ANASTACIA

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

D1.4

Final User-centred Requirements Analysis

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

Distribution level	PU
Contractual date	30.11.2018 [M23]
Delivery date	31.05.2019 [M29]
WP / Task	WP1 / T1.2
WP Leader	ATOS
Authors	S.Bianchi (SOFT), F.Nebiacolombo (SOFT), G.Viano (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.

This document only reflects the ANASTACIA Consortium's view.
The European Commission is not responsible for any use that may be made of the information it contains.

Table of contents

PUBLIC SUMMARY

ANASTACIA is developing a holistic framework (see Figure 1) for the assessment of security and privacy in complex ICT/IoT architectures and Cyber Physical Systems (CPS), using Software Defined Networks (SDN) and Network Function Virtualization (NFV) technologies (along with IoT controllers) to ensure the overall security of monitored systems, taking into account privacy constraints derived from the General Data Protection Regulation (GDPR) and other relevant regulations, standards and best practices.

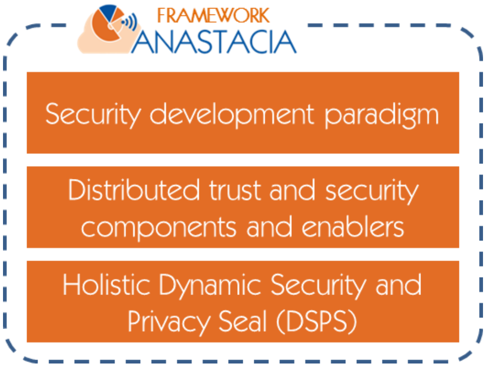

FRAMEWORK
ANASTACIA
Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)

Figure 1. ANASTACIA framework

This deliverable contains the result of the final analysis and review of the user-centred functional and non-functional requirements for the proposes ANASTACIA framework. The associated activities complement those which delivered D1.2 by duly considering (see Figure 2) the output of development activities (WP2, WP3, WP4, WP5), integration processes (WP6) and validation/evaluation phases (with feedback from end-users, EC/reviewers and Innovation Advisory Board).

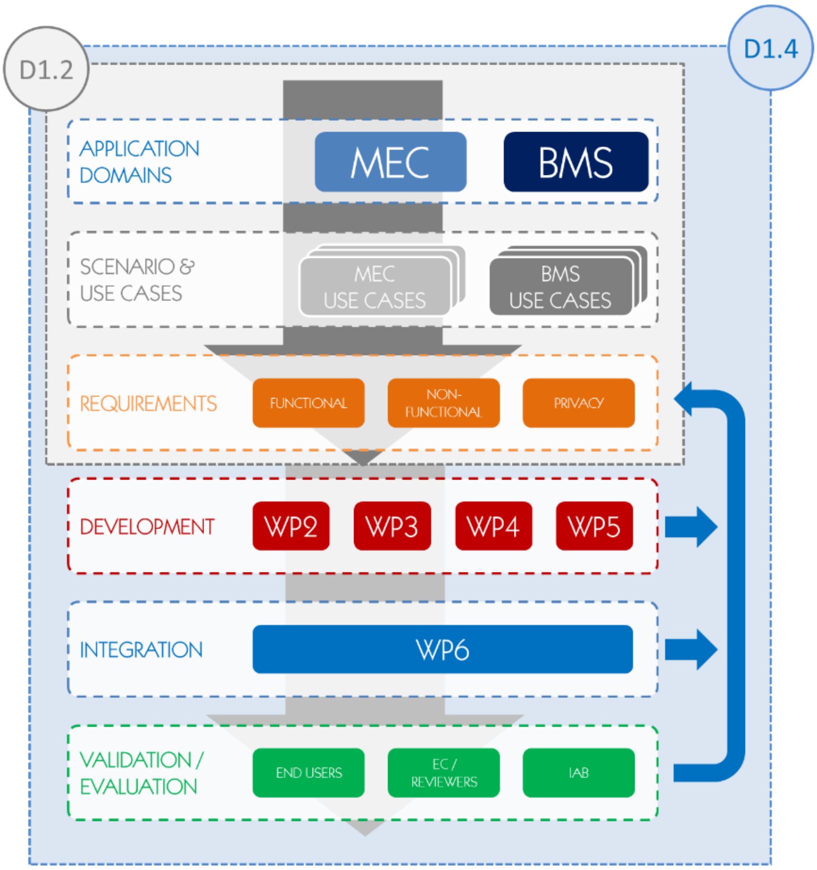


Figure 2. Requirement elicitation and review process.

1 Introduction

1.1 Aims of the document

This document starts from the results of D1.2 “User-Centred Requirement Initial Analysis” to include the final version of the functional and non-functional requirements. The main aims are:

- to verify and review validity, applicability and coverage of the requirements identified in D1.2;
- to integrate requirements identified in D1.2 with new ones obtained after the review of the results of the first validation and evaluation phase and derive actionable input for the finalization of both methodological and technical results;
- to integrate requirements identified in D1.2 with new ones emerging from input from the Innovation Advisor Board (IAB) and from the reviewers (Additional Technical Review and Key Innovations identified), as well as from the resubmitted D6.2 “Initial Use Cases Implementation and Tests Reports” (verification against the updated use cases);
- to leverage the update of requirements to derive actionable hints for the pre-industrialization phase of technical results and make the take-up of the delivered ANASTACIA framework easier and more appealing for exploitation purposes;
- to revamp and assess accordingly services and functionalities that the project will design, deliver, integrate and validate;
- to provide indication for the finalization of the architecture design.

1.2 Applicable and reference documents

This document refers to the following documents:

- Grant Agreement N°731558 and annexes (“Description of Action”)
- D1.1 Holistic Security Context Analysis (CNR, M6)
- D1.2 User-Centred Requirement Initial Analysis (SOFT, M6)
- D7.1 Initial Dissemination, Standardization and Outreach Strategy Plan (AALTO, M6)
- D7.2 Initial Exploitation and Data Management Plan (SOFT, M6)
- D1.3 Initial Architecture Design (ATOS, M9)
- D2.1 Policy-based Definition and Policy for Orchestration Initial Report (UMU, M12)
- D5.1 Dynamic Security and Privacy Seal Model Analysis Report (MAND, M24 RESUBM.)
- D2.2 Attack Threats Analysis and Contingency Actions Initial Report (CNR, M14)
- D6.1 Initial Technical Integration and Validation Report (UBITECH, M14)
- D3.1 Initial Security Enforcement Manager Report (UMU, M15)
- D2.3 Privacy Risk Modelling and Contingency Initial Report (MAND, M16)
- D3.2 Initial Security Orchestrator Report (AALTO, M18)
- D6.2 Initial Use Cases Implementation and Tests Reports (UTRC, M24 RESUBM.)
- D2.4 Secure Software Development Guidelines Initial Report (ATOS, M18)
- D7.3 First Period Dissemination, Standardization and Outreach Report (AALTO, M18)
- D8.1 1st Periodic Report (SOFT, M18)
- D3.3 Initial Security Enforcement Enablers Report (THALES, M19)
- D4.1 Initial Monitoring Component Services Implementation Report (MONT, M20)
- D6.3 Initial End-User Validation and Evaluation Report (M22 AMENDED)
- D4.2 Initial Reaction Component Services Implementation Report (CNR, M22)
- D2.5 Policy-based Definition and Policy for Orchestration Final Report (UMU, M24)
- D4.3 Initial Agents Development Report (UTRC, M24)
- D5.2 Dynamic Security and Privacy Seal Monitoring Service (AS, M24)

- D2.6 Attack Threats Analysis and Contingency Actions Final Report (CNR, M26)
- D2.7 Privacy Risk Modelling and Contingency Final Report (CNR, M28)

1.3 Revision History

Version	Date	Author	Description
1	10/10/2018	S.Bianchi (SOFT)	ToC
2	12/11/2018	S.Bianchi (SOFT)	Updated Positioning section
3	23/11/2018	G.Viano (SOFT)	Introduction section
4	21/01/2019	S.Bianchi (SOFT), F.Nebiacolombo (SOFT)	Update of ToC and new formats of requirement tables and analysis (coverage, validity etc.
5	23/02/2019	S.Bianchi (SOFT)	New Inputs section, references to First validation and White Paper
6	29/03/2019	S.Bianchi (SOFT), F.Nebiacolombo (SOFT), G.Viano (SOFT)	Review of functional and non-functional requirements according to Main Challenges and Key Innovations, updated tables
7	03/05/2019	S.Bianchi (SOFT), F.Nebiacolombo (SOFT)	General review according to formalized technical review report and associated results of plenary meeting
8	17/05/2019	S.Bianchi (SOFT)	Conclusion section, consistency check
9	20/05/2019	R. Trapero (ATOS), S.Vuppala (UTRC)	Overall review, check of new requirements
10	25/05/2019	S.Vuppala (UTRC)	Internal review process
11	31/05/2019	S.Bianchi (SOFT)	Final proofreading and delivery, according to internal review process

Note on late delivery, associated justification and risk mitigation:

As declared in the opening table, D1.4 has been delayed (nearly +6M), as it was meant to be provided on M23 (November 2018) and is instead released on mid M29 (May 2019). The justification for this late yet controlled/mitigated delivery is explained as follows (see Figure 3):

- ~2 months due to delay accumulated in the first validation phase and in the formalization of its results, agreed upon and accepted by the Consortium to optimize the feedback from evaluators (including the feedback provided by the IAB members during the plenary meeting held in late November 2018, M23);
- ~1 month due to the preparation of the technical review and the associated work on the project White Paper and the included Key Innovations;
- ~1.5 months due to the update of the review process according to the informally approved reference Main Challenges and associated Key Innovations;
- ~1 month due to the internal review of the document according to the formal feedback of the technical review and the related discussion and results of the plenary meeting held in April 2019 (M28).

To mitigate the potential risks associated to this delay (e.g. dependencies between activities and deliverables), SOFT ensured that discussion with technical work packages for the improvement and the extension of developed functionalities was kept alive and aligned with the main findings, shared with the whole Consortium although not explicitly formalized and submitted according to Project Continuous Reporting procedures.

According to the Risk Management policies defined by the project, the delay has been discussed with WP leaders in plenary meetings and mitigated by a joint effort, so to ensure that no critical impacts were caused on activities and expected results – interim results of the requirement review process were in fact effectively shared with technical WPs to steer the development activities.

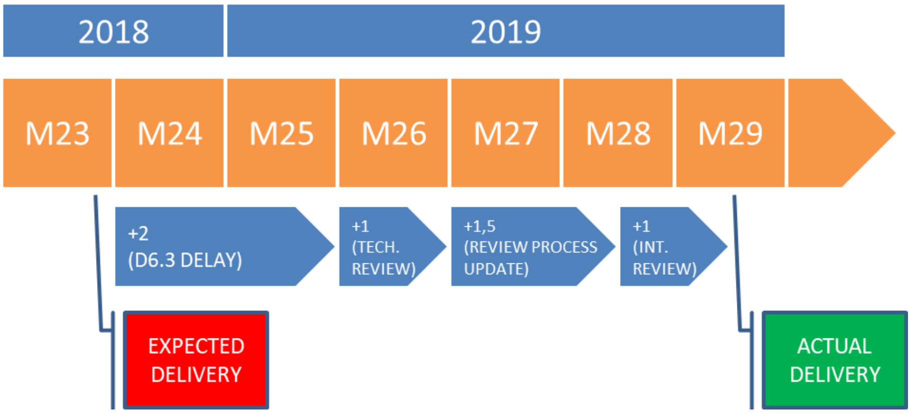


Figure 3. Justification of late delivery

1.4 ACRONYMS AND DEFINITIONS

Acronym	Definition
AAA	Authentication, Authorization and Accounting
DSS	Decision Support System
CISO	Chief Information Security Officer
CPS	Cyber Physical Systems
DoS	Denial of Service
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
DSPS	Dynamic Security and Privacy Seal
ECA	Event-Condition-Action
HSPL	High-level Security Policy Language
IoT	Internet of Things
ISP	Internet Service Provider
MEC	Mobile Edge Computing
MSPL	Medium-level Security Policy Language
NFV	Network Function Virtualization
NSF	Network Security Functions
PoC	Proof of Concept
QoS	Quality of Service
SDA	Slow DoS Attacks
SDN	Software Defined Networking
SFC	Service Function Chaining
VIM	Virtual Infrastructure Manager
VNSF	Virtual Network Security Functions

2 CONTEXTUALIZATION

2.1 SCOPE

ANASTACIA is developing a **trustworthy-by-design security framework** able to take autonomous decisions using networking technologies (such as **Software Defined Networking** and **Network Function Virtualisation**) and **intelligent and dynamic security enforcement and monitoring** methodologies and tools. The ANASTACIA framework will thus include:

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

The elicitation of requirements was initially carried out in D1.2 and was further refined during the project activities, after the first validation and evaluation phase, to support also the industrialization phase that is expected to ultimately lead to the release of an ANASTACIA-derived set of products. This deliverable D1.4 – meant to review and update the initial version – has been prepared in parallel to several others complementary activities and on the basis of i) the technical results achieved during the first integration phase, ii) the feedback collected during the first validation phase, iii) the results of the review with EC and external reviewers and iv) the support provided by the Innovation Advisory Board (see Figure 4).

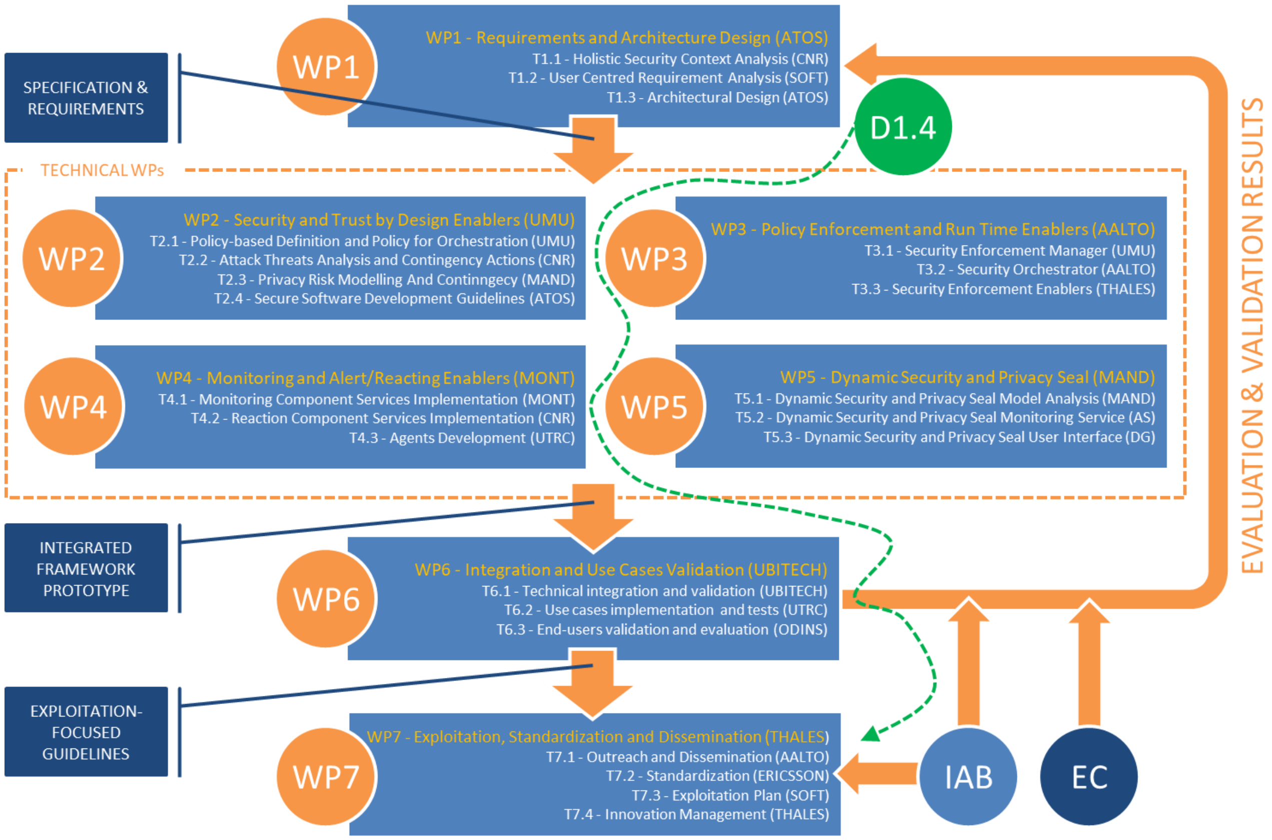

SPECIFICATION & REQUIREMENTS
WP1
WP1 - Requirements and Architecture Design (ATOS)
T1.1 - Holistic Security Context Analysis (CNR)
T1.2 - User Centred Requirement Analysis (SOFT)
T1.3 - Architectural Design (ATOS)
D1.4
TECHNICAL WPs
WP2
WP2 - Security and Trust by Design Enablers (UMU)
T2.1 - Policy-based Definition and Policy for Orchestration (UMU)
T2.2 - Attack Threats Analysis and Contingency Actions (CNR)
T2.3 - Privacy Risk Modelling And Continngecy (MAND)
T2.4 - Secure Software Development Guidelines (ATOS)
WP3
WP3 - Policy Enforcement and Run Time Enablers (AALTO)
T3.1 - Security Enforcement Manager (UMU)
T3.2 - Security Orchestrator (AALTO)
T3.3 - Security Enforcement Enablers (THALES)
WP4
WP4 - Monitoring and Alert/Reacting Enablers (MONT)
T4.1 - Monitoring Component Services Implementation (MONT)
T4.2 - Reaction Component Services Implementation (CNR)
T4.3 - Agents Development (UTRC)
WP5
WP5 - Dynamic Security and Privacy Seal (MAND)
T5.1 - Dynamic Security and Privacy Seal Model Analysis (MAND)
T5.2 - Dynamic Security and Privacy Seal Monitoring Service (AS)
T5.3 - Dynamic Security and Privacy Seal User Interface (DG)
INTEGRATED FRAMEWORK PROTOTYPE
WP6
WP6 - Integration and Use Cases Validation (UBITECH)
T6.1 - Technical integration and validation (UBITECH)
T6.2 - Use cases implementation and tests (UTRC)
T6.3 - End-users validation and evaluation (ODINS)
EXPLOITATION-FOCUSED GUIDELINES
WP7
WP7 - Exploitation, Standardization and Dissemination (THALES)
T7.1 - Outreach and Dissemination (AALTO)
T7.2 - Standardization (ERICSSON)
T7.3 - Exploitation Plan (SOFT)
T7.4 - Innovation Management (THALES)
IAB
EC
EVALUATION & VALIDATION RESULTS

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

The results of the second analytical cycle herein summarized (see Figure 5) constitute the basis for the refinement of final technical results to be delivered in Y3.

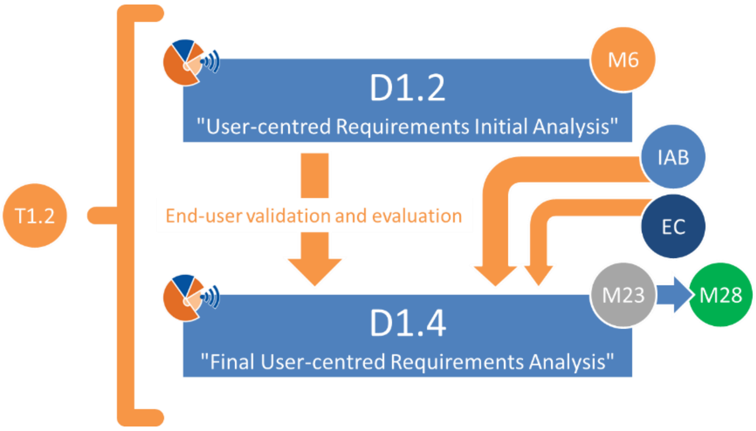

T1.2
M6
D1.2
"User-centred Requirements Initial Analysis"
IAB
End-user validation and evaluation
EC
M23
M28
D1.4
"Final User-centred Requirements Analysis"

Figure 5. Relation between deliverables D1.2 and D1.4 (associated to T1.2) and additional considered inputs.

In the document, considerations used to review/update/extend the User Centred Requirements are generically indicated by a black arrow icon and an explanatory description:

➥	<general consideration on requirements>

2.2 Positioning

As indicated in the project proposal and in D1.2, **ANASTACIA globally aims to reach TRL 5** i.e. “technology validated in relevant environment”. According to the developments carried out in the first part of the projects and the technological/methodological approaches adopted, the considerations expressed in D1.2 remains valid as for the implications of the targeted TRL 5:

- **the project is not expected to release a fully functional / product-like prototype**, but rather (as a Research & Innovation Action) to develop and validate a set of **Key Innovations** in relevant application scenarios and ambitious IoT/CPS-based use cases; this preliminary consideration has two impacts:
  - **on user requirements**: this document reviews the initial set of requirements as included in D1.2, identify new complementary ones and proposes optional ones to possibly support pre-industrialization and industrialization phases, as illustrated in Section 5, with the ultimate objective of easing the maximization of the Return on Investment (RoI) for the partners;
  - **on exploitation plans**: as anticipated, since the project is not expected to deliver a complete and qualified system, also commercial targets (associated also to the actual implementation of some specific features) might be adequately corrected.
- considering both complexity of the architecture and different maturity of the tools adopted (including proprietary solutions provided by some beneficiaries), **the global TRL of the project will be a reasoned mediation between the TRLs of the different components integrated**.

2.3 END USERS

D1.2 initially proposed a rather differentiated portfolio of potential user categories, coping at different levels with security and privacy issues and characterized by very different professional profiles, taking into consideration the holistic nature of the proposed framework:

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

To focus on specific needs and requirements, this rather broad range of user categories, spanning through highly differentiated professional expertise, was then reduced to two main groups:

- **Security Managers**
- **Privacy Managers**

whose profiles support, for example, the operational activities (see Figure 6) of

- **Cyber Physical System (CPS) Managers**

Considering the application domain used for demonstration purposes (Building Management Systems and Multi-access Edge Computing) the CPS Managers group includes, for example, Building Managers - in charge of overseeing the operational continuity of the building, considered as a "system of systems" that includes ICT (e.g. network components) and IoT (e.g. sensors, gateways etc.) architectures, supported on one side by Security Managers (e.g. CISOs), in charge of the business continuity of large ICT infrastructures, and Privacy Managers (e.g. DPOs) , in charge of compliance with legislation (e.g. GDPR).

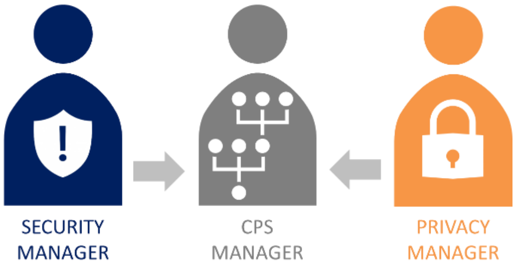


Figure 6. Targeted end user categories - simplified grouping.

Considering the nature of the project and the expected TRL, the Consortium initially agreed upon **focusing more on technical profiles and associated requirements/needs**, also considering that the initial validation phase would have involved mainly evaluators from the technical sectors and that high-level functionalities (e.g. Dynamic Privacy and Security Seal) were scheduled for release in the second half of the project.

3 INPUTS

3.1 FIRST VALIDATION AND EVALUATION RESULTS

D1.2 provided a description of **4 reference Use Cases** for each of the **application domain**s identified in the Description of Action (DoA), formalized as a narrative description, a detailed mapping onto architectural planes, a definition of the actors involved, and a structured definition of the functional steps included. The complete list is reported below for reference:

- Application Domain **Building Management Systems (BMS)**
  - Use Case **BMS.1**: Cyber-Attack at a Hospital Building
  - Use Case **BMS.2**: Insider Attack on the Fire Suppression System
  - Use Case **BMS.3**: Remote Attack on the Building Energy Microgrid
  - Use Case **BMS.4**: Cascade Attack on a Megatall Building
- Application Domain **Mobile (Multi-access) Edge Computing (MEC)**
  - Use Case **MEC.1**: Spoofing Attack on the Security Camera System
  - Use Case **MEC.2**: Man-in-the-middle Attack on the MEC Server
  - Use Case **MEC.3**: DoS / DDoS attacks using Smart Cameras and IoT devices
  - Use Case **MEC.4**: IoT-based attack in the MEC Scenario

As reported in D6.3, the first validation and evaluation phase focused on the first integrated ANASTACIA framework, tested according the Test Cases and the methodology reported in D6.2, within the operational scope of four specific use-cases implemented:

- Use Case **BMS.2**: Insider Attack on the Fire Suppression System
- Use Case **BMS.3**: Remote Attack on the Building Energy Microgrid
- Use Case **BMS.4**: Cascade Attack on a Megatall Building
- Use Case **MEC.3**: DoS/DDoS Attacks using IoT Devices

For each selected use case, a detailed description, including implementation plan and expected benefits provided by ANASTACIA framework therein, was elaborated, including data capturing (i.e. web interfaces and log consoles) from components during the execution and validation of the specific use case.

The first round of validation and evaluation:

- was carried out by 65 interviewees/end-users, whose feedback has been analysed to provide the Consortium with actionable prioritization criteria to focus on specific functionalities and features to be added or improved;
- was supported by a questionnaire divided into three parts: general features, specific operations (of each implemented use case) and related aspects of DSPS management.

Interviewees/end-users were asked to rate relevant features to be further addressed in the second cycle of framework development. Each answer was provided by a score from 1 to 5 in accordance to a Likert scale:

1. = **Very Low** – **fully disagree**,
2. = **Low** – **partially disagree**,
3. = **Medium** – **neutral**,
4. = **High** – **partially agree**,
5. = **Very High** – **fully agree**.

3.1.1 General validation and evaluation

3.1.1.1 Overall features

The results of general questions show that interviewees/end-users generally agree on main positive features of ANASTACIA framework, as shown the following table. Usability of the whole system (i.e. of all included UI/reporting systems) should be sensitively improved in the second phase of the project, other more technical features should be.

Results of General Questions about ANASTACIA framework	**MEAN**	**DEVIATION**
1. Easy to use	3,461	0,9341823
2. Intuitive user interfaces	3,663	0,9482306
3. Real-time feedback	4,139	0,7338593
4. Powerful reporting	3,969	0,8587863
5. Modular and scalable	4,076	0,820435
6. Automatic reactions to threats	4,522	0,6562033
7. Response time of monitoring module	4,014	1,0883958
8. Response time of reaction module	4,043	1,2334641
9. Response time of orchestration module	4,135	1,3574919
10. Response time of enforcement module	4,088	1,5762936

3.1.1.2 Overall comments and observations

Main valuable highlights from the collected questionnaires are reported here according to the most appreciated aspects and the most unsatisfied ones.

3.1.1.2.1 Positive overall comments and observations (PCO)

☺	**What do you like the most about the ANASTACIA framework?**
PCO-1	The overall idea for mitigation based on predefined policies. The scenarios seemed to work properly.
PCO-2	Ambitious goal to manage security aspects by detecting, monitoring and reacting to the identification of vulnerabilities or attacks. Also, the integration of different components towards this end.
PCO-3	The IoT network simulation and the respective traffic forwarding when an attack occurs.
PCO-4	It provides understandable user interfaces that can easily be used by non-specialized users.
PCO-5	Network simulation and traffic forwarding.
PCO-6	It's very useful for privacy and security concerns.
PCO-7	The end-user interfaces that facilitate understanding of the different modules of actions.
PCO-8	You can dynamically and automatically act against different kind of attacks.
PCO-9	It is an interesting approach to modulate the different actions in a network, from the network access, to the detection of the different possible attacks and alert about them in close real time to notify the correspondent agent to mitigate the attacks by using automation processes.
PCO-10	Intuitive user interfaces.
PCO-11	The variety of components which allows for a dynamic setup of the network topology to derive traffic to specific nodes using NFVs, treat security and provide countermeasure for different security threats or attack.
PCO-12	The novel, interesting and promising way of facing cybersecurity on IoT environments.
PCO-13	The reaction module that generates and enforces security policies in the system handled by the security orchestration and enforcement planes.
PCO-14	Its scalability and modularity.

☺	**What do you like the most about the ANASTACIA framework?**
PCO-15	It is an awesome framework for security mitigation relating to both intrusion prevention and detection.
PCO-16	Fast response time as well as providing with complete countermeasures for the security treats.
PCO-17	The organization in several planes, each of them dedicated to a particular goal, and interacting each other. It can be useful for a very large number of attacks, with appropriate detection and mitigation methods. The use cases presented here are interesting.
PCO-18	Its holistic approach on IoT security
PCO-19	Successful integration of key technologies and standards into a unified cybersecurity framework. From a technology standpoint, the project is challenging, ambitious and state of the art, and of high potential if complexity is properly managed. The technologies are complementary and well positioned to offer adequate monitoring, detection and reaction to cyber-attacks. Especially the SDN/NFV way is used to offer mitigation environment/infrastructure against network level attacks.
PCO-20	The capacity to provide automatic protection against potential threats.
PCO-21	Despite the usage of access control and security policy creation, which usually requires some manual tasks to be performed, the ANASTACIA framework seems to work well in terms of automatic detection of threats and, especially, identification of possible countermeasures. Not so sure about real-time detection of possible zero-day attacks, when no previous knowledge of the attack itself is available.
PCO-22	Its modularity and scalability. The novelty introduced regarding the monitoring of IoT devices.
PCO-23	The intelligence of the combination of SDN and NFV paradigms. The network is able to detect and stop an attack fastly.
PCO-24	The automated adaptability through online monitoring and testing techniques.
PCO-25	Ambitions of the ANASTACIA Framework and the fact it targets actionable results (useful and usable).
PCO-26	The capability to autodetect attacks and deploys countermeasures. It also isolates the attacker emulating a virtual copy of the victim IoT network that could allow us to study the attack.
PCO-27	DSPS GUI is very user friendly and the alert information is complete and easy to understand.
PCO-28	The fast and powerful response provided for cyber-attacks in IoT and Cloud architectures.

3.1.1.2.2 Negative overall comments and observations (NCO)

☹	**What do you dislike the most about the ANASTACIA framework?**
NCO-1	The framework could be easier to use if the platform was more integrated.
➥	Usability and (seamless) integration should be addressed and improved
NCO-2	The intelligence behind the incident detector is not clear. The attacks presented were straight forward. What would happen if the attack was a more sophisticated one?
➥	Complex (multiple attack) scenarios should be properly handled and mitigated Reasoning capabilities for autonomous mitigation should be improved
NCO-3	The architecture might be a little complex to understand and requires expertise to be properly deployed.
➥	Distributed architecture should be managed Deployment procedures should be defined accordingly
NCO-4	I don't understand why a blockchain is used in the framework. I think a centralized server would be a better idea and provide much more benefits.

☹	**What do you dislike the most about the ANASTACIA framework?**
➥	Experimental use of Blockchain technology adopted for compliance with DoA, justifications included in D5.1 (resubmitted)
NCO-5	Turning off IoT sensor as a countermeasure.
➥	Policies that interfere with CPS status should be properly defined to avoid unexpected impacts
NCO-6	It can be perceived as a very large and complicated framework.
➥	Complexity should be mitigated by usability
NCO-7	The terminology in the videos is sometimes to complex – not easy to understand for people outside the project.
➥	Usability should be addressed and improved (terminology for non-technical users)
NCO-8	Maybe it could be too complex to understand if it is the first time you see the architecture.
➥	Complexity should be mitigated by usability
NCO-9	In general, it is complex to understand.
➥	Complexity should be mitigated by usability
NCO-10	It is difficult to understand how the orchestration of different components is carried out. In addition, the definition of security policies at different levels, as well as debugging information, seems a bit complex to understand.
➥	Complexity should be mitigated by usability Information about orchestrated/enforces mitigation plans should be duly provided in plain language for non-technical users
NCO-11	It is complicated that it may add too much overhead and complexity to the IoT environment, adding possible failure points.
➥	Overhead and complexity associated to the implementation/deployment/use of the ANASTACIA framework should be generally minimized No additional failure points should be added by the orchestration/enforcement of mitigation plans
NCO-12	It is difficult to understand ANASTACIA and to use the whole framework.
➥	Complexity should be mitigated by usability
NCO-13	The current implementation level of the DSPS Seal Management.
➥	Usability should be addressed and improved (DSPS for non-technical users)
NCO-14	The attack vectors used to demonstrate the effectiveness of the framework are too common, for that reason it's hard to validate the robustness of the framework in that regards. I suggest investigating on more complex vectors that compromise the different components and give a more detailed assessment.
➥	Complex (multiple attack) scenarios should be properly handled and mitigated
NCO-15	ANASTACIA system might be quite complicated for system administrators with no or little experience with network security attacks.
➥	Complexity should be mitigated by usability Usability should be addressed and improved (system administrators)
NCO-16	We have no information about the overhead generated during the detection and mitigation of attacks. Though it may be quite low, thanks to the organization into several planes.

☹	**What do you dislike the most about the ANASTACIA framework?**
➥	Overhead and complexity associated to the implementation/deployment/use of the ANASTACIA framework should be generally minimized Performances should be generally optimized
NCO-17	From security standpoint, it remains unclear what IoT threats the project is capable/aiming to address. For instance, malware threat is a serious concern for IoT and the project should better stress its capability to address such threat. From adoption standpoint, complexity and framework settings may be a killing factor for the project. Interactions among various domain components (monitoring, orchestration, enforcement) remain complex and difficult to understand.
➥	Complex (multiple attack) scenarios should be properly handled and mitigated Complexity should be mitigated by usability Usability should be generally addressed and improved (integration/use of planes)
NCO-18	The complexity that seems to be required to configure all the components to be deployed, and all the rules that should be applied.
➥	Complexity should be mitigated by usability (configuration and deployment)
NCO-19	Not so clear why the blockchain is used and what benefits it really brings to the project with respect to other solutions
➥	Experimental use of Blockchain technology adopted for compliance with DoA, justifications included in D5.1 (resubmitted)
NCO-20	The problem of monitoring in real-time IoT end-devices, due to their limited networking and processing capabilities.
➥	Real-time monitoring and control (for attack mitigation purposes) of IoT devices should be supported
NCO-21	The GUIs can be improved a bit to be more effective.
➥	Usability should be generally addressed and improved (all GUI, DSPS included)

3.1.2 Specific validation and evaluation (SVE)

3.1.2.1 SVE1 – Dynamic Security and Privacy Seal

► **D6.3 conclusions:** *"For the DSPS evaluation, the results indicate that end-users are partially satisfied with the web user interface and reporting indicators. Moreover, the end-users are neutral with the use of blockchain in the DSPS management and are partially disagreed that the DSPS is too complex."*

Results of Specific Questions about DSPS Module	MEAN	DEVIATION
1. DSPS based on blockchain makes you feel more protected	3,511	1,0128034
2. Web user interface of DSPS is easy to understand	4,239	0,8981518
3. DSPS is too complex to be fully appreciated	2,457	1,0286712
4. DSPS provides a powerful reporting about real-time indicators	4,084	0,6603119

➥	Usability should be generally addressed and improved (DSPS included)

3.1.2.2 SVE2 – Use Case BMS.2: Insider Attack on the Fire Suppression System

► **D6.3 conclusions:** *"According to the evaluation of BMS.2 use case, the next table indicates that end-users are partially agreed with the protection provided by secure bootstrapping and distributed access control of IoT resources. Moreover, end-users are partially satisfied with the ANASTACIA components such as Kafka broker, Security Alert Service and SDN/NVF Controllers."*

Results of Specific Questions about BMS.2 Use Case	**MEAN**	**DEVIATION**
1. Network authentication using secure bootstrapping makes you feel more protected	3,867	1,1171463
2. Distributed access control for IoT resources makes you feel more protected	3,663	0,9864918
3. Kafka broker of monitoring module provides alert information that is easy to understand	3,679	0,9603531
4. Security alert service of reaction module provides a powerful reporting	3,881	0,7382432
5. Mitigations actions managed by the Security Orchestrator are too complex	2,998	1,0572622
6. IoT network simulation and traffic forwarding by SDN/NVF Controllers are useful countermeasures	4,201	0,9525338

➥ Usability should be improved (Security Orchestrator UI/console)

3.1.2.3 SVE3 – Use Case BMS.3: Remote Attack on the Building Energy Microgrid

► **D6.3 conclusions:** *"Regarding the evaluation of BMS.3 use case, the results show that end-users are partially agreed with Deep Packet Inspection for SQL-injection detection, XL-SIEM tool for Incident Detector and Traffic filtering as countermeasure. The end-users indicate its neutral opinion about the understandable console of Mitigation Action Service and the complexity of Security Orchestrator."*

Results of Specific Questions about BMS.3 Use Case	**MEAN**	**DEVIATION**
1. The attack of SQL injection included in COAP message is easy to understand	3,701	1,1048542
2. Deep Packet Inspection of monitoring module is a powerful tool to detect a SQL injection attack	4,02	0,8902943
3. XIEM-tool of monitoring module provides SQL alert notification that is easy to understand	3,755	0,8712932
4. The log console of Mitigation Action Service is enough to understand what is happening	3,509	0,8795386
5. Mitigations actions managed by the Security Orchestrator are too complex to be fully appreciated	2,79	1,0413221
6. Traffic filtering by SDN/NVF Controllers is a useful countermeasure	4,318	0,8407218

➥ Usability should be improved (Mitigation Action Service and Security Orchestrator UI/console)

3.1.2.4 SVE4 – Use Case BMS.4: Cascade Attack on a Megatall Building

► **D6.3 conclusions:** *"According to the evaluation of BMS.4 use case, the next table indicates that end-users are partially satisfied with the ANASTACIA components such as Data Analysis Agent based on machine learning, Kafka Broker of Monitoring Module and Security Alert Service for threat reporting. Moreover, the end-users express their neutral position for the complexity of Security Orchestrator."*

Results of Specific Questions about BMS.4 Use Case	**MEAN**	**DEVIATION**
1. The attack of temperature sensor manipulation is easy to understand	4,068	0,9998606
2. Data Analysis based on Machine learning is a powerful tool to detect data manipulation	3,939	0,8992535
3. Kafka-broker of monitoring module provides alert notification that is easy to understand	3,939	0,8154375
4. Security alert service provides a powerful reporting about the threat detection	3,937	0,6584405
5. Mitigations actions managed by the Security Orchestrator are too complex to be fully appreciated	2,83	1,0534558
6. The enforcement of turning off the sensor device by IoT controller is a useful countermeasure	3,893	1,0255922

➥ Usability should be improved (Security Orchestrator UI/console)

3.1.2.5 SVE5 – Use Case MEC.3: DoS/DDoS Attacks using IoT Devices

► **D6.3 conclusions:** *"Regarding the evaluation of MEC.3 use case, the next results show that end-users are partially agreed with Deep Packet Inspection for DDoS detection, XL-SIEM tool for Incident Detector and Traffic filtering as countermeasure. The complexity of mitigation actions managed by Security Orchestrator is considered neutral by the end-users."*

Results of Specific Questions about MEC.3 Use Case	MEAN	DEVIATION
1. The attack of DDoS generated by the network simulation with ICMP messages is easy to understand	4,164	1,1493945
2. Deep Packet Inspection for monitoring module is a powerful tool to detect DDoS attacks	4,002	0,9694761
3. XIEM-tool of monitoring module provides DDoS alert notification that is easy to understand	3,761	0,8666695
4. Security alert service provides a powerful reporting about the threat detection	3,96	0,8475656
5. Mitigations actions managed by the Security Orchestrator are too complex to be fully appreciated	2,817	1,1139065
6. The filtering the ICMP traffic from the sensor network by SDN controller is a useful countermeasure	4,198	0,8714848

➥ Usability should be improved (Security Orchestrator UI/console)

3.2 White Paper (WP)

This section includes a reasoned review of the ANASTACIA White Paper (issued upon EC's request on January 2019) in terms of impact on initial requirements (see D1.2) and of definition of new additional requirements.

3.2.1 Reference Scenario (RF)

The heterogeneous, distributed, and dynamically evolving nature of **Cyber Physical Systems (CPS) based on Internet of Things (IoT) and virtualised cloud architectures** introduces new and unexpected risks that cannot be solved by current state-of-the-art cyber-security solutions. A **huge number of interconnected smart devices** is drastically changing industrial and home environments by enabling new advanced services for human-beings: the IoT vision aims at seamlessly integrating the **sensing and actuation features** of common objects by leveraging their **network capabilities** to create **pervasive information systems**. To this aim, the sensing measurements generated by IoT devices can provide **contextual and valuable information** of the surrounding environments. The relevant data analysis systems can then derive appropriate **control and security decision**, which can be enforced in the physical world through the **actuation features of smart devices**. The envisioned benefits are boosting the adoption of IoT solutions in a broad range of application scenarios.

On the other hand, the increased connectivity can be exploited by malicious attackers to exploit **devices vulnerabilities**. Indeed, accounting for the **heterogeneity of IoT devices**, ranging from smart industrial machinery to simple wearable sensors, it results extremely complex to ensure the same desired **protection over different programming environments**. New zero-day (0-day) vulnerabilities and new types of attacks – such as Slow DoS Attacks (SDA) – are emerging and require a **holistic security management approach**. However, most host-centric security mechanisms do not typically fit into the resource constraints of IoT devices and networks neither properly exploit **SDN/NFV and monitoring technologies**. The absence of automated software updates, as well as misconfiguration, can notably increase the potential vulnerabilities, especially due to the unavailability of vendors' support along the whole IoT product lifecycle. **Cyber-attacks on IoT operations** are widespread because of increased internet-connectivity of equipment and devices in smart distributed deployments, such as Smart Building services. Against waves of emerging and adapting threat patterns, effective security configuration for building automation systems is beyond manual analysis or human ability. Moreover, current network security solutions present low responsiveness and can unlikely cope with the dynamic IoT environments. All these security vectors claim for new advanced mechanisms able to meet the desired defence levels.

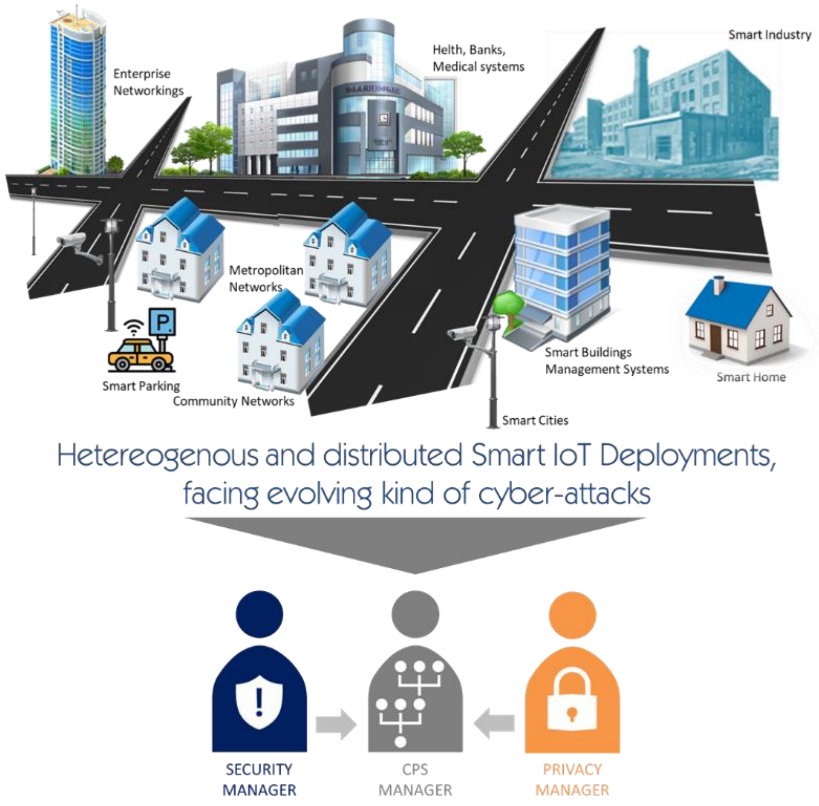

Enterprise Networkings
Helth, Banks, Medical systems
Smart Industry
Metropolitan Networks
Smart Parking
Community Networks
Smart Buildings Management Systems
Smart Home
Smart Cities
Hetereogenous and distributed Smart IoT Deployments, facing evolving kind of cyber-attacks
SECURITY MANAGER
CPS MANAGER
PRIVACY MANAGER

Figure 7. ANASTACIA main reference scenario.

New **context-aware security frameworks** are therefore needed to allow orchestrating **NFV managers, SDN controllers and IoT controllers**, thereby providing security chaining, as well as dynamic reconfiguration and adaptation of the virtual security appliances, according to monitoring and DSSs. **Virtual Network Security Functions** (vNSF) can be timely and dynamically deployed at the edge in **virtualized and softwarized entities**, to rule the security in IoT networks. Dynamic provisioning of virtual security functions towards the edge of the network can enhance scalability, necessary to deal with the huge IoT traffic.

The deployment of **Network Security Functions (NSF)** have been already successfully studied and addressed in IoT networks. However, those NSFs have not been yet properly studied and exploited in NFV/SDN-enabled IoT networks, where cyber-situational and policy-based security frameworks can be dynamically orchestrated reacting and mitigating cyber-attacks by deploying timely and wisely, in the proper location, the suitable vNSF.

In this context, **ANASTACIA is developing new methodologies, frameworks and support tools that will offer resilience to distributed smart IoT systems and scenarios against cyber-attacks, by leveraging SDN and NFV technologies**. Summarizing:

- ANASTACIA addresses the security management of distributed IoT scenarios, such as Smart Buildings or Smart Cities, that can benefit from policy-based orchestration and management approach, NFV/SDN-based solutions and novel monitoring and reaction tools to cope with new kind of cyber-attacks

➥	Policy orchestration should be efficiently managed (see policy conflist detection, policy dependencies, etc.)
➥	Usability should be improved (non-technical users/CPS managers)

- Security VNFs can be timely and dynamically orchestrated through policies to deal with heterogeneity demanded by these distributed IoT deployments, that can be deployed either at the core of at the edge, in VNF entities, in order to rule the security in IoT networks

➥	Policy orchestration should be efficiently managed (see policy conflict detection, policy dependencies, etc.)

- Dynamic and reactive provisioning of security VNFs towards the edge of the network can enhance scalability, necessary to deal with IoT scenarios

➥	Scalability should be addressed and improved (dynamic and reactive provisioning of security VNFs towards the edge of the network)

3.2.2 Research Challenges (RC)

3.2.2.1 RC1 – Interoperable and scalable IoT security management

The definition of security policies to deal with IoT heterogeneity and interoperability across IoT domains introduces several challenges related to the security models, the language and the level of abstraction. Thus, contextual IoT aspects in policies, particularities in IoT security models, policy conflicts and dependencies in orchestration policies are open research challenges that need to be solved.

➥	Policy orchestration should be efficiently managed (see detection, dependencies, etc.)

3.2.2.2 RC2 – Optimal selection of SDN/NFV-based security mechanisms

The current defence of network operators and companies is mainly based on hardware appliances. Naturally, the hardware appliances have fixed location that has to be chosen by the ISP smartly. These hardware appliances can be deployed on-premises or outsourced, and the packets/flows are redirected to these hardware appliances. Besides, some vendors are better in some attack defence such as DDoS attack or detection as DPI and others can be better for another type of attack. Moreover, these hardware appliances have a limited capacity and hence can handle a limited volume of traffic/data. As an example, for the DDoS case with a hardware of 10 Gbps DDoS defence appliance, each attack with a volume higher than this capacity cannot be handled by the defence appliance. In contrary, using the virtualization enabled by SDN and NFV allows a quick instantiation of VMs in the adequate location. Indeed, this lack of elasticity can be easily handled by VNF functions that can be chained and placed on-demand according to the incoming attacks. However, it is challenging to allocate multiple VNF requests on an NFV Infrastructure, especially in a cost-driven objective. Moreover, depending on their type and isolation considerations, VNFs can be potentially shared among several Service Function Chainings (SFC), as an example. Finally, VNFs must not be placed far from the shortest path to avoid increasing delay and network usage. The ANASTACIA project tries to answer these challenging issues.

➥	Optimal selection criteria for SDN/NFV-based security mechanisms should be defined, implemented and included in mitigation plans for proper enforcement

3.2.2.3 RC3 – Orchestration of SDN/NFV-based security solutions for IoT environments

The selection of the adequate mitigation plan and the fast enforcement of the defined policies are very challenging processes that require a lot of efforts and time. The orchestration and the enforcement of the adequate countermeasures in a short time, and without affecting the Quality of Service (QoS), introduce several challenges that must be duly considered. Also, the definition and enforcement of mitigation plans while reducing the deployment cost and by taking into account the limitations in existing infrastructure clouds are open research questions that should be addressed.

> ➥ Orchestration of SDN/NFV-based security mechanism should be ensured to support the security of complex/distributed IoT environments

3.2.2.4 RC4 – Dealing with new kind of cyber-attacks in IoT

The identification of novel types of attacks exploiting IoT networks and sensors (and the consequent protection approaches to provide advanced security from last generation threats) is also tackled by research activities carried out by the project.

> ➥ Novel types of attack should be mitigated

3.2.2.5 RC5 – Learning Decision Model for Detecting Malicious Activities

In the cyber physical world, the attacker's goal is to disrupt both the normal operations of the CPS, e.g., sensor readings, safety limits violation, status reports, safety compliance violation etc. and communication flows among devices. The continued rise of cyber-attacks together with the evolving skills of the attackers, and inefficiency of the traditional security algorithms to defend against advanced and sophisticated attacks such as DDoS, slow DoS and zero-day, necessitate the development of novel defense and resilient detection techniques. We propose an approach for learning a constraint-programming based decision model by learning a set of constraints/relations from the data that conjunctively defines both the normal operations and communication flows of a CPS. The malicious operations are detected when CPS fails to abide by the learnt decision model.

> ➥ Advanced Decision Models should be included in the Monitoring Plane to detect malicious activities and potential risks/attacks

3.2.2.6 RC6 – Hybrid IoT Security Monitoring enhanced with event correlation

Security in IoT networks introduces challenges due the restrictions of the devices. The application of both signature-based and behavioural-based security analysis for IoT networks provides an initial security level. ANASTACIA goes even beyond this point by correlating both types of events to detect hidden relations and thus identify potential threats.

> ➥ Advanced reasoning capabilities should be developed and included in the Monitoring Plane to leverage event correlation and enhance IoT security

3.2.2.7 RC7 – Quantitative evaluation of incidents for mitigation support

In ANASTACIA, incident detection is supported by a quantitative evaluation of incidents that combines several factors (incident severity, criticality of assets affected, global risk associated to the incident or cost of potential mitigations among others) to decide on the most convenient mitigation plan to enforce.

> ➥ Advanced reasoning capabilities should be developed and included in the Reaction Plane by quantitatively evaluating risks/attacks and define appropriate mitigation plans

3.2.2.8 RC8 – Developing a Dynamic Security and Privacy Seal which secures both organizational and technical data

The DSPS seeks to generate trust in the system by showcasing both the technical insights obtained from ANASTACIA on security and privacy and the wider security and personal data protection requirements that might be of relevance to the organization. To do so, the key challenge to be overcome by the system relates to the need to integrate the end-user (CISO and DPO) in the seal creation process. The DSPS will enhance the alerts generated by ANASTACIA's monitoring and reaction planes with direct technical and organizational feedback (such as Data Protection Impact Assessments or post-alert internal security audit results) from the end-user, which will be securely stored and linked to the seal to generate non-repudiable, legally valid proof of due-diligence and compliance with legal or contractual requirements.

➥	Organizational and technical information should be duly secured Support to accountability should be addressed and implemented (as for compliance with GDPR, with a focus on DPIA activities and on non-repudiable proof)

3.2.3 Key Innovations (KI)

The Research Challenges (RC) introduced in the Section before have been duly translated into a set of 8 Key Innovations (KI) proposed by the ANASTACIA project to stress its research nature and to support ambitious demonstration use cases (see Figure 8).

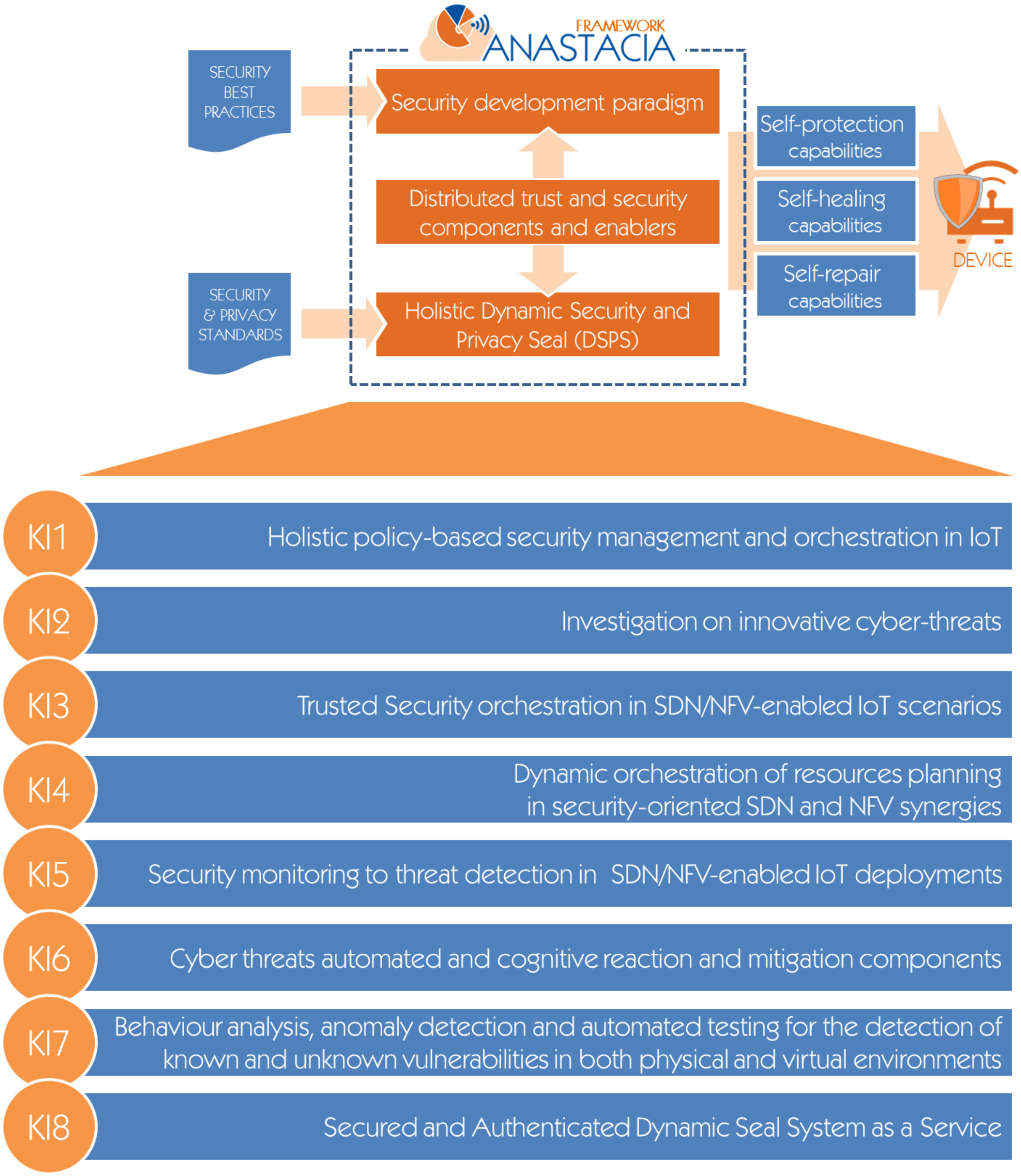

FRAMEWORK
ANASTACIA
SECURITY BEST PRACTICES
SECURITY & PRIVACY STANDARDS
Security development paradigm
Distributed trust and security components and enablers
Holistic Dynamic Security and Privacy Seal (DSPS)
Self-protection capabilities
Self-healing capabilities
Self-repair capabilities
DEVICE
KI1
Holistic policy-based security management and orchestration in IoT
KI2
Investigation on innovative cyber-threats
KI3
Trusted Security orchestration in SDN/NFV-enabled IoT scenarios
KI4
Dynamic orchestration of resources planning in security-oriented SDN and NFV synergies
KI5
Security monitoring to threat detection in SDN/NFV-enabled IoT deployments
KI6
Cyber threats automated and cognitive reaction and mitigation components
KI7
Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments
KI8
Secured and Authenticated Dynamic Seal System as a Service

Figure 8. Main Key Innovation supporting the ANASTACIA framework.

The following sections include the description of the proposed Key Innovations (as originally proposed in the ANASTACIA White Paper) and derive accordingly a set of additional/complementary requirements.

3.2.3.1 KI1 – Holistic policy-based security management and orchestration in IoT

In distributed smart IoT deployments scenarios […], the system security management is crucial. At this point, it is important to highlight that to the diversity of the current systems and services they are added a vast amount of different devices in the IoT domain, being the latter quite different among the previous approach and even among themselves. From this point of view, the current state of art shows that it is highly valuable to provide different levels of security policies to provide different levels of abstraction for different profiles of management. It is also important to highlight the difference between generic models and specific extensible models, as well as to remark then relevance of policy orchestration features and policy conflict detection. Main ANASTACIA's contributions on policies reside in the unification of relevant, new and extended capability-based security policy models (including Event-Condition-Action, ECA features), as well as policy orchestration and conflict detection mechanisms, all under a unique policy framework. To this aim, the holistic policy-based solution provides different components and features like **Policy Models**, **Policy Editor Tool**, **Policy Repository**, **Policy Interpreter**, **Policy Conflict Detection** and **Policy for Orchestration**.

ANASTACIA´s **Policy Models** thus improve the current state of the art as well as provide novelty approaches to be able to increase the security measures and countermeasures in the whole system at different levels. To this aim, ANASTACIA adopts and extend concepts and features from the state of art, to provide a unified security policy framework. I.e., ANASTACIA involves and evolves previous works by extending the already existing features as well as by providing new IoT-focused features.

The Policy Models can be instantiated by using the **Policy Editor Tool** which allows defining security policies at a high-level of abstraction through a friendly GUI. In this way, the security administrator is able to manage the security of the system by instantiating new security policies, as well as supervise the existing security policies by the Policy Repository. **The Policy Repository** registers all policy operations as well as the current status for each one. It also provides valuable policy templates to make the security management easier.

Since the security policies are instantiated in a High-level Security Policy Language (HSPL), it must be transformed in configurations for the specific devices which will enforce the security policy. To this aim, the **Policy Interpreter** is able to refine the HSPL in one or several Medium-level Security Policy Language (MSPL) policies depending on a set of identified capabilities (filtering, forwarding, etc.). This process transforms the high-level concepts into more detailed parameters but still independent to the specific technologies. Finally, these MSPL policies are translated in final configurations by using specific translator plugins for each technology. Once the configurations have been obtained, they can be enforced in the specific security enablers, understanding a security enabler as a piece of hardware or software able to implement a specific capability. Of course, a security policy only can be enforced if it does not present any kind of conflict with the already enforced ones. In this sense, the **Policy Conflict Detection** engine verifies that the new security policy will not generate conflicts like redundancy, priorities, duties (e.g. packet inspection vs channel protection), dependences or contradictions. To this aim, the security policy is processed against the rule engine which extracts context information from the policy repository and the system model to perform the necessary verifications.

Regarding the dependences, ANASTACIA also includes as part of the policy model the Policy for Orchestration concept. The **Policy for Orchestration** model allows the security administrator to specify how a set of security policies must be enforced by defining priorities and dependencies, where a security policy can depend on other security policies or even in system events like an authentication success.

Through these components and features, the policy-based ANASTACIA framework aims to cope with research challenges related with interoperability and scalability IoT security management. That is, the policy-based approach aims to deal with the heterogeneity and scalability by defining different level of abstractions, models and translation plugins. In this way, the scalability is also benefited since the policy-based approach with a high-level of abstraction makes easier to manage a large amount of devices. The policy conflict detection allows the framework to deal with several conflict types, and finally the policy for orchestration considers policy chaining by priority or dependencies in order to cover an orchestration plan.

Currently, the project is validating the related components and features by experimenting on IoT/SDN/NFV Proof of Concepts for different security capabilities like authentication, authorization and accounting (AAA), filtering, IoT management, IoT-honeynet and channel protection as it can be seen in the research outcomes.

Regarding the research outcomes and associated publications, [Zarca, 2018-1] provides a first PoC performance evaluation focused on a sensor isolation through different SDN controllers as well as a traditional firewall approach. [Zarca, 2018-2] shows the potential of the policy-based framework focused on an AAA scenario whose results are provided in [Zarca, 2019]. “Virtual IoT HoneyNets to mitigate cyber-attacks in SDN/NFV-enabled IoT networks” (paper under review) shows the dynamic deployments of IoT-honeynet networks on demand by replicating real IoT environments by instantiating the ANASTACIA IoT-honeynet policy model. It also provides performance for different kind of IoT devices and topologies. “Security Management Architecture for NFV/SDN-aware IoT Systems” [Zarca et al., 2019] shows the ANASTACIA architecture and focuses on the reaction performance of the policy-based framework.

➥	**MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS** • Extend and improve policy models and management, to support: ○ Monitoring Policies ○ Data-privacy Policies ○ Policy for Orchestration ○ Policy conflict detection (rule engine) • Implement/validate associated data-privacy enablers • Policy definition and refinement for the envisaged use cases

3.2.3.2 KI2 – Investigation on innovative cyber-threats

The CNR team involved in ANASTACIA has multi-year experience in the cyber-security field, concerning both the development of innovative cyber-attacks and intrusion detection algorithms. By exploiting the knowledge of the team, in the ANASTACIA context, deep work has been accomplished in the cyber-security context. Such work led to the identification of two innovative threats, related to the IoT and Slow DoS Attacks contexts. The novelty of such threats is demonstrated by their acceptance from the research world [Cambiaso, 2017; Vaccari, 2017]. In the following, based our description on the published works just mentioned and on the description reported in the project deliverables, the introduced new attacks are briefly described (how they work and how it is possible to protect from them).

3.2.3.2.1 IoT 0-Day attack

Being exchanged information extremely sensitive, due to the nature of IoT devices and networks, security of IoT systems is a topic to be investigated in deep. The work behind the proposed attack goes in this direction, by investigating the domotic IoT context and exploiting its components, in order to identify weaknesses that attackers may exploit.

The proposed attack is part of the ZigBee security context. ZigBee is a wireless standard introduced by the ZigBee Alliance in 2004 and based on the IEEE 802.15.4 standard, used in the Wireless Personal Area Networks (WPAN) context [Ramya, 2011]. In particular, we identified a particular vulnerability affecting AT Commands capabilities implemented in IoT sensor networks. Our work focuses on the exploitation of such weakness on XBee devices, supporting remote AT commands, exploited to disconnect an end-device from the ZigBee network and make it join a different (malicious) network and hence forward potentially sensitive data to third malicious parties. Given the nature of IoT end-devices, often associated with a critical data and operations, it may be obvious how a Remote AT Command attack represents a serious threat for the entire infrastructure. Early evaluation of the effects of the proposed attack on a real network led to validate the success of the proposed threat [Vaccari, 2017]. Obtained results prove the efficacy of the proposed attack. Moreover, since just a single packet is sent to the victim by the attacker to reconfigure it, the proposed attack should be considered as dangerous as scalable. Particularly, the time required to send such packet is minimal, so in case of multiple targeted sensors, the attack success is guaranteed.

By adopting an external level protection approach [Vaccari, 2017], the protection system is directly employed on the nodes, since agents implemented on the IoT devices are responsible for monitoring the device status and verifying that all the parameters are correct. In case the device is affected by a remote AT reconfiguration command attack, such alert information is forwarded to the IoT coordinator, and the device is designed to mitigate the attack (by autonomously reconfiguring itself, as previously described). Since not all the devices may embed a detection and mitigation system, the IoT coordinator is also supposed to monitor devices status periodically to identify disconnections, hence report them to the other ANASTACIA modules.

3.2.3.2.2 Slow DoS Attacks

Among all the methodologies used to successfully execute malicious cyber-operations, DoS attacks are executed with the aim of exhaust victim's resources, compromising the targeted systems' availability, thus affecting availability and reliability for legitimate users. These threats are particularly dangerous, since they can cause significant disruption on network-based systems [Beitollahi, 2011]. The term Slow DoS Attack, coined by the CNR research group involved in the project, concerns a DoS attack which makes use of low-bandwidth rate to accomplish its purpose. An SDA often acts at the application layer of the Internet protocol stack because the characteristics of this layer are easier to exploit to successfully attack a victim even by sending it few bytes of malicious requests [Cambiaso, 2012]. Moreover, under an SDA, an ON-OFF behavior may be adopted by the attacker [Cambiaso, 2013], which comprises a succession of consecutive periods composed of an interval of inactivity (called off-time), followed by an interval of activity (called on-time).

The innovative attack proposed is called SlowComm [Cambiaso, 2013], sending a large amount of slow (and endless) requests to the server, saturating the available connections at the application layer on the server inducing it to wait for the (never sent) completion of the requests. As an example, we refer to the HTTP protocol, where the characters sequence `\r\n\r\n` represent the end of the request: SlowComm never sends such characters, hence forcing the server to an endless wait. Additionally, during a SlowComm the request payload is sent abnormally slowly. Similar behavior could be adopted for other protocols as well (SMTP, FTP, etc.). As a consequence, by applying this behavior to a large amount of connections with the victim, a DoS may be reached. In particular, SlowComm works by creating a set of predefined connections with the victim host. For each connection, a specific payload message is sent (the payload is typically endless), one character at time (one single character per packet), by making use of the Wait Timeout [Cambiaso, 2012] to delay the sending. In this way, once the connection is established with the server (at the transport layer), a single character is sent (hence, establishing/seizing the connection at the application layer, hence, with the listening daemon). At this point, the Wait Timeout is triggered, in order to delay the sending of the remaining payload, and to prevent server-side connection closures. During our work we proved how the attack may successfully lead a DoS to different popular TCP based services [Cambiaso, 2017], hence proving that the attack is particularly dangerous.

To protect from SlowComm and Slow DoS Attacks in general, it is important to consider the following fact: *it is trivial to detect and mitigate a single attacking host, while it is extremely difficult to identify a distributed attack*. This fact derives from the fact that IP address filtering may be applied to detect and mitigate a SlowComm attack (see, for instance, our tests on `mod-security` [Cambiaso, 2017]), while in case of a distributed attack this concept may not be adopted with ease. Moreover, from the stealth perspective, the proposed attack is particularly difficult to detect while it is active, since log files on the server are often updated only when a complete request is received or a connection is closed: being our requests typically endless, during the attack log files do not contain any trace of attack. Therefore, different approaches should be adopted, for instance based on statistic [Aiello, 2013], machine learning [Katkar, 2015; Duravkin, 2014; Singh, 2015], or spectral analysis [Brynielsson, 2015]. A possible approach to adopt combines the algorithm proposed in [Aiello, 2013] and the methodology proposed in [Cambiaso, 2016] to detect running SlowComm attacks. Early version of the algorithms has been tested in laboratory, while testing on relevant environments has not been accomplished to date. Concerning the ANASTACIA platform, further work on the topic will be focused on evaluating a possible implementation of such approach, aimed to provide protection from Slow DoS Attacks by embedding innovative anomaly-based intrusion detection algorithms in a relevant environment and providing additional capabilities to the ANASTACIA framework, in the context of cyber-security applied to counter last generation threats.

MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS

- Investigate IoT network systems based on the ZigBee protocol
- Discover novel attacks exploiting XBee modules
- Propose and integrate new protection approach against the Zero-day and slow DoS attacks
- Adopt and adapt existent algorithms (by CNR, validated in laboratory) to provide protection capabilities

3.2.3.3 KI3 – Trusted Security orchestration in SDN/NFV-enabled IoT scenarios

In the ANASTACIA architecture, the security orchestrator oversees orchestrating the security enablers according to the defined security policies. The later would be generated either by the end-user or received from the monitoring and reaction plane. The security orchestration plane, through its components security orchestrator, security resource planning and policy interpreter, is able to coordinate the policies and security enables to cover the security configuration needed for different communications happen in the network. The security orchestration plane takes into account the policies requirements and the available resources in the underlying infrastructure in order to mitigate the different attacks while reducing the expected mitigation cost and without affecting the QoS requirements of different verticals. The resources in the underlying infrastructure refer to the available amount of resources in terms of CPU, RAM, and storage in different cloud providers, as well as the bandwidth communication between these network clouds.

Figure 3 depicts the main architecture of the security orchestration and enforcement plane suggested in ANASTACIA. Using SDN network, the IoT domain is connected to the cloud domain, whereby different IoT services are running. The user accesses the IoT devices, first, through the cloud domain, then the SDN enabled network and the IoT router. In fact, in ANASTACIA, the communication between a user and an IoT device happens through a chain of virtual network functions (VNFs) named service function chaining (SFC). The latter consists of three parts:

i) the ingress point, which is the first VNF in the SFC. The user initially attaches to the ingress point;

ii) The intermediate VNFs;

iii) the egress point, which is the last VNF in the SFC. The egress point should be connected to the IoT controller. As depicted in Figure 3, the order of the communications between the VNFs is defined according to the different SDN rules enforced thanks to the SDN controller. The nature and the size of the SFC would be defined according to the nature of the user (a normal or a suspicious).

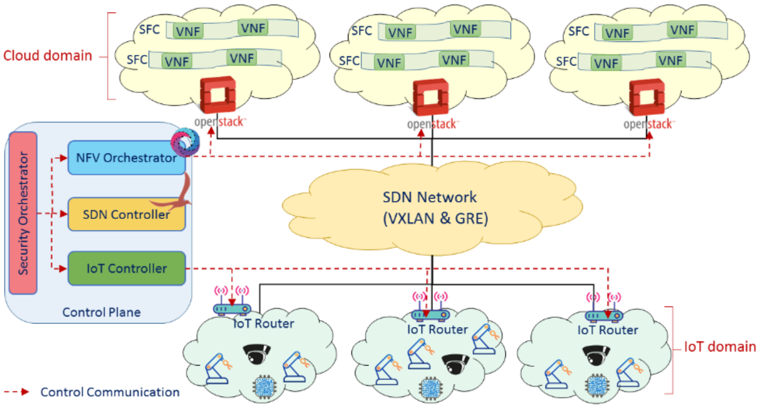
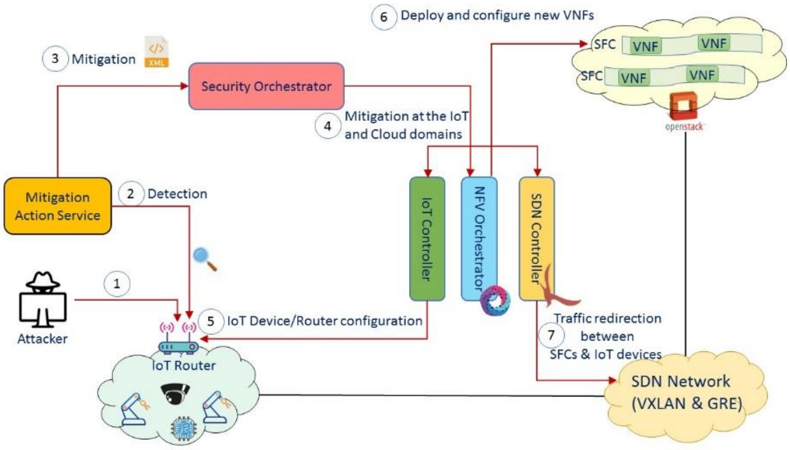


Figure 3. Security orchestration plane.

Figure 4 depicts the different steps of the orchestration and enforcement plane suggested in ANASTACIA. The attack is detected thanks to the Mitigation Action Service (MAS) component. The later sends a mitigation request (MSPL file) to the security orchestrator (Fig. 4, Step 3). To mitigate the attacks, the security orchestrator interacts with three main actors, which are (Fig. 4, Step 4):

- **IoT controller:** It provides IoT command and control at high-level of abstraction in independent way of the underlying technologies. That is, it is able to carry out the IoT management requests through different IoT constrain protocols like CoAP or MQTT. It also maintains a registry of relevant information of the deployed IoT devices like the IoT device properties and available operations. Since it knows the IoT devices status, it could be able to perform an effective communication in order to avoid the IoT network saturation when it is required a high-scale command and control operation. In “Security Management Architecture for NFV/SDN-aware IoT Systems” (Under review) can be found an example and performance of IoT management as part of a building management system. In order to mitigate different attacks, the security orchestrator interacts with the IoT controller in order to mitigate the attacks at the level of the IoT domain and prevent the propagation of the attack to other networks (Fig. 4: 4). The IoT controller enforce different security rules at the IoT router (data plane) to mitigate the attack (Fig. 4: 5).



6 Deploy and configure new VNFs
3 Mitigation
XML
Security Orchestrator
SFC
VNF
openstack
4 Mitigation at the IoT and Cloud domains
Mitigation Action Service
2 Detection
IoT Controller
NFV Orchestrator
SDN Controller
1
Attacker
5 IoT Device/Router configuration
7 Traffic redirection between SFCs & IoT devices
IoT Router
SDN Network
(VXLAN & GRE)

Figure 4. Security orchestration and enforcement in case of a reactive scenario.

- **NFV orchestrator**: In ANASTACIA, in order to ensure efficient management of SFC, we have integrated SDN controller (ONOS) with the used Virtual Infrastructure Manager (VIM), in our case OpenStack. The integration of SDN with the VIM enable the smooth communication between different VNFs that form the same SFC. After receiving the MSPL message from the MAS, the security orchestrator identifies the right mitigation plane should be implemented. If the mitigation plan requires the instantiation of new VNFs, the security orchestrator instructs the NFV orchestrator to instantiate and configure the required VNFs. In order to instantiate the required VNFs, the NFV orchestrator interacts with the VIM (Fig. 4: 6). Also, the security orchestrator interacts with the policy interpreter to translate the received MSPL to the low configuration (LSPL) needed for different VNFs. After the successful instantiation of a security VNF, the security orchestrator configures that VNF with the received LSPL (Fig. 4: 6).
  In ANASTACIA, we have also developed different virtual security enablers that should be instantiated to mitigate the different attacks. For instance, we have developed a new VNF firewall based on SDN-enabled switch and OpenFlow. OVS-Firewall is a newly developed solution that relies on OpenFlow protocol in order to create a sophisticated firewalling system. We have also proposed and developed a new security VNF, named virtual IoT-honeynet, that allows to replicate a real IoT environment in a virtual one by simulating the IoT devices with their real deployed firmware, as well as the physical location. The IoT-honeynet can be represented by an IoT-honeynet security policy, and the final configuration can be deployed transparently on demand with the support of the SDN network. “Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks” (Under review) shows the potential and performance of this approach.

- **SDN controller:** This component helps to reroute the traffic between the VNFs in different SFCs. As depicted in Fig. 4, when the mitigation action service notifies the orchestrator about an attack, the SFC would be updated by adding/inserting new security VNFs in the SFCs. The security orchestrator should push the adequate SDN rules to reroute the traffic between different VNFs in the SFC and the IoT domain (Fig. 4: 7). Also, according to the different situations, the security orchestrator can choose the SDN as security enabler. In this case, it can be the attack mitigated by pushing exploring the strength of the SDN technology. If so, the security orchestrator can instruct the SDN controller to push some SDN rules to prevent, allow or limit the communication on specified protocols and ports between different communication peers (Fig. 4: 7).

By relying in the aforementioned orchestration properties and features, as well as the SDN and IoT controllers, the ANASTACIA framework aims to cope with the research challenges related with Orchestration of SDN/NFV-based security solutions for IoT environments and currently several experiments have been carried out in different security areas.

For instance, several experiments have been carried out regarding **virtual IoT-honeynets**. This kind of VNF allows to replicate a real IoT environment in a virtual one by simulating the IoT devices with their real deployed firmware, as well as the physical location.

Furthermore, the security orchestration of ANASTACIA enables continuous and dynamic management of AAA as well as Channel Protection virtual security functions in IoT networks enabled with SDN/NFV controllers. Our scientific paper [Zarca, 2019] called “Enabling virtual AAA management in SDN-based IoT networks” shows how a virtual AAA is deployed as VNF dynamically at the edge, to enable scalable device's bootstrapping and managing the access control of IoT devices to the network. Besides, our solution allows distributing dynamically the necessary crypto-keys for IoT M2M communications and deploy virtual Channel-protection proxies as VNFs, with the aim of establishing secure tunnels (e.g. through DTLs) among IoT devices and services, according to the contextual decisions inferred by the cognitive framework. The solution was implemented and evaluated, demonstrating its feasibility to manage dynamically AAA and channel protection in SDN/NFV-enabled IoT scenarios.

A telco cloud environment may consist of multiple VNFs that can be shipped and provided, in the form virtual machine (VM) images, from different vendors. These VNF images will contain highly sensitive data that should not be manipulated by unauthorized users. Moreover, the manipulation of these VNF images by unauthorized users can be a threat that can affect the whole system setup. In ANASTACIA, we have designed and developed different tools to prevent the manipulation of different VNF images should run on top of different network clouds. In ANASTACIA, we have devised efficient methods that verify the integrity of physical machines before using them and also the integrity of virtual machine and virtual network function images before launching them [AALTO: 1, 2, 3]. For this purpose, different technologies have been investigated, such as i) Trusted Platform Module (TPM); ii) Linux Volume Management (LVM); iii) Linux Unified Key Setup (LUKS). For instance, in [AALTO: 2], we have provided a trusted cloud platform that consists of the following components:

1) TPM module that is used to store passwords, cryptographic keys, certificates, and other sensitive information. TPM contains platform configuration registers (PCRs) which can be used to store cryptographic hash measurements of the system's critical components. There are in total 24 platform configuration registers (PCRs) in most TPM modules starting from 0 till 23.
2) Trusted boot module, which is an open source tool, uses Intel's trusted execution technology (TXT) to perform the measured boot of the system. Trusted boot process starts when trust boot is launched as an executable and measures all the binaries of the system components (i.e., firmware code, BIOS, OS kernel and hypervisor code). Trust boot then writes these hash measurements in TPM's secure storage.
3) Remote attestation service, which is the process of verifying the boot time integrity of the remote hosts. It is a software mechanism integrated with TPM, to securely attest the trust state of the remote hosts. It uses boot time measurements of the system components such as BIOS, OS, and hypervisor, and stores the known good configuration of the host machine in its white list database. It then queries the remote host's TPM module to fetch its current PCR measurements. After receiving the current PCR values, it compares them against its white list values to derive the final trust state of the remote host.
4) OpenStack Resource Selection Filters component that should be integrated with the nova-scheduler. -In OpenStack, when a VNF is launched, the nova-scheduler filters pass through each host and select the number of hosts that satisfy the given criteria. Each filter passes the list of selected hosts to the proceeding filter. When the last filter is processed, OpenStack's default filter scheduler performs a weighing mechanism. It assigns weight to each of the selected hosts depending on the RAM, CPU and any other custom criteria to select a host which is most suitable to launch the VM instance.

MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS

- Design and develop efficient SFC routing algorithm to ensure security and QoS
- Enable orchestration to be also driven by policy conflict detection
  - Design and develop efficient SFC life cycle management that takes into account policy conflict and ensures QoS
- Design and develop new smart algorithm that helps the Security Orchestrator to make the optimal decisions for placing the VNFs.

3.2.3.4 KI4 – Dynamic orchestration of resources planning in Security-oriented SDN and NFV synergies

Network operators are facing different type of attacks that introduce new set of challenges to detect and to defend from the attack. However, the hardware appliances for defence or detection are neither flexible nor elastic and they are expensive. To extend the NFV MANO framework, ANASTACIA incorporates a set of intelligent and dynamic security policies that can be updated seamlessly to constantly reflect security concerns in the VNF placement through the resource planning module while still ensuring acceptable QoE. Moreover, we have defined and implement synergies between SDN controllers and NFV MANO for the purpose of coordinating security to have an effective impact by defining adequate SDN rules or the adequate virtual security appliances (VNF) to be enforced through the Security Enabler Provider module. In the following section the resource planning and the security enabler provider modules will be defined.

3.2.3.4.1 Resource planning module

During the first phase of ANASTACIA, we have done two main works. The first one focused on the selection of best service (VNF), called “The security enablers selection”, among the list of enablers selected previously by the selected Security Enabler Provider, in order cope with a security attack, and a second work focus “Mobile Edge Computing Resources Optimization”. In fact, one of our two main use cases focuses on Mobile Edge Computing, as an example, in order to secure protection of a company perimeter, based on several buildings with different usage situated in different areas using distributed resource as MEC; an emerging technology that aims at pushing applications and content close to the users (e.g., at base stations, access points, and aggregation networks), reduces the latency, improves the quality of experience, and ensures highly efficient network operation and service delivery.

During the second phase of the project, we aim to extend the resource planning module to include a dynamic Service Function Chain (SFC) requests placement that aim to reduce the routing overhead in case of an attack happen as an example. In fact, it is challenging to allocate multiple SFC requests on an NFV Infrastructure, especially in a cost-driven objective. VNFs have to be chained in a specific order. Moreover, depending on their type and isolation considerations, VNFs can be potentially shared among several SFCs. Finally, VNFs must not be placed far from the shortest path to avoid increasing SFC delay and network usage.

3.2.3.4.2 Security Enabler selection

The aim of the model is to select the best service (VNF) among the list of enablers selected previously by the selected Security Enabler Provider, in order cope with a security attack and that minimize the maximum load nodes (CPU, RAM, bandwidth) of the topology, provided by the system model. Indeed, the system information will provide relevant data about the whole infrastructure, server capacity (CPU, RAM, etc), and VNF flavours (CPU, RAM, etc). On the other hand, the Security Enablers information will provide the data regarding the available Security Enablers capable to enforce specific capabilities. The goal of the model is minimizing the maximum load nodes to improve provider cost revenue (provider energy efficiency goal). For more details please refer to the Anastacia deliverable D3.3.

3.2.3.4.3 Mobile Edge Computing Resources Optimization

Mobile Edge Computing (MEC) is an emerging technology that aims at pushing applications and content close to the users (e.g. at base stations, access points, aggregation networks) to reduce latency, improve quality of experience, and ensure highly efficient network operation and service delivery. It principally relies on virtualization-enabled MEC servers with limited capacity at the edge of the network. One key issue is to dimension such systems in terms of server size, server number and server operation area to meet MEC goals. In this work, we have proposed a graph-based algorithm that, taking into account a maximum MEC server capacity, provides a partition of MEC clusters, which consolidates as many communications as possible at the edge. We evaluate our proposal and show that, despite the spatio-temporal dynamics of the traffic; our algorithm provides well-balanced MEC areas that serve a large part of the communications.

This work has been published in a Sigcom workshop [Bouet, 2017] and extended for IEEE Transactions on Network and Service Management TNSM journal [Bouet, 2018].

3.2.3.4.4 Security Enabler Provider

The Security Enabler Provider is a component of the Security Orchestration Plane, as defined in the ANASTACIA architecture. This component is able to identify the security enablers which can provide specific security capabilities, to meet the security policies requirements. Moreover, when the Security Resource Planning, a sub-component of the security orchestrator, defined before, selects the security enabler, the Security Enabler Provider is also responsible for providing the corresponding plugin.

The Security Enabler Provider mainly interacts with the Policy Interpreter. Specifically, two different interactions have been contemplated:

- The first one will provide to the Policy Interpreter a list of security enabler candidates from the main identified capabilities.
- The second one will provide to the Policy Interpreter the specific Security Enabler Plugin in order to perform the policy translation. This policy translation process was defined in ANASTACIA D3.1 [Zarca, 2018-3], and also published in journal paper [Trapero, 2017] (formerly introduced in conference paper [Farris, 2017]).

The first role is implemented as a piece of software that from specific capabilities given as an input it will provide the more accurate enablers. The second role is also implemented as piece of software capable to translate MSPL policies into specific configuration/tasks rules according to a concrete security enabler. For more details please refer to the ANASTACIA deliverable D3.3 [Belabed, 2018].

➥	**MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS** • Design and develop smart routing for Service & Network management • Extend the resource planning module to include a dynamic Service Function Chain (SFC) requests placement that aim to reduce the routing (while most of the actual study are based on Resource Allocation • Design and develop learning methods to enhance routing and prevent attacks ○ Supervised learning ○ Reinforcement Learning • Expand the Security Resource planning in order to integrate the smart security orchestrator leveraging SDN and NFV 5G-enabler technology for cyberattack mitigation

3.2.3.5 KI5 – Security monitoring to threat detection in SDN/NFV-enabled IoT deployments

Security threat levels change dynamically as the attackers discover new breaches and try to exploit them. To cope with this challenge, the ANASTACIA project relies on SDN and NFV techniques to embed the developed security products and provide a dynamic way to deploy them when needed. In this way, the ANASTACIA project delivers a set of scientific and technological innovations, grouped in two principal key innovation areas.

Security Monitoring and Reaction Infrastructure

Saedgi et al. identify the principal challenges when securing IoT-based Cyber Physical Systems, highlighting as one of the principal challenges the development of a "*a holistic cybersecurity framework covering all abstraction layers of heterogeneous IoT systems and across platform boundaries*" [Sadeghi, 2015]. The ANASTACIA project fulfils this challenge by proposing a state-of-the-art security infrastructure composed by three principal modules:

- ***Monitoring Agents*****:** These are the components in charge of extracting the security data from the monitored network. The ANASTACIA framework has been designed flexible enough to support both physical and virtual monitoring agents, as well as to extract data from data networks (both IP and IoT networks) and from analog CPS devices. This makes the ANASTACIA framework a multilevel security platform, and therefore suitable for physical sensor networks, emulated environments and hybrid networks. In this direction, the ANASTACIA partners have worked in the implementation of monitoring agents adapted for 6LowPan and ZigBee IoT networks, as well as the development of agents capable of extracting temperature information from analog sources. These agents have been tested using the case studies of the project, aiming to be applied in wider scenarios for its final validation. Following this path, the project partners are extending even further these monitoring agents with virtualization characteristics. By means of using NFV and SDN technologies on the monitoring agents, it will be possible to deploy and (re)configure them on demand, allowing to deploy new agents on the network as a reaction to ongoing attacks. In this sense, the ANASTACIA partners are also extending the security policy language (MSPL) in order to correctly specify such type of countermeasures, allowing the deployment of new monitoring agents on the network in a complete autonomous manner.
- ***Monitoring Module*****:** This component contains the logic of the detection of security incidents. The heterogeneous monitoring agents (IoT networks and analogue agents) use a shared communication channel to publish the extracted security data. This information is then analyzed by the incident detectors (for well-known attacks) and behavior analysis modules (for zero-days attacks), emitting verdicts about the detected incidents. As stated in [Sadeghi, 2015], detecting zero-days attacks does not ensure a high security level, since well-known attacks are still used by malicious users to gain control of the systems. ANASTACIA does not only provide both types of analysis (well-known attacks and behavior analysis) but it will also use all this information to provide a deeper analysis and found correlations between already-known attacks and they behavioral analysis result, detecting hidden relationships between events coming from different sources. The ANASTACIA partners are developing such correlation engines to enhance both security analyses and provide enriched information to the reaction module.
- ***Reaction Module*****:** Using the information provided by the monitoring module (namely incidents verdicts and behavior analysis results), the reaction module has the responsibility of determining the best mitigation plan for the detected incidents. The ANASTACIA framework provides a simple yet powerful design for this component, which uses not only the incidents verdicts provided by the monitoring module, but also system model and the capabilities deployed in the network. All this information is enhanced with a risk analysis to determine the best set of countermeasures to cope with the ongoing attack. Further information about how this analysis is performed can be found in the following sections.

Novel Products for IoT- and Cloud-based SDN/NFV systems

The security infrastructure described above represents one of the principal outcomes of the project, however the partners are also working on a concrete implementation of this design. To implement this monitoring infrastructure, the partners have developed a set of technologies that fulfil the functionalities of the ANASTACIA infrastructure, generating a set of novel products ready to be deployed on IoT- and cloud-based systems. For example, partner Montimage has developed a 6LowPan network sniffer in coordination with the MMT tool to detect anomalies in IoT networks. UTRC (in collaboration with OdinS) has developed analog temperature agents and a machine learning-based behavior analysis for data sensors, allowing them to detect attacks on temperature sensor networks. ATOS has extended its XL-SIEM tool to perform the risk analysis when computing the reaction and the inclusion of the system model when computing the countermeasures to be taken. Despite the development of such products is not finished yet, the partners have managed to integrate PoC version of such technologies on a shared platform, allowing to perform initial tests and validation of the technologies. Moreover, it is envisaged to further extend this tools with a correlation engine, aiming to reveal hidden relationships between security events coming from different sources (monitoring agents) and, therefore, raising the awareness level of the whole security platform.

To further extend the offer of products, the ANASTACIA partners are preparing the solutions to be NFV- and SDN-ready, by means of adapting the solutions (especially network agents) to work as single, self-contained NFV modules. In this sense, the ANASTACIA outcomes will have the potential to be deployed in virtualized environments, be dynamically deployed as a reaction to an ongoing attack and, capable of being reconfigured if required. In this scenario, the ANASTACIA platform will have the ability to momentarily harden the security of the portions of the network are under attack, by means of deploying new agents, load new security rules on the monitoring agents/module, analyze new protocols or reconfigure the existing instances. All these actions are to be maintained until the security level has returned to normal values or the network administrator has intervened to solve the security breach.

All these novel products will have a high impact on the security market, opening business possibilities in the IoT-based CPS area.

Despite the ambition of the project is high, the ANASTACIA partners have already established the bases of the further innovations. The ANASTACIA partners will continue its efforts to fully integrate the security innovations with the SDN and NFV technologies, as well as developing a correlation engine for security events. This direction aims to provide the market with a highly-dynamic security solution, capable of not only detecting current cyber threats, but also capable of reacting against them and also deploy new security instances to adapt to the always-evolving security levels of IoT networks.

MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS

- Expand Monitoring Module with event correlation engine
- Support flexible and dynamic deployment of monitoring agents
- Support reaction policies containing “monitoring” capabilities
    - Embed SDN and NFV technologies in MMT IoT Sniffer
    - Develop translation plugins to support the deployment of new monitoring instances

3.2.3.6 KI6 – Cyber threats automated and cognitive reaction and mitigation components

The monitoring information and the incident detected are evaluated for automatic mitigation. Security policies are used to determine the security enablers supported by the IoT infrastructure. This is also used to know the mitigations that the IoT infrastructure supports. Obviously, not all mitigations work with all possible threats, and not all mitigations have the same cost. Cost is not considered here just in terms of economic impact, but also in terms of time to mitigate, computational resources required or complexity of the mitigation. ANASTACIA automatically analyses these factors and, along with the incidents detected, evaluates and decides on the most convenient mitigation in each case. To this end several data are considered in the analysis:

(1) severity of the incidents, which is received by the correlation engine at the monitoring module and takes into account the type of incident and the duration of the incident among others,
(2) importance of the assets affected, which depends on the criticality of the IoT devices affected, their location or the importance of the data they manage,
(3) the cost of the mitigation obtained either from the orchestrator in charge of enforce the available security enablers, or from the system admin in case specific expert knowledge is required.

The global risk of the incident is obtained from (1) and (2), which is used together with (3) to decide on the most convenient mitigation. A decision support service (DSS) is used to compute that information, providing with a score for each mitigation, which represents the suitability of the mitigation for the ongoing incident. The mitigation with the higher suitability score represents the most suitable mitigation, which is passed to the orchestrator for its enforcement. To this end a Mitigation Action Service (MAS) is used to translate the output of the DSS to a format that is understandable by the orchestrator. The MAS is then in charge of generating the reaction in the MSPL format. This language was selected since its XML-based structure allows specifying the type of base capability to deploy (e.g. filtering, monitoring), and the configurations of such action (e.g. involved IPs, port numbers, number of agents to deploy). The MSPL format also allows the MAS to directly send the mitigation plan to the Security Orchestrator, which will use it to deploy the computed plan.

In order to generate the MSPL file, the MAS analyses the response of the DSS by performing the following processes: (1) it identifies the countermeasure computed by the DSS; (2) it identifies the network capabilities able to execute the countermeasure; (3) it retrieves the information of the capabilities from the System Model Analysis module; (4) it builds the MSPL file to express the countermeasure, specifying the capability to use and the configurations of that capability used to apply the countermeasure.

Every incident handled by the reaction (including risk evaluation, decision support activities), the information associated to it (such as type of incident or IoT devices affected) and all the indicators that characterize the incident (such as severity, importance of assets affected, global risk of the incident or suitability of the mitigation) are passed to the Dynamic Security and Privacy Seal to update the seal status.

Currently we are developing the quantitative model that supports the assessment of incidents and mitigations for deciding on the most convenient reaction based on incident severity, criticality of the assets affected, possible mitigations and cost of mitigating them.

MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS

- Design and develop mathematical algorithms for quantitative evaluation of incidents for mitigation support (VDSS)
    - Improve the Reaction and Mitigation Action Service (MAS)
    - Define a list of suggested mitigation actions (MSPLs) with associated score
    - Consider context-awareness (system model)
    - Design and develop support for the evaluation of the effectiveness of applied reaction (reinforcement)

3.2.3.7 KI7 – Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments

Our behavioral framework automatically identifies cyber-security attacks in a given IoT environment. It uses system design and operational data to discover dependencies between cyber systems and operations of HVAC in a cyber-physical domain. We predict potential security consequences of interacting operations among subsystems and generate threat alarms. Specifically, our behavioral engine is empowering ANASTACIA's use case scenario by using "best" practices to implement security in terms of (1) adding network security (in forms of IDS/IPS), and (2) using threat intelligence to detect evasions or hidden attacks. Our developed platform can detect:

- Known attacks such as DDoS and MiTM attacks,
- IoT zero-days attacks and slow DoS attacks that might pass undetected by normal IDS/IPS [Cambiaso, 2013].

Our framework developed a monitoring component which is composed of messaging wrappers, Constraint Programming (CP) models and buffered sensor data from IoT networks. Mainly, CP model is core component of our behavioural analysis engine. First the information is gathered and analysed for learning a CP model and then it is deployed to identify any intrusion. Moreover, CP model built on continuous stream of data (i.e. time-series) where the time interval between successive updates could vary from milliseconds to minutes.

CP model consists of network of relations between building sensor data. Using this CP model, we aggregate the different types of sensor data to truly model the normal behaviour of the system that is being supervised. This model is built for monitoring at system level, but it does not prevent from including in the model information about network performance if that is exposed to it. For an example, CPU consumption of a device can be included along its actual sensor data. The variety of data that we can aggregate allows the model to be as generic or as specific as the end-user required it to be. Since the model is built on relations, we can leverage from the fact that what data effects what other data type (features).

We developed an approach to learn a CP-based decision model consisting of a set of relations to detect misbehaviour of the system. More specifically, the idea is to learn a set of relations which together when satisfied defines the normal behaviour of the system. After learning important relations, the approach discards un-important relations, and consequently creates a model with best possible relations and features of sensor nodes. In each iteration, the relation between the sensor features and all other network features further verified. Also, we identify the sensors are involved in breaking the relation and what are the set of relations are broken Following this fashion, the model is further tuned. The developed 'Monitoring' component enables continuous and integrated monitoring of multivariate signals, event logs, heartbeat signals, status reports, operational information, etc., emanating from various devices in multitude of building operational subsystems. This monitoring component also evaluates the security situation against known policies, models, threat signatures to detect abnormalities and outliers, e.g., high data download, external database or port accesses during an emergency. Such situations will be analysed by the 'Reaction' component which will evaluate the severity of the situation. Isolation and predictive mechanisms are activated to ensure that the rest of the building operations system continues as normal. Policies and rules are activated, updated and enforced by the 'Security Enforcement' component, e.g., a building emergency will lock-down the non-essential database accesses, and escalation of the emergency to the city fire brigade should be performed by any of the authorized personnel. To this end, our behavioural engine's innovation is summarized as the following key points:

- Learning constraint programming model for capturing the normal behaviour of a given cyber-physical system
- CP-model provides explanation when a potential anomaly is detected by reporting which constraints fails to satisfy the model
- User-defined constraints can be easily integrated with the constraints learn from the data
- The developed behaviour engine can handle multiple attacks of different types

MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS

- Address Advanced Persistent Threats (APT) like Slow DOS attack hard to detect with normal SIEM tools
- Design and develop mechanisms to deal with multiple attacks on same time window
- Investigate ways to find correlation between operational attacks and network attacks
- Design and develop algorithm for learning the evolving nature of attacks

3.2.3.8 KI8 – Secured and Authenticated Dynamic Seal System as a Service

Several projects have tried to address the need to enable trustable ICT deployments, however, the normative framework for security and personal data protection is evolving. New obligations are emerging from the recently adopted European General Data Protection Regulation (GDPR), with higher requirements and obligations for data controllers, as well as for data processors. In parallel, ISO standards on IT security, privacy and Information management systems are increasingly becoming market requirements. Existing seals are generally focused either on security or on privacy, but not both. Moreover, they are usually based on two separate models:

- Either ISO standard-based certification of products and information management systems respecting ISO 17065 or ISO 17021-1 and relaying on human audit and assessment;

- Or purely system-based monitoring of security, such as anti-virus applications or intrusion detection system (IDS), which are often designed independently from any standard.

Given the importance of the GDPR and ISO standards, ANASTACIA's Dynamic Privacy and Security Seal (DSPS) will seek to inform the end-user on the most relevant privacy and security issues while supporting certification and compliance activities. To this end, the DSPS will:

- Introduce a privacy-by-design and by default compliant architecture, services and graphical user interface (GUI) that seek to combine the certainty and trustworthiness of conventional certification schemes with real-time certification surveillance capabilities through the real time dynamic monitoring (provided by ANASTACIA) of the certified system[1].
- Compile alerts and threats from ANASTACIA, compatible monitoring solutions (using the STIX 2 standard) and the end-user (CISO/DPO) and showcase them through a unified GUI, displaying IoT/CPS privacy and security information while providing decision support capabilities, and data visualization (considering accessibility/ease of use requirements).
- Empower the end-user by enabling the client's Data Protection Officer (DPO) and Chief Information Security Officer (CISO) to provide feedback to the raised alerts directly through the GUI and to enhance the information obtained from the monitoring system with technical, legal, and organizational documentation. This data will be stored in a distributed storage solution (powered by Shamir Secret Sharing Scheme), which will be associated with the DSPS blockchain-based seal ledger (Hyperledger Fabric), to ensure the data is non-repudiable, immutable, and easily verifiable in direct relation to the events showcased by the DSPS both by the end-user (for internal audit and compliance purposes) and associated certification bodies (to determine the validity of relevant certifications).

The Dynamic Security and Privacy Seal (DSPS) aims to provide a holistic solution to privacy and security monitoring, addressing both the organizational and technical requirements enshrined by the GDPR through the implementation of a layered process by which: 1) an initial examination by an auditor or expert determines the baseline status of the system with regards to privacy and security of both the product or system that is to be monitored, and the organizational policies and mechanisms that surround its implementation to ensure compliance with the most relevant ISO standards (particularly if linked to a certification) and regulations; 2) ANASTACIA provides constant monitoring and reaction capabilities which are then used to update the DSPS; 3) the end-user provides feedback on the effectivity of the mitigation activities and uses the DSPS enablers to enhance transparency and accountability in the monitored system.

The resulting tool will provide the end-user with a broad perspective over the state of the monitored system which will consistently track and unify the organizational/human elements considered by personal data protection regulations with the technical insights provided by ANASTACIA's monitoring and reaction services. Once implemented, this process will not only provide advanced trust-enhancing information functionalities to ANASTACIA users, but will also serve as a surveillance solution for audit/certification/legal compliance purposes. It will generate a non-repudiable historic track of system variations and potential threats (technical and organizational) to the sealed system while enhancing the contextual information available to the client, auditors or regulatory authorities.

Current work [Quesada Rodriguez et al., 2018-2] has been focused towards developing the DSPS architecture as defined by ANASTACIA Deliverable 5.1; deploying and integrating the monitoring service and associated enablers; and refining the GUI elements that will inform the end-user and enable them to provide the required feedback. Upcoming research will seek out ways to simplify complex privacy and security information, so as to address the varying technical and legal knowledge of the potential end-users.

[1] Certification and labelling processes are usually based on system evaluation by human experts at a given period of time. The seal or label is then generated at a given period of time to certify a certain level of trust and reliability attached to the targeted solution or system deployment. The rapid evolution of security landscape and threat may turn supposedly reliable certified systems into vulnerable ones. ANASTACIA aims to inform the end-user of any change in the system's trust level while enabling certification bodies to reassess the validity of the certification.

Furthermore, research on integration with additional information sources (particularly through the STIX2 format) and privacy-management tools (such as the CNIL DPIA software) will be performed to further enhance the functionalities available through the DSPS GUI.

MAIN INDICATIONS FOR REFINED/ADDITIONAL REQUIREMENTS

- Develop the DSPS as an internal/external audit and transparency tool
- Develop the DSPS as a tool to support Privacy and Security Certification Monitoring
- Develop the DSPS for auditing data processing activities and data escrow
- Support a holistic privacy and security monitoring approach by supporting
    - Privacy-by-design and privacy-by-default features
    - Compile alerts + threats: (ANASTACIA + CISO/DPO) (+ expandable)
    - End user feedback + organizational compliance / due-diligence tracking
    - Hybrid supporting process for certification/audit schemes
    - User-friendly privacy + security information
- Identify enablers involved in privacy-sensitive processes
- Enhance the DSPS Agent to increase interoperability
- Improve the DSPS GUI to:
    - Easily convey complex privacy and security information to end-user
        - Exploring graphical and symbolic mechanisms for data conveyance
        - Adding custom visualizations/views
        - Generating a distinct graphical identity for the DSPS
        - Determining and showcasing the most relevant information for end-users
    - Streamline feedback process
        - Enable end-users to raise alerts to DSPS
        - Integrate DPIA tools
        - Enable data upload functionalities
        - Ensure correct integration of digital signature for data validation

4 REQUIREMENTS

4.1 INITIAL REQUIREMENTS

For the sake of completeness and to ease comparison and evaluation, the initial version of the requirements as expressed in D1.2 are included here for reference.

Each requirement is evaluated against the actual methodological and technological results, in particular as for components included in the overall architecture (Figure 9), to evaluate the degree of compliance of project outcomes with initial expectations.

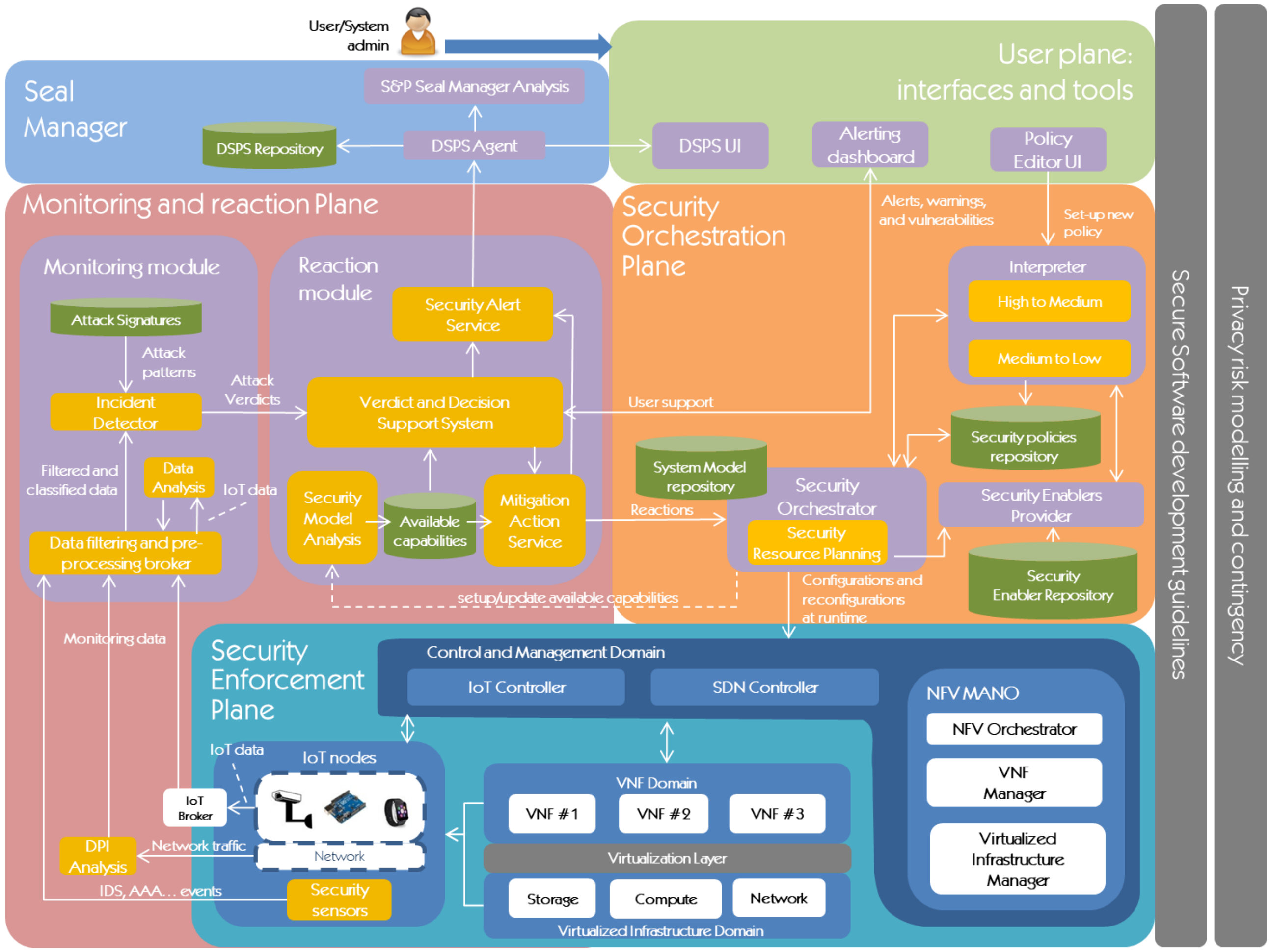

User/System admin
Seal Manager
S&P Seal Manager Analysis
DSPS Repository
DSPS Agent
User plane: interfaces and tools
DSPS UI
Alerting dashboard
Policy Editor UI
Monitoring and reaction Plane
Monitoring module
Attack Signatures
Attack patterns
Incident Detector
Attack Verdicts
Filtered and classified data
Data Analysis
IoT data
Data filtering and pre-processing broker
Reaction module
Security Alert Service
Verdict and Decision Support System
Security Model Analysis
Available capabilities
Mitigation Action Service
setup/update available capabilities
Security Orchestration Plane
Alerts, warnings, and vulnerabilities
Set-up new policy
Interpreter
High to Medium
Medium to Low
User support
Security policies repository
System Model repository
Security Orchestrator
Security Resource Planning
Reactions
Security Enablers Provider
Security Enabler Repository
Configurations and reconfigurations at runtime
Monitoring data
Security Enforcement Plane
Control and Management Domain
IoT Controller
SDN Controller
NFV MANO
NFV Orchestrator
VNF Manager
Virtualized Infrastructure Manager
IoT data
IoT nodes
IoT Broker
Network
Network traffic
DPI Analysis
IDS, AAA… events
Security sensors
VNF Domain
VNF #1
VNF #2
VNF #3
Virtualization Layer
Storage
Compute
Network
Virtualized Infrastructure Domain
Secure Software development guidelines
Privacy risk modelling and contingency

Figure 9. ANASTACIA architecture.

4.1.1 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**
➥	**COMPLETED**: Policy Editor UI included in the architecture and released	✓
FR-2	The ANASTACIA system will include a repository to store security policies	**HIGH**
➥	**COMPLETED**: Security Policy Repository included in the architecture and released	✓
FR-3	The ANASTACIA system will provide CRUD functionalities for privacy policies to be checked when data are internally processed	**HIGH**
➥	**IN PROGRESS:** Privacy Policy Repository under development	⚙
FR-4	The ANASTACIA system will include a repository to store privacy policies	**HIGH**
➥	**IN PROGRESS:** Privacy Policy Repository under development	⚙
FR-5	The ANASTACIA system will provide CRUD functionalities for the definition of the devices included in the monitored system	**MEDIUM**
➥	**IN PROGRESS:** System Model definition in progress, related management API under development, specific UI not considered so far, associated repository considered	⚙
FR-6	The ANASTACIA systems will include a repository to store device data	**MEDIUM**
➥	**IN PROGRESS:** System Model Repository included in the architecture and under development	⚙
FR-7	The ANASTACIA system will provide CRUD functionalities for the definition of the network topology included in the monitored system	**MEDIUM**
➥	**IN PROGRESS:** System Model definition in progress, related management API under development, specific UI not considered so far, associated repository considered to manage network configuration as well	⚙
FR-8	The ANASTACIA system will include a repository to store network topology data	**MEDIUM**
➥	**IN PROGRESS:** System Model Repository included in the architecture and under development, network configuration to be considered therein	⚙

ID	Name/Description	Priority*
FR-9	The ANASTACIA system will include an interactive graphical visualization of the network and of the devices included in the monitored system	**LOW**
➥	**IN PROGRESS:** As for network information and visualization, some native UIs of integrated tools are included in the architecture	⚙
FR-10	The ANASTACIA system will include components for the monitoring of network traffic	**HIGH**
➥	**COMPLETED**: Monitoring Module included in the architecture (with inner detailed components) and released	✓
FR-11	The ANASTACIA system will include agents for the monitoring (and possibly the interactive control) of devices	**HIGH**
➥	**IN PROGRESS:** IoT Agents and integration with MMT under development	⚙
FR-12	The ANASTACIA system will include reasoning capabilities to define mitigation plans according to the defined security and privacy policies	**HIGH**
➥	**IN PROGRESS:** Reaction Module include in the architecture (with inner detailed components) and related reasoning capabilities under development (see Key Innovation KI…)	⚙
FR-13	The ANASTACIA system will include orchestrating capabilities to manage the correct implementation of mitigation plans	**HIGH**
➥	**IN PROGRESS:** Orchestration Module include in the architecture (with inner detailed components) and related enforcement capabilities under development (see Key Innovation KI…)	⚙
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**
➥	**IN PROGRESS:** Orchestration Module include in the architecture (with inner detailed components) and related enforcement capabilities under development (see Key Innovation KI…)	⚙
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**

ID	Name/Description	Priority*
↪	**IN PROGRESS:** Orchestration Module include in the architecture (with inner detailed components) and related enforcement capabilities under development (see Key Innovation KI…)	⚙
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**
↪	**COMPLETED:** Blockchain-based DSPS repository included in the architecture and released	✓
FR-17	The ANASTACIA system will include reasoning capabilities to verify if the deployment of security mitigation actions alters significantly the privacy status of the monitored system, eventually deciding if proceeding or not, asking for confirmation to the system administrator	**LOW**
↪	**IN PROGRESS:** reasoning capabilities under development, management of policy conflicts, dependencies, etc. to be considered	⚙
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**
↪	**IN PROGRESS:** reporting functionalities developed for different components according to association to macro-modules (monitoring, reaction, orchestration, enforcement, DSPS)	⚙
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**
↪	**POSTPONED:** considering the low priority and the expected TRL-5, associated development stopped and postponed to pre-industrialization phase	⌛
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**
↪	**IN PROGRESS:** reasoning/self-learning capabilities under development, management of policy conflicts, dependencies, etc. to be considered	⚙

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

✓= ACHIEVED, ⚙ = IN PROGRESS, ⌛ = POSTPONED

4.1.2 Non-functional requirements

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

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

4.1.2.1 General 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**
➥	**POSTPONED:** considering the low priority and the expected TRL-5, associated development stopped and postponed to pre-industrialization phase	⌛
NFR-2	**Availability** – the ANASTACIA system will be available 24/7	**MEDIUM**
➥	**COMPLETED:** no specific constraints on service availability, continuous real-time/run-time support considered	✓
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**
➥	**POSTPONED:** considering the low priority and the expected TRL-5, associated development stopped and postponed to pre-industrialization phase	⌛
NFR-4	**Capacity** – the ANASTACIA system will have to manage a minimal set of <*N*> devices (to be defined at pilot level)	**MEDIUM**
➥	**COMPLETED:** no specific constraints on number of devices managed	✓
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**
➥	**COMPLETED:** no personal data managed internally	✓
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**
➥	**COMPLETED:** standard protocols adopted for internal communication	✓
NFR-7	**Configurability** - the ANASTACIA system will include tools for the configuration of security policies, privacy policies, network topologies, device features, VNF features	**HIGH**

ID	Name/Description	Priority*
➥	**IN PROGRESS:** see applicable functional requirements	⚙
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**
➥	**COMPLETED:** see First validation and evaluation results for specific Use Cases	✓
NFR-9	**Extensibility** – the ANASTACIA system will adopt a modular architecture and include configuration tools that allow adding features and defining customizations	**MEDIUM**
➥	**COMPLETED:** modular architecture with proper message broker and communication protocols defined to allow functional extensibility	✓
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**
➥	**COMPLETED:** standard protocols adopted for communication	✓
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**
➥	**IN PROGRESS:** dedicated performance tests to be carried out in the second validation and evaluation phase	⚙
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**
➥	**IN PROGRESS:** dedicated performance tests to be carried out in the second validation and evaluation phase	⚙
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**
➥	**COMPLETED:** real time notification support provided by interaction of inner planes with the DSPS	✓
NFR-14	**Scalability** – the ANASTACIA system will be able to transparently add/deploy new monitored IoT devices and VNFs	**HIGH**
➥	**COMPLETED:** no restriction in number of items managed by the system	✓

ID	Name/Description	Priority*
	NOTE: Scalability could be improved by adding dynamic and reactive provisioning of security VNFs towards the edge of the network	
NFR-15	**Security** – the ANASTACIA system will provide functionalities for Authentication, Authorization, and Accounting to guarantee proper access for registered users	**MEDIUM**
➥	**COMPLETED:** DSPS UI secured with specific AAA policies	✓

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

✓= ACHIEVED, ⚙ = IN PROGRESS, ⌛ = POSTPONED

4.1.2.2 Privacy requirements

The initial list of Privacy requirements included in D1.2 has been superseded by the one included in D2.7 and is included here for reference only. The updated list to be considered as final is included in Section 4.2.2.2).

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**

ID	Name/Description	Priority*
PR-4	**De-activation of authentication credentials** - Personal authentication credentials shall be de-activated if they have not been used for at least six months (except in case of technical authorization). The system will periodically check if more than six months elapsed since the last log in of each person acting under the authority of the controller or the processor and disable its credentials if usage requirements are not met. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data. *The objective is to guarantee that persons acting under the authority of the controller or the processor can only access and process personal data if they are provided with authentication credentials. The credentials are necessary for the appointed person to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.*	MEDIUM
PR-5	**Authorization** - Before the start of the processing, it is necessary to enable access to the data that are needed to perform processing operations, setting out an authorization profile for each person/homogeneous set of persons acting under the authority of the controller or the processor. Authorization profiles will be set out and configured prior to start of the processing so as to enable data controllers' access only to the data that are necessary to perform processing operations. *It will be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorization profiles still apply. ANASTACIA will work on the basis of a list of persons acting under the authority of the controller or the processor to identify categories of task and corresponding authorization profiles.*	HIGH
PR-6	**User data management** - In case of personal data collection, the system enables users to control their personal data, to access, rectify, delete or block them. It is always possible, for the users, to change the sets of data that they have shared. *The idea is to allow users to control their interaction with the project by revealing only the information they want to disclose and changing at any time the set of shared data. It is a user-centric approach that means that users have the power to play an active role in the management of their personal data. This may include the realization of a dashboard whereby the user may always keep control on the overall processing of his/her personal data.*	HIGH
PR-7	**Purpose limitation** - ANASTACIA will process personal data only for security purposes, unless the data controller configures the system to pursue other legitimate, specific and explicit purposes, determined at the time of collection of the 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*	HIGH

ID	Name/Description	Priority*
	data which are inaccurate, having regard to the purposes for which they are further processed, are erased or rectified without delay […]".	
PR-9	**Security of processing -** Personal data will be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. *As defined by Article 32 of the GDPR, as part of the security of the processing, both controller and processor must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."*	HIGH
PR-10	**Data breach information** - The Anastacia system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects. *The legal source of this requirement is found in Articles 33 and 34 of the GDPR. Information about the breach can also be provided by means of the Dynamic Privacy and Security Seal.*	HIGH
PR-11	**Encryption by default** - Encryption will be applied to all stages of handling data, including in communication, storage of data at rest, storage of keys, identification, access, as well as for secure boot process. *The legal source of this requirement is Article 32 of the GDPR, whereby it mandates the controllers and processors to ensure a level of security appropriate to the risk, including measures that have the "ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services".*	HIGH
PR-12	**Right of access** - The Anastacia system shall support the data controllers in providing to every data subject, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to: the purposes of the processing; the categories of data concerned; the recipients to whom the data are disclosed; the envisaged period of storage for the data; and the existence of automated decision-making processes within the system. *The legal source of this requirement is Article 15 of the GDPR.*	HIGH
PR-13	**Appropriate retention period** - The default personal data retention period is set at one (1) month, without prejudice to other conflicting legal obligations, which will be appraised on a case by case basis on motivated request by the data controller (e.g. in case of different retention period for internet traffic data mandated by specific law on detection and prevention of crime).	HIGH

ID	Name/Description	Priority*
	The exceptions to the one month retention policy set above may derive from the implementation of Article 15(1) of the ePrivacy Directive (Directive 2002/58/EC) at national level. Such Directive provides that: "Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period" when it is necessary to safeguard "national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".	
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 }

4.2 FINAL REQUIREMENTS

4.2.1 Functional requirements

The following additional functional requirements are introduced according to the analysis carried out in the previous sessions and will be addressed during the second half of the project. A mapping onto Research Challenges (RC), associated Key Innovations (KI), Specific Validation and Evaluation (SVE) and also Negative Comments and Observations (NCO) is provided.

NEW VERSION

ID	Name/Description	RC	KI	NCO	SVE	Priority*
FR-21	The ANASTACIA system will handle complex (e.g. multiple attack) scenarios	RC1, RC2, RC3, RC4, RC5, RC8	KI1, KI2, KI3, KI4, KI5, KI8	NCO-2, NCO-14, NCO-17		HIGH
FR-22	The ANASTACIA system will include novel reasoning capabilities for autonomous mitigation of attacks	RC1, RC3, RC4, RC6, RC7	KI1, KI3, KI4, KI6, KI7	NCO-2		HIGH
FR-23	The ANASTACIA system will be deployed as a distributed architecture (appropriate guidelines/instructions to be issued)	RC1, RC2, RC3, RC7	KI1, KI2, KI3, KI7	NCO-3		MEDIUM
FR-24	The ANASTACIA system will enforce policies that interfere with CPS status so to avoid unexpected impacts in the operational context	RC1, RC6	KI1, KI6	NCO-5		HIGH
FR-25	The ANASTACIA system will not introduce additional potential points of failure during the orchestration/enforcement of mitigation plans			NCO-11		HIGH
FR-26	The ANASTACIA system will support real-time monitoring and control of IoT for attack mitigation purposes devices	RC2, RC3, RC4, RC6	KI2, KI3, KI4, KI6	NCO-20		HIGH
FR-27	The ANASTACIA system will include security and privacy policy conflict detection to support orchestration and enforcement of mitigation plans	RC1, RC2. RC3	KI1, KI2, KI3			HIGH
FR-28	The ANASTACIA system will manage security and privacy policy dependencies to support orchestration and enforcement of mitigation plans	RC1, RC2. RC3	KI1, KI2, KI3			HIGH
FR-29	The ANASTACIA system will adopt optimal selection criteria for SDN/NFV-based security mechanisms to enforce	RC2	KI2			HIGH

ID	Name/Description	RC	KI	NCO	SVE	Priority*
FR-30	The ANASTACIA system will adopt optimal orchestration criteria for SDN/NFV-based security mechanisms to enforce	RC3	KI3			HIGH
FR-31	The ANASTACIA system will allow to mitigate 0-day attacks	RC4	KI4			HIGH
FR-32	The ANASTACIA system will allow to mitigate slow DDoS attacks	RC4	KI4			HIGH
FR-33	The ANASTACIA system will find correlation between operational attacks and network attacks	RC4	KI4			MEDIUM
FR-34	The ANASTACIA system will design and develop algorithm for learning the evolving nature of attack	RC4	KI4			MEDIUM
FR-35	The ANASTACIA system will include advanced decision models (included in the Monitoring Plane) to detect suspect IoT malicious activities and potential associated risks/attacks	RC5	Ki5			HIGH
FR-36	The ANASTACIA system will include advanced reasoning capabilities (to be included in the Monitoring Plane) to leverage event correlation and enhance IoT security	RC6	KI6			HIGH
FR-37	The ANASTACIA system will include advanced reasoning capabilities (to be included in the Reaction Plane) based on mathematical models for quantitative evaluation of risks/attacks to better define appropriate mitigation plans	RC7	KI7			HIGH
FR-38	The ANASTACIA system will define list of suggested mitigation actions with associated score based on quantitative evaluation of risks/attacks	RC7	KI7			HIGH
FR-39	The ANASTACIA system will consider context-awareness (system model) in the quantitative evalution of risks/attacks	RC7	KI7			HIGH
FR-40	The ANASTACIA system will support the evaluation of the effectiveness of applied reaction and mitigation plans (reinforcement)	RC7	KI7			HIGH

ID	Name/Description	RC	KI	NCO	SVE	Priority*
FR-41	The ANASTACIA system will support accountability as for compliance with GDPR, with a focus on DPIA activities and on non-repudiable proof	RC8	KI8			HIGH
FR-42	The ANASTACIA system will include smart routing functionalities for service & network management	RC4	KI4			HIGH
FR-43	The ANASTACIA system will include a dynamic Service Function Chain (SFC) requests placement to reduce routing	RC4	KI4			HIGH
FR-44	The ANASTACIA system will include learning methods to enhance routing and prevent attacks by supervised and/or reinforcement learning techniques	RC4	KI4			HIGH
FR-45	The ANASTACIA system will leverage SDN and NFV 5G-enabler technology for cyberattack mitigation	RC4	KI4			HIGH
FR-46	The ANASTACIA system will support flexible and dynamic deployment of monitoring agents	RC5	KI5			MEDIUM
FR-47	The ANASTACIA system will support reaction policies containing monitoring capabilities	RC5	KI5			MEDIUM
FR-48	The ANASTACIA system will embed SDN and NFV technologies in MMT IoT Sniffer	RC5	KI5			MEDIUM
FR-49	The ANASTACIA system will include translation plugins to support the deployment of new monitoring instances	RC5	KI5			MEDIUM
FR-50	The ANASTACIA system will include a DSPS as an internal/external audit and transparency tool	RC9	KI9			HIGH
FR-51	The ANASTACIA system will include a DSPS as a tool to support Privacy and Security Certification Monitoring	RC9	KI9			HIGH
FR-52	The ANASTACIA system will a DSPS for auditing data processing activities and data escrow	RC9	KI9			HIGH

ID	Name/Description	RC	KI	NCO	SVE	Priority*
FR-53	The ANASTACIA system will allow end user feedback to support organizational compliance / due-diligence tracking	RC9	KI9			MEDIUM
FR-54	The ANASTACIA system will support streamline feedback process by enabling end-users to raise alerts to DSPS	RC9	KI9			MEDIUM
FR-55	The ANASTACIA system will support streamline feedback process by integrating DPIA tools	RC9	KI9			MEDIUM
FR-56	The ANASTACIA system will support streamline feedback process by enabling data upload functionalities	RC9	KI9			MEDIUM
FR-57	The ANASTACIA system will support streamline feedback process by ensuring correct integration of digital signature for data validation	RC9	KI9			MEDIUM

* { LOW , MEDIUM , HIGH }

4.2.2 Non-functional requirements

4.2.2.1 General requirements

The general non-functional requirements as initially defined in D1.2 maintain their validity throughout the project activities and technical developments and are therefore confirmed in this final version, as a general reference for the second validation phase too (see Section 4.1.2.1).

Considering the feedback collected, an additional usability requirement with several specific hints is added to the global list:

ID	Name/Description	RC	KI	NCO	SVE	Priority*
NFR-16	**Usability** – the ANASTACIA system will generally hide complexity by providing differentiated views/UIs • Improve the DSPS GUI to: ○ Easily convey complex privacy and security information to end-user ○ Exploring graphical and symbolic mechanisms for data conveyance			NCO-1, NCO-6, NCO-8, NCO-9, NCO-10, NCO-12, NOC-13, NCO-15, NCO-16, NCO-17, NCO-21	SVE1, SVE2, SVE4, SVE5	HIGH

ID	Name/Description	RC	KI	NCO	SVE	Priority*
	○ Adding custom visualizations/views ○ Generating a distinct graphical identity for the DSPS ○ Determining and showcasing the most relevant information for end-users ● Overhead and complexity associated to the implementation/deployment/use of the ANASTACIA framework should be generally minimized ● Usability of Security Orchestrator UI/console should be improved ● Usability of Mitigation Action Service and Security Orchestrator UI/console should be improved ● Complexity should be mitigated by usability for configuration and deployment processes ● Usability should be addressed and improved (terminology for non-technical users) ● Information about orchestrated/enforced mitigation plans should be duly provided in plain language for non-technical users					

4.2.2.2 Privacy requirements

The contents of this section actualize the privacy requirements as initially expressed in D1.2 and further refined in D2.3. In deliverable D2.7, these requirements are mapped onto specific ANASTACIA's capabilities, components and enablers (with particularly reference to network-level monitoring and mitigation), to demonstrate and towards their implementation in the use-cases to be addressed by ANASTACIA according to D1.2 and D6.2. These high-level requirements (indicated in D2.7 as "Personal Data Protection Requirements") aim at translating the constraints expressed in the GDPR and other relevant sources into a set of technical requirements to be addressed by ANASTACIA's monitoring systems and enablers.

ID	Name/Description	Priority*
PR-1	**Enable privacy safeguards by default** *Privacy safeguards shall be enabled by default, without requiring further intervention by the user.*	HIGH
PR-2	**Identification of data categories, non-processing of special categories, and protection of traffic and location data** *ANASTACIA should incorporate express organizational and technical measures to avoid the processing of sensitive data and/or the identification of sensitive data from any of the datasets and measurements available to the system (apply the data minimization principle and storage limitation principles, among others). Special care must be taken to identify the categories of data which might have been involved in a potential breach in the monitored system, to ensure that the correct remedial and informational measures are adopted.*	HIGH
PR-3	**Data management and respect of data subject rights** *This requirement aims to fulfil several of the rights granted by the GDPR to data subjects, including the rights of access, rectification, opposition and deletion of personal data. This requirement has several additional implications: a) In compliance with the right of information, the data subject is to be informed as soon as possible after a breach to his/her personal data has taken place; b) the right of access entails also the requirement to ensure that the system upon which such right is to be exercised is available as soon as possible after facing a data breach, so as to ensure the data subject remains in control of his personal data. Finally, all necessary measures are to be incorporated to ensure that whenever a request for deletion has been received from the data subject, any controllers or processors which possess copies of the information should be informed, asked to comply with such request.*	HIGH
PR-4	**Data retention** *A reasonable retention period should be set, after the expiration of which, data should be erased or de-identified. Unnecessary personal data should be erased by the system without undue delays. All processes related to ANASTACIA end-users should utilize reasonable or non-extensive data retention periods as well as implement any technical measures as necessary to ensure that unnecessary personal data are neither requested nor registered by the system (storage limitation and data minimization principles). Effective deletion of the data should be ensured and transparency on the followed procedures kept towards the end-users.*	MEDIUM
PR-5	**Deidentification of Personal Data** (Anonymization, Pseudonymization, Non-identifiability) *The GDPR recognizes that the rights of access, rectification and erasure (including the right to be forgotten), restriction of processing, and data portability shall no longer be applicable when the controller of personal data is able to demonstrate that it is not able to identify a data subject. This requirement then focuses on the information and practices that are necessary to ensure that identifiability is no longer possible.*	HIGH
PR-6	**Records and audit of processing activities and disclosures**	HIGH

ID	Name/Description	Priority*
	This requirement should be introduced and considered for all monitoring activities for which ANASTACIA is utilized "based on the assumption that the ANASTACIA framework would be deployed in the context of personal data processing activities which are not defined by ANASTACIA itself, yet by the entity deploying ANASTACIA's system as a service; in that regard, ANASTACIA will typically fulfil the tasks of a Data Processor, and in so doing it provides some means to achieve the purposes set by another entity, the Data Controller"(Bianchi et al., 2017, p. 62).	
PR-7	**Security of processing (prevention of unauthorized access, alteration, disclosure and destruction of personal data)** *This high-level requirement aims to ensure the introduction of technical and organizational security safeguards to protect personal data by both the monitored IT systems and ANASTACIA. From an organizational point of view, the requirement addresses the need to define, implement (and update) security mechanisms and policies to the very design of the system.*	**HIGH**
PR-8	**Data breach information** *In direct relation with the transparency and accountability principles enshrined by the GDPR, the ANASTACIA system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects.*	**HIGH**
PR-9	**Encryption of personal data by default** *All personal data should be encrypted whenever it is stored or transferred, and strong encryption mechanisms should always be used.*	**HIGH**
PR-10	**Update and review privacy measures** *Technical and organizational measures to ensure the privacy of end-users should be implemented and periodically updated/reviewed as necessary to ensure their effectiveness. Organizational and technical processes to ensure the effectiveness of security measures are required by the GDPR and constitute part of ANASTACIA's principal objectives. Generally, this requirement calls for audits and cross-verification of the security measures that have been implemented, and of the verification mechanisms themselves to maximize accountability and transparency and ensure the security and confidentiality of personal data.*	**HIGH**

5 RECOMMENDATIONS

The proposed ANASTACIA holistic (cyber-)security and privacy framework spans over different levels of technical complexity and addresses different needs (from methodological guidelines to dynamic real-time sealing/certification, through the integration of a complex set of enablers and components into different collaborating planes). The requirements released in this document therefore cover a rather large scope, ranging from technical features – such as interoperability/integrability/autonomic features etc. – up to more operational features – that privilege high-level aspects such as usability, configurability, etc. This section thus summarizes main recommendations for the pre-industrialization phase as a reference decalogue to be considered in further development/integration/evaluation activities as well as in the update of the Exploitation Roadmap (defined in WP7) and the related final exploitation plans (D7.5).

#	Description
1	USABILITY: the ANASTACIA framework should deliver easy-to-use tools and intuitive user interfaces since it addresses a differentiated audience (CPS managers, CISOs, DPOs)
2	DINAMICITY: the ANASTACIA framework should deliver to end-users (CPS managers, CISOs, DPOs) real-time feedback about monitoring / reaction / orchestration / enforcement activities as well as updated information on security-/privacy-compliance status.
3	REPORTING: the ANASTACIA framework should include customizable reporting functionalities to extract and format actionable information on security and privacy status (see e.g. accountability)
4	MODULARITY: the ANASTACIA framework should be based on a modular to guarantee i) easy extension of functionalities, ii) integration with third party's systems, iii)
5	SCALABILITY: the ANASTACIA framework should be able to seamlessly scale up from simple to complex CPS/IoT architectures
6	CAPABILITY: the ANASTACIA framework should provide innovative functionalities (advanced risk/attack detection, automatic reactions to threats)
7	PERFORMANCE: the ANASTACIA framework should deliver its functionalities (monitoring / reaction / orchestration / enforcement) within an acceptable time frame, ensuring a suitable response time that sensitively improve the overall reaction time
8	INTEROPERABILITY: the ANASTACIA framework should provide interfaces to expose collected and elaborated information to third party's systems (e.g. detected risks/attacks, affected items, defined mitigation plans, implemented mitigation actions, potential privacy breaches, DSPS status history, etc.)
9	EXPLOITABILITY: the ANASTACIA framework should be designed and implemented to allow for functional evolution and associated exploitation of both integrated and single components/planes, also exploring innovative delivery paths (e.g. Secured and Authenticated Dynamic Seal System as-a-Service)
10	ACCOUNTABILITY: the ANASTACIA framework should provide end-users (CPS managers, CISOs, DPOs) with manageable tools supporting the accountability principle as for security (e.g. ISO27001 certification) and privacy (e.g. GDPR) compliance

6 Conclusions

A set of 20 high-level functional requirements, 15 non-functional requirements and 16 privacy requirements (mainly GDPR-derived) has been initially formalized in D1.2 to support software architects and developers in the formalization of the ANASTACIA architecture and in the definition of the included components, modules and interfaces. Privacy-related constraints to be considered at design and development level (to provide end-users with useful indication for compliancy of the monitored system with the upcoming GDPR) were then superseded by requirements as expressed in D2.7. The analysis included in this deliverable further extended and refined (considering different complementary inputs) this initial list, to fine tune the final prototype and thus ease the start of the pre-industrialization phase. The final lists include 57 additional functional requirements, 1 additional non-functional requirement and 10 (rationalized) privacy requirements.

Considering the addressed TRL, the Consortium initially focused on technical end-user profiles and associated needs, stressing more definition and implementation of functional and non-functional requirements associated to the inner architectural components. As a result, this deliverable includes a general self-assessment of the current actual coverage of identified requirements and proposes additional ones (on the basis of the feedback collected during the first validation phase and the Research Challenges/Key Innovations as indicated in the position White Paper).

According to the recommendations formalized, during the second part of the project and building upon the technical results and the level of integration achieved, the Consortium will proceed to cover also higher level requirements (in particular non-functional ones), integrating valuable feedback from interested stakeholders and optimize the released prototypes that will undergo a pre-industrialization/optimization process.

7 REFERENCES

References as included in the ANASTACIA White Paper – included for completeness:

[Aiello, 2013] Aiello, M., Cambiaso, E., Scaglione, S., & Papaleo, G. (2013, July). A similarity based approach for application DoS attacks detection. In Computers and Communications (ISCC), 2013 IEEE Symposium on (pp. 000430-000435). IEEE.

[AALTO: 1] S. Lal, A. Kalliola, I. Oliver, K. Ahola, and T. Taleb, "Securing VNF Communication in NFVI," in Proc. IEEE CSCN'17, Helsinki, Finland, Sep. 2017.

[AALTO: 2] -S. Lal, I. Oliver, S. Ravidas, T. Taleb, "Assuring Virtual Network Function Image Integrity and Host Sealing in Telco Cloud," in Proc. IEEE ICC 2017, Paris, France, May 2017.

[AALTO: 3] -S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," in IEEE Communications Magazine., Vol. 55, No. 8, May 2017, pp. 211 – 217.

[Beitollahi, 2011] Beitollahi, H., & Deconinck, G. (2011). A dependable architecture to mitigate distributed denial of service attacks on network-based control systems. International Journal of Critical Infrastructure Protection, 4(3-4), 107-123.

[Belabed, 2018] D Belabed, M Bouet, D Rivera, P Sobonski, A Molina Zarca "Initial Security Enforcement Enablers Report" Anastacia EU project deliverable D3.3.

[Bouet, 2017] M. Bouet, V. Conana, Geo-partitioning of MEC resources, ACM MECOMM '17, August 21, 2017, Los Angeles, CA, USA

[Bouet, 2018] M. Bouet, V. Conana, Mobile Edge Computing Resources Optimization: A Geo-Clustering Approach, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 15, NO. 2, JUNE 2018

[Brynielsson, 2015] Brynielsson, J., & Sharma, R. (2015, August). Detectability of low-rate HTTP server DoS attacks using spectral analysis. In Advances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on (pp. 954-961). IEEE.

[Cambiaso, 2012] Cambiaso, E., Papaleo, G., & Aiello, M. (2012, October). Taxonomy of slow DoS attacks to web applications. In International Conference on Security in Computer Networks and Distributed Systems (pp. 195-204). Springer, Berlin, Heidelberg.

[Cambiaso, 2013] Cambiaso, E., Papaleo, G., Chiola, G., & Aiello, M. (2013). Slow DoS attacks: definition and categorisation. International Journal of Trust Management in Computing and Communications, 1(3-4), 300-319.

[Cambiaso, 2016] Cambiaso, E., Papaleo, G., Chiola, G., & Aiello, M. (2016). A Network Traffic Representation Model for Detecting Application Layer Attacks. International Journal of Computing and Digital Systems, 5(01).

[Cambiaso, 2017] Cambiaso, E., Papaleo, G., & Aiello, M. (2017). Slowcomm: Design, development and performance evaluation of a new slow DoS attack. Journal of Information Security and Applications, 35, 23-31.

[Duravkin, 2014] Duravkin, I. V., Carlsson, A., & Loktionova, A. S. (2014). Method of slow-attack detection. Системи обробки інформації, (8), 102-106.

[Quesada Rodriguez et al., 2018-1] Quesada Rodriguez, Adrian; Bajic, Bojana; Crettaz, Cédric; Menon, Mythili; Pacheco Huamani, Ana María; Kim, Eunah; Loup, Vincent; Ziegler, Sébastien. "Dynamic Security and Privacy Seal Model Analysis". 2018. H2020 Anastacia EU project deliverable 5.1.

[Quesada Rodriguez et al., 2018-2] Quesada Rodriguez, Adrian; Bajic, Bojana; Crettaz, Cédric; Filipponi, Matteo; Pacheco Huamani, Ana María; Perlini, Adriano, Kim, Eunah; Loup, Vincent; Ziegler, Sébastien. “Dynamic Security and Privacy Seal Monitoring Service”. 2018. H2020 Anastacia EU project deliverable 5.2.

[Zarca et al., 2019] Zarca, A.M., Bernabe, J.B., Trapero, R., Rivera, D., Villalobos, J., Skarmeta, A., Bianchi, S., Zafeiropoulos, A. and Gouvas, P., 2019. Security Management Architecture for NFV/SDN-aware IoT Systems. IEEE Internet of Things Journal.