ANASTACIA

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

D2.4

Secure Software Development Guidelines Initial Report

This document aims to be used as reference for developers in order to implement secure IoT/CPS infrastructures. The methodology presented in this document permits to exhaustively follow the development of secure preventive actions within the implementation of components and mechanisms included in a IoT/CPS infrastructure, allowing also for the backwards traceability analysis of implementation activities and the evaluation of severity and criticality of security threats.

Distribution level	PU
Contractual date	30.06.2018 [M18]
Delivery date	30.06.2018 [M18]
WP / Task	WP2 / T2.4
WP Leader	UMU
Authors	Ruben Trapero (ATOS), Stefano Bianchi (SOFT), Enrico Cambiaso (CNR), Alejandro. Molina (UMU, Sofianna Menesidou (UBITECH), Rafael Marin-Perez (ODINS), Yacine Khettab (AALTO)
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

Index of figures

Index of tables

PUBLIC SUMMARY

This deliverable presents a complete methodology that supports the development of secure software. It is based on the analysis and evaluation of security requirements and security threats, including also their impact, criticality and severity within the developed platform. The main result of this methodology is a set of guidelines for supporting the implementation of actions to prevent security threats. This methodology feeds from several existing approaches, such as the secure software development created by Microsoft, the threat taxonomy produced by ENISA and the threat modelling developed in OWASP. These approaches have been adapted to fit in the particularities of an IoT/CPS infrastructure. This deliverable describes this methodology and applies it to the development of the ANASTACIA platform as one of the most representative examples of the development of a secure IoT/CPS infrastructure.

The result of the methodology consists on a set of prevention actions to mitigate (or at least reduce the probability of) being affected by security threats. These prevention actions set the baseline for the implementation of concrete implementation actions. In fact, this methodology has been validated in the context of the ANASTACIA framework, providing feedback to the component implementation activities about concrete actions for the development of secure software components.

Additionally, the methodology presented here allows for an easy traceability of the development process, from prevention actions to security requirements, which can be used to follow up the fulfilment of the security requirements. All together helps to focus the developing efforts on platform components with higher priority, which is given by the results of the methodology presented here.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document aims to be used as reference for developers in order to implement secure IoT/CPS infrastructures. The methodology presented in this document permits to exhaustively follow the development of secure preventive actions within the implementation of components and mechanisms included in a IoT/CPS infrastructure, allowing also for the backwards traceability analysis of implementation activities and the evaluation of severity and criticality of security threats.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- D1.2: User-centred Requirement Initial Analysis
- D1.3: Initial Architectural Design
- D2.2: Attack Threats Analysis and Contingency Actions Initial Report

1.3 REVISION HISTORY

Version	Date	Author	Description
0.1	21.12.2017	ATOS	ToC
0.2	16.1.2018	ATOS	Methodology
0.2	27.2.2018	UMU	Related work
0.3	10.3.2018	SOFT	Requirements
0.4	10.4.2018	CNR	Threats and requirements mapping
0.5	18.4.2018	ODINS/UBITECH	Threats and preventions mapping
0.6	20.4.2018	ATOS	Compilation of inputs and calculation of criticality and severity
0.7	4.5.2018	ALL	ANASTACIA approach for implementing preventions
0.8	20.5.2018	ALL	Mapping of preventions to ANASTACIA components
0.9	31.5.2018	ATOS, SOFT	Section filling and descriptions
1.0	15.6.2018	ATOS	Integrated version
1.0.1	22.6.2018	CNR	Internal review version
1.0.2	25.6.2018	ATOS	Final version

1.4 Acronyms and Definitions

Acronym	Meaning
AAA	Authentication Authorization Accounting
CA	Certification Authority
CPS	Cyber Physical Systems
DNS	Domain Name Service
DREAD	Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability
DSPS	Dynamic Security and Privacy Seal
DTLS	Datagram Transport Layer Security
ECC	Elliptic-curve cryptography
GUI	Graphic User Interface
IMPI	Intelligent Platform Management Interface
IoT	Internet of Things
NIDS	Intrusion detection system
OWASP	Open Web Application Security Project
P2M	Peer2Mail
PANA	Protocol for Carrying Authentication for Network Access
SDN	Software Defined Network
SSL	Secure Socket Layer
VNF	Virtual Network Function

2 RELATED WORK

Security and privacy aspects have become fundamental elements to consider to achieve a dependable global digital society. As technology evolves, it is important to make efforts to deliver a reliable and secured-by-design environment at each single technology. This approach is especially important in paradigms like IoT, where considerable heterogeneous deployments of devices are expected in a few years.

Fortunately, today we can find relevant documentation which provide a series of guidelines for secure software development considering main identified security threads and different technologies. Among the most relevant ones, the European Union Agency for Network and Information Security (**ENISA**) provides baseline security recommendations for IoT [1], where ENISA includes an IoT thread analysis over several IoT architectures to provide a good horizontal security approach in the context of the IoT ecosystem. This approach highlights that, to protect the IoT deployment, it is necessary to protect all systems involved, i.e., not only IoT devices, but also the network and the back-ends, since some security problems are not IoT specific, but rather inherited from the use of networking technologies.

Specifically, authors separate recommendations and good practices in three main categories: Policies, Organisational and Technical. The use of adequate policies according on the activity and the scope is the first recommendation, providing different actions and reactions depending on the criticality of the architecture. Through the application of the correct policies it is then easier to adopt approaches like security-by-design or privacy-by-design. For the second category, authors expose the importance of establishing organisational criteria for information security, highlighting points like the end-of-life strategy and the training of the personnel in terms of security and privacy aspects. Finally, regarding the technical category, it provides a set of technical measures to cope with security best practices, depending on the security area. For instance, to take advantage of secure hardware, it is suggested to establish trust during the bootstrapping process, to establish hard-to-crack passwords, to sign the device software by an authorised trust entity, to change the default credentials, to implement a fine-grained authorisation mechanism, to select properly standard and strong encryption algorithms and keys, to use of standardised security protocols, even to split of the network in order to ease the network section isolation. Concerning the technical category, it is also suggested to keep the components updated during the time, in order to protect from latest threats.

Following with the **ENISA** IoT recommendations, [2] exposes security challenges and best practices in the IoT environment. Specifically, authors remark an increase in monetisation of cyber-crime, crime as a service and of targeted attacks, e.g. ransomware or Mirai botnet. Among best practices, it is recommended an EU cybersecurity certification framework by ENISA, where products and services could be certified to ensure that they are adequate for their supposed purposes. This approach is aligned with the previous recommendations where the necessity to establish a trust authority is highlighted. Regarding the framework, it considers different areas such critical and high-risk areas, widely deployed digital products and, finally, low cost mass market products such as IoT devices [3]. Focusing on IoT, ENISA provides different recommendations and guidelines for different scenarios considering several IoT deployments. [4] provides good practices and recommendations for security and resilience of smart home environments, especially in the security of the development process including the design, development and testing phases. [5] shows guidelines to improve cyber security in smart cars, to improve information sharing and clarify liability amongst industry actors, to achieve consensus on technical standards for good practices or even to build tools for security analysis. [6] suggest advices regarding security and resilience for smart health service and infrastructures, including security good practices at organizational and technical levels, similarly to previous recommendations but also providing new ones (e.g., to establish effective enterprise governance for cyber security, implement state-of-the-art security measures, provide specific IT security requirements for IoT components in the hospital or invest on NIS products). Finally, [7] establish guidelines for smart cities, suggesting actions for municipalities, the European Commission and Member States, IoT

Operators, manufacturers and standard organizations. These guidelines are aligned with the main aim, i.e., regulation, certification and standardization of the IoT environments.

The **Cloud Security Alliance (CSA**), in [8], shows detailed low-level guidelines for a layered security protection to defend IoT assets. With this approach, CSA aims to cope with the challenges of the convergence between the Information Technology (IT) and the Operational Technology (OT), combining physical and cybersecurity components. Among other recommendations at the network layer, it suggests to use not only the basic firewall security features, but also Deep Packet Inspection (DPI) capabilities. They also recommend performing exercises of network access control and penetration tests regularly. At Application layer, it is important to use appropriate authentication and authorization mechanisms, perform scanners looking for hardcoded logins. If a project uses third-party libraries, it is important to maintain an inventory of those libraries and keep them updated, checking also possible vulnerabilities. At device level, the first recommendation resides on to ensure the IoT device is running the last firmware version. From here, they offer guidelines that include to verify the source of the updates, to change the default password (implementing a strong password policy), to change the default passwords on Bluetooth devices or to establish lockouts based on idle time and maximum attempts to authenticate. At Physical layer, it is mandatory the set-up a physical identity and access management infrastructure, establishing access control policies, distributing carefully the physical keys, monitoring cameras and devices, also documenting graphically the location of devices. Finally, the Human layer is related with security leader's designation, security and privacy training, vulnerabilities reporting and documenting all information regarding risks and security, establishing rankings according with the criticality.

On this topic, in [9] the GSM Association (**GSMA)** proposes security guidelines for the IoT service ecosystem. First, GSMA provides a set of answers to frequently asked security questions (how are users authenticated, how it is possible to identify anomalous endpoint behaviour, how can the service restrict an abnormal behaving point, how can be determined if a service has been hacked, what can I do once the service has been compromised or how should administrators interact with servers and services). Then, authors separate the recommendations in different levels (critical, high, medium and low). These recommendations include implementation of a Trusted Computing Base from a risk analysis, understanding it like a set of hardware, software, protocols and policies which will form the basis for any given computing platform. They also recommend the definition of: organizational root of trust (i.e. PKI architecture), bootstrapping method for defining parameters like authentication configurations, securitization of infrastructure for systems exposed to the public internet, providing among others DDoS resistance, load balancing, redundancy and firewalls. Other recommendations include the definition of a persistent storage model for long term availability, the definition of an administration model (which must include the administration authentication/authorization types, even how the administrator will interact with the resources), the definition of logging and monitoring mechanisms in order to detect anomalies like an increase of network traffic, abnormal CPU utilization and so on.

Regarding virtualization, in [10] **NIST** provides a guide to security for full virtualization technologies. Specifically, for the hypervisor, they establish some recommendations such as: keep the hypervisor updated, restrict the administrative access and protect all management communications, synchronize the virtualized infrastructure with a trusted time server, disconnect unused physical hardware or just enable extra hypervisor features if required (clipboard or file sharing…). For the guest OS, the best practices include the use of different authentication solutions and, in case one guest has been compromised, it is recommended to assume a potential infection to the rest of guests. Regarding the virtualized infrastructure advices, the recommendations are like those applicable in physical resources. For instance, if a virtual hard drive will be shared by several guests, only those guests should have access to the resource. Finally, the document establishes a clear difference among server and desktop virtualizations, since in desktop virtualizations the ability to control images is added. At this point, the recommendation is to provide a well-secured gest OS image for the desktop environment. This is strong recommended in e.g. teleworking cases. Once main recommendations are introduced, the document performs a secure virtualization planning and deployment, considering the following phases for the life-cycle: i) the initiation phase is related to the necessary tasks before the design of the virtualization solution, considering, among others, virtualization requirements and organization policies; ii) the planning and design phase specifies the technical characteristics of the solution; iii) the implementation phase performs the configuration and testbed deployments including event logging, network management, authentication, authorization, and so on; iv) the operation and maintenance phase is focused on security tasks and monitoring to detect attacks, incidents or malfunction, v) a disposition phase is focused on the end-of-life of the virtualization solution.

With regards to exploiting virtualization for networking, ONAP in [11] provided a simplified an easy comprehensive vision of the VNF guidelines provided by the **ETSI** SWA 001 document [12]. It exposes the main desirable properties for a VNF focusing on different capabilities. From the design point of view, the VNF should be carefully decomposed into loosely coupled, granular, re-usable VNF components (VNFCs) that can be distributed and scaled on a Network Cloud, providing independency of deployment, configuration and upgrade. Also, VNF must support horizontal scaling by adding/removing instances on demand, being able to manage their state. Regarding the resiliency, the VNF must be designed to survive to punctual failures over the platform. This is generally achieved through the replication in a distributed system. Security is also a vital point of this kind of technology and must be considered in the full life-cycle of the VNF. Beyond network security properties to apply to connect (if it is required) the new VNF with the rest of the architecture, there are several security requirements to tackle like VNF general security, identity and access management, API security, security analytics and data protection requirements. Moreover, each VNF should be accompanied of strong testing methodologies, continuous integration software to deploy as fast as possible the new software changes over the VNF. Also, it is desirable to provide lifecycle events and alarms.

In SDN terms, [13] is focused on providing guidelines for SDN experimentation and validation in Large-Scale real-world scenarios, presenting the “OpenFlow in Europe: Linking Infrastructure and Applications (OFELIA)” testbed project, which consists in a collaborative creation of an experimental OpenFlow-based research facility. To establish the experimentation guidelines, authors used several real SDN interconnected networks intending to emulate 1 million inhabitants. At this point, a list of main required components is provided, which include OpenvSwitch (OvS) as virtual switch, Floodlight as SDN controller, Queue installer as Floodlight queue extension, RouteFlow to provide virtualized IP routing services over OpenFlow enabled hardware, or a QoS Platform.

Related to SDN topics as well, **ENISA** in [14] shows the main architecture for SDN networks/5G, specifying different threads for the main components of the architecture, focusing then on good practices, threat mitigations and recommendations at different levels. Regarding the mitigation practices, authors shows an overview of a considered tools or techniques, as well as technical recommendations such as establishing mandatory encryption and authentication in the SDN North Bound Interface (NBI), South Bound Interface (SBI) and communications between SDN controllers (EWBI). Authors also recommend using sandboxing through network and application isolation, especially during the development process. Regarding the organisational recommendations, they are quite similar to those summarized on previous guidelines, focusing on allocation of responsibilities, keeping systems updated or using adequate security methods.

Finally, The Open Web Application Security Project (**OWASP**) in [15] provides an overview of software security and risk principles, focusing them in secure coding practices by coding area, including recommendations for input validation, authentication and password management, session management, cryptographic practices, data protection and communication security, and general coding good practices like use testbed and approved managed code.

3 RESEARCH METHODOLOGY

This section describes the methodology defined for the creation of guidelines for developing secure software over IoT/CPS. The process is based on an analytic approach that adapts the actions (for example, implementation actions) to the specific needs of an IoT/CPS deployment.

The development of secure software has become paramount during the last years. The time and resources consumed for correcting security issues once the software has been already complete is way higher than when the software has been designed secure. Many approaches have already been defined, as it has been already described in Section 2. ANASTACIA has used the Software Development Lifecycle defined by Microsoft [16] as starting point for the current methodology, simplifying it to be used within an IoT/CPS platform.

The process is summarized in Figure 3-1. It starts with the analysis of the security requirements and the threats associated to them, studying the impact of unfulfilling the requirement and the severity of the security threats. With this information, a set of prevention actions are defined, which are translated to concrete guidelines.

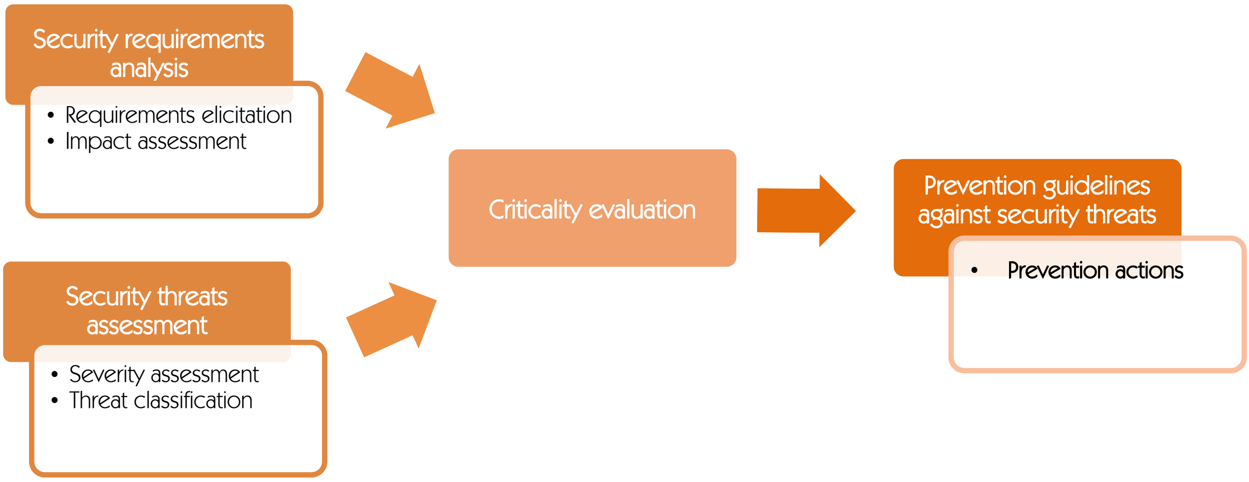
Security requirements analysis
• Requirements elicitation
• Impact assessment
Security threats assessment
• Severity assessment
• Threat classification
Criticality evaluation
Prevention guidelines against security threats
• Prevention actions

Figure 3-1. Research methodology for the definition of security guidelines for IoT/CPS

The three steps can be detailed as follows:

Security requirements analysis

Every platform has its own security requirements, depending on the criticality of the domain where it is used. Additionally, the importance of every requirements may be different depending on the domain where it is applied. Thus, it is necessary to evaluate and classify the requirements, which will indicate the level of relevance within the platform and will determine the priority of the security prevention actions to be carried out.

As already mentioned, the elicitation of the requirements depends on the analysed domain. In the case of ANASTACIA, we will consider the requirements elicited in WP1, which will be used as a valid sample of the more relevant requirements of a IoT/CPS deployment.

The next step comprises the assessment of the impact of every requirement. This assessment is based on a classification of the requirements per its relevance within three security aspects: integrity, availability and confidentiality. In general, three scores are given for every aspect (high, medium and low). These scores are used to determine the level of impact of every requirement within the assets (components, network, IoT devices, protocols, etc.) of the platform in case of their unfulfilment. These levels have been adapted and extended based on the ones defined by the IoT Security Foundation [17] and depends on the scores given to the aforementioned security aspects. The following table is used for the definition of such levels:

Table 3-1. Impact level according to the security aspects for IoT (source: IoT Security Foundation [17])

Compliance class	Security Objective		
	Integrity	Availability	Confidentiality
Level 0	Low	Low	Low
Level 1	Medium	Medium	Low
	Low	Medium	Medium
	Medium	Low	Medium
	Low	Low	High
	Low	High	Low
	High	Low	Low
Level 2	High ≠ Medium ≠ Low		
	Medium	Medium	Medium
Level 3	Medium	High	Medium
	High	Medium	Medium
	Medium	Medium	High
	High	High	Low
	Low	High	High
	High	Low	High
Level 4	Medium	High	High
	High	Medium	High
	High	High	Medium
Level 5	High	High	High

Every level represents the impact that every requirement has in the platform, with regards to either assets or data. Every level is incremental, which mean that the effects of a certain level include also the effects of the lower levels.

- Level 0: the unfulfilment of the requirement entails little impact on individuals or assets of the organization. Data is not affected.
- Level 1: the unfulfilment of the requirement entails a limited impact on individuals or assets of the organization. Data is not affected.
- Level 2: the unfulfilment of the requirement affect to the operation of certain devices due to certain threats. Data is not affected.
- Level 3: the unfulfilment of the requirement affect to the operation of certain devices due to certain threats. Non-sensitive data is affected.
- Level 4: the unfulfilment of the requirement entail the leakage of sensitive data including sensitive personal data.

- Level 5: the unfulfilment of the requirement might impact to the critical infrastructure or even cause personal injury.

The following template will be used to define the impact and the values for the three security aspects studied for every requirement.

Table 3-2. Requirements assessment template

Req ID	Description	Integrity	Availability	Confidentiality	Impact Level
Req_id		*Low/Medium/High*	*Low/Medium/High*	*Low/Medium/High*	*0,1,2,3,4,5*

The result of this analysis will be used for the evaluation of the criticality of the security requirements, which will be further used to determine the importance of the prevention guidelines. Before evaluating the criticality, it is also necessary to evaluate the threats associated to the elicited security requirements. This activity can be carried out in parallel to the requirements analysis.

Security Threats Assessment

It is very difficult to be protected against any threat. Sometimes it is because the system is too large and it is not easy to consider all the potential dangers. Sometimes it is because many threats are not known at the time of developing the components of a platform, as new bugs are discovered and new attacks are constantly appearing (zero day attacks). Therefore, any system is exposed to threats, known and unknown ones. One way to analyse the exposition to a threat is evaluating the security requirements that try to mitigate them. Figure 3-2 depicts the process that supports this threat assessment.

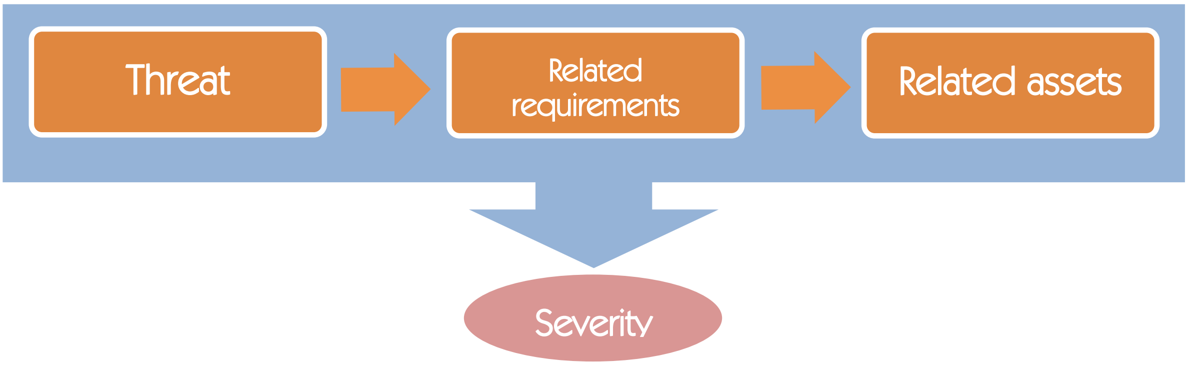

Figure 3-2. Threat assessment process

The following template will be used to list the threats and related security requirements.

Table 3-3. Template for requirements related to threats

Threat ID	Threat description	Related security Requirements
A unique id given to the threat	*Description of the threat*	*IDs of the requirements*

This process is used to evaluate the severity of the threats. This severity is evaluated following the DREAd methodology [18]. The DREAd methodology gives scores to five aspects that are related to security threats. The number of levels for each score can vary although it is mandatory that they use the same scale (for example, from 0 to 10):

- *Damage (D)*: indicates the impact against the assets of the infrastructure, which, depending on the degree if damage, might affect to the correct operation of the device.
- *Reproducibility (R)*: indicates how easy the threats is to be repeated.
- *Exploitability (E)*: indicates the expertise required to be able to exploit this threat.

- *Affected user (A)*: different criteria can be chosen here. It can indicate the number of users affected for the threat or can also indicate the importance of the users affected (user admins vs restricted users).
- *Discoverability (d)*: indicates how easy or difficult is to discover the threat.

The average score of every aspect represents the severity of the threat and will be used to define the criticality of the requirements. Notice that we are assuming that the five aspects have the same level of importance. It is possible to assign different levels of importance to different aspects (for example, for a very critical infrastructure the aspect “Damage” might be more important that the rest).

The following template will be used to evaluate the severity of the threats identified. We have also included the assets affected for the threat. This will allow for an easy traceability and evaluation of the impact.

Table 3-4. Template for quantifying the severity of threats.

Threat ID	Threat	Related ANASTACIA elements	Partial scores for severity {0, 5, 10}					Severity (risk)
			D	R	E	A	d	
Unique ID of the threat		*List of assets*						*Average of partial scores*

Criticality evaluation

The following step comprises the calculation of the criticality of the requirements, based on the impact of the requirements and the severity of the related threats.

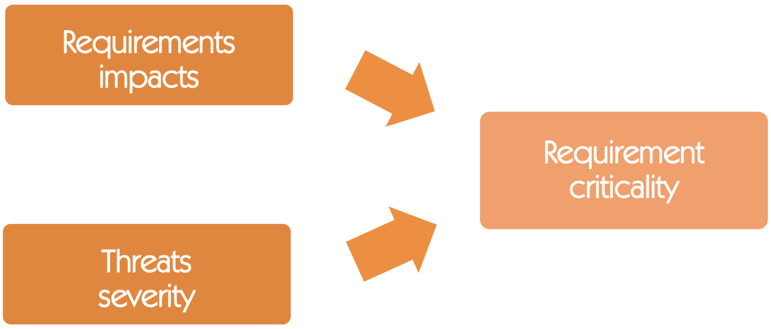

Figure 3-3. Input for the requirements criticality

For calculating the criticality it is necessary to normalize the impact level of the requirements to the scale used for the threats severity. This impact level was defined as a six steps level (from 0 to 5) while the scale of the threat severity as a number between 0 and 10. Therefore, a possible normalization would be the following:

$$\hat{C} = S * \frac{k}{K};\ k = (0, \dots, K)$$

With:

Ĉ = Normalized Criticality
S = Threat severity
K = Maximum requirement impact level

For the aforementioned example, the criticality level results in the following:

Table 3-5. Normalization of criticality levels

Criticality level	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Score	0	*10 * 1/5*	*10 * 2/5*	*10 * 3/5*	*10 * 4/5*	10

Note that there are more complex algorithms existing in other domains, such as the Multi Criteria Decision Making – MCDM [19], or algorithms considering the non-linear definitions of levels. However, they were not considered in this context, as these algorithms are more suitable for cases where the importance of the different criteria differs or when there is a hierarchical relationship between them.

These scores are used to determine the priority of the security requirements. This is important, as it allows developers to know what components are exposed to what threats and therefore what are the threats that need to be prevented yet at design time. Knowing this information, it is possible to define guidelines to be considered during the development of components. This also allows to perform a backwards traceability: in case of a successful attack we can know what are the threats associated to the attack, and thus what security requirement are affected and therefore what components might be affected.

Prevention guidelines against security threats

The last step comprises the definition of concrete guidelines to prevent security threats. To this end, the results of the previous steps provides a good input to know about the priority of actions defined in these guidelines. Previous steps provide a mapping between the expected security requirements, the related threats and the components affected. Additionally, the criticality shows what is the level of importance of every security requirement, which is calculated considering variables such as the impact and the severity of the related threats. Next figure represents the process for defining security guidelines based on the severity and criticality defined for threats and security requirements. The process considers the components affected by the threats, and relevant for the security requirements defined.

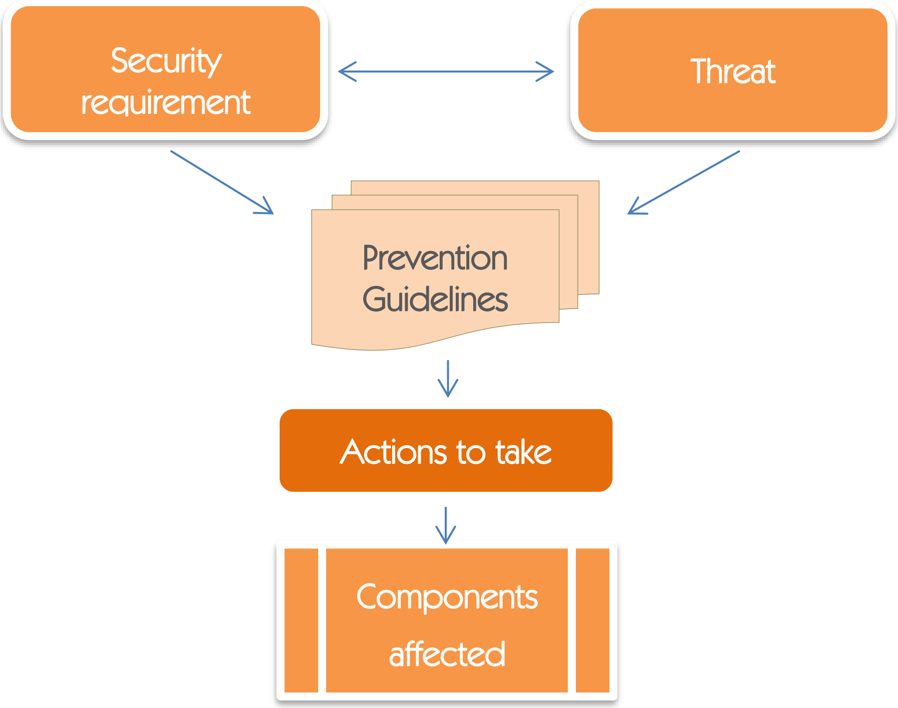

Figure 3-4. Process for the definition of guidelines

The following template will be used for the definition of the prevention guidelines. The actions included in the guidelines will be mapped to the threats that they are preventing, and to the components affected. The type of component is also included, which will determine the type of prevention action to be implemented in such component.

Table 3-6. Security guidelines for the prevention of threats

Thread ID	Security Threats	Prevention recommendation guidelines	ANASTACIA approach	Components affected

4 IMPACT OF SECURITY REQUIREMENTS ON IOT/CPS

In order to provide actionable information on the main security functionalities and constraints that must be covered by these guidelines, this section provides a summary and a classification of the security related requirements, after the extension and refinement process that has been initiated and carried out in WP1 (Task 1.2 “User Centred Requirement Analysis”) and that will produce deliverable D1.4 “Final User-Centred Requirement Analysis”. This section also works as validation of the complete methodology described in the previous section. To this end we have used the development of the ANASTACIA platform as context for this validation.

For every security-related requirement, considering its role as for covering Integrity, Availability and Confidentiality constraints, scores (**LOW**, MEDIUM, **HIGH**) have been assigned and the Impact Level has been calculated as for the criteria indicated in Table 3-1.

This approach allows to have the security-related requirements classified by level of importance with respect to security objectives.

Table 4-1. Requirements assessment: evaluation of impact

Req ID	DESCRIPTION	Integrity	Availability	Confidentiality	Impact Level
UFR-1	The ANASTACIA system will provide CREATE functionality for security policies that must be autonomously applied in case a threat is detected	HIGH	HIGH	MEDIUM	4
UFR-2	The ANASTACIA system will provide RETRIEVE functionality for security policies that must be autonomously applied in case a threat is detected	HIGH	HIGH	MEDIUM	4
UFR-3	The ANASTACIA system will provide UPDATE functionality for security policies that must be autonomously applied in case a threat is detected	HIGH	HIGH	MEDIUM	4
UFR-4	The ANASTACIA system will provide DELETE functionality for security policies that must be autonomously applied in case a threat is detected	LOW	LOW	LOW	0
UFR-9	The ANASTACIA system will provide tools that automatically enforce the security policy to apply in case a threat is detected	HIGH	HIGH	MEDIUM	4
UFR-11	The ANASTACIA system will provide CREATE functionalities for the definition of the devices included in the monitored system	MEDIUM	MEDIUM	LOW	1
UFR-12	The ANASTACIA system will provide RETRIEVE functionalities for the definition of the devices included in the monitored system	MEDIUM	MEDIUM	MEDIUM	2
UFR-13	The ANASTACIA system will provide UPDATE functionalities for the definition of the devices included in the monitored system	LOW	LOW	LOW	0

UFR-14	The ANASTACIA system will provide DELETE functionalities for the definition of the devices included in the monitored system	LOW	LOW	LOW	0
UFR-15	The ANASTACIA system will provide CREATE functionalities for the definition of the network topology included in the monitored system	MEDIUM	MEDIUM	LOW	1
UFR-16	The ANASTACIA system will provide RETRIEVE functionalities for the definition of the network topology included in the monitored system	HIGH	HIGH	LOW	3
UFR-17	The ANASTACIA system will provide UPDATE functionalities for the definition of the network topology included in the monitored system	HIGH	MEDIUM	LOW	2
UFR-18	The ANASTACIA system will provide DELETE functionalities for the definition of the network topology included in the monitored system	LOW	LOW	LOW	0
UFR-19	The ANASTACIA system will include an interactive graphical visualization of the network of the monitored system	LOW	LOW	LOW	0
UFR-20	The ANASTACIA system will include an interactive graphical visualization of the devices included in the monitored system	LOW	LOW	LOW	0
UFR-21	The ANASTACIA system will include components for the monitoring of network traffic	HIGH	HIGH	HIGH	5
UFR-22	The ANASTACIA system will include agents for the monitoring of devices	HIGH	HIGH	HIGH	5
UFR-23	The ANASTACIA system will include functionalities for the interactive control of devices	MEDIUM	MEDIUM	LOW	1
UFR-24	The ANASTACIA system will include reasoning capabilities to filter relevant data out of information collected through network monitoring	MEDIUM	MEDIUM	MEDIUM	2
UFR-25	The ANASTACIA system will include reasoning capabilities to filter relevant data out of information collected through device monitoring	LOW	LOW	LOW	0
UFR-26	The ANASTACIA system will include reasoning capabilities to identify potential security threats	HIGH	HIGH	HIGH	5
UFR-28	The ANASTACIA system will include reasoning capabilities to define mitigation plans according to the defined security and privacy policies and the identified threats and breaches, and to verify if the deployment of security mitigation actions	HIGH	HIGH	HIGH	5

	alter significantly the privacy status of the monitored system, eventually deciding if proceeding or not od asking for confirmation to the system administrator				
UFR-29	The ANASTACIA system will include orchestrating capabilities to manage the correct implementation/orchestration of mitigation plans	HIGH	HIGH	HIGH	5
UFR-30	The ANASTACIA system will include capabilities to implement mitigation plans by means of proper security enablers	HIGH	HIGH	HIGH	5
UFR-31	The ANASTACIA system will include enforcing capabilities to deploy mitigation actions in the monitored system at IoT level	HIGH	HIGH	HIGH	5
UFR-32	The ANASTACIA system will include enforcing capabilities to deploy mitigation actions in the monitored system at SDN level	HIGH	HIGH	HIGH	5
UFR-33	The ANASTACIA system will include enforcing capabilities to deploy mitigation actions in the monitored system at NFV levels	HIGH	HIGH	HIGH	5
UFR-34	The ANASTACIA system will include reasoning capabilities to define the status of the Dynamic Security and Privacy Seal (DSPS) for the monitored system according to the information received as for identified threats & breaches and the associated mitigation plans	MEDIUM	MEDIUM	MEDIUM	2
UFR-35	The ANASTACIA system will include a web interface for the visualization of 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)	MEDIUM	MEDIUM	LOW	1
UFR-36	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)	LOW	LOW	LOW	0
UFR-37	The ANASTACIA system will include functionalities to retrieve the history of the DSPS status for the monitored system	LOW	LOW	LOW	0

UFR-38	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, storing it on a dedicated repository	LOW	LOW	LOW	0
UFR-39	The ANASTACIA system will include functionalities to retrieve reports generated for the monitored system	LOW	LOW	LOW	0
UFR-40	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	LOW	LOW	0
UFR-41	The ANASTACIA systems will include autonomic reasoning/self-learning capabilities to modify/adapt security policies according to the previously defined mitigation plans and deployed mitigation actions	LOW	LOW	LOW	0
UFR-42	The ANASTACIA systems will include autonomic reasoning/self-learning capabilities to modify/adapt privacy policies according to the previously defined mitigation plans and deployed mitigation actions	LOW	LOW	LOW	0
UFR-43	The ANASTACIA system will include functionalities to translate high-level policies to low-level policies to be enforced on the monitoring system	LOW	LOW	LOW	0
UFR-44	The ANASTACIA system will include functionalities to allow seamless exchange of data between the different modules included in the different planes	HIGH	LOW	LOW	1
UFR-59	The ANASTACIA system will include functionalities to update in a timely manner the knowledge base that ensures it is able to recognize and address new security risks as they arise/are generated due to technological advances.	LOW	LOW	LOW	0
UFR-61	The ANASTACIA system will provide functionalities to cope with IOTs functions heterogeneity that must be conveyed in an abstract way to user services	HIGH	LOW	LOW	1
UFR-62	The ANASTACIA system will enable remote control and configuration of devices included in the monitoring system	HIGH	HIGH	HIGH	5

UFR-63	The ANASTACIA system will provide functionalities to allow that a IoT device is properly registered and identified before interacting to a service	HIGH	HIGH	HIGH	5
UFR-64	The ANASTACIA system will provide functionalities to allow that a IoT device shall be authorized to interact with a service	HIGH	HIGH	HIGH	5

Of the above 43 security related requirements (extracted from the extended version of 64 privacy and security requirements resulting from WP1), 16 requirements have an Impact Level 0, 6 requirements have an Impact Level 1, 4 requirements have an Impact Level 2, 1 requirement has Impact Level 3, 4 requirements have Impact Level 4 and finally 12 requirements have Impact Level 5, as reported in Table 4-2.

Table 4-2. Impact levels for security related requirements - occurrences and associated percentages

Adopted color	Impact level	Occurrences	Percentages
🟩	0	16	37%
🟩	1	6	14%
🟨	2	4	9%
🟧	3	1	2%
🟧	4	4	9%
🟥	5	12	28%

The percentages of calculated impact levels are visually depicted in Figure 4-1, that highlights how over 50% of requirements (~60%) are classified with a LOW/MEDIUM impact level (from 0 to 2) and nearly 40% are classified with a MEDIUM/HIGH impact level (from 3 to 5).

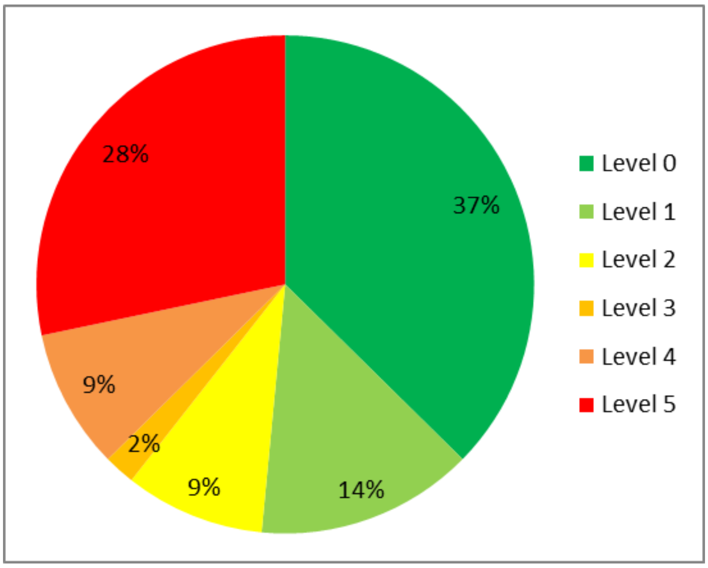

Figure 4-1. Percentages of impact levels as for security-related requirements

The following charts also provide a quick glance of the distribution of the Impact Levels, for the sake of analysis and comprehension.

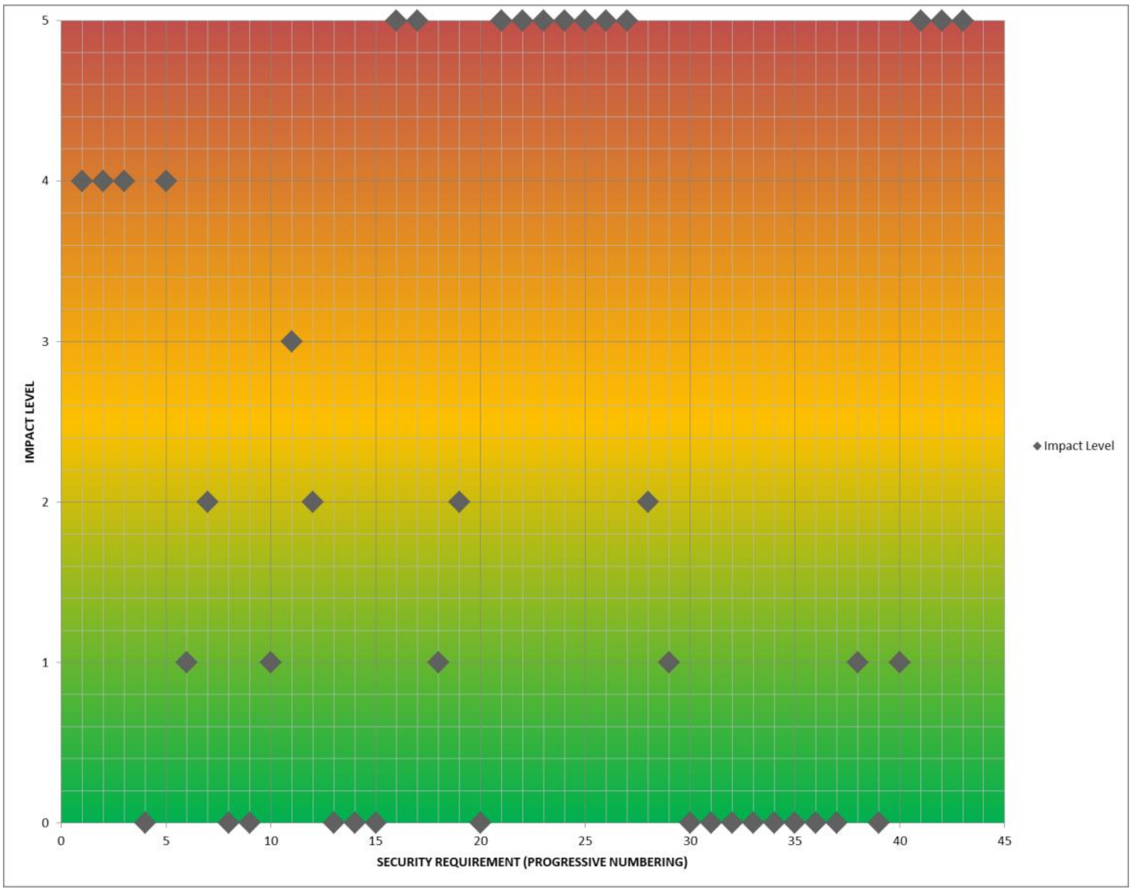

Figure 4-2. Overview of severity of calculated impact levels for security-related requirements.

5 GUIDELINES FOR SECURITY THREATS PREVENTION

Next step in the evaluation methodology comprises the elicitation of security threats in the IoT/CPS domain. This section presents the identified main security threats, linking them to the security requirements elicited in the previous section and evaluating the severity and criticality of these threats which will be used to determine the most relevant ones, the actions to prevent them and the priority of such preventions.

5.1 SECURITY THREATS ASSESSMENT

During deliverable D2.2 an initial study of active and passive attacks was presented, which resulted in 11 categories of attacks. This section extends the initial study reported in D2.2, adding more granularity to the categories identified. To this end, the list of security threats here presented feeds from the ENISA Threat taxonomy report [20]. It is worth noticing that, from the complete threat taxonomy produced by ENISA, we have selected those that are, to some extent, relevant for a IoT/CPS infrastructure. In order to justify the relevance of such threats we have also mapped every threat to the affected security requirements.

The following table shows the list of threats, their description and the related requirements for every threat given by its requirement identifier. Annex I also shows a different representation of the mapping between requirements and threats

Table 5-1. Security threats vs requirements

Threat ID	Threat	Description	Related Requirements
T1	Data flow from device is interrupted	External or internal intermission might entail the interruption of the data generated by a device	UFR-1 UFR-2 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-2 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-3 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T2	Code execution due to buffer overflow vulnerability	Threat of exploiting a buffer overflow vulnerability which would allow to write outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-2 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T3	Unauthorized access to the platform by malicious users	Access to platform by malicious users which might entail access to resources with different possible levels of privilege.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-12 UFR-16 UFR-17 UFR-21 UFR-22 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T4	Denial of Service attacks (Spoofing,	Threat of service unavailability due to	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17

	Flooding, Ping of Death, WinNuke, XDoS)	massive requests for services through Ping-ICMP	UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T5	SQL Injection	Threat of utilizing custom web applications embedded within social media sites, which can lead to installation of malicious code onto computers to be used to gain unauthorized access.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T6	0-day vulnerability to remotely target a device	Threat of attacks using 0-day or known IT assets vulnerabilities.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-11 UFR-12 UFR-15 UFR-16 UFR-17 UFR-21 UFR-22 UFR-23 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T7	Malware spread via network to exploit sensitive sensors	Threat of spreading malware from an infected computer to others by exploiting vulnerabilities of the devices exposed to the network	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T8	Identity fraud	Threat of identity theft action.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T9	Unsolicited & infected e-mail	Threat emanating from unwanted emails that may contain infected attachments or links to malicious / infected web sites.	UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-62 UFR-63 UFR-64
T10	Malicious code/software activity	Threat of malicious code or software execution.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T11	Abuse of information leakage	Threat of leaking important information.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29

			UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T12	SSL CA infiltration	Threat of use of rogue certificates.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T13	Manipulation of hardware & software	Threat of unauthorised manipulation of hardware and software.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-11 UFR-12 UFR-15 UFR-16 UFR-17 UFR-21 UFR-22 UFR-23 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T14	Routing table manipulation	Threat of route packets of network to IP addresses other than that was intended via sender by unauthorised manipulation of routing table	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T15	DNS spoofing	Threat of falsification of DNS information	UFR-1 UFR-2 UFR-3 UFR-9 UFR-11 UFR-12 UFR-15 UFR-16 UFR-17 UFR-21 UFR-22 UFR-23 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T16	DNS poisoning	Threat of falsification of DNS information	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T17	Falsification of configuration	Threat of intentional manipulation due to falsification of configurations.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-

			61 UFR-62 UFR-63 UFR-64
T18	Autonomous System hijacking	Threat of overtaking by the attacker the ownership of a whole autonomous system and its prefixes despite origin validation.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T19	Misuse of audit tools	Threat of nefarious actions performed using audit tools (discovery of security weaknesses in information systems).	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T20	Falsification of records	Threat of intentional data manipulation to falsify records	UFR-1 UFR-2 UFR-3 UFR-9 UFR-11 UFR-12 UFR-15 UFR-16 UFR-17 UFR-21 UFR-22 UFR-23 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T21	Unauthorised use of administration of devices & systems	Threat of nefarious action due to unauthorised use of devices and systems	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T22	IMPI Protocol	Threat of unauthorised access to the information systems / network.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T23	DNS Register Hijacking	Threat of unauthorised access to the information systems / network.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T24	Unauthorised installation and use of software	Threat of nefarious action due to unauthorised use of software.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-

			61 UFR-62 UFR-63 UFR-64
T25	Unauthorised installation of software	Threat of unauthorised installation of software which might derive into unwanted malware software.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T26	Abuse of personal data compromising confidential information	Threat of illegal use of personal data	UFR-1 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-2 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T27	Abuse of authorizations	Threat of using authorised access to perform illegitimate actions	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T28	Malware infection using hoax attacks	Threat of loss of IT assets security due to cheating such as scam emails or phishing attempts	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T29	Badware (Virus, Worm, Trojan, Rootkit, Botnets, Spyware, Scareware)	Threat of malicious code or software execution.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-11 UFR-12 UFR-15 UFR-16 UFR-17 UFR-21 UFR-22 UFR-23 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T30	Remote activity (execution)	Threat of nefarious action by attacker remote activity.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T31	Targeted attacks (including ATP)	Threat of sophisticated, targeted attack which combine many attack techniques.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T32	War driving	Threat of locating and possibly exploiting	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-

		connection to the wireless network.	30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T33	Interception compromising emissions	Threat of disclosure of transmitted information using interception and analysis of compromising emission.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T34	Targeted espionage attempts to obtain sensitive information	Threat of obtaining information secrets by dishonest means	UFR-1 UFR-2 UFR-9 UFR-12 UFR-21 UFR-22 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-62 UFR-63 UFR-64
T35	Rogue hardware	Threat of manipulation due to unauthorized access to hardware.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T36	Interfering radiations	Threat of failure of IT hardware or transmission connection due to electromagnetic induction or electromagnetic radiation emitted by an outside source.	UFR-1 UFR-2 UFR-3 UFR-9UFR-11 UFR-12 UFR-15 UFR-16 UFR-17 UFR-21 UFR-22 UFR-23 UFR-24 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-62 UFR-63 UFR-64
T37	Replay of messages	Threat in which valid data transmission is maliciously or fraudulently repeated or delayed.	UFR-1 UFR-3 UFR-9 UFR-16 UFR-17 UFR-2 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T38	Network reconnaissance and information gathering	Threat of identifying information about a network to find security weaknesses.	UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-62 UFR-63 UFR-64
T39	Man in the middle/ session hijacking	Threats that relay or alter communication between two parties.	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64

T40	Repudiation of actions	Threat of intentional data manipulation to repudiate action.	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T41	Damage caused by a third party (External or internal)	Threats of damage to IT assets caused by third party	UFR-1 UFR-2 UFR-3 UFR-9 UFR-16 UFR-17 UFR-21 UFR-22 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-44 UFR-61 UFR-62 UFR-63 UFR-64
T42	Loss of (integrity of) sensitive information	Threats of losing information or data, or changing information classified as sensitive	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T43	Loss of information in the cloud or destruction of devices, storage media and documents	Threats of losing information or data	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64
T44	Information leakage	Threat of leaking important information	UFR-1 UFR-2 UFR-3 UFR-4 UFR-9 UFR-11 UFR-12 UFR-13 UFR-14 UFR-15 UFR-16 UFR-17 UFR-18 UFR-19 UFR-20 UFR-21 UFR-22 UFR-23 UFR-24 UFR-25 UFR-26 UFR-28 UFR-29 UFR-30 UFR-31 UFR-32 UFR-33 UFR-34 UFR-35 UFR-36 UFR-37 UFR-38 UFR-39 UFR-40 UFR-41 UFR-42 UFR-43 UFR-44 UFR-59 UFR-61 UFR-62 UFR-63 UFR-64

The next step in the methodology is the evaluation of the severity of every threat. The severity is evaluated using the OWASP model, as described in section 3. The five factors used in the OWASP model are mapped to three possible scores. The meaning of every score depends on the factor to evaluate and on the domain where it is applied. In this case, the following table represents the scores used for every factor and its meaning for the IoT/CPS context:

Table 5-2. Scores used for the calculation of the threat severity

Aspect	Possibility	Score	Description
Damage	Low	0	Very few assets are potentially affected by this threat (20% of total at most)
	Medium	5	A medium number of assets are potentially affected by this threat (between 20% and 60% of total)
	High	10	Many devices are potentially affected by this threat (more than 60% of total)
Reproducibility	Not easy	0	The threat can be repeated just under very specific

			circumstances which are difficult to achieve (for example, just when an asset is online)
	Easy	5	The threat is easy to be repeated because the circumstances that allows its occurrence are likely to happen (for example, assets exposed to the public internet)
	Very easy	10	The threat can be repeated very easily, (for example, just by sending emails or pushing a button)
Exploitability	Expert	0	Very high expertise is required to be able to exploit the threat (for example, just by specialized hackers that exploit zero day vulnerabilities)
	Skilled	5	Malicious users with technical skills are able exploit the threat (for example, trigger denial of service attacks using well known Linux distributions)
	Newbie	10	Users with very basic expertise are able to exploit the threat (for example, sending emails with infected attachments)
Affected Users	Few/not important	0	Very few (or not privileged users) are affected by the threat (for example, users without access to the core of the infrastructure)
	Quite a few	5	The threat affects to a relevant number of users which might have access to relevant (not critical) parts of the infrastructure (for example users with read-only permissions to access to databases)
	Many/very important	10	The threat affects to many users or to very relevant ones (for example, sys admins with writing permissions)
discoverability	Unknown threats	0	The threat is extremely difficult to be discovered (for example, zero day vulnerabilities)
	Exploitation tool needed	5	The threat is exploitable by using tools available on the Internet (e.g. applications to exploit Wi-Fi networks, metasploit scripts, etc.)
	Direct exploitation	10	No specific tools are required to exploit the threat (e.g. send of an exploitation message/SMS, open an exploitation URL, etc.)

These scores have been used to evaluate the severity of every threat. Expert knowledge from members of the ANASTACIA consortium have been used to assign the corresponding scores to every aspect of the DREAd methodology and for every threat. The total severity is calculated as the average of the partial scores given for every aspect evaluated.

The following table shows the list of threats and the corresponding partial scores and severity. The table also represents the ANASTACIA components that might be exposed to every threat. This mapping will be used to trace threats and prevention actions, in order to know what are the prevention actions that every component should take care of (for example, to implement specific mechanisms to support those preventions).

Table 5-3. Evaluation of security threats severity

Threat ID	Threat	Related ANASTACIA elements	Partial scores for severity {0, 5, 10}					Average severity
			D	R	E	A	d	
T1	Data flow from device is interrupted	All components	5	10	5	10	5	7

T2	Code execution due to buffer overflow vulnerability	Policy Editor Tool Incident detector Attack Signatures Security policies repository Verdicts and Decision Support System Security Enabler Repository Security orchestrator	10	10	0	5	0	5
T3	Unauthorized access to the platform by malicious users	IoT nodes	10	5	5	5	5	6
T4	Denial of Service attacks (Spoofing, Flooding, Ping of Death, WinNuke, XDoS)	All components	0	10	10	5	5	6
T5	SQL Injection	Security orchestrator Attack signatures Security policies repository Verdict Reactions Security Enabler Repository	10	5	0	10	0	5
T6	0-day vulnerability to remotely target a device	All components	10	0	0	5	0	3
T7	Malware spread via network to exploit sensitive sensors	Policy Editor Tool Attack Signatures Orchestrator Security Enabler Repository	5	10	5	5	10	7
T8	Identity fraud	User plane components Databases of the infrastructure	10	5	5	5	0	5
T9	Unsolicited & infected e-mail	User plane components IoT nodes	5	10	10	10	5	8
T10	Malicious code/software activity	All components	10	0	0	0	0	2
T11	Abuse of information leakage	All components	5	0	5	5	0	3
T12	SSL CA infiltration	All components	5	0	0	5	10	4
T13	Manipulation of hardware & software	User plane components Incident detector Verdict and Decision Support System IoT nodes IoT networks	10	0	0	5	0	3
T14	Routing table	All components	0	0	5	5	0	2

	manipulation							
T15	DNS spoofing	IoT network	5	0	0	10	5	4
T16	DNS poisoning	IoT network	5	0	0	10	5	4
T17	Falsification of configuration	All components	10	0	0	0	0	2
T18	AS hijacking	IoT network	5	0	0	0	0	1
T19	Misuse of audit tools	IoT nodes	0	0	5	0	0	1
T20	Falsification of records	All components	0	0	5	5	0	2
T21	Unauthorised use of administration of devices & systems	All components	10	5	5	5	5	6
T22	IMPI Protocol	All components	5	0	0	5	0	2
T23	DNS Register Hijacking	User plane components IoT network	0	10	10	5	5	6
T24	Unauthorised installation and use of software	All components	5	5	5	0	10	5
T25	Unauthorised installation of software	All components	5	5	5	0	10	5
T26	Abuse of personal data compromising confidential information	IoT nodes User plane components All databases of the platform Incident Detector Verdict and Decision Support System	5	0	5	5	0	3
T27	Abuse of authorizations	User plane components IoT nodes	5	0	5	5	0	3
T28	Malware infection using hoax attacks	Incident Detector Verdict and Decision Support System	10	10	10	10	5	9
T29	Badware (Virus, Worm, Trojan, Rootkit, Botnets, Spyware, Scareware)	All components	5	10	5	5	10	7
T30	Remote activity (execution)	All components	5	5	5	0	5	4
T31	Targeted attacks (including ATP)	All components	10	5	5	5	5	6

T32	War driving	All components	0	0	5	5	5	3
T33	Interception compromising emissions	All components	5	10	0	5	5	5
T34	Targeted espionage attempts to obtain sensitive information	All components	0	0	10	0	0	2
T35	Rogue hardware	IoT nodes	5	5	5	5	5	5
T36	Interfering radiations	IoT network IoT nodes Virtualized Infrastructure Domain Control and Management Domain Monitoring components	5	10	0	5	5	5
T37	Replay of messages	All components	5	10	0	5	5	5
T38	Network reconnaissance and information gathering	All components	5	0	5	5	0	3
T39	Man in the middle/ session hijacking	All components	5	5	5	10	5	6
T40	Repudiation of actions	User plane components	5	10	5	5	0	5
T41	Damage caused by a third party (External or internal)	All databases of the platform	5	0	0	5	0	2
T42	Loss of (integrity of) sensitive information	All components	10	0	5	0	5	4
T43	Loss of information in the cloud or destruction of devices, storage media and documents	All databases of the platform	10	0	5	0	5	4
T44	Information leakage	IoT network IoT nodes Virtualized Infrastructure Domain Control and Management Domain Monitoring components All databases of the platform	10	0	5	0	5	4

In order to better visualize the results of the analysis, the following graph represents the severity of the threats ordered from the most important ones to the less important ones. It is worth noticing that in this evaluation all aspects have been considered with the same weight. Depending on the domain it is possible that the assignment of scores can give more importance to some aspect. For example, in an infrastructure where the personal information is critical (such as the infrastructure of a bank) the Damage and the Affected User aspects might have a higher weight rather than rest, as threats with a high score in these aspects mean that a potential attack would allow attackers to can have access to databases where critical personal information is stored.

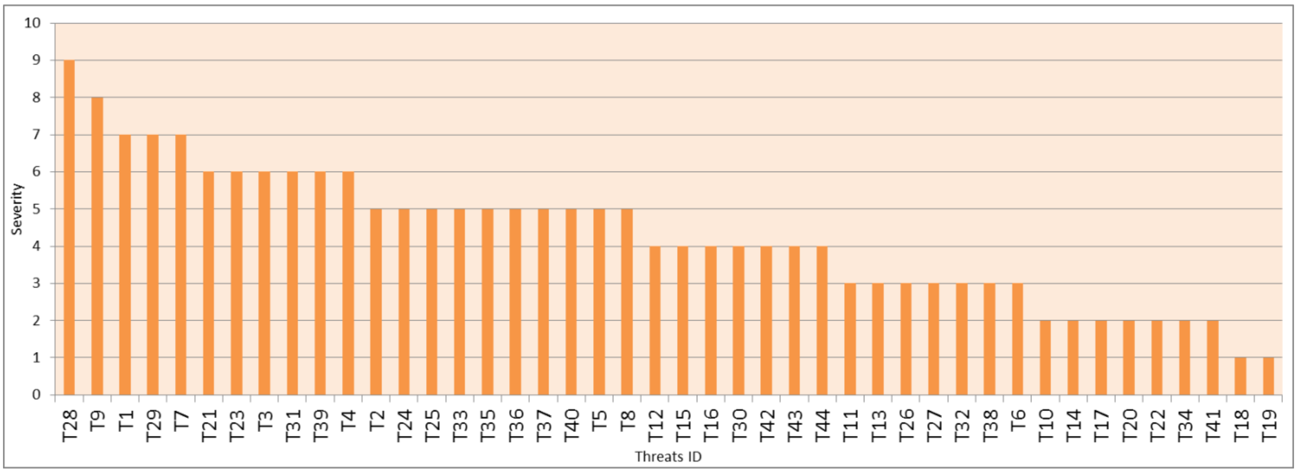

Figure 5-1. Severity of the security threats identified

The mapping between threats and requirements will allow to calculate the criticality of every requirement. The requirements criticality, rather than the relevance of its numerical value, allows to compare several requirements in terms of threats and their severity. Requirements with a high criticality would require more attention at implementation time. Additionally, with the mapping between threats and requirements and knowing the ANASTACIA components that are related to the identified security threats, we can give a higher priority to those components related to requirements with high criticality.

The following table demonstrates the calculation of the criticality for the requirement UFR-1. Following the methodology described in section 3, the impact of the requirement is normalized to a scale between 0 and 10, to match the scale of the threat severity. The average severity is calculated using the severity of all the threats that are related to this requirement. The total severity and the impact of the requirement is combined to estimate the criticality of the requirement. Annex I shows the mapping between requirements and threats, which allows to easily identify the threats that are related to every requirement.

Table 5-4. Example of evaluation of requirements criticality for UFR-1

	Impact level (normalized from In order to provide actionable information on the main security functionalities and constraints that must be covered by these guidelines, this section provides a summary and a classification of the security related requirements, after the extension and refinement process that has been initiated and carried out in WP1 (Task 1.2 “User Centred Requirement Analysis”) and that will produce	Threat severity (0-10) (grouping threats)	Criticality (0 – 10)

	deliverable D1.4 “Final User-Centred Requirement Analysis”. This section also works as validation of the complete methodology described in the previous section. To this end we have used the development of the ANASTACIA platform as context for this validation. For every security-related requirement, considering its role as for covering Integrity, Availability and Confidentiality constraints, scores (LOW, , HIGH) have been assigned and the Impact Level has been calculated as for the criteria indicated in Table 3-1. This approach allows to have the security-related requirements classified by level of importance with respect to security objectives. Table 4-1)				
UFR-1	8	Related threats[1]	Partial threat severity	Total severity	(8+4,43)/2 = 6,21
		T1-T17	5,47	4,43	
		T19-T46	2,78		
		T48-T56	5,04		

The criticality obtained for the rest of the requirements are shown in Annex I. The following graph compares the criticality of every requirement, which also allows to identify the requirements that need more attention when implementing the platform. As we can see, the requirements relevant for the core of the ANASTACIA platform (i.e., orchestration related requirements) are labelled with a high criticality. We can also identify three main groups of requirements. The very critical ones, with a criticality score over 5.5, the medium ones, with a criticality score between 2.5 and 5.5 and the low critical ones with a score under 2.5. It is worth noticing that requirements with a “low criticality” do not mean that they will not be considered appropriately during the implementation of the platform: all requirements are important and relevant. Every group is identified in Figure 5-2 with a different colour. This assessment technique provides with a quantitative measure related to security threats and based on the impact of incidents over a IoT/CPS infrastructure. This methodology is flexible and can be adapted to the specific characteristics of the infrastructure to protect just by tuning the impact of the requirements and the severity of the security threats.

[1] Related threats are grouped in the table for the sake of simplicity

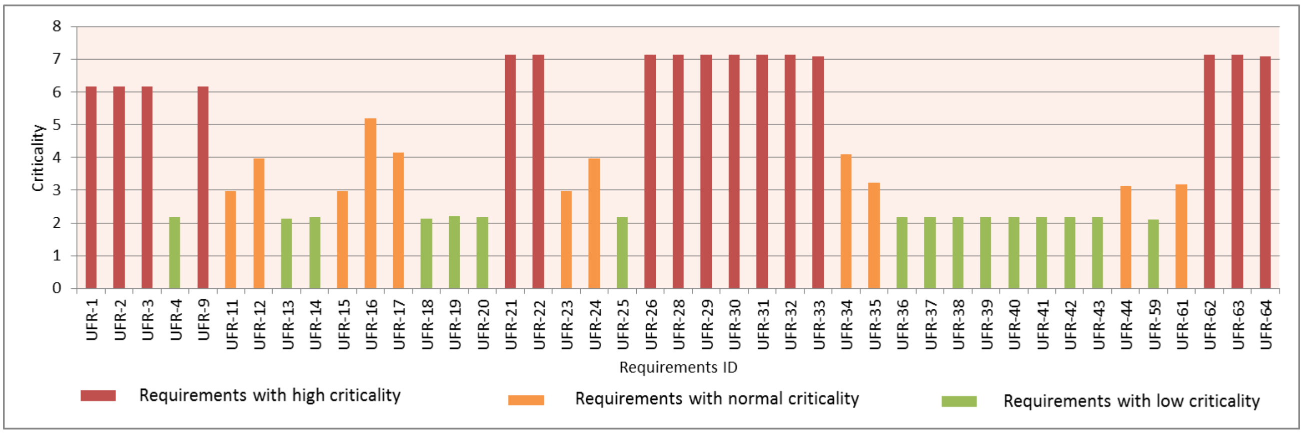

Figure 5-2. Requirements criticality per security threats

Next section will study the possible actions to prevent the identified threats and will reason about them, providing guidelines for the development of the ANASTACIA platform.

5.2 Guidelines against Security Threats in IoT/CPS

This section provides with actions to prevent the security threats elicited in the previous section. The preventive actions here presented aims at being implemented in IoT/CPS infrastructures. They have been defined based on the expert knowledge obtained mainly from members of the ANASTACIA consortium and based on the feedback received from the early developments implemented so far.

The following table summarizes the list of prevention actions mapped to the security threat that can mitigate. It is worth noticing that some preventions can be used to mitigate more than one threat. This is important because a prevention can be very relevant if it can prevent more than one threat, or in case these threats have a high criticality or if the related requirements are important (this is, have a high impact in the platform).

Table 5-5. Prevention against security threats

Thread id	Security Threats	Prevention recommendation
T1	Data flow from device is interrupted	P1 - Log access activities to detect the attack and prevent unauthorized access
T2	Code execution due to buffer overflow vulnerability	P2 - Perform scheduled vulnerability assessments based on latest updates on discovered vulnerabilities. P3 - Apply the latest updates on software and firmware for devices and computers deployed in the targeted infrastructure.
T3	Unauthorized access to the platform by malicious users	P4 - Provide distributed authorization mechanisms to control the access to devices & systems
T4	Denial of Service attacks (Spoofing, Flooding, Ping of Death, WinNuke, XDoS)	P1 - Log access activities to detect the attack and prevent unauthorized access P5 - Use input validation P6 - Use the principle of least privilege
T5	SQL Injection	P7 - Block network traffic from the attack source based on IP filtering
T6	0-day vulnerability to remotely target a device	P2 - Perform scheduled vulnerability assessments based on latest updates on discovered vulnerabilities P5 - Use input validation

T7	Malware spread via network to exploit sensitive sensors	P3 - Apply the latest updates on software and firmware for devices and computers deployed in the targeted infrastructure.
T8	Identity fraud	P8 - Testing activities will allow to minimize the insertion of malicious code in the system
T9	Unsolicited & infected e-mail	P9 - Use strong authentication algorithms, preferably based on PKI
T10	Malicious code/software activity	P1 - Log access activities to detect the attack and prevent unauthorized access P10 - Provide with antivirus/antimalware scans
T11	Abuse of information leakage	P10 - Provide with antivirus/antimalware scans P2 - Perform scheduled vulnerability assessments based on latest updates on discovered vulnerabilities
T12	SSL CA infiltration	P11 - Apply periodic updates of SSL CA P10 - Provide with antivirus/antimalware scans
T13	Manipulation of hardware & software	P12 - Provide authentication protocol for new hardware connected to the network with identification and sequence number. P13 - Schedule recurring assessments of authorizations P14 - Manage privileged sessions (such as control outbound traffic) P6 - Use the principle of least privilege
T14	Routing table manipulation	P15 - Provide secure routing mechanism based on SDN, software definition network in the control plane P16 - Use access control mechanisms P17 - Use anomaly detection techniques P14 - Manage privileged sessions (such as control outbound traffic)
T15	DNS spoofing	P18 - Use DNSSEC
T16	DNS poisoning	P18 - Use DNSSEC
T17	Falsification of configuration	P19 - Provide assessments for configuration values P13 - Schedule recurring assessments of configuration (à what type of assessment?)
T18	Autonomous System hijacking	P20 - Use TPM to provide mutual attestation
T19	Misuse of audit tools	P13 - Schedule recurring assessments of authorizations P14 - Manage privileged sessions (such as control outbound traffic)
T20	Falsification of records	P21 - Provide data analysis tools to validate records according to historical data P22 - Schedule recurring assessments and validation of records P23 - Log activities to detect modifications P24 - Use integrity mechanisms
T21	Unauthorised use of administration of devices & systems	P4 - Provide distributed authorization mechanisms to control the access of devices & systems P16 - Use access control mechanisms
T22	IMPI Protocol	P16 - Use access control mechanisms
T23	DNS Register Hijacking	P18 - Use DNSSEC P25 - Enabling HTTPS for all web apps and services
T24	Unauthorised installation and use of software	P16 - Use access control mechanisms (user profiles) P16 - Use access control mechanisms

T25	Unauthorised installation of software	P16 - Use access control mechanisms (user profiles) P16 - Use access control mechanisms
T26	Abuse of personal data compromising confidential information	P26 - Provide privacy mechanism based on encryption scheme of personal data P27 - Security awareness and continuous education of all the involved users
T27	Abuse of authorizations	P28 - Provide a maximum lifetime for using authorization keys P29 - Enforcing short lifetime of authorization keys
T28	Hoax	P27 - Security awareness and continuous education of all the involved users
T29	Badware (Virus, Worm, Trojan, Rootkit, Botnets, Spyware, Scareware)	P10 - Provide with antivirus/antimalware scans
T30	Remote activity (execution)	P16 - Use access control mechanisms
T31	Targeted attacks (including ATP)	P10 - Provide with antivirus/antimalware scans
T32	War driving	P30- Provide authenticated wireless access points P16 - Use access control mechanisms
T33	Interception compromising emissions	P31 - Provide secure communication channel for integrity and confidentiality P17 - Use anomaly detection techniques
T34	Targeted espionage attempts to obtain sensitive information	P32 - Obfuscate or encrypt data P17 - Use anomaly detection techniques
T35	Rogue hardware	P4 - Provide distributed authorization mechanisms to control the access to devices & systems P33 - Use TPM make sure that hardware is trusted
T36	Interfering radiations	P35 - Apply dynamic scheme to detect interferences and change radio channel P17 - Use anomaly detection techniques
T37	Replay of messages	P35 - Provide secure channel with sequence number for M2M communication P31 - Provide secure communication channel for integrity and confidentiality P36 - Use of timestamps
T38	Network reconnaissance and information gathering	P31 - Provide secure communication channel for integrity and confidentiality
T39	Man in the middle/ session hijacking	P35 - Provide secure channel with sequence number for M2M communication P25 - Enabling HTTPS for all web apps and services P37 - Enforcing short session timeouts
T40	Repudiation of actions	P4 - Provide distributed authorization mechanisms to control the access to devices & systems P38 - Use digital signatures on the performed actions
T41	Damage caused by a third party (External or internal)	P39 - Schedule recurring backup of the information in multiple places

T42	Loss of (integrity of) sensitive information	P32 - Obfuscate or encrypt data P39- Schedule recurring backup of the information in multiple places
T43	Loss of information in the cloud or destruction of devices, storage media and documents	P39 - Schedule recurring backup of the information in multiple places
T44	Information leakage	P39 - Schedule recurring backup of the information in multiple places P17 - Use anomaly detection techniques

We can do a bit of reasoning with the data obtained till now. For example, we can compare the severity of the security threats with the above mapping between preventions and threats. We can estimate the priority of every prevention with respect to the rest by aggregating the values of severity for every threat (Annex II shows all the severity scores). This result is represented in the following graph. As already mentioned for criticality and severity, the numerical values are worthless by themselves. The relevance of these numerical values lies on the comparison between the values obtained for the rest of the preventions. For example, we can see from the results obtained in this analysis that the most relevant prevention corresponds to the usage of access control mechanisms. On the other side, it is the usage of Trusted Platform Modules (TPM) as the prevention with the lowest priority. The effectiveness of TPMs are well proven in the state of practice but its application to the IoT/CPS context is quite limited and specific to very concrete elements of the infrastructure (i.e., just to certain IoT devices), reducing its criticality and the priority of the related prevention actions.

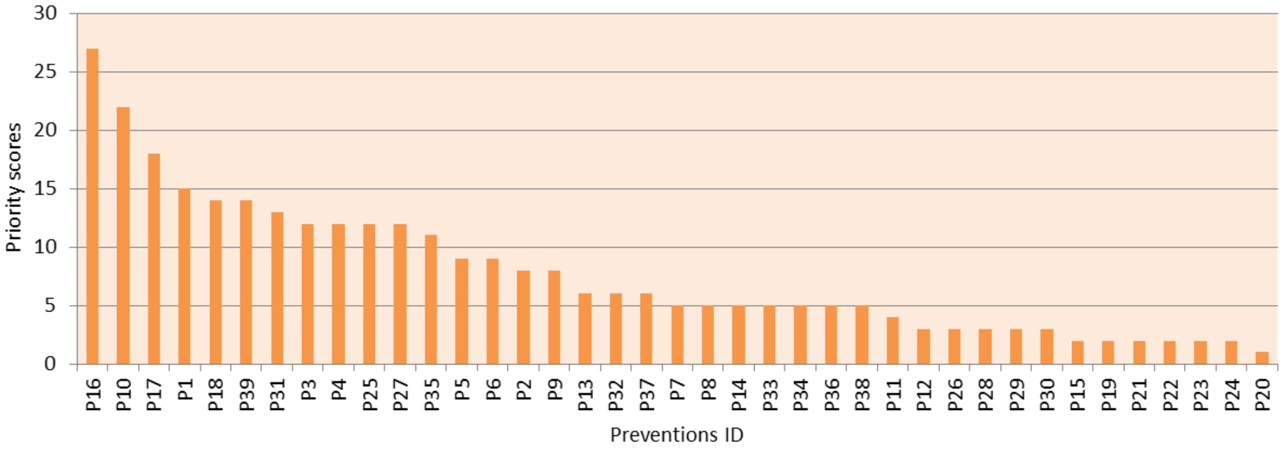

Figure 5-3. Preventions priority

We can go one step beyond this preventions priority, by checking how these preventions impact on the current development of the ANASTACIA platform. To this end, we have described the approaches that the ANASTACIA platform is following to prevent the threats that have been identified in this document. We have also mapped such implementation actions to the relevant components of the ANASTACIA architecture.

Using this analysis, we can trace back the development of the ANASTACIA components: starting from the prevention actions we can go back in the process and check what are the security requirements that are related to every prevention actions. Among other things, this helps to check what are the security threats prevented and establish priorities when developing the platform components.

The following table summarises the result of this mapping, describing how ANASTACIA is tackling with the implementation of every prevention action, and specifying what are the components of the ANASTACIA architecture that are related to them (refining the “Threat vs ANASTACIA components” done in Table 5-3). As we can see, there are some prevention actions apparently not implemented in ANASTACIA. This is not a problem as long as the prevention actions not covered remains with a low priority. However, it is convenient to check the development of some components in case of a prevention action that has a higher priority. This proves again the usefulness of the presented methodology, because it can also help to guarantee that good practices are followed when developing the software of the required components, paying attention to the important targets and focusing the efforts towards the development of a robust and secure infrastructure.

Table 5-6. ANASTACIA approach for the prevention of security threats

Prevention	ANASTACIA approach	ANASTACIA components
P1 - Log access activities to detect the attack and prevent unauthorized access	• Trusted communication among ANASTACIA components using encrypted data and PKI to manage trust among components • GUIs built over https, with valid certificates issued by a trusted CA. ANASTACIA deployed AAA controllers that logs the access activity to IoT devices • ANASTACIA has deployed with agents compiling the access activities log and monitors anomalous access attempts	All components
P2 - Perform scheduled vulnerability assessments based on latest updates on discovered vulnerabilities	• Distributed sensors provide monitoring agents with logs (i.e., NIDS sensors such as snort) • Dynamic deployment of virtual sensors through VNFs (i.e., virtual honeypots) providing with events • ANASTACIA counts with reaction capabilities to mitigate incidents detected at the IoT platform, including also the mitigation of known or discovered vulnerabilities by scheduling the patching or update of the firmware of IoT devices	Policy Editor Tool Incident detector Attack Signatures Security policies repository Verdicts and Decision Support System Security Enabler Repository
P3 - Apply the latest updates on software and firmware for devices and computers deployed in the targeted infrastructure.	• Mitigation actions are designed at the orchestrator in order to guarantee the compatibility of the actions with the IoT platform and interfaces. • ANASTACIA plans to execute periodic secure update procedures in order to keep the systems updated, without compromising the functionalities.	Policy Editor Tool Attack Signatures Orchestrator Security Enabler Repository
P4 - Provide distributed authorization mechanisms to control the access of devices & systems	• In AAA architecture, DCAPBac protocol provides a distributed scheme for the generation and verification of capability tokens which will be used to send the authorizations with the query from the user to subscribe to a topic or request an actuation in IoT devices.	IoT nodes
P5 - Use input validation	• The development of ANASTACIA components relies on secure software practices, which includes implementation of data validation	All components

	mechanisms to prevent code injection or buffer overflow vulnerabilities. Additionally, ANASTACIA includes detection capabilities for code injection such as SQL injection.	
P6 - Use the principle of least privilege	- ANASTACIA plans to design security policies and authorization procedures through the adoption of least privilege approaches.	User plane components Incident detector Verdict and Decision Support System IoT nodes
P7 - Block network traffic from the attack source based on IP filtering	- SDN controller provides IPv4 and IPv6 filtering of network traffic from the attack source. - ANASTACIA reaction component plans to deploy IP filtering policies/rules on network nodes in order to mitigate running threats, by dropping packets coming from malicious source IP addresses using SDN	Security orchestrator Attack signatures Security policies repository Verdict Reactions Security Enabler Repository
P8 - Testing activities will allow to minimize the insertion of malicious code in the system	- ANASTACIA includes sensors capable to detect code injection, such as SQL injection. The ANASTACIA agents and incident detector are capable of correlating events received from such sensors and alert about them	User plane components Databases of the infrastructure
P9 - Use strong authentication algorithms, preferably based on PKI	- Usage of trusted certificates when accessing dashboards and other management tools - In AAA architecture, ECC protocol is an elliptic curves solution for constrained IoT devices to enables authentication based on PKI. The approach provides security mechanisms such as encryption and digital signature.	User plane components IoT nodes
P10 - Provide with antivirus/antimalware scans	- ANASTACIA will attach different kinds of sensors and detection tools to the IoT platform. The ANASTACIA agents, in charge of collecting events from these sensors and detection tools, can be extended to receive events from antivirus/antimalware tools that might be installed in the platform to protect	All components
P11 - Apply periodic updates of SSL CA	- This prevention will not apply during the project development although remains as a good practice for all components requiring user authentication or the usage of a secure communication channel	Policy Editor Tool Dynamic Security and Privacy Seal User Interface Security sensors Data Filtering and pre-processing broker

P12 - Provide authentication protocol for new hardware connected to the network with identification and sequence number.	• This prevention will not apply during the project development although remains as a good practice for all connected devices	IoT nodes
P13 - Schedule recurring assessments of authorizations	• PANA is a network authentication protocol for constrained IoT device ANASTACIA plans to periodically review authorization procedures and authorized accounts for the protected components.	IoT nodes
P14 - Manage privileged sessions (such as control outbound traffic)	• In AAA architecture, DCAPBac protocol provides recurring assessments of authorizations. • ANASTACIA plans to guarantee quality of service for privileged hosts (e.g. sensitive services requiring high availability), by working on network nodes configuration.	IoT nodes IoT network
P15 - Provide secure routing mechanism based on SDN, software definition network in the control plane	• ANASTACIA provide with SDN/NFC orchestration based on security policy which allows to deploy security enablers to react to incidents and enforce the fulfilment of the security policy	Security orchestrator Security Enabler Repository IoT network
P16 - Use access control mechanisms	• In AAA architecture, DCAPBac protocol provides access control mechanisms to resources of IoT devices and IoT-Broker • ANASTACIA plans to deploy strong authentication procedures/protocols to access sensitive nodes.	All components
P17 - Use anomaly detection techniques	• ANASTACIA deployed an Incident Detector that correlates events monitored and generate alerts for the anomalies detected	IoT network IoT nodes Virtualized Infrastructure Domain Control and Management Domain Monitoring components
P18 - Use DNSSEC	• This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT network
P19 - Provide	• Configuration schemes for ANASTACIA	All components

assessments for configuration values	components will be documented and tested before committing them	
P20 - Use TPM to provide mutual attestation	• This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT network
P21 - Provide data analysis tools to validate records according to historical data	• ANASTACIA provides with anomalous behaviour analysis capabilities by incorporating deep learning techniques that feed from current and past data to infer potential anomalies on IoT devices.	Data Analysis
P22 - Schedule recurring assessments and validation of records	• UTRC Data analysis can provide assessments and validation of temperature values in real time.	Data Analysis
P23 - Log activities to detect modifications	• ANASTACIA has deployed agents compiling the access activities logs	Incident Detector Data filtering and pre-processing broker
P24 - Use integrity mechanisms	• DTLS protocol provides the security services such as integrity, authentication and confidentiality in P2M communication. • ANASTACIA uses TCP based communications to guarantee network level integrity of the exchanged data.	All components IoT network
P25 - Enabling HTTPS for all web apps and services	• ANASTACIA uses HTTPS connections for all the components deployed at the user plane: seal manager GUI, incident dashboard and policy editor tool	User plane components IoT network
P26 - Provide privacy mechanism based on encryption scheme of personal data	• ANASTACIA provides with a Data Management plan that regulates the use of personal data	IoT nodes User plane components All databases of the platform
P27 - Security awareness and continuous education of all the involved users	• ANASTACIA includes security guidelines and privacy risk modelling and contingency assessment that provides with a useful source of information for system admin training and continuous education.	Incident Detector Verdict and Decision Support System
P28 - Provide a maximum lifetime for using authorization	• In AAA architecture, DCAPBac protocol provides a maximum lifetime for using capability tokens that are authorization keys.	IoT nodes User plane components

keys	• Periodically schedule change of authorization keys. This is a good practice that is not a priority during the project development although it remains very relevant for a real environment.	
P29 - Enforcing short lifetime of authorization keys	• In AAA architecture, DCAPBac protocol provides short time of authorization keys. • Periodically schedule change of authorization keys. This is a good practice that is not a priority during the project development although it remains very relevant for a real environment.	User plane components IoT nodes
P30 - Provide authenticated wireless access points	• IoT devices with wireless access will be protected with secure authentication, adding also AAA logging to detect unauthorized access attempts	IoT nodes
P31 - Provide secure communication channel for integrity and confidentiality	• DTLS protocol provides the security services such as integrity, authentication and confidentiality in P2M communication. • ANASTACIA components will communicate each other by using secure connections	IoT nodes All components
P32 - Obfuscate or encrypt data	• In AAA architecture, ECC protocol provides security mechanisms such as encryption and digital signature. • ANASTACIA will encrypt sensitive communications and stored data through the adoption of well-known encryption protocols able to guarantee confidentiality.	IoT nodes All components
P33 - Use TPM make sure that hardware is trusted	• This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT nodes
P34 - Apply dynamic scheme to detect interferences and change radio channel	• This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT nodes
P35 - Provide secure channel with sequence number for M2M communication	• DTLS protocol provides security services such as integrity, authentication and confidentiality in P2M communication.	All components
P36 - Use of timestamps	• DTLS protocol provides the security services such as integrity, authentication and confidentiality in P2M communication.	All components
P37 - Enforcing short	• This prevention will not apply during the project	User plane components

session timeouts	development although remains as a good practice to be considered in a real production environment.	
P38 - Use digital signatures on the performed actions	• In AAA architecture, ECC protocol provides security mechanisms such as encryption and digital signature.	User plane components
P39 - Schedule recurring backup of the information in multiple places	• ANASTACIA plans to execute periodic backups, prior to updates.	All databases of the platform

For the sake of completeness, we have carried out a mapping between the defined preventions and the security requirements. In general, most of the preventions are, to some extent, covering most of the security requirements while some of them are only affecting a smaller subset of requirements. It is worth noticing that some preventions covering a small set of requirements (i.e., P21 to P24) are labelled with a low priority in Figure 5-3.

		Preventions																																					
Req ID (more to less critical)		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P33	P34	P35	P36	P37	P38	P39
	UFR-62	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-63	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-21	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-26	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-28	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-29	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-30	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-31	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-32	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-22	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-33	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-64	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	UFR-1	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨
	UFR-2	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨
	UFR-3	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨
	UFR-9	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨
	UFR-16	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨
	UFR-17	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨
	UFR-34	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-24	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-12	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-35	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-61	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	▨
	UFR-44	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	▨
	UFR-11	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-15	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-23	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	▨	▨	▨	▨	▨	□	▨	□	▨
	UFR-19	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-4	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-14	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-20	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-25	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-36	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-37	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-38	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-39	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-40	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-41	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-42	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-43	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-13	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-18	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨
	UFR-59	▨	▨	▨	▨	▨	▨	□	▨	□	▨	▨	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	▨	▨	▨	▨	▨	□	▨	▨	▨	□	▨	□	▨	□	▨

▨ Prevention relevant for the requirement

□ Prevention not relevant for the requirement

Figure 5-4- Mapping between security requirements and preventions of security threats

6 CONCLUSIONS

This document details a process for creating guidelines for the development of a secure IoT/CPS infrastructure. This process is supported by a comprehensive methodology based on the evaluation of requirements and threats. On the one side, the security requirements are evaluated in terms of three factors: integrity, availability and confidentiality. This is used to evaluate the impact of every requirement within the global security status of the platform. On the other side security threats are evaluated by using the DREAd methodology specified by OWASP to calculate the severity of every threat. In the following step threats and requirements are linked while the impact of the requirements and the severity of the security threats are combined to calculate the criticality of every requirement. In parallel to this analysis the security threats are mapped to actions that allow to prevent them. These preventions can be mapped to the threats severity in order to determine the priority of some preventions over others. Tracing back the analysis we can identify what are the preventions related to every security requirement. We can use this analysis to check (1) that all the requirements are mapped to at least one prevention action, and (2) that these actions allow to prevent some of the specified security threats.

This methodology has been validated within the development activities of the ANASTACIA framework by using the requirements produced in WP1, extracting the security requirements that are relevant for this methodology, and a list of threats that extend the ones produced in T2.2 by incorporating an additional level of detail.

The work presented here will be use to improve the current developments of the ANASTACIA components, being constantly updated as long as the development progresses.

7 REFERENCES

[1] ENISA, Baseline Security Recommendations for IoT:
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[2] ENISA, Security Challenges and best practices in the IoT Environment:
https://www.enisa.europa.eu/publications/ed-speeches/security-challenges-and-best-practices-in-the-iot-environment

[3] Vaccari, I., Cambiaso, E., & Aiello, M. (2017). Remotely Exploiting AT Command Attacks on ZigBee Networks. *Security and Communication Networks*, *2017*.

[4] ENISA, Security and Resilience of Smart Home Environments:
https://www.enisa.europa.eu/publications/security-resilience-good-practices

[5] ENISA, Cyber Security and Resilience of Smart Cars:
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[6] ENISA, Cyber Security and Resilience for Smart Hospitals:
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

[7] ENISA, Architecture Model of the Transport Sector in Smart Cities:
https://www.enisa.europa.eu/publications/smart-cities-architecture-model

[8] Cloud Security Alliance CSA, Security Guidance for Early Adopters of the Internet of Things (IoT):
https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

[9] GSMA, IoT Security Guidelines for Service Ecosystems:
http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.12-v1.1.pdf

[10] NIST, Guide to Security for Full Virtualization Technologies:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

[11] ONAP, VNF Guidelines for Network Cloud and OpenECOMP:
https://wiki.onap.org/download/attachments/1015849/VNF%20Guidelines%20for%20Network%20Cloud%20and%20OpenECOMP.pdf?api=v2

[12] ETSI, Network Functions Virtualisation (NFV), Virtual Network Functions Architecture:
http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf

[13] Joao Goncalves, David Palma, Luis Cordeiro, Sachin Sharma, Didier Colle, Adam Carter and Paulo Simoes. "Software-Defined Networking: Guidelines for Experimentation and Validation in Large-Scale Real World Scenarios":https://biblio.ugent.be/publication/5736787/file/5736792.pdf

[14] ENISA, Threat Landscape and Good Practice Guide for Software Defined Networks/5G. https://www.enisa.europa.eu/publications/sdn-threat-landscape

[15] The Open Web Application Security Project OWASP, Secure Coding Practices Quick Reference Guide: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[16] Security Development Lifecycle (SDL) – Microsoft
https://www.microsoft.com/en-us/SDL/about/default.aspx

[17] IoT Security Compliance Foundation – IoT Security Foundation
https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf

[18] Threat Risk Modelling by OWASP
https://www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

[19] Asghar, Sohail. "A survey on multi-criteria decision making approaches." *Emerging Technologies, 2009. ICET 2009. International Conference on*. IEEE, 2009.

[20] ENISA Threat taxonomy report https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

8 ANNEX I. DETAILED EVALUATION OF REQUIREMENTS CRITICALITY

		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28	T29	T30	T31	T32	T33	T34	T35	T36	T37	T38	T39	T40	T41	T42	T43	T44	T45	T46	T47	T48	T49	T50	T51	T52	T53	T54	T55	T56		
Req ID	Impact (N)	7	5	6	6	5	3	7	5	8	6	6	6	6	6	6	2	3	4	3	2	4	4	2	1	1	2	6	2	6	5	5	3	3	3	9	7	4	6	3	5	3	2	5	1	5	7	5	6	6	5	3	7	5	8	6	6	Threat Severity	Criticality
UFR-1	8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	4,70	6,35
UFR-2	8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	4,70	6,35
UFR-3	8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	4,70	6,35
UFR-4	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-9	8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	4,70	6,35
UFR-11	2	x	x		x	x	x				x	x	x	x	x	x				x	x	x	x	x	x	x				x														x		x								x	x	x		4,75	3,38
UFR-12	4	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x		x	x	x	x	x	x						x	x	x	x	x	x								x	x	x	x	4,35	4,18
UFR-13	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x	x	x	x	x	x	x	x						x			x					x					x	x	x	x	4,81	2,41
UFR-14	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-15	2	x	x		x	x	x				x	x	x	x	x	x				x	x	x	x	x	x	x				x														x		x								x	x	x		4,75	3,38
UFR-16	6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x		x	x		x				x	x	x	x	x	x			x	x	x	x		x	x	x	x	x	x	x	x		4,85	5,42
UFR-17	4	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x		x	x		x				x	x	x	x	x	x			x	x	x	x		x	x	x	x		x	x	x		4,73	4,36
UFR-18	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x		x	x					x					x	x	x	x	4,81	2,41
UFR-19	0	x	x		x	x		x			x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,97	2,48
UFR-20	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-21	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,70	7,35
UFR-22	10	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,69	7,35
UFR-23	2	x	x		x	x	x				x	x	x	x	x	x				x	x	x	x	x	x	x				x														x		x								x	x	x		4,75	3,38
UFR-24	4	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x						x	x	x	x	x	x								x	x	x	x	4,34	4,17
UFR-25	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-26	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,70	7,35
UFR-28	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,65	7,33
UFR-29	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,65	7,33
UFR-30	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,65	7,33
UFR-31	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,65	7,33
UFR-32	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,65	7,33
UFR-33	10	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,59	7,30
UFR-34	4	x	x	x	x	x	x		x		x	x	x	x	x	x	x	x	x	x						x	x	x		x	x	x	x	x	x						x	x	x	x		x										x	x	4,58	4,29
UFR-35	2	x	x		x	x	x				x	x	x	x	x	x				x						x				x														x										x	x	x		5,33	3,67
UFR-36	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-37	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-38	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-39	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-40	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-41	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-42	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-43	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x			x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,90	2,45
UFR-44	2	x	x	x		x	x	x	x								x	x		x	x	x	x	x	x	x	x		x	x		x				x	x	x	x	x	x			x	x	x	x		x	x	x	x		x	x	x		4,49	3,24
UFR-59	0	x	x		x	x			x		x	x	x	x	x	x		x	x		x		x	x	x	x		x		x	x	x	x	x	x						x			x					x					x	x	x	x	4,78	2,39
UFR-61	2	x	x	x		x	x	x	x									x		x	x	x	x	x	x	x	x		x	x		x				x	x	x	x	x	x			x	x	x	x		x	x	x	x		x	x	x		4,56	3,28
UFR-62	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,67	7,33
UFR-63	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,67	7,33
UFR-64	10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	4,67	7,33

Figure 8-1. Complete evaluation of threats and requirements

9 ANNEX II. DETAILED MAPPING BETWEEN THREATS AND PREVENTIONS

	Threats																																												
	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28	T29	T30	T31	T32	T33	T34	T35	T36	T37	T38	T39	T40	T41	T42	T43	T44	
	7	5	6	6	5	3	7	5	8	2	3	4	3	2	4	4	2	1	1	2	6	2	6	5	5	3	3	9	7	4	6	3	5	2	5	5	5	3	6	5	2	4	4	4	<- Threat severity
Preventions																																													Prevention priority
P1	x			x						x																																			15
P2		x									x																																		8
P3		x					x																																						12
P4			x																		x														x					x					12
P5				x		x																																							9
P6				x									x																																9
P7					x																																								5
P8								x																																					5
P9									x																																				8
P10										x	x	x																	x			x														22
P11												x																																	4
P12													x																																3
P13													x				x		x																										6
P14													x	x																															5
P15														x																															2
P16														x							x	x		x	x					x		x													27
P17														x																			x	x		x								x	18
P18															x	x							x																						14
P19																	x																												2
P20																		x																											1
P21																				x																									2
P22																				x																									2
P23																				x																									2
P24																				x																									2
P25																							x																x						12
P26																										x																			3
P27																										x		x																	12
P28																											x																		3
P29																											x																		3
P30																																x													3
P31																																	x				x	x							13
P32																																		x								x			6
P33																																			x										5
P34																																				x									5
P35																																					x		x						11
P36																																					x								5
P37																																							x						6
P38																																								x					5
P39																																									x	x	x	x	14

Figure 9-1. Complete evaluation between threats and preventions