ANASTACIA

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

D1.3

Initial Architectural Design

This deliverable presents the results of ANASTACIA Task 1.3. The aim of the task is to design the ANASTACIA framework. This deliverable includes the initial design of the ANASTACIA architecture, including the methodology carried for its design.

Distribution level	PU
Contractual date	30.09.2017 [M9]
Delivery date	30.09.2017 [M9]
WP / Task	WP1/T1.3
WP Leader	Atos
Authors	Ruben Trapero (ATOS), Diego Rivera (MONT), Tarik Taleb, Ivan Farris (AALTO), Dallal Belabed (THALES), Cédric Crettaz (MAND), Antonio Skarmeta, Jorge Bernal, Alejandro Molina, Jordi Ortiz (UMU), Rafael Marín Pérez (ODINS), Alie El-Din Mady (UTRC), Stefano Bianchi (SOFT)
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

Index of figures

Index of tables

PUBLIC SUMMARY

This deliverable includes the initial design of the ANASTACIA architecture. The creation of the ANASTACIA reference architecture has followed an incremental analysis process that starts from the requirements and context analysis carried out in D1.1 and D1.2. The design methodology has also been described in this document. This analysis has been used to identify the main objects involved in ANASTACIA, which has derived into a conceptual model. This conceptual model has a twofold utility: on the one side it represents the way that ANASTACIA is modelling security for IoT/CPS platforms. On the other hand it helps to identify the involved elements, the pieces of information managed, and the terminology of the concepts used in the project. This conceptual model is used as reference for the creation of the ANASTACIA architecture.

Additionally, this deliverable also shows the envisioned system model for ANASTACIA. This system model shows how the ANASTACIA framework is positioned within an IoT infrastructure. In general terms, ANASTACIA will work on top of an IoT infrastructure and merged the control elements of the IoT platform such as IoT controllers or virtual interfaces.

Both the system model and the conceptual model are used as inputs for design of the ANASTACIA architecture. The ANASTACIA architecture has been designed as a set of layers derived from the main activities identified from the conceptual model: security policy set-up, security policy enforcement, monitoring, reaction and the seal creation. These activities are also described in detail in this deliverable. The individual components that are part of every plane of the architecture and the main interfaces between them are also detailed in this deliverable. D1.3 has given priority to the definition and design of security policies and its enforcement, which is the basis for the functional specification of the ANASTACIA framework. Details on privacy considerations (including the incorporation of privacy elements to the enforced policy) will be given in the final report of the ANASTACIA architecture that will be delivered in D1.5.

The design of the ANASTACIA architecture has been done in close collaboration with the technical work packages (WP2-3-4-5), as its outcomes will be used as input to guide the implementation activities.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

The main objective of the ANASTACIA project is the development of a trustworthy-by-design autonomic security framework with testing, validation and security optimization capabilities. ANASTACIA combines several elements from different domains: from IoT controllers to virtual functions accessible through SDN/NFV interfaces, orchestration of security policies and enforcement of security preferences in heterogeneous scenarios. This document describes the initial results on the design of the ANASTACIA framework, including the description of the complete process for the design of the ANASTACIA architecture. The ANASTACIA framework and the details of all the components involved in the architecture lays the foundations of the rest of the WPs of the project, namely the technical WP (WP2, 3, 4, and 5). These WPs will trigger the implantation activities based on the design and results reported in this deliverable.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- Grant Agreement N°731558 – Annex I (Part A) – Description of Action
- Consortium Agreement v1.0 – December 6th 2016
- D1.1 – Holistic Security Context Analysis
- D1.2 – User-centred Requirement Initial Analysis

1.3 REVISION HISTORY

Table 1. Document revision history

Version	Date	Author	Description
0.1	22.5.2017	Ruben Trapero (ATOS)	Skeleton of expected contents
0.2	30.6.2017	Ruben Trapero (ATOS)	First set of inputs
0.3	10-7-2017	ALL	First integrated draft
0.8	07-08-2017	ALL	First complete draft
0.9	28-08-2017	Ruben Trapero (ATOS) and Stefano Bianchi (SOFT)	Added acronyms and requirements coverage
0.10	01-09-2017	ALL	Version released for UMU review
0.11	15-09-2017	Ruben Trapero (ATOS)	Revised version
1.0	25-09-2017	Ruben Trapero (ATOS)	Final version released, ready to be delivered

1.4 Acronyms and Definitions

Table 2. List of acronyms

Acronym	Meaning
BMS	Building Management Systems
CPS	Cyber Physical System
CRUD	Create, Read, Update, and Delete
DSPS	Dynamic Security and Privacy Seal
FR	Functional Requirement
GDPR	General Data Protection Regulation
HSPL	High Security Policy Language
IoT	Internet of Things
MANO	Management and Orchestration
MEC	Mobile (Multi-access) Edge Computing
MMT	Montimage Monitoring Tool
MSPL	Medium Security Policy Language
MTTR	Mean Time to Recovery
NFR	Non-Functional Requirement
NFV	Network Function Virtualization
PR	Privacy Requirement
SDN	Software Defined Networking
SIEM	Security Information and Event Management

2 DESIGN METHODOLOGY

The ANASTACIA consortium has carried out an exhaustive and comprehensive analysis process in order to carry out the design of the ANASTACIA framework. The final objective has been the fulfilment of the requirements and expected functionalities as described in D1.2, supported by the context analysis carried out in D1.1. Furthermore, there has been a continuous feedback between the tasks in charge of capturing requirements and the task responsible for designing the ANASTACIA framework.

The design methodology is based on the obtaining different partial achievements, which adds additional concreteness to the design of the ANASTACIA architecture. Figure 1 represents the roadmap for obtaining such partial achievements. The process comprises three phases:

- **Phase 1 - Result expected: ANASTACIA Reference Model**. The result of this Phase represents the highest level of abstraction and the lowest level of granularity. The main objects participating in ANASTACIA and their respective relationships are defined.
- **Phase 2 – Result expected: ANASTACIA High Level Architecture**. The result of this Phase represents a higher level of concreteness by grouping the elements identified in Phase 1 according to common functionalities.
- **Phase 3 – Result expected: ANASTACIA Detailed Architecture**. The result of this Phase represents the highest level of concreteness, by specifying components and interactions between them. This achievement is the previous step to the implementation activities.

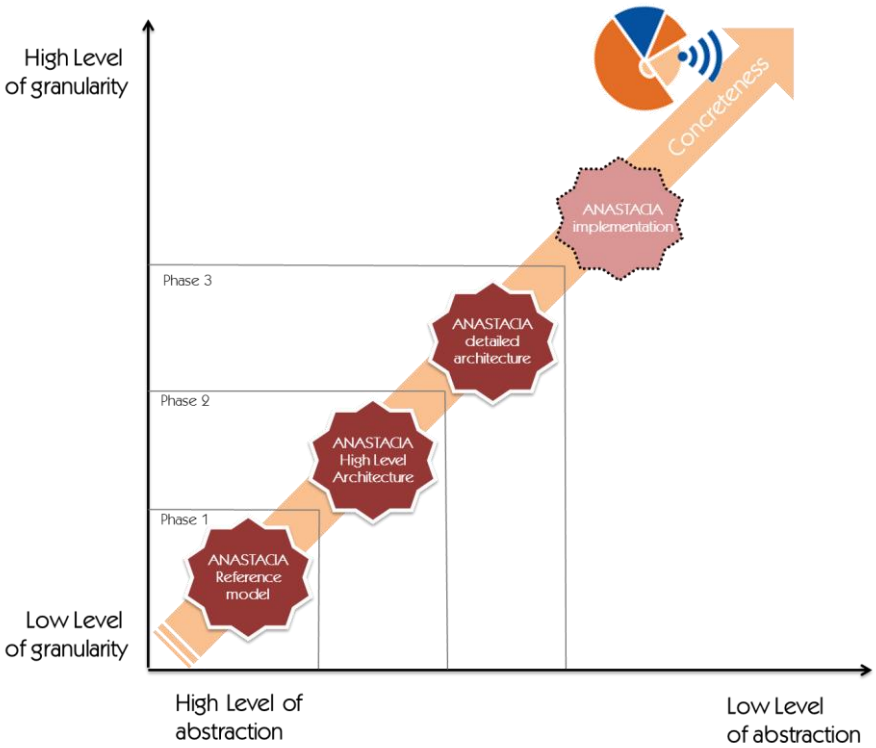


Figure 1. ANASTACIA achievements expected during the architecture design

An incremental process for designing the framework has been used for obtaining the achievements expected in each phase. Every step of the process adds an additional degree of detail by analysing (1) the results obtained from other activities in ANASTACIA, (2) partners' previous experience and (3) other related projects. Figure 2 represents the process followed in the methodology to design the ANASTACIA framework. The process starts with the analysis of the requirements and use cases done in D1.2. This analysis is also supported by the context analysis created in D1.1, which has been used as background for

every requirement identified in D1.2. The initial concept envisioned for ANASTACIA before the start of the project is also used as reference input during the design process. Section 3 describes the overview of the elicited requirements and the way they have been used in the design of the ANASTACIA framework. The following step comprises the identification of the elements that participates in ANASTACIA. This is the previous step to the creation of the ANASTACIA reference model. These elements have been identified based on the use cases elicited in D1.2, which derive from the requirements evaluated in that deliverable. These elements are then organized into groups, also identifying the existing relationships among them. This results in the ANASTACIA reference model, which accomplishes Phase 1 of the design. The details of the ANASTACIA reference model, and how it was created, are described in Section 4. Section 4 concludes with the ANASTACIA system model which is based on the ANASTACIA reference model and on the work done during the inception of the project.

The following step comprises the classification of the elements included in the ANASTACIA reference model. This classification has been done according to functional criteria and considering the ANASTACIA system model. The result is the high level architecture of ANASTACIA, which is the general framework that will include the concrete components that will be implemented after the design phase. Mapping this high level architecture to the main activities identified in ANASTACIA (and derived mainly from the use cases obtained in T1.2) results in the ANASTACIA detailed architecture. This finalizes Phase 3 and is the previous step to the implementation activities. The detailed architecture specifies modules, components, interfaces and main interactions within the ANASTACIA framework and with external participants, such as the IoT platform to protect and its available resources. The process to create the high level and detailed architecture is specified in Section 5, while Section 6 describes the main activities carried out by ANASTACIA and Section 7 details every component of the detailed architecture.

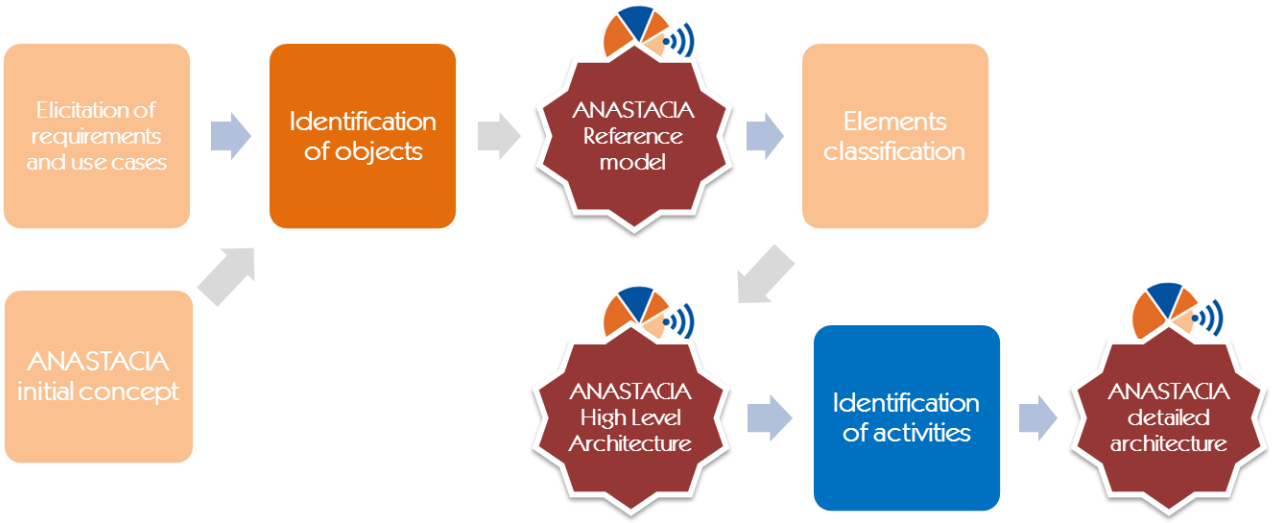


Figure 2. Design methodology followed in ANASTACIA

The design activities described in the following sections have been carried out in continuous feedback with the technical WPs (WP2-3-4-5), which are in charge of developing the security policies (WP2), policy enforcement (WP3), monitoring and reaction capabilities (WP4), and the security and privacy seal (WP5). This will prevent future misalignment between design and implementation activities. A continuous refinement of the design achievements have been done during the initial 9 months of the project (from M1 to M9), as long as WP2-3-4-5 were beginning and progressing.

Notwithstanding that the design of the ANASTACIA framework is considered stable, potential adjustments, derived from the implementation activities, are foreseen, especially in what regards to the interfaces between modules and components.

3 OVERVIEW OF REQUIREMENTS

In D1.2 “User-centred Initial Requirements Analysis” several use cases were defined according to the two pilot domains:

- **Mobile (Multi-access) Edge Computing [MEC]**
  - Spoofing attack on the security camera system [UC_MEC.1]
  - Man-in-the-middle attack on the MEC server Scenario [UC_MEC.2]
  - DoS / DDoS attacks using smart cameras and IoT devices [UC_MEC.3]
  - IoT-based attack in the MEC Scenario [UC_MEC.4]
- **Building Management Systems [BMS]**
  - Cyber-attack at a hospital building [UC_BMS.1]
  - Insider attack on the fire suppression system [UC_BMS.2]
  - Remote attack on the building energy microgrid [UC_BMS.3]
  - Cascade attack on a megatall building [UC_BMS.4]

In addition, three main reference high-level functionalities, which can be considered horizontal and common to any application domain, were also introduced:

- **Reference functionalities**
  - Policy management
  - Monitored system management
  - Attack management

Main functional (identifier: FR-<N>) and non-functional (identifier: NFR-<N>) requirements have been defined accordingly, after an iterative formalization process that included also the identification of “responsibilities” for each plane included in the initial concept envisioned during the inception of ANASTACIA. Both the requirements elicited in D1.2 and the initial concept depicted in Figure 3 has been used to support the architecture design process, as it is described in the following subsections.

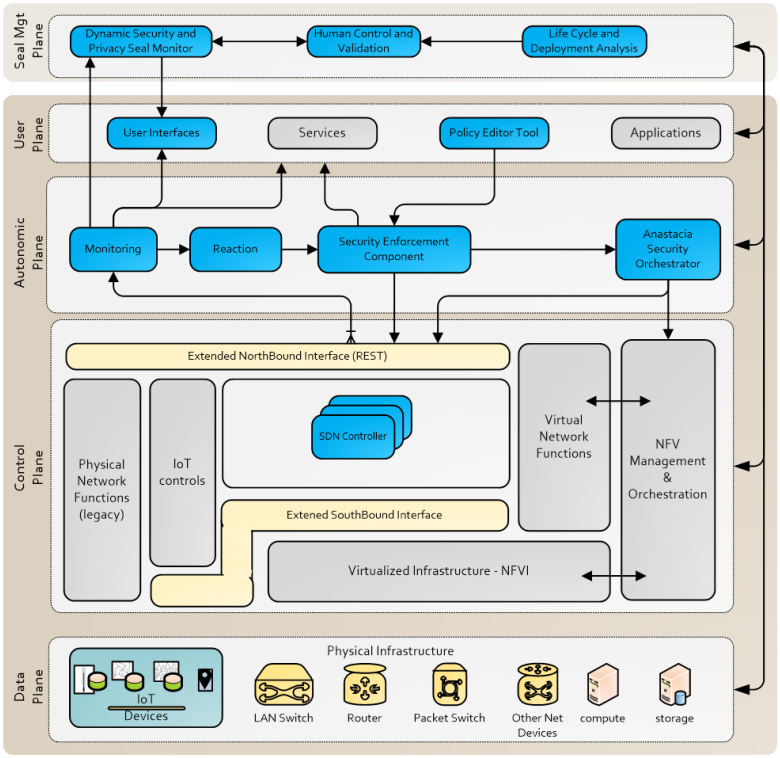


Figure 3. ANASTACIA initial concept (as included in the project proposal)

According to a dedicated analysis, privacy requirements (identifier: PR-<N>), compliant with GDPR, have been identified too, in order to support the definition of the policies that will be used to manage the Dynamic Security and Privacy Seal (DSPS) under development in WP5.

3.1 FORMALIZATION OF REQUIREMENTS

The following sections includes functional, non-functional and privacy requirements (inspired by GDPR) as reported in D1.2 for the sake of internal reference in this deliverable.

3.1.1 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 deploy new security-related VNF to better assess security constraints in real time)	**HIGH**
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 on 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**

ID	Name/Description	Priority*
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 }

3.1.2 Non-functional requirements

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 }

3.1.3 Privacy requirements

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 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.*	**HIGH**
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*	**HIGH**

ID	Name/Description	Priority*
	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.	
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 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.*	**HIGH**
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 organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudo-anonymization 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 organizational 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, unauthorized 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*	**HIGH**

ID	Name/Description	Priority*
	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".	
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** }

3.2 MAPPING OF FORMALIZED REQUIREMENTS

All requirements have been assigned a simple level of priority ({ **LOW** , **MEDIUM** , **HIGH** }) in order to ease the organization of development activities. Figure 4 visually summarizes their overall positioning, highlighting how that the majority of requirements (and, in particular, those related to privacy, as evidently supported by the nature and the scope of the project) has been actually classified as having **HIGH** priority.

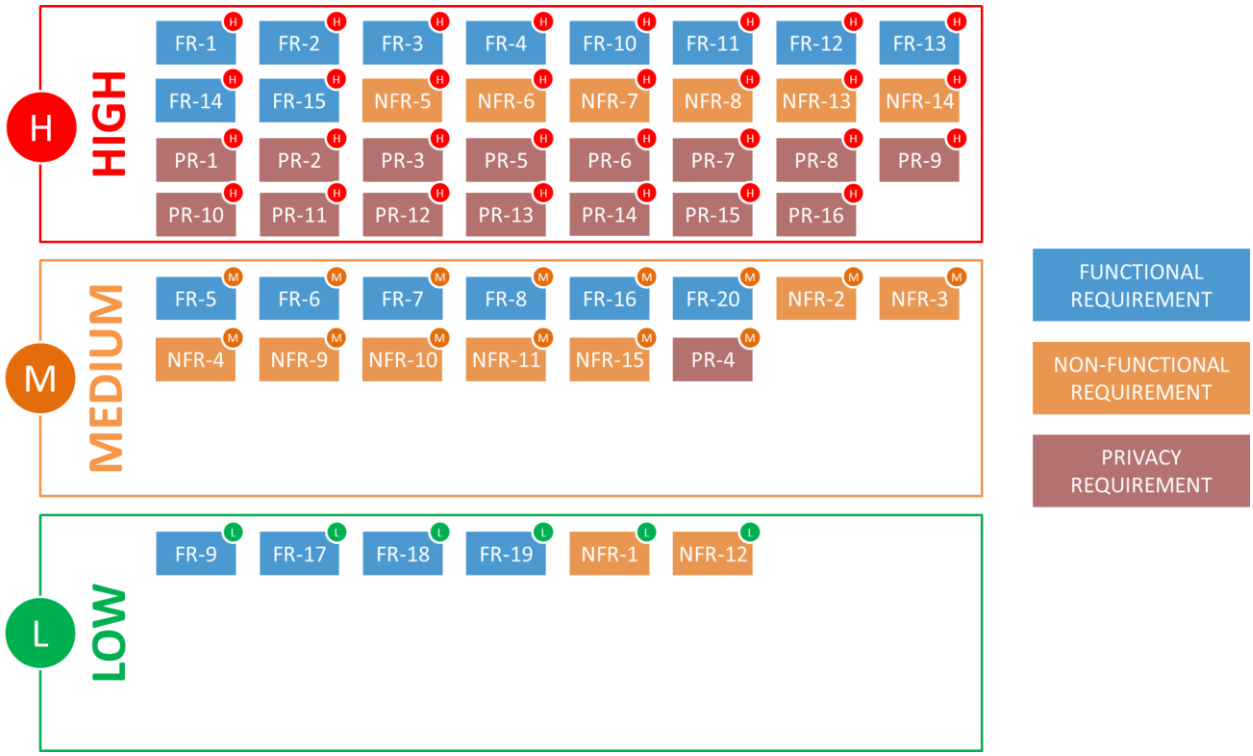


Figure 4. Overview of functional, non-functional and privacy requirements, grouped by priority.

In order to ease the architecture design phase, the following sections propose a mapping the different categories of identified requirements onto the initial architecture schema, in order to stress which plane (or, possibly, inner module/component) has to guarantee the compliancy with the expressed constraint or the provision of the expected functionality.

Mapping of functional requirements

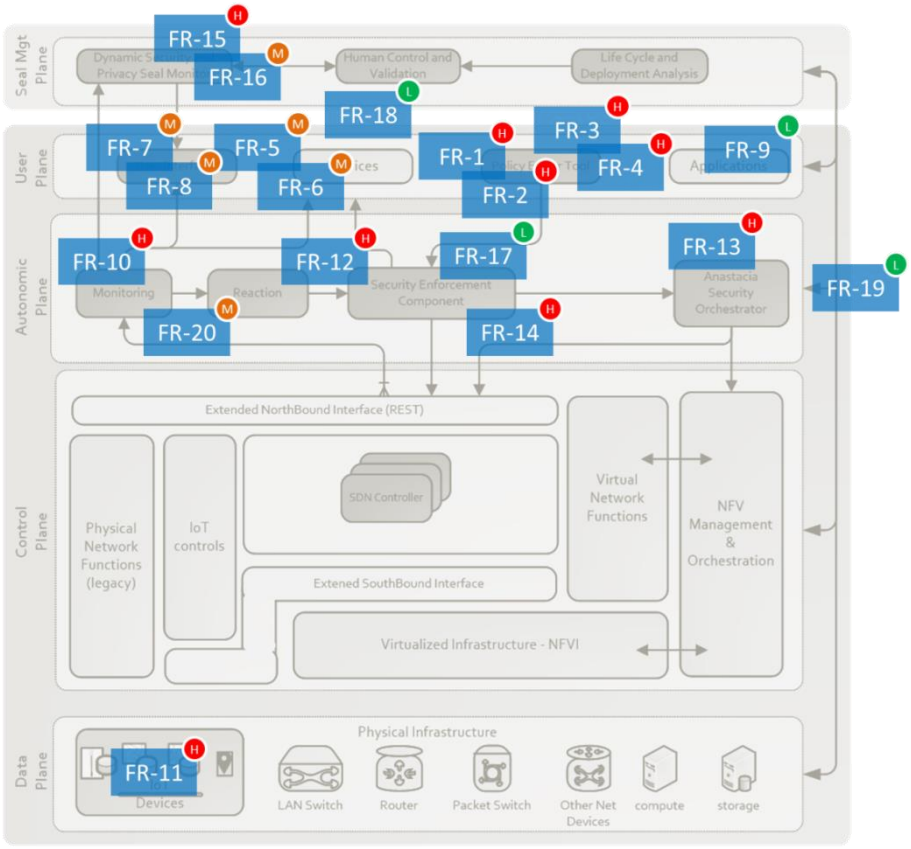


Figure 5 visually summarizes the mapping of the 20 identified functional requirements (identifier: FR-<N>) on the initial architecture schema: the majority concentrates on the upper planes – **Autonomic Plane**, **User Plane** and **Seal Management Plane**. Zooming into each single plane, a more detailed mapping onto inner modules/components can be carried out, as included in the following table:

Table 3. Functional requirements mapping into ANASTACIA

PLANE	MODULE/COMPONENT	FUNCTIONAL REQUIREMENTS PRIORITY
Seal Management Plane	DSPS Monitor	FR-15^{H}, FR-16^{H}
User Plane	Policy Editor Tool	FR-1^{H}, FR-2^{H}, FR-3^{H}, FR-4^{H}
User Plane	User Interface/Services	FR-5^{H}, FR-6^{H}, FR-7^{H}, FR-8^{H}, FR-9^{H}, FR-18^{H}, FR-19^{H}
Autonomic Plane	Monitoring	FR-10^{H}, FR-20^{H}
Autonomic Plane	Reaction	FR-12^{H}, FR-17^{H}, FR-20^{H}
Autonomic Plane	Security Orchestration	FR-13^{H}
Autonomic Plane	Security Enforcement	FR-14^{H}
Data Plane	IoT device	FR-11^{H}

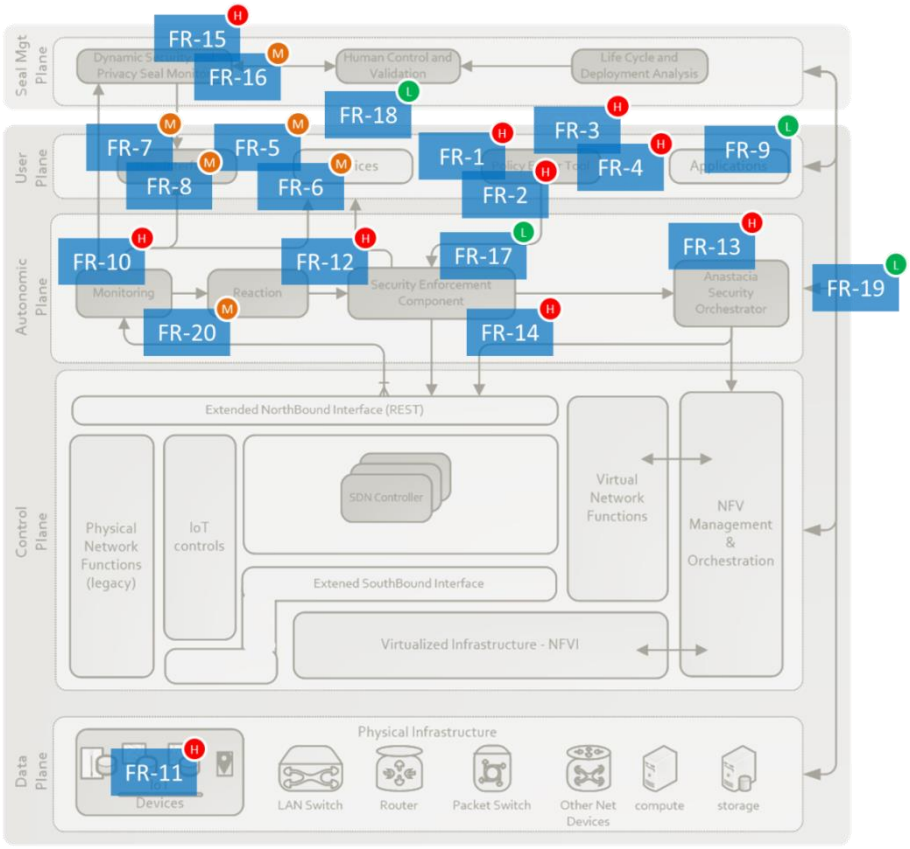


Figure 5. Mapping of functional requirements onto architectural planes.

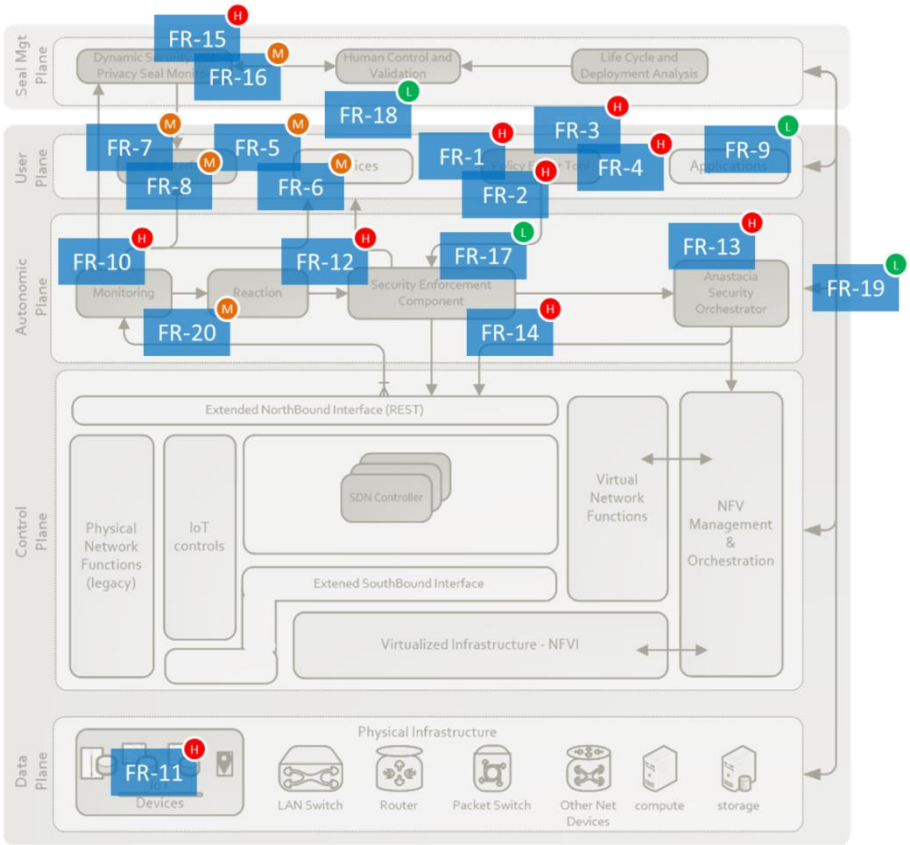


Figure 5 visually summarizes a tentative mapping of the 15 identified non-functional requirements (identifier: NFR-<N>) on the initial architecture schema: the majority concentrates again on the upper planes – **Autonomic Plane**, **User Plane** and **Seal Management Plane**. It is worth highlighting anyway that, due to the horizontal nature of these requirements, analysist and developers should check the applicability of each criterion all over the architecture to be defined. Zooming into each single plane, a detailed tentative mapping onto inner modules/components can be carried out as for functional requirements, as included in the following table:

Table 4. Non-functional requirements mapping into ANASTACIA

PLANE	MODULE/COMPONENT	NON-FUNCTIONAL REQUIREMENTS PRIORITY
Seal Management Plane	Human Control and Validation	NFR-1[H], NFR-2[H], NFR-15[H]
Seal Management Plane	DSPS Monitor	NFR-5[H]
User Plane	User Interface, Services Policy Editor Tool	NFR-1[H], NFR-2[H], NFR-3[H], NFR-7[H], NFR-9[H]
User Plane	User Interface, Services	NFR-13[H], NFR-15[H]
Autonomic Plane	Monitoring	NFR-8[H], NFR-10[H], NFR-11[H]
Autonomic Plane	Reaction	NFR-8[H], NFR-10[H], NFR-12[H]
Autonomic Plane	Security Orchestration	NFR-10[H], NFR-12[H]
Autonomic Plane	Security Enforcement	NFR-10[H]
Data Plane	IoT device	NFR-4[H], NFR-14[H]

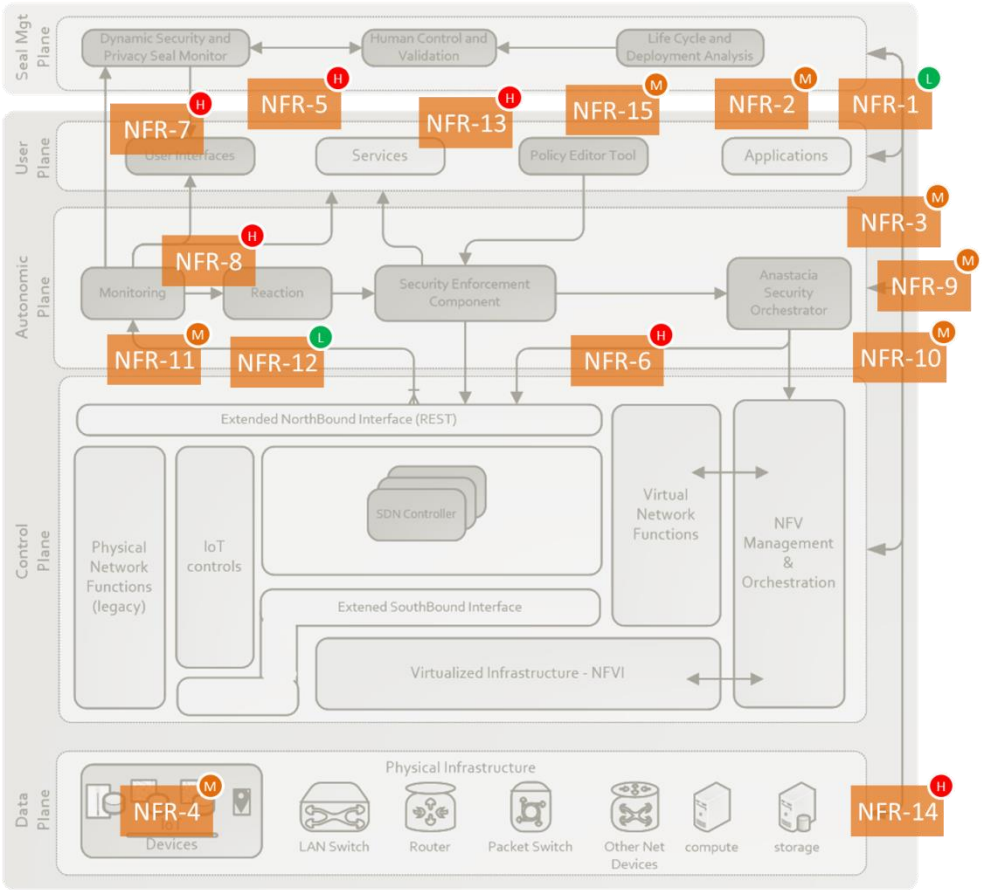


Figure 6. Tentative mapping of non-functional requirements onto architectural planes.

3.2.1 Mapping of privacy requirements

As for privacy requirements (identifier: PR-<N>), considering their general validity and overarching scope (see Figure 7), an exact mapping onto planes and inner modules/components is not particularly significant, as the compliancy to the identified constraints (mainly GDPR-derived) must be necessarily guaranteed throughout the entire ANASTACIA architecture.

In the same way as for non-functional requirements (privacy ones are not functional indeed, although they have been kept separated for a better differentiation), analysts and developers will check at any architectural level the related compliancy of envisaged modules/components in order to ensure that no "weak" links are included along the process elaboration chain (MONITORING →REACTION → ORCHESTRATION → ENFORCEMENT).

Table 5. Privacy requirements mapping into ANASTACIA

PLANE	MODULE/COMPONENT	PRIVACY REQUIREMENTS PRIORITY
ALL	ALL	PR-1^{H}, PR-2^{H}, PR-3^{H}, PR-4^{M}, PR-5^{H}, PR-6^{H}, PR-7^{H}, PR-8^{H}, PR-9^{H}, PR-10^{H}, PR-11^{H}, PR-12^{H}, PR-13^{H}, PR-14^{H}, PR-15^{H}, PR-16^{H}

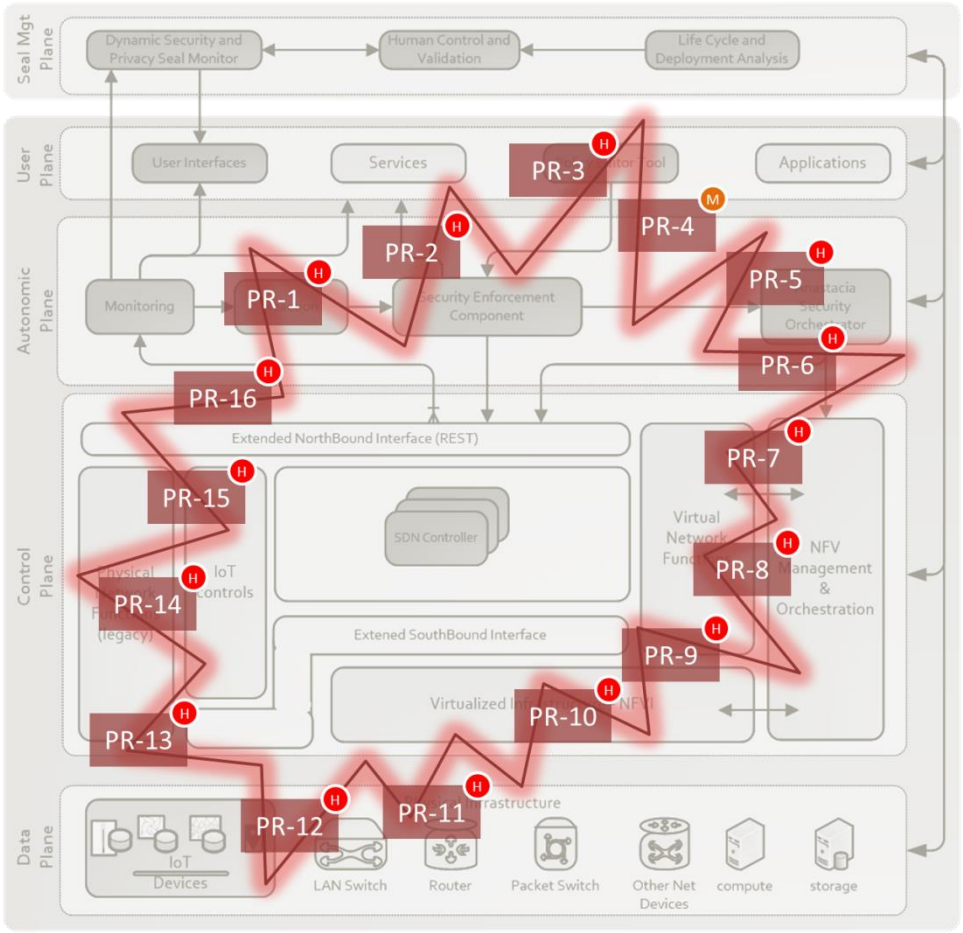


Figure 7. Mapping of privacy requirements onto architectural planes (overall validity).

4 ANASTACIA CONCEPTUAL MODEL FOR IOT/CPS SECURITY

Prior to the representation of the complete ANASTACIA architecture it is necessary to analyse the elements involved in the expected framework and the relationship between them. To this end, conceptual models are key tools to represent the abstract ideas of a system, which, at the same time, enhance the understanding of the system to represent. Furthermore, it helps to represent in a consistent way the system details, thus facilitating the agreement between the members of the consortium. As it defines the elements involved in the framework, it also helps to define the terminology used for every element and domain identified.

Therefore, this section represents the conceptual model designed to represent the ANASTACIA. The advocated conceptual model provides an abstract representation of the ANASTACIA framework. This conceptual model will be used to design the ANASTACIA global architecture, including the components involved in every process that ANASTACIA will carry out. The ANASTACIA conceptual model is partially based on the IoT Domain Model created by the EU FP7 project IoT-A [1], extending it with the specific characteristics for security protection that ANASTACIA is aiming, such as security monitoring, security policies enforcement and reaction capabilities. The inception of this conceptual model uses the results of the comprehensive analysis carried out in D1.1 and D1.2: from the former the technological analysis was used to identify the elements involved in IoT infrastructures and in the management of security for such platforms; the latter was used to evaluate the requirements elicited, in order to define the expected functionalities that support the use cases identified.

Figure 8 depicts a high representation of the main elements involved in ANASTACIA. This figure represents how a user or system admin is using applications which make use of resources offered by an IoT System. At the same time Applications deploy policies which are enforced in the IoT System and managed by a security management entity. On top of that the level of security of an IoT platform is represented by a Dynamic Security and Privacy Seal.

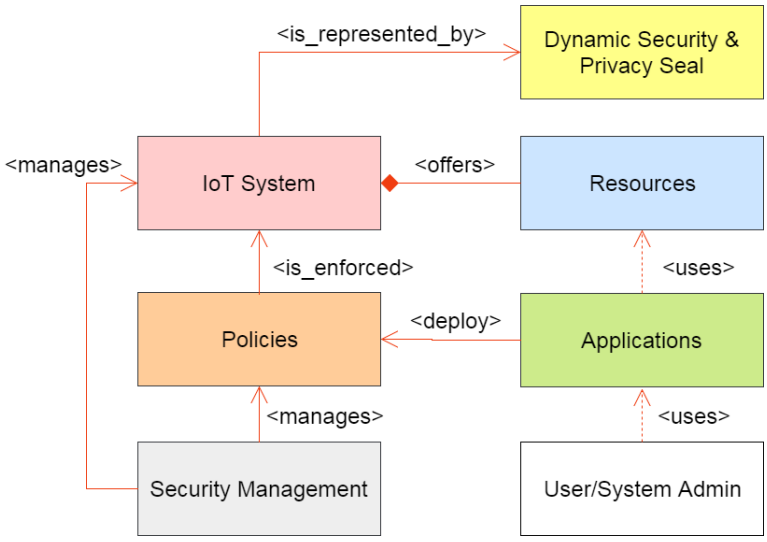


Figure 8. High level ANASTACIA conceptual model

This high level conceptual model roughly describes the main flow of ANASTACIA which articulated through the management of security policies across the IoT System. There is a direct correspondence between every element of this high level conceptual model and the WPs of ANASTACIA:

- **Policies** include the definition of the security and privacy policies that will be used within the ANASTACIA platform and enforced in the IoT System. This includes the format, language and content of the policy. WP2 is in charge of defining the details of this element as for security, WP5 as for privacy.

- **Applications** represent the interface between the ANASTACIA platform and the user and system admins, through which they can interact, configure and manage the ANASTACIA platform. WP2 is in charge of defining the details of this element.
- **IoT System** represents the set of IoT devices installed and running on an infrastructure. The IoT System is monitored in order to check the fulfilment of a security policy and configured/reconfigured to react to potential threats or attacks affecting the IoT System. WP3 is in charge of defining the orchestration and enforcement mechanisms for deploying a security policy over an IoT System. Every action is carried out respecting the defined privacy policies.
- The **Resources** element represents what devices installed and running on an IoT System are able to offer to applications. WP3 will also manage such resources (either on-devices or virtual resources) as part of the orchestration and enforcement mechanisms mentioned for the IoT System.
- The **Security Management** element covers the management of the policies within an IoT System. This includes activities such as monitoring or reaction activities. WP4 is in charge of defining such mechanisms.
- The **Dynamic Security and Privacy Seal** represents the level of security of the IoT System, which is part of WP5 activities.

A deeper analysis can be done in order to determine the concrete functionalities covered by every element of this high level conceptual model. A more exhaustive study of every element, considering the requirements and use cases resulting from D1.1 and D1.2, results in the conceptual model represented in Figure 9. Every element appearing in Figure 8 is split into several elements:

- The **IoT system** (pink elements in Figure 9). The elements herein included represent the objects involved in the actual service provisioning. In general, an IoT system is composed of several **Devices** which can be used either for retrieving static information (**Tags**), dynamic information (**Sensors**) or for performing actions (**Actuators**). For instance, an IoT platform would correspond to a smart building and all the sensors, machines, actuators, installed in such smart building are the Devices that are part of such IoT Platform.
- The **Resources** available at Devices (blue elements in Figure 9). Resources are offered by Devices and used by services built on top of the IoT Infrastructure. Types of resources can be (1) **On-device Resources** (for example, the information given by a temperature sensor) or (2) **Network Resources** (for example, cloud storage). From a technical point of view, these resources are accessible through interfaces which are offered to Applications in order to interact with Devices, either to retrieve some information, trigger some action, or to use resources available in the network.
- **Security Policies** (orange elements in Figure 9). Security Policies are defined by **User/System Admins** and enforced in the IoT System. The enforcement is performed through a set of specific **Security Configurations** that are applied in the IoT System. Additionally, a Security Policy is composed of one or more **Capabilities** which represents the basic features that can be configured to enforce a security policy (e.g., channel protection, filtering, anti-virus or parental control).. Capabilities can extend other capabilities in order to cover a wider scope within the system.
- **Applications** for managing security (green elements in Figure 9). These applications would use the **Resources** offered by devices and will allow for the definition of Security Policies through **Policy Editors**. These applications can also provide visualization capabilities about security related events, such as attacks, threats or alarms, in **Dashboards** and other **Tools**.
- **Security Management** (grey elements in Figure 9). The elements included in this category are responsible for the management of the enforcement and fulfilment of Security Policies set for an IoT System. This includes the retrieval of **Monitoring Data** from the Devices of an IoT System. This is done by **Agents** which interpret the Capabilities associated to the Monitoring Data. At the same time, a **Reasoner** combines the Monitoring Data extracted by Agents from Devices with the Capabilities included in a Security Policy. The result is a set of **Alerts** or **Threats** which can be visualized by Applications. **Reactions** can also be created which are enforced in the IoT system to

mitigate the detected Threats. These Reactions are created according to the Capabilities supported by an IoT System, which is defined through a **Security Model**.

- The **Dynamic Security and Privacy Seal** (yellow elements in Figure 9) is the element in charge of performing the evaluation of the IoT System, providing with a snapshot of the current status of an IoT system in terms of security.

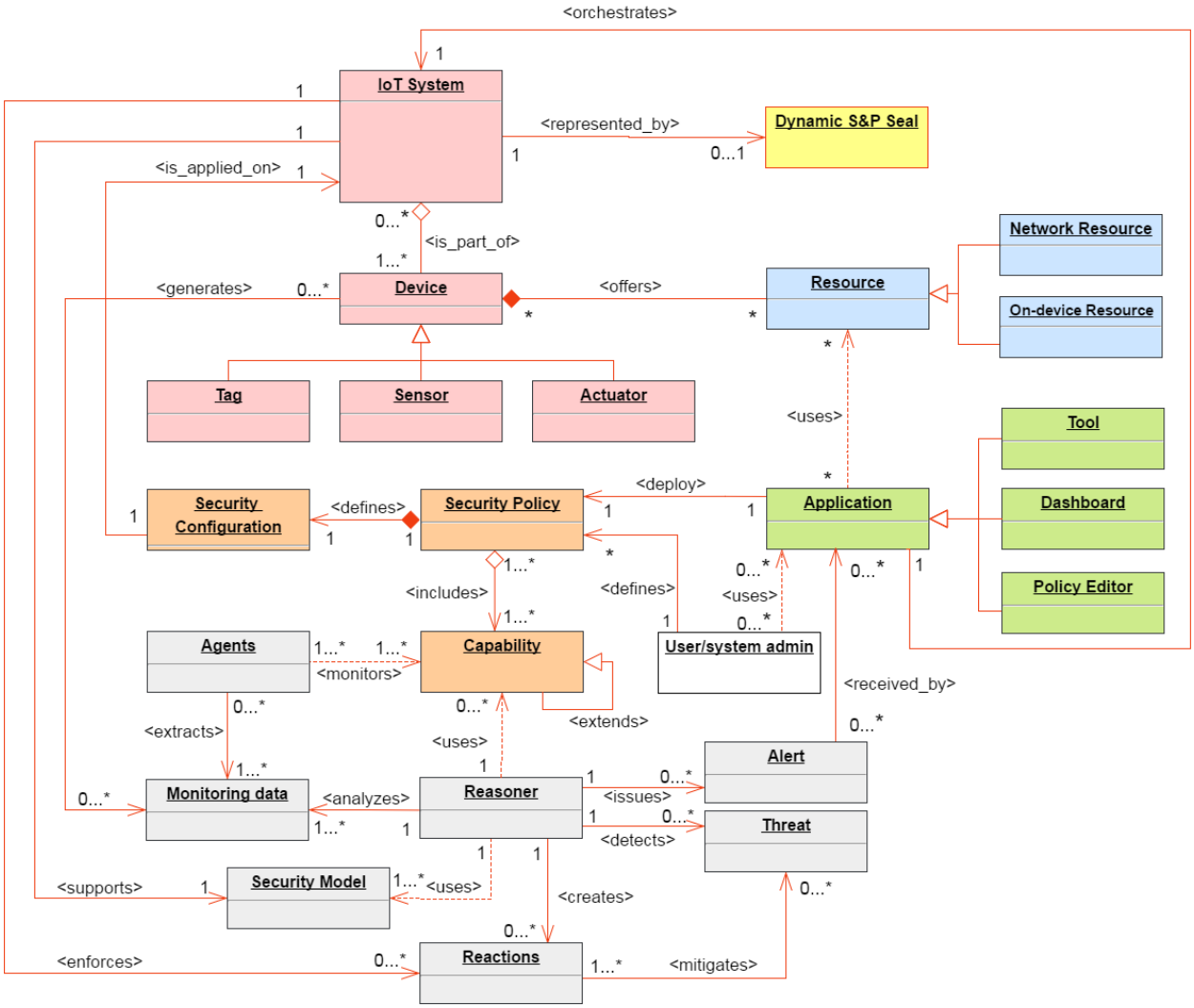


Figure 9. ANASTACIA conceptual model

The aforementioned conceptual model gives a complete overview of every concept managed within ANASTACIA. It provides a comprehensive representation of the adaptive security architecture for IoT Systems that ANASTACIA is tackling. The ANASTACIA conceptual model represents the management of monitoring data, which can be retrieved by using continuous monitoring approaches, carrying out the enforcement of security policies and being self-adjustable through the creation of reactions that prevent potential threats or react to ongoing attacks.

This conceptual model is the basis for the creation of the ANASTACIA architecture. The following section describes the process used to create the ANASTACIA architecture, which uses the elements identified in the conceptual model and the activities specified between them.

4.1 ANASTACIA SYSTEM MODEL

The ANASTACIA system model provides a representation of how the ANASTACIA framework can be integrated within a system. Figure 10 depicts the ANASTACIA system model. ANASTACIA is envisioned to

enable trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures. In general terms, an IoT Infrastructure can be seen as a system with two well differentiated planes. The Data Plane is closer to the physical domain and is composed of IoT devices, the network that interconnect them and in general, the elements providing resources, such as servers or routers. On top of the Data Plane there is the Control Plane that enables the management of the underlying devices. This include either IoT Controllers that directly control the devices resources (sometimes even integrated in the same device) or Virtual Interfaces (i.e., VNFs) that are able to control/access to the Data Plane resources through the Cloud.

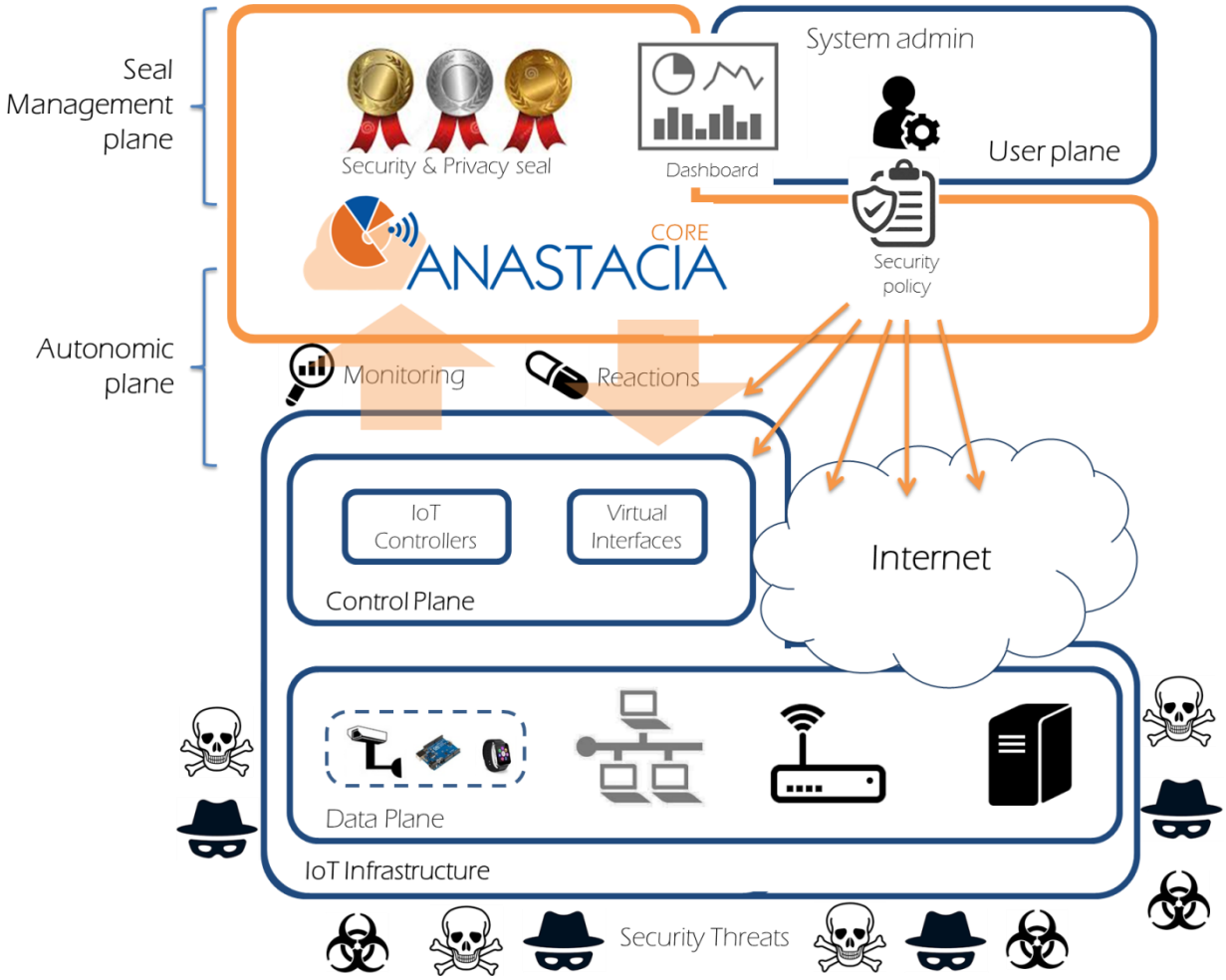


Figure 10. ANASTACIA system model

IoT platforms are currently threatened by a myriad of external dangers. New attacks targets IoT platforms taking advantage of existing vulnerabilities in Devices, poorly managed/configured security settings (i.e., default passwords) or even by using social engineering techniques that engage users to install malwares or disclose passwords.

ANASTACIA is built on top of IoT platforms to protect them against such threats. ANASTACIA is conceived as a policy based framework where system admins (at the User plane) set a specific security policy that must be fulfilled within an IoT platform. This security policy is enforced within the IoT platform by orchestrating its resources (devices, services, etc.). The control of the fulfilment of the security policy is carried out by the ANASTACIA framework at the Autonomic plane by monitoring the IoT platform and detecting threats and ongoing attacks. Additionally the ANASTACIA framework is able to create and trigger reactions that mitigate the effects of attacks, prevent against threats and guarantee the fulfilment of the security policy.

One of the most novel features of ANASTACIA is carried out at the Seal Management plane, built on top of the ANASTACIA framework. At this plane a dynamic seal is created, representing the current level of security of the IoT platform.

5 ANASTACIA GENERAL ARCHITECTURE

The ANASTACIA system model (as presented in Figure 10) is structured as a set of layers that provide a broad view of the framework and stand out its integration within IoT infrastructures. ANASTACIA is envisioned as a framework integrated on top of an IoT infrastructure where IoT devices, physical and virtual network elements interact in the **Data Plane**. On top of that, the **Control Plane** manages the computing, storage, and networking resources in the Data Plane by leveraging SDN controllers, NFV orchestration platforms, and IoT controllers.

Figure 11 represents the high level view of the ANASTACIA framework, which extends the ANASTACIA system model by expanding the functions of the ANASTACIA core. The **Autonomic Plane** includes the components that provide the ANASTACIA framework with its intelligence and dynamic behaviour. This plane can be divided into three sub-planes, which carry out specific activities within the framework:

- The **Security Orchestrator Plane** organizes the resources that support the Enforcement Plane, carrying out activities such as the transformation of security properties to configuration rules and aligning the security policies defined by the security interpreter with the provisioning of relevant security mechanisms. It has the whole vision of the underlying infrastructure and the resources and interfaces available at the Security Enforcement Plane.
- The **Security Enforcement Plane** connects the ANASTACIA core with the IoT Platform (Data and Control planes), managing the interactions among objects and components for the enforcement of the security policy defined at the User Plane. This plane supports the enforcement of configurations and reactions triggered by the Security Orchestrator Plane, in order to preserve the expected security level. At this plane, the agents that support the monitoring of IoT devices or the enforcement of reactions are instantiated, either if they are operating on remote or directly attached to the device.
- The **Monitoring and Reaction Plane** connects to the IoT Platform through the Security Enforcement Plane in order to collect security-focused information related to the system behaviour. At this plane, intelligent data-driven automated and contextual monitoring of activities at embedded devices, legacy systems and IoT devices by retrieving signals, event logs, traces, heartbeats signals, status reports or operational information. This plane also evaluates the fulfilment of the security policy by checking security models or threats signatures, detecting anomalies and creating reactions to mitigate such anomalies, in terms or reconfigurations and alerts to system administrators.

Additionally, on top of the architecture, the User Plane and the Seal Management Plane interact with the Autonomic plane:

- The **User Plane** includes interfaces, applications and tools that help system administrators to manage the IoT platform through the ANASTACIA framework. For example, at this plane system admins are able to edit the security policies that govern the underlying IoT platform.
- The **Seal Management Plane** is in charge of providing users with a real-time indicator of the overall security level.

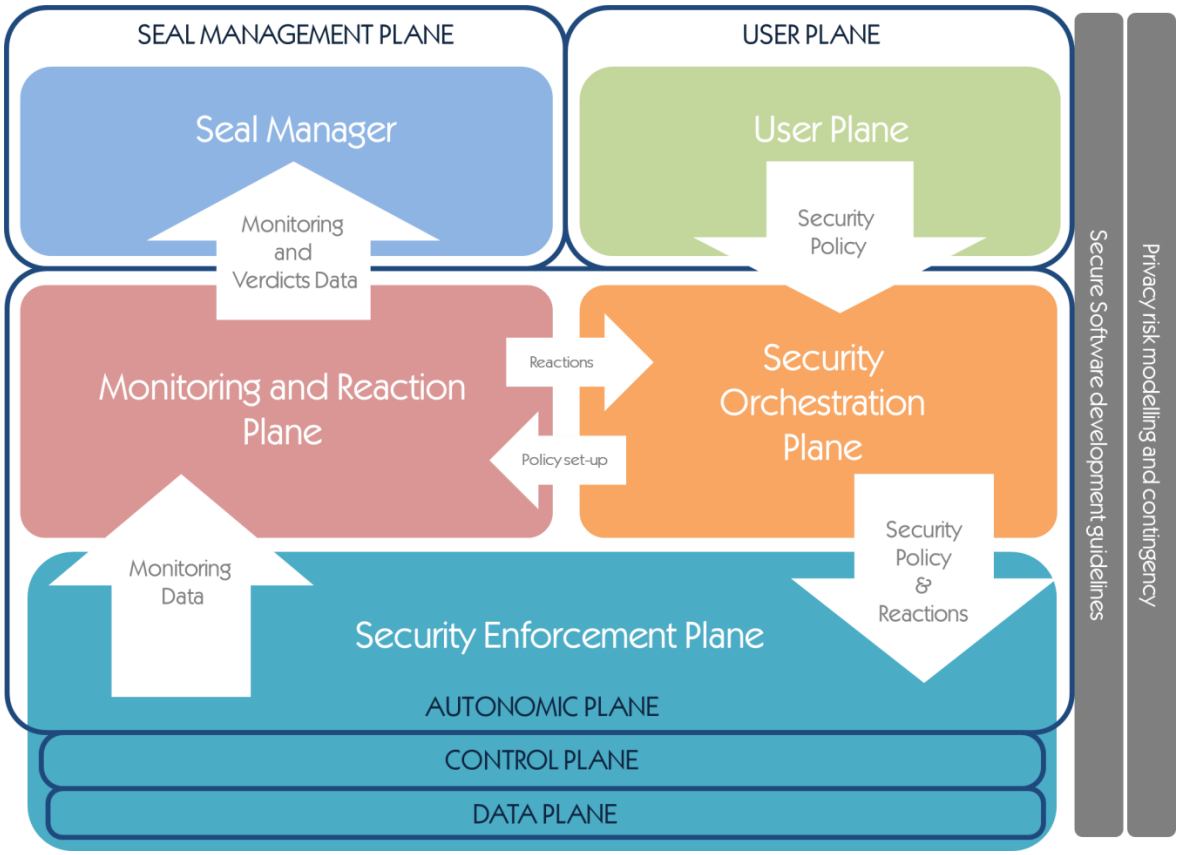


Figure 11. High level ANASTACIA framework

The next step of the methodology comprises the definition of the detailed architecture. The high level architecture can be used to identify the main activities to be carried out by the ANASTACIA framework, which is used to identify the specific components that are part of every identified plane. By analysing the use cases reported in D1.2 we can identify five main activities to be supported by the platform:

- **Security policy set-up activity**. This is the initial process triggered once a security policy has been defined by the user. In this process the policy has to be configured in the platform in order to be enforced. The interpretation of the security policy claims, the configurations required to monitor the security controls associated to a policy or the definition of thresholds to identify policy violations, are some activities carried out by this process.
- **Security policy orchestration activity**. Once the policy has been defined, it is necessary to enforce the controls specified within the policy. To orchestrate the selected IoT/SDN/NFV-based security enablers, appropriate interactions with the relevant management modules are required.
- **Security monitoring activity**. In this process the monitoring information is extracted from the devices through monitoring agents and according to the security controls interpreted from the security policy. In this activity, the monitoring data is filtered and aggregated in order to carry out its analysis and the detection of anomalies.
- **Security reaction activity**. In this process the detected anomalies are evaluated to design counter measures in order to mitigate the effects of attacks and potential threats.
- **Dynamic security and privacy seal creation activity**. In this process, relevant information about detected threats, monitored information is evaluated to create a seal that determine the level of security guaranteed/offered by an IoT platform.

Section 6 describes every process in detail, including components involved, conditions and sequence details. We can match activities to these planes and identify sub activities that determine the components.

The **Security policy set-up** activity requires the following components:

- An **Editor** at the User plane that can be used by the User/System admin to set the Security policy to be enforced in the IoT platform.
- An **Interpreter** in the Security Orchestration Plane that will transform the Security policy (closer to a human readable policy) to a machine readable policy that is able to represent lower configurations parameters.
- A **Security Enabler Provider** in the Security Orchestration Plane, that is able to identify the security enablers which can provide specific security capabilities, so to meet the security policies requirements.
- A **Security orchestrator** in the Security Orchestration Plane is responsible for selecting the security enablers to be used in the policy refinement process and configuring the Monitoring and Reaction Plane according to the security policy to enforce.

The **Security policy orchestration** activity requires the following components:

- A **Security orchestrator** that has the whole vision of the subjacent infrastructure and is able to trigger the enforcement of the defined policies using the corresponding configurations or tasks obtained during the policy refinement process.
- The elements contained in the Security Enforcement Plane, including the **IoT controllers, NVF orchestrators, SDN controllers** and, in general, all the elements enabling the configuration of the resources offered by the IoT devices and the physical/virtual network elements in the underlying infrastructure, as shown in Figure 10.

The **Security monitoring** activity requires the following components:

- A set of **Monitoring Agents** interfacing between the Monitoring and Reaction Plane and the Security Enforcement Plane. These agents are responsible for retrieving monitoring Data from the devices.
- A **Monitoring module** in the Monitoring and Reaction Plane that filter and process monitoring data received from IoT devices. To this end, this module would require several subcomponents:
    - A **Data Filtering and pre-processing**. This component will filter the raw monitoring data received from agents, carrying out an initial pre-processing of the received information in order to be correctly analysed. The filtering activity will be carried out based on the initial configuration received from the Security Orchestrator during the Security policy set-up.
    - **A Data Analysis** that will analyse the filtered monitoring data to detect potential threats or ongoing attacks. This component is supported by a set of Attack signatures that keep track of the latest attacks and their signatures in order to identify them.

The **Security reaction** activity requires the following components:

- A **Reaction module** in the Monitoring and Reaction Plane that receive the detected threats and attacks and create the countermeasures that react to them. This module would require several subcomponents:
    - A **Security Model Analysis**, which is configured during the Security Policy Set-up with the Security Models available at the IoT platform. The security models determine the set of possible actions that can be carried out at the IoT platform, and will determine the reactions that can be deployed in the IoT platform. These security models are related to the configurations created by the Policy Interpreter, as will be described Section 6.1.
    - A **Verdict and Decision Support System** that, according to the available Security Model and according to a set of pre-configured reactions, is able to determine the most suitable countermeasure to mitigate the detected attack/threat.
    - A **Mitigation Action Service** that transforms the proposed countermeasures to a format that is suitable to be implemented by the Security Orchestrator.

- A **Security Alert Service** that notifies the User/System Admin about the alerts, events or countermeasures found for a specific threat/attack. This model is compatible with the User/System admin supporting the reaction module, for example, to choose one specific countermeasure or to give permissions to apply it.

The **Dynamic security and privacy seal creation** activity takes place at the **Seal Manager** and requires information from the Monitoring and Reaction Plane. The **Seal Manager** includes the following components:

- A **Dynamic Security and Privacy Seal**, in charge of analysing the system and creating the seal that determines the current security level offered by the platform.
- A **Dynamic Security and Privacy Seal User Interface** that is used by the User/System admin to visualize the current status of the IoT platform.

Mapping these identified components to the planes of the high level architecture results in the detailed ANASTACIA architecture represented in Figure 12. The diagram shows also the relationship between components.

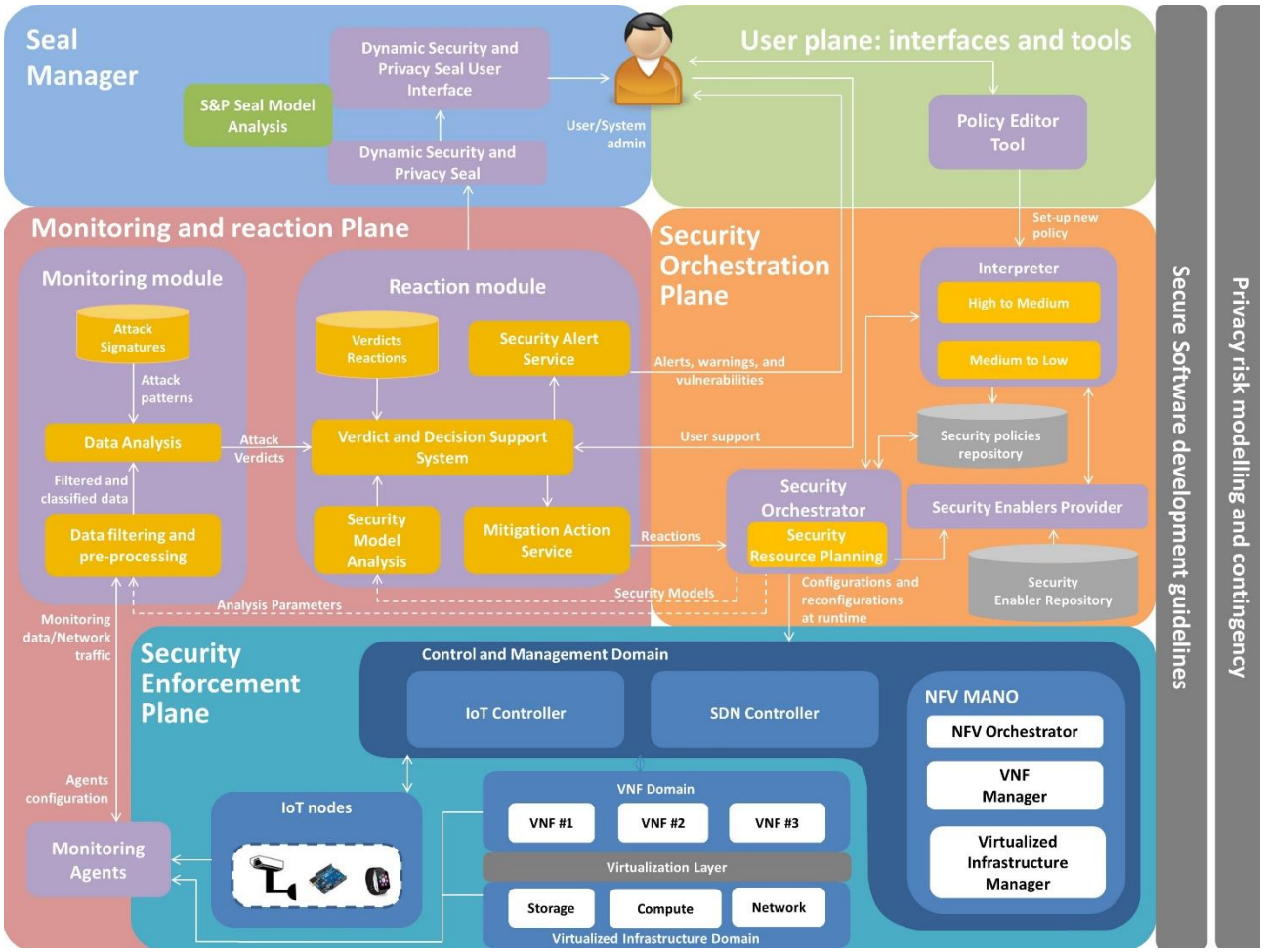


Figure 12. ANASTACIA architecture

The following sections will describe in detail the processes implemented by the ANASTACIA framework, the components of the architecture and the main interfaces identified.

6 ANASTACIA MAIN ACTIVITIES

The main activities to be carried out by the ANASTACIA framework are derived from the analysis of the use cases (as reported in D1.2) and the high level architecture described in Section 5. As already described, the main activities resulting from this analysis are: Security policy set-up, Security Policy Orchestration, Security Monitoring, Security Reaction, and Dynamic Security and Privacy Seal creation. The following subsections describe every process in detail.

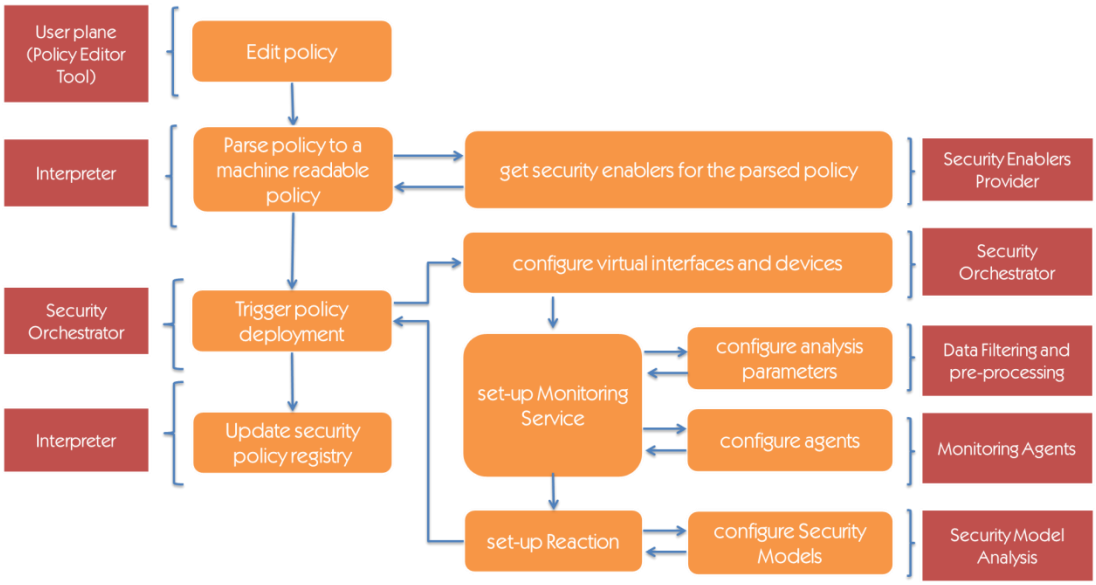
6.1 PRIVACY AND SECURITY POLICY SET-UP ACTIVITY

Every IoT platform is composed of many different types of devices, which might differ a lot in the resources available, the protocols implemented, or the connectivity technology used. The criticality of the domain where the IoT devices are working might also differ a lot. Additionally, some domains are prone to receive more attacks than others, particularly if they contain personal data, given the economic or strategic interest from attackers. As a result, different privacy and security requirements might apply to different IoT platforms. ANASTACIA is based upon a policy based strategy for the enforcement and management of privacy and security requirements over an IoT platform. Privacy and Security policies are a flexible way to tailor the privacy and security requirements needed by an IoT platform to the specific domain where the IoT platform is deployed. Policies also ease the security management activities required to control the fulfilment of the claims included in the policy, allowing to set up the monitoring activities, setting up measurements, thresholds, the creation of alerts, reaction activities, etc. Therefore, before the privacy and security policy is actually enforced, it is required to configure several components of the ANASTACIA framework in order to set-up the detection of attacks, threats and possible violations of the policy. The privacy and security policy set-up process carry out these activities as it is detailed in Table 6.

Table 6. Activity description: Security policy set-up

Security policy set-up	
Description	A security policy is defined by the User/System admin and is deployed within the ANASTACIA framework. The policy has to be interpreted by the framework in order to configure the IoT platform (devices, sensors, actuators, agents) properly and according to the security requirements defined in the policy. The monitoring and reaction systems must be configured in order to detect threats or attacks that compromise any of the claims specified in the policy.
Precondition	The IoT system must be deployed and working The interfaces that interconnect to the IoT platform (VNC, SDN, IoT controllers) must available.
Postcondition	*Not applicable*

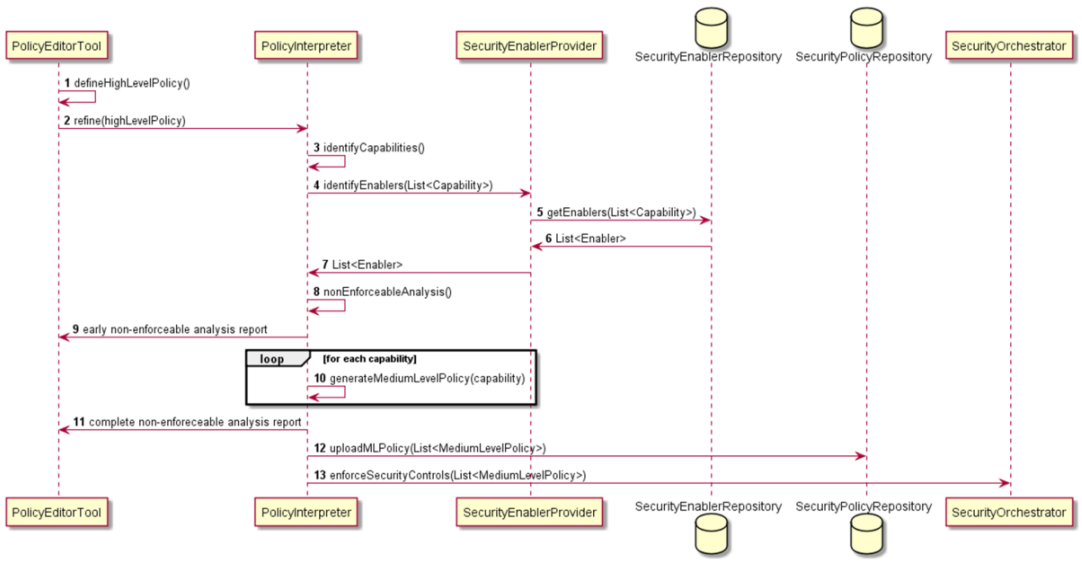
Activity Flow



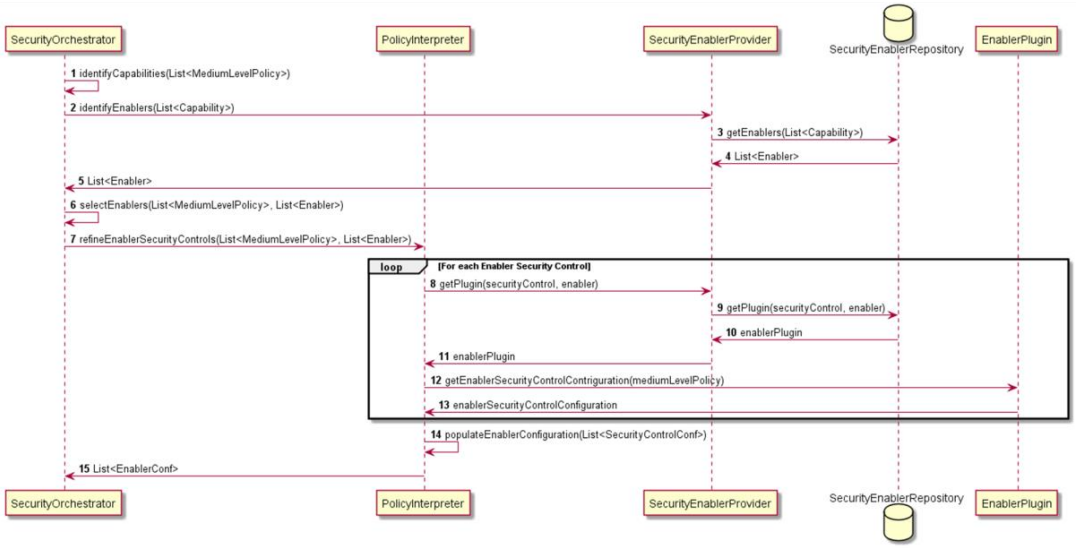
Sequence Diagram

The complete flow is divided into three sequence diagrams: The process that parses the high level policy into a machine readable format, the transformation of the content of the policy into low level configuration rules and the process for configuring the monitoring and reaction subsystems. The interpretation of the security policy to a machine readable policy follows a gradual process, where the policy is firstly transformed into a Medium Security Policy Language (MSPL) and then transformed into a low level configuration. The following diagrams depict these processes.

Policy Refinement High to Medium Security Policy Language

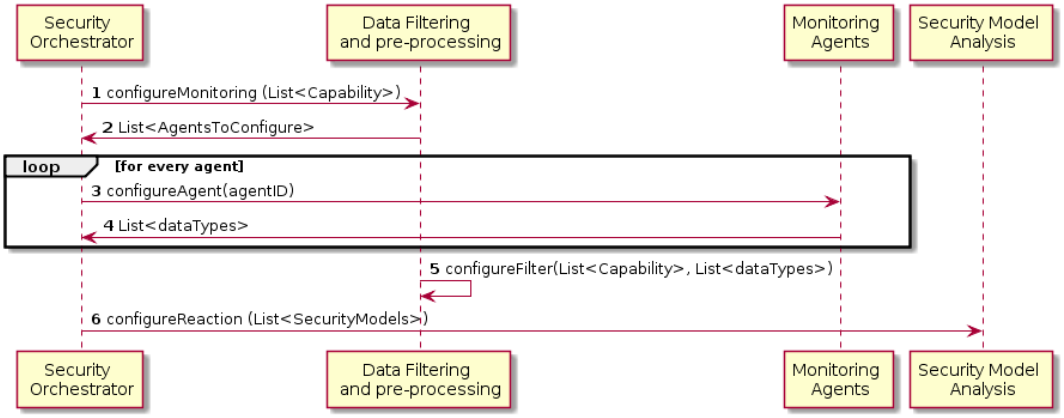


Policy Refinement MSPL to Low Level Configuration



The second process takes care to perform the refinement among MSPL policies and Enablers/VNFs configurations or tasks. In this case, when the Security Orchestrator receives the MSPL policies to apply, first identifies the available Enablers/VNFs and after performs a specific selection of them which will cover the policy enforcement, then request to the Policy Interpreter for a refinement process of a MSPL policy into a specific Enabler/VNF configuration or task (security control). The Policy Interpreter then obtains a specific plugin in charge to translate MSPL policies to specific low-level configuration/tasks for the specific Enabler/VNF and invoke it. When are obtained all configurations/tasks capable to enforce the policy, them are populated and returned to the Security Orchestrator.

Monitoring and Reaction configuration



The third process is in charge of carrying out the preparation of the Monitoring and Reaction components based on the obtained configurations/task in the previous process. In this sense, the Security Orchestrator requests configuration actions to the involved modules in order to maintain the framework updated according to the applied policies.

6.2 PRIVACY AND SECURITY POLICY ORCHESTRATION ACTIVITY

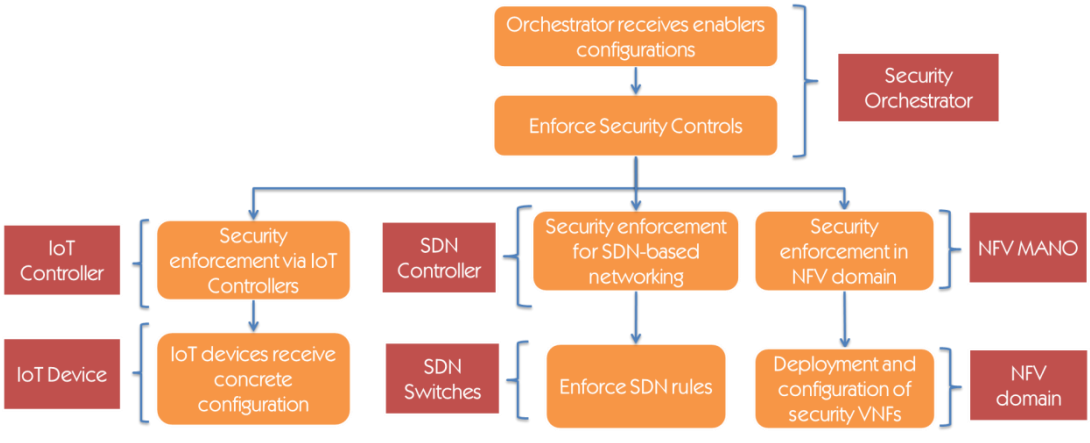
Once the ANASTACIA platform has been properly configured for policy, it is necessary to enforce the required security controls in the devices running in the IoT platform and in the network infrastructure.

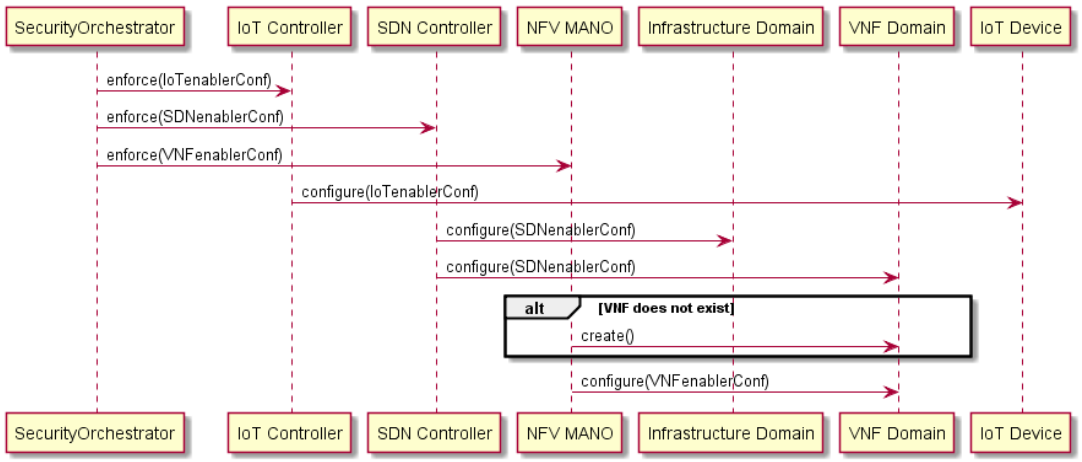
After the Security Orchestrator has received the Security Enablers' configurations, it must start an orchestration process accounting for the whole vision of the subjacent infrastructure. To this aim, the Security Orchestrator is in charge of efficiently managing the enforcement over different environments, such as IoT, NFV, SDN, by interacting with relevant control and management modules. In case of SDN, the Northbound APIs of the SDN controller can be exploited to require the enforcement of relevant flow rules. The SDN controller will interacts with physical/virtual SDN switches to instil the required traffic flow rules.

To deploy and configure security VNFs, the ANASTACIA orchestration can refer to the Management and Orchestration (MANO) components and data models specified by the ETSI ISG NFV architecture. In that sense, the NFV MANO components are in charge of creating the required security VNF, applying the specified configuration. The deployment of VNFs can also require appropriate modification in the traffic flows, so that the packet can be processed according to the security requirements. In this vein, the SDN Controller can also provide support, receiving the specific configuration about changes on a flow and enforcing the corresponding flow modifications over physical/virtual SDN switches.

To manage security controls of IoT devices, the Security Orchestrator relies on specific IoT controllers, which communicate with the IoT devices via different IoT management protocols, such as Constrained Application Protocol (COAP), Lightweight Machine to machine (LWM2M), RESTCONF.

Table 7. Activity description: Security Policy Orchestration

Security Policy Orchestration	
Description	This process orchestrates the different security enablers by interacting with relevant control and management modules, in order to enforce the security policy set-up requested by the User/System admin.
Precondition	A privacy and security policy has been setup in the system.
Postcondition	The security enablers are appropriately configured, as specified by the security policies.
Activity Flow	

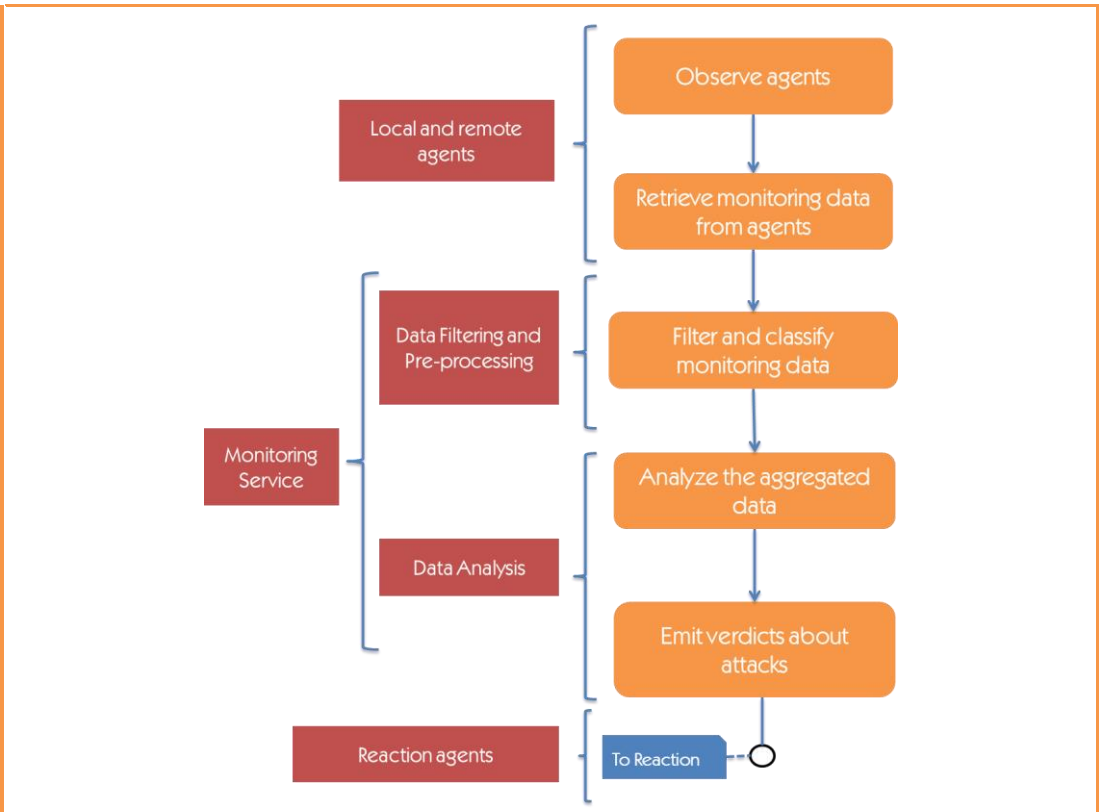
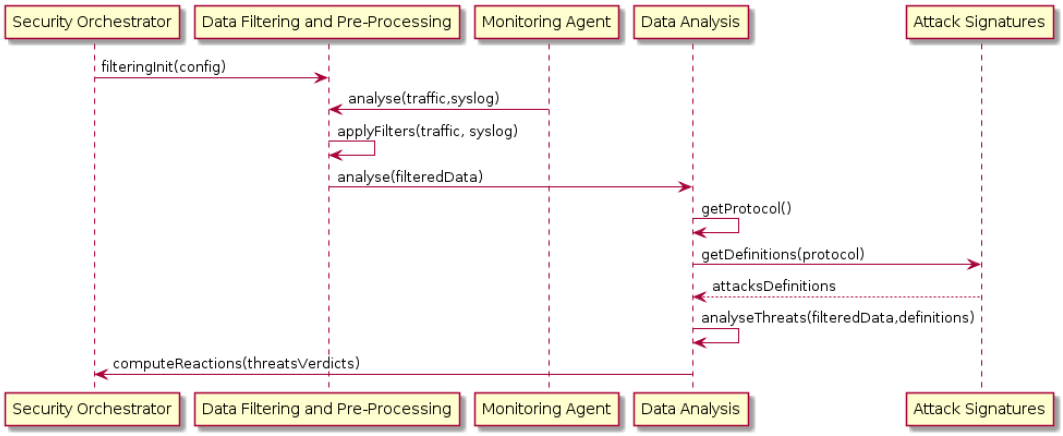
Sequence Diagram	

6.3 PRIVACY AND SECURITY MONITORING ACTIVITY

As mentioned above, the privacy and security policy is processed from a high level description to a machine readable low level format. This low level format contains a set of (security) capabilities that can be transformed into a set of configurations required by the IoT platform, which are used to enforce the security policy. These capabilities can also be used to define the specific parameters that need to be monitored, which will also determine the monitoring data, required to detect potential violations of the privacy and security policy. The monitoring data is retrieved from Monitoring Agents which capture the data traffic searching for security flaws and attacks.

Table 8. Activity description: Security Monitoring

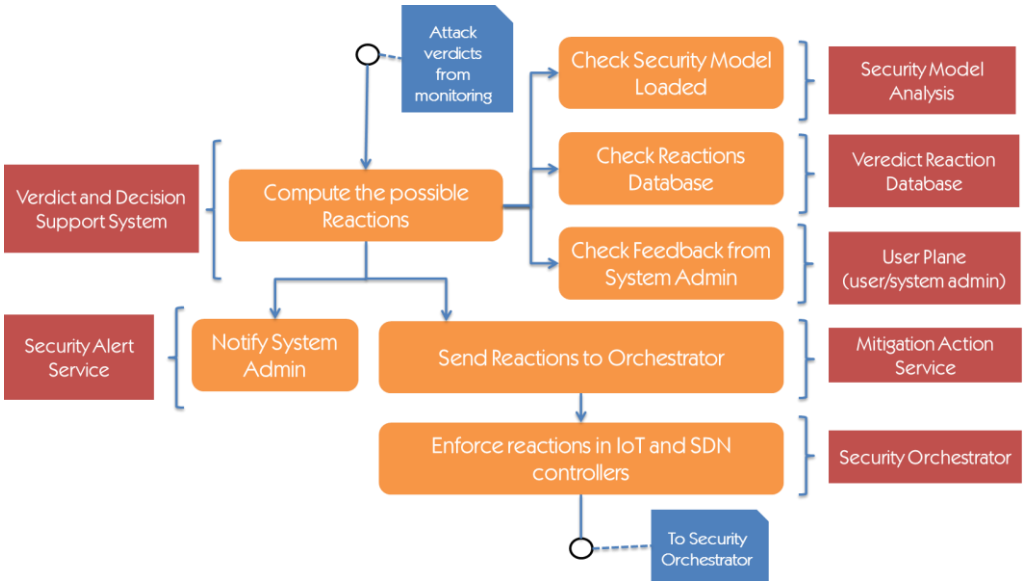
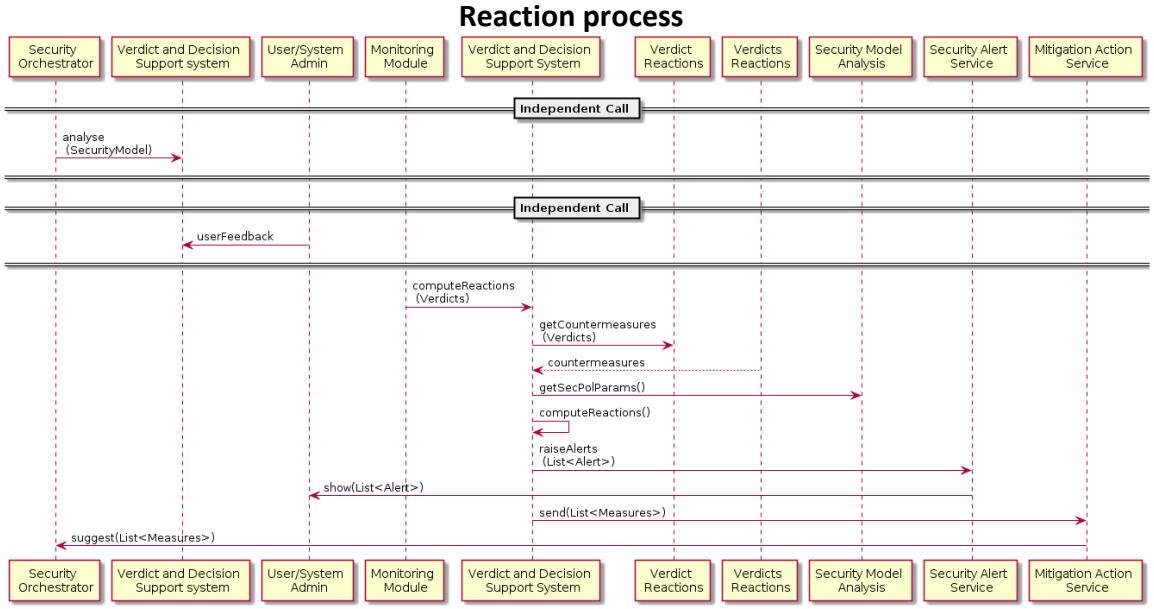
Security Monitoring	
Description	This process retrieves data from IoT devices through Monitoring Agents, which is filtered, processed and analysed, issuing verdicts about anomalies occurring in the monitored platform (potential threats or ongoing attacks). The identified events are notified to the reaction module.
Precondition	A privacy and security policy has been setup in the system Monitoring agents has been set-up for the enforced security policy The Monitoring Module has been set-up for the enforced security policy
Postcondition	Not applicable

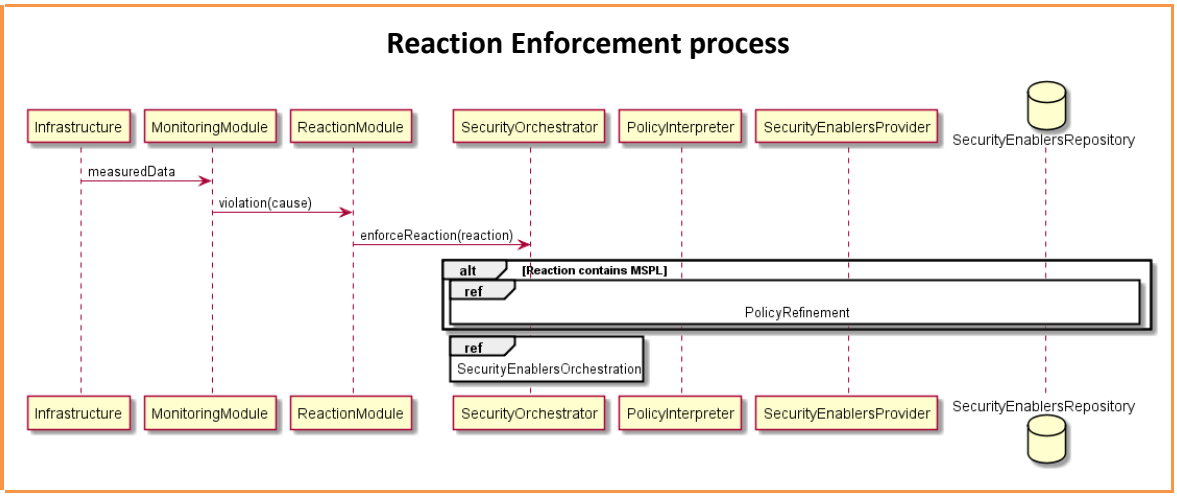
Activity Flow	
Sequence Diagram	

6.4 SECURITY REACTION ACTIVITY

The ANASTACIA platform is designed to automatically react to threats or attacks, including those that may have an impact on personal data, providing automatic protection capabilities that prevent or react to the violation of a privacy and security policy. To this end, the platform is able to execute the most appropriate countermeasure(s) to react against detected security issues. The Reaction module is the core of the mitigation capability supported by the ANASTACIA framework, and is responsible for the Privacy and Security Reaction process described in this section. Additionally, the security reaction process is also able to notify to User/System admins who might provide feedback, trigger critical countermeasures that require explicit consent or even to override the security policy when required.

Table 9. Activity description: Security Reaction

Security Reaction	
Des-cription	The security reaction process uses the policy violations detected by the monitoring module to create countermeasures that react to threats or attacks, triggering the enforcement of the countermeasures and notifying system admins.
Pre-condition	A security policy has been setup in the system A set of anomalies has been detected by the monitoring modules and notified to the reaction module
Post-condition	The countermeasures proposed must be enforceable by the IoT platform.
Activity Flow	
Sequence Diagram	Two sequence diagrams describe this process: the process for evaluation of verdicts received from the Monitoring Module to create reactions, and the process of enforcing the created reactions 

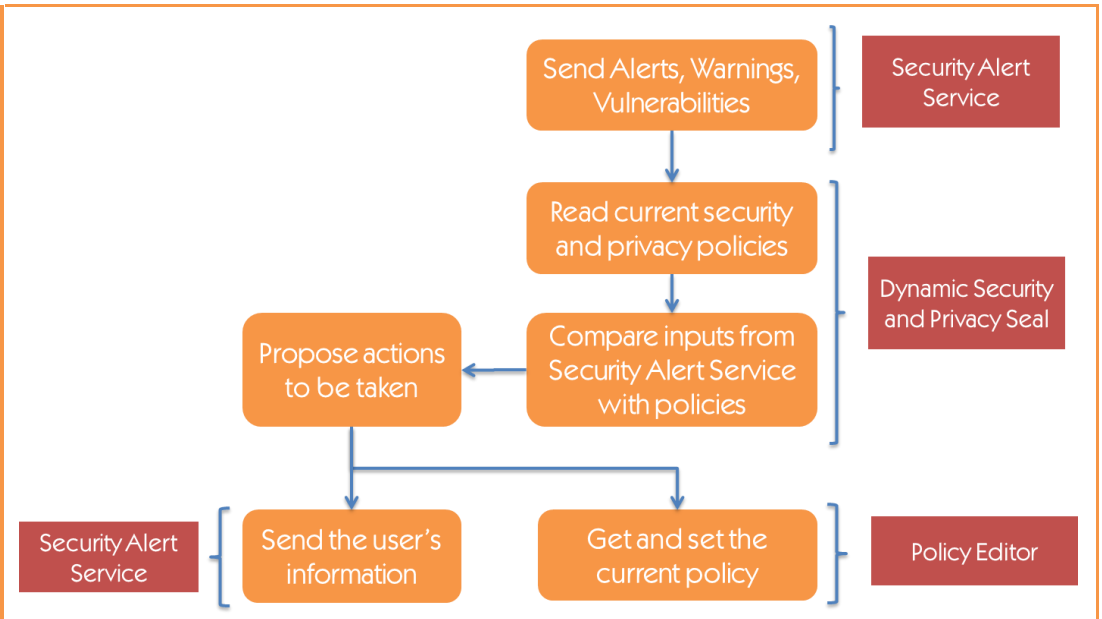
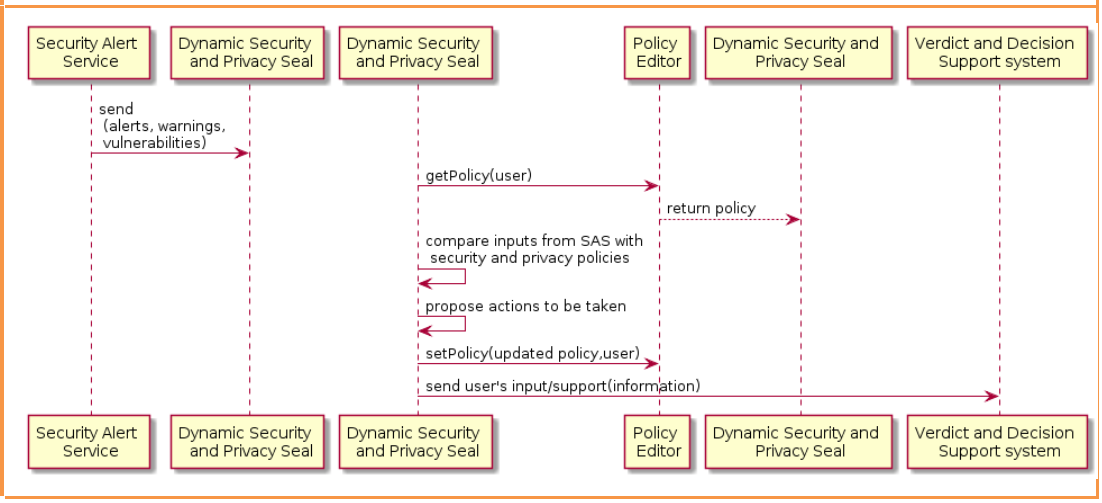


6.5 Dynamic Security and Privacy Seal Creation Activity

The Dynamic Security and Privacy Seal is set to become a graphical, real-time representation of the overall status of the system. The dynamic seal will reflect not only the instantaneous state, but will also consider the history and reliability over time of the system, in line with the most relevant ISO standards, and accounting for legal obligations, the system will describe the quality of the security and privacy risks to then present them to the end-user. To this end, the system will interact with the Security Monitoring and Reaction layers in order to retrieve information on attacks and countermeasures and verify if the seal has been broken. It will so enable administrators and data controllers to introduce policies to address any risks or system's failures.

Table 10. Activity description: Dynamic Security and Privacy Seal Creation

Dynamic Security and Privacy Seal Creation	
Description	Using security and privacy standards, the Dynamic Security and Privacy Seal monitors in real time the security and privacy and provides a graphical representation of the system status to the end-user.
Precondition	Four conditions must be met: • Anastacia platform is connected to an IoT System to be analysed in real time. • A security policy has been setup in the system • A privacy policy has been setup in the system The end-user is connected to the Anastacia platform through the graphical user interface.
Postcondition	The Anastacia platform should react to the user inputs and take action in response to the defined security and privacy policies

Activity Flow	
Sequence Diagram	

7 COMPONENTS DETAILS

This section details every component included in the ANASTACIA general architecture described in Section 5. The description of every component follows a structured approach which merges both the architecture designed and the ANASTACIA main activities described in Section 6. The description of every component relies on the following fields:

- **Function**: Describe the purpose and main role of the component within the ANASTACIA architecture
- **Subcomponent**: List the components (if applicable) that are running inside the described component.
- **Sources**: List the components that provide data or any other input to the described component.
- **Consumer**: List the components that feed from the activities or data produced by the described component.
- **ANASTACIA activities involved**: List the ANASTACIA activities (as one of the described in Section 6) where the described components participate.
- **Available assets**: Describe the available assets (tools, methodologies, techniques, etc.) that are foreseen to be used for the development of the described component.

The following subsections describe the components grouped by their respective planes: User, Security Orchestration, Monitoring and Reaction, Seal Manager Plane. Notice that elements included in the Enforcement plane (comprising mainly devices and interfaces) are not described at this stage of the project.

7.1.1 User plane

The User plane contains the policy editor tool which allows User/System admins to define the security policies to be enforced by the ANASTACIA platform. Table 11 describes this component.

Table 11. Policy Editor Tool description

Policy Editor Tool	
Function	The Policy Editor tool provides to the user the capability to generate High Security Policies Language (HSPL) policies using a friendly GUI.
Subcomponent	(Not applicable)
Sources	Security Policy Repository
Consumers	Policy Interpreter
ANASTACIA activities involved	Security Policy Set-up
Available assets	The Policy Editor Tool could be implemented using a WEB frontend, employing WEB framework technologies or even a desktop application. It could be possible to reuse some functionality from SECURED-FP7 project for the WEB part.

7.1.2 Security orchestration plane

The security orchestration plane contains the components in charge of interpreting the security policies set-up from the user plane (Interpreter, Table 12, Security Enabler Provider, Table 13), as well as carrying out the enforcement of security policies, execution of reactions and triggering monitoring and reaction configuration (Security Orchestrator, Table 14).

Table 12. Interpreter description

Interpreter	
Function	The Policy Interpreter is in charge of performing the refinement processes from High level Security Policy (HSPL) to Medium level Security Policy (MSPL) and from MSPL to Enablers/VNFs configuration or tasks.
Subcomponent	High to Medium Service (HSPL to MSPL) Medium to Lower Service (MSPL to specific configurations/tasks)
Sources	Policy Editor Tool Orchestrator Security Enabler Provider
Consumers	Orchestrator
ANASTACIA activities involved	Security Policy Set-up Security Orchestration
Available assets	SECURED FP7 Security Policy Module [4]

The Security Enabler Provider is able to identify the list of security enablers which can provide specific security capabilities to meet the security policies requirements. Besides, it also provides the security properties given by the interpreter into enabler plugins.

Table 13. Security Enabler Provider description

Security Enablers Provider	
Function	It undertakes the task of mapping source-code metadata security properties (provided as output by the Security Policy Interpreter) into appropriate configurations to enforce these security properties. Thus, this component will be endowed with an interface for delivering security M2Lplugins (Medium2Lower), which, in turn, will allow translating policies from MSPL to Low-level configurations. Moreover, the Security Enablers Provider provides the list of the available enablers accounting for specific security capabilities, to meet the security policies requirements.
Subcomponent	(Not applicable)
Sources	Security Policy Interpreter
Consumers	Security orchestrator

ANASTACIA activities involved	Security Policy Set-up Security Orchestration
Available assets	Beta implementations of some few Security M2Lplugins (Medium2Lower), that allows translating from policies specified in MSPL to low level configuration, are already available in the EU SECURED project [https://github.com/SECURED-FP7/secured-spm]. Including for instance M2L-IpTables plugin to generate iptables using as baseline a filtering policy specified in MSPL.

In general terms, the security orchestrator coordinates all the activities carried out by the ANASTACIA framework, being involved in the configuration of a new security policy, in the configuration of monitoring and reaction activities, in the execution of counter measures and of course in the enforcement of security policies. A specific subcomponent, the Security Resource Planning, is in charge of efficiently selecting the security enablers to meet the required security policies and defining strategies for their provisioning.

Table 14. Security Orchestrator description

Security Orchestrator	
Function	The ANASTACIA Security Orchestrator is in charge of orchestrating the security enablers according to the defined security policies. To this aim, it is involved in the selection of the security enablers accounting for their security capabilities, the available resources in the underlying infrastructure, and the policies requirements. Once received the configuration of the security enablers by the Policy Interpreter, the Security Orchestrator interacts with relevant SDN/NFV/IoT control and management components, so to enforce the required features in the IoT devices and in the physical/virtual network elements of the underlying infrastructure.
Subcomponent	Security Resource Planning: This submodule is in charge of efficiently selecting the available security enablers to meet the required MSPL security policies. This submodule will define and develop appropriate strategies to enforce security by exploring the SDN, NFV, and IoT technologies, accounting for the available resources in the underlying infrastructure and the policies requirements. In this vein, it provides functions like optimal path selection, load balancing, traffic rerouting, etc.
Sources	Interpreter, Security Enablers Provider, Reaction
Consumers	Security Enforcement Plane (Control and Management Domain components), Interpreter, Monitoring Module, Reaction Module
ANASTACIA activities involved	Security Policy Set-up Security Orchestration Security Monitoring Security Reaction
Available assets	To orchestrate the configuration of the security enablers over the Security Enforcement Plane, the Security Orchestrator can leverage standardized interfaces, protocols, and available open source software libraries to interact with relevant management components: SDN controllers, such as ONOS (http://onosproject.org/) or OpenDayLight

	(https://www.opendaylight.org/); and NFV MANO modules, e.g., OpenBaton (https://openbaton.github.io/) or OSM (https://osm.etsi.org/).

7.1.3 Monitoring and reaction plane

The monitoring and reaction plane carry out the incident detection activities, using the security policy to detect potential violations and envisioning possible countermeasures to prevent or react to such violations. Given the importance of these activities, this plane has been divided into two big modules: the Monitoring module and the Reaction module.

7.1.3.1 Monitoring module

The monitoring module contains the components directly involved in retrieving monitoring data from the IoT platform, and its analysis to detect incidents compromising the validity of the security policy. Table 15 provides with a description of the Monitoring module while Table 16, Table 17,

Table 18 and Table 19 describes the components running inside the Monitoring module.

Table 15. Monitoring Module description

Monitoring Module	
Function	Retrieve monitoring data from the IoT platform, filtering and processing it to detect potential threats or attacks that might entail the violation of the security policy.
Subcomponent	Data Analysis Data Filtering and pre-processing Attack Signatures Database
Sources	Monitoring Agents Security Orchestrator (Security Orchestrator Plane)
Consumers	Verdict and Decision Support System (Reaction Module) Dynamic Security and Privacy Seal (Seal Manager)
ANASTACIA activities involved	Security Policy Set-up Security Monitoring Dynamic Security and Privacy Seal creation
Available assets	Check individual monitoring subcomponents description for details.

The subcomponents that are part of the Monitoring module have a very specific role within the monitoring activities carried out in ANASTACIA. Monitoring data is retrieved from Monitoring Agents (Table 16), which is filtered and pre-processed to be transformed into a suitable format (Table 17). Filtered data is analysed (Table 19) in order to detect incidents. Such incidents are identified by using information from previous attack or attack patterns previously detected (

Table 18).

Table 16. Monitoring Agents description

Monitoring Agents	
Function	Retrieve monitoring raw data from IoT devices.
Subcomponent	(Not applicable)
Sources	IoT Nodes (Security Enforcement Plane) VNF (Security Enforcement Plane)
Consumers	Data filtering and pre-processing (Monitoring Module)
ANASTACIA activities involved	Security Monitoring
Available assets	At the time of writing this document, two types of monitoring agents are considered: • MMT Probes: These are the network sniffers that extract the information and feed them to the MMT Security engine. It is possible to embed this software in small devices (like a Raspberry PI, for example) or simply run it as another application in a dedicated machine. SIEM Agents: Depending on the data to be analysed and processed, ATOS XL-SIEM tool supports a wide range of agents. These agents analyse syslogs and generate events that will be correlated in the core of the tool.

Table 17. Data Filtering and Pre-processing description

Data Filtering and Pre-processing	
Function	Retrieve monitoring data from the IoT platform, filtering and processing in order to provide it ready for the data analysis component.
Subcomponent	(Not applicable)
Sources	Monitoring Agents
Consumers	Data Analysis
ANASTACIA activities involved	Security Monitoring
Available assets	Component has been designed and will be implemented using leading-edge opens source solutions like Apache Kafka, Apache Storm, MongoDB, in order to filter the monitoring input and provide streams of enriched data to the data analysis component.

Table 18. Attack Signatures Database description

Attack Signatures Database	
Function	This Database is conceived as a repository, containing the specifications of the security issues and attacks that will be detected in the platform.
Subcomponent	(Not applicable)
Sources	(Not applicable)
Consumers	Data Analysis Component in the Monitoring Module
ANASTACIA activities involved	Security Policy Set-up Security Monitoring
Available assets	Montimage Security Properties: Montimage has already defined the condition for detecting security issues and attacks. These properties will be adapted to the particular use cases of ANASTACIA or new ones will be created to cover the missing threats.

Table 19. Data Analysis description

Data Analysis	
Function	Analyse the data extracted, filtered and pre-processed, looking for security issues and attacks. This analysis will generate the respective verdicts of the tested properties.
Subcomponent	(Not applicable)
Sources	Data Pre-processing and Filtering Attacks Signatures Database
Consumers	Reaction Module
ANASTACIA activities involved	Security Policy Set-up Security Monitoring Security Reaction Dynamic Security and Privacy Seal creation
Available assets	Montimage Monitoring Tool (MMT): this monitoring tool uses MMT Security, a DPI-based security library that evaluates security properties. This library will also be integrated into the ANASTACIA platform as a part of the analysis component. Atos XL SIEM: the reasoner component of this tool (based on Esper and Apache Storm) will be used as part of the core logic of the Data Analysis Component

7.1.3.2 Reaction module

Reaction module is the core of the mitigation capability supported by the ANASTACIA framework, and is responsible for the Security Reaction. Table 20 describes the Reaction module. Its subcomponents are described in Table 21, Table 22, Table 23, Table 24 and Table 25.

Table 20. Reaction Module description

Reaction Module	
Function	In this module the detected anomalies are evaluated to design counter measures in order to mitigate the effects of attacks and potential threats. The Security Model Analysis Hierarchical network model is used to produce hierarchical scale-free network topology, where the network model is updated based on the mitigation action used. Each node is associated with security features to identify the possible security mitigation action that can be applied. Thenceforth, the Data analysis and virtual sensing mechanisms (done by the Verdict and Decision Support System) are used for system-level reaction, where virtual device behaviour is used to compensate the abnormal device behaviour. So, the reactions prepared by the mitigation action service based on verdict and decision support system information are sent to the security orchestrator. Finally, the security Alert services alerts the user/ system admin fetched from verdict and decision support system.
Subcomponent	• A Security Model Analysis, which is configured during the Security Policy Set-up with the Security Models available at the IoT platform. The security Models are based on the Low Level Configurations created by the Policy Interpreter (see Table 6).The security models determine the set of possible actions that can be carried out at the IoT platform, and will determine the reactions that can be deployed in the IoT platform. • A Verdict and Decision Support System that, according to the available Security Model and according to a set of pre-configured reactions, is able to determine the most suitable countermeasure to mitigate the detected attack/threat. • A Mitigation Action Service that transforms the proposed countermeasures to a format that is suitable to be implemented by the Security Orchestrator. • A Security Alert Service that notifies the User/System Admin about the alerts, events or countermeasures found for a specific threat/attack. This model is compatible with the User/System admin supporting the reaction module, for example, to choose one specific countermeasure or to give permissions to apply it. • Verdicts Reactions, which is a database that holds a list of all the possible countermeasures for each detected attack or security issue
Sources	Monitoring module, Interpreter, Security Orchestrator
Consumers	Dynamic security and privacy seal, Interpreter, Security Orchestrator, User/System admin
ANASTACIA activities involved	Security Reaction
Available assets	Check individual monitoring subcomponents description for details.

The Reaction module feeds mainly from the incidents detected by the Monitoring modules. Such incidents are received and processed in order to decide for the most suitable countermeasure to mitigate the

detected incident Table 21. Countermeasures are created according to a set of predefined reactions (Table 23) which are created and updated according to the capabilities currently being enforced in the IoT platform (Table 22). System admins are notified about countermeasures applied as well as the alerts that has been detected (Table 24). Additionally, reactions are transformed into a suitable format so that they can be applied within the IoT platform (Table 25).

Table 21. Verdict and Decision Support System description

Verdict and Decision Support System	
Function	It acts as the core intelligence for the reaction module. It is in charge of analysing the verdicts from the detecting module retrieve the possible list of countermeasures and compute the list of final reactions that will be deployed in order to enforce the security module loaded into the platform. This computation considers also the feedback from the system administrator, who can override decisions taken a priori by this component. As a result of this process, the component generates the set of countermeasures to apply on the network and raises alerts that will be shown to the system administrator.
Subcomponent	(Not applicable)
Sources	Data Analysis (Monitoring Module) Security Model Analysis (Reaction Module) Verdicts Reactions (Reaction Module) User/System admin (User plane)
Consumers	Security Alert Service (Reaction Module) Mitigation Action Service (Reaction Module)
ANASTACIA activities involved	Security Reaction
Available assets	Data analysis and virtual sensing: these mechanisms are used for system-level reaction, where virtual device behaviour is used to compensate the abnormal device behaviour [2].

Table 22. Security Model Analysis description

Security Model Analysis	
Function	This component as the interface with the Security Orchestrator. The latter will feed the Reaction and Detection Module with the security model, in order to assist the selection of the reactions. The Security Model will extract the required information from the security model that will allow the Decision System to compute the set of suggested countermeasures to deploy.
Subcomponent	(Not applicable)
Sources	Security Orchestrator
Consumers	Verdict and Decision Support System

ANASTACIA activities involved	Security Reaction
Available assets	Hierarchical network model: used to produce hierarchical scale-free network topology, where the network model is updated based on the mitigation action used. Each node is associated with security features to identify the possible security mitigation action that can be applied [3].

Table 23. Verdicts Reactions Database description

Verdicts Reactions Database	
Function	This component is a database that holds a list of all the possible countermeasures for each detected attack or security issue. The whole set of possible reactions can be extended by inserting new reactions in this database.
Subcomponent	(Not applicable)
Sources	Expert knowledge, external sources
Consumers	Verdict and Decision Support System
ANASTACIA activities involved	Security Reaction
Available assets	Previously observed security verdict reactions. Database can be used in different forms, such as SQL.

Table 24. Security Alert Service description

Security Alert Service	
Function	This service will provide all the functions required by the ANASTACIA platform to raise alerts and warnings in the monitoring frontend. The main goal of this module is to provide the platform the means to alert the system administrator about detected security issues or attacks.
Subcomponent	(Not applicable)
Sources	Verdict and Decision Support System
Consumers	User Plane
ANASTACIA activities involved	Security Reaction
Available assets	Security alerts prepared based on the information fetched from verdict and decision support system. SQL database can be used to store the data fetched from the verdict and decision support system. Python GUI library can be used to build a dashboard to present

	possible attacks.

Table 25. Mitigation Action Service description

Mitigation Action Service	
Function	Once the countermeasures have been calculated, they require to be transmitted to the Security Orchestrator, which will implement the measurements. In this sense, Decision System will use this service to communicate the information in a standard format, which will guarantee the modularity of the solution.
Subcomponent	(Not applicable)
Sources	Verdict and Decision Support System (Reaction module)
Consumers	Security Orchestrator Users interfaces of ANASTACIA
ANASTACIA activities involved	Security Monitoring Security Reaction Dynamic Security and Privacy Seal creation
Available assets	Reactions prepared by mitigation action service based on verdict and decision support system information for security orchestrator. SQL database can be used to store different mitigation associated to attack type.

7.1.4 Seal manager plane

Built on top of the ANASTACIA architecture, the seal manager plane provide with a mean of evaluating the level of security of an IoT platform. Table 26 describes the component that carries put such evaluation.

Table 26. Dynamic Security and Privacy Seal description

Dynamic Security and Privacy Seal	
Function	Using security and privacy standards, the Dynamic Security and Privacy Seal monitors in real time the security and privacy and provides a graphical representation of the system status to the end-user.
Subcomponent	GUI for user GUI for data controller / admin Web server Database for privacy policies Logs
Sources	Security alert service Policy editor
Consumers	Policy editor

	Verdict and decision support system
ANASTACIA activities involved	Dynamic Security and Privacy Seal creation
Available assets	MySQL Database for privacy policies repository Web framework for designing the GUI Web server

8 INTERFACES DEFINITION

This section describes the main interfaces within the ANASTACIA architecture. This description provides with an initial analysis of the information exchange between the main components of the ANASTACIA architecture. Such description will guide the implementation activities carried out in WP2-3-4-5. At this stage of the design only the interfaces among modules have been described. However, we have also added some internal interfaces, which, due to importance within the framework, deserve an early definition. Figure 13 shows the ANASTACIA architecture which includes the interfaces between modules. More specifically the interfaces described in this section are the following:

- **High to Medium interface (H2MI)**, and **Medium to Lower interface (M2LI)**: Interfaces between the User Plane and the Orchestration plane used for translating and refine policies. H2MI and M2LI provide information with different levels of granularity, having M2LI a lower level of granularity than the information provided by H2MI. These interfaces are also used internally by the Security Orchestrator to get details about the capabilities that needs to be enforced within the IoT platform.
- **Monitoring Configuration Interface (MCI), Reaction Security Configuration Interface (RCI)**: Interfaces between the Orchestration plane and the Monitoring and Reaction planes, used for the configuration of monitoring and reaction activities.
- **IoT-oriented Security Enforcement Plane Interface (IOTI), SDN-oriented Security Enforcement Plane Interface (SDNI), NFV-oriented Security Enforcement Plane Interface (NFVI)**: Interfaces between the Orchestration plane and the Enforcement plane, are used for the configuration and reconfiguration of IoT devices (through IoT controllers, SDN or NFI interfaces) in order to enforce certain security policy.
- **Security Alerts and Warnings Interface (SAWI)**: Interface between the Reaction module and the user plane which is used for the notification to the User/System admin about relevant information regarding alarms, countermeasures, etc.
- **Countermeasures Suggestions Interface (CSI)**: Interface between the Reaction module and the Orchestrator to exchange information about the countermeasures to be enforced in the IoT platform in order to react to certain incident.
- **Monitoring Verdicts Interface (MVI)**: Interface between the Monitoring module and the Reaction module used for exchanging information about detected incidents.
- **Security Enabler Provider Plugin Interface (SEPPI)**: Interface exposed by the Security Enablers Provider. It is used to get an appropriate enabler plugin during the lower policy refinement done at the Policy Interpreter, as well as providing the list of available security enablers. .

The following subsections describe these interfaces by detailing the following information:

- **Description**: describes the purpose of the interface
- **Component providing the interface**: describes the component that is offering the described interface.
    - **Input data**: describes the data that is required by the described interface.
    - **Output data**: describes the data that is returned by the described interface
- **Consumer components**: describes the components that are using the described interface..
- **Pre-conditions**: describes the potential mandatory actions that are required to be carried out before calling the described interface.
- **Post-conditions**: describes the mandatory actions to be carried out just after running the described interface.

- **ANASTACIA activities involved**: list the ANASTACIA activities where the described interface participates.

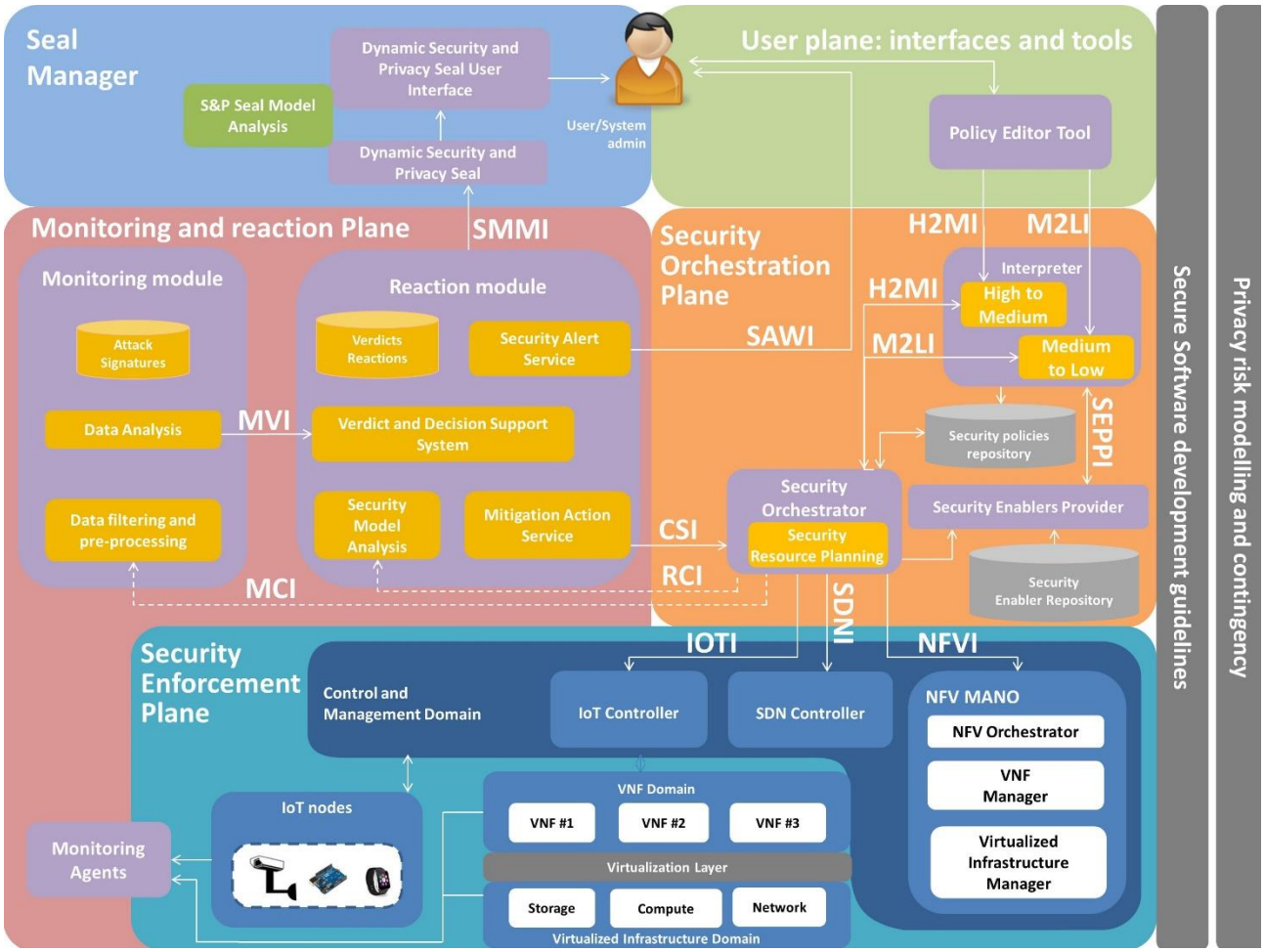


Figure 13. ANASTACIA architecture: Interfaces view

8.1 INTERFACES FOR POLICY SET-UP

The following tables describe the interfaces involved in the set-up of a new policy, comprising the interpretation of a security policy set-up at the editor, involving the interfaces H2MI (Table 27), M2LI (Table 28), SEPPI (Table 29), and the configuration of the monitoring and reaction modules which involve interfaces MCI (Table 30) and RCI (Table 31).

Table 27. Policy Orchestrator -> Interpreter H2M (H2MI)

High to Medium interface (H2MI)		
Description	The interface allows to request a policy refinement from a High level Security Policy (HSPL) to a Medium level Security Policy (MSPL).	
Component providing the interface	Policy Interpreter	
	Input data	HSPL policy
	Output Data	MSPL policy

Consumer components	Policy Editor Tool Security Orchestrator
Pre-conditions	To define the HSPL policy using a specific format (for example, XML). To define the enablers using a specific format (for example, in XML). To define associations (for example, `user:address`) Codify the previous data in an structured format (for example, using JSON)
Post-conditions	(Not applicable)
ANASTACIA activities involved	○ Security Policy Set-up

Table 28. Policy Orchestrator -> Interpreter M2L (M2LI)

Medium to Lower interface (M2LI)		
Description	The interface allows to request a policy refinement from a Medium level Security Policy (MSPL) to a specific enabler configuration/task	
Component providing the interface	Policy Interpreter	
	Input Data	MSPL policy
	Output Data	Enabler configuration/task
Consumer components	Policy Editor Tool Security Orchestrator	
Pre-conditions	To build a data structure (i.e., using JSON) including the MSPL rules and the security control name that will be used for the policy enforcement.	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Security Policy Set-up ○ Security Orchestration ○ Security Monitoring ○ Security Reaction	

Table 29. Interpreter -> Security Enabler Provider (SEPPI)

Security Enabler Provider Plugin Interface (SEPPI)		
Description	The interface allows to request for a plugin which implements the MSPL to Enabler translation.	
Component providing the	Security Enabler Provider	
	Input Data	Enabler name

interface	**Output Data**	Enabler translator plugin
Consumer components	Policy Interpreter	
Pre-conditions	There must be a correspondence between the security control name and the code location in the Security Enabler Provider.	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Security Policy Set-up ○ Security Orchestration	

Table 30. Orchestrator -> Monitoring definition (MCI)

Monitoring Configuration Interface (MCI)		
Description	This interface allows configuring the Monitoring Module from the Security Orchestrator. It is intended to provide the required parameters to refine the detection of potential threats on the network.	
Component providing the interface	Data Filtering Component (Monitoring Service)	
	Input Data	List of Security Policies' Capabilities (in form of MSPL). The Monitoring Module will use this information to infer the configuration of the Monitoring service.
	Output Data	(Not applicable)
Consumer components	Security Orchestrator	
Pre-conditions	The Security Policies capabilities (policy refined to MSPL) should be generated by the Policy Interpreter in the Policy Set-up process.	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Security Orchestration ○ Security Monitoring ○ Security Reaction ○ Security Policy set-up	

Table 31. Orchestrator -> Reaction definition (RCI)

Reaction Security Configuration Interface (RCI)	
Description	This interface allows the Security Orchestrator to provide the Security Model-related data to the Reaction Module. In general terms, this information will be composed by the Capabilities of the Security Policy and the applied countermeasures on the network as a reaction to a detected security issue.

Component providing the interface	Security Model Analysis (Reaction Module)	
	Input Data	○ Security Policies capabilities ○ List of applied security countermeasures to enforce the Security Policies
	Output Data	(Not applicable)
Consumer components	Security Orchestrator	
Pre-conditions	The Security Policies capabilities should be generated by the Policy Interpreter in the Policy Set-Up process. When sending the countermeasures, these have to be decided considering the suggestions provided by the Reaction Module using the CSI (see below).	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Security Orchestration ○ Security Reaction ○ Security Policy set-up	

8.2 INTERFACES FOR POLICY ENFORCEMENT

The following interfaces are used for the enforcement of security policies in IoT devices. Three possible ways of enforcing a policy can be used depending on the interface used:

- Policy enforcement using SDN controllers through the SDNI (Table 32)
- Policy enforcement using NFV-MANO modules through the NFVI (Table 33)
- Policy enforcement using IoT controllers through the IOIT (Table 34)

Table 32. Security Orchestrator <-> SDN controllers (SDNI)

SDN-oriented Security Enforcement Plane Interface (SDNI)		
Description	This interface allows to manage the SDN networking configuration via the SDN controller(s). The Security Orchestrator can request the enforcement of the SDN traffic flow rules received as outcome of the policy refinement process.	
Component providing the interface	SDN controller(s)	
	Input Data	Configuration of SDN-based traffic flows.
	Output Data	Information about the status of configured SDN-based traffic flows.
Consumer components	Security Orchestrator	
Pre-conditions	SDN-based networking (both control and data planes) must be operative. Low-level configuration of the SDN-based flow rules must be provided by the "Security	

	Policy Set-up" process.
Post-conditions	(Not applicable)
ANASTACIA activities involved	• Security Orchestration • Security Reaction

Table 33. Security Orchestrator <-> NFV MANO modules (NFVI)

NFV-oriented Security Enforcement Plane Interface (NFVI)		
Description	This interface allows to manage the security VNFs via the ETSI-oriented NFV MANO modules. The Security Orchestrator can request the enforcement of the security VNFs according to the configurations generated by the policy refinement process.	
Component providing the interface	NFV MANO (Management and Orchestration) modules	
	Input Data	Configuration of the security VNFs and relevant networking requirements.
	Output Data	Information about the status of configured security VNFs.
Consumer components	Security Orchestrator	
Pre-conditions	NFV MANO modules and virtualization infrastructures must be operative. Low-level configuration of the security VNFs and relevant networking requirements must be generated by the "Security Policy Set-up" process.	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	• Security Orchestration • Security Reaction	

Table 34. Security Orchestrator <-> IoT controllers (IOTI)

IoT-oriented Security Enforcement Plane Interface (IOTI)		
Description	This interface allows to manage the configuration of IoT nodes via specific IoT controllers. The Security Orchestrator can request the enforcement of the security controls within the IoT nodes according to the configurations generated by the policy refinement process.	
Component providing the interface	IoT controllers	
	Input Data	Configuration of the security controls for the IoT nodes.
	Output Data	Information about the status of configured security controls in the IoT nodes.
Consumer components	Security Orchestrator	

Pre-conditions	IoT nodes and relevant IoT controller must be operative. Low-level configuration of the security controls for the IoT nodes..
Post-conditions	(Not applicable)
ANASTACIA activities involved	• Security Orchestration • Security Reaction

8.3 INTERFACES FOR MONITORING AND REACTION

The following interfaces are used for exchanging relevant data required for the fulfilment of a security policy within an IoT platform. This includes:

- The notification of detected incidents between the Monitoring and the Reaction modules through the MVI (Table 35)
- The notification of alerts and countermeasures from the Reaction module to the User/System admin through the SAWI (Table 36)

Table 35. Monitoring -> Reaction definition (MVI)

Monitoring Verdicts Interface (MVI)		
Description	This interface is intended to provide the required monitoring information from the Monitoring to the Reaction Module. The transferred data is mainly composed of the verdicts of the security properties tested on the network.	
Component providing the interface	Verdict and Decision Support System (Reaction Module)	
	Input Data	Verdicts about the security issues and attacks potentially detected in the network.
	Output Data	(Not applicable)
Consumer components	Data Analysis (Monitoring Module)	
Pre-conditions	A security policy must have been set-up in the monitoring and reaction modules and enforced in the IoT platform	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Security Monitoring ○ Security Reaction	

Table 36. Reaction -> User/System Administrator definition (SAWI)

Security Alerts and Warnings Interface (SAWI)	
Description	This interface will transfer the alerts and warnings from the Reaction Module to the end-user interfaces. It is designed as a communication channel between the Reaction Module and the ANASTACIA User Plane.

Component providing the interface	Security Alert Service (Reaction Module)	
	Input Data	List of security alerts and warnings, including information about the incidents detected and the devices affected. Optionally, proposed countermeasures can also be submitted to the end-user asking for her consent.
	Output Data	(Not applicable)
Consumer components	End-user interface	
Pre-conditions	(Not applicable)	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Security Monitoring ○ Security Reaction	

Table 37. Reaction -> Orchestrator definition (CSI)

Countermeasures Suggestions Interface (CSI)		
Description	This interface was conceived to transmit the set of suggested countermeasures from the Reaction module to the Security Orchestrator	
Component providing the interface	Security Orchestrator	
	Input Data	List of envisioned countermeasures
	Output Data	Acknowledgement in the reception of the envisioned Reaction module's countermeasures
Consumer components	Verdicts and Decision Support System (Reaction Module)	
Pre-conditions	A security policy must have been set-up in the monitoring and reaction modules and enforced in the Security Enforcement plane	
Post-conditions	The orchestrator will carry out the appropriate activities to enforce the envisioned countermeasures.	
ANASTACIA activities involved	○ Security Orchestration ○ Security Reaction	

8.4 INTERFACES FOR SEAL CREATION

The following interface SMMI (Table 38) is used for the exchange of the relevant data that the seal manager needs in order to create the Dynamic Security and Privacy Seal.

Table 38. Reaction -> Seal Manager definition (SMMI)

Seal Manager Metadata Interface (SMMI)		
Description	The interface provides the requested information to evaluate the security and the privacy in a real-time fashion. The security and privacy policies defined by the user are stored inside the policies repository and an interface is available to retrieve and set them from the seal manager.	
Component providing the interface	Dynamic Security and Privacy Seal	
	Input Data	Alerts, warnings, vulnerabilities, MSPL-based capabilities
	Output Data	Information provided to the user through the graphical user interface (GUI), Security and Privacy policies
Consumer components	Security Alert Service, Security Model Analysis	
Pre-conditions	A security policy must have been set-up in the monitoring and reaction modules and enforced in the IoT platform	
Post-conditions	(Not applicable)	
ANASTACIA activities involved	○ Dynamic security and privacy seal creation	

9 REQUIREMENTS COVERAGE

This final section links the requirements elicited in D1.2 and reported in section 2 to the components of the ANASTACIA architecture as identified and detailed above, in order to support developers in checking the advancement in requirement coverage during the development and integration activities

The result is summarized in the following table, where every component is mapped to the requirements that it covers/contributes to satisfy.

Table 39. Requirements coverage

Component	Functional Requirements covered (Req ID)	Non-functional Requirements covered (Req ID)	Privacy Requirements covered (Req ID)
Policy Editor Tool	FR-1, FR-2, FR-3, FR-4,	NFR-1, NFR-2, NFR-3, NFR-5, NFR-6, NFR-7, NFR-9, NFR-10, NFR-15	As privacy requirements must be guaranteed at any level and by any function, all components contribute to their satisfaction as for their functional role: PR-1, PR-2, PR-3, PR-4, PR-5, PR-6, PR-7, PR-8, PR-9, PR-10, PR-11, PR-12, PR-13, PR-14, PR-15, PR-16
Security Orchestrator	FR-13, FR-14, FR-17, FR-18, FR-19, FR-20	NFR-2, NFR-4, NFR-5, NFR-6, NFR-8, NFR-10, NFR-12, NFR-14	
Interpreter	FR-1, FR-2, FR-12	NFR-2, NFR-5, NFR-6, NFR-12	
Security Enablers Provider	FR-5, FR-6, FR-7, FR-8, FR-12, FR-13, FR-14, FR-17, FR-18, FR-19	NFR-2, NFR-4, NFR-5, NFR-6, NFR-8, NFR-10, NFR-12, NFR-14	
Monitoring module	FR-10, FR-12, FR-18, FR-19	NFR-2, NFR-4, NFR-5, NFR-6, NFR-8, NFR-11, NFR-12, NFR-13, NFR-14	
Data Analysis	FR-12, FR-19	NFR-2, NFR-5, NFR-6, NFR-8, NFR-11, NFR-12	
Data Correlation	FR-12, FR-19	NFR-2, NFR-5, NFR-6, NFR-8, NFR-11, NFR-12	
Reaction module	FR-12, FR-18, FR-19	NFR-2, NFR-5, NFR-6, NFR-8, NFR-11, NFR-12, NFR-14	
Verdict and decision support system	FR-12, FR-17, FR-18, FR-19, FR-20	NFR-2, NFR-4, NFR-5, NFR-6, NFR-8, NFR-11, NFR-12, NFR-14	
Security Alert Service	FR-12, FR-18, FR-19	NFR-2, NFR-5, NFR-6, NFR-8, NFR-11, NFR-12	
Security Model Analysis	FR-12	NFR-2, NFR-5, NFR-6, NFR-8	

Component	Functional Requirements covered (Req ID)	Non-functional Requirements covered (Req ID)	Privacy Requirements covered (Req ID)
Mitigation Action Service	FR-12, FR-17, FR-18	NFR-2, NFR-3, NFR-4, NFR-5, NFR-6, NFR-8, NFR-10, NFR-12, NFR-13, NFR-14	
Monitoring Agent	FR-10, FR-11	NFR-2, NFR-4, NFR-5, NFR-6, NFR-8, NFR-9, NFR-12, NFR-14	
Reaction Agent	FR-14	NFR-2, NFR-4, NFR-5, NFR-6, NFR-8, NFR-9, NFR-12, NFR-14	
Dynamic security and privacy seal	FR-9, FR-15, FR-16, FR-18	NFR-1, NFR-2, NFR-3, NFR-4, NFR-5, NFR-6, NFR-7, NFR-9, NFR-10, NFR-12, NFR-13, NFR-14, NFR-15	

10 CONCLUSIONS

In this document we have detailed the ANASTACIA architecture and the methodology used for its creation. Firstly we analysed the requirements, use cases and context analysis carried out in D1.1 and D1.2. This information was used to create a conceptual model for ANASTACIA that identifies objects participating in the framework, relationships between them and the terminology used. It was also defined the system model of the ANASTACIA framework. This system model helped to identify the way that the ANASTACIA framework will be integrated within an IoT platform. Both the system model and the conceptual model were used to define the ANASTACIA architecture. The design of the architecture started with the definition of a high level architecture, based on well-defined planes: user, orchestration, monitoring & reaction, enforcement and seal. This high level architecture was completed with the components in charge of carrying out specific activities within every plane and with the main interfaces between the main components of the architecture.

This deliverable closes the initial design phase, which was achieved at M6 through the milestone MS9 and which results are reported here. The initial stage of the design is therefore completed and the implementation activities can continue with the ANASTACIA architecture as reference. This deliverable includes details about components and interfaces that have been defined in collaboration with the technical WPs (WP2-3-4-5), which guarantee the consistency between the implementation activities and the design.

However, it is foreseen that slight modifications will be required to the architecture as long as the project advances, although it is expected that, if any, the changes will be minor and the current architecture is considered stable and robust enough to achieve the objectives of the project. To this end, the final modifications and an additional level of granularity for the architecture is expected to be reported in D1.5 (Final Architectural Design, M36), where further details on interfaces, activities and the incorporation of privacy aspects to the enforced policies will also be added.

REFERENCES

[1]. Internet of Things – Architecture project (IoT-A). "D1.3: Updated reference model for IoT v1.5". Editor: Andreas Nettstraäter (FhG IML). 16.7.2012. EU FP7 project. Contract Agreement: 257521

[2]. K. Paridari, A. Mady, S. L. Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg, and M. Boubekeur, "Cyber-physical-security framework for building energy management system," ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), April 2016.

[3]. A. Mady, D. Mehta, D. M. Shila, and M. Boubekeur, "Towards resilient cyber security for embedded devices on internet," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (2016), vol. 0, pp. 1–2, Dec. 2016.

[4]. Marco Vailini. "D4.1. Policy Specification". SECURED FP7. 2015. Available online: https://www.secured-fp7.eu/files/secured_d41_policy_spec_v0100.pdf. Last accessed: August 2017.