated after emptying and sanitizing the tank with major setbacks on the overall logistics and durability of the facility itself. The service life of LNG storage tanks is in fact significantly reduced by unplanned maintenance as this imposes significant thermal stress. On average LNG tanks shall not face more than three full loading/unloading cycles for extraordinary maintenance.

Substantially the critical elements of an LNG storage tank are the devices used to control the temperature (including insulation). Their failure can compromise the successful send out and the stability of the tank itself.

2.5 GAS VALUE CHAIN DIMENSIONS: PRODUCTION, STORAGE, TRANSMISSION, AND DISTRIBUTION

2.5.1 Extraction

The first phase of the gas production process is the extraction from the well. The well consists of a borehole which the hydrocarbon mixture runs through to the surface. The key elements of the well are:

1. The Blow Out Preventer;
2. The Christmas Tree;
3. The Corrosion Inhibitors Injection;
4. The Lift System.

2.5.2 Treatment

In this section different components of the gas treatment process are analyzed.

Separator:

When gas is extracted as an element of a multi-phase mixture it must be separated from liquid components (oil and water). This is conducted in a pressure vessel, normally in the shape of a barrel that can be orientated both vertically and horizontally.

The separator fulfils its purpose in four stages:

1. Inlet
2. Flow distribution
3. Gravity coalescence
4. Outlet

The gas enters the chamber through an appropriate device that initiates separation. In most cases they are inexpensive, especially because part of the gas would already be separated inside the pipeline. However, their adequate choice is key to the overall performance as the use of the wrong device would lead to foaming with associated loss of efficiency.

The flow distribution consists of a plate that regularizes the flow whilst demisting and breaking the foam of the mixture. The net free area of the plate shall be sufficient as to avoid solid build-up on the upstream side.

In this zone the water is separated from the oil. Water is heavier than oil and will sit at the bottom of the mixture and will be separated by means of vertical plates that will also increase the shearing of the foam on the surface and improve demisting performance.

Finally, the water is flushed out, the oil and the gas are recovered at the outlet sections.

Normally sensors and controls for the operation of the separator are located at the inlet and outlet sections of the separator.

Sweetening:

The sweetening process is the process through which acids and oxides, mainly H_2S, CO and CO_2, are removed by means of an amine shower. Amines are regenerated by means of a recovery process through which the amines are boiled and separated from the acidic content of the mixture.

The sweetening system presents different types of critical components:

1. The gas pressure and relevant measuring sensors;
2. The gas inlet and outlet channels;
3. The temperature of the amine boiler.

The last one in particular is extremely important as sabotaging the recovery system can induce cracking of the amine into its elementary components which are highly reactive and corrosive. This could lead to major disruption with environmental and human safety (HS) implications.

Compromising the outlet channels might instead increase pressure in the absorber with severe health and safety implications.

2.5.3 Storage

The most important type of gas storage is in underground reservoirs. There are three principal types — depleted gas reservoirs, aquifer reservoirs and salt cavern reservoirs.

Gas storage is principally used to meet load variations. Gas is injected into storage during periods of low demand and withdrawn from storage during periods of peak demand. Balancing the flow in pipeline system ensures that pipeline pressure are kept within design parameters thereby ensuring operational integrity of the pipeline.

In the shipment department, storage is relevant to meet contractual balance. Without access to such storage facilities, any disturbance in inflow would directly impact the delivery causing heavy penalties or loss of business. Storage is also used as a buffer to balance the periodic mid and long term fluctuations in demand and supply in the overall business architecture. A classic example of this is the demand fluctuations in summer and winters.

The benefits of gas storage can be put into various other situations anywhere between major accidents to local/regional political stand-off or disturbance. In absence of storage stations, it will be impossible to maintain a continuous supply gas to the end-users in such a widely spread infrastructure topology [12].

2.5.4 Transmission and Distribution

The gas production phases can be divided in mainly three classes:

1. Upstream where the gas is extracted from the reservoir and processed– i.e. produced. This phase actually involves explorations and field development as well but these are not included in the current scope of the project;
2. Midstream generally includes the transport and storage. The gas is mainly shipped by means of high/medium pressure pipelines to downstream facilities, or other transportation media in case of LNG (tankers, trucks and rails);
3. Downstream involves the final refinement and distribution of the gas including low pressure transport to the final users and sale.

2.6 THREAT EVENTS TYPES

In order to generate an exhaustive threat list, different scientific journals describing existing threats and hazards are being studied. There are different reports and databases which contain information on surveys performed ranging from 1960 to 2016 by different commissions to document the accidents related to operational pipelines. The primary source of the following study is the European Gas pipeline Incident data Group (EGIG) report.

Based on the location, geo-politics, climate and so on, hazard sources may be related to a number of activities during the lifetime of the pipeline system, including design, routing, materials, welding, corrosion protection and construction, operations, pressure control, testing and hand over.

Several types of incidents have been identified by the gas and oil pipeline industry in the past according to their initial causes (EGIG). They are more frequently classified in the following seven cause categories:

1. External interference or third-party activity including political/geo-political interference
2. Corrosion
3. Construction defect and mechanical or material failure
4. Natural hazards
5. Operational error
6. Cyber attacks
7. Other or unknown errors

Based on the annual failure frequency data, the proportion of incidents caused by corrosion, external interference, construction/material defects or other unknown causes for these incidents have been analyzed in the EGIG report. The analysis found that external interference remains the major cause of gas leakages in the European and US gas transmission infrastructures.

Corrosion and construction/material defects are incident causes with particular importance in the gas transmission infrastructure of the former Soviet Union and the liquid pipeline networks in Europe and the US. Corrosion is becoming important for European gas infrastructure with aged lines (30 years or more). Extended gas transmissions as in the former Soviet Union with large diameter lines (e.g. 5.6”) experiences frequent failures mainly due to mechanical defects and corrosion, while external interference is of considerably lower importance (17%). This may be so because of the highly dispersed network in large areas which are not densely populated but also because of insufficient inspection and maintenance. The hazardous liquid spillages show different characteristics than those of the gas lines.

In reference to Papadakis [13], incidents due to corrosion are dominant, followed by external interference for the period 1970-1993 it can be concluded that efforts have been put in the control of third-party activity while pipe ageing is now becoming a major problem.

Failure frequencies of both gas and liquid transmission lines in Europe, the US and the former Soviet Union are decreasing. External interference, mostly third-party activity involving interference using machinery, has been recognized as a dominant failure mechanism both in gas and oil-industry pipelines. Failure rates connected with a particular mechanism e.g. external interference show a different spread over several diameters in different systems. High frequencies of failures caused by third party interference have been obtained in pipelines with a diameter between 5 and 16". Further analysis involving more detailed data e.g. burial depth, wall thickness, is required in order to establish the links between failure mechanisms and operational parameters of the pipeline. To conclude, identification of pipeline hazards associated with all different functions of the systems is essential for risk analysis since many important consequences are often connected with specific functions such as valves and other parts of the system.

This subsection presented an abstract of the threats and vulnerabilities involving the gas CI. This is being studied and documented in detail as a part of another task under this project. For a dimensional analysis on the level of the CM, at least the following attributes will be considered, also in combination:

1. Natural, anthropogenic, man-made
2. Accidental, intentional, sabotage, terroristic
3. Physical, cyber, cyber-physical
4. Short-term, long-term duration of threat
5. Social and Geo-political
6. Operational and Management

2.7 RESILIENCE MANAGEMENT STEPS

This section describes a general resilience management process aiming at enhancing and sustaining the resilience of a system.

Thereby resilience management constitutes a process that includes all activities to ensure, enhance and sustain resilience as an ability of a system. An underlying objective that arises in this context is to organize and to structure the activities to get an applicable process. To this end preceding developments [14] yielded the following resilience management steps:

A. Defining the system
B. Assessing resilience
C. Enhancing resilience
D. Maintaining
E. Restoring
F. Transforming

Thereby the resilience management steps are divided in the time periods before, during and after a disruption and can be related to resilience stages phases as depicted by **Error! Reference source not found.** which is described in the following.

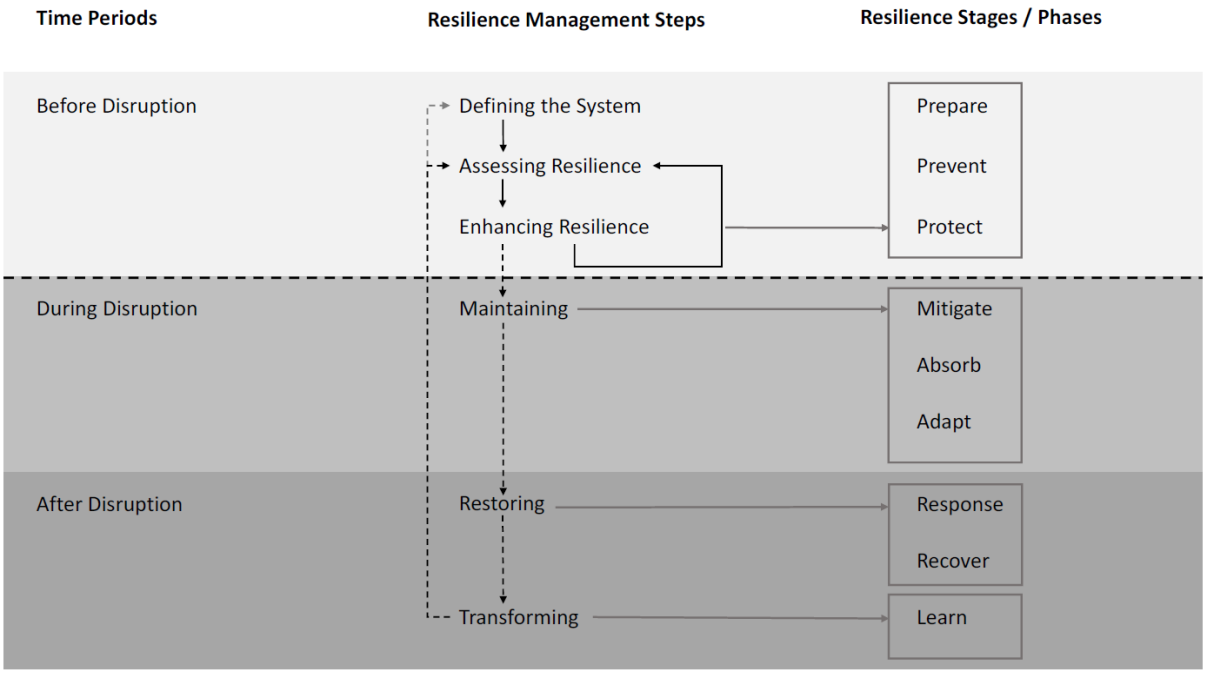

Figure 2.3: Resilience Management Step [14]

Starting with the time period before disruption the system needs to be defined: This includes the definition of the system boundaries, the description of influences that are expected as well as the identification of the stakeholders that are addressed. Thereafter the resilience of the system is assessed in order to identify its weak points and the gaps in the resilience implementation.

Based on this the resilience can be enhanced by developing appropriate measures. These include measures to prevent disruptive events on the one hand and to prepare as well as to protect the considered system on the other hand. The main objective during the disruption is the preservation of the critical functions of the system. This is covered by the maintaining step which addresses (1) the mitigation of the disruption impact to an acceptable level, (2) absorption or compensation of the impact of the event by the system's robustness and (3) the adaption of system to the new circumstances implied by the disruptive event.

After the disruption the system performance has to be restored preferably to a level equal to that before the disruption took place. Thereby a restoration in a short time is a major aim. The corresponding system abilities that are addressed in this time period are the respond and recover capacity. These typically needs to be developed before the disruption occurs.

Transformation of the system constitutes the last resilience management step involving a process of learning from the event and feedback. The last-named learning process enables iteration as indicated with dashed arrows to the left of the resilience management steps that leads to a successive improvement of the system's resilience. As already mentions above, disruption are rare so that an additional shorter iteration loop including the assessment and the enhancement step is recommended as indicated by the solid arrow connecting these two steps.

In summary, at least the following dimensional attributes are recommended within the resilience management dimension:

1. Prepare
2. Prevent
3. Protect
4. Mitigate

5. Absorb
6. Adapt
7. Response
8. Recover
9. Learn

2.8 TECHNICAL RISK AND RESLIENCE CONTROL CAPABILTIES ADDRESSED

In order to achieve resilience and ensure security, existing and new gas infrastructures have to avoid and resist to hazards and absorb their impacts more efficiently and more effectively (classical risk control). They also have to accommodate and recover the effects of a hazard more efficiently, timely and safely (resilience). Hence, they also have to be designed/restored to coordinate more efficiently across the various phases of a disaster risk management cycle.

Hence it is important to make sure that risk control and resilience is really built operationally and is considered as a driving principle for an owner/operator of Critical Infrastructure. The SecureGas CONOPS follows a panarchy loop of continuous development and improvement, and serves as a basis to achieve Resilience and Security for European Gas CI.

In practical terms, in order to achieve completeness, the SecureGas solution will adapt and extend the existing components so that to add extended features which makes them compliant with the CM as well as with the requirements of the HLRA. Prerequisite actions include a state-of-the-art analysis in order to identify the existing limitations and barriers in practice as well as the current challenges, constraints and needs of the Infrastructure Managers and Operators in terms of security against both physical and cyber threats.

SecureGas success will depend on the effective implementation and use of the components developed under the high-level framework. Hence the technology providers will seek to adapt and customize the existing, already mature, components in order to cover the needs as defined by the end-users. To do this, technology providers and business case owners will interact in order to define how the various components can be integrated into the High-Level Architecture and how they will interact to serve the purpose of achieving the required Level of Service (LoS).

The Concept of Operations (CONOPS) will guide the implementation and integration process. Following the extended SecureGas components, as previously developed and incremented, will be customized, integrated and deployed, into the project Application cases. On the basis of the defined CONOPS, activities, processes, timeline, and roles will be identified and defined for each business case so that to make sure that the Business Case development is made according to the principle of agility, effectiveness and clarity or roles.

The table below lists specific challenges and their scope regarding the generation of risk control and resilience and how they are overcome within the SecureGas approach.

Table 2.3: Challenges and SecureGas approach

Specific Challenge or Scope	How SecureGas will address the challenge
Disruptions in the operation of countries' critical infrastructure may result from many kinds of hazards and physical and/or cyber-attacks on installations and their interconnected systems. …. A comprehensive, yet installation-specific, approach is needed to secure existing or future … connected and interdependent installations ….. Budgetary constraints … require …new security solutions, … cost-effective, and possibly more automated.	SecureGas adopts a comprehensive, yet installation specific, approach to the Security and Resilience of Critical Infrastructure, with a focus on the Gas network. The Conceptual Model and the High-Level Reference Architecture provide a blue print and the rules for its implementation on how Gas installations and systems have to be planned, designed, constructed, operated and maintained to be secure and resilient against physical, cyber and the combination of cyber and physical threats.

Solutions developed should cover: forecast, assessment of physical and cyber risks, prevention, detection, response, and in case of failure, mitigation of consequences … and fast recovery after incidents, over the life span of the infrastructure, with a view to achieving the security and resilience of all functions performed by the installations.	SecureGas addresses the Resilience of Gas CI and aims at integrating the Resilience capabilities (Plan/Prepare, Absorb, Recover and Adapt) in the Disaster Risk Management Cycle (Preparation, Response, Recovery and Mitigation) within an Asset Life-Cycle perspective, thus securing to achieve resilience across the various phases of the life-cycle of an infrastructure.
They should: (a) assess in detail all aspects of interdependent physical …. . and cyber threats and incidents, … and the cascading risks …; *(b) demonstrate the accuracy of their risk assessment approach using specific examples and scenarios of real life and by comparing the results with other risk assessment methodologies;* *(c) develop improved real-time, evidence-based security management of physical and cyber threats, taking account of the ageing of existing infrastructure;* *(d) provide scenarios and recommendations for policy planning, engagement of the civil society, and investment measures encompassing all aspects*	(a) SecureGas extended components have been selected on the basis of complementarity to address various type of threats and cascading events. (b) SecureGas will perform a characterization and ranking of the complete range of cyber, physical and cyber-physical risks for gas CI. (c) Specific application cases are dedicated to the provision of Risk-Based security asset management services, along the entire life-cycle of the infrastructure. (d) SecureGas will deliver a "white paper" addressing evaluation, lessons learnt and recommendations, including those coming from a Cost Benefit Analysis (CBA) for cyber-physical resilience of Gas CI.
Innovative methods should be proposed for sharing information with the public in the vicinity of the installations … for the protection of first responders such as rescue teams, security teams …	SecureGas aims at the implementation of a dedicated approach in communicating information to the public, paying attention to the balance among safety and security aspects, starting from existing practices in the sector.

2.8.1 Analysis of the proposed system and respective advantages offered

In line with the challenges and scope described in Table 2.3, the following table below summarizes technologies and technology areas mainly addressed by SecureGas, representing the project technological offering.

Table 2.4: SecureGas technological offering

Tech. Area: Technologies for Situational Awareness and Decision Support for Cyber-Physical Threats
Safety & Security (S&S) Platform for Gas CI
Autonomous docking station and UAV-based asset management
Geohazards Assessment for Decision Support
Tech. Area: Technologies for information processing and management
Data Analytics and Machine Learning for cyber-physical anomaly detection
Blockchain for data transmission and integrity verification
Tech. Area: Technologies for Detection, Identification and Early Warning
Intrusion and defect detection

Cognitive framework for biometrics and video analytics
Tech. Area: Technologies for Joint Cyber-Physical Security Risk Management and Resilience Modelling
Joint cyber-physical risk and resilience modelling and management, Fast gas network modelling and attacks simulation for infrastructure security assessment

Taking into account the technology areas reported in the above table, most of them can be sorted in the following technical resilience capabilities as defined in [15]:

1. Sensing (Surveillance)
2. Situation representation (sense making)
3. Decision making
4. Activation (action), including adaption

2.9 PERSONS AND FUNCTIONS AFFECTED

Apart from the assets that can be potentially affected, the following is a non-exhaustive list of the persons involved in the entire functioning (not necessarily physical operations) of a Gas Critical Infrastructure.

1. Workers
2. Team leaders
3. Decision makers and planners
4. Operators
5. Members of the advisory board
6. Regulators
7. Third parties
8. Politics
9. Consumers

2.10 RECOMMENDED GAS INFRASTRUCTURE CONCEPTUAL MODEL

The Conceptual Model constitutes of an abstract description of the gas supply infrastructure, its threats and the corresponding security system. In the following an example (sample part) of the SecureGas Conceptual Model is depicted in a simplified form for the sake of clarity.

Furthermore, a construction procedure to obtain the CM is presented. The construction procedure thereby relies on the dimensions introduced in the previous section **Error! Reference source not found.** to section 2.9. The complete CM can be obtained applying the construction procedure to all dimensions identified.

Based on the CM example, an example of a CONOPS derivation is then given on the basis of the CM example. It is self-evident that a complete CM is necessary to derive the complete set of CONOPS. On the other hand, for a well-defined technical security solution, a limited CM of the related gas supply system secured is sufficient.

2.10.1 Construction procedure of the Conceptual Model (CM)

In the following, the construction of the CM is provided:

1. Selection of dimensions for the threats, the gas system and the security system.
2. Filling the dimensions with attributes.
3. Derivation of threats entity by combining the attributes each one out of one threat dimension.
4. Derivation of gas system entity by combining the attributes each one out of one gas system dimension.
5. Derivation of security system entity by combining the attributes each one out of one security system dimension.
6. Specification of the gas system independent threat entities according to the gas system entities.

2.10.2 Derivation of Concept of Operations (CONOPS)

Based on the Conceptual Model (CM) as defined in the previous subsection 2.10.1 Concepts of Operation (CONOPS) can be derived. This can be achieved by linking the gas infrastructure specific threats entities with the security system entities. Unlike the derivation of the entities in section 2.10.1 where almost all combinations are meaningful, the combinations of the gas infrastructure specific threats entities with the security system entities that lead to reasonable concepts of operation are few.

In the following it is shown how this example is captured in the scheme of the proposed CM. In the following, one example for CONOPS derivation is given for which some of the cells in the CM-scheme (Figure below) are colored in red.

Within the example, the following situation is considered:

“A predictive simulation of the gas infrastructure undertaken by a member of the control room of a distribution infrastructure informs him about the consequences of his planned activities. He is able to realize that he is about to do a mistake by operating the valve remotely. Thus a disruption is prevented.”

In the following this example situation is fitted into the framework of the conceptual model in order to get a structured representation of it. Starting from the attributes of the threats dimensions this example picks ‘worker’ of the ‘actor’-dimension and ‘accidently’ of the ‘motive’-dimension resulting in the gas system independent threat entity ‘internal human failure’.

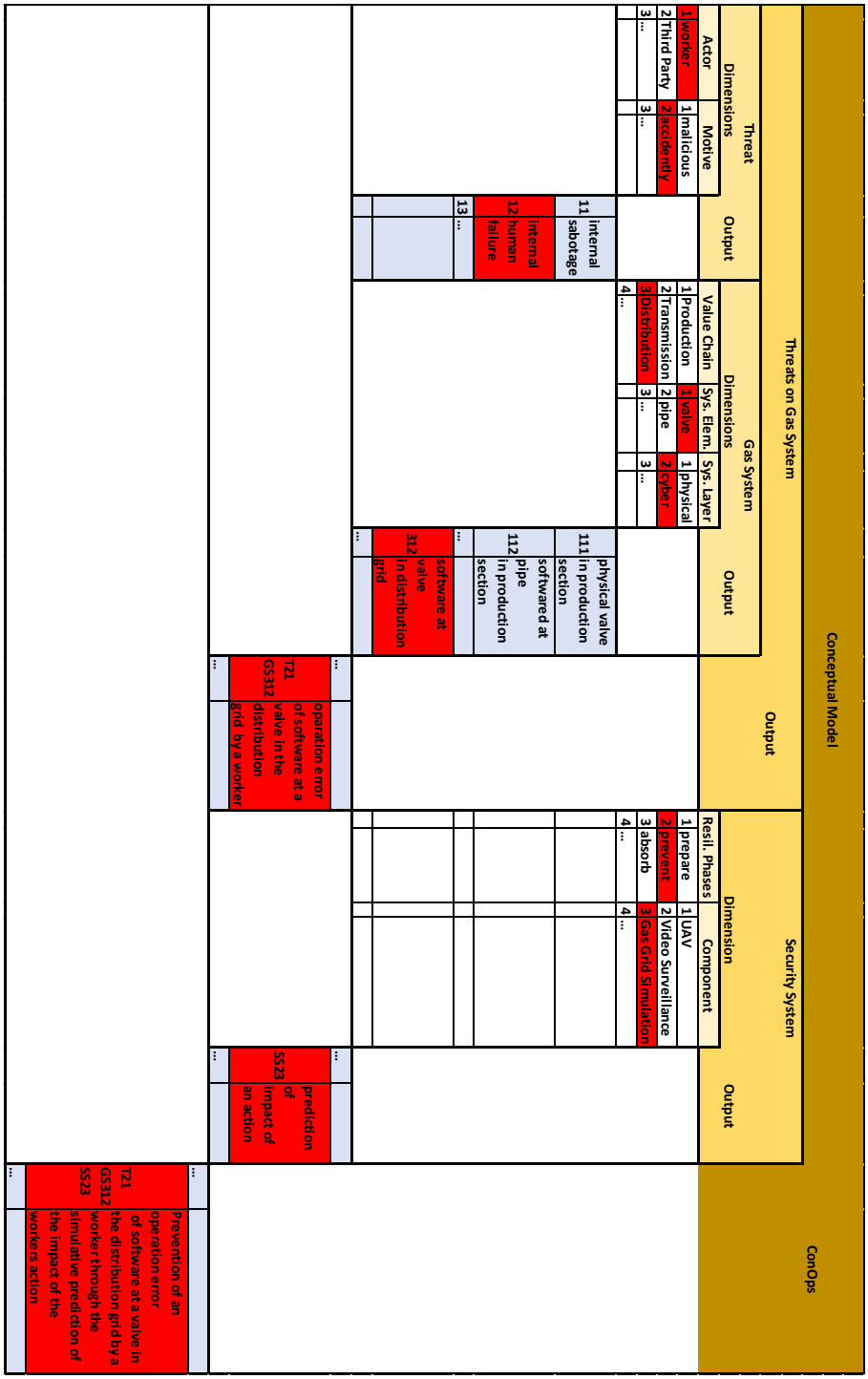

Figure 2.4: Example of the SecureGas Conceptual Model illustrating the derivation of a sample CONOPS.

The next step comprises the selection of ‘distribution’ from the ‘value chain’ dimension of the Gas System, ‘valve’ of the ‘system element’-dimension and ‘cyber’ of the ‘system layer’-dimension. This combination of three attributes leads to the Gas System entity ‘software at valve in distribution infrastructure’. Combining the thus obtained entities leads then in turn to the gas infrastructure specific threat entity ‘operation error of software at a valve in the distribution infrastructure accidently causes by a worker’.

Furthermore, the attribute ‘prevention’ of the ‘resilience phase’-dimension and the attribute ‘gas infrastructure simulation’ of the ‘component’-dimension is selected resulting in the ‘prediction of impact of an action’ entity. As a last step the gas infrastructure specific threat entity is combined with the security entity resulting in the CONOPS which reads ‘prevention of an operation error of steering software at a valve in the distribution infrastructure by a simulative prediction of the impact of the worker’s action’.

In summary, the section showed how to construct a conceptual model for a given gas supply (sub) system, a related security system as well as the CMs can be used to specify CONOPS for the gas subsystem under consideration.

3 CONOPS

3.1 LITERATURE REVIEW ON CLASSICAL CONOPS APPROACHES

3.1.1 Defintions of CONOPS in related domains

Concepts of Operations (CONOPS) have been defined and described, in several documents, papers and standards. In the following list, several CONOPS definitions are presented as derived from the most commonly used references:

1. A user oriented document that describes system characteristics of the to-be-delivered system from the user's viewpoint [4].
2. Verbal or graphical statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources [16].
3. A user-oriented document that describes the characteristics for a proposed asset or system from the viewpoint of any individual or organizational entity that will use it in their daily work activities or who will operate or interact directly with it [17].
4. Both an analysis and a formal document that describes how an asset, system, or capability will be employed and supported. The CONOPS is a communication vehicle to inform stakeholders of the intended uses and methods of support of assets, systems, or capabilities [18].
5. CONOPS describe the organization's assumptions or intent in regard to an overall operation or series of operations of the business with using the system to be developed, existing systems and possible future systems [7].
6. A conceptual overview of the proposed system, describing the desired characteristics of the system from the user's viewpoint [19].

When translated to the gas supply security system solutions as provided by SecureGas, CONOPS can be defined as a concise description of use cases of the technical security solutions. In addition, as defined by the working definition, the CONOPS in the present context use the system and security system dimensions.

3.2 OVERVIEW ON CURRENT STATUS OF GAS SECURITY MANAGEMENT SYSTEMS AND GAPS

The following section briefly presents the current practices of security management from the perspective of upstream and midstream gas systems. In order for the completeness of the section, a surface view of potential gaps in the system are also mentioned. As the project progresses, these sections will be updated to provide a comprehensive abstract of existing security systems, gaps and how SecureGas addresses them.

Typical current practice of security management (physical and cyber) for upstream and midstream gas systems:

1. Operational monitoring in control room
2. Procedures and guidelines in case of events
3. Preparation and training to manage all identified credible critical events
4. Communication channels with public authorities (police, fire brigades), mainly oral communication via phone
5. Use of meteorological forecast and local measurement stations to cover the effects of weather, temperature, wind direction
6. Additional possible surveillance systems e.g.:
    a. Fiber-optic
    b. Viber-acoustic
    c. Cameras (optic, IR)
    d. Local access control of plants and facilities
    e. Satellite surveillance (SAR) for geo hazards
7. Operational room covers emergency in operation, health (occupational safety) and security
8. There is not a dedicated security system as such, but security issues are integrated in overall operation, often taken from different additional systems (other than the operational system)
9. Emergency, maintenance and repair operative local teams receive alarms by UMTs, email, etc.

Observations and potential gaps:

1. Current security systems are not real-time integrated with operational system
2. Pipelines surveillance systems are stand-alone systems
3. Remote control room information versus local authority and responder knowledge
4. Integration is conducted on the level of personal communication
5. Simulation is only conducted in case of events, e.g. using plum-model for gas dispersion
6. No total automation (also not desired)
7. Not all information are spatially visualized
8. Partial dashboard layered visualization
9. Partial uncertainty communication
10. No online overall current/ expected security event assessment

The following summarizing observations can be made. At the moment there is no overall security assessment system. During the business activity, operators cover many separate EU, national and company's regulations. Such regulations are also employed in case of damage events.

Third party interference is a big cause of pipeline failures. Transmission system operators recognize the seriousness of the various pipeline threats and manage the risk of pipelines by implementing cohesive integrity management systems where a mix of one or multiple controls are utilized to manage many types of pipeline threats.

The sector is expected to benefit by adopting new technology such as intelligent and remote systems for monitoring the pipeline's real time performance and integrity. The integrated and intelligent systems would enable sustainable and effective asset management. It is felt that further advancements are required to develop cost effective systems.

3.3 GENERATING COMPLETE CONOPS OF A SECURITY SOLUTION OR OF A SECURITY SYSTEM: ASSESSMENT PROCESS OPTIONS

This section addresses the question how to determine the concept of operations (CONOPS) for a single technical security solution as well as all concepts of operation (CONOPS) of a technical security management system. The approach resorts to the conceptual model (CM) as developed in chapter 2. Sections below show how to leverage the CM to generate a complete description of the CONOPS or use case of the technical solution in terms of the dimensions of the CM and the attributes of each dimension.

In the following subsections we consider a single technical security solution as well as a set of such solutions, e.g. as part of and including a technical security management system.

3.3.1 CONOPS for security solutions or security management systems by identifying which combinations of dimensional attributes are covered

The aim is to achieve a complete description of the use case of a technical solution, a set of technical solutions or a security system (each module or tool contained is treated as security solution as well as the toolbox (system of system) itself). This is achieved by using a set of relevant dimensions as developed as Conceptual Model (CM) for the description of the gas supply system, the security solution or security management system. As will be shown, the process comprises the improvement of the conceptual modelling itself as well in an iterative and convergent process for the CONOPS generation.

The process is detailed as follows:

(1) List the inputs for your CONOPS generation, e.g. verbose descriptions of technical security solution(s), etc.

(2) List the initial dimensions and their attributes

(3) Assess coverage of technical solutions by dimensions and attributes, and add new ones if necessary, respectively

(4) Define a meaningful sorting of the dimensions for your technical security solutions (same for all)

(5) Select a technical security solution

(6) Select the dimensional attribute(s) covered for each dimension of the conceptual model by the technical security solution, also providing arguments why the attributes are covered and how

(7) Iterate and converge by going to (3) till CONOPS are generated for all technical solutions

(8) List the dimensions addressed and the attributes addressed for each technical solution, including arguments why

The described process generates filled CONOPS templates for security solutions showing which main attributes are covered and why. It generates the same template for each security solution, i.e. it uses the same

- Number of dimensions,
- Dimension names,
- Attribute numbers within each dimension and
- Attribute names within each dimension.

Thus, the approach generates a set of single or multiple attributes for each dimension being most relevant for each CONOPS of each security solution. This generates a complete description of the operational use cases of technical security solutions (CONOPS), consisting of the set of attributes and the related explanations

$$\text{CONOPS}_i = \begin{pmatrix} \text{Dimension}_{i1}, \{\text{set of attributes of Dimension}_{i1}\ \text{covered}\}, \{\text{Explanations for Dimension}_{i1}\} \\ \text{Dimension}_{i2}, \{\text{set of attributes of Dimension}_{i2}\ \text{covered}\}, \{\text{Explanations for Dimension}_{i2}\} \\ \dots \\ \dots \\ \text{Dimension}_{iN_D}, \{\text{set of attributes of Dimension}_{iN_D}\ \text{covered}\}, \{\text{Explanations for Dimension}_{iN_D}\} \end{pmatrix},$$

where $i = 1,2,\cdots,N_{TS}$ is the number of technical solutions considered and N_D is the number of dimensions of the CM finally used. For each dimension $N_{ij}, j = 1,2,\cdots,N_i^D$ attributes are used. Please note that the set of attributes of at dimension may be empty if the dimension is not applicable or relevant, which formally also can be defined as an attribute value.

This approach is best suited if a security solution or security system is already in operation, planned or exists as a concept. Depending on the information available the resolution of the approach is refined.

3.3.2 CONOPS for security systems by looking at all dimensional combinations within a 5-step risk management process

This approach resorts to the 5-step risk management scheme of ISO 31000, see e.g. [20] to cover all dimensions in a systematic way.

The process can be characterized as follows:

(1) List the inputs for your CONOPS, e.g. short verbose descriptions of (intended) technical security solution(s), scope(s), or only objectives of your security solutions, etc.

(2) List all initial conceptual model dimensions and their attributes

(3) Conduct risk management steps:

  (a) Assess context of your technical security solution(s), including identification of security generation objectives

  (b) Determine physical, cyber and cyber-physical risks

  (c) Analyze risks

  (d) Evaluate risks

  (e) Mitigate risks

(4) In (a) to (e) use conceptual model dimensions to refine the descriptions (dimensions can be used serval times); Assess coverage of technical solutions by dimensions and attributes, and add new ones if necessary; Define a meaningful standard recommendation of use of the dimensions throughout (a) to (e)

(5) Iterate and converge by going to (3) till CONOPS are generated for all technical solutions

(6) List the dimensions and attributes addressed for each technical solution, including arguments why

Please note that dimensions can be used several times within steps (a) to (e). For instance, the dimensions system layers and system elements can be used for the identification of risks and the description of the mitigation measures. For instance, gas leakage is a physical risk or threat. A fiber-optic detection system uses at least the technical layer (e.g. sensors, hardware and communication technology) and the cyber layer (e.g. communication protocols, command and control room) and the organizational layer (operators in command room and maintenance personnel).

For instance, in (a) one could use the dimensions gas system business domains, system layers and resilience cycle phases to define the boundaries of the security system when focusing for instance on leakage detection during operation of gas physical transmission systems.

This approach is also suited for achieving very generic objectives for a system under consideration, e.g. “control single cyber, physical and cyber physical risks, as well as their combination”. Thus, the approach is capable to design new security solutions or even security management systems for gas supply subsystems or overall systems. However, the drawback is that it might start from very generic objectives only requiring a lot of input.

In the project context of SecureGas, the present approach is considered less relevant since the business case owners have already an idea which types of threats they want to cover, which technology they want to explore etc. In this sense it is not necessary to start from a level plain field.

3.3.3 CONOPS for security systems by looking at all dimensional combinations by resilience management

The approach proposed by subsection 3.3.3 is similar to that of the last subsection 3.3.2, but replaces the analytical risk management steps with resilience cycle steps. They can be divided in steps before, during and after an event, i.e. there is a logical or time sorting. This sorting may differ depending on the threat considered.

The following 5 steps are often used in the civil security research context, in particular regarding critical infrastructure protection, see [21]. It has been shown that they also can be applied to engineering resilience solutions, in particular for generating security, see [15]. The dimensions are

1. Prepare
2. Prevent
3. Protect
4. Respond
5. Recover

When resorting to active protection systems also the following additional steps are used, which can be considered as a refinement

1. Prepare (organizational, cyber, technical, physical including physical-structural; for all steps 2 to 6)
2. Detect
3. Prevent
4. Protect (active protection in case of events)
5. Respond
6. Recover (to improved) system performance

7. Learn and adapt (covers all steps 2 to 6)

Using the last resilience management attributes, the following process for CONOPS generation is proposed:

(1) List the inputs for your CONOPS, e.g. short verbose descriptions of (intended) technical security solutions, scope of CONOPS to be generated, etc.

(2) List all initial conceptual model dimensions and their attributes

(3) Use resilience cycle steps to describe your security solution(s):

  (a) Prepare (organizational, cyber, technical, physical including physical-structural; for all steps (b) to (f))

  (b) Detect

  (c) Prevent

  (d) Protect (active protection in case of events)

  (e) Respond

  (f) Recover (to improved) system performance

  (g) Learn and adapt (covers all steps b to g)

(4) In (a) to (g) use conceptual model dimensions to refine the descriptions (dimensions can be used serval times); Assess coverage of technical solutions by dimensions and attributes, and add new ones if necessary; Define a meaningful standard recommendation of use of the dimensions throughout (a) to (h)

(5) Iterate and converge by going to (3) till CONOPS are generated for all technical solutions

(6) List the dimensions addressed and the attributes addressed for each technical solution, including arguments why

This approach is especially suited for active novel solutions that intend to actively stop events from unfolding or mitigating events post events. It has a strong focus on resilience enhancement when compared to the approach based on risk management which focuses on the reduction of the frequency of (basic) events and on immediate robustness of systems (low initial vulnerability) as presented in the final subsection 3.3.4.

The drawback is that the approach does not explicitly incorporate any risk ranking for the selection of most relevant technical security solutions. It is strongly focusing on the actual event control rather than considering risk ranking. Even if this of course can be considered by step (a) by requiring that the risk management dimension is covered, which is implicitly already covered in step (4).

3.3.4 CONOPS genration using panarchy approach using additoinal dimension in steps along the main process: joint risk and resilience assessment and management panarchy process

In the literature several approaches have been proposed for performance-based resilience management which include extensions of risk management as a special case. In terms of resilience management, risk management focuses on the reduction of the frequency of events (reduction of susceptibility) and the increase of robustness (decrease of initial damage, decrease of vulnerability).

Resilience management in a narrower sense focuses on improving system behavior poste disruption events. That is on reducing the system performance loss time, on increasing its recovery slope and on achieving as fast as possible the initial performance or even increasing the final performance when compared to the initial system performance, and similar objectives. A sample process that can be conducted analytically or by using quantitative performance function is shown in Figure below, see [22] and [23].

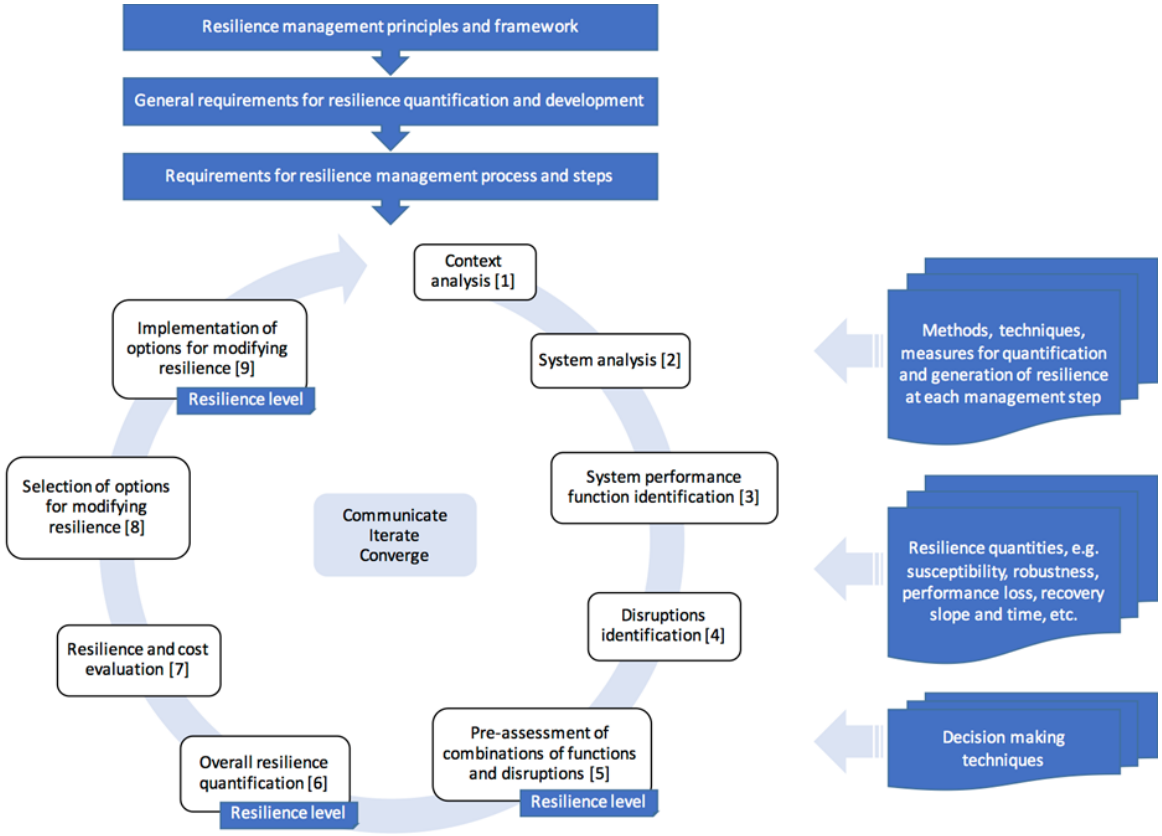

Figure 3.1: CONOPS Resilience management process based on deductive system performance function assessment. The step-wise management process can be quantified, resorts to approaches and tools as appropriate, and is designed for critical infrastructure protection

The advantage of the process shown in Figure 3.1 is that it can be conducted analytically as well as semi-quantitatively and quantitatively. Furthermore, that it is focusing on system performance quantities, which can also be identified as parts of the key performance indicators (KPI) of the system.

A disadvantage is that is does not use the well-known risk and resilience cycles explicitly, respectively. This holds true even if the process used can be shown to be an extension of classical risk management it takes account of most the resilience engineering paradigms, see Figure 3.3 below, see [22] and [23].

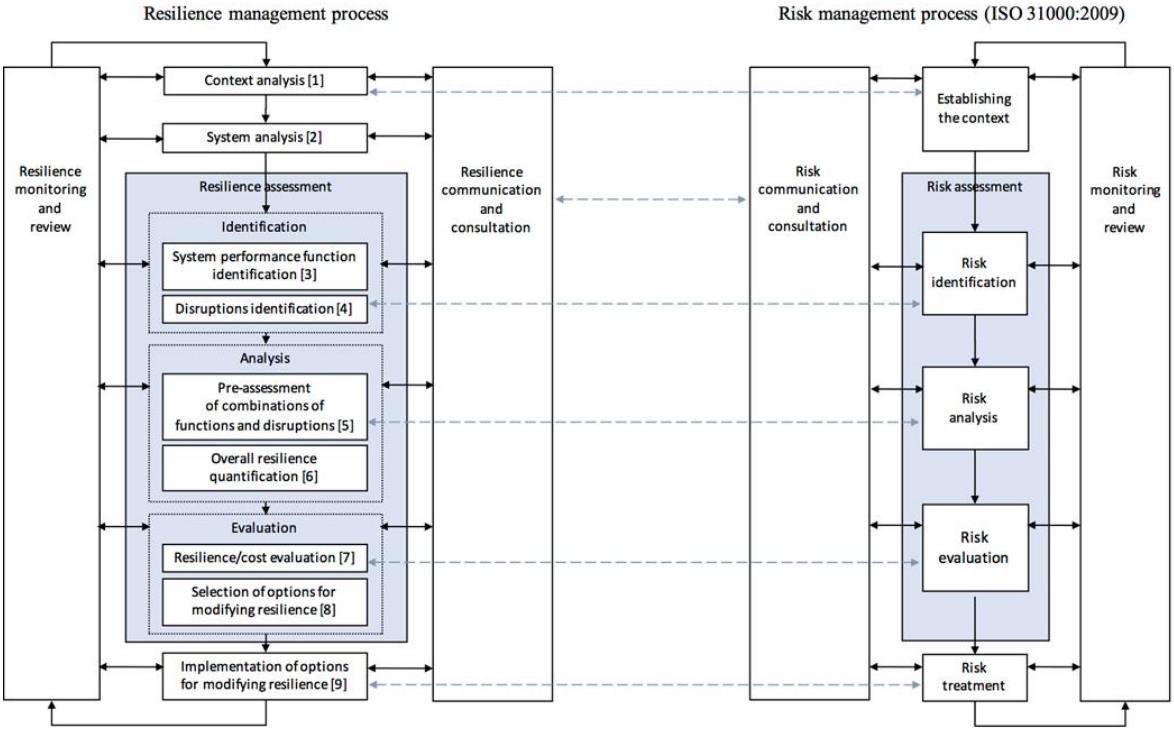

Figure 3.2: Resilience management process as extension of risk management process

A more analytical heuristic approach that uses both, the risk cycle and the resilience cycle, is to combine risk management and resilience management. To this end the table below lists the steps already used in subsection 3.3.2 and subsection 3.3.3. The advantage is that each step can be covered on abstract level using tables and is also made explicit in the process. In addition, the processes can be quantified. Table 3.2 lists typical risk management and resilience (emergency) management steps.

Table 3.1: Typical steps of risk management (risk management cycle) and resilience management (resilience cycle). Similar steps are marked as dark green, light green or by using slanted fonts

Risk management steps taking into account effects post event, Risk cycle	Resilience management steps, Resilience cycle
(1) System context analysis *(2) Risk event and potential resilience issue identification* *(3) Risk and resilience analysis, single and overall* *(4) Risk and resilience evaluation* *(5) Risk mitigation and resilience improvement*	*(1) Preparation, including Protection before event* (2) Detection of events (3) Prevention (4) Absorption, Protection (during and after event) (5) Response (6) Recovery, including system improvement (7) Learning and *adaption*

The 7-th step of the resilience cycle can be considered as an activity that is conducted during and after and event. However, it can also be an activity in preparation of an event and an activity that is conducted during a disruption event occurs.

Figure 3.4 visualizes the risk and resilience assessment cycle and the resilience response cycle.

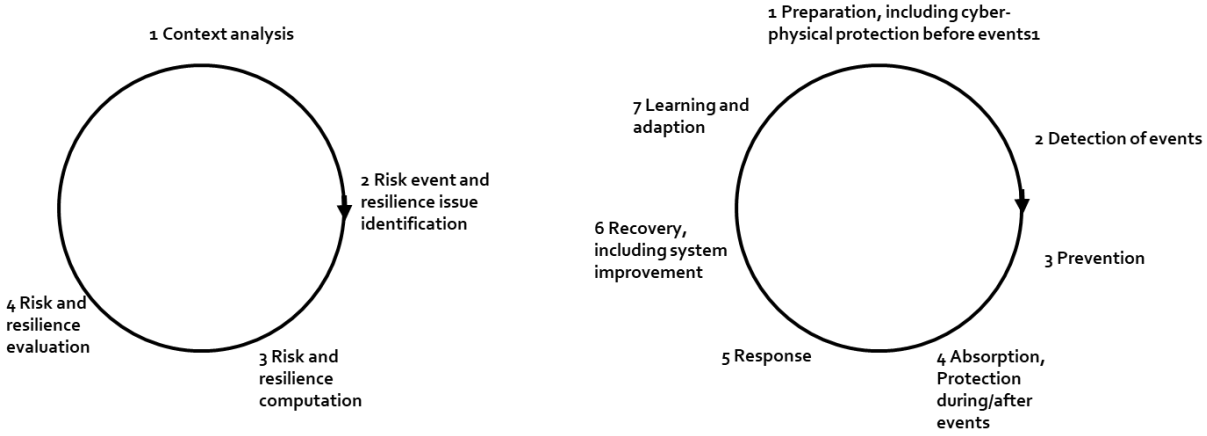

Figure 3.3: Risk cycle (left) and resilience cycle (right) using the steps of Error! Reference source not found.**Table 3.2**

In the following, two options are proposed to merge the risk and resilience assessment scheme and the disruption management (timeline, logic) scheme. The first one assumes that the most similar steps are the identification of risk events and resilience issues on the one hand side and the actual detection of occurring events or issues on the other hand. The second option assumes that the most similar steps are the implementation of risk control and resilience enhancement measures on the one hand side and the preparation before events on the other hand side.

Both approaches assume that the joint risk and resilience assessment process is not part of the preparation step of the resilience management circle. Also, that related steps, such as the just two mentioned ones and the adoption and learning step, can be distinguished. Obviously, this are key assumptions to take advantage of the resilience paradigm of focusing more on the post event and learning options in case of damage events as well as on the unfolding nature of responding to disruptions.

Figure 3.5 shows the correspondence of steps and Figure 3.6 the panarchy scheme in case of taking advantage of the similarity of the step risk event and resilience issue identification with the step event detection.

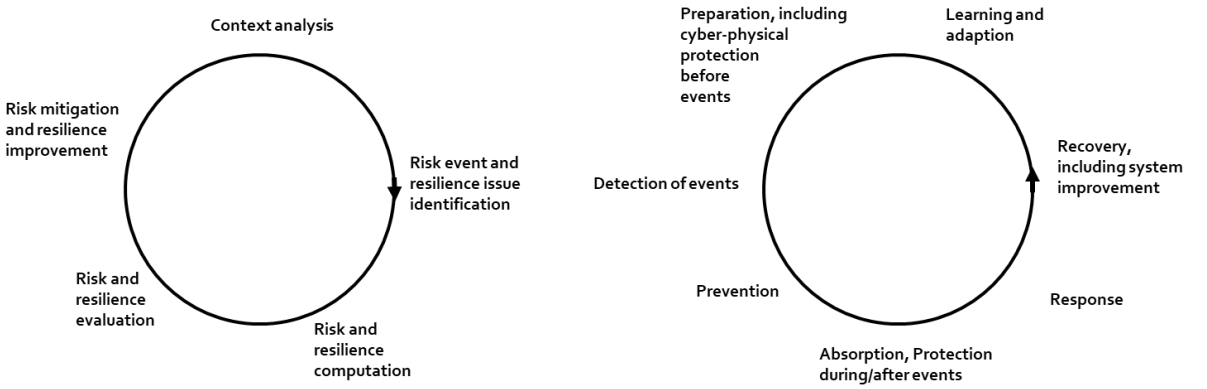

Figure 3.4: Process step identification option for the risk and resilience assessment cycle and the resilience/catastrophe cycle. Option of using the transition from potential events and resilience issues to real event detection.

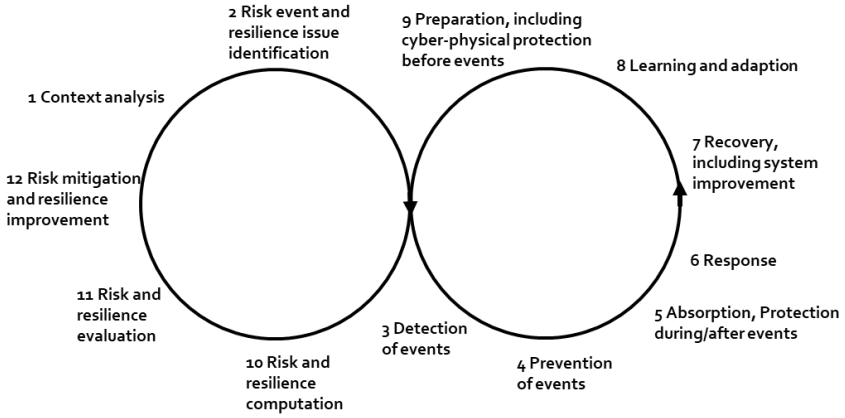

Figure 3.5: Joint risk and resilience assessment and management panarchy taking advantage of the transition from potential events and resilience issues to real event detection.

The panarchy option proposed by Figure 3.6 assumes that both cycles are iteratively conducted, i.e. if there are no events the assessment loop is iterated till convergence. In this sense, known events (e.g. historic events) would already have been taken into account, of course only if known ahead. That is, the iterate, communicate and converge concept is understood for loops as well as for panarchies. In addition is noted that for instance the left hand side loop classically only covers known risks whereas the right hand side loop also covers unknown risks.

When compared to the second option, see Figure 3.7 and 3.8, the first option of generating a joint risk and resilience assessment, risk control and resilience improvement as well as resilient disruption response panarchy process scheme is identified to be less convincing. For the second option when compared with the first option the following statements hold:

- Each loop can be conducted almost completely (before moving over to the second loop).
- The steps close to the intersection are more similar.
- The joining idea seems to be less conceptual (preparation, planning, adaption and learning versus switch between potential events or issues and real event).
- The second option has the potential to further reduce the analysis steps (however only with the drawback of being less explicit and less concept-inclusive).

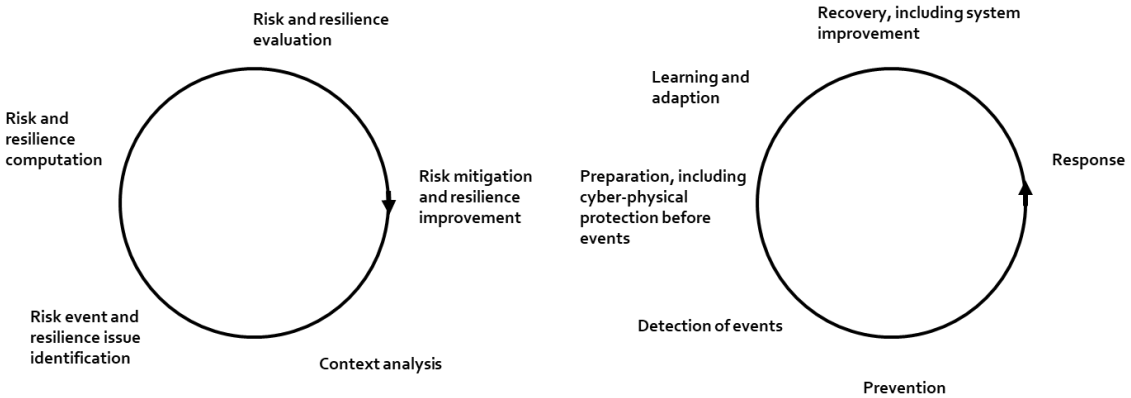

Figure 3.6: Process step identification option for the risk and resilience assessment cycle and the resilience/catastrophe cycle. Second option of using the transition from the risk mitigation measures and resilience improvement measures from the generalized risk and resilience assessment process to the preparation step of the resilience cycle.

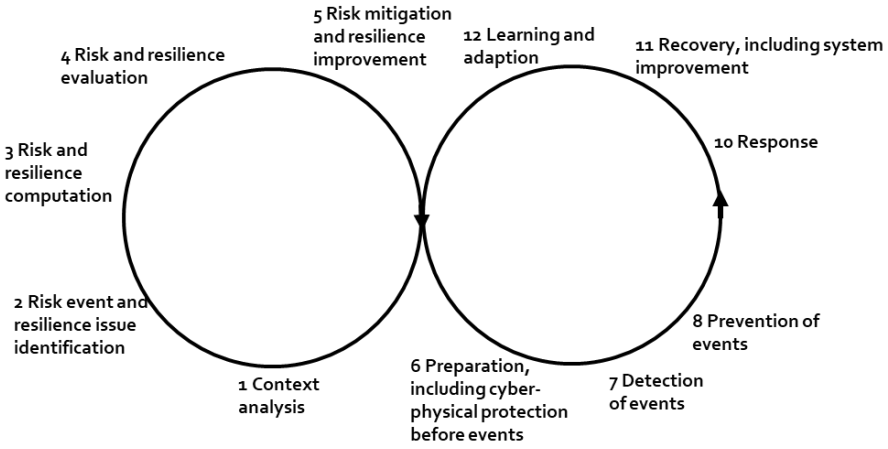

Figure 3.7: Joint risk and resilience assessment and management panarchy. This panarchy takes advantage of the similarity of the step improvement of (classical) risk control and (more novel) resilience with the preparation step of the resilience cycle.

As shown in subsection 3.3.1 to subsection 3.3.3, this process can be iterated and converged taking advantage of the additional dimensions of the conceptual model. However, this time the dimension risk and resilience assessment and resilience cycle phases are the core loop. Hence there is formally one dimension less to be considered.

To conclude, an overall process similar as given in subsection 3.3.3 can be provided by replacing the resilience cycle steps with all the panarchy steps of Figure 3.8.

In summary, for rather known technical security solutions:

- The approach discussed in subsections 3.3.1 is recommended for CONOPS generation.

For novel overall security systems any approach as presented in subsections 3.3.2 to subsection 3.3.4 can be used:

- The approach based on risk management is more classical, with resilience cycle steps only taken into account as additional dimensions.
- The approach based on the resilience cycle is more modern in the sense of the resilience paradigm.
- The approach based on the joint risk and resilience assessment and management panarchy is integrative and unites the risk and resilience assessment and the risk event control and resilience response management.

In particular, the risk management approach allows to check the coverage of all potential risks by formulating the abstract objective to mitigate all known risks.

3.4 CONOPS EXAMPLES

3.4.1 CONOPS example UAV surveillance of leckages

Natural gas transmission pipeline inspections are mainly carried out on the ground by walking surveys using mobile gas detectors to check leakages. This method is very time-consuming and labor-intensive.

A remote gas detection system using Unmanned Aerial Vehicles (UAV) could make it much more effective. Airborne infrared laser-based remote gas detection system installed on board a UAV drone could be capable of precisely detecting even very low methane concentrations. It could also report photographic documentation of inspection flights providing

knowledge of the general condition of the pipeline route, places where pipeline is over ground (exposed, air crossings) and state of objects.

This infrared laser-based remote gas detection method is based on the Differential Absorption Lidar (DIAL) measurement principle, an established active remote sensing method for detecting different gases in the atmosphere. The LIDAR (Light Detection and Ranging) technique involves transmitting laser light and detecting and analyzing the light back-scattered by the atmosphere or a solid target object like the ground. Trace gas concentrations can be determined by tuning the laser wavelength to the spectral signature and absorption characteristics of the gas to be measured).

Table 3.3 gives details for above mentioned CONOPS example regarding UAV leakage detection and surveillance

Table 3.2: Transmission system. Example CONOPS for UAV leakage detection and surveillance.

Dimension	Description for selected attribute
Business area	Natural gas transmission pipelines
Resilience cycle phase covered (preparation, prevention, detection, response, recovery, learning/adaption)	Detection of leakage; localization, data transfer and processing, prioritization of defects, decisions on response to event, mitigation measures, repairs.
System layer affected/covered	All buried and above ground gas transmission pipelines
Subsystem elements covered	Valves, gas distribution stations, gas measurement stations, compressor stations.
Risk management phases affected (context analysis, risk identification, risk analysis, risk evaluation, risk mitigation)	Risk identification, localization, data processing and analysis, evaluation, risk mitigation and elimination
Persons affected or working with solutions	Personnel locally operating and supervising transmission system. Staff working in control room Contractors providing repair, modernization and new construction services. Managers in charge for operation of the system
Stakeholders, decision makers	Engineers, managers of the operation and engineering divisions, managing directors of the company.
System life-cycle phase	Installation, maintenance and operation, repair and modernization.
Threats covered	Hazards to people, environment and infrastructure
Technical resilience capabilities covered	Detection and surveillance. Data processing, Decision making. Actions to eliminate the risks.

3.4.2 CONOPS example pipline disruption detection and further non-static failures

The main physical risks to be addressed when dealing with Asset Integrity of gas pipelines are Third Party Interference (TPI), impact bending, spillages and leakages due to corrosion, land sliding, fatigue, etc. (see Chapter 2.6 – data from European Gas pipeline Incident data Group (EGIG)). In addition to physical risks, cyber risks causing issues to the digital control systems

are relevant as well. The table below gives details for the above mentioned CONOPS example with a focus on monitoring and detection of pipeline disruption.

Table 3.3: Production System. Example CONOPS for gas transport third party interference

Dimension	Description for selected attributes and Comments
Business area	Natural gas transport, including Gas pipelines arriving in Europe with both offshore (submarine) and onshore parts; Examples of existing pipelines: from Algeria to Spain, from Tunisia to Italy (Sicilia), from Libya to Sicilia; NorthStream I, from Russia to Germany Examples of pipelines in construction: TAP is from Albania to South Italy, NorthStream I, from Russia to Germany, Turkish Stream, from Russia to Turkey
Resilience cycle phase covered (preparation, prevention, detection, response, recovery, learning/adaption)	Preparation, Detection, Response, Recovery, Learning/Adaption Detection of problem; Localization of interference or leakage; response to event, including repair; System learn from each correct/ non-correct identified failure and operation stages, e.g. high pressure/low pressure, valve open/closed
System layer affected/covered	Physical layer (mechanical asset integrity), Technical layer, Cyber layer Purpose is to monitor existing physical facilities (e.g. pipeline sections and stations) Installation on existing assets (retrofitting): installation comprises technical (sensor, electronics) and cyber elements (DCS, digital control system, SCADA); Telecommunication (e.g. W-FI, fiber optics, UMTS facilities) is used for remote control and data management;
Subsystem elements covered	Compressor stations, valve sections, pipeline sections, compressor stations, medium/terminal stations, metering stations
Risk management phases affected (context analysis, risk identification, risk analysis, risk evaluation, risk mitigation)	Mitigate risks Ongoing mitigation measure to control risks
Persons affected or working with solutions	Personnel in remote control rooms; Internal team that determines standard maintenance actions; Internal teams that maintain the detection system; External teams that install the detection technology; Internal spare part management team;
Stakeholders, decision makers	Decision makers on installation of system. Managing directors of company, Persons in charge of decisions on investments (capex) and on operative costs (opex).
System life-cycle phase	Partial installation, Operation and Maintenance, Retrofitting

Threats covered	Geohazards: seismic, landslides, flooding, fire; Man-made: Third party interference (by accident), construction work; agriculture, other at nodes Intentional: Sabotage, terrorism, theft attempt
Technical resilience capabilities covered	Sensing, Modelling/Sense making, Decision making, Action/Actuation Continuous sensing, evaluation and clustering of data, segmentation of the pipeline routing

4 CONCLUSIONS

The figure below summarizes the main steps and contents covered in in this document, which constitutes a preliminary version of the SecureGas Conceptual Model (CM) and Concept of Operations (CONOPS) approaches and applications. Figure 4.1 below shows the steps conducted based on the definitions of CM as an abstract dimensional (a Gas Critical Infrastructure) (sub) system description, in particular its security system, as well as the definition of CONOPS as a dimensional analysis and description of application use cases of technical security solutions of gas supply (sub) systems.

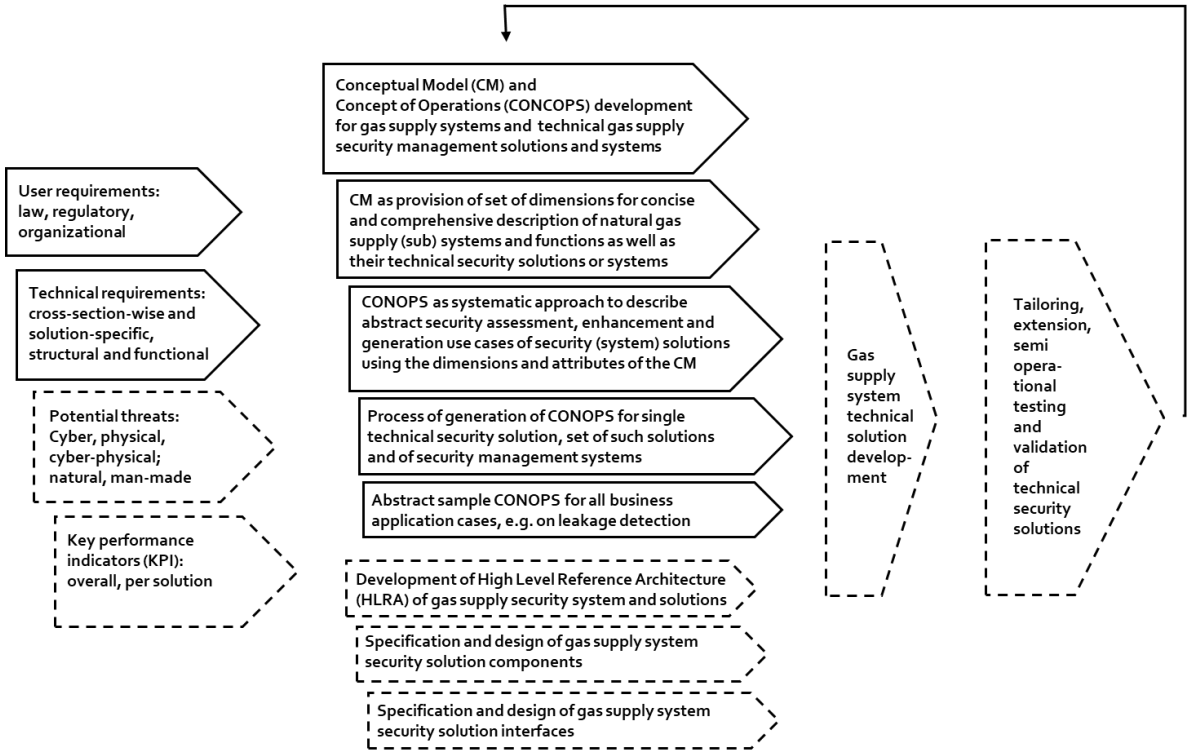

Figure 4.1: Inputs for CM and CONOPS approach and application and its relation to further system development steps

In addition, Figure 4.1 indicates how the CM and CONOPS approach and application relates to the necessary inputs such as user requirements, technical requirements, potential threats to be covered, performance indicators of solutions, system specifications as well as the expected further use of the CM and CONOPS during development, implementation, testing, validation and improvement. Main advantages are expected from the CM and CONOPS approach for the SecureGas High Level Reference Architecture (HLRA) development as well as the specification of the technical security solutions in all three application cases.

As indicated, the CM and CNOPOS approach will be refined after a first round of application cases.

4.1 RECOMMENDED GAS INFRASTRUCTURE AND GAS INFRASTRUCTURE SECURITY SOLUTION CONCEPTUAL MODEL (CM)

The report motivates and derives an abstract Conceptual Model (CM) for Gas CI systems and Gas CI security systems. It is required to be abstract enough to be understood by operational, management and decision-making persons but at the same time to be refined enough to allow for a concise description of properties and functions of gas supply subsystems and their functions. At the same time, the CM should be sufficient to leverage it for the concise formulation of Concepts of Operations (CONOPS) for gas supply system security solutions and systems.

It has been found that the CM can be defined by the following steps:

(1) Determination of scope of gas supply and/or security subsystem to be considered

(2) Identification of describing conceptual dimensions and related attributes for the scope of interest, including their sorting and wording, by resorting to the dimensions and attributes introduced in this report

(3) Use of the dimensions and their attributes to describe the

   a. gas supply subsystem of interest and

   b. its related technical security solutions and/or management system

(4) Iterate steps (1) to (3) till convergence

(5) Documentation and visualization of CM

Depending on the level of abstraction and the subsystem considered, the CM will cover rather many or rather few attributes of each dimension. Moreover, it has been found that the CM generation is highly iterative, i.e. as soon as new technical security solutions were described also the scope, the describing dimensions and attributes as well as the descriptions using the dimensions and attributes needed to be modified or extended.

The present interim version report of the CM is believed to already contain almost all of the abstract system dimensions and attributes that need to be addressed by the conceptual model of the gas supply system and gas supply security solutions and security system.

In the following, sample CM dimensions including attributes are given for illustration. They are chosen such that they suffice to describe a gas supply subsystem that is covered by a sample technical security solution for which sample CONOPS are presented in the next conclusion chapter section 4.2.

The sample CM for a gas supply subsystem describes the physical supply infrastructure system including valves, pumps and pressure and flow measurements. The related security solutions aim in particular at assessing its availability and function in case of disruptions. The technical security solution is predictive simulation of the effects of (partial) physical disruptions of the gas infrastructure.

Using the developed CM, the description reads for example

1. Natural gas supply application cases covered: e.g. transmission or distribution including storage
2. Gas supply system elements covered: e.g. pipes, valves, pumping stations, storage facilities, technical and cyber equipment to measure pressures and flows
3. System layer covered: e.g. physical, technical
4. etc.

In addition, the following CM dimensions are used to achieve the coverage of the related technical security system in the present example:

5. Natural gas supply subsystem life cycle phases considered: e.g. planning, planning of extensions, planning of increase of performance, risk control or resilience, maintenance, operation, disruption response and repair
6. Risk management, resilience cycle and joint risk and resilience assessment and improvement panarchy phases covered: e.g. context analysis, risk identification, risk computation, risk mitigation, preparation, learning and adaption, response and recovery

7. System type of solution: e.g. cyber, computational, organizational
8. Persons involved: e.g. planners, maintenance, response and emergency managers, decision makers, technical simulation staff,
9. Threats covered: e.g. all physical and cyber threats that lead to (partial) leakages, pump or storage loss

4.2 RECOMMENDED CONOPS/ USE CASE DESCRIPTION APPROACH USING THE CONCEPTUAL MODEL

The report proposed and discussed serval options to use the developed Conceptual Model (CM) to determine concepts of operations (CONOPS) for technical cyber-physical security solutions of gas supply subsystems. All of them take advantage of the description dimensions of the gas supply system as developed within the conceptual model. It was emphasized that it is a key requirement of concepts of operation to determine the use case of the technical security solution in a straightforward understandable, comprehensive and concise way. Therefore, it was proposed to describe the use of the technical security solutions in tabular form using abstract system dimensions and respective attributes for each dimension along with comments.

The generation of such tables is rather straightforward when an idea of a technical security solution already exists. The tentative dimensions and attributes of the CM can be used to explicitly describe in detail the use case, i.e. the concept of operation of the technical security solution. This can be described by a step-wise process:

- Determination of CONOPS by dimensional analysis covering all combinations of dimensions using the dimensions and attributes proposed by the CM.

On the other hand, if as set of security solutions or even an overall security system needs to be assessed or generated, more generic processes can be employed, including:

- CONOPS generation by extending a cyber-physical risk management process with conceptual model dimensions (more focusing on classical risk control);
- CONOPS generation by extending a cyber-physical resilience response management process (resilience cycle) with conceptual model dimensions (more focusing on resilience enhancement);
- CONOPS generation by joint cyber-physical risk control and resilience assessment and enhancement panarchy process (risk and resilience panarchy), which intergraded risk and resilience analysis and management.

It has been found that the risk management based overall CONOPS generation process can also be considered as assessing all known and describable threats when requiring the risk management objective to control all known potential risk events to an acceptable level considering single as well as multipole potential event. In this case it can also be nicely illustrated how the consideration of additional dimensions has been conducted: the process needs to consider the disruption effects till sufficient recovery of system performance is reached thus covering the dimension resilience cycle management steps. In a similar way, all other dimensions were considered within the designed processes.

Using the sample conceptual model of section 4.1, the CONOPS of the rather detailed technical security solution “Predictive simulation of effects on pressure in case of gas infrastructure leakages” can be described as follows:

Using the CM, the description reads for example

1. Gas supply application cases covered: e.g. transmission
2. Gas supply system elements covered: e.g. pipes
3. System layer covered: e.g. physical, technical
4. etc.
5. Gas supply subsystem life cycle phases considered: e.g. risk control or resilience, disruption response and repair
6. Risk management, resilience cycle and joint risk and resilience assessment and improvement panarchy phases covered: e.g. risk identification, risk computation, risk mitigation, preparation, learning and adaption, response and recovery

7. System type of solution: e.g. cyber, computational
8. Persons involved: e.g. technical staff doing simulation, operation and emergency room operators, planners, response and emergency managers, decision makers,
9. Threats covered: e.g. all physical and cyber threats that lead to (partial) leakages of pipes.

REFERENCES

[1] Rob McLean and Chris Isidore, CNN Business. PG&E files for bankruptcy after California wildfires. https://edition.cnn.com/2019/01/29/business/pge-bankruptcy-fires/index.html (Accessed September 25, 2019).

[2] COMMISSION OF THE EUROPEAN COMMUNITIES. COMMUNICATION FROM THE COMMISSION on a European Program for Critical Infrastructure Protection, **2006**.

[3] Software Engineering Institute, Carnegie Mellon University. The Arcade Game Maker Pedagogical Product Line, **2009**.

[4] IEEE Std 1362™-1998 (R2007). IEEE guide for information technology--: System definition-- concept of operations (CONOPS) document, **1998**.

[5] Software & Systems Engineering Standards Committee of the IEEE Computer Society. ISO/IEC/IEEE 29148:2011(E), Systems and software engineering — Life cycle processes — Requirements engineering, **2011**.

[6] American Institute of Aeronautics and Astronautics; International Council on Systems Engineering; American National Standards Institute. *Guide to the preparation of operational concept documents;* American Institute of Aeronautics and Astronautics: Reston, Va., **2012**.

[7] IEEE Standards Association. Systems and software engineering -- Life cycle processes -- Requirements engineering, **2018**.

[8] Sokolowski, J.; Turnitsa, C.; Diallo, S. *A Conceptual Modeling Method for Critical Infrastructure Modeling*, **2008**.

[9] Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, **2014**, *121*, 43–60.

[10] Kotiadis, K.; Robinson, S. In: *2008 WINTER SIMULATION CONFERENCE, VOLS 1-5*; IEEE: 345 E 47TH ST, NEW YORK, NY 10017 USA, **2008**; pp. 951–958.

[11] Zanjirani Farahani, R.; Bakhshayeshi Baygi, M.; Mostafa Mousavi, S. 20 - Risk Management in Gas Networks: A Survey. In: *Logistics Operations and Management*. Farahani, R.Z., Rezapour, S., Kardar, L., Eds.; Elsevier: London, **2011**; pp. 421–439.

[12] Natural gas storage (Wikipedia). Natural gas storage: Usage (Accessed September 20, 2019).

[13] Papadakis, G.A. Major Hazard pipelines: a comparative study of onshore transmission accidents. *Journal of Loss Prevention in the Process Industries*, **1999**, *12*, 91–107.

[14] RESILENS. Realising European ReSILiencE for Critical INfraStructure: D5.2 Initial CONOPS Framework, **2016**.

[15] Häring, I.; Ebenhöch, S.; Stolz, A. Quantifying Resilience for Resilience Engineering of Socio Technical Systems. *Eur J Secur Res*, **2016**, *1*, 21–58.

[16] US Department of Defense. *Quadrennial Defense Review Report*, **February 2010**.

[17] Coast Guard Publication 3-0 (Operations). *Operations*, **February 2012**.

[18] U.S. Department of Homeland Security. *Fact Sheet*, **December 21, 2010**.

[19] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA ERA PMO). CONCEPT OF OPERATIONS (CONOPS v4.0), **2004**.

[20] AS/NZS ISO 31000:2009. *Risk management - Principles and guidelines*, **2009**.

[21] Thoma, K.; Scharte, B.; Hiller, D.; Leismann, T. Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches. *Eur J Secur Res*, **2016**, *1*, 3–19.

[22] Häring, I.; Sansavini, G.; Bellini, E.; Martyn, N.; Kovalenko, T.; Kitsak, M.; Vogelbacher, G.; Ross, K.; Bergerhausen, U.; Barker, K.; Linkov, I. Towards a Generic Resilience Management, Quantification and Development Process:

General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies. In: *Resilience and Risk*. Linkov, I., Palma-Oliveira, J.M., Eds.; Springer Netherlands: Dordrecht, **2017**; Vol. *6*; pp. 21–80.

[23] Linkov, I.; Palma-Oliveira, J.M. *Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains*, **2017**.

APPENDIX A

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