ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

D1.2

User-centred Requirements Initial Analysis

Definition and formalization of the functional and non-functional user requirements for the ANASTACIA framework, providing an overall description of the main services to be delivered and presenting the associated scenarios and Use Cases

Distribution level	PU
Contractual date	30.06.2017 [M6]
Delivery date	30.06.2017 [M6]
WP / Task	WP1 / T1.2
WP Leader	ATOS
Authors	S.Bianchi (SOFT), G.Troglio (SOFT), D. Belabed (THALES), A.Mady (UTRC), I.Farris (AALTO), L.Scudiero (AS), D.Rivera (MONT), R.Trapero Burgos (ATOS)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

ANASTACIA has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

Table of contents

PUBLIC SUMMARY

ANASTACIA will design, develop, evaluate and deliver a holistic framework (Figure 3) for the assessment of security and privacy in complex ICT systems, in particular IoT network architectures and Cyber Physical Systems (CPS).

Several technologies will be leveraged to obtain innovative results in the autonomic definition and implementation of mitigation plans to neutralize attacks or limit damages: in particular, ANASTACIA will use Software Defined Networks (SDN) and Network Function Virtualization (NFV) technologies, along with IoT controllers, to ensure the overall security of monitored systems, taking into account privacy constraints derived from the General Data Protection Regulation (GDPR) and other relevant regulations, standards and best practices.

Figure 1. ANASTACIA framework

This deliverable contains the result of the initial analysis of the user-centred functional and non-functional requirements for the ANASTACIA framework. Considering their relevance and the novelty aspect associated to the contextual assessment of both security and privacy by mean of the Dynamic Security and Privacy Seal (DSPS), privacy requirements have been kept separated from other (more technical) requirements.

The activity took into consideration different categories of users, focusing more on technical profiles in consideration of the expected Technology Readiness Level (TRL) 5 expected at the end of the project. Interviews with privileged observers were carried out to integrate the requirement analysis too.

Two application domains (Figure 2) have been considered for the elicitation of requirements and will be used for evaluation purpose during the validation phase: Mobile (Multi-access) Edge Computing (MEC) and Building Management System (BMS).

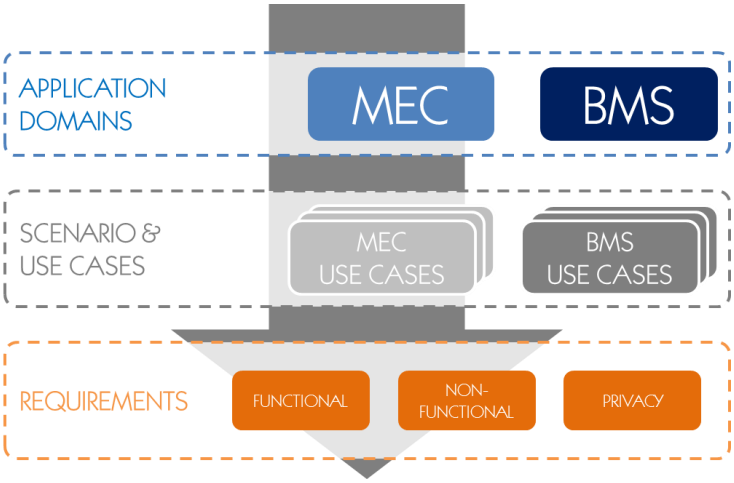

Figure 2. Requirement elicitation process

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document defines the user requirements for the ANASTACIA framework. The main aims are:

- to clarify and give an overall description of the services that the project will design and deliver;
- to describe the methodologies adopted in requirement elicitation and formalization;
- to present the Use Cases based methodology adopted for the functional requirements analysis;
- to define the technical requirements;
- to define the functional/non-functional requirements;
- to perform the Use Case analysis and modelling;
- to give some initial architectural indications about the software modules to be developed.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- Grant Agreement N°731558 and annexes ("Description of Action")
- D1.1 "Holistic Security Context Analysis"
- D1.3 "Initial Architecture Design"
- D7.2 "Initial Exploitation and Data Management Plan"

1.3 REVISION HISTORY

Version	Date	Author	Description
1	15/01/2017	G.Troglio (SOFT)	ToC (as proposed at the kick-off meeting)
2	26/01/2017	G.Troglio (SOFT)	Positioning, methodology
3	24/03/2017	S.Bianchi (SOFT)	Scenarios and use cases
4	30/04/2017	G.Troglio (SOFT)	Use Case templates
5	12/05/2017	S.Bianchi (SOFT)	Interviews, questionnaires, mock-ups
6	26/05/2017	D. Belabed (THALES), A.Mady (UTRC), D. Rivera (MONT)	Contributions on updated MEC and BMS use cases, technical integration requirements
7	05/06/2017	I.Farris (AALTO)	Contribution on updated MEC use case
8	07/06/2017	L.Scudiero (AS)	Privacy requirements
9	16/06/2017	G.Troglio (SOFT)	UML diagrams, requirement formalization
10	26/06/2017	R.Trapero Burgos (ATOS)	Update of UML diagrams
11	30/06/2017	S.Bianchi (SOFT)	Internal review, final editing and proof-reading

1.4 Acronyms and Definitions

Acronym	Definition
BGP	Border Gateway Protocol
BMS	Building Management Systems
CRUD	Create/Retrieve/Update/Delete
DoA	Description of Action
DPO	Data Protection Officer
DSPS	Dynamic Security and Privacy Seal
ECSO	European Cyber Security Organization
FR	Functional Requirement
GDPR	General Data Protection Regulation
MEC	Mobile Edge Computing / Multi-access Edge Computing
MVP	Minimum Viable Product
NFR	Non-functional Requirement
NFV	Network Function Virtualization
PR	Privacy Requirement
SDN	Software Defined Network
TRL	Technology Readiness Level
UC	Use Case
UML	Unified Modeling Language
VID	Virtualized Infrastructure Domain
VNF	Virtual Network Function

2 CONTEXTUALIZATION

2.1 SCOPE

ANASTACIA will develop a **trustworthy-by-design security framework** which will address all the phases of the **ICT Systems Development Lifecycle (SDL)** and will be able to take autonomous decisions through the use of new networking technologies such as **Software Defined Networking (SDN)** and **Network Function Virtualisation (NFV)** and **intelligent and dynamic security enforcement and monitoring** methodologies and tools. The ANASTACIA framework will thus include:

1. a **security development paradigm** based on the compliance to security best practices and the use of the security components and enablers;
2. a **suite of distributed trust and security components and enablers**, able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures;
3. a **holistic Dynamic Security and Privacy Seal**, combining security and privacy standards and real time monitoring and online testing.

The elicitation of user requirements for such a holistic framework definitively embraces all the components meant to ensure that addressed application domains will be provided with advanced capabilities (see Figure 3) for:

- **self-protection**,
- **self-healing**, and
- **self-repairing**.

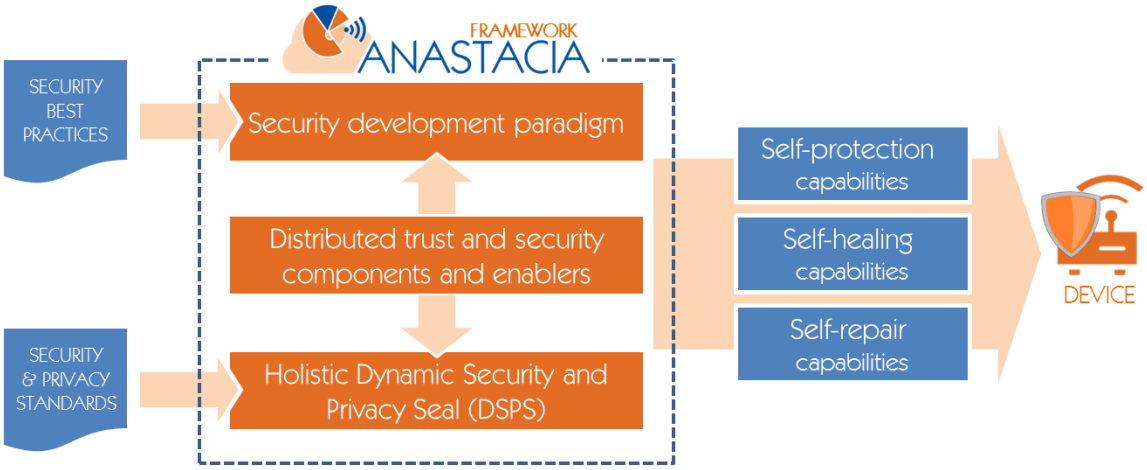

Figure 3. ANASTACIA framework components and provided functionalities

This deliverable has been prepared in parallel with several others complementary activities (see Figure 4). The results of the preliminary analysis included therein are thus mainly focused on inspiring technical work packages on how to take into considerations end users' needs while designing and developing the methodological and technical offerings expected from the ANASTACIA project.

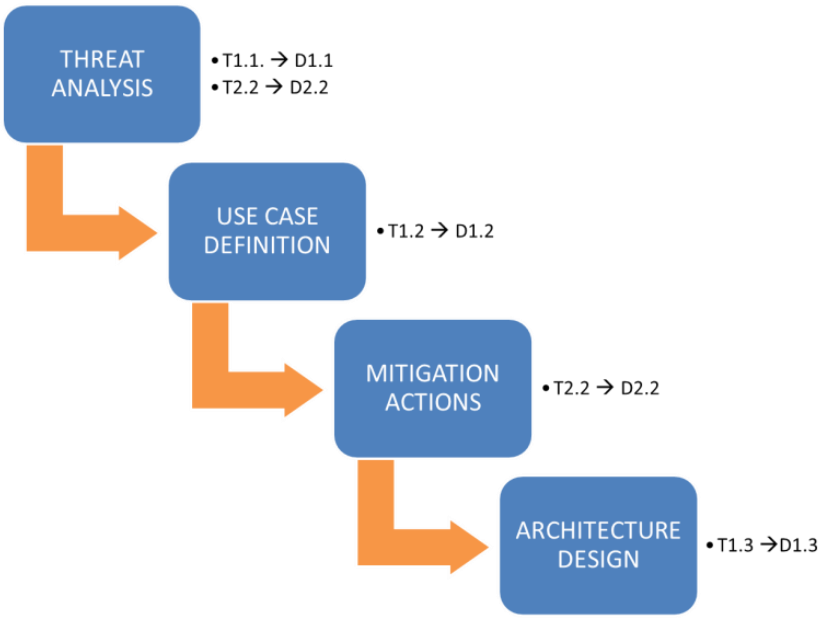

Figure 4. Relations between project's parallel activities that impact on end-user requirements.

This initial analysis will be further refined during the project, and in particular after the first validation and evaluation phase, in order to support also the industrialization phase that might ultimately lead to the release of an ANASTACIA-derived set of products.

The results of the second analytical cycle will be included in D1.4 "Final User-Centred Requirements Analysis" (see Figure 5) , which will constitute the basis for the refinement of technical results.

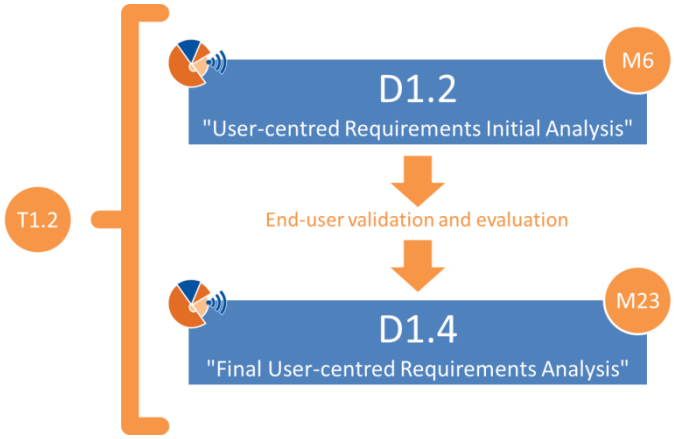

Figure 5. Relation between deliverables D1.2 and D1.4 associated to T1.2.

2.2 POSITIONING

The overall maturity of the ANASTACIA technology will be guaranteed by early prototyping and iterative improvement cycles focused on the two different business scenarios addressed, Mobile Edge Computing (MEC) and Building Management System (BMS).

As clearly indicated in the project proposal, considering the nature of the project (Research and Innovation Action) and the complexity of the addressed domain (cybersecurity in IoT/CPS and SDN/NFV architectures), **ANASTACIA globally aims to reach TRL 5** (see Figure 6).

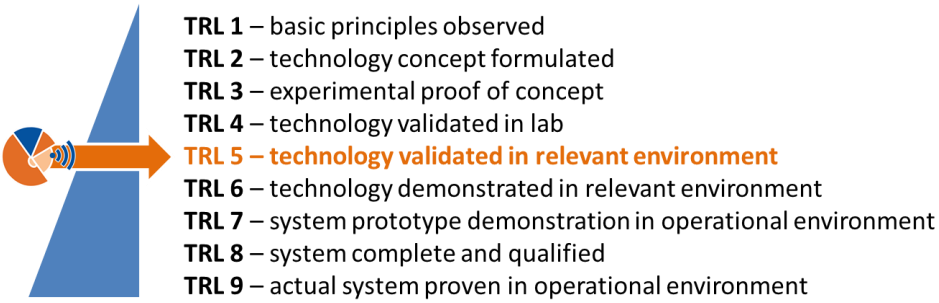

Figure 6. TRL positioning of the ANASTACIA project results.

The targeted TRL 5 positioning implies that:

- the project is not expected to release a fully functional / product-like prototype, but to validate innovative technologies in relevant environments (namely, the two MEC and BMS scenarios); this condition has two distinct impacts:
    - on user requirements: the intention of the authors of this deliverable is not to limit the analysis of requirements to the expected TRL5 but to consider also pre-industrialization and industrialization phase, providing an analysis that might ease the conversion of technological results into a product;
    - on exploitation plans: as anticipated, since the project is not expected to deliver a complete and qualified system, also commercial targets (associated also to the actual implementation of some specific features) might be adequately corrected.
- considering the complexity of the architecture and the different maturity of the technologies and tools to be adopted and integrated (including proprietary solutions provided by some beneficiaries), the envisaged TRL of the different ANASTACIA framework components will be monitored separately to verify the final global positioning (see Figure 7).

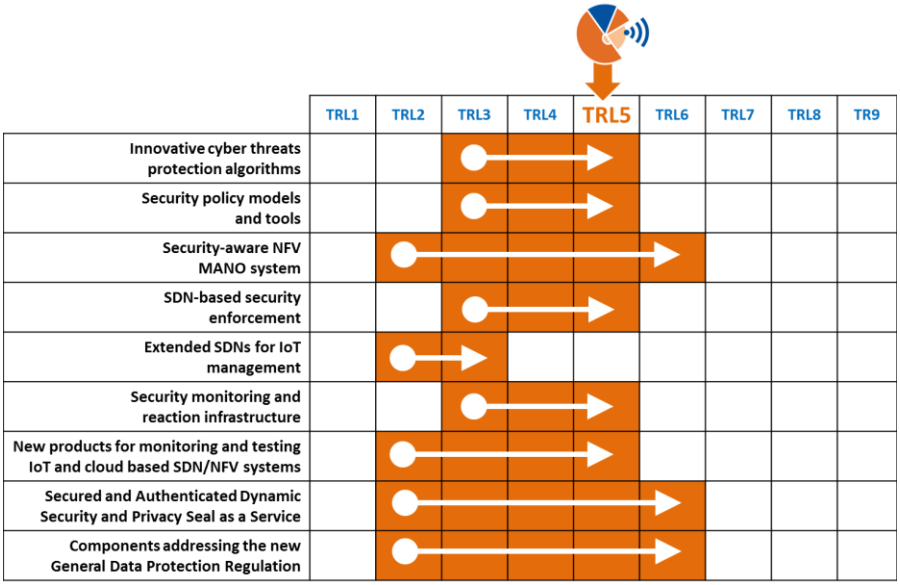

Figure 7. Expected TRL shifts for the preliminary identified sets of ANASTACIA components.

The analysis included herein is therefore meant to elicit the requirements of a potential ANASTACIA-powered product or solution, leaving to an internal discussion among beneficiaries and technology providers the final decision on which developments should be prioritized to allow a proper demonstration in the addressed use cases.

2.3 END USERS

The context of use of the main services which will be included in the ANASTACIA framework potentially includes several different user categories, all coping at different levels with security and privacy issues:

- SW developers
- IoT architects/developers
- SDN architects/developers
- NFV architect/developers
- Security managers
- Solution integrators
- Chief Security Officer (CSO)
- Chief Technology Officer (CTO)
- Chief Information Officer (CIO)
- Chief Information and Security Officer (CISO)
- Mobile Edge Computing/Multi Access Edge Computing (MEC) stakeholders
- Building Management System (BMS) stakeholders
- System / Network administrators
- Security professionals/consultants
- Lawyers
- GDPR-associated actors (e.g. Data Protection Officer, Data Processor, Data Controller, etc.)

Since **the holistic framework under development spans over different levels of technical complexity and addresses different needs** (from methodological guidelines to dynamic real-time sealing/certification, through a complex set of enablers and components), the requirements that can be expressed by the categories mentioned above can be really different in terms of e.g. complexity, usability, UI: whereas technical profiles might be more interested in interoperability/integrability/autonomic features etc., end-users (mainly those involved in the management procedures in the addressed domains) might privilege other high-level aspects such as usability aspects, configurable dashboards, report generation, etc.

Considering the declared project positioning in terms of TRL, the Consortium agrees to **focus in this initial phase more on technical profiles and associated needs**, stressing more the analysis on functional and non-functional requirements associated to the inner architectural components. Nevertheless, the Consortium also considers the possibility to gradually target all the aforementioned groups as for dissemination and exploitation activities, in order to gain visibility in the sector, integrate potential valuable feedback from interested stakeholders and finally optimize the released prototypes.

2.3.1 Interviews

As indicated in the DoA, part of the activities of task T1.2 included **interviews and focus groups with potential end-users and stakeholders** organized to preliminarily identify the user needs, discuss expected development and compare expectations with the overall methodological an technical approach adopted within the project. To this end, a simple questionnaire was designed to gather general information on the perceived value-added of the ANASTACIA's offering as well as on contextual information on other potential application domains, with the overall goal of generalizing the technical solutions primarily designed to be applied and evaluated in the MEC/MAEC and BMS scenarios. The "**Stakeholders & end users' questionnaire**" was designed to:

- briefly introduce the main ANASTACIA concepts;

- gather an overall evaluation of ANASTACIA's objectives (in terms of priority);
- collect information of contextual cybersecurity issues (in pilot domains and other domains);
- obtain indications on non-technical features interesting for stakeholders/customers.

The questionnaire was forwarded to a list of selected privileged observers and stakeholders in order to minimize the efforts to gather meaningful feedback (participants' effort was not covered by a dedicated budget, since they work for institutions that are not directly involved in the project):

- **Innovation Advisory Board Members**
  - Diego R. Lopez (Telefonica, ES)
  - Jesus Luna (Bosch, DE)
  - Christian Mastrodonato (Konica Minolta, UK)
  - Stefano Secci (LIP6, FR)
- **Privileged observer in pilot domains**
  - BMS: Vijay Lakamraju (Cybersecurity Leader for UTC products, US)
  - MEC/MAEC: Stefano Secci (LIP6, FR)
- **Others professional experts**
  - Roberto Pastorino (Cleis Security, System Engineer, IT)
  - Oriano Sità (Italeaf, Chief Information Officer, IT)
  - Lorenzo Papini (Selesoft, Geographic TLC Network Expert, IT)
  - Marco Grechi (Senior SCADA Systems & Telecomms Specialist, Member of IEC TC57, IT)
  - Luca Caviglione (Researcher at CNR-ISSIA, IT)
  - Mark Miller (CEO of CONCEPTIVITY, Vice Chairman of EOS, Member of the Board of Directors at European Cyber Security Organisation, UK)

Annexes include short CVs and the questionnaires with the participants' answers. For the sake of privacy, no correspondence between interviewees and questionnaires is reported. Section 5 includes an analysis of the feedback collected to be provided to designers and software architects as general guidelines.

2.3.2 Questionnaire

Privileged observers', Stakeholders' & End Users' questionnaire

Introduction

The heterogeneous, distributed, and dynamically evolving nature of Cyber Physical Systems (CPS) based on Internet of Things (IoT) and virtualised cloud architectures introduces new and unexpected risks that cannot be solved by current state-of-the-art security solutions.

For this, new paradigms and methods are required in order

- to build security into the ICT system at the outset,
- to adapt to changing security conditions,
- to reduce the need to fix flaws after deploying the system, and
- to provide the assurance that the ICT system is secure and trustworthy at all times.

The main objective of the ANASTACIA project is to address these concerns by researching, developing and demonstrating a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures.

To this end, ANASTACIA will develop a **trustworthy-by-design security framework** which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools.

The ANASTACIA framework will include:

- a **security development paradigm** based on the compliance to security best practices and the use of the security components and enablers (this will provide assisted security design, development and deployment cycles to assure security-by-design);
- a suite of **distributed trust and security components and enablers**, that are able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation of the system to mitigate new and unexpected security vulnerabilities);
- a **holistic Dynamic Security and Privacy Seal**, combining security and privacy standards and real time monitoring and online testing (this will provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users).

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
2. How is cybersecurity generally managed in your domain[3]?
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
6. Who do you think might use ANASTACIA in your domain?
7. Who do you think might benefit the most from ANASTACIA in your domain?
8. Would you consider using a solution based on ANASTACIA (see description above)?
9. Is there any recommendation you would like to give our project at design / development phase?
10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use		has intuitive / adaptive user interfaces	
low cost		provides real-time feedback	
powerful reporting		includes dynamic network topology	
well supported		developed by big vendors	
flexible to customise		modular architecture	
scalable to grow		compliant with standards	
large, well-known vendor		autonomous reaction to threats	
good feedbacks / reputation		self-healing / self-repair capabilty	
integrates with other software		highly configurable (e.g. rule editing)	
licensed as open-source		other (.....)	

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

Figure 8. Stakeholders' & end users' questionnaire (introduction and evaluation form)

3 USE CASE METHODOLOGY

This chapter briefly illustrates the methodology adopted in designing the Use Cases in the user requirements analysis. A Use Case template is also proposed on the basis of a comparative analysis of models suggested by OO approaches and UML.

3.1 GOALS

The main objectives of Use Cases are to find out, describe and record functional and non-functional requirements, by writing scenarios of use of the system to be designed, in order to fulfil the various goals.

A Use Case eases the definition of the set of requirements according to which the system needs to behave, describing an interaction between external actors and the system and documenting the specific functions that the system will perform.

A complete and detailed definition of possible Use Cases usually guarantees a correct development with less effort in fixing functional bugs and also provides a trustable guideline for tests and validation of the solutions developed.

3.2 MODEL

In the following, the terminology adopted for the definition of the Use Cases is defined.

- A **scenario** describes a user story and presents the involvement of the system in achieving a predefined goal and the system expected functionalities. A scenario is usually written in narrative form and defines the users of the technology, their needs, and their knowledge. Scenarios are generally written at the beginning of a project, during discovery and requirement gathering phases. They provide guidelines for the design and development phases, by providing tangible faces, names and stories for how the technology will be used.
- A **user story** is meant to replace long and complex documentation with short sentences that describes the needs of a user. They are short and granular: each story describes a single task or action. User stories are defined during development, usually before (or at the beginning of) each development sprint.
- A **use case** captures the actions that are required to accomplish a goal. It defines the interactions between external actors and the system. A use case describes each step of the process including inputs, outputs, errors, and exceptions and presents multiple “paths” that can be taken by any user at any time.
- A **usage scenario** is a single path through the use case.
- An **actor** interacts with the system to achieve a predefined goal. Actors can be either humans or external systems: they must be able to make decisions.
- A **UML diagram** is a visual representation of a written usage scenario. A diagram can be generated for each usage scenario, in order to formalize it.
- A **Use Case Template** is a form which allows to collect and structure all the information required to define and clarify a Use Case.

Figure 9 provides a graphical representation of the aforementioned definitions and their connections.

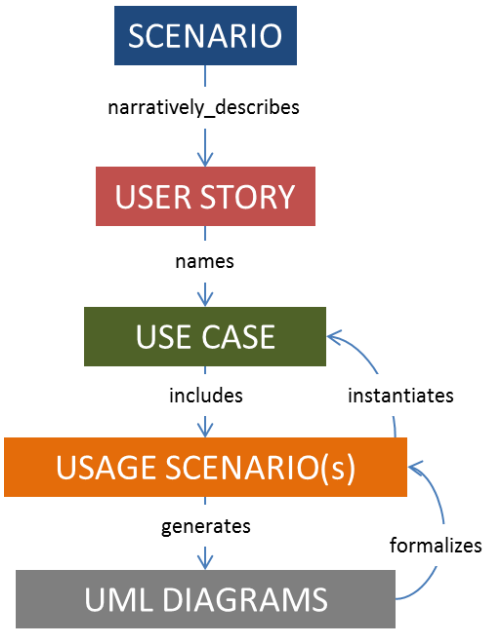

Figure 9. Graphical representation of the Use Case terminology and relations.

3.3 GUIDELINES

A Use Case has at least a name and a step-by-step description of a basic course of action, including:

- triggering events;
- necessary event response;
- pre-conditions and post-conditions;
- sequence of exchanged messages and performed actions;
- data exchanged;
- non-functional technical constraints (reliability, performance, cost etc).

Each Use Case is then composed by a beginning, a main body and an ending.

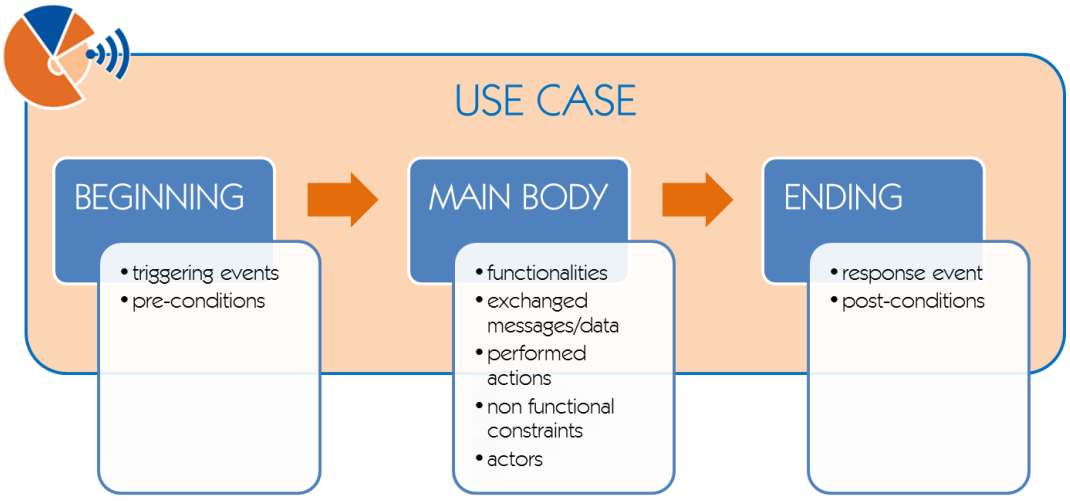

Figure 10. Use Case composition

Figure 10 lists all the attributes that are necessary to build *in scope* Use Cases: other complementary fields/attributes are listed and described in the Use Case template and can be optional.

The Use Cases are developed iteratively through three steps:

- inception;
- elaboration;
- construction.

During the *inception* phase the Use Case form should be the simplest one, e.g. one of the following:

- Use Case name + brief description (one to five sentences describing what the Use Case does);
- Use Case name + outline (bulleted list of Use Case steps without alternative flows).

In this phase the end-users suggest the main scenarios of use of the system and compare them with the technological opportunities suggested by the developers / software engineers.

The *elaboration* phase is where architectural relevance and risk factors of the Use Case are stated. In this phase the Use Cases are detailed so to enable developers to build and test derived scenarios.

During the *construction* phase the remaining behavior of the system is filled in by detailing the remaining Use Cases' flows.

At the end of these three phases all the necessary fields of the template are usually completely filled in, and the Use Case UML diagrams development can start to help formalizing the requirements for developers.

3.3.1 Contextualization

In order to create *in scope* Use Cases, the domain of the project has to be clearly defined, identifying:

- overall context of the project;
- main data categories
- main stakeholders;

The list of *in scope* Use Cases should be derived from this context analysis.

Each Use Case should describe an action that is necessary for the user to achieve a project goal or objective and should not be overly complex.

3.3.2 Validation

In order to avoid the analysis of *out of scope* Use Cases (or a wrong definition of priority) it is necessary to validate each Use Case investigating if and how it models a functionality of the system (this check can be achieved by defining a set of specific questions).

This phase should also filter available Use Cases defining an outline for the different release of the system by gradually integrating solutions to different Use Cases.

3.3.3 Naming

There are two ways to generate Use Case and actors names:

1. listing all the actors and then naming relative Use Cases;
2. listing all the Use Cases and then naming each Use Case's actors.

Considering the applications ANASTACIA will be developed for, in this first phase the project will adopt the second modality, focusing first on functionalities and services of the system and then deriving all participating actors (it should also be considered that in Use Cases theory an actor is a specific role played by an entity and not an entity itself, i.e. a person or a system can play as different actors within different

Use Cases). All qualified objects appearing in Use Cases' names will be properly defined in the project glossary and added to the domain model as a class, entity or attribute.

3.3.4 Style

As a general approach, Use Cases has been written in an essential style, keeping out collateral topics such as user interfaces and technical requirements and focusing on actors' intent, i.e. ignoring when possible "how" an interaction between the actors and the system is performed and concentrating on "what" they do which produce a valuable result.

While developing the Use Cases it is also necessary to maintain a correct level of detail, considering that it is possible at any phase to scale both up and down in terms of sophistication and formality, depending on actual needs. Once a correct formalization is obtained, the Use Cases can be generalized or further specified easily: the necessity of defining super and sub Use Cases could result eventually in a partial review of the previous design activity.

3.3.5 Template

The following template derived from the Cockburn's Use Case Template[1] is proposed:

USE CASE TEMPLATE		
A	**Use Case ID**	*UC_ID*
B	**Use Case Name**	*action verb + [qualified] object*
1.	**Primary actors**	List of primary actors involved in Use Case
2.	**Supporting actors**	List of supporting actors involved in Use Case
3.	**Description**	Description of the Use Case
4.	**Stakeholders' interests**	Stakeholders and their interests in the Use Case
5.	**Triggers**	Any external event or Use Case that triggers this Use Case
6.	**Pre-conditions**	The state of the system and values for pertinent attributes before the Use Case
7.	**Normal flow**	[*UC_ID*]
		Course of Actions 1. Step_1… 2. Step_2 3. Step_3…
8.	**Alternate flows**	Alternative flow ID [*UC_ID-AF_ID*] & name
		Course of Actions 1a. Step_1a 2a. Step_2a …
9.	**Flow exceptions**	Exception ID [*UC_ID-EXC_ID*] & name
10.	**Post-conditions**	The state of the system and values for pertinent attributes after the Use Case , no matter which flows were executed
11.	**Additional requirements**	List any additional requirements that the Use Case must meet
12.	**Notes and issues**	List of notes and issues to be resolved

[1] http://alistair.cockburn.us/usecases/uctempla.doc

4 SCENARIOS AND USE CASES

This chapter includes the description of several addressed scenarios, which help defining a functional description of the goals of ANASTACIA and an overview of the requirements that the software services to be developed need to address.

The technological solutions proposed by ANASTACIA will be tested and demonstrated in two extremely influential business sectors: **Mobile Edge Computing** (now commonly indicated also as Multi Access Edge Computing) and **Building Management Systems**.

For each proposed scenario, whenever considered relevant, the advantages led by ANASTACIA will be presented mapped onto the envisaged architectural planes (as preliminary indicated in the project proposal, see Figure 11):

1. the **data plane** that establishes network communication between devices and components;
2. the **control plane** that manages the resource usage and real-time operation of the services;
3. the **autonomic plane** that defines mitigation plans and enforces security mechanisms and real-time reconfiguration and adaptation of the services;
4. the **user plane** that provides interfaces and tools to end-users for policy definition, service monitoring and management;
5. the **seal management plane** combining security and privacy standards with real time monitoring.

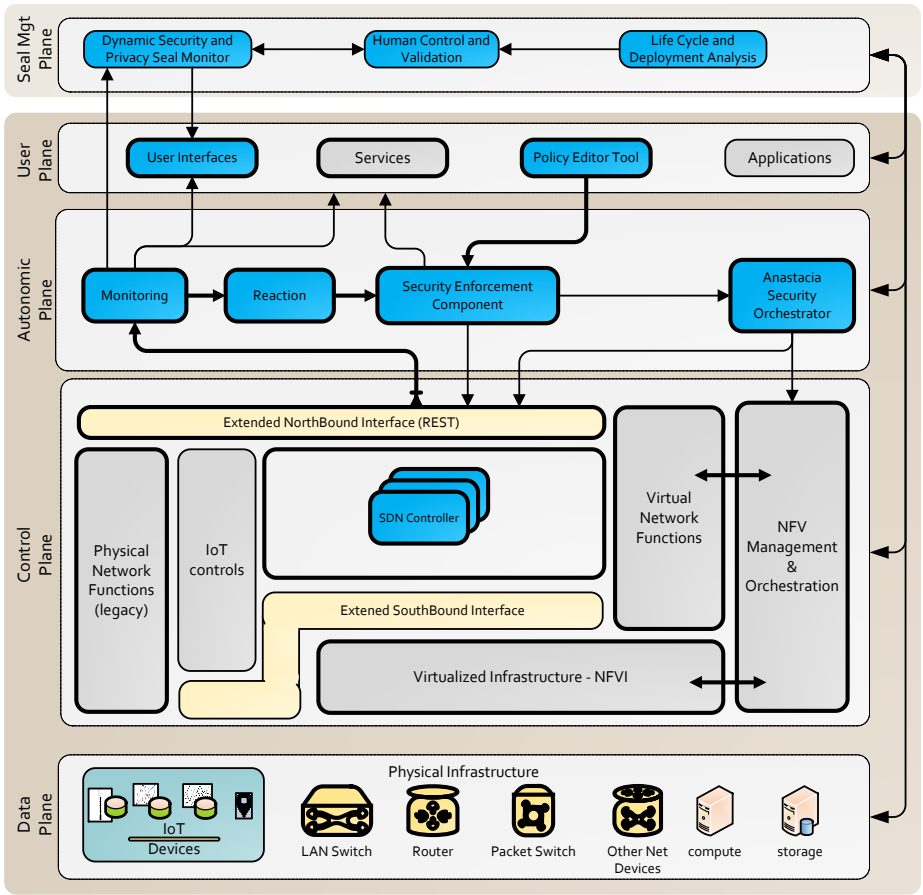

Figure 11. ANASTACIA architecture (and associated planes) as initially included in the project proposal

4.1 REFERENCE SCENARIO

4.1.1 Secure/privacy-compliant Campus ICT infrastructure management

This first overarching use case is the result of an exercise carried out by the whole Consortium during the plenary meeting in Murcia (ES) in early May 2017, meant to go through the whole architecture to identify 1) a reference general "functional behaviour", 2) the main functionalities to be provided to support it and 3) possibly missing modules/components. This use case therefore goes through all the main ANASTACIA conceptual planes (see Figure 12) whereas the other following sections includes more specific use cases derived from the pilot domains where the ANASTACIA framework will be evaluated.

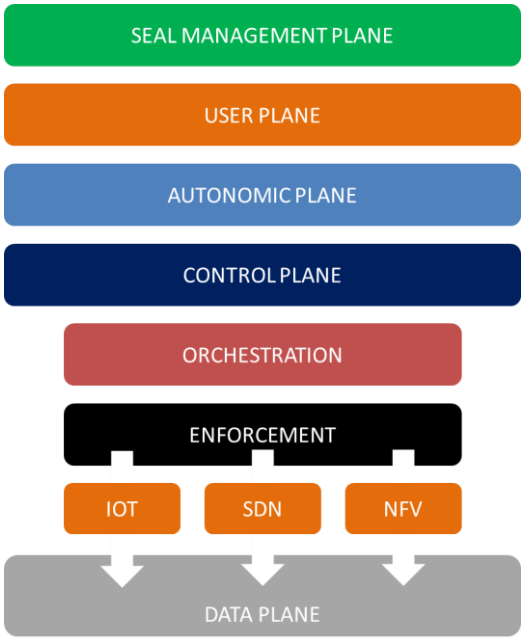

Figure 12. ANASTACIA architecture planes (simplified view)

4.1.1.1 Narrative description

The Keamanan Campus is renowned for having a sophisticated ICT/IoT infrastructure that controls all main buildings and facilities in the Campus, which are under the direct responsibility of the Campus Manager, Mr Cahaya Budi.

In parallel to several BMS tools, Mr Budy has a brand new installation of an ANASTACIA-powered security & privacy monitoring solution, which allows him to have an immediate view of the status of the monitored infrastructure without the burden of checking different dashboards and inspecting technical logs: a nice Dynamic Security & Privacy Seal (DSPS) change its status according to detected threats, whereas a simplified UI summarizes the main mitigation actions autonomously undertaken by the system. The DSPS is green since the ANASTACIA-powered solutions was installed, several months ago, when Mr Budi also easily configured the main security policies according to the internal Campus regulations.

Yet, on a sunny Monday morning, an anomalous traffic is detected coming from a part of the network devoted to the management of CCTV security cameras, that

register videos from many different places and forward them to a proxy server, where streaming are pre-processed before relevant information (i.e. video sections in which people access restricted labs) are sent for storage and further inspection to the CED in the central control room.

The potential threat is immediately detected by the system that, according to the security policies currently deployed, notifies Mr Budi changing the colour of the DSPS (from green to orange), suggesting potential privacy breaches that should be further investigated and starting the definition of a mitigation plan meant to limit any potential damage.

The ANASTACIA-powered system takes action at three different levels:

1) as for IoT devices under potential attack (this time, the CCTV cameras), the system momentarily shuts them down to limit any further problem;

2) at security level, by means of dedicated security VNFs, the system automatically deploys several different virtual appliances (a firewall, an AAA server, an Intrusion Detection System) in order to intensify the monitoring and reinforce the overall security level;

3) at network level, the system reconfigures the whole setup in order to leverage SDN functionalities and temporarily isolate the part of the network under attack, redirecting the traffic to a duplicated pre-processing edge server according to the newly defined network. Cameras are then gradually reactivated, in order to verify which specific device has been hacked or if the detected anomalous traffic has to be considered somehow a "false positive".

Mr Budi, who is not a network expert and ignores most of the sophisticated network/security technologies that are used by the system to define and enforce the mitigation plan, gets a simplified report of the main actions undertaken.

Furthermore, he also receives a notice on potential privacy issues that should be further investigated, since he is also the Campus Data Controller: in particular, the identified threats, impacting on a server that processes video streaming captured when access to restricted labs are detected by motion sensors, might have caused a data leakage related to sensitive information, and deserve further attention by the ICT staff, that is thus immediately summoned for an internal meeting to verify any data leakage.

Notwithstanding the mitigation actions were successfully undertaken and all functionalities were efficiently restored, the DPSP stays orange, until a manual confirmation that also privacy issues have been duly addressed is provided by Mr Budi and the ICT staff – both security and privacy are then fully restored.

4.1.1.2 Architectural planes

*The **Data Plane** ensures that all IoT devices are properly monitored and controlled by ANASTACIA distributed agents and enablers.*

*The **Control Plane** provides a fully-fledged set of controlling functionalities encompassing IoT, SDN and VNF controllers, able to enforce the mitigation plan that has been automatically generated by the system to put the system back in a secure and privacy-compliant state.*

*The **Autonomic Plane** is able to define the contingency actions and support the whole monitoring/reaction/orchestration cycle.*

*The **User Plane** includes the configuration tools for privacy and security policy definition, used to define the main constraints that must be satisfied at system level.*

*The **Seal Management Plane** finally provides a dynamic view of the security and privacy-compliancy of the monitored system.*

4.1.1.3 Involved actors

Generally speaking, the main actors involved in this overarching use case includes:

- the monitored system;
- the ANASTACIA system;
- the system manager;
- the external attackers.

4.1.1.4 Use case steps

See the following formalized template.

4.1.1.5 Use case O.1

USE CASE O.1		
A	**Use Case ID**	*UC_O.1*
B	**Use Case Name**	*Overarching use case*
	Primary actors	ANASTACIA platform
	Supporting actors	Administrator, monitored system, cyber-attackers
	Description	The ANASTACIA platform, installed to protect the ICT infrastructure of a Campus, detects a potential attack and define a mitigation plan that encompasses all the control functionalities at IoT/SDN/VNF levels.
	Stakeholders' interests	To protect the Campus ICT infrastructure from any potential attack.
	Triggers	An anomalous traffic from a CCTV camera is detected.
	Pre-conditions	The Campus is instrumented with ANASTACIA agents and enablers to support the full monitoring/reaction/orchestration/enforcement cycle. The network and all included devices are fully modelled and documented. Security and privacy policies are in place properly configured.
	Normal flow	[*UC_O.1*]

Course of Actions

1. The ANASTACIA platform monitors signals, event logs, status reports, network traffic, etc.
2. The ANASTACIA platform detects a running attack.
3. The ANASTACIA platform notifies the detected attack.
    a. As for security, a feedback on the potential nature of the threat is provided, along with all available technical information.
    b. As for privacy (as no cause-effect can be defined a priori between threat and privacy breach), a feedback on the potential effects of the threat to be further investigated is provided.
    c. As for the Dynamic Security and Privacy Seal, the status is changed accordingly.
4. The ANASTACIA platform defines a mitigation plan according to the predefined security and privacy policies.
    a. As for IoT-level, mitigation actions are planned accordingly (e.g. direct commands, patches etc.) – in this case, the system momentarily shuts cameras down to limit any further problem;
    b. As for SDN-level, mitigation actions are planned accordingly (e.g. reconfiguration of the network) – in this case, at network level, the system reconfigures the whole setup in order to leverage SDN functionalities and temporarily isolate the part of the network under attack, redirecting the traffic to a duplicated pre-processing edge server according to the newly defined network.
    c. As for VNF-level, mitigation actions are planned accordingly – in this case, the system automatically deploys several different virtual appliances (a firewall, an AAA server, an Intrusion Detection System) in order to intensify the monitoring and reinforce the overall security level.
5. The ANASTACIA platform checks if the mitigation plan alters somehow the original privacy policies and notifies the modification accordingly, orchestrating and enforcing the plan according to the defined priorities.
6. The ANASTACIA platform orchestrates the mitigation plan, leveraging actions at IoT/SDN/NFV level.
7. The ANASTACIA platform enforces the mitigation actions included in the mitigation plan.
8. The ANASTACIA platform checks that all original functionalities are fully restored after the successful implementation of the mitigation plan.
9. The ANASTACIA platform provides a feedback (e.g. log/list of reconfigurations/actions) on the implemented mitigation plan and change the status of the DSPS accordingly.
    a. Two different actions are executed: from one side, activities logging (to storage drives); from the other one, alert and warning notification (to the user/administrators).

	Alternate flows		
	Flow exceptions		
	Post-conditions	The operability of the ICT system of the Campus has been re-established and all functionalities are restored.	
	Additional requirements	Real time notification of the attack. Immediate suspension of data flow in case of suspected attack.	
	Notes and issues		

4.2 MOBILE (MULTI-ACCESS) EDGE COMPUTING

4.2.1 Spoofing attack on the security camera system

4.2.1.1 Narrative description

A smart security camera system was installed in a city to prevent illegal actions. The recorded videos are sent to nearby MEC servers which can operate a data pre-treatment before sending interesting information to the Cloud. A group of hackers wants to have access to the unprocessed videos to obtain critical information about citizens, in order to blackmail them. They want to use a spoofing technique to make the cameras believe their servers are the MEC servers. They managed to get the IP address of the server and they are able to use it.

To prevent this attack, Bob, the Administrator, will use ANASTACIA to ensure that the security camera systems allows data exchange only between trusted equipment, by using secure protocols, authentication, correct network access controls and system design. ANASTACIA will be used to monitor and use Penetration Testing modules to quickly react in order to eliminate this intrusion. ANASTACIA will be used to provide a quality-of-security seal that ensures that systems are correctly patched against such technique and will deploy Firewalls with DPI capability VNF in the proper locations.

4.2.1.2 Architectural planes

*ANASTACIA architecture **Data Plane** will ensure Bob that all the elements of the security camera system are well connected to allow safe and secure operations.*

*The **Control Plane** will offer Bob advanced SDN technologies that will enable secure communication of security cameras content with traffic isolation. The control plane will ensure that the different MEC network elements can be trusted, avoiding cameras to give their information to the wrong, malicious server. Moreover, the NFV infrastructure will allow moving the video services running into*

MEC infrastructure in a different location in order to escape from the spoofing attack.

*The **Autonomic Plane** will reduce the manual tasks that such service needs for security configuration, and most of all, allows to dynamically adapt it to the current situation function of what monitoring observes. The 'Monitoring' component will enable continuous monitoring of different signals, event logs, status reports, video information, etc., in order to enable the detection of a behaviour hiding a spoofing attack considering known policies, models, and threat signatures. e.g., malicious users using the MEC server IP address to obtain information from a camera. Such situations will be analysed by the 'Reaction' component which will evaluate the gravity of the situation. After that, isolation and predictive mechanisms will be activated to ensure that the rest of the camera security system is not affected. Policies and rules are activated, updated, and enforced by the 'Security Enforcement' component, e.g., frequently changing the MEC server IP address and making sure that trusted cameras know the new address.*

*The components of the **User Plane** will help Bob in the deployment of ANASTACIA security environment. Through the 'User Interface', Bob can configure and supervise the different autonomic security functions running to ensure the video service securing. The 'Policy Editor' component will enable Bob to define high level network access control policies (e.g., who has access to the MEC Server), inter-networking, reaction and escalation regulations.*

4.2.1.3 Functionalities

In the following paragraphs, the main functionalities are listed, divided per plane.

4.2.1.3.1 Data plane

ANASTACIA platform protects the elements of the security camera systems and ensures that their connection is safe and secure.

4.2.1.3.2 Control plane

ANASTACIA platform orchestrates the communication among network devices, through advanced SDN technologies.

ANASTACIA platform ensures that the different MEC network elements can be trusted, avoiding cameras to give their information to the wrong, malicious server.

ANASTACIA platform allows moving the video services running in the MEC infrastructure in a different location to escape from the spoofing attack, thanks to the NFV technologies.

4.2.1.3.3 Autonomic plane

The Autonomic plane enables the platform to dynamically adapt to the current situation, providing the following functionalities.

ANASTACIA platform (through the monitoring component) monitors signals, event logs, status reports, etc.

ANASTACIA platform enables the detection of a behaviour hiding a spoofing attack considering known policies, models, and threat signatures.

ANASTACIA platform (through the reaction component) analyses the gravity of the situation.

ANASTACIA platform activates predictive mechanisms to isolate the attack.

ANASTACIA platform (through the Security Enforcement component) activates, updates, and enforces its policies and rules.

4.2.1.3.4 User plane

ANASTACIA platform (through the user interface) enables the user to configure and supervise the different autonomic security functions to secure the video service.

ANASTACIA platform (through the Policy Editor component) enables the user to define high level network access control policies (e.g., who has access to the MEC Server), inter-networking, reaction and escalation regulations.

4.2.1.4 Involved actors

The actors are:

- The **system administrator** of a smart security camera system, which was installed in a city to prevent illegal actions.
- The **ANASTACIA platform**, installed and used by the administrator in order to ensure that the security camera systems allows data exchange only between trusted equipment, by using secure protocols, authentication, correct network access controls and system design.
- A group of **hackers**, who want to have access to unprocessed videos stored in a system server, in order to obtain critical information about citizens and to be able to blackmail them.

4.2.1.5 Use case steps

The use case is divided into the following steps.

- The hackers get the IP address of the server.
- The hackers try to access the server.
- The ANASTACIA platform monitors signals, event logs, status reports, etc.
- The ANASTACIA platform detects an intrusion.
- The ANASTACIA platform scores the gravity of the attack.
- The ANASTACIA platform reacts to eliminate the intrusion, activating isolation and predictive mechanisms:
    - The ANASTACIA platform sends an alert to the system administrator
    - The ANASTACIA platform changes the IP address of the server.
- The ANASTACIA platform enables the administrator to configure and supervise the functions.
- The administrator reacts to the alert:
    - The system administrator identifies the attack as a real intrusion.
    - The system administrator accepts the change of IP address.

4.2.1.6 Use case MEC.1

In the following table, the first use case is presented.

USE CASE MEC.1		
A	**Use Case ID**	*UC_MEC.1*
B	**Use Case Name**	*Spoofing attack to a smart security camera system*

	Primary actors	ANASTACIA platform
	Supporting actors	Administrator, cyber-attackers
	Description	The ANASTACIA platform, installed to protect a network infrastructure including a smart security camera system, detects and reacts to a spoofing attack
	Stakeholders' interests	To protect the system from a spoofing attack and avoid the intrusion
	Triggers	A crew of hackers gets the IP address of the server and tries to access it.
	Pre-conditions	A smart security camera system was installed and the ANASTACIA platform was deployed and configured to protect all the acquired, exchanged and stored data.
	Normal flow	[*UC_MEC.1*]
		Course of Actions 1. The ANASTACIA platform monitors signals, event logs, status reports, etc. 2. The ANASTACIA platform detects an intrusion. 3. The ANASTACIA platform scores the gravity of the attack. 4. The ANASTACIA platform reacts to eliminate the intrusion, activating isolation and predictive mechanisms a. The platform sends an alert to the system administrator b. The platform changes the IP address of the server. 5. The ANASTACIA platform enables the administrator to configure and supervise the functions. 6. The administrator reacts to the alert: a. The administrator identifies the attack as a real intrusion. b. The administrator accepts the change of IP address
	Alternate flows	
	Flow exceptions	
	Post-conditions	The state of the system has been re-established, the hackers attack has been avoided, and the server IP address has been changed. Information flow from the camera system is maintained.
	Additional requirements	Real time notification of the attack. Immediate suspension of data flow in case of suspected attack.
	Notes and issues	

4.2.2 Man-in-the-middle attack on the MEC server Scenario

4.2.2.1 Narrative description

A SME offers security camera systems to its clients by proposing Mobile Edge Computing Solutions. Eve is a disgruntled employee who wants to damage the company's image, by spreading on the internet sensitive security videos from its employer's biggest client. Their security cameras are sending all of the recorded videos to MEC servers, deployed by the security SME in its client sites, to operate the information processing. As Eve was working in this biggest client security cameras project, she illegally kept all the credentials and certificates enabling her to decrypt the transmission between the MEC server and the cameras, which allows her to organize a man-in-the-middle attack, and download the videos on her home computer.

However, Bob, the administrator will use ANASTACIA to ensure that the system can react to minimize such attacks. ANASTACIA will assist BOB to provide an enforced network access policy and allow him to protect the change of credentials.

4.2.2.2 Architectural planes

*ANASTACIA architecture **Data Plane** will ensure Bob that all the elements of the security camera system are well connected to allow safe and secure operations.*

*The **Control Plane** will offer Bob advanced software defined networking (SDN) technologies that will enable secure deployment and operation of security cameras. The control plane will ensure that the network elements can be trusted, avoiding cameras to give their information to the wrong, malicious server. Moreover, the NFV infrastructure will allow moving the video services running into MEC infrastructure in a different location in order to escape from a man-in-the-middle attack.*

*The **Autonomic Plane** will reduce the manual tasks that such service need for security configuration, and most of all, allows to dynamically adapt it to the current situation function of what monitoring observe. The 'Monitoring' component will enable continuous a monitoring of different signals, event logs, status reports, video information, etc., in order to enable the detection of a behaviour hiding a man-in-the-middle attack considering known policies, models, and threat signatures. e.g., frequently changing the certificates and passwords. Eve, using credentials and certificates to get information from a camera will be analysed by the 'Reaction' component which will evaluate the gravity of the situation. After that, isolation and predictive mechanisms will be activated to ensure that the rest of the camera security system is not affected. Policies and rules are activated, updated and enforced by the 'Security Enforcement' component, e.g., frequently changing the certificates and passwords.*

*The components of the **User Plane** will help Bob in the deployment of ANASTACIA security environment. Through the 'User Interface', Bob can configure and supervise the different autonomic security functions running to ensure the video service securing. The 'Policy Editor' component will enable Bob to define high level network access control policies (e.g., who has access to the MEC Server), inter-networking, reaction and escalation regulations.*

4.2.2.3 Functionalities

In the following paragraphs, the main functionalities are listed, divided per plane.

4.2.2.3.1 Data plane

ANASTACIA platform protects the elements of the security camera systems and ensures that their connection is safe and secure.

4.2.2.3.2 Control plane

ANASTACIA platform orchestrates the communication among network devices, through advanced SDN technologies.

ANASTACIA platform ensures that the different MEC network elements can be trusted, avoiding cameras to give their information to the wrong, malicious server.

ANASTACIA platform allows moving the video services running into MEC infrastructure in a different location to escape from the spoofing attack, thanks to the NFV technologies.

4.2.2.3.3 Autonomic plane

The Autonomic plane enables the platform to dynamically adapt to the current situation, providing the following functionalities.

ANASTACIA platform (through the monitoring component) monitors signals, event logs, status reports, etc.

ANASTACIA platform enables the detection of a behaviour hiding a man-in-the-middle attack considering known policies, models, and threat signatures.

ANASTACIA platform (through the reaction component) analyses the man-in-the-middle activity and evaluates the gravity of the situation.

ANASTACIA platform activates predictive mechanisms to isolate the attack.

ANASTACIA platform (through the Security Enforcement component) activates, updates, and enforces its policies and rules.

4.2.2.3.4 User plane

ANASTACIA platform (through the user interface) enables the user to configure and supervise the different autonomic security functions to secure the video service.

ANASTACIA platform (through the Policy Editor component) enables the user to define high level network access control policies (e.g., who has access to the MEC Server), inter-networking, reaction and escalation regulations.

4.2.2.4 Involved actors

The actors are:

- The **administrator** of a security camera system, based on Mobile Edge Computing solutions.
- The **ANASTACIA platform**, installed and used by the system administrator in order to ensure that the security camera systems allows data exchange only between trusted equipment, by using secure protocols, authentication, correct network access controls and system design.
- A disgruntled **employee** who wants to damage the company's image, by spreading on the internet sensitive security videos from its employer biggest client.

4.2.2.5 Use case steps

The use case is divided into the following steps.

- The employee illegally keeps all the credentials and certificates enabling her to decrypt the transmission between the MEC server and the cameras.
- The employee organizes a man-in-the-middle attack and downloads the videos on her home computer.
- The ANASTACIA platform monitors signals, event logs, status reports, etc.
- The ANASTACIA platform detects a man-in-the-middle illegal behaviour.
- The ANASTACIA platform scores the gravity of the attack.
- The ANASTACIA platform reacts to protect the system, activating isolation and predictive mechanisms:
    - The ANASTACIA platform sends an alert to the system administrator.
    - The ANASTACIA platform changes the certificates and passwords.
- The ANASTACIA platform enables the administrator to configure and supervise the functions.
- The administrator reacts to the alert:
    - The administrator identifies the alert as a real attack.
    - The administrator accepts the change of certificates and passwords.

4.2.2.6 Use case MEC.2

In the following table, the second use case is presented.

USE CASE MEC.2		
A	**Use Case ID**	*UC_MEC.2*
B	**Use Case Name**	*Man-in-the-middle attack to a smart security camera system*
	Primary actors	ANASTACIA platform
	Supporting actors	Administrator, employee
	Description	The ANASTACIA platform, installed to protect a smart security camera system, reacts to a man-in-the-middle attack
	Stakeholders' interests	Protect the system from a man-in-the-middle attack and avoid the illegal use of the protected data.
	Triggers	A disgruntled employee illegally keeps all the credentials and certificates enabling her to decrypt the transmission between the MEC server and the cameras. She tries to download the videos on her home computer.
	Pre-conditions	A smart security camera system was installed and the ANASTACIA platform was deployed and configured to protect all the acquired, exchanged and stored data.
	Normal flow	[*UC_MEC.2*]

		Course of Actions 1. The ANASTACIA platform monitors signals, event logs, status reports, etc. 2. The ANASTACIA platform detects a man-in-the-middle illegal behaviour. 3. The ANASTACIA platform scores the gravity of the attack. 4. The ANASTACIA platform reacts to protect the system, activating isolation and predictive mechanisms: a. The ANASTACIA platform sends an alert to the system administrator. b. The ANASTACIA platform changes the certificates and passwords. 5. The ANASTACIA platform enables the administrator to configure and supervise the functions. 6. The administrator reacts to the alert: a. The administrator identifies the alert as a real attack. b. The administrator accepts the change of certificates and passwords.
	Alternate flows	
	Flow exceptions	
	Post-conditions	The state of the system has been re-established, the employee attack has been avoided, and the protocols and passwords have been changed.
	Additional requirements	Real time notification of the attack. Immediate suspension of data flow in case of suspected attack.
	Notes and issues	

4.2.3 DoS / DDoS attacks using smart cameras and IoT devices

4.2.3.1 Narrative description

The smart security cameras and IoTs can be used for a massive distributed denial-of-service (DDoS) as the attack that disrupted U.S. internet traffic on the October 21th 2016, where the attacks were made possible by the large number of unsecured internet-connected digital devices, such as home routers and surveillance cameras. Even though some of these devices are not powerful computers, they can generate massive amounts of bogus traffic, especially using a large numbers of IoT devices.

All these bogus traffic are sent to targeted servers. In the MEC architecture these traffic will pass through the MEC server, since this server is situated at the access.

To prevent this attack, Bob, the Administrator, will use ANASTACIA to ensure that MEC server will detect the attack and react to mitigate it. Moreover, ANASTACIA will be used to monitor and use Penetration Testing modules to quickly react in order to eliminate this intrusion. ANASTACIA will be used to provide a quality of security seal that ensures that systems are correctly patched against such technique and will deploy the adequate number of VNF security functions such as Firewalls and DPI in the proper locations.

4.2.3.2 Architectural planes

*ANASTACIA architecture **Data Plane** will ensure Bob that all the elements of the security camera system are well connected to allow safe and secure operations.*

*The **Control Plane** will offer Bob advanced Software Defined Networking (SDN) technology that will enable collecting in real time crucial data information regarding the state of the network. Besides, it allows Bob to reconfigure the network on demand. Moreover, the NFV infrastructure will allow the instantiation of the different security functions in the right place, as an example, if some security module is overloaded by the DDoS attack a security Virtual Network Function can be add it immediately to divide the load and mitigate the attack.*

*The **Autonomic Plane** will reduce the manual tasks that such service needs for security configuration, and most of all, allows to dynamically adapt it to the current situation function of what monitoring observes. The 'Monitoring' component will enable continuous monitoring of different signals, event logs, status reports, video information, etc., in order to enable the detection of a behaviour hiding a DDoS attack considering known policies, models, and threat signatures. e.g., SYN flood,* DNS amplification and elephant flow attacks*. Such situations will be analysed by the 'Reaction' component which will evaluate the gravity of the situation. After that, the orchestrator will be enabled in order to set up the best strategy defense by computing the best VNFs placement and by configuring the network based on SDN.*

*The components of the **User Plane** will help Bob in the deployment of ANASTACIA security environment. Through the 'User Interface', Bob can configure and supervise the different autonomic security functions. The 'Policy Editor' component will enable Bob to define high level network access control policies (e.g., who has access to the MEC Server), inter-networking, reaction and escalation regulations.*

4.2.3.3 Functionalities

In the following paragraphs, the project functionalities are listed, divided per plane.

4.2.3.3.1 Data plane

ANASTACIA platform protects the elements of the security camera systems and ensures that their connection is safe and secure.

4.2.3.3.2 Control plane

ANASTACIA platform orchestrates the communication among network devices, through advanced SDN technologies.

ANASTACIA platform ensures that the different MEC network elements can be trusted, and detect if there is a DDoS attack.

ANASTACIA platform allows instantiation of security VNFs into MEC infrastructure in a different location to escape from the attack, thanks to the NFV and SDN technologies.

4.2.3.3.3 Autonomic plane

The Autonomic plane enables the platform to dynamically adapt to the current situation, providing the following functionalities.

ANASTACIA platform (through the monitoring component) monitors signals, event logs, status reports, etc.

ANASTACIA platform enables the detection of a behaviour hiding a DDoS attack considering known policies, models, and threat signatures.

ANASTACIA platform (through the reaction component) analyses the gravity of the situation.

ANASTACIA platform activates predictive mechanisms to isolate the attack.

ANASTACIA platform (through the Security Enforcement component) activates, updates, and enforces its policies and rules.

4.2.3.3.4 User plane

ANASTACIA platform (through the user interface) enables the user to configure and supervise the different autonomic security functions.

ANASTACIA platform (through the Policy Editor component) enables the user to define high level network access control policies (e.g., who has access to the MEC Server), inter-networking, reaction and escalation regulations.

4.2.3.4 Involved actors

The actors are:

- The **administrator** of a MEC network system.
- The **ANASTACIA platform**, installed and used by the system administrator in order to ensure that the network systems are secure and allows data exchange only between trusted equipment, by using secure protocols, authentication, correct network access controls and system design.
- A group of **hackers**, who want to perform a DDoS attack in order to shut down the network.

4.2.3.5 Use case steps

The use case is divided into the following steps.

- The hackers get the IP address of IoT and cameras.
- The hackers try to launch a DDoS attack to the network.
- The ANASTACIA platform monitors signals, event logs, status reports, etc.
- The ANASTACIA platform detects an intrusion.
- The ANASTACIA platform scores the gravity of the attack.
- The ANASTACIA platform reacts to mitigate the attack, activating isolation and predictive mechanisms:
    - The ANASTACIA platform sends an alert to the system administrator
    - The ANASTACIA instantiates security VNFs to stop the attacks.
- The ANASTACIA platform enables the administrator to configure and supervise the functions.
- The administrator reacts to the alert:
    - The administrator identifies the attack as a real intrusion.
    - The administrator accepts the new VNFs.

4.2.3.6 Use case MEC.3

In the following table, the first use case is presented.

USE CASE MEC.3		
A	**Use Case ID**	*UC_MEC.3*
B	**Use Case Name**	*DoS or DDoS attacks using smart cameras and IoTs*
	Primary actors	ANASTACIA platform
	Supporting actors	Administrator, cyber-attackers
	Description	The ANASTACIA platform, installed to protect a MEC network system, reacts to a DDoS attack
	Stakeholders' interests	To protect the system from a DDoS attack and avoid the intrusion
	Triggers	A group of hackers gets the IP address of IoTs and cameras and use if for DDoS attack.
	Pre-conditions	A MEC network system and IoTs and/or smart security cameras was installed and the ANASTACIA platform was deployed and configured to protect all the acquired, exchanged and stored data.
	Normal flow	[*UC_MEC.3*]

		Course of Actions 1. The ANASTACIA platform monitors signals, event logs, status reports, etc. 2. The ANASTACIA platform detects an intrusion. 3. The ANASTACIA platform scores the gravity of the attack. 4. The ANASTACIA platform reacts to eliminate the intrusion, activating isolation and predictive mechanisms a. the platform sends an alert to the system administrator b. the monitoring module triggers the Reaction Module, c. the Security Orchestrator receives information from the reaction module and use the output of the interpreter to cope with the malicious on-going attack d. the Security Orchestrator decides to stop the malicious traffic by computing the number of the needed security VNFs and sending the relevant request to the SDN controller. 5. The ANASTACIA platform enables the administrator to configure and supervise the functions. 6. The administrator reacts to the alert: a. The administrator identifies the attack as a real intrusion. b. The administrator accepts the new VNFs.
	Alternate flows	
	Flow exceptions	
	Post-conditions	The state of the system has been re-established, the hackers attack has been avoided, and the a new VNs have been instantiated.
	Additional requirements	
	Notes and issues	

4.2.4 IoT-based attack in the MEC Scenario

4.2.4.1 Narrative description

Telco networks are experiencing a drastic revolution embracing the opportunity to deploy Cloud Edge environments to host third-party services near to IoT devices. Edge-based service deployment can provide reduced latency compared to Cloud-based provisioning and offer location-based contextual data awareness. In this vein, a SME which provides security video surveillance via camera systems is interested in enhancing the video pre-processing by

leveraging the resources provided by the MEC environments. Furthermore, accounting for the increased number of attacks related to IoT devices, the SME would require a higher level of security for their surveillance services, monitoring the traffic generated by its cameras and mitigating potential security threats.

To guarantee the required security features, the Telco provider will adopt the ANASTACIA framework within its system, by appropriately integrating it with the existing network and service mechanisms, such as SDN, NFV, and cloud edge computing technologies. In this way, the Telco provider will be able to offer advanced Security-as-a-Service solutions, exploiting its capillary and flexible cloud-based network infrastructure. To meet the security requirements of the video surveillance SME, appropriate virtual instances of detection systems (e.g., IDS) will be deployed in the edge environment and will analyse the traffic generated by the cameras.

In this scenario, a group of hackers aims at exploiting vulnerabilities in the cameras used by the video surveillance SME to generate attacks (such as DoS, scanning, etc.) against sensitive servers, which can be either the MEC hosting servers to create an interruption in the processing of security videos or external third-party Internet servers. The monitoring modules deployed by the ANASTACIA framework are able to fast detect the on-going attacks and to trigger the orchestration of appropriate countermeasures, such as isolating the compromised cameras by modifying the forwarding paths of software-based networks.

4.2.4.2 Involved actors

The actors are:

- The **administrator** of a video surveillance company, which deploy several cameras to provide security alerts by advanced video processing.
- The **ANASTACIA platform**, installed and used by the Telco operator, to provide SECurity-as-a-Service (SECaaS) solutions in a cloud edge-based network. In particular, appropriate security mechanisms can be deployed exploiting the enhanced computing and network capabilities of edge cloud data centers, deployed within the Telco network.
- A group of **hackers**, who want to exploit security cameras vulnerabilities to launch attacks against sensitive targets.

4.2.4.3 Use case steps

The use case is divided into the following steps.

- The video surveillance SME administrator requires an enhanced level of security for its cameras within the edge environment.
- The ANASTACIA framework deploys a virtualized security appliance to inspect the data generated by the cameras.
- The hackers exploit a security vulnerability in the cameras and get access to the cameras.
- The hackers launch an attack (e.g., DoS, scanning, etc.) exploiting the compromised cameras.
- The ANASTACIA platform detects the on-going attack.
- The ANASTACIA platform scores the gravity of the attack.
- The ANASTACIA platform reacts to eliminate the intrusion:
    - The ANASTACIA platform sends an alert to the system administrator

- The ANASTACIA platform isolates the compromised cameras.
- The ANASTACIA platform enables the administrator to configure and supervise the security functions.

4.2.4.4 Use case MEC.4

In the following table, the first use case is presented.

USE CASE MEC.4		
A	**Use Case ID**	*UC_MEC.4*
B	**Use Case Name**	*IoT-based attack in the MEC Scenario*
	Primary actors	ANASTACIA platform
	Supporting actors	Administrator, cyber-attackers
	Description	The ANASTACIA platform, installed to protect a MEC-based security camera system, reacts and mitigates attack generated by compromised cameras
	Stakeholders' interests	To protect the system from a camera attack and avoid system misbehaviour
	Triggers	A group of hackers generate a malicious attack (e.g., DoS, scanning, etc.) by leveraging compromised cameras
	Pre-conditions	A smart security camera system was installed and the ANASTACIA platform was deployed and configured to provide security features according to the video administrator requirements.
	Normal flow	[*UC_MEC.4*]

		Course of Actions 1. The ANASTACIA deploy appropriate virtualized security functions to inspect traffic generated by the cameras. 2. The ANASTACIA platform detects a malicious attack (e.g., DoS, scanning, etc.). 3. The ANASTACIA platform scores the gravity of the attack. 4. The ANASTACIA platform reacts to eliminate the attack: a. The platform sends an alert to the system administrator b. The platform isolates the compromised cameras. 5. The ANASTACIA platform enables the administrator to configure and supervise the functions. 6. The administrator reacts to the alert: a. The administrator identifies the attack as a real intrusion. b. The administrator accepts the isolation of the compromised cameras.
	Alternate flows	
	Flow exceptions	
	Post-conditions	The malicious attack has been stopped and the compromised nodes are isolated.
	Additional requirements	
	Notes and issues	

4.3 BUILDING MANAGEMENT SYSTEMS

4.3.1 Cyber-attack at a hospital building

4.3.1.1 Narrative description

Annihilos is a criminal gang who takes credit in destroying the reputation of big businesses. They are targeting BetterDays, a large international healthcare provider. The operations of BetterDays include owning and operating several hospitals worldwide, providing health insurance, and running ambulance and emergency services in many countries.

Annihilos intends to exploit a zero-day vulnerability in the building management system that BetterDays uses in a large city hospital. The vulnerability allows the building management system to accept an external internet-based emergency web service message that will bring elevators and escalators in emergency mode to designated floors and overriding automatic

operations of HVAC systems. But the emergency mode will also activate the fire safety services in the respective floors too. Annihilos plans to activate emergency in several floors simultaneously using several lifts. Since the fire-safety system listens, activates and responds to the emergency by activating the sprinklers and foams, it is possible to increase the risk of structural damage to the building and threat of lives in the hospitals. The false alarm could be escalated throughout the BetterDays hospital building as well as invite the city's fire-brigade response. Moreover, by accessing the HVAC network, Annihilos could switch-off emergency terminal units, overwrite heating and cooling set-points in various floors, stress the heating equipment towards damage, etc. Annihilos could increase the energy consumption, utility and HVAC maintenance costs of BetterDays hospital building.

In addition, during the panic, Annihilos gang members plan to gain physical unauthorized access to the data-centre of the hospital whose secure doors will be disengaged during an emergency. Annihilos could install rogue applications in the datacentre workstations to transfer or transmit sensitive data of their business and private data of their clients. Subsequent to the emergency, the rogue applications in data-centre workstations will allow Annihilos to launch a remote attack (e.g., via SQL injection) on the servers that host the hospital document management system.

Chris, the hospital manager, can use ANASTACIA to ensure that BetterDays is safe from any such attack from Annihilos, as described in the following session.

4.3.1.2 Architectural planes

*The **User Plane** will provide interfaces, applications, services and tools that help users to drive and govern the ANASTACIA security framework.*

*The **Data Plane** of the ANASTACIA architecture will ensure Chris that all building operations subsystems to the ANASTACIA framework are well-connected to ensure their safe and secure operations. These subsystems are the integrated building management systems, the access control systems, the elevator management systems, the HVAC systems, and the fire-safety and security systems.*

*The **Control Plane** of ANASTICIA will offer Chris advanced software defined networking (SDN) technologies that will enable secure deployment and operation of IoT services of internet-connected and embedded devices such as security cameras, network of fire-panels, access control locks and barriers, remote elevator controllers, network of HVAC thermostats, equipment and controllers, emergency response network controllers, and remote hand-held monitors.*

*The **Autonomic Plane** will be very useful for Chris to avoid many manual and labour intensive management tasks.*

The 'Monitoring' component will enable continuous and integrated monitoring of multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems. The 'Monitoring' component will evaluate the security situation against known policies, models, threat signatures to detect abnormalities and outliers, e.g., high data download, external database or port accesses during an emergency. Such situations will be analysed by the

'Reaction' component which will evaluate the severity of the situation. Isolation and predictive mechanisms will be activated to ensure that the rest of the building operations system continues as normal. Policies and rules are activated, updated and enforced by the 'Security Enforcement' component, e.g., a building emergency will lock-down the non-essential database accesses, and escalation of the emergency to the city fire brigade should be performed by any of the authorized personnel.

The components of the 'User Plane' will help Chris to expedite the deployment of ANASTACIA security framework and ensure he gets what he's promised. The 'User Interface' component allows Chris to evaluate all components in the entire hierarchy of the hospital building operations. It will organize and abstract operations, functionalities, events, configurations, devices, subsystems, building users, etc., in a logical and lucid manner for humans to interpret and manage the heterogeneous and critical hospital building network. The 'Policy Editor' component will enable Chris to define physical and network access control policies (e.g., who has access to the data-centre), inter-network connectivity and authorization rules (e.g., what are the rules for engaging multiple elevators), reaction and escalation regulations (e.g., which situations should the HVAC air-handlers and terminal equipment override).

4.3.1.3 Functionalities

In the following paragraphs, the project functionalities are listed, divided per plane.

4.3.1.3.1 Data plane

ANASTACIA platform ensures that all the building operations subsystems are well-connected and that they can operate safely and securely.

4.3.1.3.2 Control plane

ANASTACIA platform, through SDN technologies, enables the secure deployment and operation of IoT services of internet-connected and embedded devices.

4.3.1.3.3 Autonomic plane

The Autonomic plane supports the platform user to avoid many manual and labour intensive management tasks.

ANASTACIA platform (through the monitoring component) monitors multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems.

ANASTACIA platform evaluates the security situation against known policies, models, threat signatures to detect abnormalities and outliers.

ANASTACIA platform (through the reaction component) analyses the detected abnormalities and outliers and evaluates the severity of the situation.

ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal.

ANASTACIA platform (through the Security Enforcement component) activates, updates, and enforces its policies and rules.

4.3.1.3.4 User plane

The components of the 'User Plane' help the user to expedite the deployment of ANASTACIA security framework.

ANASTACIA platform (through the user interface) allows the user to evaluate all components in the entire hierarchy of the building operations. It organizes and abstracts operations, functionalities, events, configurations, devices, subsystems, building users, etc., in a logical and lucid manner for humans to interpret and manage the heterogeneous and critical hospital building network.

ANASTACIA platform (through the Policy Editor component) enables the user to define physical and network access control policies, inter-network connectivity and authorization, reaction and escalation regulations.

4.3.1.4 Involved actors

The actors are:

- The hospital **manager**, responsible for the building safety.
- The **ANASTACIA platform**, installed and used by the hospital manager in order to ensure the safety of the building in case of cyber-attacks.
- A **criminal gang** attacking a healthcare provider

4.3.1.5 Use case steps

The use case is divided into the following steps.

- The criminal gang plans:
  - to activate emergency in several floors of the hospital simultaneously using several lifts,
  - to switch-off emergency terminal units,
  - to overwrite heating and cooling set-points in various floors,
  - to stress the heating equipment towards damage, etc.
- The gang members plan:
  - to gain physical unauthorized access to the data-centre of the hospital,
  - to install rogue applications in the datacentre workstations to transfer or transmit sensitive data,
  - to launch a remote attack on the servers that host the hospital document management system.
- The ANASTACIA platform monitors multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems.
- The ANASTACIA platform detects an intrusion.
- The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation.
- The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal:
  - The ANASTACIA platform sends an alert to the building manager
  - The ANASTACIA platform lock-down the non-essential database accesses.
- The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations.
- The administrator reacts to the alert:
  - The manager identifies the attack as a real intrusion.
  - The manager accepts the changes suggested by the ANASTACIA platform.

4.3.1.6 Use case BMS.1

In the following table, the third use case is presented.

USE CASE BMS.1		
A	**Use Case ID**	*UC_BMS.1*
B	**Use Case Name**	*Cyber-attack to a hospital building management system.*
	Primary actors	ANASTACIA platform
	Supporting actors	Hospital manager, criminal gang
	Description	The ANASTACIA platform, installed to protect a hospital building, reacts to a cyber-attack
	Stakeholders' interests	Protect the system from a cyber-attack and avoid the illegal use of sensitive data.
	Triggers	A criminal gang plans to attack the building management system of a city hospital.
	Pre-conditions	A building management system was installed within a city hospital and the ANASTACIA platform was deployed and configured to protect all the sensitive data.
	Normal flow	[*UC_BMS.1*]
		Course of Actions 1. The ANASTACIA platform monitors multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems. 2. The ANASTACIA platform detects an intrusion. 3. The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation. 4. The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal: a. The ANASTACIA platform sends an alert to the building manager b. The ANASTACIA platform lock-down the non-essential database accesses. 5. The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations. 6. The administrator reacts to the alert: a. The manager identifies the attack as a real intrusion. b. The manager accepts the changes suggested by the ANASTACIA platform.

	Alternate flows		
	Flow exceptions		
	Post-conditions	The state of the system has been re-established, the cyber-attack has been avoided, and the database-accesses have been locked-down in time.	
	Additional requirements		
	Notes and issues		

4.3.2 Insider attack on the fire suppression system

4.3.2.1 Narrative description

Adam, the operations technician, is a disgruntled employee who intends to cause economic cost to his employer by damaging building assets such as electronic controllers, servers, CCTV cameras, furniture, etc. To carry out his sinister motive, he intends to exploit the building operations workstation he is entrusted with. The workstation is used to manage the fire-alarm panel input/output. He could compromise the workstation by installing malware via a USB drive. This workstation has network access beyond the reach of much of the network access controls such as firewalls and authentication, authorization, and accounting mechanisms deployed upstream. Adams's intention is to use the malware to exploit an unpatched application that controls the fire alarm panel in order to activate unauthorised release of pressurized water or gas suppressants to flood and damage the building.

Bob, the operations manager, will use ANASTACIA to ensure that appropriate network and system design, implementation, monitoring and reaction are considered to minimise such an insider attack. ANASTACIA will assist Bob to provide a quality of security seal that ensures that systems within the building are correctly patched against known malware and that proper deployment of firewalls with deep packet inspection capability that act as points of demarcation between back-end workstations and IoT/CPS controllers. More importantly, ANASTACIA will assure Bob that should pressurized fire suppressants are released to areas vulnerable to fire, other building operations such as evacuation of occupants, alerting of wardens and responders, elevator and escalator operations, ventilation, etc., follow the emergency operation mode.

4.3.2.2 Architectural planes

*The **Data Plane** of the ANASTACIA architecture will ensure Bob that all building assets are well-connected to ensure their safe and secure operations. These assets are electronic controllers, servers, CCTV cameras, etc.*

*The **Control Plane** of ANASTACIA will ensure Bob that appropriate network and system design, implementation, monitoring and reaction are considered to minimise any possibility of attack. Advanced software defined networking (SDN) technologies will enable secure deployment and operation of IoT services of internet-connected and embedded devices.*

*The **Autonomic Plane** will be very useful for Bob to avoid many manual and labour intensive management tasks. The 'Monitoring' component will enable continuous and integrated monitoring of multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems. The 'Monitoring' component will evaluate the security situation against known policies, models, threat signatures to detect abnormalities and outliers. It will ensure that systems within the building are correctly patched against known malware and that firewalls are properly deployed. Any abnormality will be analysed by the 'Reaction' component which will evaluate the severity of the situation. Isolation and predictive mechanisms will be activated to ensure that the rest of the building operations system continues as normal. Policies and rules are activated, updated and enforced by the 'Security Enforcement' component, e.g., assuring Bob that suppressants are released to areas vulnerable to fire.*

*The **User Plane** will provide interfaces, applications, services and tools that help users to drive and govern the ANASTACIA security framework. The components of the User Plane will help Bob to expedite the deployment of ANASTACIA security framework and ensure he gets what he's promised. The 'User Interface' component allows Bob to evaluate all components in the entire hierarchy of the building operations. It will organize and abstract operations, functionalities, events, configurations, devices, subsystems, building users, etc., in a logical and lucid manner for humans to interpret and manage the building network. The 'Policy Editor' component will enable Bob to define physical and network access control policies (e.g., who has access to the data-centre), inter-network connectivity and authorization rules (e.g., what are the rules for the evacuation of occupants), reaction and escalation regulations.*

4.3.2.3 Functionalities

In the following paragraphs, the project functionalities are listed, divided per plane.

4.3.2.3.1 Data plane

ANASTACIA platform ensures that all the building operations subsystems are well-connected and that they can operate safely and securely.

4.3.2.3.2 Control plane

ANASTACIA platform, through SDN technologies, enables the secure deployment and operation of IoT services of internet-connected and embedded devices.

4.3.2.3.3 Autonomic plane

The Autonomic plane supports the platform user to avoid many manual and labour intensive management tasks.

ANASTACIA platform (through the monitoring component) monitors multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems.

ANASTACIA platform evaluates the security situation against known policies, models, threat signatures to detect abnormalities and outliers.

ANASTACIA platform (through the reaction component) analyses the detected abnormalities and outliers and evaluates the severity of the situation.

ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal.

ANASTACIA platform (through the Security Enforcement component) activates, updates, and enforces its policies and rules.

4.3.2.3.4 User plane

The components of the 'User Plane' help the user to expedite the deployment of ANASTACIA security framework.

ANASTACIA platform (through the user interface) allows the user to evaluate all components in the entire hierarchy of the building operations. It organizes and abstracts operations, functionalities, events, configurations, devices, subsystems, building users, etc., in a logical and lucid manner for humans to interpret and manage the heterogeneous and critical hospital building network.

ANASTACIA platform (through the Policy Editor component) enables the user to define physical and network access control policies, inter-network connectivity and authorization, reaction and escalation regulations.

4.3.2.4 Involved actors

The actors are:

- The **operations manager**, responsible for the building safety.
- The **ANASTACIA platform**, installed and used by the operations manager in order to ensure that appropriate network and system design, implementation, monitoring and reaction are considered to minimise any possible attack.
- The **operations technician**, a disgruntled employee, who intends to cause economic cost to his employer by damaging building assets

4.3.2.5 Use case steps

The use case is divided into the following steps.

- The operation technician plans:
    - to exploit the building operations workstation he is entrusted with, that is used to manage the fire-alarm panel input/output, by installing malware via a USB drive
    - to use the malware to exploit an unpatched application that controls the fire alarm panel,
    - to activate unauthorised release of pressurized water or gas suppressants to flood and damage the building.

- The ANASTACIA platform provides a quality of security seal that ensures that systems within the building are correctly patched against known malware and that proper deployment of firewalls.
- The ANASTACIA platform detects an intrusion.
- The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation.
- The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal:
    - The ANASTACIA platform sends an alert to the operation manager
    - The ANASTACIA platform locks-down the attacked workstation.
- The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations.
- The administrator reacts to the alert:
    - The manager identifies the attack as a real malware.
    - The manager accepts the changes suggested by the ANASTACIA platform.

4.3.2.6 Use case BMS.2

In the following table, the forth use case is presented.

USE CASE BMS.2		
A	**Use Case ID**	*UC_BMS.2*
B	**Use Case Name**	*Insider attack to a fire suppression system*
	Primary actors	ANASTACIA platform
	Supporting actors	Operations manager, operation technician
	Description	The ANASTACIA platform, installed to protect a building, reacts to an insider attack
	Stakeholders' interests	Protect the system from an insider attack and avoid any damage to the building assets.
	Triggers	The operations technician, a disgruntled employee, plans to exploit the building operations workstation he is entrusted with, by installing malware via a USB drive.
	Pre-conditions	The ANASTACIA platform was deployed and configured to protect the building operations.
	Normal flow	[*UC_BMS.2*]

		Course of Actions 1. The ANASTACIA platform provides a quality of security seal that ensures that systems within the building are correctly patched against known malware and that proper deployment of firewalls. 2. The ANASTACIA platform detects an intrusion. 3. The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation. 4. The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal: a. The ANASTACIA platform sends an alert to the operation manager b. The ANASTACIA platform locks-down the attacked workstation. 5. The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations. 6. The administrator reacts to the alert: a. The manager identifies the attack as a real malware. b. The manager accepts the changes suggested by the ANASTACIA platform.
	Alternate flows	
	Flow exceptions	
	Post-conditions	The state of the system has been re-established, the employee attack has been avoided.
	Additional requirements	
	Notes and issues	

4.3.3 Remote attack on the building energy microgrid

4.3.3.1 Narrative description

Clara is an ex-colleague of David who is the plant manager at Eisen Inc., a steel producer. Clara is now a security contractor for the competitor of Eisen Inc. Not surprisingly, Clara is aware of the existence of a misconfigured network path (any source IP address) for a utility provider (trusted IP address) of Eisen Inc. This allows the external energy provider to directly interface with the SCADA (supervisory control and data acquisition) system of the Eisen Inc's energy

microgrid. But the SCADA data historian is accessible due to an unpatched bug in the networking middleware that allows a privileged escalation of access. Clara will exploit this bug to launch a remote attack (e.g., via SQL injection) on the database servers that host the SCADA data historian. She could steal Eisen Inc.'s business credentials, overwrite boiler setpoints, rewrite activation ratios between generators and battery, fake network demands, etc. Clara could increase the energy consumption and utility costs of Eisen, stress the generators and boilers towards damage, and disable the shut-down capability of the blast-furnace13.

David will use ANASTACIA to ensure that the Eisen Inc.'s network access policy enforcement is not compromised. Further, ANASTACIA will help David to detect insecure operations of the processes, equipment or controllers. David will rest assured that the reactive and resilient features of ANASTACIA will activate safe-mode of operations should abnormalities occur.

4.3.3.2 Involved actors

The actors are:

- The plant **manager**, responsible for the energy microgrid safety.
- The **ANASTACIA platform**, installed and used in order to ensure the safety of the energy microgrid.
- An ex-employee, attacking the plant, by modifying the SCADA data.

4.3.3.3 Use case steps

The use case is divided into the following steps.

- The ex-employee plans to launch a remote attack (e.g., via SQL injection) on the database servers that host the SCADA data historian.
- The plans to:
    - steal the plant business credentials, overwrite boiler setpoints, rewrite activation ratios between generators and battery, fake network demands, etc.
    - to increase the energy consumption and utility costs of the plant, stress the generators and boilers towards damage, and disable the shut-down capability of the blast-furnace13.
- The ANASTACIA platform monitors multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems.
- The ANASTACIA platform detects an intrusion.
- The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation.
- The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the plant operations system continues as normal:
    - The ANASTACIA platform sends an alert to the building manager
    - The ANASTACIA platform activates safe-mode of operations.
- The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations.
- The administrator reacts to the alert:
    - The manager identifies the attack as a real intrusion.
    - The manager accepts the changes suggested by the ANASTACIA platform.

4.3.3.4 Use case BMS.3

In the following table, the third use case is presented.

USE CASE BMS.3		
A	**Use Case ID**	*UC_BMS.3*
B	**Use Case Name**	*Remote attack to an energy microgrid*
	Primary actors	ANASTACIA platform
	Supporting actors	Plant manager, plant ex-employee
	Description	The ANASTACIA platform, installed to protect an energy microgrid, reacts to an ex-employed remote intrusion
	Stakeholders' interests	Protect the system from a remote and avoid the violation of sensitive data.
	Triggers	An ex-employee plans to remotely attack the plant by accessing the SCADA server and violating the stored data.
	Pre-conditions	A SCADA system was installed within an energy microgrid and the ANASTACIA platform was deployed and configured to protect all the sensitive data.
	Normal flow	[*UC_BMS.3*]
		Course of Actions 1. The ANASTACIA platform monitors multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems. 2. The ANASTACIA platform detects an intrusion. 3. The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation. 4. The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the plant operations system continues as normal: a. The ANASTACIA platform sends an alert to the building manager b. The ANASTACIA platform activates safe-mode of operations. 5. The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations. 6. The administrator reacts to the alert: a. The manager identifies the attack as a real intrusion. b. The manager accepts the changes suggested by the ANASTACIA platform.

	Alternate flows	
	Flow exceptions	
	Post-conditions	The state of the system has been re-established, the ex-employee attack has been avoided, and the protocols and passwords have been changed.
	Additional requirements	
	Notes and issues	

4.3.4 Cascade attack on a megatall building

4.3.4.1 Narrative description

FoulGame is a notorious group of criminal hackers who specialize in attacks on internet-connected services of global brands. They have set their eyes to destroy the brand name of Hilltop Group who owns many iconic hotels worldwide. FoulGame intends to use internet-connectivity of the buildings operations to create an emergency in a mega-tall hotel building. They hope that the emergency will generate panic, trap the guests in escape elevators, activate fire-suppression sprinklers, confuse first-responders, etc.

FoulGame wants to exploit a zero day vulnerability of the HVAC system network that allows an external service such as an internet-service or original equipment manufacturer (OEM) to set default values (e.g., -40 ºC) to temperature sensors. For practical reasons, HVAC zonal temperatures are also monitored by the fire safety systems as a precaution. But if the temperature exceeds a threshold (e.g., +80 ºC), an emergency is activated. This could cascade to alarms and sprinklers activating, air-handlers stopping, elevators becoming disabled, fire-doors and corridors closing, etc. Risk to lives of occupants due to activation of fire-suppression systems, depletion of oxygen in the air, and rush and stampede in the stairwells will be catastrophic.

Hilltop Group can use ANASTACIA to identify and rate cyber-security security vulnerabilities automatically for the entire building. ANASTACIA will use system design and operational data to discover dependencies between cyber-physical systems and operations for the entire megatall structure. Hilltop Group will use ANASTACIA to predict potential security consequences of interacting operations between subsystems and generate threat isolation strategies. ANASTACIA will continuously enforce access and security policies and resilient control strategies comprehensively at various cyber-physical levels, viz.,the temperature sensors, fire-panels, elevator system managers, air-handling unit controllers, fire-suppression sprinkler systems, etc.

4.3.4.2 Architectural planes

*The **Data Plane** of the ANASTACIA architecture will ensure that all building assets are well-connected and they are in a secure and operation mode. These assets are electronic controllers, sensors, actuators, etc.*

*The **Control Plane** of ANASTICIA will ensure that appropriate network and system design, implementation, monitoring and reaction are considered to minimise any possibility of attack.*

*The **Autonomic Plane** will be very useful for Hilltop Group to avoid many manual and labour intensive management tasks. The 'Monitoring' component will enable correlating the signals collected from different cyber-physical subsystems in order to identify any malicious behaviour due to an attack. The 'Monitoring' component will evaluate the security situation against known policies, models, threat signatures to detect abnormalities and outliers. It will ensure that systems within the building are correctly patched against known malware and that firewalls are properly deployed. Any abnormality will be analysed by the 'Reaction' component which will evaluate the severity of the situation. Isolation and predictive mechanisms will be activated to ensure that the rest of the building operations system continues as normal. Policies and rules are activated, updated and enforced by the 'Security Enforcement' component.*

*The **User Plane** will provide interfaces, applications, services and tools that help users to drive and govern the ANASTACIA security framework. The components of the User Plane will help Hilltop Group to expedite the deployment of ANASTACIA security framework. The 'User Interface' component allows Hilltop Group to evaluate all components in the entire hierarchy of the building operations. It will organize and abstract operations, functionalities, events, configurations, devices, subsystems, building users, etc., in a logical and lucid manner for humans to interpret and manage the building network. The 'Policy Editor' component will enable Hilltop Group to define physical and network access control policies (e.g., who has access to the data-centre), inter-network connectivity and authorization rules (e.g., what are the rules for the evacuation of occupants), reaction and escalation regulations.*

4.3.4.3 Involved actors

The actors are:

- The building **manager**, responsible for the building security and safety.
- The **ANASTACIA platform** installed and used in order to ensure the safety of the building.
- A criminal hacker, attacking the building by modifying the temperature sensor data.

4.3.4.4 Use case steps

The use case has the following steps.

- The criminal hacker exploits zero day vulnerability for internet-connected temperature sensor.
- The hacker uses this sensor vulnerability to connect to the sensor whenever it is online and manipulates the temperature value by increasing it up to 80C. This data tempering will trigger the fire alarm, the evacuation alarm, deactivation of elevators and HVAC heat exchangers.

- The ANASTACIA platform monitors the physical and cyber behaviour correlate, such as temperature value, with other sensing and actuation values in the same zone and adjacent zones.
- The ANASTACIA platform detects outlies, which can be due to an intrusion or malicious activities.
- The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation.
- The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the building operations system continues as normal:
    - The ANASTACIA platform sends an alert to the building manager
    - The ANASTACIA platform activates safe-mode of operations.
- The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations.
- The administrator reacts to the alert:
    - The manager identifies the attack as a real intrusion.
    - The manager accepts the changes suggested by the ANASTACIA platform.

4.3.4.5 Use case 2.4

In the following table, the use case is formalized.

USE CASE BMS.4		
A	**Use Case ID**	*UC_BMS.4*
B	**Use Case Name**	*Cascade attack on a megatall building*
	Primary actors	ANASTACIA platform
	Supporting actors	building manager, criminal hacker
	Description	The ANASTACIA platform, installed to protect a megatall building, reacts to a criminal hacker remote data tempering
	Stakeholders' interests	Protect the system from a remote data tempering for sensitive sensor and actuation data.
	Triggers	A criminal hacker plans to gain control over critical temperature sensor to manipulate the temperature value and hence triggering the fire and evacuation alarms.
	Pre-conditions	A building automation system was installed within a megatall building and the ANASTACIA platform was deployed and configured to protect all the sensitive data points.
	Normal flow	[*UC_BMS.4*]

		Course of Actions 1. The ANASTACIA platform monitors cyber and physical signals and correlate their behaviours in building operational subsystems. 2. The ANASTACIA platform detects an intrusion. 3. The ANASTACIA platform analyses the detected abnormalities and outliers and evaluates the severity of the situation. 4. The ANASTACIA platform activates predictive mechanisms to ensure that the rest of the plant operations system continues as normal: a. The ANASTACIA platform sends an alert to the building manager b. The ANASTACIA platform activates resilient and safe-mode of operations. 5. The ANASTACIA platform enables the manager evaluate all components in the entire hierarchy of the building operations. 6. The administrator reacts to the alert: a. The manager identifies the attack as a real intrusion. b. The manager accepts the changes suggested by the ANASTACIA platform.
	Alternate flows	
	Flow exceptions	
	Post-conditions	The state of the system has been re-established, the criminal hacker attack has been avoided, the device has been isolated, and the device vulnerability has been reported.
	Additional requirements	
	Notes and issues	

4.4 REFERENCE FUNCTIONALITIES

From the pilot domain-specific scenarios and use cases reported above, the following reference simplified use cases, linked to the main identified functionalities, have been derived and formalized as UML Use Case diagrams, to facilitate further analysis and implementation by software architects and developers.

Basic CRUD (Create, Retrieve, Update, Delete) Use Cases (in yellow) are included for the sake of completeness and no further detailed as rather self-explanatory (cascade actions should be nevertheless properly managed at design and development phase).

4.4.1 Policy management

Main reference Use Cases for policy management are associated to both security and privacy policies, as both aspects must be managed by the ANASTACIA platform.

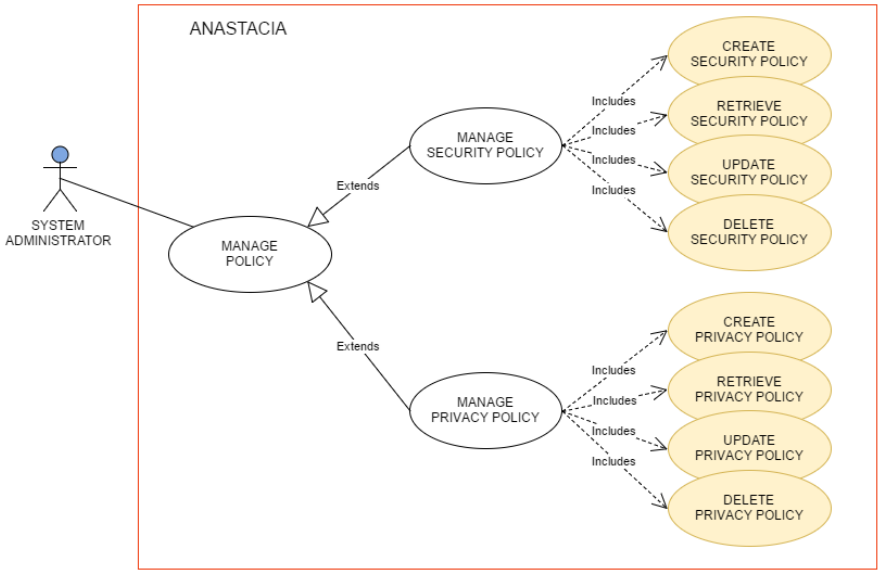

Figure 13. Policy management overall Use Case diagram

4.4.2 Monitored system management

Main reference Use Cases for monitored system management are associated to device and network management, as both elements must be managed by the ANASTACIA platform in order to configure all monitored and controlled items as well as to control them by IoT/SDN/VFV controllers.

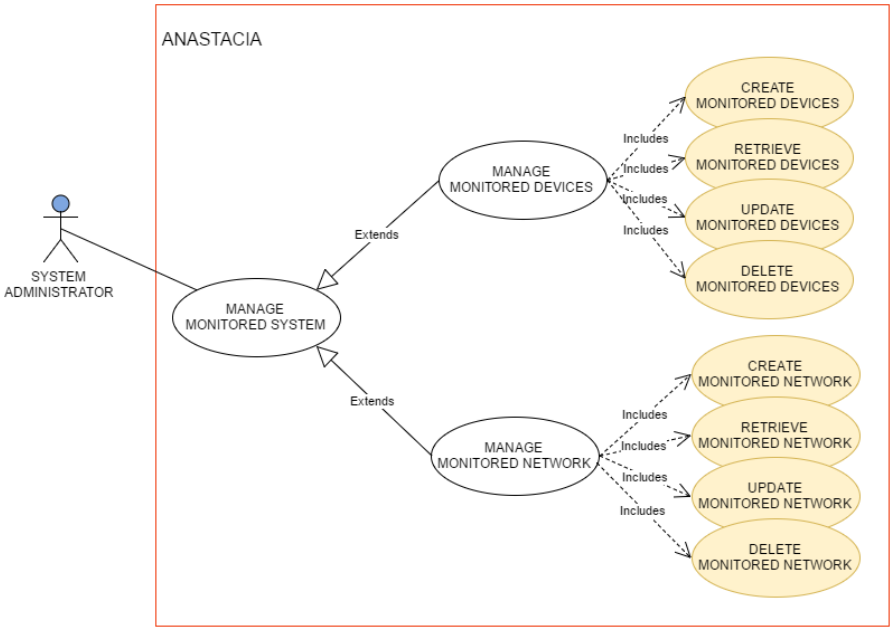

Figure 14. Monitored system management overall Use Case diagram

4.4.3 Attack management

Main reference Use Cases associated to attack management are somehow interconnected with the whole ANASTACIA draft architecture and encompasses the majority of the expected functionalities.

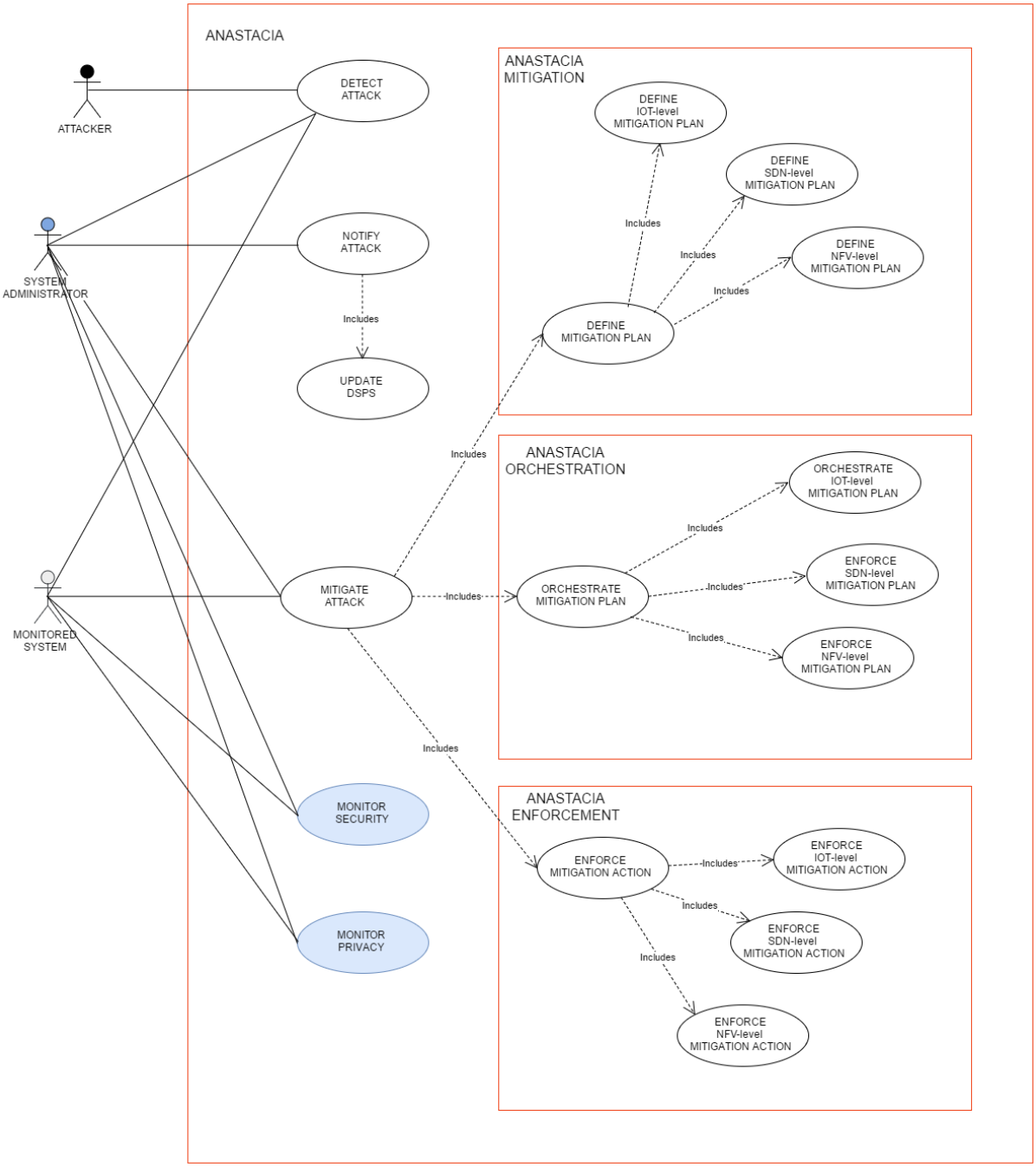

Figure 15. Attack management overall Use Case diagram

5 QUESTIONNAIRE ANALYSIS

This section summarizes the main findings obtained from the analysis of the questionnaires received from IAB members and privileged observers. The results are meant to help the Consortium in the prioritization of objectives and of the features.

5.1 OBJECTIVES

Interviewees were asked to rate the four original overall objective of ANASTACIA. The highest (average) score was assigned to Objective N°1:

> *To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.*

		INTERVIEWEE											
	OBJECTIVE	1	2	3	4	5	6	7	8	9	10	11	AVG RATING
1	To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	3	5	5	4	5	2	5	5	3	5		**4,2**
2	To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	5	5	3	4	5	2	3	5	5	4		**4,1**
3	To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	5	3	4	3	4	3	3	3	3	4		**3,5**
4	To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	4	3	4	3	4	5	5	3	2	5		**3,8**

Figure 16. Heatmap visualization of the evaluation of the ANASTACIA objectives

5.2 FEATURES

Interviewees were asked to rate a set of general features to be considered during the development.

Top 5 general features that ANASTACIA developers should take into account are:

1. SCALABLE TO GROW
2. COMPLIANT WITH STANDARDS
3. EASY TO USE
4. INTEGRATES WITH OTHER SOFTWARE
5. MODULAR ARCHITECTURE

		INTERVIEWEE											
	FEATURE	1	2	3	4	5	6	7	8	9	10	11	RESULT
1	EASY TO USE	5	5	4	4	4	3	5	4	3	5		4,20
2	LOW COST	3	3	3	3	3	4	3	4	2	4		3,20
3	POWERFUL REPORTING	3	2	4	4	5	4	3	3	3	3		3,40
4	WELL SUPPORTED	5	3	4	5	4	2	5	5	4	3		4,00
5	FLEXIBLE TO CUSTOMISE	3	3	4	4	4	4	3	5	4	4		3,80
6	SCALABLE TO GROW	4	4	5	4	4	4	4	5	4	5		4,30
7	LARGE, WELL-KNOWN VENDOR	4	3	3	3	3	2	2	2	4	2		2,80
8	GOOD FEEDBACKS / REPUTATION	4	2	4	5	3	5	3	4	4	4		3,80
9	INTEGRATES WITH OTHER SOFTWARE	5	3	3	5	3	3	5	5	5	5		4,20
10	LICENSED AS OPEN-SOURCE	3	2	4	2	3	3	4	3	1	3		2,80
11	HAS INTUITIVE / ADAPTIVE USER INTERFACES	5	3	4	4	4	2	5	5	2	5		3,90
12	PROVIDES REAL-TIME FEEDBACK	4	4	4	5	4	2	4	5	3	3		3,80
13	INCLUDES DYNAMIC NETWORK TOPOLOGY	5	4	3	4	4	2	3	5	4	3		3,70
14	DEVELOPED BY BIG VENDORS	3	2	3	3	2	2	2	2	4	2		2,50
15	MODULAR ARCHITECTURE	5	3	4	5	4	4	4	5	4	3		4,10
16	COMPLIANT WITH STANDARDS	5	3	4	5	5	3	5	3	5	5		4,30
17	AUTONOMOUS REACTION TO THREATS	5	3	4	4	3	4	3	5	2	5		3,80
18	SELF-HEALING / SELF-REPAIR CAPABILTY	5	3	4	3	3	3	3	5	2	4		3,50
19	HIGHLY CONFIGURABLE (E.G. RULE EDITING)	3	3	4	5	4	5	3	5	5	3		4,00
20	OTHER (...)												

Figure 17. Heatmap visualization of the evaluation of general features to be considered.

SCALABLE TO GROW	4,30
COMPLIANT WITH STANDARDS	4,30
EASY TO USE	4,20
INTEGRATES WITH OTHER SOFTWARE	4,20
MODULAR ARCHITECTURE	4,10
WELL SUPPORTED	4,00
HIGHLY CONFIGURABLE (E.G. RULE EDITING)	4,00
HAS INTUITIVE / ADAPTIVE USER INTERFACES	3,90
FLEXIBLE TO CUSTOMISE	3,80
GOOD FEEDBACKS / REPUTATION	3,80
PROVIDES REAL-TIME FEEDBACK	3,80
AUTONOMOUS REACTION TO THREATS	3,80
INCLUDES DYNAMIC NETWORK TOPOLOGY	3,70
SELF-HEALING / SELF-REPAIR CAPABILTY	3,50
POWERFUL REPORTING	3,40
LOW COST	3,20
LARGE, WELL-KNOWN VENDOR	2,80
LICENSED AS OPEN-SOURCE	2,80
DEVELOPED BY BIG VENDORS	2,50

Figure 18. Ranked general features to be considered.

5.3 MAIN HIGHLIGHTS

Main valuable highlights from the collected questionnaires are reported here, grouped by question. Answers in their entirety are included in the Annexes.

1. **Which is your level of expertise in SDN, NFV, CPS and IoT respectively ?**
   - *<omissis>*
2. **How is cybersecurity generally managed in your domain?**
   - *"Standard approach: firewall, password protection, antivirus + antispam"*
   - *"Manual intervention, monitoring and reaction by legally responsible system engineers."*
   - *"Mainly re-active management"*

- *"Cyber Security is an overall aspect of a Telecom Equipment and it involves both the carried traffic than the Control Plane/Network Manager System. SW platform (i.e. Linux Based or proprietary) are up to date for security threats even if not on a Common Platform as ANASTACIA may be. Cyber Security Audits are typically performed in pre delivery phase of a product."*
- *"Smart Building: with classical solutions, e.g., firewalls, NATs, etc."*
- *"We use a multilayer approach , essentially using the Security in Depth paradigm."*
- *"There is cyber security related to secure product design and protection of Company infrastructure. Cloud systems and infrastructure is managed by IT. Product security is managed by Engineering."*

3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?

- *"My domain is mostly related to cybersecurity issues in Internet routing and communication connection management. In Internet routing, it is possible under certain exploit conditions to alter DNS mapping (name to IP address) hence affecting connection confidentiality and integrity. Moreover, by hijacking Internet route, one can easily make Internet-reachable services down or run man-in-the-middle attacks. In terms of connection management, the distributed nature of the Internet and the end-to-end nature of connection suffers from important vectors of attacks to end systems."*
- *"a. Very low risk acknowledgement and understanding, b. Lack of expertise, c. Lack of easy to deploy solutions, d. Lack of multi-tenancy solutions, e. Lack of integration between Infrastructure Composability and Security Management"*
- *"The correct identification of related ICT risks and mitigation measures (e.g., which security controls to implement), while providing alignment with relevant internal/external regulations."*
- *"The key cybersecurity issues associated to TLC are from level 1 to level 4 OSI Stack attack, aften are DoS or Sniffing also at physical level (Optical Intrusion) or DCN DoS."*
- *"Exfiltration of sensitive data, including covert channels and attacks that can endanger the physical security of individuals."*
- *"Standardize authentication, confidentiality and RBAC in power systems management information exchange and secure communication from DoS (Denial of Service)."*
- *"We face primarily denial of services attempt and botnet infection attempt"*
- *"(1) Legacy products that are in the field for 10+ years and are not easily patchable (2) increasing sophistication of cyber-attacks"*

4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?

- *"For Internet routing attacks, it is well known there are major threats related to DNS mapping and BGP route hijacking. (i) For DNS mapping, the adoption of DNSSEC is proceeding well and the threat is manageable. (ii) For BGP, the adoption of BGP security extensions recently defined is not proceeding well due to lack of technical and economic incentives (too costly to deploy, for securing a too rare event). An example is the interruption of Youtube services in 2008 due to a Youtube ban ordered by Pakistan government which was automatically spread to neighbouring countries due to errors in configuring BGP. Another example was run in Defcon 2008 where it was demonstrated who the whole conference Internet traffic could be captured by attackers by running real-time a BGP hijacking attack on the corresponding Decon network. For Internet connection and service availability threats: (i) some providers of some densely populated countries are able to inject scripted active code in HTTP relayed web content in billions of different HTTP sessions concurrently hence easily causing distributed denial of service attacks and potentially blocking any Internet-reachable service. This is known to happen in China. (ii) Some IoT device vendors seeking the least possible cost are selling millions of devices not secured against remote control and hence the generation of DDOS attacks. This was recently proven for domestic web surveillance cameras."*

- *"Nothing relevant to my mind. But HPE reports underline how 70% of business have been actually breached without realising it."*
- *"I've been witness of a DoS over DCN at a Regional Carrier in the USA, it was generated by a wrong configuration of firewalling"*
- *"In general, many Building Automation Systems have been designed for a less-aggressive and sophisticated cybersecurity scenario. Standards like EIB/KNX, LON or BACnet, were designed many years ago with very limited focus on IT security as well as when the IoT paradigm still was in its infancy."*
- *"For example, power outage occurred in December 2015 in Ukraine due to a cyber-attack. The attack was acted by embedding the Blackenergy malware in MS Office documents and delivered via e-mail to individual of electricity company IT network."*
- *"On IoT domain, the sole Mirai Botnet made big news; from our sensors we are seeing multiple attempt a day from infected appliances getting blocked. On SDN side we are currently unaware of anything in the wild actively exploited but for any increase in architecture complexity there is usually an increased risk."*
- *"The Target attack of 2013 is a related attack; Several 10s of millions of credit card information was stolen. Hackers leverages vulnerabilities through a channel created for HVAC vendor support and used that to connect to secure systems"*

5. **Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?**
   - *"No"*
   - *"Yes, many of which are off-the-shelf solutions or few are developed/maintained in-house. Higher focus on monitoring, enforcing and user-friendly configuration. Minor focus on DSPS due to the lack of tools/standards."*
   - *"ICT Firewalls, MSPP Equipment (ALU 1850TSS-100)"*
   - *"YES, CERTIFICATION AND THE SECURITY AND PRIVACY SEAL: […] THE EUROPEAN SECURITY LABEL WITHIN WORKING GROUP 10 (INNOVATION) UNDER THE EUROPEAN RESEARCH AND INNOVATION FORUM EFFORTS GOING BACK TO 2009. THE INITIAL CONCEPT IS CONTAINED IN A WHTE PAPER DEVELOPED WITHIN THE EUROPEAN JOINT RESEARCH CENTRE."*
   - *"We use online monitoring and testing tools but nothing with real time reaction capabilities."*
   - *"I am not aware of any."*
6. **Who do you think might use ANASTACIA in your domain?**
   - *"Network Manager"*
   - *"[To raise awareness on security flaws present in a given network to] network administrators and legal responsible persons."*
   - *"Our Managed Services Division to provide Managed Security Services"*
   - *"Mostly security compliance officers, security architects, CERT team, and security operations."*
   - *"Telecom equipment manufacturer, telecom provider Tier 1"*
   - *"IoT-based providers, especially for automations in Industry 4.0, e.g., intelligent manufactory, IoT and cloud offloading scenario."*
   - *"CISO and Security Engineers"*
   - *"Those primarily requiring IoT infrastructure protection and these could be a wide variety."*
7. **Who do you think might benefit the most from ANASTACIA in your domain?**
   - *"Network and system management"*
   - *"Network administrators and legal responsible persons"*
   - *"Customers, Customers' Employees, Service Providers"*
   - *"Apart from the previously mentioned, also end-users willing to assess the trustworthiness of our products and services (related to the DSPS)."*
   - *"Telecom equipment manufacturer"*

- *"End-users."*
- *"The ECSO"*
- *"System engineers tasked to manage and maintain complex systems."*
- *"IT team of companies"*

8. **Would you consider using a solution based on ANASTACIA (see description above)?**
   - *"Yes, for the EPC management and monitoring"*
   - *"Yes, provided it can allow a multi-tenancy deployment"*
   - *"Yes, even if it is out of the scope of my knowledge. In other words, ANASTACIA is surely of interest, but I can't evaluate how does it cost in terms of portability over legacy services, additional hardware/software requirements, need of migrating pre-existent frameworks over new deployments."*
   - *"YES, THE LABEL COULD BE SOMETHING TO LOOK TOWARD TOGETHER"*
9. **Is there any recommendation you would like to give our project at design / development phase?**
   - *"Focus on Internet connection attacks and related DDoS vectors."*
   - *"Take into account Service Provider [and that] most of the threats are in SMBs market, who are usually unaware or poorly informed"*
   - *"Align as much as possible with existing standards and industrial best-practices, in particular related to the topic of DSPS."*
   - *"Test security and do formal analysis over protocols and implementation as to prevent covert channels, data exfiltration or possible side channel to leak sensitive information."*
   - *"A good practice is the use of a PKI infrastructure and X.509 certificates to authenticate servers, software and users. Furthermore, protect communication channels applying, for example, the IEC 62351-3 requirements."*
   - *"Work toward a high level of interoperability with third party solutions."*
   - *"Requirements need to be laid down very clearly. The operation should be clarified using real use-case scenarios and extensively tested with a large number of test cases. The designers need to think like hackers!"*

6 REQUIREMENTS

6.1 FUNCTIONAL REQUIREMENTS

ID	Name/Description	Priority*
FR-1	The ANASTACIA system will provide CRUD functionalities for security policies that must be autonomously applied in case a threat is detected	**HIGH**
FR-2	The ANASTACIA system will include a repository to store security policies	**HIGH**
FR-3	The ANASTACIA system will provide CRUD functionalities for privacy policies to be checked when data are internally processed *NOTE: the privacy requirements (restrictions and related compliancy) generally apply to the way data are managed internally by the ANASTACIA system and not to the way data are managed by the monitored systems/application*	**HIGH**
FR-4	The ANASTACIA system will include a repository to store privacy policies	**HIGH**
FR-5	The ANASTACIA system will provide CRUD functionalities for the definition of the devices included in the monitored system	**MEDIUM**
FR-6	The ANASTACIA systems will include a repository to store device data	**MEDIUM**
FR-7	The ANASTACIA system will provide CRUD functionalities for the definition of the network topology included in the monitored system	**MEDIUM**
FR-8	The ANASTACIA system will include a repository to store network topology data	**MEDIUM**
FR-9	The ANASTACIA system will include an interactive graphical visualization of the network and of the devices included in the monitored system	**LOW**
FR-10	The ANASTACIA system will include components for the monitoring of network traffic	**HIGH**
FR-11	The ANASTACIA system will include agents for the monitoring (and possibly the interactive control) of devices	**HIGH**
FR-12	The ANASTACIA system will include reasoning capabilities to define mitigation plans according to the defined security and privacy policies	**HIGH**
FR-13	The ANASTACIA system will include orchestrating capabilities to manage the correct implementation of mitigation plans	**HIGH**
FR-14	The ANASTACIA system will include enforcing capabilities to deploy mitigation actions in the monitored system at IoT/SDN/NFV levels (i.e. it is able to control IoT devices, to change the network configuration by means of SDN functionalities, to	**HIGH**

	deploy new security-related VNF to better assess security constraints in real time)	
FR-15	The ANASTACIA system will include a dedicated adaptive web interface for the Dynamic Security and Privacy Seal (DSPS) which includes a dynamic/real-time graphical representation of the status of the monitored system (as for its current compliancy with defined security and privacy policies) along with an explanatory legend for the different versions (e.g. green, yellow, orange, red)	**HIGH**
FR-16	The ANASTACIA system will include a repository to store DSPS status and changes over time, along with 1) causes (e.g. detected threats and related device/topology information) and 2) actions (e.g. mitigation plans and modification in device/topology configurations)	**MEDIUM**
FR-17	The ANASTACIA system will include reasoning capabilities to verify if the deployment of security mitigation actions alter significantly the privacy status of the monitored system, eventually deciding if proceeding or not od asking for confirmation to the system administrator	**LOW**
FR-18	The ANASTACIA system will provide a reporting functionality that generates reports on 1) detected attacks, 2) affected items, 3) defined mitigation plans, 4) implemented mitigation actions, 5) potential privacy breaches	**LOW**
FR-19	The ANASTACIA system will provide interfacing APIs to expose information related to 1) detected attacks, 2) affected items, 3) defined mitigation plans, 4) implemented mitigation actions, 5) potential privacy breaches	**LOW**
FR-20	The ANASTACIA systems will include autonomic reasoning/self-learning capabilities to modify/adapt security and privacy policies according to the previously defined mitigation plans and deployed mitigation actions	**MEDIUM**

*{ **LOW** , **MEDIUM** , **HIGH** }

6.2 NON-FUNCTIONAL REQUIREMENTS

The following non-functional requirements (referred in general to the ANASTACIA system, as the entity encompassing all integrated technical components) potentially apply to all identified use cases.

Due to the targeted TRL 5 and the nature of the expected technical results (prototypes demonstrated in relevant domains) some product/SLA-oriented requirements are classified as having a LOW priority and will be possibly considered later on during the industrialization phase.

ID	Name/Description	Priority*
NFR-1	**Accessibility** – as for UI (e.g. web dashboards), accessibility guidelines will be taken into consideration (e.g. https://www.w3.org/WAI/intro/wcag)	**LOW**
NFR-2	**Availability** – the ANASTACIA system will be available 24/7	**MEDIUM**
NFR-3	**Backup** – the ANASTACIA system will include automatic configurable back-up procedures and associated storage facilities for all relevant data (e.g. security and privacy configurations, mitigation plans, SDN configurations, VNF deployments, etc.)	**MEDIUM**

NFR-4	**Capacity** – the ANASTACIA system will have to manage a minimal set of <*N*> devices (to be defined at pilot level)	**MEDIUM**
NFR-5	**Certification/Compliance (PRIVACY)** – as for the internal processing of information, the ANASTACIA system will be compliant with the GDPR as for the identified Privacy Requirements	**HIGH**
NFR-6	**Certification/Compliance (SECURITY)** – the ANASTACIA system will adopt the *de facto/de iure* standards as for security protocols to use as for internal communication/interfaces	**HIGH**
NFR-7	**Configurability** - the ANASTACIA system will include tools for the configuration of security policies, privacy policies, network topologies, device features, VNF features	**HIGH**
NFR-8	**Effectiveness** – the ANASTACIA system will be able (at least) to notify attacks and potential privacy threats and (possibly) to identify a suitable mitigation plan and (possibly) to enforce mitigation actions, returning the monitored system in a safer status	**HIGH**
NFR-9	**Extensibility** – the ANASTACIA system will adopt a modular architecture and include configuration tools that allow adding features and defining customizations	**MEDIUM**
NFR-10	**Interoperability** – the ANASTACIA system will adopt *de facto/de iure* standards for interfacing with third parties' systems (e.g. exposed API) exposing e.g. main reporting functionalities	**MEDIUM**
NFR-11	**Performance** (response time/ throughput) – the ANASTACIA system will monitor ICT infrastructure in real time and will immediately notify detected threats and potential privacy breaks, independently from the number of monitored devices	**MEDIUM**
NFR-12	**Recoverability** (mean time to recovery - MTTR) – the ANASTACIA system will be able to detect and notify a threats within <ΔT>, to define a mitigation plan within <ΔT>, to orchestrate a mitigation plan within <ΔT>, to enforce mitigation plan actions within <ΔT> (ΔT to be defined at pilot level)	**LOW**
NFR-13	**Reporting** – the ANASTACIA system will include functionality for real time notification of cyber-attacks and of potential privacy breaches (summarized by the DSPS) and will provide end users with the possibility to download reports on all managed events and actions undertaken	**HIGH**
NFR-14	**Scalability** – the ANASTACIA system will be able to transparently add/deploy new monitored IoT devices and VNFs	**HIGH**
NFR-15	**Security** – the ANASTACIA system will provide functionalities for Authentication, Authorization, and Accounting to guarantee proper access for registered users	**MEDIUM**

*{ **LOW** , **MEDIUM** , **HIGH** }

6.2.1 Privacy requirements

The design of the system architecture is a crucial phase to ensure the security and privacy of the information processed therein. In fact, according to Regulation 679/2016 (hereinafter "GDPR"),

> ***"the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data***

protection by default. *Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations".*

Moreover the system must be embedded with **appropriate technical and organizational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- **policies and procedures to periodically test the security** resilience of a system (e.g., penetration tests, vulnerability assessments, etc.) and carry out the relevant remediation activities;
- a well-defined internal procedure to alert the system administrators when any **data breaches take place.**

The following Privacy Requirements ("PR") are drawn from the GDPR amongst those relevant for ANASTACIA, and adapted to the foreseen architecture, based on the assumption that the ANASTACIA framework would be deployed in the context of personal data processing activities which are not defined by ANASTACIA itself, yet by the entity deploying ANASTACIA's system as a service; in that regard, ANASTACIA will typically fulfil the tasks of a **Data Processor**, and in so doing it provides some means to achieve the purposes set by another entity, the Data Controller.

ID	Name/Description	Priority*
PR-1	**Data management** – The ANASTACIA system must automatically record all internally generated data, storing these data into the ANASTACIA platform, while minimizing the collection of personal data. *The system will be designed so as to support interfaces, at application level, that allow users to control the data processing taking place within the platform.*	**HIGH**
PR-2	**Data back-ups** – Back-up operations will be carried out periodically, so as to ensure the continuity of the system and prevent the loss of data. *ANASTACIA will provide back-ups for each system's tools, in order to ensure the maintenance and the continuity of information and complete traceability of each activity.*	**HIGH**
PR-3	**Authentication of identities** – Pursuant to GDPR Articles 28 and 29, persons acting under the authority of the controller or the processor shall process personal data on instructions from the controller. This requires, first of all, that they must have individual authentication credentials composed by a personal ID code and a secret	**HIGH**

	password with at least eight characters; if this is not allowed, the password shall consist of the maximum permitted number of characters and it shall not contain any item that can be easily related to the person in charge of processing. It shall be also modified when it is first used as well as at least every six months, thereafter. Alternatively, these credentials shall consist in an authentication device that shall be used and held exclusively by the person acting under the authority of the controller or the processor or in a biometric feature (possibly, in both cases, associated with either an ID code or a password). *The whole system will collect different types of data and it will be designed to ensure the privacy and trust of the users. In order to do this, each identity accessing the system will be authenticated and appropriately authorised to be able to use it. Where necessary (e.g. when the system is used to process health data), strong authentication (e.g. two-factor authentication, double opt-in, biometric recognition, etc.) methods must be supported.*	
PR-4	**De-activation of authentication credentials** - Personal authentication credentials shall be de-activated if they have not been used for at least six months (except in case of technical authorization). The system will periodically check if more than six months elapsed since the last log in of each person acting under the authority of the controller or the processor and disable its credentials if usage requirements are not met. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data. *The objective is to guarantee that persons acting under the authority of the controller or the processor can only access and process personal data if they are provided with authentication credentials. The credentials are necessary for the appointed person to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.*	**MEDIUM**
PR-5	**Authorization** - Before the start of the processing, it is necessary to enable access to the data that are needed to perform processing operations, setting out an authorization profile for each person/homogeneous set of persons acting under the authority of the controller or the processor. Authorization profiles will be set out and configured prior to start of the processing so as to enable data controllers' access only to the data that are necessary to perform processing operations. *It will be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorization profiles still apply. ANASTACIA will work on the basis of a list of persons acting under the authority of the controller or the processor to identify categories of task and corresponding authorization profiles.*	**HIGH**
PR-6	**User data management** - In case of personal data collection, the system enables users to control their personal data, to access, rectify, delete or block them. It is always possible, for the users, to change the sets of data that they have shared. *The idea is to allow users to control their interaction with the project by revealing only the information they want to disclose and changing at any time the set of shared data. It is a user-centric approach that means that users have the power to play an active role in the management of their personal data. This may include the realization of a dashboard whereby the user may always keep control on the overall processing of his/her personal data.*	**HIGH**
PR-7	**Purpose limitation** - ANASTACIA will process personal data only for security purposes, unless the data controller configures the system to pursue other legitimate, specific and explicit purposes, determined at the time of collection of the	**HIGH**

	data. *This requirement implements the purpose limitation principle set forth by Article 5 (1) point (b) of the GDPR. Moreover, the Art. 29 WP has provided an in-depth analysis of this principle in its Opinion 03/2013 on purpose limitation.*	
PR-8	**Data accuracy and updating** - Personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or processed, will be erased or rectified. *The normative base of data accuracy and updating is Article 5 (1) point (d) of the GDPR which states: "[…] personal data shall be: […] d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate, having regard to the purposes for which they are further processed, are erased or rectified without delay […]".*	**HIGH**
PR-9	**Security of processing -** Personal data will be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. *As defined by Article 32 of the GDPR, as part of the security of the processing, both controller and processor must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*	**HIGH**
PR-10	**Data breach information** - The Anastacia system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects. *The legal source of this requirement is found in Articles 33 and 34 of the GDPR. Information about the breach can also be provided by means of the Dynamic Privacy and Security Seal.*	**HIGH**
PR-11	**Encryption by default** - Encryption will be applied to all stages of handling data, including in communication, storage of data at rest, storage of keys, identification, access, as well as for secure boot process. *The legal source of this requirement is Article 32 of the GDPR, whereby it mandates the controllers and processors to ensure a level of security appropriate to the risk, including measures that have the "ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services".*	**HIGH**
PR-12	**Right of access** - The Anastacia system shall support the data controllers in providing to every data subject, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to: the purposes of the processing; the categories of data concerned; the recipients to whom the data are disclosed; the envisaged period of storage for the data; and the existence of automated decision-making processes within the system. *The legal source of this requirement is Article 15 of the GDPR.*	**HIGH**

PR-13	**Appropriate retention period** - The default personal data retention period is set at one (1) month, without prejudice to other conflicting legal obligations, which will be appraised on a case by case basis on motivated request by the data controller (e.g. in case of different retention period for internet traffic data mandated by specific law on detection and prevention of crime). *The exceptions to the one month retention policy set above may derive from the implementation of Article 15(1) of the ePrivacy Directive (Directive 2002/58/EC) at national level. Such Directive provides that: "Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period" when it is necessary to safeguard "national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".*	**HIGH**
PR-14	**Right of erasure** - The ANASTACIA platform must ensure that the right of erasure exercised by data subjects towards the data controller is enforced, when the conditions set out by law are met. The assessment must be performed by the data controller; personal data shall be erased if one of the criteria listed below is applicable: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject has withdrawn the consent on which the processing is based, and where there is no other legal ground for the processing; (c) the data subject objects to the processing on grounds relating to his or her particular situation, and there are no overriding legitimate grounds for the processing; (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject. *This obligation stems from Article 17 of the GDPR, which in turn builds upon Article 12 of Directive 95/46/EC.*	**HIGH**
PR-15	**Data Portability** - The ANASTACIA platform must be able to support the data controller in responding to requests for data portability lodged by the data subjects. This entails that the data subject shall receive the data in a structured, commonly used and machine-readable format. *This obligation stems from Article 20 of the GDPR. The capacity of a system to make data portable to another system needs interoperability as a prerequisite.*	**HIGH**
PR-16	**Regular Monitoring of Security** - The ANASTACIA platform will regularly monitor the system's status in terms of security for personal data. The system will be able to provide real time information on the level of security, also through the Dynamic Privacy and Security Seal. *This obligation stems from Article 32 of the GDPR, which requires controllers and processors to implement measures for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*	**HIGH**

*{ **LOW** , **MEDIUM** , **HIGH** }

6.2.2 Additional technical integration requirements

This section includes some technical guidelines and preliminary notes for integration of proprietary tools/SW (provided by partners) within the overarching ANASTACIA architecture. Further related activities will be carried out later on in the project by technical work packages and WP6 “Integration and Use Case Validation” in particular.

6.2.2.1 Integration of IoT agents

This section provides preliminary analysis for IoT agent integration requirements. It is important to highlight that recommendations illustrated below will be subject to change during integration phase. All integration and implementation changes to requirements will be described and duly illustrated in following deliverables in further stages of ANASTACIA project.

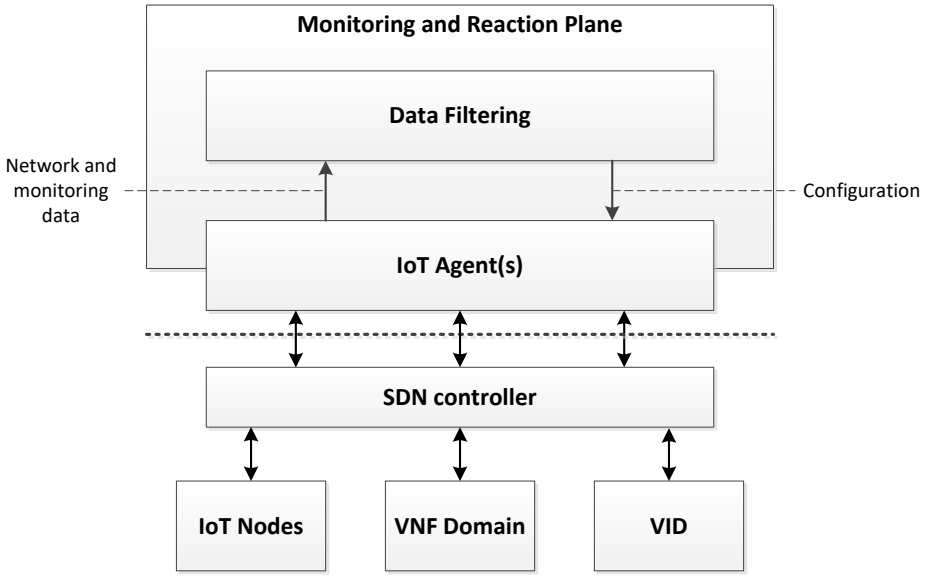

Figure 19. IoT agents functional cooperation with ANASTACIA systems.

Functional requirements:

IoT agent software package will be performing the following operations in cooperation with other ANASTACIA modules:

1. Obtain IoT devices monitoring data;
2. Acquire additional information from VNF (Virtualized Network Function) domain;
3. Receive data from VID (Virtualized Infrastructure Domain);
4. Provide gathered monitoring data back to data correlation module deployed in monitoring and reaction plane;
5. Receives agent configuration from data correlation module and execute appropriate actions to reflect requests on it.

SW requirements:

Depending on how SW infrastructure will be implemented, requirements for IoT agent(s) require having proper interfaces defined between the module and other ANASTACIA subsystems.

Deployment flexibility

Depending on the ANASTACIA HW infrastructure system capabilities, agents can be deployed in a form of software containers running with Docker Engine or separately prepared scripts or compiled code. Deployment constraint will include IoT devices only, due to large variety of HW configurations and performance characteristics that might restrict agent functionality due to performance penalty added to IoT device by agent software. Final deployment solution will be finalized during integration work.

Protocols compatibility

IoT agent will be embedded as part of middleware infrastructure and will mediate between different subsystems. The connectivity will be realized via different type of protocols that will depend on modules to which agent will be connected (data correlation, IoT nodes, VNF domain, VID). To enable full support, IoT agents will provide required protocol support for all interfaces. The agent architecture will remain open to accommodate all surrounding components and provided seamless integration with ANASTACIA architecture. Recommended agent protocol will be REST with JSON notation to model data passed between ANASTACIA modules as depicted on Figure 11 to communicate with control plane. Agent might also support any additional protocols required to communicate with ANASTACIA components. Second case will be used as last resort integration effort in case if REST API will not be able to provide mandatory functionality required by agent.

Security configuration support

Interacting modules should provide transport encryption (i.e. https for REST API) depending on components location. Encryption will not be enforced in case when components are co-located on the same machine or same network subnet in order to speed-up deployment and interoperability testing on initial phase. Once basic functionality compliance will be reached, security mechanisms can be restored to close any potential security gaps in ANASTACIA system.

Interface specification:

There are several interfaces that will be integrated to enable IoT Agent functionality. The interfaces might share lots of commonality and might be merged to simplify component deployment and integration processes. Interface details will be established during ANASTACIA integration process.

6.2.2.2 Integration of MMT

This section provides the insights of the requirements to integrate the Montimage Monitoring Tool (MMT) with other proprietary systems. In particular, it includes a description of the modifications required in both MMT and third-party tools in order to make them work together in the context of the ANASTACIA project.

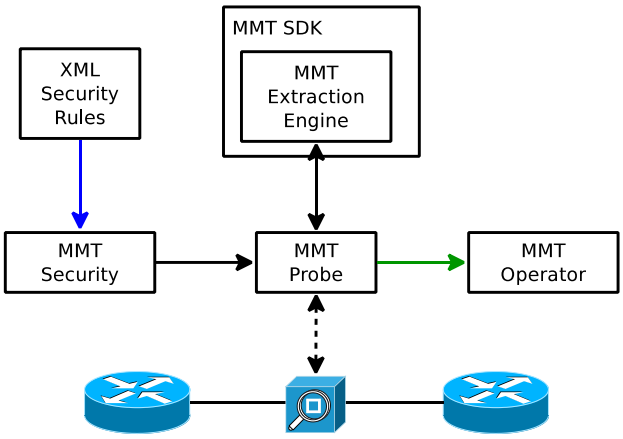

Figure 20. MMT architecture.

Figure 20 presents the main architecture of MMT. The main feature of the architecture is its modular approach, which allows each module to be decoupled from the whole tool to work in an independent manner. Being this said, the MMT software can be integrated to cover different parts of the ANASTACIA framework.

MMT Probe:

MMT-Probe is the main application of the tool. It uses the MMT-SDK library that implements the Deep Packet/Flow Inspection (DPI/DFI) techniques for classifying and extracting the needed metadata. It also uses the MMT-Security library to analyse the extracted metadata to detect anomalies. The Probe is thus able to analyse live data on the network, extracting information about the used protocols and flows traversing the network and detect security breaches. In addition, the probe can be configured to analyse new protocols in the form of plugins of the Probe, which are then compiled into the Probe application.

MMT Security:

This is the security analysis library used by the MMT-Probe. Its functionality allows analysing the data extracted by the MMT Probe in order to detect security issues and attacks on the monitored network traffic. The rules (also referred as security properties) specify the sequence of events that need to be detected and are expressed in XML files. Each rule defines a context and a trigger that allows detecting both wanted of not wanted security or functional behaviour (i.e., sequence of network events related to IP packets or flows in time).

MMT Operator:

MMT-Operator is the front-end of the tool. It is a web-based application that allows visualising, in near real-time, network traffic statistics and alerts or notifications detected by the verification of the security properties. In addition, this application also offers the possibility of collecting historical data about the analysis, aggregating it to offer historical reports and graphics.

Deployment Flexibility

As stated before, MMT has been conceived with a modular approach, which allows deploying each component independently. Each component of the tool uses a set of internal communication mechanisms to communicate with other components, transmitting the required information to the next part of the computation performed. Some of the mentioned communication channels rely in proprietary technologies, while others use standards protocols.

Protocol Compatibility

The ANASTACIA consortium has agreed to establish and use standard protocols to communicate between the different components of the framework. In particular, three principal protocols are under evaluation for later implementation, linking:

- **Agents to Monitoring Tool**: Since the MMT Probe works analysing directly the raw data of the network, the PCAP format provides a complete and standard support to transmit all the information required by this module.
- **Monitoring to Reaction**: Both the Monitoring and the Reaction modules will be formed by the composition of multiple submodules brought by different partners. These requirements impose the constraint of defining a common communication protocol between the two modules. To this end, the ANASTASCIA partners have already proposed the Intrusion Detection Message Exchange Format (IDMEF)[2] as the format to transfer the detected security breaches from the Monitoring to the Reaction module.
- **Reaction to Security Orchestrator**: Finally, the suggested set of countermeasures computed by the Reaction modules needs to be transmitted to the Security Orchestrator, which is in charge of deploying the final countermeasures to enforce the security policy. The communication of the

[2] https://www.ietf.org/rfc/rfc4765.txt

suggested measures should be done by using a clear representation, which is the case of the OpenC2 protocol[3] proposed by the ANASTACIA partners.

MMT has already been designed to work directly with both live captures (by means of the PCAP library) and PCAP files. The tool is already fully compatible with the first scenario.

However, for the Monitoring to Reaction and Reaction to Security Orchestrator communications, MMT does not have a predefined communication protocol since it relies on a script to define what needs to be done in reaction to a security breach.

In this sense, the Integration of MMT into these components will require an adaptation of the MMT capabilities in order to support the agreed communication protocols once the viability study is finished in the project.

The adaptations of MMT to use standard communication protocols will allow the tool to work in collaboration with other third-party components, taking advantage of their features to provide added value to the ANASTACIA platform.

[3] http://openc2.org/

7 CONCLUSIONS

A set of 20 high-level functional requirements, 15 non-functional requirements and 16 privacy requirements (mainly GDPR-derived) has been formalized to support software architects and developers in the formalization of the ANASTACIA architecture and in the definition of the included components, modules and interfaces.

Requirements includes also privacy-related constraints that should be taken into consideration at design and development level to provide end-users with useful indication for compliancy of the monitored system with the upcoming GDPR.

The analysis included in this deliverable will be further extended and refined after the first cycle of validation and evaluation in order to better address requirements that might be expressed during the related activities, and fine tune the final prototype to ease the start of the pre-industrialization phase.

The results of this revamp will be duly documented in the second release of this document – D1.4 “Final User-centred Requirements Analysis” – and will contribute to the refinement and release of the final ANASTACIA prototypes.

8 ANNEX 1 – INTERVIEW QUESTIONNAIRES

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	5
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	5
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	5
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	3

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
   - SND – Low
   - NFV – Low
   - CPS – Medium
   - IoT – High
2. How is cybersecurity generally managed in your domain[3]?
   - mainly re-active management
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
   - Very low risk acknowledgement and understanding
   - Lack of expertise
   - Lack of easy to deploy solutions
   - Lack of multi-tenancy solutions
   - Lack of integration between Infrastructure Composability and Security Management
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
   - Nothing relevant to my mind. But HPE reports underline how 70% of business have been actually breached without realising it
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
   - No
6. Who do you think might use ANASTACIA in your domain?
   - Our Managed Services Division to provide Managed Security Services
7. Who do you think might benefit the most from ANASTACIA in your domain?
   - Customers, Customers' Employees, Service Providers
8. Would you consider using a solution based on ANASTACIA (see description above)?
   - Yes, provided it can allow a multi-tenancy deployment
9. Is there any recommendation you would like to give our project at design / development phase?
   - Take into account Service Provider
   - Take into account most of the threats are in SMBs market, who are usually unaware or poorly informed
10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

easy to use	4	has intuitive / adaptive user interfaces	5
low cost	4	provides real-time feedback	5
powerful reporting	3	includes dynamic network topology	5
well supported	5	developed by big vendors	2
flexible to customise	5	modular architecture	5
scalable to grow	5	compliant with standards	3
large, well-known vendor	2	autonomous reaction to threats	5
good feedbacks / reputation	4	self-healing / self-repair capabilty	5
integrates with other software	5	highly configurable (e.g. rule editing)	5
licensed as open-source	3	other (……)	

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	5
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	3
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	3
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	5

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]? Medium, Medium, High, High
2. How is cybersecurity generally managed in your domain[3]? It is not very clear what is the meaning of "managed" in this context, do you refer to best practices/standards or something else? If related to my assumption, then I would say Cyber Physical Systems and IoT
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain? The correct identification of related ICT risks and mitigation measures (e.g., which security controls to implement), and while providing alignment with relevant internal/external regulations.
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How? This information cannot be disclosed without an NDA.
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones? Yes, many of which are off-the-shelf solutions or few are developed/maintained in-house. Higher focus on monitoring, enforcing and user-friendly configuration. Minor focus on DSPS due to the lack of tools/standards.
6. Who do you think might use ANASTACIA in your domain? Mostly security compliance officers, security architects, CERT team, and security operations.
7. Who do you think might benefit the most from ANASTACIA in your domain? Apart from the previously mentioned, also end-users willing to assess the trustworthiness of our products and services (related to the DSPS).
8. Would you consider using a solution based on ANASTACIA (see description above)? Yes
9. Is there any recommendation you would like to give our project at design / development phase? Align as much as possible with existing standards and industrial best-practices, in particular related to the topic of DSPS.
10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	5	has intuitive / adaptive user interfaces	5
low cost	3	provides real-time feedback	4
powerful reporting	3?	includes dynamic network topology	3?
well supported	5	developed by big vendors	2
flexible to customise	3	modular architecture	4
scalable to grow	4	compliant with standards	5
large, well-known vendor	2	autonomous reaction to threats	3

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

good feedbacks / reputation	3	self-healing / self-repair capabilty	3
integrates with other software	5	highly configurable (e.g. rule editing)	3
licensed as open-source	4	other (……)	na

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	2
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	2
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	3
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	5

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
   MEDIUM

2. How is cybersecurity generally managed in your domain[3]?
   Other Domains: CyberSecurity is an overall aspect of a Telecom Equipment and it involves boith the carried traffic than the ControlPlane/Network Manager System. SW platform (i.e. Linux Based or proprietary) are up to date for security threats even if not on a Common Platform as ANASTACIA may be. CyberSecurity Audits are typically performed in pre delivery phase of a product.

3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
   The key cybersecurity issues associated to TLC are from level 1 to level 4 OSI Stack attack, often are DoS or Sniffing also at physical level (Optical Intrusion) or DCN DoS.

4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
   I' ve been witness of a DoS over DCN at a Regional Carrier in the USA, it was generated by a wrong configuration of Firewalling

5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
   ICT Firewalls, MSPP Equipment (ALU 1850TSS-100)

6. Who do you think might use ANASTACIA in your domain?
   Telecom equipment manufacturer, telecom provider Tier 1

7. Who do you think might benefit the most from ANASTACIA in your domain?
   Telecom equipment manufacturer

8. Would you consider using a solution based on ANASTACIA (see description above)?
   Yes, I would

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

9. Is there any recommendation you would like to give our project at design / development phase?
No, there isn't at the moment.

10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	3	has intuitive / adaptive user interfaces	2
low cost	4	provides real-time feedback	2
powerful reporting	4	includes dynamic network topology	2
well supported	2	developed by big vendors	2
flexible to customise	4	modular architecture	4
scalable to grow	4	compliant with standards	3
large, well-known vendor	2	autonomous reaction to threats	4
good feedbacks / reputation	5	self-healing / self-repair capabilty	3
integrates with other software	3	highly configurable (e.g. rule editing)	5
licensed as open-source	3	other (.....)	

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	5
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	5
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	4
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	4

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
   LOW
2. How is cybersecurity generally managed in your domain[3]?
   Pilot Doman
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
   Standardize authentication, confidetiality and RBAC in power systems management information exchange and secure communication from DoS (Denial of Service).
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
   For example, power outage occurred in December 2015 in Ukraine due to a cyber attack. The attack was acted by embedding the Blackenergy malware in MS Office documents and delivered via e-mail to individual of electricity company IT network.
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
6. Who do you think might use ANASTACIA in your domain?
7. Who do you think might benefit the most from ANASTACIA in your domain?
8. Would you consider using a solution based on ANASTACIA (see description above)?
9. Is there any recommendation you would like to give our project at design / development phase?
   Authentication and Confidentiality in configuration and control operations.
   A good practice is the use of a PKI infrastructure and X.509 certificates to authenticate servers, software and users. Futhermore, protect communication channels applying, for example, the IEC 62351-3 requirements.
10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	4	has intuitive / adaptive user interfaces	4
low cost	3	provides real-time feedback	4
powerful reporting	5	includes dynamic network topology	4
well supported	4	developed by big vendors	2
flexible to customise	4	modular architecture	4
scalable to grow	4	compliant with standards	5
large, well-known vendor	3	autonomous reaction to threats	3
good feedbacks / reputation		self-healing / self-repair capabilty	3
integrates with other software	3	highly configurable (e.g. rule editing)	4

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

licensed as open-source | 3 | other (.....) |

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	4
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	4
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	3
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	3

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
   We are primarily interested in IoT and NFV technologies but as of today we have a LOW expertise in both of them.
2. How is cybersecurity generally managed in your domain[3]?
   We use a multilayer approach , essentially using the Security in Depht paradigm.
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
   We face primarily denial of services attempt and botnet infection attempt
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
   On IoT domain, the sole Mirai Botnet made big news ; from our sensors we are seeing multiple attempt a day from infected appliances getting blocked. On SDN side we are currently unaware of anything in the wild actively exploited but for any increase in architecture complexity there is usually an increased risk.
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
   We use online monitoring and testing tools but nothing with real time reaction capabilities.
6. Who do you think might use ANASTACIA in your domain?
   CISO and Security Engineers
7. Who do you think might benefit the most from ANASTACIA in your domain?
   System engineers tasked to manage and maintain complex systems.
8. Would you consider using a solution based on ANASTACIA (see description above)?
   Yes I would.
9. Is there any recommendation you would like to give our project at design / development phase?
   Work toward a high level of interoperability with third party solutions.
10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	4	has intuitive / adaptive user interfaces	4
low cost	3	provides real-time feedback	5
powerful reporting	4	includes dynamic network topology	4
well supported	5	developed by big vendors	3
flexible to customise	4	modular architecture	5
scalable to grow	4	compliant with standards	5
large, well-known vendor	3	autonomous reaction to threats	4

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

good feedbacks / reputation	5	self-healing / self-repair capabilty	3
integrates with other software	5	highly configurable (e.g. rule editing)	5
licensed as open-source	2	other (……)	

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	5
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	3
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	4
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	4

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
   Very high in regards to CPS and IoT but low in SDN and NFV
2. How is cybersecurity generally managed in your domain[3]?
   There is cyber security related to secure product design and protection of Company infrastructure. Cloud systems and infrastructure is managed by IT. Product security is managed by Engineering
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
   (1) Legacy products that are in the field for 10+ years and are not easily patchable (2) increasing sophistication of cyber attacks
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
   The Target attack of 2013 is a related attack; Several 10s of millions of credit card information was stolen. Hackers leverages vulnerabilities through a channel created for HVAC vendor support and used that to connect to secure systems
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
   I am not aware of any
6. Who do you think might use ANASTACIA in your domain?
   Those primarily requiring IoT infrastructure protection and these could be a wide variety
7. Who do you think might benefit the most from ANASTACIA in your domain?
   IT team of companies
8. Would you consider using a solution based on ANASTACIA (see description above)?
   If the key objectives are met, then yes
9. Is there any recommendation you would like to give our project at design / development phase?
   Requirements need to be laid down very clearly.
   The operation should be clarified using real use-case scenarios and extensively tested with a large number of test cases. The designers need to think like hackers.

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	4	has intuitive / adaptive user interfaces	4
low cost	3	provides real-time feedback	4
powerful reporting	4	includes dynamic network topology	3
well supported	4	developed by big vendors	3
flexible to customise	4	modular architecture	4
scalable to grow	5	compliant with standards	4
large, well-known vendor	3	autonomous reaction to threats	4
good feedbacks / reputation	4	self-healing / self-repair capabilty	4
integrates with other software	3	highly configurable (e.g. rule editing)	4
licensed as open-source	4	other (.....)	

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	5
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	5
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	3
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	3

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]? low
2. How is cybersecurity generally managed in your domain[3]? Standard approach: firewall, password protection, antivirus + antispam
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain? Anti-intrusion detection (anti-virus+anti-spam)
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
6. Who do you think might use ANASTACIA in your domain? Network Manager
7. Who do you think might benefit the most from ANASTACIA in your domain? Netowrk and system management
8. Would you consider using a solution based on ANASTACIA (see description above)? Yes for the EPC management e monitoring
9. Is there any recommendation you would like to give our project at design / development phase? no
10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	5	has intuitive / adaptive user interfaces	3
low cost	3	provides real-time feedback	4
powerful reporting	2	includes dynamic network topology	4
well supported	3	developed by big vendors	2
flexible to customise	3	modular architecture	3
scalable to grow	4	compliant with standards	3
large, well-known vendor	3	autonomous reaction to threats	3
good feedbacks / reputation	2	self-healing / self-repair capabilty	3
integrates with other software	3	highly configurable (e.g. rule editing)	3
licensed as open-source	2	other (……)	

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	3
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	5
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	5
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	4

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?

SDN: HIGH; NFV: HIGH; CPS: MEDIUM; IoT: LOW.

2. How is cybersecurity generally managed in your domain[3]?

Manual intervention, monitoring and reaction by legally responsible system engineers.

3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?

My domain is mostly related to cybersecurity issues in Internet routing and communication connection management.

In Internet routing, it is possible under certain exploit conditions to alter DNS mapping (name to IP address) hence affectinv connection confidentiality and integrity. Moreover, by hijacking Internet route, one can easily make Internet-reachable services down or run man-in-the-middle attacks.

In terms of connection management, the distributed nature of the Internet and the end-to-end nature of connection suffers from important vectors of attacks to end systems.

4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?

For Internet routing attacks, it is well known there are major threats related to DNS mapping and BGP route hijacking.

(i) For DNS mapping, the adoption of DNSSEC is proceeding well and the threat is manageable.
(ii) For BGP, the adoption of BGP security extensions recently defined is not proceeding well due to lack of technical and economic incentives (too costly to deploy, for securing a too rare event). An example is the interruption of Youtube services in 2008 due to a Youtube ban ordered by Pakistan government which was automatically spread to neighbouring countries due to errors in configuring BGP. Another example was run in Defcon 2008 where it was demonstrated who the whole conference Internet traffic could be captured by attackers by running real-time a BGP hijacking attack on the corresponding Decon network.

For Internet connection and service availability threats:

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

(i) some providers of some densely populated countries are able to inject scripted active code in HTTP relayed web content in billions of different HTTP sessions concurrently hence easily causing distributed denial of service attacks and potentially blocking any Internet-reachable service. This is known to happen in China.

(ii) Some IoT device vendors seeking the least possible cost are selling millions of devices not secured against remote control and hence the generation of DDOS attacks. This was recently proven for domestic web surveillance cameras.

5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?

No.

6. Who do you think might use ANASTACIA in your domain?

To raise awareness on security flaws present in a given network to network administrators and legal responsible persons.

7. Who do you think might benefit the most from ANASTACIA in your domain?

Network administrators and legal responsible persons.

8. Would you consider using a solution based on ANASTACIA (see description above)?

Yes.

9. Is there any recommendation you would like to give our project at design / development phase?

Focus on Internet connection attacks and related DDoS vectors.

10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	5	has intuitive / adaptive user interfaces	5
low cost	3	provides real-time feedback	4
powerful reporting	3	includes dynamic network topology	5
well supported	5	developed by big vendors	3
flexible to customise	3	modular architecture	5
scalable to grow	4	compliant with standards	5
large, well-known vendor	4	autonomous reaction to threats	5
good feedbacks / reputation	4	self-healing / self-repair capabilty	5
integrates with other software	5	highly configurable (e.g. rule editing)	3
licensed as open-source	3	other (.....)	na

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	3
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	5
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	3
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	9

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?
   NONE, NONE, LOW, HIGH
2. How is cybersecurity generally managed in your domain[3]?
   Smart Building: with classical solutions, e.g., firewalls, NATs, etc.
3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?
   Exfiltration of sensitive data, including covert channels and attacks that can endanger the physical security of individuals.
4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?
   In general, many Building Automation Systems have been designed for a less-aggressive and sophisticated cybersecurity scenario. Standards like EIB/KNX, LON or BACnet, were designed many years ago with very limited focus on IT security as well as when the IoT paradigm still was in its infancy.
5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?
   Not aware.
6. Who do you think might use ANASTACIA in your domain?
   IoT-based providers, especially for automations in Industry 4.0, e.g., intelligent manufactory, IoT and cloud offloading scenario.
7. Who do you think might benefit the most from ANASTACIA in your domain?
   End-users.
8. Would you consider using a solution based on ANASTACIA (see description above)?
   Yes, even if it is out of the scope of my knowledge. In other words, ANASTACIA is surely of interest, but I can't evaluate how does it cost in terms of portability over legacy services, additional hardware/software requirements, need of migrating pre-existent frameworks over new deployments.
9. Is there any recommendation you would like to give our project at design / development phase?
   Test security and do formal analysis over protocols and implementation as to prevent covert channels, data exfiltration or possible side channel to leak sensitive information.

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	3	has intuitive / adaptive user interfaces	2
low cost	2	provides real-time feedback	3
powerful reporting	3	includes dynamic network topology	4
well supported	4	developed by big vendors	4
flexible to customise	4	modular architecture	4
scalable to grow	4	compliant with standards	5
large, well-known vendor	4	autonomous reaction to threats	2
good feedbacks / reputation	4	self-healing / self-repair capability	2
integrates with other software	5	highly configurable (e.g. rule editing)	5
licensed as open-source	1	other (.....)	

Objectives

Can you please rate from 1 (low) to 5 (high) the relevance of our objectives?

To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.	5
To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT and, more generally, smart objects communications.	4
To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.	4
To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.	5

Would you please briefly answer the following questions?

1. Which is your level of expertise[1] in SDN, NFV, CPS and IoT respectively[2]?

   WE ARE DEVELOPING A CYBERSECURITY CERTIFICATION SYSTEM WITHIN THE EUROPEAN CYBER SECURITY ORGANISATION (ECSO) – I AM THE CHAIRMAN OF THE RESPONSIBLE SUB-WORKING GROUP AND I AM A MEMBER OF THE ECSO BOARD OF DIRECTORS

2. How is cybersecurity generally managed in your domain[3]?

   MY EXPERTISE IS IN THE STANDARDISATION, TESTING AND CERTIFICATION INDUSTRY AND AS MENTIONED ABOVE

3. Can you provide a quick overview of the key cybersecurity issues associated to your domain?

   WE ARE WORKING UPON THE CERTIFICATION OF IOT WITH A MANDATE FROM THE EUROPEAN COMMISSION UNDER THE CYBERSECURITY PPP.

4. Are you aware of any big cyber security breach in your domain? If yes, what happened? How?

   AGAIN, MY RELEVANCE IS IN THE REALM OF CYBERSECURTIY CERTIFICATION

5. Are there systems supporting today the ANASTACIA's functionalities in your domain? If yes, which ones?

   YES, CERTIFICATION AND THE SECURITY AND PRIVACY SEAL I WAS THE CREATOR OF THE INITIAL CONCEPT OF THE EUROPEAN SECURITY LABEL WITHIN WORKING GROUP 10 (INNOVATION) UNDER THE EUROPEAN RESEARCH AND INNOVATION FORUM EFFORTS GOING BACK TO 2009. THE INITIAL CONCEPT IS CONTAINED IN A WHTE PAPER DEVELOPED WITHIN THE EUROPEAN JOINT RESEARCH CENTRE.

6. Who do you think might use ANASTACIA in your domain?

   IT WILL BE IMPORTANT TO COORDINATE CYBERSECURITY CERTIFICATION EFFORTS

7. Who do you think might benefit the most from ANASTACIA in your domain?

   THE ECSO

[1] [NONE – LOW – MEDIUM – HIGH]
[2] Software Defined Networks, Network Function Virtualization, Cyber Physical Systems, Internet of Things
[3] Pilot Domain 1: Mobile Edge Computing - Pilot Domain 2: Smart Building Management Systems – Others domains

8. Would you consider using a solution based on ANASTACIA (see description above)?

YES, THE LABEL COULD BE SOMETHING TO LOOK TOWARD TOGETHER

9. Is there any recommendation you would like to give our project at design / development phase?

10. Would you please rate from 1 (low) to 5 (high) the relevance of the following features?

easy to use	5	has intuitive / adaptive user interfaces	5
low cost	4	provides real-time feedback	3
powerful reporting	3	includes dynamic network topology	3
well supported	3	developed by big vendors	2
flexible to customise	4	modular architecture	3
scalable to grow	5	compliant with standards	5
large, well-known vendor	2	autonomous reaction to threats	5
good feedbacks / reputation	4	self-healing / self-repair capabilty	4
integrates with other software	5	highly configurable (e.g. rule editing)	3
licensed as open-source	3	other (……)	

9 ANNEX 2 – INTERVIEWEES

This section includes a short overview of interviewees' CVs.

9.1 INNOVATION ADVISORY BOARD MEMBERS

Diego R. Lopez (Telefonica)

Senior Technology Expert at Telefonica I+D, Chair of ETSI NFV ISG, Co-chair of IRTF's NFVRG. Since October 2011 he is in charge of Technology Exploration at the Global CTO Unit, within Telefónica I+D. His responsibilities are related to the definition and coordination of research projects in the areas of new networking technologies and network infrastructures. He is directly involved in activities related to network virtualization, core optimization, AAA, traffic analysis, and infrastructure security. He is actively participating in the ETSI ISG on Network Function Virtualisation (NFV), which he chairs. HE is acting as representative of Telefónica in bodies related to network technologies, and chairing the IRTF NFV Research Group. He has been appointed by the European Commission as member of the High Level Expert Group on Scientific Data e-Infrastructures (HLEG-SDI). He received my MS from the University of Granada in 1985, and his PhD degree from the University of Seville in 2001, with a thesis related to AI and fuzzy logic, and their application to control problems. Since 1985 he has worked for several private and public organisations, developing and deploying communication services. From 2000 to 2011 he was responsible for the Middleware Area of RedIRIS, the Spanish National Research and Educational Network. As part of these tasks he actively participated in national and international working groups and projects, and he collaborated in several versions of the e-Infrastructure Reflection Group White Paper, under the auspices of the EU Presidency, in areas related to security and digital identity services. His current areas of interest are network middleware, network virtualization, infrastructural and mediation services, infrastructural security, the application of AI techniques to network management and security, and new network architectures. Specialities: NFV and Software Networks. Internet middleware. Federated architectures. Directories (LDAP). Identity management systems: SAML, OpenID, OAuth. PKI. Internet security.

Jesus Luna (Bosch)

Security Architect at Robert Bosch Inc. Experienced researcher, developer and manager in the field of IT security, with more than 14 years working with public and private industries. Specially focused on mechanisms aimed to protect Cloud and Grid infrastructures and, other Service Oriented Architectures in different application fields (i.e. financial, eHealth and Government 2.0).Fluent in English and with excellent communication skills thanks to active participation in academia (conference participant, theses adviser) and industrial forums. Specialties: Security and Privacy in Cloud, Grid computing, VANETs and WSN.

Christian Mastrodonato (Konica Minolta)

Chief Technologist at Konica Minolta, Inc. Since 2007 he works in Digital Innovation managing business units, large projects and programmes in enterprise, consulting and public funding environments, with very diverse application fields, from construction and energy to healthcare and business electronics and large breadth of technologies from Artificial Intelligence and Machine Learning to IoT and Semantic Technologies. His experience covers all the aspects of Digital innovation from business (M&A, bid management, client engagement, partnerships, programme management, P&L) to technology management (technology strategy, architecture design, agile development, IP management).

Stefano Secci (LIP6)

Stefano Secci is an Associate Professor at the Universite Pierre et Marie Curie (UPMC - Paris VI - Sorbonne Universites), Paris, France, conducting research within the PHARE group, Networks and Systems department, CNRS LIP6. He received the M.Sc. degree in communications engineering from Politecnico di Milano, Milan, Italy, in 2005, and a dual Ph.D. degree in computer science and networks from Politecnico di

Milano (Networks group) and Telecom ParisTech (NMS group), France, in 2009. In 2010, he worked as Post-Doctoral Fellow with NTNU (Q2S), Norway, and George Mason University (CNL), USA. Before the Ph.D., in 2005-2006, he worked as a Research Associate with Ecole Polytechnique de Montreal (GERAD), Canada, and with Politecnico di Milano, and as a Network Engineer with Fastweb Italia, Italy. Dr Secci is IEEE Senior member.

9.2 PRIVILEGED OBSERVERS IN PILOT DOMAINS (MEC/BMS)

MEC: Stefano Secci (LIP6)

Stefano Secci is an Associate Professor at the Universite Pierre et Marie Curie (UPMC - Paris VI - Sorbonne Universites), Paris, France, conducting research within the PHARE group, Networks and Systems department, CNRS LIP6. He received the M.Sc. degree in communications engineering from Politecnico di Milano, Milan, Italy, in 2005, and a dual Ph.D. degree in computer science and networks from Politecnico di Milano (Networks group) and Telecom ParisTech (NMS group), France, in 2009. In 2010, he worked as Post-Doctoral Fellow with NTNU (Q2S), Norway, and George Mason University (CNL), USA. Before the Ph.D., in 2005-2006, he worked as a Research Associate with Ecole Polytechnique de Montreal (GERAD), Canada, and with Politecnico di Milano, and as a Network Engineer with Fastweb Italia, Italy. Dr Secci is IEEE Senior member.

BMS: Vijay Lakamraju (Cybersecurity Leader for UTC products)

Assoc. Director leading product cyber security related functions for the commercial businesses of UTC, comprising of world leading companies that provide building and residential systems such as HVAC, elevator, physical security and life safety systems.

9.3 OTHERS PROFESSIONAL EXPERTS

Roberto Pastorino (Cleis Security, System Engineer)

System Engineer at Cleis Security S.r.l. IT professional, Experienced in Microsoft Servers and Active Directory, MDaemon mail server, experienced in supporting small business needs (near-to-zero budget / high demands / higher expectations) Specialties: Networking, LAN, WAN, client - server architecture, TCP/IP and networking protocols, systems deployment, network security. Microsoft operating systems, MDaemon mail server, Wireshark network dissection.

Oriano Sità (Italeaf, Chief Information Officer)

Responsible in TerniEnergia Group / Italeaf for IT infrastructure management and related projects of unification of group information systems. Also CIO and Networks & Systems Manager with focus in Harmonization of networks and systems between group companies, Systems management and system resource coordination, Management of technology purchases for companies, Modernization of systems, Virtualization of internal systems, System Management

Lorenzo Papini (Selesoft, Geographic TLC Network Expert)

Strategic Account at Proteco Group. Specialized in customer support for critical situation which requires fast intervention, problem solving and high skills. Being the man who makes the things happen, using the skills acquired in all the field of Telecom Equipment manufacturing (HW/SW) and installation. Using human communication skills which make me possible to talk up from CEO to the junior engineer or field installer. Ability to work in globalised environment, interacting with customers and development team worldwide.

Marco Grechi (Senior SCADA Systems & Telecomms Specialist, Member of IEC TC57)

Senior SCADA Systems & Telecomms Specialist - Member of IEC TC57. Software/Firmware design & development, Hardware systems design, Industrial telecommunications & cyber security, Industrial SCADA systems, Power Management and Oil & GAS plants controls, Member of CEI CT57 and IEC TC57 WG3

(Telecontrol Protocols) and WG15 (Data and Communication Security). Active participation in the IEC TC57 WG15 meetings. IEC project leader and editor of the Technical Specification IEC 62351-100-1 "Conformance Testing of IEC 62351-5 and its derivatives". Involved in the updating of IEC 62351-5 and IEC 60870-5-7.

Luca Caviglione (Researcher at CNR – ISSIA)

Luca Caviglione participated in many Research Projects funded by the EU, by ESA, and by Siemens COM AG. He is author and coauthor of more than one hundred academic publications about TCP/IP networking, p2p systems, QoS architectures and wireless networks. He participates in TPCs of several conferences, and gives talks about IPv6 and p2p. In 2006 he was with the Italian National Consortium for Telecommunications - Genoa Research Unit. Since 2007, he works at the Istituto di Studi sui Sistemi Intelligenti per l'Automazione, Italian National Research Council, Genoa, Italy. He is a WG Leader of the Italian IPv6 Task Force and he has filed, as a coauthor, several patents in the field of p2p. Luca is also a Professional Engineer. From April 2011, he is Associate Editor of the Transactions on Emerging Telecommunications Technologies, Wiley. Specialties: p2p Networking, Traffic Analysis, Cocoa programming, Social Networks, Technical Writing, Network Security.

Mark Miller

CEO of CONCEPTIVITY (www.conceptivity-switzerland.com), Vice Chairman of EOS, Member of the Board of Directors at European Cyber Security Organisation, European Cyber Security Organisation (ECSO) IMD (International Institute for Management Development) - Business Programs, Supply Chain Security, Cybersecurity & Logistics Specialties: Supply Chain Security & Logistics