



Multimodal Transport System: System Modelling, Risk Analysis and Management, GDPR Compliance

Work Package	WP2 Use-cases and Vulnerabilities modelling
Task	T2.2 Cross-domain threat analysis
Authors	Christos Lyvas, Kostas Maliatsos, Costas Lambrinoudakis, Athanasios Kanatas, Andreas Menegatos, Thrasyvoulos Giannakopoulos, Christos Kalloniatis.
Dissemination Level	PU
Status	Final
Due Date	30/09/2021(initial) 31/05/2022 (review changes)
Document Date	30/09/2021(initial) 31/05/2022 (review changes)
Version Number	1.0

Quality Control

	Name	Organisation	Date
Editor	Konstantinos Maliatsos	UPRC	30/09/2021 31/05/2022 (review changes)
Peer review 1	Liivar Luts / Andrew James Roberts	TALLINN / TALTECH	29/09/2021
Peer review 2	Fabio Podda	AMT	28/09/2021
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	30/09/2021 30/05/2022 (review changes)
Authorised by	Vasileios Sourlas	ICCS	30/09/2021

(Quality Manager)			30/05/2022 (review changes)
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	30/09/2021 31/05/2022 (review changes)

Contributors

Name	Organisation	Date
Konstantinos Maliatsos	UPRC	25/08/2021
Costas Lambrinoudakis	UPRC	25/09/2021
Athanasios Kanatas	UPRC	25/09/2021
Christos Kalloniatis	UPRC	27/08/2021
Andreas Menegatos	UPRC	01/09/2021
Thrasyvoulos Giannakopoulos	UPRC	05/09/2021
Christos Lyvas	UPRC	29/08/2021
Costas Lambrinoudakis	UPRC	14/05/2022
Christos Lyvas	UPRC	23/05/2022
Konstantinos Maliatsos	UPRC	31/05/2022

Document Revision History

Version	Date	Modification	Partner
0.1	25/08/2021	Table of Contents	UPRC
0.2	27/08/2021	Conceptual Model	UPRC
0.3	29/08/2021	Threats - Assets	UPRC
0.4	31/08/2021	Vulnerabilities	UPRC
0.5	31/08/2021	Threats Vulnerabilities	UPRC
0.6	01/09/2021	CVEs	UPRC
0.7	05/09/2021	CVEs Examples	UPRC
0.8	12/09/2021	Risk Analysis Description	UPRC
0.9	20/09/2021	GDPR	UPRC
1.0	30/09/2021	Integration of review comments	UPRC
1.05	23/05/2022	Suggestions and comments from project interim review	UPRC, ICCS
1.1	31/05/2022	Integration of minor	UPRC

		corrections due to project officer and reviewer comments	
--	--	----------------------------------------------------------	--

Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The CitySCAPE Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

1. Introduction.....	8
1.1 Project Introduction.....	8
1.2 Deliverable Purpose	8
1.3 Deliverable Purpose	9
1.4 Inputs from other projects	9
1.5 Outline of the Document.....	10
2. Conceptual Model.....	11
3. System Architecture and Assets.....	28
3.1 Basic Assets.....	28
3.2 System Assets.....	30
3.3 Schematic representation of composite assets	35
4. Threats.....	41
4.1 Association between Threats and Assets.....	41
5. Vulnerabilities.....	107
5.1 List of generic vulnerabilities	107
5.2 Association between Threats and Vulnerabilities.	110
6. Modeling cascading risks and threats with fault-trees.....	116
6.1 Definition of terms in the modified fault trees for threat analysis..	117
6.2 Design principles for the mFFTA.....	121
7. Dynamic Risk Analysis Paradigm.....	125
7.1 Rationale.....	125
7.2 NVD, CVE, CWE, CAPEC and ENISA Threat Relations.....	125
7.3 Dynamic Operation examples	128
8. GDPR.....	130
8.1 Background and purpose.....	130
8.2 Definitions.....	131
8.3 The GDPR processing principles	135
8.4 The GDPR rights afforded to individuals (data subjects)	139
8.5 Security of personal data.....	142
8.6 Data protection impact assessment.....	143
8.7 Personal Data Protection in the CitySCAPE project (Design Phase)	144
8.8 Personal Data Protection in the CitySCAPE project (Development Phase).....	149
8.9 Privacy and data Protection methodology.....	155

9. Conclusions.....	167
10. References.....	167

List of Figures

Figure 1: The conceptual model in the analysis chain (J. Sokolowski, 2010) ...	11
Figure 2: CITYSCAPE Conceptual Model.....	14
Figure 3: Analysis of Basic Assets Types	16
Figure 4: Tallinn Architecture High Level Overview	31
Figure 5: Genoa Architecture High Level Overview.....	31
Figure 6: Validator Mobile Device Composite Asset of Genoa Use Case.....	37
Figure 7: Ticketing System Server Composite Asset of Genoa Use Case	38
Figure 8: Communication Platform as a Service (CPaaS) Composite Asset of Tallinn Use Case.....	39
Figure 9: Trolley Composite Asset of Tallinn Use Case.....	40
Figure 10: Example of the use of basic events in the mFTTA.....	119
Figure 11: Example of the use of conditional events in the mFTTA	120
Figure 12: Example on the use of transfer blocks in mFTTAs.....	120
Figure 13: A minimalistic example of an mFTTA for a web service (basic asset of a composite asset e.g., Ticketing System).....	124
Figure 14: Relation between NVD, CVE, CWE, CAPEC and Threats	125
Figure 15: Known affected software configurations for CVE-2021-0430 (NIST, 2021).....	128
Figure 16: Known affected software configurations for CVE-2017-3167 (NIST, 2021).....	129
Figure 17: Known affected software configurations for CVE-2020-16119 (NIST, 2021).....	130
Figure 18: GDPR Compliant Personal Data Management Methodology.....	156
Figure 19. Output of Stage 1	157
Figure 20. Output of Stage 2	159
Figure 21. Output of Stage 3.....	161
Figure 22. Conceptual Framework of Impact Assessment.....	164
Figure 23. Risks and Feared events.....	165
Figure 24. Factors used to estimate risks.....	165
Figure 25. Output of Stage 4	166

List of Tables

Table 1: Tasks related to the deliverable	9
Table 2 Use Case: infomobility GENOA	20
Table 3 Use Case: E-ticketing GENOA.....	23
Table 4: Use Case: Last Mile Extension TALLINN	27
Table 5: Basic Assets List	30
Table 6: Identified relationships between basic assets.....	30
Table 7 Tallinn Composite Asset List.....	32
Table 8 Genoa Composite Asset List.....	32
Table 9: Basic Assets of Tallinn Architecture	34
Table 10: Basic Assets of Genoa Architecture.....	35
Table 11: CitySCAPE Identified Threats	42

Table 12: Threats of Genoa Use Case's Composite Assets.....	70
Table 13: Threats of Tallinn Use Case's Composite Assets	106
Table 14: List of High-Level Vulnerabilities.....	110
Table 15: Association Among High-Level Vulnerabilities and Identified Threats of CitySCAPE Use Cases.....	116
Table 16: Logical gates used in mFTTAs.....	118
Table 17: Information per case	154

List of Abbreviations and Acronyms

Abbreviation	Meaning
2G	Second Generation Cellular Network
3G	Third Generation Cellular Network
5G	Fifth Generation Network
AV	Autonomous Vehicle
AVM	Automated Vehicle Monitoring
CPaaS	Communications Platform-as-a-Service
ENISA	European Union Agency for Cybersecurity
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
HW	Hardware
ICCS	Institute of Communication and Computer Systems
ITS	Intelligent Transport Systems
LTE	Long Term Evolution
MaaS	Mobility-As-A-Service
mFTTA	modified Fault Trees for Threat Analysis
NFC	Near-Field Communication
OS	Operating System
RSU	Road-Side Unit
SMS	Short Message Service
SW	Software
TST	Threat Sequence and Transformation graph

Executive Summary

This deliverable presents the results of the work carried out during Task 2.2 entitled “Cross-domain threat analysis”. The main objectives of the task were to: a) present a detailed investigation of the current threat landscape

against the major Operators of Essential Services (OES) and the Digital Service Providers (DSP), b) model the multi-modal transportation ecosystem under the CitySCAPE context and propose a risk analysis methodology for it, and c) study and investigate the different categories of personal data that will be processed by the multimodal under the requirements.

While the results for the threat landscape, were provided in “D2.2 Analysis NIS directive Cross domain threats and proof of concepts”, in this deliverable:

- A new risk analysis approach is presented with the proposal of a new conceptual model capable to robustly and hierarchically support risk modeling of the multimodal transport ecosystem.
- In conjunction with the work delivered by D2.4 “Cascading Risks in the Multimodal Transportation Platforms”, the multimodal ecosystem architecture for the CitySCAPE use cases is defined with identification of assets and their interconnections. CitySCAPE follows an asset-based risk analysis approach – where all types of assets are considered (Hardware, Software, Connectivity, Data, Users, etc.)
- As a next step, and following the conceptual model, the threats that can harm the system are identified and associated with the system assets. Then, the vulnerabilities related to the multimodal ecosystem are presented and associated with the threats, in order to form a triplet (asset, threat, vulnerability) that will be used for risk evaluation.
- Instead of performing static risk analysis on use-case specific environments, it was decided to propose a dynamic risk analysis system based on the conceptual model that can be updated in real-time by external sources. The specific approach will be developed as part of the CitySCAPE framework and evaluated (WP5).
- The cascading methodology is also integrated into the risk model with the use of fault-trees.
- Finally, GDPR requirements and compliance was investigated defining the axes for the application development with respect to the rights of data owners (right to object storage/processing, right to be forgotten, right to restrict processing and more).

1. INTRODUCTION

1.1 Project Introduction

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation.

CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which consists of 15 partners from 6 European countries, united in their vision to cover the cybersecurity needs of the multimodal transportation.

More specifically, the CitySCAPE software toolkit will:

- ✓ Detect suspicious traffic-data values and identify persistent threats
- ✓ Evaluate an attack's impact in both technical and financial terms
- ✓ Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks
- ✓ Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

The project duration extends from September 2020 to August 2023.

1.2 Deliverable Purpose

The purpose of the document is to propose a complete risk analysis model suitable for the heterogeneous and dynamically changing multimodal ecosystem.

A basic axis of the CitySCAPE approach was not to execute a non-reusable static risk analysis based on the use cases, but to utilize the use cases to define a risk analysis concept that can support dynamic reconfiguration taking also into account privacy requirements in the GDPR context and cascading threats.

The specified dynamic risk analysis framework will be implemented as a software engine in the context of WP5 and the Risk Analysis and Impact Assessment Tool in order to maximize its impact and reusability.

The document is provided in M13 of the project marking the completion of Tasks 2.2 and 2.3 and summarizing their achievements. Furthermore, the document aims to facilitate the efforts in security assurance investigations (Task 2.5), the system architecture and user and system requirements elicitation of WP3 (User/system requirements & architecture).

1.3 Deliverable Purpose

Besides the internal project reviewers, the project reviewers and the project partners, this deliverable is addressed to any interested reader (i.e., public dissemination level). This deliverable targeted audience is intended for reading by all transport and cybersecurity experts in the field, especially those in the public sector.

However, the approach (conceptual model), the hierarchical asset modelling, the threat and vulnerability elicitation can be used for the implementation of similar frameworks addressing cyber-security aspects in essential services and critical infrastructure defined under the NIS directive. The deliverables outcomes have direct relevance to the following CitySCAPE tasks:

Table 1: Tasks related to the deliverable

Task	Relationship
T2.4 Security assurance methodology and tools	The deliverable provides lists of assets, threats, vulnerabilities, risk evaluation aspects and methods to analyse interdependencies that can be utilized in the application of security assurance tasks of T2.4.
T3.2 System requirements elicitation	The deliverable provides the conceptual model that can be applied for the design of the CitySCAPE framework as a whole, as well as architectural views of the systems described in the use cases. This information will assist the efforts for system requirement elicitation and system architecture definition.
T3.3 Secure multi-modal transport architectures	
T5.5 Risk analysis and impact assessment engine	The deliverable provides description of the framework that will be implemented as Risk Analysis and Impact Assessment Toolkit in T5.5.
T5.6 Financial impact assessment engine	The followed approach will also influence the developments in T5.6 and the financial impact and cost/benefit assessment engine (FIMCA) and the way it interacts with RITA.

1.4 Inputs from other projects

The development of the new risk analysis and modelling methodology considered the outputs from two EU-funded projects:

- H2020 SAFERtec: The steps of the SAFERtec risk analysis methodology were used as reference and basis for the new risk analysis approach developed in CitySCAPE.
- CEF Telecom project, 2CeVau: Information concerning the threat and vulnerability analysis was investigated.

1.5 Outline of the Document

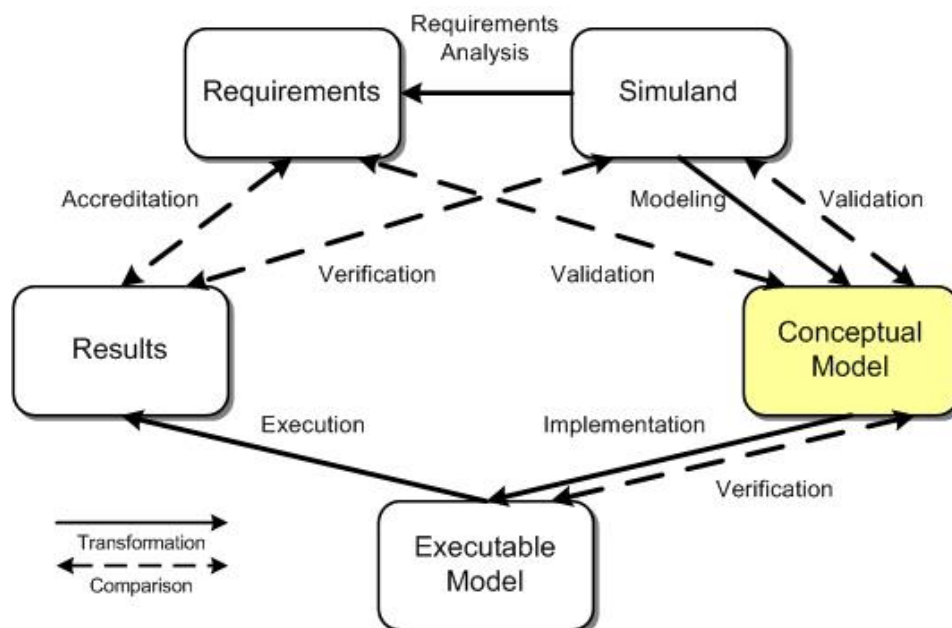
The document is structured as follows:

- Chapter 2:
 - The conceptual model is proposed together with specific instantiation examples based on the CitySCAPE use cases.
- Chapter 3:
 - The system architecture based on the defined use-cases and definition of basic assets is presented, as well as a methodology for the hierarchical definition of composite assets.
- Chapter 4:
 - The list of threats and their association with the system assets is provided.
- Chapter 5:
 - The list of vulnerabilities and their association with the system threats is provided.
- Chapter 6:
 - The Dynamic Risk Analysis Paradigm is presented and how it can be implemented to provide updated risk analysis results in real-time.
- Chapter 7:
 - An approach to model the cascading threat methodology in the risk analysis framework using modified fault-trees is described.
- Chapter 8:
 - Analysis of the Personal Data Protection approach in the CitySCAPE project is provided.
- Chapter 9:
 - A summary of conclusions is made.

2. CONCEPTUAL MODEL

One of the most important steps for achieving the goals of the project is to identify the key terms and the connection between them. The tool for achieving this is the conceptual model which serves the following purposes:

- Describe the basic concepts of the proposed system
- Constitutes a common language that stakeholders and analysts will consider
- Enhances the understanding of the system
- Provides a point of reference for designers and developers
- It is a critical part of the system documentation



J. Sokolowski, C. Banks, *Modeling and Simulation Fundamentals: Theoretical Underpinnings and Practical Domains*, Wiley, 2010, pp 333

Figure 1: The conceptual model in the analysis chain (J. Sokolowski, 2010)

In the above figure the role of conceptual model in the system development stages is presented. As it can be seen, through the conceptual models, engineers can express the language of the system to be which directly can assist in the creation of the executable models for simulation purposes prior to the actual system implementation. In addition, the whole developing team can reason about the identified functional and non-functional requirements of the proposed system as well to validate them on the latter stages of the system development. In complex interconnected systems like the CITYSCAPE ecosystem, we consider the conceptual model to be a valuable tool prior to system design and implementation since the design of the conceptual model provided to the whole team the ability to:

- Establish the core entities of CITYSCAPE
- Define the actual scope of the project

- Create a base model that will be the basis for all future models
- Provide a common understanding among all partners about the key concepts and their relationship in the CITYSCAPE domain

Based on CITYSCAPE goals and objectives the key entities and their relationships are presented in the conceptual model in figure 1. More specifically, the first entity is the **Transport Ecosystem** which interacts with a number of **users** as well as various **entities** that actually define this ecosystem. **Users** can be either trusted or untrusted, while the trusted users are separated in two categories, the general ones and the privileged ones. Users are also interacting with the Entities as the latter constitute the way for communicating and participating in the transport ecosystem. Entities interact with the Transport Ecosystem, interact with other entities but they also interact with assets. **Assets** are independent, operable elements of **basic assets** that can collaborate together in order to build entities in the Transport Ecosystem. Assets are the basic concept regarding the functionality of the ecosystem and their behaviour is mainly described based on the basic assets that they are composed of. **Basic assets** are the minimum functional asset that belong to the ecosystem. Basic assets can live alone or be combined together in order to perform a larger asset and/or entity. The categories of the basic assets are:

- Hardware Assets
 - Sensors-Actuators
 - Power Supply
 - Computational Device
 - HW Interface
 - IO Devices
 - Storage
- Data
 - Backup Data
 - Configuration Data
 - Operation-Application Data
 - System Data
 - Test Data
 - Audit Data
- System Software
 - Embedded System Firmware
 - Native API
 - Hypervisor
 - Operating System
 - Containers-VMs
- Application Software
 - Web-based Services

- Application Software
 - DB Management Systems
- Users
 - System Users
 - End Users
 - Contractors-Subcontractors
- Communication Network
 - Communication Protocol
 - Network Interfaces
 - Network Controller
 - Network Stack

The description of every basic asset must contain the following information (beside the aforementioned type of asset):

- Name of asset
- Vendor of asset
- Product Name
- Version

The following figure, figure 2 presents the aforementioned information in an entity-relationship diagram.

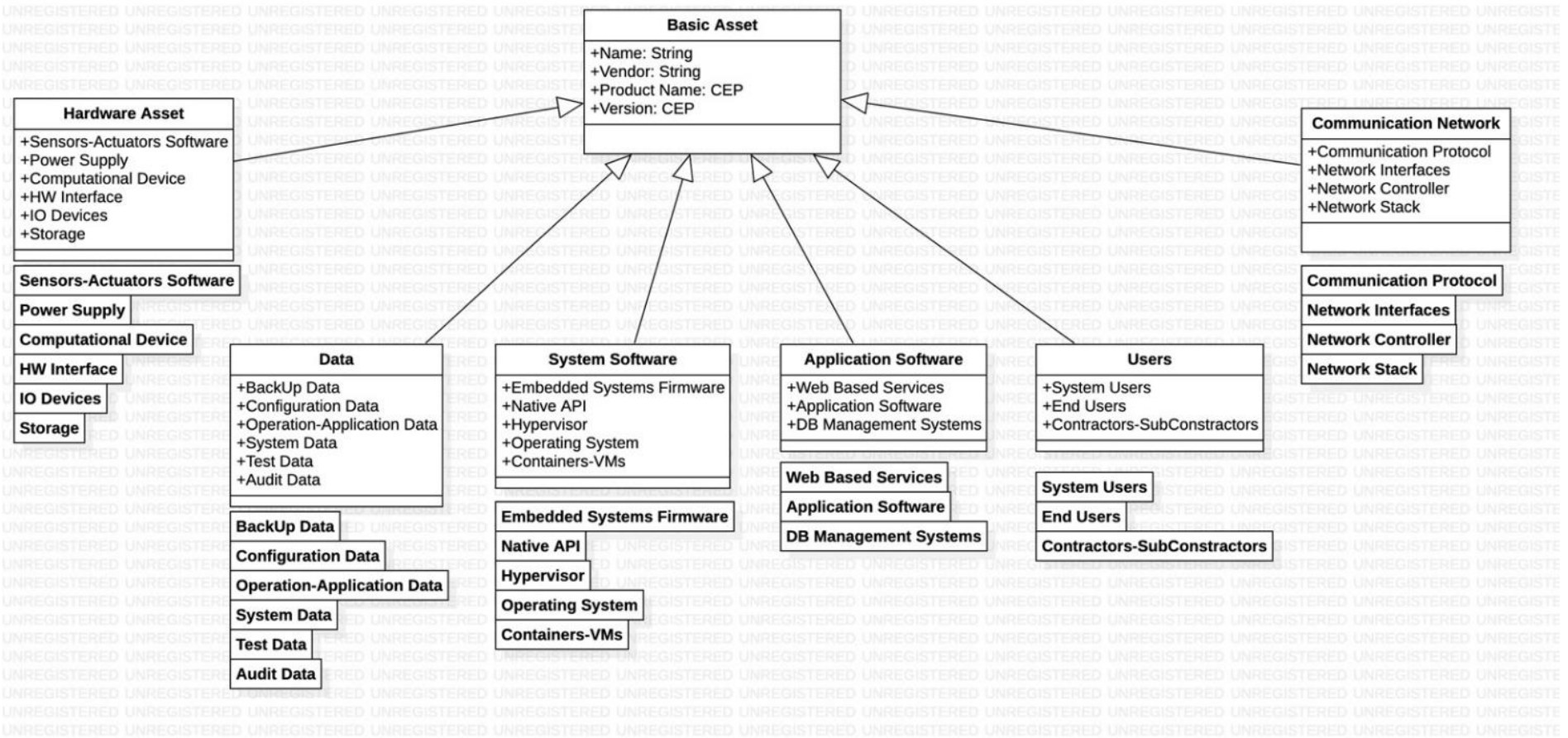


Figure 3: Analysis of Basic Assets Types

The use of a **repository** of assets is important in order to track all assets compositions for increasing reusability and keeping track of various applications in the context of the transport ecosystem. All types of users as well as the basic assets interact with each other through a Communication Layer. **Communication layer** is linked with the users since the latter are accessing the assets through the communication layer while the basic assets are the only entity linked with the communication layer since all other types (Assets and Entities) are superset of those basic assets.

From the risk analysis point of view it is clear that the conceptual model presents entities that impact (or constraint) the operation of the functionality of specific entities through the identification of various security/privacy related requirements. More specifically, the transport ecosystem as a whole is constraint by the **GDPR objectives** derived from current **legislation** meaning that these objectives will eventually introduce new legal and/or organizational requirements to the ecosystem in order for the latter to be GDPR compliant. **Security and privacy objectives** are also introduced in the system either by the **stakeholders** and/or the threat analysis. Security objectives are mainly introducing technical requirements from basic security constraints like Confidentiality, Integrity, Availability, Accountability, Non-Repudiation, Authenticity and Safety. These objectives assist stakeholders and software analysts in identifying specific technical security requirements that should be implemented based on the goals and objectives of the transport ecosystem. Similar, from the privacy point of view, the privacy objectives are mainly introducing technical requirements from basic privacy constraints like anonymity, pseudonymity, unlikability, undetectability and unobservability. It is obvious that the introduction of security and/or privacy requirements will constraint the operation of the basic assets, communication layer, asset and entities since these are the entities that offer the functionality to the proposed system. Given that, the same entities that offer the functionality on the proposed system introduce a number of **vulnerabilities** which are exploited by **threats (and cascading threats)** for harming the system. Threats can be either introduced by **malicious actors** (users) and/or by stakeholders. Two repositories, the **threat repository** and the **vulnerability repository** are considered critical for the design and implementation of any type of transport ecosystem since known threats and vulnerabilities belonging to the knowledge of security analysts and developers will provide valuable input during any type of risk analysis conducted prior or during implementation and validation stages. For this type of systems, it is critical to also define a way for calculating **risk per threat**. Following the conceptual model, three are the basic parameters. The **vulnerability level**, the **Threat Occurrence Probability** and impact that the specific threat will cause when a specific vulnerability is exploited.

In the following tables three instantiations of the proposed conceptual model are presented following the “infomobility” case study, the “E-ticketing” case study and the “Last mile Extension” case study.

Conceptual Model's Concepts	Scenario 1 Use Case: infomobility GENOA
GDPR OBJECTIVES	Art. 22 GDPR, Automated individual decision-making, including profiling. Data subject uses the AMT application every day and have the right not to be subject to a decision based solely on automated processing, including profiling, (in this case travel habits, profiling browsing behaviour) .
PRIVACY OBJECTIVES	AMT website navigation must be anonymous and pseudonymization measures must be implemented.
SECURITY OBJECTIVES	Infomobility server must be compliant with security objectives, hence technical measures must be implemented to assure information availability.
TRANSPORT ECOSYSTEM	Transport ecosystem entails infomobility scenarios
ENTITY(IES)-EDGE	Assets are the entities-edges of the system
ASSETS	In this case 8 assets are involved: <ol style="list-style-type: none"> 1. Mobile network (2G / 4G)¹ 2. Smart display 3. AVM system 4. Infomobility server 5. Service Management System 6. Website 7. Mobile Application 8. Smartphone
BASIC ASSETS	Assets are segregated into basic assets. <u>(Correlation between asset's numeration and this numeration)</u> . <ol style="list-style-type: none"> 1. 2G Modem, Microcontroller, Display, SIM card 2. Alarms, speakers, network interfaces (ethernet), Physical computing units, Operating System, Application Server, Databases and DBMS, Log files, configuration data 3. Physical computing units, Operating System, Application Server, Web

¹ In the course of the project, 5G solutions may be integrated in the use cases. In this scenario, 5G will be integrated as a network asset and proper adjustments will be made and reported in the validation report of the CitySCAPE platform.

	<p>services, Databases and DBMS, Log files, configuration data</p> <ol style="list-style-type: none"> Same as 3 Same as 3 Physical computing units, Operating System, Web Server, Content Management System, Web services, Databases and DBMS, Log files, configuration data Application, Log files, configuration data, Keys Computing system, Smartphone OS, mobile application, sensors
REPOSITORY OF ASSETS	Aforementioned basic assets are part of the repository of assets.
USER	Multiple kind of user co-exist in this info-mobility scenario, not only trusted (privilege or general users) but also untrusted users may exist.
COMMUNICATION LAYER AND/OR INTERFACE	<p>Assets communicate in different ways throw interfaces (<u>correlation between asset's numeration and this numeration</u>).</p> <ol style="list-style-type: none"> Via network Through 2G modem Standard computer hw interfaces (USB, Serial), Standard computer, I/O (Keyboard, Mouse), Network interfaces (Ethernet, Wifi, 4G, Bluetooth), OS interfaces (SSH, Telnet, RDP, etc.) , Application, interfaces (APIs, REST, etc.), Database connectors, File Transfer Services (e.g., FTP) Same as 3 Same as 3 Network interfaces (Ethernet, Wifi, 4G, Bluetooth), OS interfaces (SSH, Telnet, RDP, etc.), Web interfaces (APIs, REST, etc.), Servlet interface, Database connectors, File Transfer Services (e.g., FTP), Administrator UI, User UI Application interfaces – APIs to Web services, GUI, Permissions to use from phone: GNSS, Camera to scan Citypass, barcode, Microphone (vocal search), NFC reading for quickly, register Citypass User interfaces
VULNERABILITES	Info-mobility server may be vulnerable due to insufficient filtering/validation of browser input from users (directory traversal vulnerabilities).
VULNERABILITY LEVEL	Stakeholders define vulnerability level.

VULNERABILITY REPOSITORY	Vulnerability repository contains all the vulnerabilities of the transport ecosystem such as the aforementioned directory traversal vulnerabilities allocated in web server software (info mobility server and application code (AMT mobile application)).
THREATS	Directory traversal attack in the info-mobility server.
CASCADING THREATS	Malicious actor has the ability to view restricted files, which could provide the attacker with more information required to further compromise the system.
THREATS REPOSITORY	Threat repository contains all the threats associated with the vulnerabilities of the system.
THREATS OCCURENCE PROBABILITY	Stakeholders define threat occurrence probability level.
MALICIOUS ACTOR & STAKEHOLDERS	Malicious actors as well as stakeholders may introduce threats, in this case a malicious actor tries to access files.
IMPACT LEVEL	Exploitation of the system's vulnerabilities creates an impact level, in this case directory traversal attack has a X impact.
RISK PER THREAT	Multiplication of vulnerability level (directory traversal attack), threat occurrence probability (of directory traversal attack) and impact level (data monitoring etc.) shows risk per threat.

Table 2 Use Case: infomobility GENOA

Conceptual Model's Concepts	Scenario 2 Use Case: E-ticketing GENOA
GDPR OBJECTIVES	Where processing is to be carried out on behalf of a controller (<u>in this case third party payment provider or cloud services</u>), the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. Art. 28 GDPR
PRIVACY OBJECTIVES	Unobservability of the user. This implies that all uninvolved subjects cannot sufficiently distinguish whether or not exists, for example only validator (or other privilege users) have the right to check the user's ticket and have access to personal data through a special, unique barcode, and validation machines must not observe and track, unless it is made anonymously. Besides, anonymity of subjects involved in the item of interest (e-ticketing

	system) is provided even against the other subjects involved in that item of interest (administrators who oversee services must not distinguish users, anonymous user monitoring).
SECURITY OBJECTIVES	Integrity objectives. Appropriate security measures must be applied to prevent data from being modified from unauthorized party. For example, illustrated data from the ticketing system must be consistent and trustworthy during the entire life cycle.
TRANSPORT ECOSYSTEM	Transport ecosystem entails E-ticketing
ENTITY(IES)-EDGE	Assets are the entities-edges of the system
ASSETS	In this case 8 assets are involved: <ol style="list-style-type: none"> 1. Mobile Network (2G / 4G) 2. Ticketing System 3. Subscription System 4. Website 5. Mobile Application 6. Verificator's application 7. Verificatory device 8. Smartphone
BASIC ASSETS	Assets are segregated into basic assets. (<u>Correlation between asset's numeration and this numeration</u>). <ol style="list-style-type: none"> 1. - 2. Physical computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data 3. Same as 2 4. Physical computing units, Operating System, Web Server, Content Management System, Web services, Databases and DBMS, Log files, configuration data 5. Application, Log files, configuration data, Keys 6. Application, Log files, configuration data, Keys 7. Micro-controller, Camera, Firmware/Middleware, Software components, Log files, configuration data 8. Computing system, Smartphone OS, mobile application, sensors
REPOSITORY OF ASSETS	Aforementioned basic assets are part of the repository of assets.

USER	Multiple kind of user co-exist in this info-mobility scenario, not only trusted (privilege or general users) but also untrusted users may exist.
COMMUNICATION LAYER AND/OR INTERFACE	<p>Assets communicate in different ways throw interfaces (<u>correlation between asset's numeration and this numeration</u>).</p> <ol style="list-style-type: none"> 1. Via network. 2. Standard computer hw interfaces (USB, Serial), Standard computer I/O (Keyboard, Mouse), Network interfaces (Ethernet, Wifi, 4G, Bluetooth), OS interfaces (SSH, Telnet, RDP, etc.), Application interfaces (APIs, REST, etc.), Web services, Database connectors, File Transfer Services (e.g., FTP) 3. Same as 2 4. Standard computer hw interfaces (USB, Serial), Standard computer I/O (Keyboard, Mouse), Network interfaces (Ethernet, Wifi, 4G, Bluetooth), OS interfaces (SSH, Telnet, RDP, etc.) , Web interfaces (APIs, REST, etc.), Servlet interface, Database connectors, File Transfer Services (e.g., FTP), Administrator UI, User UI 5. Application interfaces – APIs to Web services, GUI, Permissions to use from phone: GNSS, Camera to scan Citypass barcode, Microphone (vocal search), NFC reading for quickly register Citypass 6. Same as 5 7. Camera - QR reader, NFC, RFID, Mobile network interface (4G), debugging port, User Interface, Web services 8. User interfaces
VULNERABILITES	Verificator application-barcode scanner presents a potential vulnerability. Application's OS could be exploited with a fake-malicious bar-code (SQL injection etc.).
VULNERABILITY LEVEL	Stakeholders define vulnerability level.
VULNERABILITY REPOSITORY	Vulnerability repository contains all the vulnerabilities of the transport ecosystem such as the aforementioned SQL injection via barcode
THREATS	SQL injection via barcode
CASCADING THREATS	Malicious actor may manage to get access to the host computer through the application.

THREATS REPOSITORY	Threat repository contains all the threats associated with the vulnerabilities of the system.
THREATS OCCURENCE PROBABILITY	Stakeholders define threat occurrence probability level.
MALICIOUS ACTOR & STAKEHOLDERS	Malicious actors as well as stakeholders may introduce threats, in this case a malicious actor tries to harm the system with a malicious barcode.
IMPACT LEVEL	Exploitation of the system's vulnerabilities creates an impact level, in this case SQL injection via barcode has a X impact.
RISK PER THREAT	Multiplication of vulnerability level, threat occurrence probability and impact level shows risk per threat.

Table 3 Use Case: E-ticketing GENOA

Conceptual Model's Concepts	Scenario 3 Use Case: Last Mile Extension TALLINN
GDPR OBJECTIVES	Art.26 GDPR Joint controllers (Tallinn transportation authority and Tallinn university of technology).
PRIVACY OBJECTIVES	All privacy objectives must be applied (anonymity, pseudonymity, unlinkability, unobservability, undetectability)
SECURITY OBJECTIVES	All security objectives must be applied (confidentiality, integrity, availability, Accountability, non-repudiation, authenticity)
TRANSPORT ECOSYSTEM	Transport ecosystem entails last mile extension use case
ENTITY(IES)-EDGE	Assets are the entities-edges of the system
ASSETS	In this case 29 assets are involved: <ol style="list-style-type: none"> 1. Mobile Network (4G/5G/) 2. Adhoc vehicular network 3. Real-time monitoring system 4. Payment service system 5. Cross-border teleoperation services 6. Thoreb On-Board Computer 7. Thoreb Internal Driver Display Screen 8. Thoreb Communication Module 9. Thoreb Internal Passenger Display Screen 10. Switch 11. Video surveillance system 12. Radio modem 13. HMI Machine Validator 14. Transit Gateway 15. Communication Module 16. Vehicle on-board unit

	17. Camera Sensors 18. Camera Data 19. GNSS 20. IMU 21. Ultrasonic Sensors 22. LIDAR 23. Local Dynamic Map 24. Communication modem 25. Operating System 26. Self-driving application 27. Fernride Cross-border Teleoperation Module 28. HSM 29. Actuators
BASIC ASSETS	Assets are segregated into basic assets. <u>(Correlation between asset's numeration and this numeration).</u> <ol style="list-style-type: none"> 1. – 2. – 3. Physical or virtual computing units, Operating System, Application Server, Web services, Databases and DBMS, Log files, configuration data 4. Same as 3 5. Same as 3 6. Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data 7. Hardware I/O, Hardware Display, Hardware Display, On-board computer, Ethernet, Firmware, OS, Software components, Log and configuration files. 8. Modem, Middleware / Router OS, GNSS, Log and configuration files 9. Hardware I/O, Hardware Display, Hardware Display, On-board computer, Ethernet, Firmware, OS, Software components, Log and configuration files. 10. Hardware – Network ports, Firmware/Router OS, web application 11. Hardware – Cameras, on-board controllers, firmware, software components, video data. 12. Modem, Middleware / Router OS, GNSS, Log and configuration files 13. Hardware (network interfaces, sensors, credit card, micro-computer, touch

	<p>display), Firmware, OS, Log and configuration files</p> <p>14. Physical computing units, Operating System, APIs, Application Server, Software components, Local data assets (databases), Log files, configuration data</p> <p>15. Modem, Firmware, Log and configuration files</p> <p>16,17,18,19,20,21,22,24,25,26,27,28,29. -</p>
REPOSITORY OF ASSETS	Aforementioned basic assets are part of the repository of assets.
USER	Multiple kind of user co-exist in this last mile extension scenario, not only trusted (privilege or general users) but also untrusted users may exist. More specifically users are <u>1. Transport Management Stakeholders, 2. End-users, 3. Operators, 4. Support Users 5. External stakeholders.</u>
COMMUNICATION LAYER AND/OR INTERFACE	<p>Assets communicate in different ways throw interfaces (<u>correlation between asset's numeration and this numeration</u>).</p> <ol style="list-style-type: none"> 1. Via network 2. Via ITS messages to anyone part of the ITS-V2X network 3. Standard computer hw interfaces (USB, Serial), Standard computer I/O (Keyboard, Mouse), Network interfaces (Ethernet, Wifi, 4G, Bluetooth), OS interfaces (SSH, Telnet, RDP, etc.) , Application interfaces (APIs, REST, etc.), Database connectors, File Transfer Services (e.g., FTP) 4. Same as 3 5. Same as 3 6. CAN bus connection, Mobile network connections, Standard computer hw interfaces (USB, Serial), OS interfaces (SSH, Telnet, RDP, etc.), Other network, interfaces (Ethernet, Wifi, Bluetooth), Application interfaces (APIs, REST, etc.), Database connectors 7. Ethernet network interface, Driver GUI, ITxPT standard, interfaces (MQTT), (Netex, SIRI, OJP, Tigr), debugging port, computer hw interfaces (USB) 8. 3G/4G radio connection, Network interface (Ethernet), Communication module admin panel 9. Ethernet network interface, ITxPT standard interface, (MQTT), (Netex, SIRI,

	<p>OJP, Tigr), debugging port, computer hw interfaces (USB)</p> <p>10. Network interfaces (Ethernet), Switch module admin panel, VLANs, vSwitches, ITxPT interfaces (MQTT), (Netex, SIRI, OJP, Tigr)</p> <p>11. Network interfaces (Ethernet), ITxPT standard interfaces (MQTT), (Netex, SIRI, OJP, Tigr)</p> <p>12. RS232, V2X radio</p> <p>13. Network interfaces - RFID, Ethernet, NFC, QR Code, Credit Card, User Interface</p> <p>14. Standard computer hw interfaces (USB, Serial), Standard computer I/O (Keyboard, Mouse), Network interfaces (Ethernet), OS interfaces (SSH, Telnet, RDP, etc.), Application interfaces (APIs, REST, JSON etc.), Web services, Database connectors, Interfaces for ISO8583 (financial transactions)</p> <p>15. CAN bus</p> <p>16. Standard computer hw interfaces (USB, Serial), Standard computer I/O (Keyboard, Mouse), Network interfaces (Ethernet, CAN)</p> <p>17. -</p> <p>18. Access from repository</p> <p>19,20,21,22. CAN bus interface</p> <p>23. Application interfaces (APIs, REST, JSON etc.), Web services, Database connectors</p> <p>24. Network interface (Ethernet, CAN), V2X, 4G/5G</p> <p>25. OS interfaces (SSH, Telnet, RDP, etc.)</p> <p>26. Application interfaces (APIs, REST, JSON etc.), Messaging protocols, Web services, Database connectors</p> <p>27. -</p> <p>28. Network interface (Ethernet), Physical access (USB, Serial), HSM interfaces</p> <p>29. Network interface (Ethernet, CAN)</p>
VULNERABILITES	Multiple kind of vulnerabilities exist. For example, A man-in-the-middle attack in the RFID system.
VULNERABILITY LEVEL	Stakeholders define vulnerability level.
VULNERABILITY REPOSITORY	Vulnerability repository contains all the vulnerabilities of the transport ecosystem such as the aforementioned man-in-the-middle attack in the RFID system.
THREATS	Man-In-The-Middle attack

CASCADING THREATS	The hacker listens the communication between a tag and reader and then intercepts and manipulates the information.
THREATS REPOSITORY	Threat repository contains all the threats associated with the vulnerabilities of the system.
THREATS OCCURENCE PROBABILITY	Stakeholders define threat occurrence probability level.
MALICIOUS ACTOR & STAKEHOLDERS	Malicious actors as well as stakeholders may introduce threats, in this case a malicious actor tries to harm the system.
IMPACT LEVEL	Exploitation of the system's vulnerabilities creates an impact level.
RISK PER THREAT	Multiplication of vulnerability level, threat occurrence probability and impact level shows risk per threat.

Table 4: Use Case: Last Mile Extension TALLINN

3. SYSTEM ARCHITECTURE AND ASSETS

The risk analysis approach extends the approach followed in (SaferTEC, 2017) into a more flexible and resilient framework with the use of the new conceptual model, the hierarchical definition of assets and the dynamic risk analysis paradigm. Sequentially, the initial risk analysis approach relies on existing methodologies, namely EBIOS, SecureTropos, and Priis (ANSSI), (Mouratidis, 2011), (Kalloniatis, 2005). The methodology is implemented in steps, which are loosely followed during the CitySCAPE approach. The steps include:

1. Identification of Assets – which includes the process of identifying the tangible or intangible entities of the system that have value and should be protected.
2. Organizational domain mapping – which includes the architectural view of the system/organization
3. Threat modelling – which contains the identification of threats for the system.
4. Elicitation of security vulnerabilities – which contains the definition of security vulnerabilities.
5. Security and privacy requirements analysis

In order to develop a cascading threat methodology in Task 2.3 of the project, the identification of assets and the definition of the system architecture was performed and reported in D2.4. For completeness a summary of the results is presented in this section. Additionally, the schematic modelling of composite assets based on basic assets is described.

3.1 Basic Assets

According to the approach described in D2.4:

- A set of basic assets is identified. These are generic asset types that are generally found in ICT platforms.
- The basic assets are combined together in order to model more complicated assets that can be found in a given implementation. These assets are called, according to the conceptual model, “composite assets”.
- The integration of multiple basic assets together is performed through the definition of relationships between basic assets.
- If a composite asset cannot be decomposed into basic assets, then it should be included as a basic asset.
- When the composite assets are identified, decomposition to a set of basic assets should be performed. The basic assets should be interconnected through defined relations.

- The hierarchical modeling of the system assets as composite assets composed by multiple interconnected basics has the main advantage of inheritance. All threats and vulnerabilities from or linked to a basic asset are inherited by the composite system asset, if the composite asset contains the specific basic asset. For example, “The server has an operating system”, means that the server will inherit the vulnerabilities of the operating system.
- Differentiation and filtering among instantiations of a basic asset can be performed through object tagging. Thus, the basic asset may be “operating system” with tag: “Linux distro”. Therefore, a vulnerability will be activated only to composite assets having operating systems with the specific Linux distribution.

The list of basic assets contains:

Asset Group ID	Asset Group	Asset ID	Basic Asset Type
AS-HW	Hardware	AS-HW-01	Sensors/Actuators Hardware
		AS-HW-02	Power supply
		AS-HW-03	Computational Device
		AS-HW-04	HW Interface
		AS-HW-05	I/O Devices
		AS-HW-06	Storage
AS-DA	Data	AS-DA-01	Backup Data
		AS-DA-02	Configuration Data
		AS-DA-03	Operation Data / Application Data
		AS-DA-04	System Data
		AS-DA-05	Test Data
		AS-DA-06	Audit Data
AS-SS	System Software	AS-OS-01	Embedded Systems Firmware
		AS-OS-02	Native API
		AS-OS-03	Hypervisor
		AS-OS-04	Operating System
		AS-OS-05	Containers / VMs
AS-SO	Application Software	AS-SO-01	Web-Based Services
		AS-SO-02	Application Software
		AS-SO-03	Database Management Systems

AS-US	Users	AS-US-01	System Users (Administrators, operators, security experts)
		AS-US-02	End Users (CPaaS users - travelers)
		AS-US-03	Contractors/Sub-contractors (3 rd parties)
AS-NE	Communication Network	AS-NE-01	Communication Protocol
		AS-NE-02	Network Interfaces
		AS-NE-03	Network Controller (HW)
		AS-NE-04	Network Stack (SW)

Table 5: Basic Assets List

As an addition, the possible relationships between assets are included in Table 6. It is noted that the list is not exhaustive, but it is based on the analysis performed for the defined CitySCAPE use cases. If needed, new relationships can be defined and added.

Relationships between assets
X stores Y
X uses Y
X hosts Y
X uses resources by Y
X invokes Y
X exports/exposes Y
X connects to Y
X belongs to Y
X controls Y
X interacts with Y
X decrypts/encrypts Y
X provides to Y
X handles Y

Table 6: Identified relationships between basic assets

3.2 System Assets

The high-level architectural overview of the Tallinn and Genoa use cases as already defined in CitySCAPE deliverable 2.4 are depicted in Figure 4 and Figure 5, respectively.

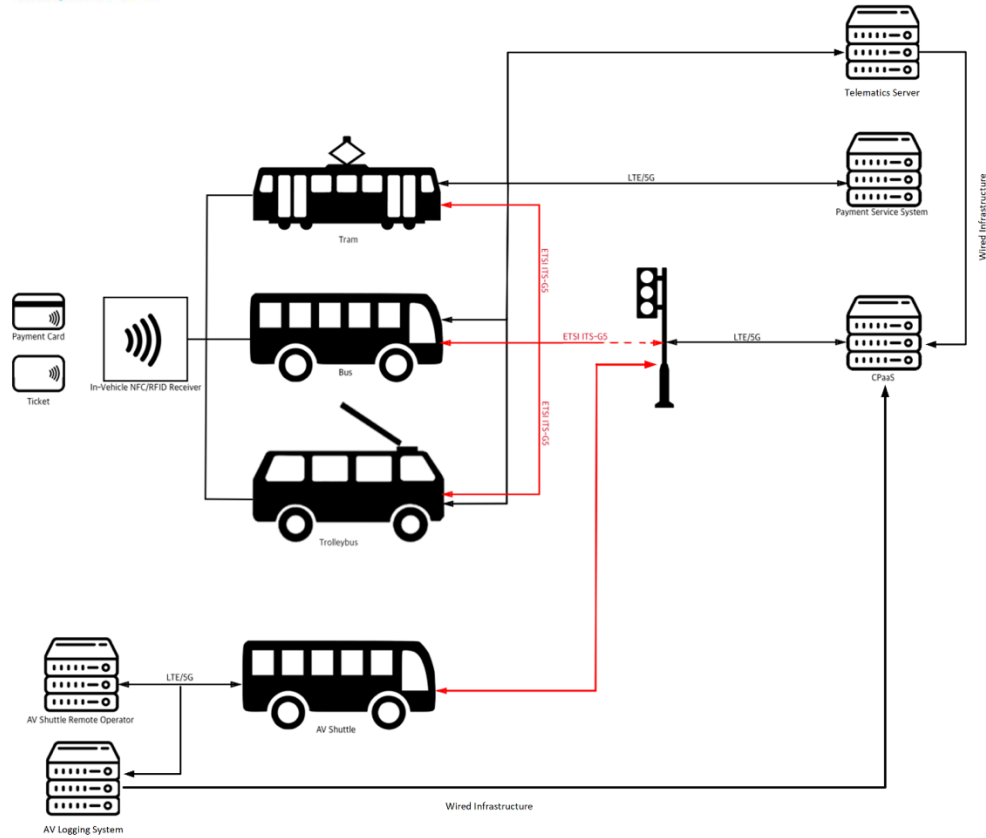


Figure 4: Tallinn Architecture High Level Overview

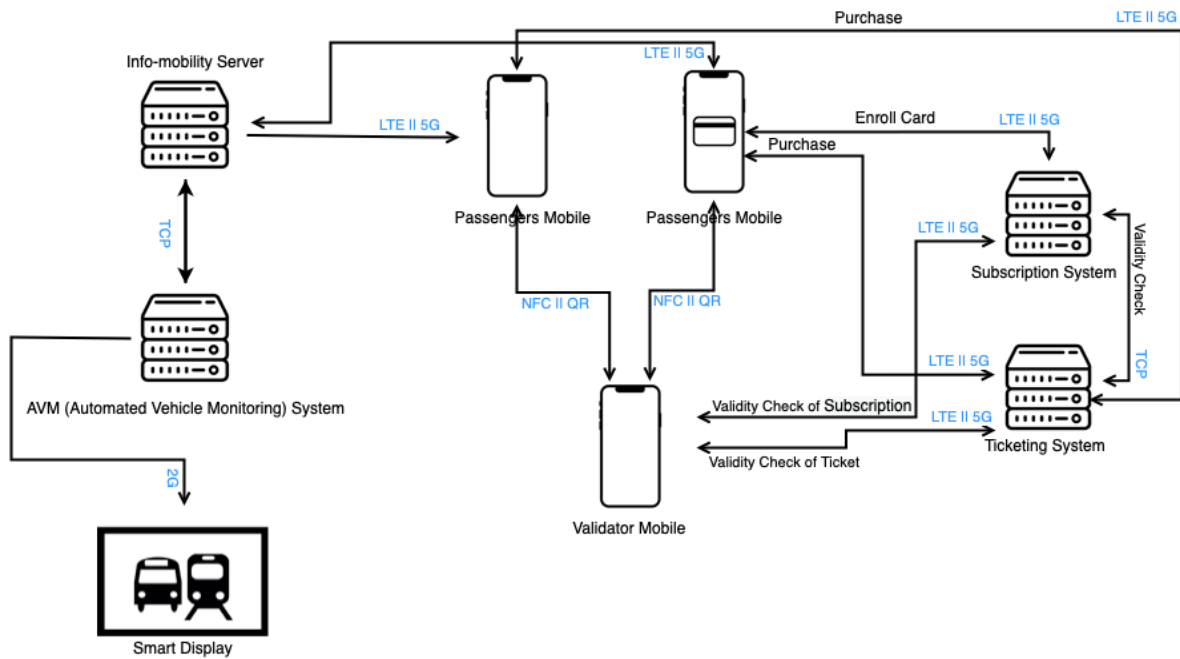


Figure 5: Genoa Architecture High Level Overview

According to the architectures, Table 7 and Table 8 present the composite asset list for the two reference systems, as described in D2.4.

Composite Asset ID	Asset Name
COM-TAL-AS-01	Autonomous Vehicle (AV) Shuttle
COM-TAL-AS-02	Autonomous Vehicle (AV) Shuttle Remote Operator
COM-TAL-AS-03	Communications Platform-as-a-Service (CPaaS)
COM-TAL-AS-04	Payment Service System
COM-TAL-AS-05	Roadside Unit (RSU)
COM-TAL-AS-06	Tram
COM-TAL-AS-07	Bus
COM-TAL-AS-08	Trolleybus
COM-TAL-AS-09	Autonomous Vehicle (AV) logging server
COM-TAL-AS-10	Telemetry Server

Table 7 Tallinn Composite Asset List

While for the Genoa use case, the list of Composite Assets is given in Table 8.

Composite Asset ID	Asset Name
COM-GEN-AS-01	AVM (Automated Vehicle Monitoring) System
COM-GEN-AS-02	Passenger Mobile Device and Application
COM-GEN-AS-03	Smart Display
COM-GEN-AS-04	Subscription System
COM-GEN-AS-05	Ticketing System
COM-GEN-AS-06	Validator Mobile Device and Application
COM-GEN-AS-07	Info-mobility Server

Table 8 Genoa Composite Asset List

Table 9 and Table 10 show all the involved basic assets for the two architectures, i.e., all the components that are used to constitute the composite assets and implement the use case. To assist our analysis and indicate threats to any appropriate component, each involved composite

asset (i.e., passenger mobile devices, trolleybuses, roadside units) comprises several basic assets.

Basic Asset Name	Basic Asset Type	Asset ID
Native Application	Application Software	AS-SO-02
Application Data	Operation Data / Application Data	AS-DA-03
Application Keys	Operation Data / Application Data	AS-DA-03
Application Database	Database Management Systems	AS-SO-03
Native API	Native API	AS-OS-02
OS	Operating System	AS-OS-04
OS Services	Operating System	AS-OS-04
OS Data	System Data	AS-DA-04
HSM Interface	Operating System	AS-OS-04
Firmware and Drivers	Operating System	AS-OS-04
H/W Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
HSM	Computational Device	AS-HW-03
HMI	I/O Devices	AS-HW-05
Actuator	Sensors/Actuators Hardware	AS-HW-01
Sensor	Sensors/Actuators Hardware	AS-HW-01
Display	I/O Devices	AS-HW-05
Storage	Storage	AS-HW-06
Network Controller	Network Controller (HW)	AS-NE-03
Network Stack ITS-G5	Network Stack (SW)	AS-NE-04
Network Interface ITS-G5	Network Interfaces	AS-NE-02
Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04
Network Interface LTE (4G)	Network Interfaces	AS-NE-02
Network Stack 5G	Network Stack (SW)	AS-NE-04
Network Interface 5G	Network Interfaces	AS-NE-02
Camera	I/O Devices	AS-HW-05
Web API	Web-Based Services	AS-SO-01
Web Service	Web-Based Services	AS-SO-01
Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04
Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02
VM Management Interface	Web-Based Services	AS-SO-01
Hypervisor	Operating System	AS-OS-04

Table 9: Basic Assets of Tallinn Architecture

Basic Asset Name	Basic Asset Type	Asset ID
Mobile Application	Application Software	AS-SO-02
Application Data	Operation Data / Application Data	AS-DA-03
Application Keys	Operation Data / Application Data	AS-DA-03
Application Database	Database Management Systems	AS-SO-03
Native API	Native API	AS-OS-02
OS	Operating System	AS-OS-04
OS Services	Operating System	AS-OS-04
OS Data	System Data	AS-DA-04
Firmware and Drivers	Operating System	AS-OS-04
H/W Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
Display	I/O Devices	AS-HW-05
Storage	Storage	AS-HW-06
Network Controller	Network Controller (HW)	AS-NE-03
Network Stack NFC	Network Stack (SW)	AS-NE-04
Network Interface NFC	Network Interfaces	AS-NE-02
Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04
Network Interface LTE (4G)	Network Interfaces	AS-NE-02
Network Stack 5G	Network Stack (SW)	AS-NE-04
Network Interface 5G	Network Interfaces	AS-NE-02
Camera	I/O Devices	AS-HW-05
Network Stack 5G	Network Stack (SW)	AS-NE-04
Web API	Web-Based Services	AS-SO-01
Web Service	Web-Based Services	AS-SO-01
Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04
Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02
Native Application	Application Software	AS-SO-02
OS	Embedded Systems Firmware	AS-OS-01
OS Services	Embedded Systems Firmware	AS-OS-01
Network Stack GSM (2G)	Network Stack (SW)	AS-NE-04
Network Interface GSM (2G)	Network Interfaces	AS-NE-02

Communication Protocol	Communication Protocol	AS-NE-01
------------------------	------------------------	----------

Table 10: Basic Assets of Genoa Architecture

3.3 Schematic representation of composite assets

The decomposition of composite assets into basic assets is a top-down approach that allows us to discover all the involved essential inner elements that comprise a composite asset along with their interconnections. In order to schematically model the decomposition process E-R diagrams were used, where Entities are the basic assets (Table 5) and Relationships (Table 6) are the interconnection types among them. At this point, cardinalities between two entities of the graph were not defined.

A cyber-physical system with the complexity of a multimodal transport system contains application software, software that provides operational and functional services, hardware devices (I/O, sensors, actuators, and more), data, network protocols, networking devices and more. In order to be able to accurately model a composite asset, effort was spent in order to provide schematics in a layered view. More specifically, the layers include:

- The application software
- The underlying software (Operating system, firmware, hypervisor, etc.)
- The data
- The hardware
- The network

The layered approach provides the following benefits:

- We can simplify analysis by isolating and providing results only for the higher layers (e.g., applications) assuming that the lower layers are trusted. This will make the risk analysis approach possible even if we have no information for e.g., the underlying hardware.
- We can create logical – functional links for peer layers between different assets.

This detailed analysis enables us to identify threats per each layer of a composite asset and assign the appropriate vulnerabilities and threats to each one of them. In order to make the figures more readable, colour coding was used to separate the different layers per asset. More specifically:

- operating system is colored in red,
- application is colored in blue,
- database is colored in purple,
- network is colored in green and
- hardware is colored in yellow

Figure 6: Validator Mobile Device Composite Asset of Genoa Use Case illustrates the basic assets that comprise the composite asset of the ticket validator's mobile device from the Genoa use case. We can identify, among others, how the application programming interface (API) as a native component is exported into the application in order for any mobile application to communicate with the underline operating system's (OS) features. Additionally, in Figure 7: Ticketing System Server Composite Asset of Genoa Use Case

we can identify how the operating system provides storage to the web application of the Ticketing System Server Composite Asset of Genoa Use Case. Moreover, regarding the Tallinn's use cases, Figure 8: Communication Platform as a Service (CPaaS) Composite Asset of Tallinn Use Case depicts how the hypervisor of the CPaaS virtual environment provides resources to the virtual machines of the infrastructure and Figure 9: Trolley Composite Asset of Tallinn Use Case illustrates how the Hardware Security Module (HSM) of a connected vehicle protects the application space cryptographic materials.

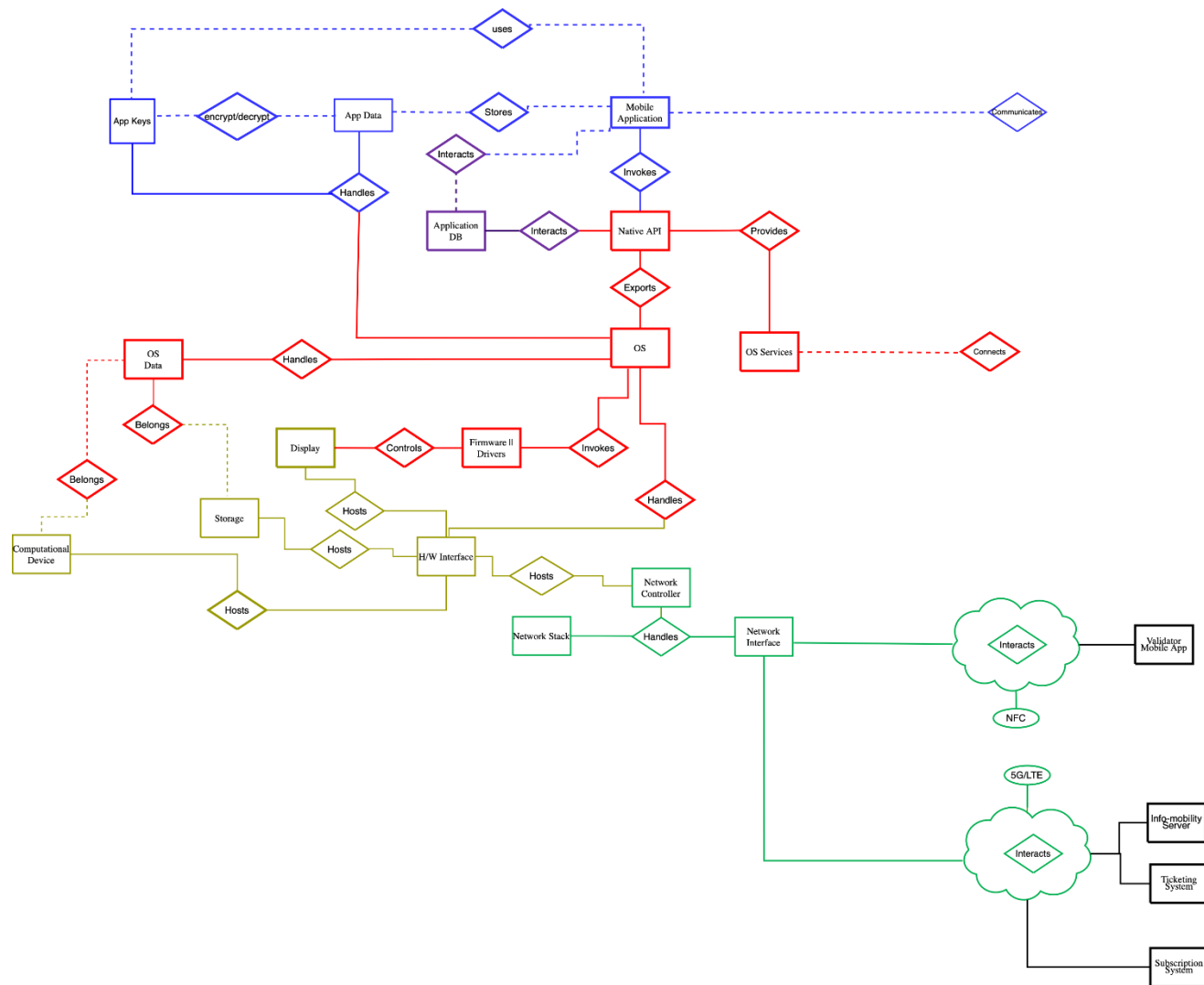


Figure 6: Validator Mobile Device Composite Asset of Genoa Use Case

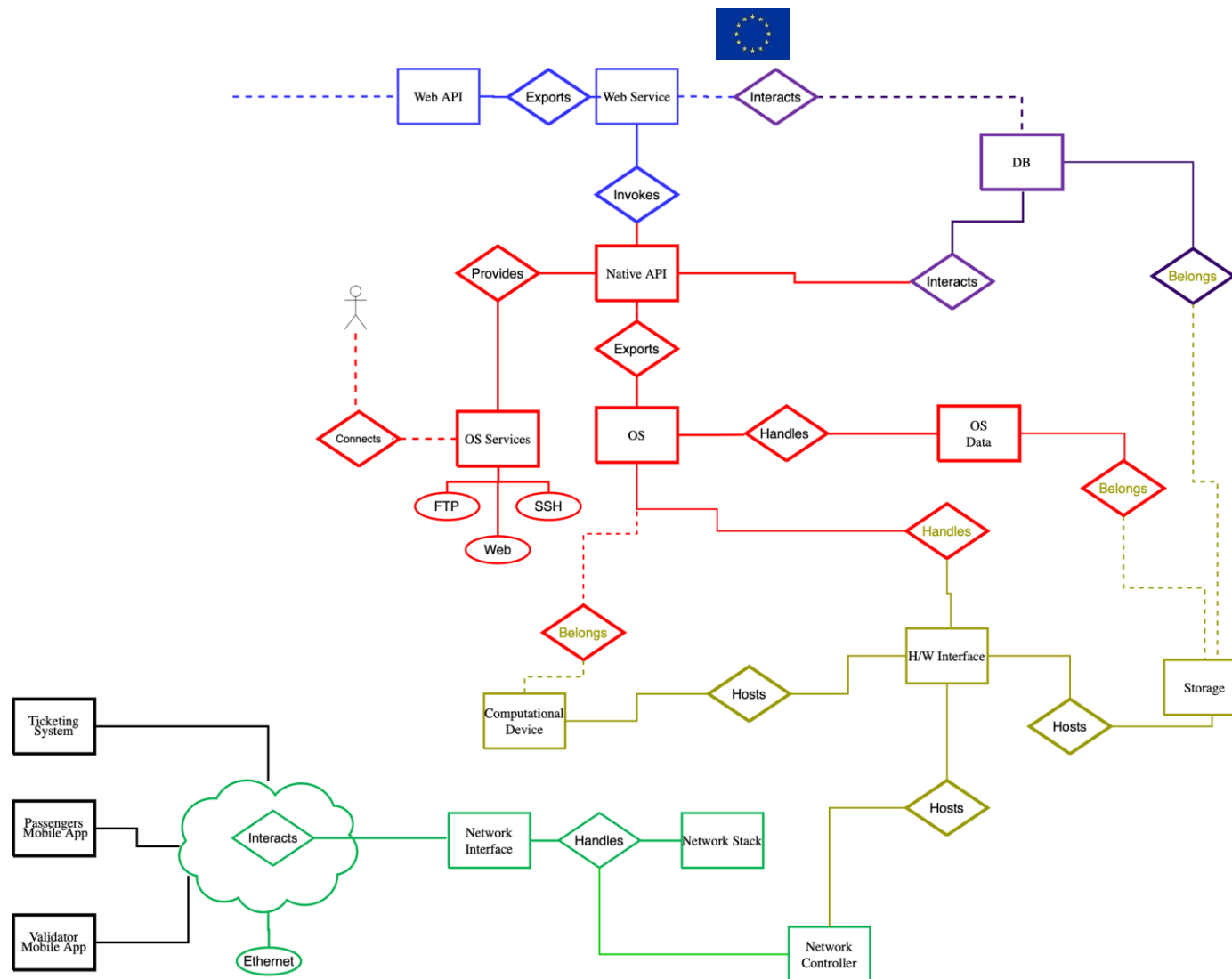
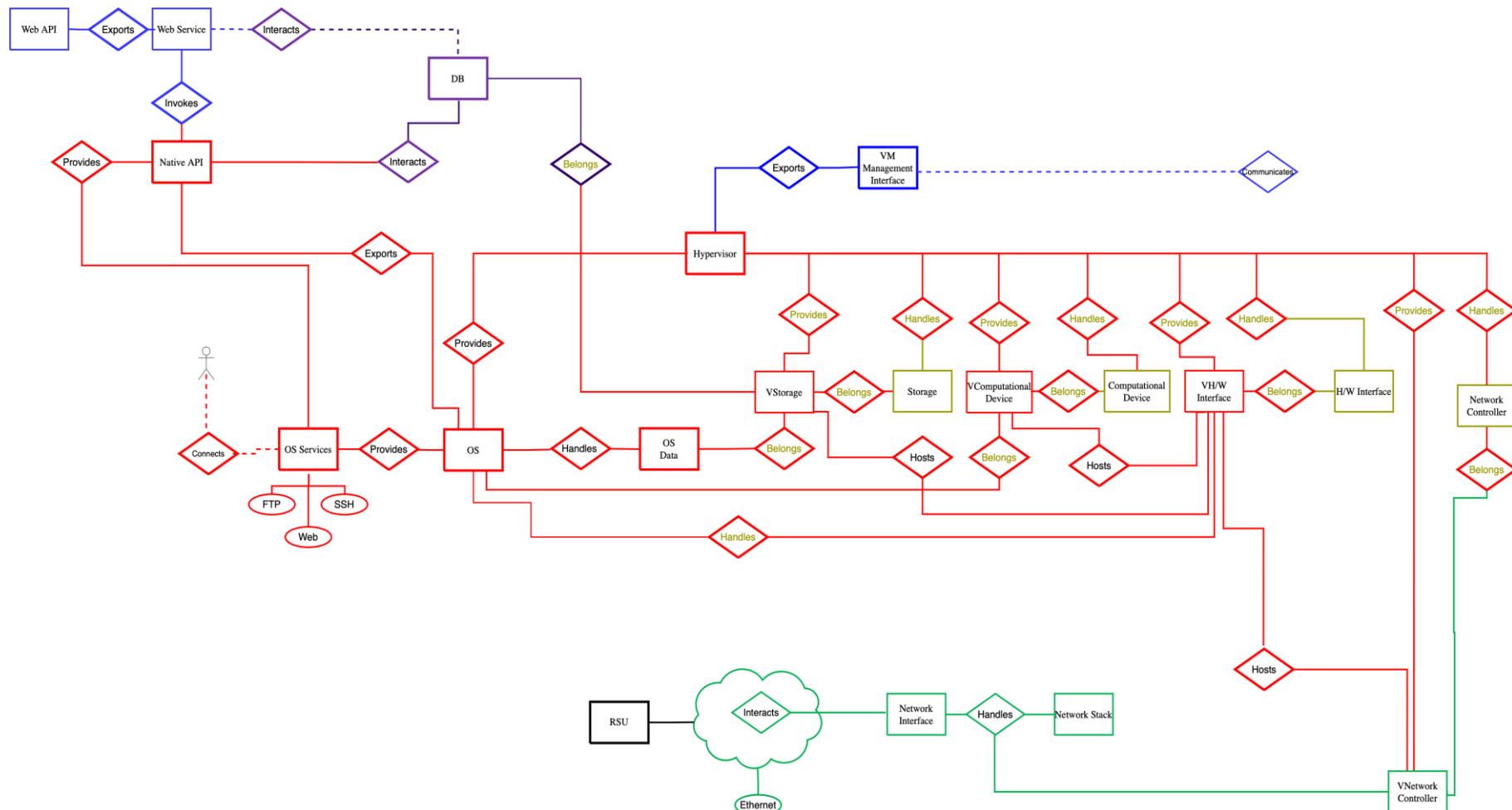


Figure 7: Ticketing System Server Composite Asset of Genoa Use Case



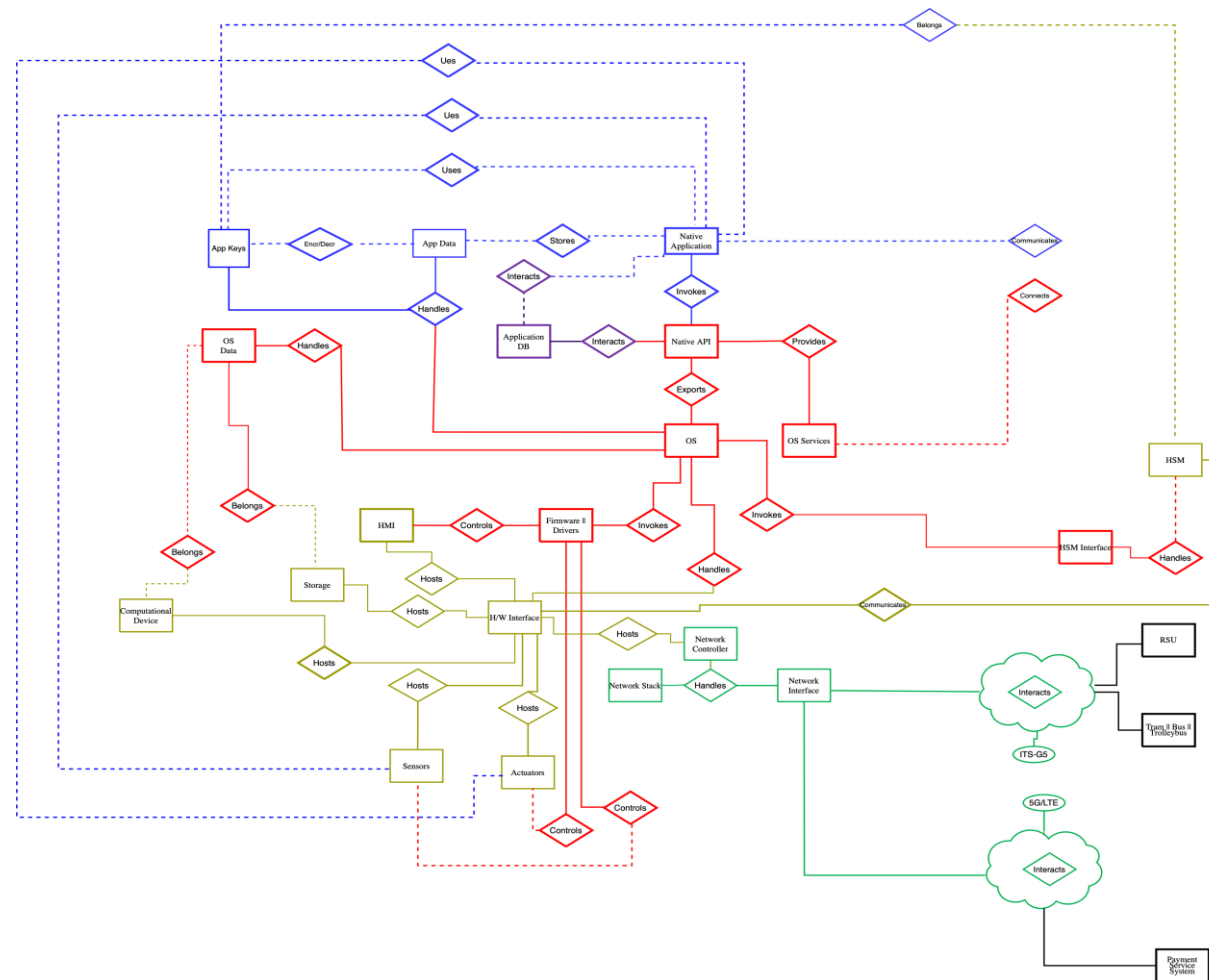


Figure 9: Trolley Composite Asset of Tallinn Use Case

4. THREATS

This section provides the results of the security threat analysis that was based on D2.2 and partially performed in D2.4.

4.1 Association between Threats and Assets

The correlation between Tallinn and Genoa use cases assets, their identified threats and the threat implementation impact is provided. Table 7 provides the composite assets of the Genoa use case, while Table 8 the assets of the Tallinn use case.

Table 11 depicts the identified threats applied to both cities' use cases assets. In the table, the basic information security requirements, i.e., Confidentiality, Integrity and Availability are denoted as C, I, and A.

Type	Threat ID	Threat	Impact		
			C	I	A
SW	TH-01	Malware Injection	X	X	X
SW/NET	TH-02	Denial of Service			X
DATA	TH-03	Modification of Information / Data Manipulation	X	X	X
NET	TH-04	Man in the Middle	X	X	X
NET	TH-05	Interception of Information	X		
NET	TH-06	Replay of Messages		X	X
NET	TH-07	Network Outage			X
HW	TH-08	Failures of Devices			X
SW/NET	TH-09	Failure of System			X
NET	TH-10	Loss of Support Services			X
SW/NET	TH-11	Software Exploitation / Malicious Code Injection	X	X	X
HW	TH-12	Natural Disaster			X
HW	TH-13	Environmental Disaster			X
HW/SW	TH-14	Device Modification	X	X	X
HW	TH-15	Device Destruction (Sabotage)			X
HW	TH-16	Device Loss or Theft	X		
DATA	TH-17	Unintentional Disclosure of Data	X		
HW	TH-18	Attacks on Decommissioned Device	X		
NET	TH-19	Phishing Attacks	X	X	X
NET	TH-20	Network Spoofing	X	X	X
SW/NET	TH-21	Resource Exhaustion/Lack of resources			X
SW	TH-22	Isolation/Virtualization Abuse	X	X	X

SW/NET	TH-23	Management Interface Compromise	X	X	X
HW/SW/NET	TH-24	Unauthorized Access to Premises	X	X	X
SW/NET	TH-25	Abuse of Authorisation / Privilege Escalation	X	X	X
DATA	TH-26	Loss/Leakage of Information	X		X
SW/NET	TH-27	Abuse of Authentication	X	X	X
SW/NET	TH-28	Identity Theft	X	X	
SW/NET	TH-29	Social Engineering	X	X	X

Table 11: CitySCAPE Identified Threats

Table 12 depicts the identified threats for each Genoa's composite asset, while Table 13 shows the identified threats regarding Tallinn's composite assets.

The table below provide additional information regarding the applicability of a threat (in the column Likelihood) to an asset for each identified threat and basic asset association.

Threats apply to specific basic assets, but their applicability varies based on the composite asset they belong. For instance, the threat of "TH-22 - Isolation/Virtualization Abuse" applies only in cases where an operating system is executed under the control of a hypervisor, such as the Subscription System of the Genoa Use Case and is not applicable for any other case such as the Validator's Mobile Device. Therefore, is "TH-22" a threat for an operating system? The answer is yes. Is it applicable at any condition? The answer is no – the operating system should be hosted on a virtual machine. Therefore, the "likelihood" variable is an indicator if the specific composite asset is indeed a virtual machine or virtual network function.

In another example, the "TH-13 - Environmental Disaster" threat applies to hardware components. However, this threat regards only the cases where hardware basic assets are embedded into composite assets located in remote physical locations (i.e., the H/W Interface of Payment Service System / Autonomous Vehicle - AV Logging System) and not in mobile devices (such as the Passenger Mobile Device or the Validator Mobile Device) where reside along with their users. In the CitySCAPE risk analysis, each composite asset was investigated in order to extract the applicability of a threat on the asset. The result of the consultation made by Task 2.2 security experts with the CitySCAPE CPaaS implementations for the "likelihood" variable considering the high-level models of Figure 4 and Figure 5 is presented in the last column of Table 12 and Table 13 for the Genoa and Tallin use cases respectively.

Composite Asset Name	Basic Asset Name	Basic Asset Type	Asset ID	Threat	Threat ID	Likelihood
Passenger Mobile Device	Mobile Application	Application Software	AS-SO-02	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
				Modification of Information / Data Manipulation	TH-03	1
				Loss/Leakage of Information	TH-26	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Data	Operation Data / Application Data	AS-DA-03	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1

	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	0
				Isolation/Virtualization Abuse	TH-22	0
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	0
				Resource Exhaustion	TH-21	1

				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Firmware and Drivers	Operating System	AS-OS-04	Malware Insertion	TH-01	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Unauthorized Access to Premises	TH-24	0
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0

				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Display	I/O Devices	AS-HW-05	Device Destruction (Sabotage)	TH-15	0
				Device Loss or Theft	TH-16	1
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access to Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Device Modification	TH-14	0
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1

	Network Stack NFC	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface NFC	Network Interfaces	AS-NE-02			
	Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface LTE (4G)	Network Interfaces	AS-NE-02			
	Network Stack 5G	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface 5G	Network Interfaces	AS-NE-02			
Validator Mobile Device	Mobile Application	Application Software	AS-SO-02	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
				Modification of Information / Data Manipulation	TH-03	1
				Loss/Leakage of Information	TH-26	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1

	Application Data	Operation Data / Application Data	AS-DA-03	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1

				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	0
				Resource Exhaustion	TH-21	0
				Isolation/Virtualization Abuse	TH-22	0
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	0
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Firmware and Drivers	Operating System	AS-OS-04	Malware Insertion	TH-01	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	0

				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Unauthorized Access To Premises	TH-24	0
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Display	I/O Devices	AS-HW-05	Device Destruction (Sabotage)	TH-15	0
				Device Loss or Theft	TH-16	1
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1

				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Device Modification	TH-14	0
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack NFC	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface NFC	Network Interfaces	AS-NE-02			
	Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface LTE (4G)	Network Interfaces	AS-NE-02			
	Network Stack 5G	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1

	Network Interface 5G	Network Interfaces	AS-NE-02			
Ticketing System	Web API	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Identity Theft	TH-28	1
				Modification of Information / Data Manipulation	TH-03	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Data	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1

				Modification of Information / Data Manipulation	TH-03	1
	Web Service	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1

	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	1
				Isolation/Virtualization Abuse	TH-22	1
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1

				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1

				Unauthorized Access to Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02			
AVM (Automated Vehicle Monitoring) System / Info-mobility server	Web API	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Identity Theft	TH-28	1
				Management Interface Compromise	TH-23	1

				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Platform Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Data	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1
				Modification of Information / Data Manipulation	TH-03	1
	Web Service	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1

				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1

				Resource Exhaustion	TH-21	1
				Isolation/Virtualization Abuse	TH-22	1
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1

	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1

	Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02			
Subscription System	Web API	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Identity Theft	TH-28	1
				Modification of Information / Data Manipulation	TH-03	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Platform Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Data	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1

	Web Service	Web-Based Services	AS-SO-01	Modification of Information / Data Manipulation	TH-03	1
				Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1

	Native API	Native API	AS-OS-02	Abuse of Authentication	TH-27	1
				Loss/Leakage of Information	TH-26	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	1
				Isolation/Virtualization Abuse	TH-22	1
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1

	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1

				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02			
Smart Display	Native Application	Application Software	AS-SO-02	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
				Modification of Information / Data Manipulation	TH-03	1

				Loss/Leakage of Information	TH-26	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Data	Operation Data / Application Data	AS-DA-03	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Embedded Systems Firmware	AS-OS-01	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	1
				Malicious Insider	TH-35	1

	OS Services	Embedded Systems Firmware	AS-OS-01	Isolation/Virtualization Abuse	TH-22	0
				Failure of System	TH-09	1
				Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	0
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
			AS-HW-04	Device Modification	TH-14	1

	Computational Device	Computational Device		Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Display	I/O Devices	AS-HW-04	Device Destruction (Sabotage)	TH-15	1
				Device Loss or Theft	TH-16	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1

				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack GSM (2G)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface GSM (2G)	Network Interfaces	AS-NE-02			
LTE (4G)	–	Communication Protocol	AS-NE-01			
5G	–	Communication Protocol	AS-NE-01	Man in the Middle	TH-04	1
				Interception of Information	TH-05	1
				Replay of Messages	TH-06	1
				Loss of Support Services	TH-10	1
				Phishing Attacks	TH-19	1
				Network Outage	TH-07	1
				Network Spoofing	TH-20	1
				Denial of Service	TH-02	1
Wired (TCP/IP)	–	Communication Protocol	AS-NE-01	Man in the Middle	TH-04	1
				Interception of Information	TH-05	1
				Replay of Messages	TH-06	1
				Phishing Attacks	TH-19	1
				Malicious Insider	TH-35	1

				Network Outage	TH-07	1
				Network Spoofing	TH-20	1
				Denial of Service	TH-02	1
NFC	–	Communication Protocol	AS-NE-01			
GSM (2G)	–	Communication Protocol	AS-NE-01	Man in the Middle	TH-04	1
				Interception of Information	TH-05	1
				Replay of Messages	TH-06	1
				Malicious Insider	TH-35	1
				Phishing Attacks	TH-19	1
				Loss of Support Services	TH-10	1
				Network Outage	TH-07	1
				Network Spoofing	TH-20	1
				Denial of Service	TH-02	1

Table 12: Threats of Genoa Use Case's Composite Assets

Composite Name	Asset	Basic Asset Name	Basic Asset Type	Asset ID	Threat	Threat ID	Likelihood
Tram or Bus or Trolleybus		Native Application	Application Software	AS-SO-02	Denial of Service	TH-02	1
					Software Exploitation / Malicious Code Injection	TH-11	1

				Abuse of Authentication	TH-27	1
				Modification of Information / Data Manipulation	TH-03	1
				Loss/Leakage of Information	TH-26	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Data	Operation Data / Application Data	AS-DA-03	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1

				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	0
				Isolation/Virtualization Abuse	TH-22	0
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	0
				Resource Exhaustion	TH-21	1

				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	HSM Interface	Operating System	AS-OS-04	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
	Firmware and Drivers	Operating System	AS-OS-04	Malware Insertion	TH-01	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Unauthorized Access to Premises	TH-24	0
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	0

	Computational Device	Computational Device	AS-HW-03	Failures of Devices	TH-08	1
				Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Data Leakage Resulting From Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	0
	HMI	I/O Devices	AS-HW-05	Failures of Devices	TH-08	1
				Device Destruction (Sabotage)	TH-15	0
				Data Leakage Resulting From Device Loss or Theft	TH-16	1
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	Sensors/Actuators	Sensors/Actuators Hardware	AS-HW-01	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0

				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Device Modification	TH-14	0
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	HSM	Computational Device	AS-HW-03	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0

				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack ITS-G5	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface ITS-G5	Network Interfaces	AS-NE-02			
	Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface LTE (4G)	Network Interfaces	AS-NE-02			
	Network Stack 5G	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
Roadside Unit (RSU)	Native Application	Application Software	AS-SO-02	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1

				Abuse of Authentication	TH-27	1
				Modification of Information / Data Manipulation	TH-03	1
				Loss/Leakage of Information	TH-26	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Data	Operation Data / Application Data	AS-DA-03	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1

				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	0
				Isolation/Virtualization Abuse	TH-22	0
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	0
				Resource Exhaustion	TH-21	1

				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	HSM Interface	Operating System	AS-OS-04	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
	Firmware and Drivers	Operating System	AS-OS-04	Malware Insertion	TH-01	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Unauthorized Access To Premises	TH-24	0
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	0

	Computational Device	Computational Device	AS-HW-03	Failures of Devices	TH-08	1
				Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Camera	Sensors/Actuators Hardware	AS-HW-01	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Sensors/Actuators	Sensors/Actuators Hardware	AS-HW-01	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0

				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Smartphones Device	TH-18	1
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Device Modification	TH-14	0
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	HSM	Computational Device	AS-HW-03	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0

				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack ITS-G5	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface ITS-G5	Network Interfaces	AS-NE-02			
	Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface LTE (4G)	Network Interfaces	AS-NE-02			
	Network Stack 5G	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface 5G	Network Interfaces	AS-NE-02			
Payment Service System / Autonomous Vehicle (AV) Logging System	Web API	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1

				Modification of Information / Data Manipulation	TH-03	1
				Management Interface Compromise	TH-23	1
				Identity Theft	TH-28	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Data	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1
				Modification of Information / Data Manipulation	TH-03	1
	Web Service	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1

				Loss/Leakage of Information	TH-26	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1

				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	1
				Isolation/Virtualization Abuse	TH-22	1
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1

				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1

				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02			
Communications Platform-as-a-Service (CPaaS)	Web API	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1

				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Data	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1
				Modification of Information / Data Manipulation	TH-03	1
	Web Service	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1

				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1

	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	1
				Isolation/Virtualization Abuse	TH-22	1
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	VM Management Interface	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Identity Theft	TH-28	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1

	Hypervisor	Operating System	AS-OS-04	Abuse of Authorisation / Privilege Escalation	TH-25	1
				Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1
				Malware Insertion	TH-01	1
				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Isolation/Virtualization Abuse	TH-22	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface		Device Modification	TH-14	1

			AS-HW-04	Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Device	TH-18	1
				Unauthorized Access To Premises	TH-24	1

				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1
				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02			
Autonomous Vehicle (AV) Shuttle Remote Operator	Web API	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Identity Theft	TH-28	1
				Modification of Information / Data Manipulation	TH-03	1
				Management Interface Compromise	TH-23	1

				Abuse of Authentication	TH-27	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Data	Operation Data / Application Data	AS-DA-03	Loss/Leakage of Information	TH-26	1
				Unintentional Disclosure of Data	TH-17	1
				Modification of Information / Data Manipulation	TH-03	1
	Web Service	Web-Based Services	AS-SO-01	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Loss/Leakage of Information	TH-26	1
				Management Interface Compromise	TH-23	1
				Abuse of Authentication	TH-27	1

				Abuse of Authorisation / Privilege Escalation	TH-25	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System		Malware Insertion	TH-01	1

			AS-OS-04	Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	1
				Isolation/Virtualization Abuse	TH-22	1
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	1
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1

				Unauthorized Access To Premises	TH-24	1
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	1
				Natural Disaster	TH-12	1
				Environmental Disaster	TH-13	1
				Device Loss or Theft	TH-16	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Smartphones Device	TH-18	1
				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	1
				Device Modification	TH-14	1

				Environmental Disaster	TH-13	1
				Natural Disaster	TH-12	1
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02			
Autonomous Vehicle (AV) Shuttle	Native Application	Application Software	AS-SO-02	Denial of Service	TH-02	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
				Modification of Information / Data Manipulation	TH-03	1
				Loss/Leakage of Information	TH-26	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1

	Application Data	Operation Data / Application Data	AS-DA-03	Modification of Information / Data Manipulation	TH-03	1
				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Keys	Operation Data / Application Data	AS-DA-03	Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	Application Database	Database Management Systems	AS-SO-03	Loss/Leakage of Information	TH-26	1
				Modification of Information / Data Manipulation	TH-03	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Unintentional Disclosure of Data	TH-17	1
				Abuse of Authentication	TH-27	1
	Native API	Native API	AS-OS-02	Loss/Leakage of Information	TH-26	1

				Abuse of Authentication	TH-27	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
	OS	Operating System	AS-OS-04	Malware Insertion	TH-01	1
				Abuse of Authorisation / Privilege Escalation	TH-25	1
				Resource Exhaustion	TH-21	0
				Isolation/Virtualization Abuse	TH-22	0
				Failure of System	TH-09	1
	OS Services	Operating System	AS-OS-04	Denial of Service	TH-02	0
				Resource Exhaustion	TH-21	1
				Software Exploitation / Malicious Code Injection	TH-11	1
				Abuse of Authentication	TH-27	1
	OS Data	System Data	AS-DA-04	Modification of Information / Data Manipulation	TH-03	1

				Unintentional Disclosure of Data	TH-17	1
				Loss/Leakage of Information	TH-26	1
	HSM Interface	Operating System	AS-OS-04	Loss/Leakage of Information	TH-26	1
				Abuse of Authentication	TH-27	1
	Firmware and Drivers	Operating System	AS-OS-04	Malware Insertion	TH-01	1
	H/W Interface	HW Interface	AS-HW-04	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Unauthorized Access To Premises	TH-24	0
				Device Loss or Theft	TH-16	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Computational Device	Computational Device	AS-HW-03	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0

				Unauthorized Access To Premises	TH-24	1
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	HMI	I/O Devices	AS-HW-05	Device Destruction (Sabotage)	TH-15	0
				Device Loss or Theft	TH-16	1
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	Camera	Sensors/Actuators Hardware	AS-HW-01	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Sensors/Actuators	Sensors/Actuators Hardware	AS-HW-01	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0

				Device Loss or Theft	TH-16	0
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Storage	Storage	AS-HW-06	Device Loss or Theft	TH-16	1
				Attacks on Decommissioned Smartphones Device	TH-18	1
				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Device Modification	TH-14	0
				Environmental Disaster	TH-13	0
				Natural Disaster	TH-12	0
				Failures of Devices	TH-08	1
	HSM	Computational Device	AS-HW-03	Device Modification	TH-14	0
				Natural Disaster	TH-12	0
				Environmental Disaster	TH-13	0
				Device Loss or Theft	TH-16	0

				Unauthorized Access To Premises	TH-24	0
				Device Destruction (Sabotage)	TH-15	0
				Failures of Devices	TH-08	1
	Network Controller	Network Controller (HW)	AS-NE-03	Failures of Devices	TH-08	1
	Network Stack ITS-G5	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface ITS-G5	Network Interfaces	AS-NE-02			
	Network Stack LTE (4G)	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface LTE (4G)	Network Interfaces	AS-NE-02			
	Network Stack 5G	Network Stack (SW)	AS-NE-04	Software Exploitation / Malicious Code Injection	TH-11	1
	Network Interface 5G	Network Interfaces	AS-NE-02			
LTE (4G)	–	Communication Protocol	AS-NE-01			
5G	–	Communication Protocol	AS-NE-01	Man in the Middle	TH-04	1
				Interception of Information	TH-05	1

				Replay of Messages	TH-06	1
				Network Outage	TH-07	1
				Network Spoofing	TH-20	1
				Phishing Attacks	TH-19	1
				Loss of Support Services	TH-10	1
				Denial of Service	TH-02	1
Wired (TCP/IP)	–	Communication Protocol	AS-NE-01	Man in the Middle	TH-04	1
				Interception of Information	TH-05	1
				Replay of Messages	TH-06	1
				Malicious Insider	TH-35	1
				Phishing Attacks	TH-19	1
				Network Outage	TH-07	1
				Network Spoofing	TH-20	1
				Denial of Service	TH-02	1
NFC	–	Communication Protocol	AS-NE-01			
ITS-G5	–	Communication Protocol	AS-NE-01	Man in the Middle	TH-04	1
				Interception of Information	TH-05	1
				Replay of Messages	TH-06	1
				Phishing Attacks	TH-19	1
				Malicious Insider	TH-35	1

				Loss of Support Services	TH-10	1
				Network Outage	TH-07	1
				Network Spoofing	TH-20	1
				Denial of Service	TH-02	1

Table 13: Threats of Tallinn Use Case's Composite Assets

5. VULNERABILITIES

5.1 List of generic vulnerabilities

For the sake of completeness, this section provides several identified high-level vulnerabilities used in the risk analysis of the Genoa and Tallinn use cases. Table 14 includes vulnerabilities that apply to Genoa and Tallinn composite assets obtained from the vulnerability repository (CASES, MOSP, 2021) of MONARC (CASES, MONARC Method Guide, 2020) risk analysis methodology. Their static and generic nature does not allow us to conduct dynamic risk analysis over CitySCAPE architectures. Therefore, the proposed adaptive and dynamic risk analysis methodology that will be used in the assessment of the CitySCAPE architectures will include CVEs, as further described in Section 7.

Vulnerability ID	Vulnerability
VU-CO-01	Access point allowing unlawful eavesdropping
VU-CO-02	Additional software can be added for storing, transmitting or corrupting information (e.g., keylogger)
VU-CO-03	Ageing of the equipment
VU-CO-04	Ageing of the medium
VU-CO-05	Communication in broadcast mode
VU-CO-06	Equipment accessible to unauthorised persons
VU-CO-07	Equipment sensitive to electrical disturbances (voltage drops, overvoltage, transient power-cuts)
VU-CO-08	Equipment that is complex to use or not user-friendly
VU-CO-09	Fragility of equipment
VU-CO-10	Incorrect operating conditions
VU-CO-11	Incorrect sizing (e.g. too much data for the maximum passband)
VU-CO-12	Interface side effects (compatibility problems between protocols, etc.)
VU-CO-13	Interface with a function that allows eavesdropping
VU-CO-14	Maintenance fault
VU-CO-15	Media accessible to unauthorised persons
VU-CO-16	Medium and supports whose characteristics allow eavesdropping (e.g. Ethernet, wireless communication systems)
VU-CO-17	No accessible user support

VU-CO-18	No authentication of equipment connected to the network
VU-CO-19	No physical protection
VU-CO-20	No robust access control system
VU-CO-21	Obsolete hardware
VU-CO-22	Physical access to communication support or equipment allowing eavesdropping equipment to be installed
VU-CO-23	Physical or logical access to a relay allowing eavesdropping equipment to be installed
VU-CO-24	Poor equipment reliability
VU-CO-25	Poor management of pilot releases and configurations
VU-CO-26	Poor medium reliability
VU-CO-27	Possibility of adding software derivations
VU-CO-28	Possibility of circuit derivation
VU-CO-29	Possibility of corrupting a communication
VU-CO-30	Possibility of incorrect configuration, installation or modification of relays
VU-CO-31	Possibility of interfering with data transmitted via the communication media
VU-CO-32	Possibility of remote administration of the system using non-encrypted administration tools
VU-CO-33	Possibility of remote system administration
VU-CO-34	Possibility of remote system administration from any station
VU-CO-35	Possibility of subjecting the relays to an excessive number of requests or intense interference (e.g. denial of service attacks such as smurfing, SYN flood etc.)
VU-CO-36	Presence of a communication network with the outside allowing exchange of information
VU-CO-37	Presence of protocol that has no authentication function
VU-CO-38	Protocol not allowing safe authentication of the sender of a communication
VU-CO-39	The equipment can be accessed by everyone
VU-CO-40	The interfaces can be accessed by everyone
VU-CO-41	The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)
VU-CO-42	Users lack competency

VU-OS-01	The operating system allows a session to be opened without password
VU-OS-02	The operating system is not checked before installation
VU-OS-03	Resource sharing makes it easy for unauthorised persons to use the system
VU-OS-04	Use of a standard operating system on which logical attacks have already been carried out
VU-OS-05	Connection passwords not sufficiently complex
VU-OS-06	Possibility of creating or modifying system commands
VU-SO-01	Software that is complex to use
VU-SO-02	Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)
VU-SO-03	Use of an obsolete version of the operating system or applications
VU-SO-04	Single internally-developed applications
VU-SO-05	No encryption system
VU-SO-06	Software can be used by everyone (e.g., no password required for remote administration of a workstation)
VU-SO-07	No restriction on software entry points
VU-SO-08	No implementation of basic security rules applicable to the operating system and software
VU-SO-09	Use of non-evaluated software
VU-SO-10	No protection against the use of advanced privileges
VU-SO-11	Possibility of modifying or corrupting the software
VU-SO-12	No sure means of identification
VU-SO-13	No procedure or system for authorising personnel to modify data
VU-SO-14	No monitoring of data integrity
VU-SO-15	No management of profile privileges (administrators, users, guest, etc.)
VU-SO-16	Possibility of installing a backdoor or Trojan horse in the operating system
VU-SO-17	Non-upgradable software
VU-SO-18	Obsolete software
VU-SO-19	Applications are not checked before installation
VU-SO-20	Possibility of incorrect configuration, installation or modification of the operating system
VU-SO-21	No systematic qualification procedure before installation or updating

VU-SO-22	Lack of training in maintaining and operating new equipment
VU-SO-23	Possible side effects after updating a software component
VU-SO-24	Application requiring computing resources not matched by the equipment (e.g. insufficient RAM)
VU-SO-25	No filter to protect the system against saturation
VU-SO-26	Possible existence of hidden functions introduced during the design and development phase
VU-SO-27	Software retrieval from a non-authenticated source
VU-SO-28	Presence of residual data used by the software
VU-SO-29	Possibility of adding an eavesdropping programme such as a Trojan horse
VU-SO-30	Password for accessing the system or application changed rarely or not at all
VU-SO-31	Use of easily-observed passwords to access the system or application (shape on keyboard, short password)

Table 14: List of High-Level Vulnerabilities

5.2 Association between Threats and Vulnerabilities.

This section correlates the identified threats from the CitySCAPE D2.4 and the identified high-level vulnerabilities from the previous section in Table 15.

Vulnerability ID	Vulnerability	Threat ID	Threat
VU-CO-01	Access point allowing unlawful eavesdropping	TH-04	Man in the Middle
		TH-05	Interception of Information
VU-CO-02	Additional software can be added for storing, transmitting or corrupting information (e.g. keylogger)	TH-01	Malware Injection
VU-CO-03	Ageing of the equipment	TH-08	Failures of Devices
VU-CO-04	Ageing of the medium	TH-08	Failures of Devices
VU-CO-05	Communication in broadcast mode	TH-05	Interception of Information
		TH-04	Man in the Middle

		TH-06	Replay of Messages
VU-CO-06	Equipment accessible to unauthorised persons	TH-15	Device Destruction (Sabotage)
		TH-14	Device Modification
VU-CO-07	Equipment sensitive to electrical disturbances (voltage drops, overvoltage, transient power-cuts)	TH-07	Network Outage
VU-CO-08	Equipment that is complex to use or not user-friendly	TH-09	Failure of System
VU-CO-19	Fragility of equipment	TH-08	Failures of Devices
		TH-15	Device Destruction (Sabotage)
VU-CO-10	Incorrect operating conditions	TH-08	Failures of Devices
VU-CO-11	Incorrect sizing (e.g., too much data for the maximum passband)	TH-02	Denial of Service
VU-CO-12	Interface side effects (compatibility problems between protocols, etc.)	TH-09	Failure of System
VU-CO-13	Interface with a function that allows eavesdropping	TH-05	Interception of Information
VU-CO-14	Maintenance fault	TH-09	Failure of System
VU-CO-15	Media accessible to unauthorised persons	TH-15	Device Destruction (Sabotage)
VU-CO-16	Medium and supports whose characteristics allow eavesdropping (e.g. Ethernet, wireless communication systems)	TH-20	Network Spoofing
VU-CO-17	No accessible user support	TH-09	Failure of System
VU-CO-18	No authentication of equipment connected to the network	TH-05	Interception of Information
VU-CO-19	No physical protection	TH-15	Device Destruction (Sabotage)
VU-CO-20	No robust access control system	TH-27	Abuse of Authentication
		TH-26	Loss/Leakage of Information

		TH-28	Identity Theft
VU-CO-21	Obsolete hardware	TH-08	Failures of Devices
VU-CO-22	Physical access to communication support or equipment allowing eavesdropping equipment to be installed	TH-05	Interception of Information
VU-CO-23	Physical or logical access to a relay allowing eavesdropping equipment to be installed	TH-05	Interception of Information
VU-CO-24	Poor equipment reliability	TH-09	Failure of System
VU-CO-25	Poor management of pilot releases and configurations	TH-09	Failure of System
VU-CO-26	Poor medium reliability	TH-09	Failure of System
VU-CO-27	Possibility of adding software derivations	TH-11	Software Exploitation / Malicious Code Injection
VU-CO-28	Possibility of circuit derivation	TH-02	Denial of Service
		TH-08	Failures of Devices
VU-CO-39	Possibility of corrupting a communication	TH-04	Man in the Middle
VU-CO-30	Possibility of incorrect configuration, installation or modification of relays	TH-09	Failure of System
VU-CO-31	Possibility of interfering with data transmitted via the communication media	TH-04	Man in the Middle
VU-CO-32	Possibility of remote administration of the system using non-encrypted administration tools	TH-23	Management Interface Compromise
		TH-26	Loss/Leakage of Information
VU-CO-33	Possibility of remote system administration	TH-23	Management Interface Compromise
VU-CO-34	Possibility of remote system	TH-23	Management Interface Compromise

	administration from any station		
VU-CO-35	Possibility of subjecting the relays to an excessive number of requests or intense interference (e.g. denial of service attacks such as smurfing, SYN flood etc.)	TH-02	Denial of Service
VU-CO-36	Presence of a communication network with the outside allowing exchange of information	TH-26	Loss/Leakage of Information
VU-CO-37	Presence of protocol that has no authentication function	TH-27	Abuse of Authentication
VU-CO-38	Protocol not allowing safe authentication of the sender of a communication	TH-27	Abuse of Authentication
VU-CO-39	The equipment can be accessed by everyone	TH-15	Device Destruction (Sabotage)
VU-CO-40	The interfaces can be accessed by everyone	TH-26	Loss/Leakage of Information
VU-CO-41	The relays identify neither the sources nor the destinations (example of impact: system vulnerable to spoofing attacks)	TH-20	Network Spoofing
VU-CO-42	Users lack competency	TH-09	Failure of System
VU-SO-01	Software that is complex to use	TH-09	Failure of System
VU-SO-02	Possibility of the operating system being subjected to badly formed requests and data (e.g. buffer overflow)	TH-11	Software Exploitation / Malicious Code Injection
		TH-25	Abuse of Authorisation / Privilege Escalation
		TH-22	Isolation/Virtualization Abuse

VU-SO-03	Use of an obsolete version of the operating system or applications	TH-25	Abuse of Authorisation / Privilege Escalation
		TH-22	Isolation/Virtualization Abuse
		TH-11	Software Exploitation / Malicious Code Injection
VU-SO-04	Single internally-developed applications	TH-09	Failure of System
VU-SO-05	No encryption system	TH-03	Modification of Information / Data Manipulation
		TH-04	Man in the Middle
		TH-26	Loss/Leakage of Information
VU-SO-06	Software can be used by everyone (e.g. no password required for remote administration of a workstation)	TH-28	Identity Theft
		TH-23	Management Interface Compromise
		TH-26	Loss/Leakage of Information
		TH-27	Abuse of Authentication
VU-SO-07	No restriction on software entry points		
VU-SO-08	No implementation of basic security rules applicable to the operating system and software	TH-11	Software Exploitation / Malicious Code Injection
		TH-25	Abuse of Authorisation / Privilege Escalation
VU-SO-09	Use of non-evaluated software	TH-09	Failure of System
VU-SO-10	No protection against the use of advanced privileges	TH-25	Abuse of Authorisation / Privilege Escalation
VU-SO-11	Possibility of modifying or corrupting the software	TH-11	Software Exploitation / Malicious Code Injection
		TH-25	Abuse of Authorisation / Privilege Escalation
VU-SO-12	No sure means of identification	TH-27	Abuse of Authentication
VU-SO-13	No procedure or system for authorising personnel to modify data	TH-03	Modification of Information / Data Manipulation
VU-SO-14	No monitoring of data integrity	TH-03	Modification of Information / Data Manipulation

VU-SO-15	No management of profile privileges (administrators, users, guest, etc.)	TH-25	Abuse of Authorisation / Privilege Escalation
VU-SO-16	Possibility of installing a backdoor or Trojan horse in the operating system	TH-01	Malware Injection
VU-SO-17	Non-upgradable software	TH-11	Software Exploitation / Malicious Code Injection
VU-SO-18	Obsolete software	TH-11	Software Exploitation / Malicious Code Injection
		TH-25	Abuse of Authorisation / Privilege Escalation
VU-SO-19	Applications are not checked before installation	TH-11	Software Exploitation / Malicious Code Injection
VU-SO-20	Possibility of incorrect configuration, installation or modification of the operating system	TH-09	Failure of System
VU-SO-21	No systematic qualification procedure before installation or updating	TH-09	Failure of System
VU-SO-22	Lack of training in maintaining and operating new equipment	TH-09	Failure of System
VU-SO-23	Possible side effects after updating a software component	TH-09	Failure of System
VU-SO-24	Application requiring computing resources not matched by the equipment (e.g. insufficient RAM)	TH-21	Resource Exhaustion/Lack of resources
		TH-02	Denial of Service
VU-SO-25	No filter to protect the system against saturation	TH-21	Resource Exhaustion/Lack of resources
VU-SO-26	Possible existence of hidden functions introduced during the design and development phase	TH-11	Software Exploitation / Malicious Code Injection
VU-SO-27	Software retrieval from a non-authenticated source	TH-01	Malware Injection

VU-SO-28	Presence of residual data used by the software	TH-26	Loss/Leakage of Information
VU-SO-29	Possibility of adding an eavesdropping programme such as a Trojan horse	TH-01	Malware Injection
VU-SO-30	Password for accessing the system or application changed rarely or not at all	TH-28	Identity Theft
VU-SO-31	Use of easily-observed passwords to access the system or application (shape on keyboard, short password)	TH-28	Identity Theft
VU-OS-32	The operating system allows a session to be opened without password	TH-26	Loss/Leakage of Information
		TH-27	Abuse of Authentication
VU-OS-33	The operating system is not checked before installation	TH-09	Failure of System
VU-OS-34	Resource sharing makes it easy for unauthorised persons to use the system	TH-25	Abuse of Authorisation / Privilege Escalation
VU-OS-35	Use of a standard operating system on which logical attacks have already been carried out	TH-11	Software Exploitation / Malicious Code Injection
		TH-25	Abuse of Authorisation / Privilege Escalation
VU-OS-36	Connection passwords not sufficiently complex	TH-28	Identity Theft
VU-OS-37	Possibility of creating or modifying system commands	TH-11	Software Exploitation / Malicious Code Injection

Table 15: Association Among High-Level Vulnerabilities and Identified Threats of CitySCAPE Use Cases

6. MODELING CASCADING RISKS AND THREATS WITH FAULT-TREES

Fault tree analysis (Marvin Rausand, 2004) is a deductive technique, used in system reliability theory and models, where we start with a specified critical event (system failure or an accident), and create a logic diagram that displays the interconnection

and interdependencies between a critical event in a system and the causes for this event.

In this section, a modelling approach is presented that customizes the fault trees used in functional analysis and failure modelling in order to propose a technique to present the interrelationships between threats, vulnerabilities, security controls and impact/requirements, as well as to model the cascading threats between systems or system assets. The specific approach was named “hierarchical modified fault trees for threat analysis” (mFTTA).

6.1 Definition of terms in the modified fault trees for threat analysis

Top Event:

In conventional fault tree analysis, the top event expresses the failure under investigation. In mFTTA, the top event expresses *the impact of an implemented risk*, or else, the *failure to satisfy a security requirement*. At the following, the top even in the mFTTA will be referred as the “impact”.

Assuming that we attempt to model a system containing multiple components, an mFTTA instance expresses the impacts for a specific component in the system. According to the conceptual model presented in Sec. 2, various levels of detail/granularity can be defined. More specifically:

- An ecosystem may be comprised of various entities (L1).
- An entity may be comprised of various assets (L2).
- An asset may be comprised of various assets (L3).

Therefore, by taking as reference the L2 level of detail, an mFTTA instance expresses the impacts for a specific asset. The notation $mFTTA(I_x, A_x)$ is used to denote the mFTTA for impact I_x at asset A_x .

Especially interesting for the analysis are the impacts that are identified to be relevant to cascading threats in the methodology presented in D2.4, i.e.:

- Loss of transmitted information/data (I_1)
- Loss of stored information/data (I_2)
- Disclosure of transmitted information/data (I_3)
- Disclosure of stored information/data (I_4)
- Modification of transmitted information (I_5)
- Modification of stored information/data (I_6)
- Interruption of service (I_7)

The specific impacts (leading to cascading risks) are used to link mFTTAs from different assets or systems. This means that these impacts may be related with transfer blocks that are used to interconnect different mFTTAs, thus modelling cascading effects (transfer blocks are defined in the following paragraphs).

Logical Gates

The relationship between input events and output represented in the leaf nodes of the mFTTA are expressed with the use of Boolean gates. More specifically,

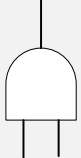

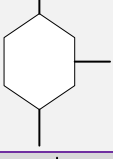
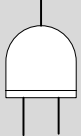

Symbol	Description
	AND gate - the output occurs only if all inputs occur.
	OR gate - the output occurs if any input occurs
	Inhibit gate - the output occurs if the input occurs under an enabling condition specified by a conditioning event.
	Priority AND gate - the output occurs if the inputs occur in a specific sequence specified by a conditioning event.
	NOT gate – the output occurs when the input does not occur.

Table 16: Logical gates used in mFTTAs.

It is noted that, in contrast with conventional fault trees, in mFTTAs:

- Exclusive OR gates are not used since no applicability for the specific gate was found in the use cases.
- NOT gates are used, despite the fact that they are not used in conventional fault trees. This is due to the fact that the lack of an event cannot be linked to a failure. However, NOT gates have applicability in mFTTAs, in order to include the effect of a security control in avoiding the implementation of a threat on an asset.

Basic Events

The fault trees are a top-down method aiming at analysing the effects to a set of basic causes. These events at the lowest level of the fault tree are called *basic events*. The notation for the basic event is a circle.

The basic events in the mFTTA are:

- *Primary threats*, as defined in D2.4, that are threats that they are standalone and may appear without requiring any conditions (prerequisites) to have been met. The primary threats are usually materialized by an attack. Currently, attacks are not included in the mFTTAs explicitly.

- *Security controls*, i.e., countermeasures that can be used to cover existing system vulnerabilities. To be more specific, the absence of a security control is practically considered a basic event that may have sequences combined with a materialization of a threat.

An example can be seen in Figure 10. In the specific example, it is shown that the existence of the threat “Man-in-the-Middle eavesdropping” can be materialized and have consequences in the absence of an effective encryption algorithm.

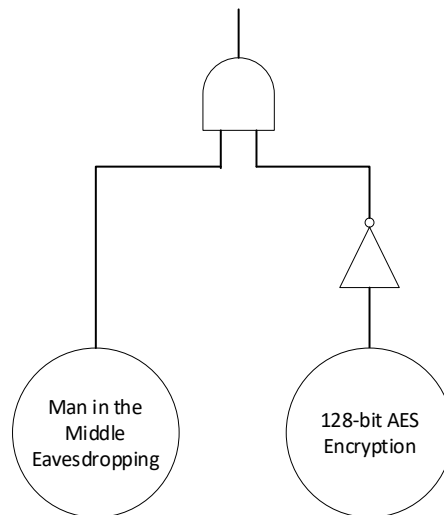


Figure 10: Example of the use of basic events in the mFTTA

Intermediate Events

In fault trees, an intermediate event is an event triggered by an event or combination of events from the lower levels of the fault tree.

In the case of the mFTTAs, the intermediate event may be:

- A vulnerability that may be exploited by a threat.
- A secondary threat, or a cascading threat. However, at this point the term cascading threat is used to describe a secondary threat materialized at the same asset as a consequence of a primary threat.

As an example, the threat “Malicious code injection” can allow the materialization of another threat, e.g., “Compromise of management interface”.

Intermediate events are denoted with rectangular blocks.

Conditional Events

In fault trees, conditions may be defined to restrict or affect logic gates. Moreover, the conditional events are related with the inhibit gates.

In mFTTAs, conditional events may be used in a different context to include in the analysis security controls that do not have 100% effectiveness. Unlike the example depicted in Figure 10, countermeasures against availability attacks or misbehaviour detection controls do not have 100%. Therefore, system disturbance may be possible even when security controls exist. An example is depicted in

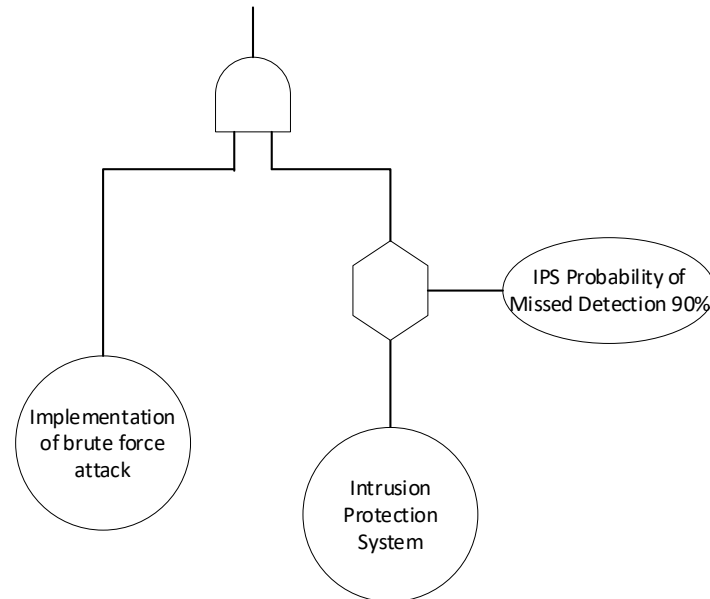


Figure 11: Example of the use of conditional events in the mFTTA

Transfer Blocks

Based on the aforementioned analysis and the methodology in D2.4, a set of impacts may act as a cascading threat that can exploit a vulnerability of a different asset. For example, the “disclosure of transmitted information” for an asset, is transferred as “disclosure of stored information” for a different asset, as long as the two assets are communicating with each other. The use of transfer blocks in mFTTA is depicted in Figure 12.

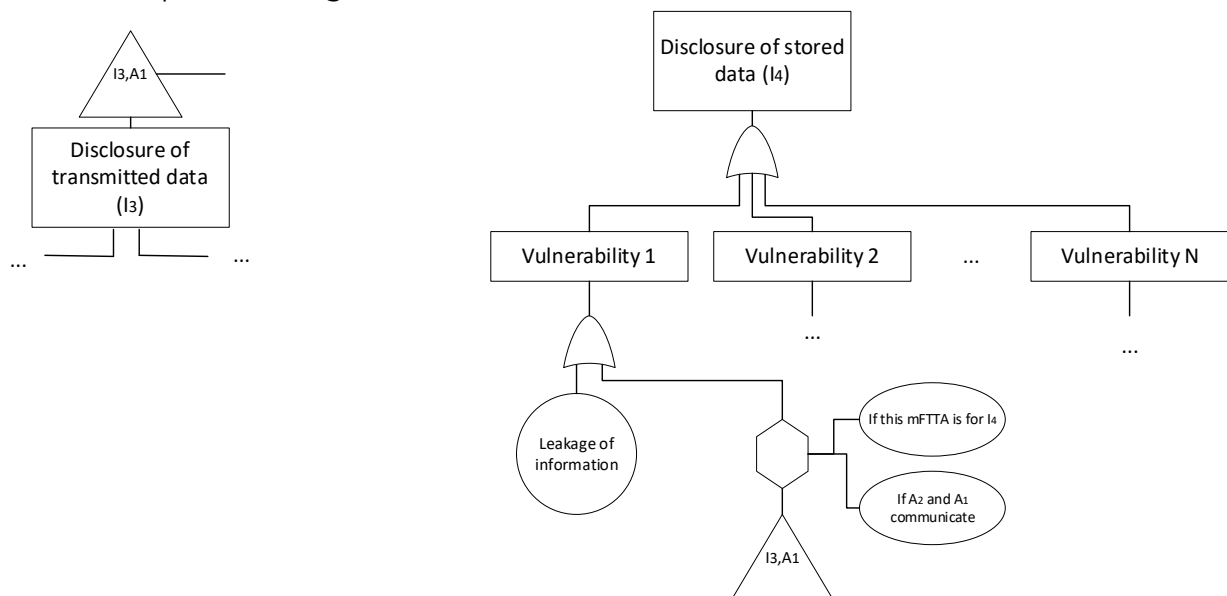


Figure 12: Example on the use of transfer blocks in mFTTAs

Based on the example, if the risk for asset A_1 that has the impact I_3 materializes, then the impact cascades as a threat – with identical consequences as the Leakage of Information threat to asset A_2 ,

- If A_1 and A_2 are connected. The connection between assets is indicated by the system architecture, i.e., schematics like Figure 4, Figure 5 in Sec. 3.3, or Tables 16 and 17 in D2.4, and
- When we form the mFFTA for I_4 impact, since according to Figure 9 in D2.4, I_3 triggers the risk with I_4 as a cascading effect, the transfer-out block is introduced at the lower level of the tree.

6.2 Design principles for the mFFTA

The following steps describe as a top-down approach the formulation of the mFFTAs for risk analysis and cascading threat assessment. It is assumed that, a system composed by several assets is examined (L2 level of detail/granularity).

1. The system is decomposed into assets. Analysis is performed initially per asset. Let's assume that asset A_x is selected.
2. According to the security requirements for A_x , a number of mFTTAs is defined – one for each requirement, or in better words, one for each *failure to fulfill the requirement*. Let's now focus on mFFTA(A_x, I_y), i.e., the modified fault tree for threat analysis that investigates the impact I_y for the asset A_x .
3. If I_y may transform as an event that can trigger a risk on a different asset, then a transfer out block is inserted. In order to identify if I_y causes cascading effects, for the CitySCAPE use cases, Figure 9 in D2.4 is used.
4. The second level in mFFTA is answering to the question “*which vulnerabilities expose to a risk with impact I_y* ”. Therefore, the second level includes vulnerabilities as “intermediate events” denoted with rectangular blocks.
5. Logical gates are used to interconnect the second level with the top. In a common case, a simple OR gate will imply that the exploitation of at least one of the selected vulnerabilities will lead to impact I_y . In case more complicated schemes are required to materialize the specific risk, other logical gates may be used accordingly.
6. The immediately lower level contains secondary threats (if any). As mentioned before, a secondary threat may be collateral consequence of the materialization of a primary threat. The existence of secondary threats is optional and it depends on the characteristics of the investigated asset. More than one layers with secondary threats may exist, if necessary, in order, for example, to model a pile up of three threats back-to-back. It is noted that secondary threats can only be triggered by threats at the same mFFTA.
7. For each of the secondary threats, security controls may be added (with deterministic or conditional performance). The security controls are added either through a NOT gate or through an inhibit gate (and one or more conditions).
8. The lower level contains the primary threats and corresponding security controls. The questions that are practically answered are:
 - Which threats can exploit each of the vulnerabilities at the second level?
 - Which security control is installed to prevent the exploitation of the vulnerability? Which is the effectiveness of the security control?

- Does a threat cascade as a secondary threat for the investigated asset?
9. Threats and security controls are combined through properly selected logical gates and they are eventually connected with the corresponding threats. In general, threats are combined with security controls with AND gates, while threats (and security controls) are connected to the vulnerabilities through OR gates.
 10. If, through inspection of Figure 9 in D2.4 or any equivalent model/table, it is found that I_y may be triggered by the impact of I_z of a risk implemented on a different asset, then a “transfer-in” block is added in the threat level for assets connected with A_x with an inbound connection.

Through the 10-step process, it is possible to create mFTTAs in a systematic way that can be easily implemented in a computer program, as long as the following associations are known:

- Connections between assets.
- Security requirements, or else generic risk impacts per asset.
- Vulnerabilities associated with the specific risk or requirement.
- Threats associated with assets.
- Threats associated with vulnerabilities.
- Interconnection between impacts.
- Interconnection between threats.

In the CitySCAPE platform, the mFTTAs will be programmatically implemented as part of the RITA engine (WP5) to implement the cascading threat model and calculate the risk by taking into account cascading effects. All the required information is already available in this deliverable and D2.4. Thus:

- The system architecture and Tables 16, 17 in D2.4 provide the connection between asset
- Impacts and the interconnection between impacts is provided in Figure 9 of D2.4.
- Vulnerabilities and their association with risks can be extracted by the tables in Sec. 5 combined with the Figure 9 of D2.4.
- Association between Threats and Assets is provided in Sec. 4.
- Association between Threats and Vulnerabilities is provided in Sec. 5.
- Interconnection between assets is provided in Figure 9 of D2.4.

Note 1: If we consider the threat materialization as independent events, the fault trees can be easily used to calculate the overall probability of a failure (or in the case of mFTTAs an impact). If there are dependencies among threat materializations, the mFTTA can be used for approximate calculation of the overall probability of an impact, as long as, the correlation coefficients between events are known.

Note 2: In CitySCAPE, mFTTAs are used as modelling tools that will be utilized for software engineering in the implementation of the Risk Analysis and Impact Assessment (RITA) engine in the course of WP5. Additionally, the fault trees are a

nice visual tool, where an interested researcher can study the cascading process triggered by cyber-security events. However, in the CitySCAPE context, the entities and assets are very complicated, with many requirements, threats, vulnerabilities leading also to very complicated mFFTAs.

Note 3: The specification of countermeasures and security controls was not part of the objectives of the specific Task. Countermeasure proposals will be provided in the course of T5.6 and they will be used/utilized

In Figure 13, an exemplary mFFTA is presented. The example refers to the L1 level of detail and more particularly the “*Loss of Transmitted Information*” impact for a basic asset “*Web Service*” of the composite asset “*Ticketing System*” (from the Genoa use case). However, due to the complexity of the asset, in order to help with the visibility and readability of the mFFTA, the specific example has been simplified with the merging/removal of some threats and/or vulnerabilities.

Moreover, since there is no knowledge of specific countermeasures, two indicative security controls (a deterministic and a conditional) have been inserted for visualization purposes. Finally, the impact “*Loss of Transmitted Information*” according to the methodology of D2.4, may trigger a cascading threat to other assets with impact “*Loss of Stored Information*”

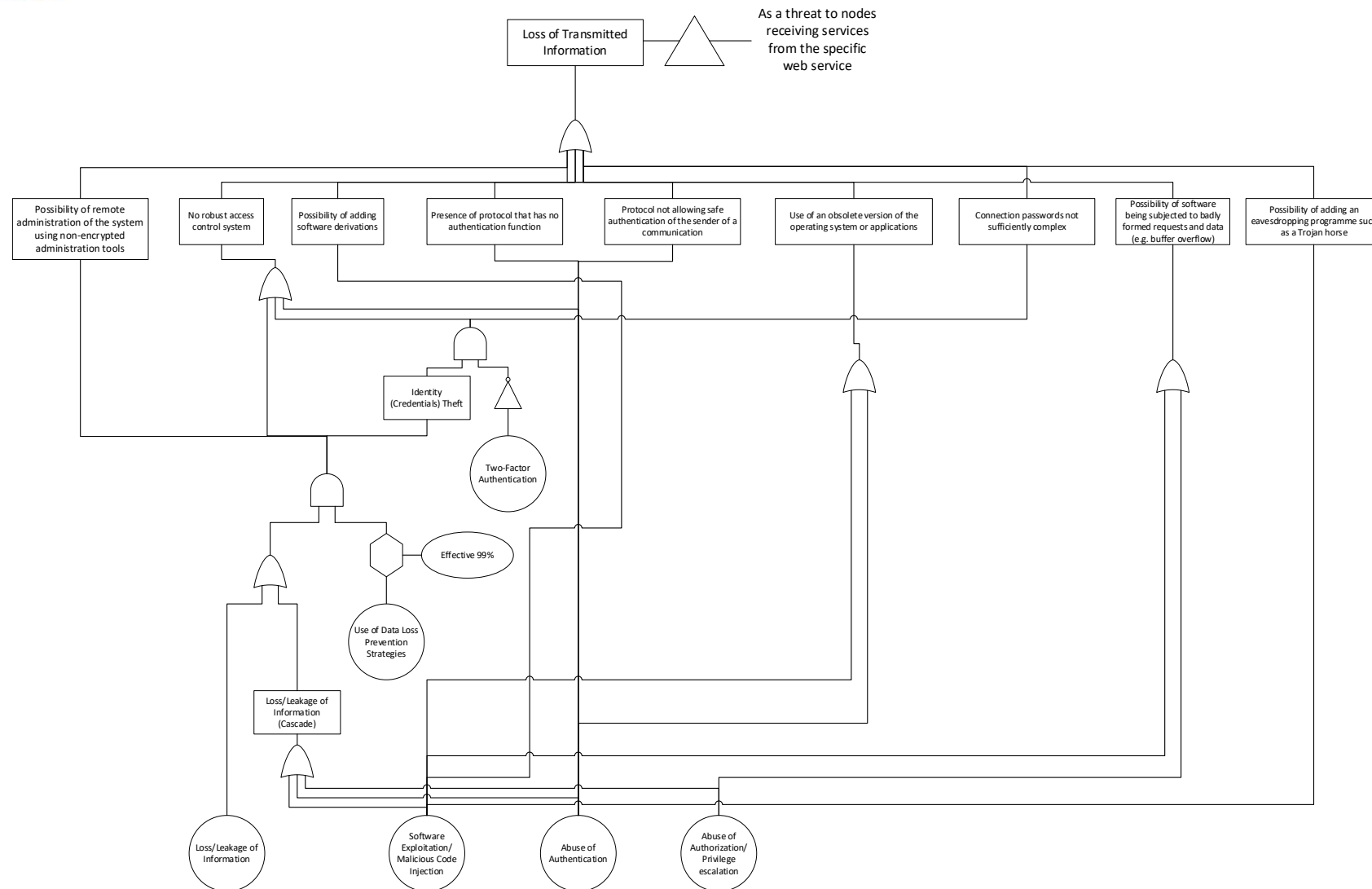


Figure 13: A minimalistic example of an mFTTA for a web service (basic asset of a composite asset e.g., Ticketing System)

7. DYNAMIC RISK ANALYSIS PARADIGM

7.1 Rationale

Conventional Risk Analysis (RA) methodologies suffer from several limitations, primarily because of their static nature. For example, they include static lists of vulnerabilities in their analysis or require constant reassessment (López, Pastor, & L. Villalba, 2013) (Riesco & Villagrà, 2019). To this end, we propose a dynamic, adaptable risk analysis method that automatically assigns new vulnerabilities to the CitySCAPE architecture's assets and automatically evaluates the impact of the successful exploitation of a vulnerability.

7.2 NVD, CVE, CWE, CAPEC and ENISA Threat Relations

Our dynamic risk analysis is based on four data sources, namely the National Institute of Science and Technology's National Vulnerability Database (NIST NVD), MITRE's Common Vulnerability Enumeration (CVE), Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC). Through these sources and the threats, we linked to them, we are able to dynamically link known vulnerabilities to the threats they may pose to our infrastructure. Below is a diagram of the sources we use and how they are interlinked in order to accomplish our dynamic risk analysis.

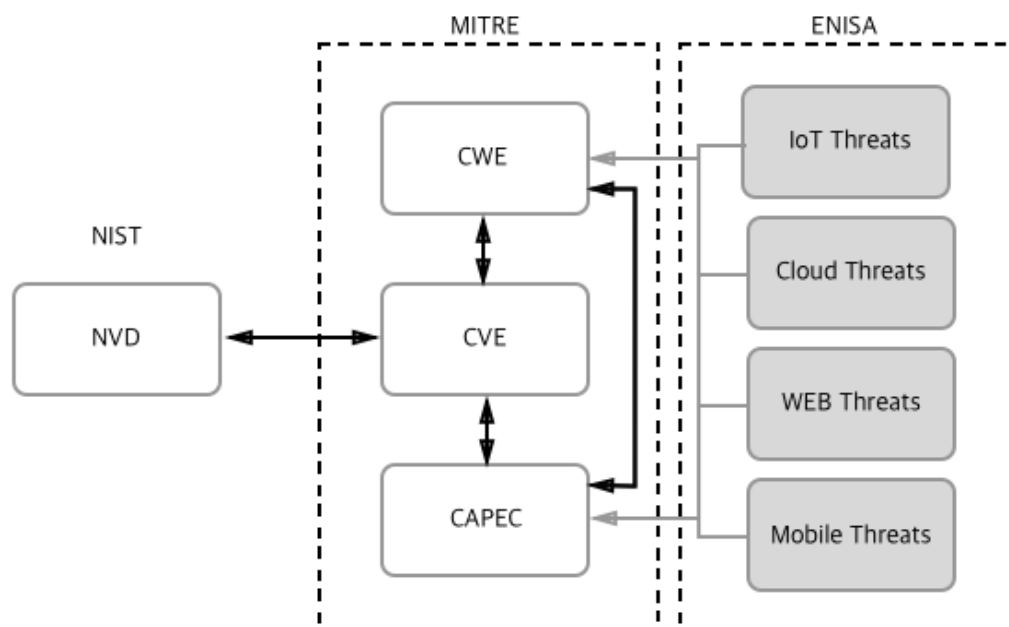


Figure 14: Relation between NVD, CVE, CWE, CAPEC and Threats

Our first source of information is the U.S. National Institute of Standards and Technology, a government agency that focuses on scientific research,

including software and hardware. It also cooperates with the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Defence. Our second source is the MITRE Foundation also known as MITRE a non-profit organization that focuses on research and development and operates several federally funded research and development centres (FFRDCs) including the National Cybersecurity FFRDC and the Homeland Security Systems Engineering and Development Institute (HSSEDI). Finally, our last source of information is the European Union Agency for Cybersecurity (ENISA), a European Union agency that focuses on cybersecurity and performs legislative tasks, promotes EU states cooperation, provides information on new and upcoming technologies, accumulates and shares knowledge on cybersecurity etc. It provided us with documents with which we generated our threat list.

Common Vulnerabilities and Exposures (CVE) is a database of publicly disclosed vulnerabilities, with each vulnerability having its own record. It is maintained by MITRE and funded by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). While copyrighted by MITRE it is done so in the interest of maintaining it free and open for all. CVE contains relatively little information about a vulnerability including the unique identifier, the vulnerability status such as RESERVED or DISPUTED, a short description and references to the vulnerability. CVE entries are created by CVE Numbering Authorities (CNAs), organizations involved in finding and reporting vulnerabilities. They typically include vendors, vulnerability researchers as well as bug bounty programs. CVE also allows for the ability to control the disclosure of a vulnerability in a responsible manner. Each CVE follows a standardized naming scheme containing the CVE prefix, followed by the year the vulnerability was discovered or published, and a unique identifier with 4 or more digits. (CVE, 2021) Its stream of information is the main input source of NISTs National Vulnerability Database.

The National Vulnerability Database (NVD) is a list of vulnerabilities maintained by the U.S. National Bureau of Standards and Technology Computer Security Division, Information Technology Laboratory (ITL), with funding from the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). It is represented using the Security Content Automation Protocol (SCAP). (NIST, 2021) This enables automated vulnerability management and security measurement. Once a vulnerability is published on the CVE list the NVD is tasked with generating further information on the vulnerability. This information includes:

- A Common Weakness Enumeration from within the CWE-1003 view.

- A Common Product Enumerator (CPE), which is what determines the products that are affected by a specific vulnerability.
- Common Vulnerability Scoring System (CVSS) metrics, regarding the severity and impact of the vulnerabilities

NVD also actively maintains and updates the list in order to keep it up to date. (NIST, 2021) The reason that NVD is useful is because it provides us with a framework with which to correlate our assets to potential vulnerabilities, through CPE. Due to the vast number of vulnerabilities a manual correlation between a vulnerability and a threat becomes impractical. CitySCAPE aims to overcome this issue by correlating the limited number of Common Weakness Enumerations that are assigned to vulnerabilities in general.

Common Weakness Enumeration (CWE) is a list of common software and hardware weaknesses supported by the community. It is maintained by MITRE and sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Ever since CVE was released the need for to categorize weaknesses that may lead to vulnerabilities was crucial and in 2006 MITRE launched CWE in order to help standardise weakness categorization, as well as raise awareness of those weaknesses in order to prevent them from occurring in the first place by highlighting their existence and impact. (CWE, 2020)

Common Attack Pattern Enumeration and Classification (CAPEC) is a catalogue that provides users with information on how adversaries exploit weaknesses in applications in order for them to better understand the attacks and consequently be prepared for them. Like CVE and CWE CAPEC is also maintained by MITRE and sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). (CAPEC, 2021) It compliments CWE in helping software and hardware development teams be aware of common potential attack vectors in their products and help to harden them. (CWE, 2020)

CVE records number approximately 160.00 as of September 2021 (CVE, 2021). Because of that, a manual classification of the threats that each vulnerability poses are infeasible. Our goal is to extract the threats of each vulnerability, based on the underlying weaknesses using CWE, or their attack patterns using CAPEC. Our threats were generated based on several ENISA reports, namely: a) Baseline Security Recommendations for IoT (ENISA, 2017), that focuses mainly on IoT on critical infrastructure, b) the ENISA Smartphones: Information security risks, opportunities and recommendations for users report (ENISA, 2010), c) the Cloud Computing Security Risk Assessment (ENISA, 2009), d) the ENISA Threat Landscape For 5G Networks (ENISA, 2020), e) the Smart Grid Threat Landscape and Good Practice Guide (ENISA, 17), f) Port Cybersecurity - Good practices for cybersecurity in the maritime

sector, (ENISA, 2019) and finally the ENISA good practices for security of Smart Cars (ENISA, 2019). Also, another report that supplied us with valuable information during the process of developing our list of threats was the 'Survey of threats and security measures for data transmission over GSM/UMTS networks' (Fisher, Markscheffel, Frosch, & Buettner, 2012). These reports provided us with a good mixture of common threats for various fields including critical infrastructures, as well as threats to new technologies including 5G and IoT.

7.3 Dynamic Operation examples

In this chapter we are going to illustrate how our risk analysis tool applies in conditions where a certain threat (or group of threats) affects one or more of the assets contained in our inventory. In detail, we provide a few operation examples in order to describe:

- how our tool identifies an emerging threat (or group of threats) and correlates it/them with specific targeted assets' weaknesses and
- how the tool generates and appends a numerical score based on the threat's impact to assess its criticality.

7.3.1 Scenario 1: Out-of-bounds vulnerability

A high-value asset of the Genoa's system architecture is an Android phone that hosts the AMT mobile application. In this scenario, we suppose that the mobile phone runs an Android version of either 10 or 11. The mere fact that the phone runs each one of these Android versions is likely to imperil various components of it (AS-OS-02, AS-OS-04, AS-DA-04) to the CVE-2021-0430 vulnerability, as we are given to understand from the CPE information that is linked with the particular CVE and is listed below:

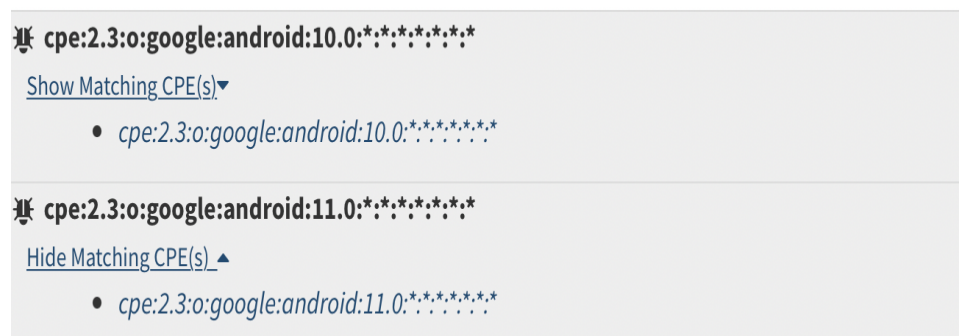


Figure 15: Known affected software configurations for CVE-2021-0430 (NIST, 2021)



According to (NIST, 2021) a missing bound check in this vulnerability may result in an out of bounds write, potentially allowing Remote Code Execution (RCE) at the targeted device by using an appropriately crafted NFC packet. From the information listed in the NVD, we are also informed that the specific vulnerability is associated with the CWE-787 named as 'Out-of-bounds Write'. Given the fact that our tool has stored all the possible relationships between the CVEs and the CWEs, when it receives the specific CVE identifier it automatically matches it to the TH-11 'Software Exploitation-Malicious code injection' threat via the CWE-787 identifier.

7.3.2 Scenario 2: Improper authentication vulnerability

This scenario applies to the HTTP web servers that are used either in Genoa's (e.g., infomobility server) or Tallinn's (e.g., Payment Service System) infrastructure system. In detail, if one or more of the Apache web servers that constitute the aforementioned systems' architecture run an httpd version of 2.2.x prior to 2.2.33 or 2.4.x prior to 2.4.26, potentially exposes the AS-OS-04 (Operating system) of each one of them to the CVE-2017-3167 vulnerability. Considering the provided description for the particular CVE (NIST, 2021), we are notified that a function (i.e. *ap_get_basic_auth_pw()*) which is used by system components that do not belong to the authentication phase is likely to be exploited by malicious users to bypass the authentication mechanism.



 cpe:2.3:a:apache:http_server:*****:* Show Matching CPE(s)▼	From (including) 2.2.0	Up to (excluding) 2.2.33
 cpe:2.3:a:apache:http_server:*****:* Show Matching CPE(s)▼	From (including) 2.4.0	Up to (excluding) 2.4.26

Figure 16: Known affected software configurations for CVE-2017-3167 (NIST, 2021)

From the information listed in the NVD, we are informed that the specific vulnerability is associated with the CWE-287 named as 'Improper authentication' (CWE, 2021). Thus, in this case, when our tool receives the specific CVE identifier, it automatically matches it to both the TH-02 'Denial of Service' and the TH-21 'Software Exploitation-Malicious code injection' threat via the CWE-287 identifier.

7.3.3 Scenario 2: Use-after-free vulnerability

This scenario affects the proper functionality of the system components that make use of web services in both the Genoa's and Tallinn's system architecture. In particular, if a web service (AS-SO-01) runs an Ubuntu LTS release version of 12.04 and upwards then it is automatically vulnerable to the CVE-2020-16119 (NIST, 2021), as we are informed from the CPE information that are correlated with the specific vulnerability and is depicted below:

 cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:* Show Matching CPE(s)▼
 cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:* Show Matching CPE(s)▼
 cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:* Show Matching CPE(s)▼
 cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:* Show Matching CPE(s)▼
 cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:lts:*:* Show Matching CPE(s)▼

Figure 17: Known affected software configurations for CVE-2020-16119 (NIST, 2021)

According to (NIST, 2021), the use-after-free vulnerability gives an attacker the opportunity to target any -unpatched- Linux device by reusing a DCCP socket with an attached dccps_hc_tx_ccid object as a listener after being released. In addition, the specific vulnerability is associated with the CWE-416 named as 'Use-after-free' (CWE, 2021). As we have already mentioned, our tool retains the complete set of associations between the CVEs and the CWEs. Thus, in this case, as soon as it receives the specific CVE identifier it automatically assigns it to the TH-21 'Software Exploitation-Malicious code injection' threat via the aforementioned CWE identifier.

8. GDPR

8.1 Background and purpose

The protection of natural persons in relation to processing of their personal data is a fundamental right protected under article 8(1) of the Charter of Fundamental rights of the EU, as well as under article 16 (1) of the Treaty on the Functioning of the EU.

Data protection in Europe was, until recently, regulated by the Data Protection Directive 95/46/EC. However, constant technological

developments, digitalisation and globalisation, as well as people intension to share a huge amount of data online, have challenged the data protection regime and have called for a reform that will warrant a strong and coherent data protection framework in the EU. Effective protection of personal data throughout the Union, strengthening of the subjects' rights when processing of their personal data takes place, setting in detail data controllers' obligations and warranting free flow of personal data within the Union are only some of the issues the new General Data Protection Regulation (GDPR) aims to address.

The GDPR is the successor of Directive 95/46/EC of 24 October 1995. GDPR entered into force in May 2016 and became fully enforceable in May 2018 throughout the EU. GDPR, contrary to the recently repealed Data Protection Directive, is a regulatory tool of broad and direct effect that intends to address any inconsistency in national laws and to succeed a harmonised data approach among Member States.

GDPR regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU. The Regulation does not apply to the processing of personal data of deceased persons or of legal entities. Its provisions do not apply to data processing by an individual for purely personal reasons or for activities carried out in one's home provided there is no connection to a professional or commercial activity.

8.2 Definitions

The basic definitions under the GDPR, as of more relevance to the CitySCAPE project, include:

a) Personal Data

The definition of "personal data" is included in Article 4(1) of the GDPR: **personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The notion of "identifiability" is further analysed in the Regulation and more specifically in Recital 26 where a proportionality test is used in order to assess each time what data may pertain to identifiable individuals. The recital reads as follows: *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are*

reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". If the test is not passed, then such data are considered anonymous and the law does not apply on them.

b) Special categories of data

Special attention should be given to categories of data that do not fall under the generic definition of personal data mentioned above. These include:

- **genetic data** that include personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **biometric data** that include personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; and
- **data concerning health** that refer to personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. The first two categories constitute additions in the data protection field that come as a result of scientific developments in their respective fields.

The above categories of data fall under the definition of special categories of personal data. It should be mentioned that the term sensitive data that was used in the Directive is replaced in the new Regulation by the term "special categories of personal data". According to article 9 (1) of the GDPR "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited". Exceptions to this rule are included in par. 2 of the same Article 9, as outlined below under (d).

c) Pseudonymisation

Another definition that should be included in this analysis as of relevance to the CitySCAPE project is that of "pseudonymisation". The term is a new entry in the text of the GDPR. In essence, pseudonymisation means *"the processing of personal data in such a manner that the personal data can*

no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person” (Art. 4(5)). For the avoidance of any doubt regarding whether or not pseudonymised data should be treated as personal data recital 26 of the GDPR clarifies that: “personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person”. What matters in practice is not the process of pseudonymisation as such but whether the natural person could be, at the end of the day, be identified.

d) “Processing” of personal data

A definition of “processing” of personal data is provided under Article 4(2) of the Regulation. Processing therefore means “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”. The processing principles are described below under section 8.3.

The Regulation makes explicit reference to processing of special categories of personal data in its article 9. In this context, apart from the basic principles that should apply to any processing of personal data, in the event that special categories of data are concerned, processing shall be prohibited. Article 9(2) however names the exceptions to this general prohibition. In particular, paragraph 1 shall not apply if one of the following applies:

- a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

- d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- e. processing relates to personal data which are manifestly made public by the data subject;
- f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

e) Controllers – processors – joint controllers – recipients

The definition of a **controller** is provided under article 4(7) of the GDPR. According to said provision controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others,

determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”. New addition introduced by the Regulation is the explicit reference to the notion of joint controllers. Article 26 of the Regulation states that “Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation [...]”.

Article 4(8) defines a **processor** as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

Finally, a **recipient** is defined under article 4(9). In particular, “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not”.

8.3 The GDPR processing principles

8.3.1 The personal data processing principles in general

Principles relating to processing of personal data are listed in Article 5 of the GDPR. If one wanted to compare the old legislative framework with the new one, one would reach the conclusion that the processing principles remain, in their essence, the same, however they have been worded in a more solid way. In addition, the principles of transparency and accountability have been added to the list of principles, thus contributing further to individual protection during processing of personal data.

In this context Article 5 of the Regulation reads as follows:

1. Personal data shall be:
 - a. processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**)
 - b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
 - c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
 - d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are

inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

To sum up, the processing principles provided under the GDPR are the principles of:

- lawfulness, fairness and transparency
- limited purpose
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

8.3.2 Fair, lawful and transparent processing

a) Lawfulness

According to Article 5.1(a) of the EU GDPR, "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)". This principle of lawfulness of processing is further defined in its Article 6, where it is stated that "processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject

prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks". Consequently, the principle of lawfulness of the processing requires that one of the above legal bases and not cumulatively all six of them, needs to apply in order for the processing to be conducted lawfully.

Consequently, the lawful grounds for processing operations are six:

- consent,
- performance of a contract,
- compliance with a legal obligation,
- protection of vital interests,
- public interest,
- overriding interest of the controller.

b) Transparency

As far as **the principle of transparency** is concerned, article 5.1(a) of the GDPR states that personal data must also be processed in a transparent manner. Further guidance on what transparency exactly means is provided in Recital 39: *"[...] It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data."*

8.3.3 The principle of accountability

As already mentioned, the principle of accountability is a new addition under the GDPR. According to Article 5.2 of the EU GDPR, “*the controller shall be responsible for and be able to demonstrate compliance with paragraph 1 [the basic personal data processing principles]*”. Consequently, it is the data controller’s obligation to undertake the necessary measures, both organisational, technical or other in order to be ready, to demonstrate that the data protection law has been observed. Internal policies, appointment of a DPO or conducting DPIAs are some examples of compliance with the principle of accountability.

8.3.4 Individual consent

Informed consent of the subjects participating in a research is the first and perhaps the most important part of conducting research ethically. When it comes to personal data processing in particular, individual consent is arguably the most important legal ground for processing personal data lawfully. It’s the only legal ground that lies exclusively upon the individual’s personal decision to have his/her personal data processed.

A definition of consent is provided under article 4(11) of the GDPR: consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

More details on the specific criteria which individual consent should meet are provided under recital 32 of the GDPR: “Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided”.

Additional conditions for consent are listed in article 7 of the Regulation. In more detail:

- the controller shall be responsible to demonstrate that the data subject has consented to processing of his or her personal data;
- if consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters;
- the data subject shall be free to withdraw his/her consent at any time;
- When the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, it should always be examined whether the consent has indeed be provided freely;

The Regulation refers separately to the conditions applicable to child's consent in relation to information society services (Article 8 of the GDPR).

8.4 The GDPR rights afforded to individuals (data subjects)

8.4.1 General

Rights of the data subject are dealt with in Chapter III of the GDPR. In particular, Article 12 sets the way (the “modalities”) that rights listed in the next articles are to be exercised:

- any information to the data subjects should be provided by the controller in a transparent and easily accessible form;
- the information shall be provided in writing;
- the controller shall facilitate the exercise of the data subjects' rights;
- the controller shall also provide information on action taken on a request under Articles 15-22 to the data subject without undue delay;
- if the controller does not take action on the request of the data subject, the controller shall inform the data subject of the reasons for not taking action;
- information shall be provided for free.

The rights attributed to data subjects are regulated under articles 13 to 21 and are the right to information, the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to restriction of processing, the right to data portability, and the right to object.

8.4.2 The right to information

The right to information is regulated in two articles, namely Articles 13 and 14. Distinction is made between cases where the information was obtained from the data subject and other cases. In this context, article 13 regulates the case where personal data have been collected from the data subject. In this case, the controller shall at the time when personal data are obtained, provide the data subject with the following information:

- a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- b) the contact details of the DPO , where applicable;
- c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- e) the recipients or categories of recipients of the personal data, if any;
- f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Paragraph 2 of Article 13 lists the additional information the controller needs to provide to the data subject when collecting his/her personal data, such as the period for which the personal data will be stored, the existence of the right to request access to the data or erasure, the right to withdraw consent at any time etc.

Article 14 lists the information to be provided to the data subject where personal data have not been obtained from the data subject itself. Paragraph 5 of article 14 sets some exemptions of the controllers' obligation to provide information, for instance when the provision of such information proves impossible or would involve a disproportionate effort or where personal data must remain confidential etc.

8.4.3 The right to access the data

The right of access by the data subject is regulated under article 15 of the Regulation. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed and if yes, access to such data as well as information regarding, among others, the purpose of processing, the recipients to whom the data have been or will be disclosed the existence of the right to request rectification, the right to lodge a complaint and others, the right to request rectification etc. Paragraph 3 of article 15 sets the subject's right to request a copy of his/her personal data from the controller.

It is noted that the right to rectification is regulated separately in article 16. In particular, the data subject shall have the right to obtain from the

controller without undue delay the rectification of inaccurate personal data concerning him or her.

8.4.4 The right to erasure (right to be forgotten)

Article 17 of the Regulation grants individuals the right to have their personal information deleted by data controllers if specific conditions as these are listed in its paragraph 1 are met. For instance, the personal data have been unlawfully processed or they are no longer necessary in relation to the purpose for which they were collected, or the data subject has withdrawn his/her consent and others. In the event that the controller has made such data public, reasonable steps (including technical measures) will be taken to notify controllers who are processing the personal data accordingly. Finally, the “right to be forgotten” (actually, to erasure of data) will not be applicable if it contrasts with the rights of freedom of expression and information as well as for several other, more expected, legal grounds (compliance with a legal obligation, public interest, archiving purposes, etc., as set in paragraph 3).

8.4.5 The right to restriction of the processing

Article 18 of the Regulation regulates the right to restriction of the personal data processing. The conditions under which a data subject may exercise his/her rights are listed in the first paragraph of article 18 and include, for instance, the contest by the data subject of the accuracy of the personal data processed by the controller or the claim that the processing is unlawful and therefore the data subject opposes the erasure of his/her personal data. Recital 67 mentions some methods the controller may use to restrict the processing of personal data, such as, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website.

8.4.6 The right to data portability

Data portability is dealt with under article 20 of the GDPR and includes the data subject’s right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The right to data portability is provided to data subjects under two conditions:

- a) the processing is carried out by automated means;
- b) the processing is based on consent or on a contract.

8.4.7 The right to object

The right to object is laid down in Article 21 of the GDPR. Recital 69 of the Regulation clarifies the conditions under which a data subject may object to his/her data being processed. The recital reads as follows: Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject. In other words, the exercise by an individual of its right to object to its personal data being processed by a controller essentially includes a balancing of rights and legitimate interests: on the one hand an individual is interested in having its data no longer processed and on the other hand a controller may have an interest in continuing to process such data despite the individuals' objections.

8.5 Security of personal data

8.5.1 Security of the personal data processing

Security of the processing is regulated under article 32 of the GDPR. Both the controller and the processor need to implement technical and organisational measures to ensure a level of security including among others:

- a) the pseudonymisation and encryption of personal data;
- b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in timely manner in the event of a physical or technical incident;
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

All measures should be proportionate to the risk involved and the severity for the rights and freedoms of natural persons in the event of a personal data breach.

8.5.2 Data Breach Notifications

Article 33 regulates the process of notifying to the supervisory authority a personal data breach. A “personal data breach” is defined in the text of the GDPR, in Article 4(12), as “*a breach of security leading to the accidental or*

unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". When this happens, controllers shall, according to article 33, par. 1 "without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay". The obligation of notification burdens the processor as well, who, shall notify the controller without undue delay after becoming aware of a personal data breach (article 33 par.2). Paragraph 3 lists the minimum information the notification must contain, such as the nature of the data breach, the name and contact details of the DPO, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach.

Whereas article 33 deals with the notification of a breach to the supervisory authority, article 34 regulates the communication of a data breach to the data subject. This obligation burdens the controller in any case where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in article 33(2). Paragraph 3 of article 34 sets the conditions under which the communication to the data subject is not required. In particular par. 3 reads as follows *"The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner".*

8.6 Data protection impact assessment

The "tool" of the impact assessment is a new entry under the GDPR. It is suggested as an extra security measure in all cases where a type of processing is likely to result in high risk to the rights and freedoms of natural persons. The assessment of the impact of the envisaged processing

operations on the protection of personal data is carried out by the processor prior to the processing. Par. 3 of the article 35 specifically lists the case where a DPIA shall be required:

- a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- c) a systematic monitoring of a publicly accessible area on a large scale.

Paragraph 7 of article 35 lists the minimum content of the assessment. In particular, it should contain:

- a description of the processing and its purposes;
- an assessment of the necessity and proportionality of the processing in relation to the purpose of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks, including security measures and mechanisms, to ensure the protection of personal data and to demonstrate compliance with the GDPR.

8.7 Personal Data Protection in the CitySCAPE project (Design Phase)

8.7.1 Determining the processing activities and their scope

The first element that needs to be considered, when designing CitySCAPE, is to specify the scope of all the processing activities that will be implemented and which will involve processing of personal data. In order to help the CitySCAPE partners with this preliminary assessment, the following list contains some key questions that will assist them to determine the scope and the details of the envisaged processing activities (if any). Please note that the list is not exhaustive and that other issues may need to be taken into account, in light of the specific context.

- Will any personal data be processed in the context of a specific CitySCAPE processing activity?

- Will any special categories of personal data be processed in the context of a specific CitySCAPE processing activity?
- For each of the processing activities envisaged, how will the personal data be collected?
- If personal data will be processed in the context of a specific CitySCAPE processing activity, determine the categories of personal data (including special categories of personal data) that will be processed.
- What is the purpose of each CitySCAPE processing activity?
- Will the personal data processed, for any of the processing activities envisaged, be disclosed to any recipients? If so, which personal data and to which recipients?
- If the personal data will be disclosed to recipients, are these recipients' processors, controllers or joint-controllers?
- If the personal data will be disclosed to recipients, are these recipients located inside or outside the EU/EEA?
- What are the means used for the processing of any personal data?

The above elements merely provide the context in which the controller should consider the safeguards that should be adopted in order to comply with the data protection principles and the GDPR in general. Following this initial assessment of the processing activities, the rest of this Section will address certain key issues / questions that must be considered in order to ensure that the processing is in line with the data protection principles and complies with the other GDPR requirements.

8.7.2 The Data Protection Principle

The fundamental principles of the GDPR, listed and detailed in section 8.3, must also be taken into account during the design phase of CitySCAPE. The following list contains a number of key questions that will support the CitySCAPE Partners to ensure that any of the envisaged processing activities (determined on the basis of the checklist above) are in line with the fundamental data protection principles, or to determine the type of measures that should be taken in order to satisfy these data protection principles.

- How is it ensured that the data subjects, whose personal data is processed by CitySCAPE, are informed in a clear and simple manner about those processing activities?
- Has an appropriate legal basis been determined for each of the envisaged processing activities? In case of processing of special categories of personal data, which specific condition, under Article 9 of GDPR, is applicable?

- Have you specified the purpose for which each envisaged CitySCAPE processing activity is conducted?
- As regards the categories of personal data that will be processed by each specific processing activity, does this only include personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they would be processed?
- Is it possible to carry out the processing using anonymized data?
- Is it possible that certain personal data that will be processed will become outdated at some point? If so, has it been considered how to keep this personal data up to date?
- Is it possible that certain personal data that will be processed are inaccurate? If so, has it been considered how these data can be rectified?
- Will all personal data that is collected in the context of CitySCAPE, only be kept in identifiable form to the extent strictly necessary in relation to the purpose(s) for which they are collected? Would this be the case in respect of (i) the amount of personal data collected; (ii) the extent of their processing; (iii) the period of their storage; and (iv) their accessibility? In other words: have appropriate retention periods been established for all categories of personal data?
- If personal data are kept in an identifiable form longer than strictly necessary in relation to the purposes for which they are collected, are these personal data processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organizational measures to safeguard the rights and freedoms of the data subject?
- Which accountability tools have been put in place to demonstrate compliance with the GDPR requirements?

8.7.3 Meeting Other GDPR Requirements

Apart from the obligation to introduce measures that implement the fundamental data protection principles, Article 25 of GDPR also stipulates that a controller must "*implement appropriate technical and organisational measures, such as pseudonymisation, which are designed [...] to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*". In the following sections, we will address the most important categories of GDPR requirements that need to be considered in the context of the CitySCAPE project.

8.7.3.1 Lawfulness of processing

For every CitySCAPE activity that involves processing of personal data it must be ensured that an appropriate legal basis has been determined. The GDPR sets out six different grounds for processing activities to be lawful, only one of which is relevant in the context of CitySCAPE: processing on the basis of consent.

8.7.3.2 Informing the Individuals

When processing personal data, through the CitySCAPE processing activities, it is necessary to ensure that the individual (data subject) knows about the processing and is informed of his or her rights under the GDPR. The GDPR provides a list of all information that must be provided to individuals. That information must be provided at the time when the personal data are collected. It should moreover be provided in a manner that is easily accessible and to the point, using clear and plain language.

Data subjects are typically informed of processing of their personal data through a privacy policy. This will be a crucial element for ensuring and demonstrating compliance of the CitySCAPE offered services with privacy requirements, as the privacy policy is easily accessible and visible to all.

8.7.3.3 Data Subjects' Rights

The GDPR gives a number of rights to individuals whose personal data are processed: the right of information, the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object and the right not to be subject to automated decision-making. It should be ensured that individuals whose personal data are processed in the context of CitySCAPE are able to exercise these rights in an easy manner.

Thus the project should establish how the data subjects' rights will be dealt with; for instance through a dedicated central system for handling data subject requests such as a dedicated email address or web page.

8.7.3.4 Contractual Relations

It should be verified whether, in the context of CitySCAPE, third parties will be also involved in the processing of the personal data collected by the consortium and if so, whether this is truly necessary. If that is indeed the case, it is necessary to determine the status of that third party with respect to the personal data, i.e. controller, joint controller, or (sub)processor.

8.7.3.5 International Transfers

The GDPR provides for a general principle according to which the transfer of personal data to any country outside the European Economic Area ("EEA") is prohibited unless that third country ensures an adequate level of privacy protection. So far, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United Kingdom as providing adequate protection. In these cases, personal data can move freely as if it were a transfer within the EEA. The CitySCAPE Partners must therefore consider whether any such international transfer outside the EEA to a third country not offering an adequate level of protection is necessary. This would for instance be the case when deciding to rely on a US-based cloud service provider. In this case, personal data cannot be transferred freely without additional measures being in place, according to Schrems II. More specifically, on 16/07/2020 the Court of Justice of the European Union (CJEU) issued a very important ruling in the context of the examination of Case C311/18 Data Protection Commissioner of Ireland v. Facebook & Max Schrems' (Schrems II). In that decision, the CJEU ruled the EU-US Privacy Shield (Commission Decision 2016/1250) invalid. By the same decision, the CJEU considered that standard contractual clauses 2010/87 (hereinafter SCC) for the transfer of personal data to processors established outside the EU (Commission Decision 2010/87) remain valid for the transfer of personal data to the US, subject to specific conditions. In particular, prior to any transfer based on the SCC, the exporter – with the help of the data importer – must examine whether the level of data protection guaranteed by the GDPR is ensured in the third country concerned, taking into account the circumstances of the particular transfer and any additional measures the exporter can take. If the exporter concludes that an adequate level of protection is not provided, they must suspend the transfer and/or terminate the contract with the importer.

8.7.4 Security of Processing

In addition to the legal and procedural requirements imposed by GDPR, it is crucial during the CitySCAPE design phase to identify all the security requirements that should be satisfied in order to achieve the required level of protection for the system and for the personal data being processed. While the requirements listed below are not exhaustive, they provide an overview of the most important elements that need to be considered in order to minimise the risk that any of the personal data is lost, unlawfully accessed, corrupted or in any way misused.

It is thus the responsibility of the CitySCAPE partners to implement appropriate security measures to prevent the personal data they process

from being compromised in any way. This means that the partners will need to:

- Determine who is responsible for ensuring security of processing
- Make sure the appropriate organisational and technical security measures are in place
- Make sure that technical measures are backed up by robust security and privacy policies and reliable, well-trained employees
- Be able to respond to and remedy any breach of security swiftly and effectively.

According to GDPR, the data controller is responsible to determine the appropriate level of security for each one of the processing activities. The required protection level differs for each processing activity, as it depends on the actual risks faced by the processing activity in question but also on the severity of the impact that a potential security may have. Thus, before deciding what security measures to implement, the CitySCAPE partners need to conduct a risk assessment. To this respect, the following questions should be considered:

- Has a risk assessment been conducted to determine the appropriate level of security for each of the different processing activities envisaged in the context of CitySCAPE?
- Have the nature, scope, context and purposes of each of the envisaged processing activities been taken into account in the context of such a risk assessment?
- Has it been assessed, in the context of such risk assessment, how valuable, sensitive or confidential the processed personal data is to the individuals concerned?
- Has it been assessed, in the context of such risk assessment, what damage could potentially be caused to those individuals if a personal data breach were to occur? This includes in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
- Have the state of the art and the costs of implementation been taken into account in the context of such risk assessment?
- Has this risk assessment been documented and included in the relevant accountability file?

8.8 Personal Data Protection in the CitySCAPE project (Development Phase)

Once the initial security and privacy considerations have been made in the design phase of CitySCAPE, these considerations need to be translated into

concrete measures and safeguards in the development phase. The present section is structured in the same manner as section 8.7 above. For each of the aspects addressed in that section, a list of questions is provided to help the CitySCAPE partners ensure that CitySCAPE is developed in a privacy-compliant manner.

8.8.1 General Considerations

Before addressing the specific processing aspects, it is important to consider several issues that may affect the choice of the protection measures that will be adopted. Indicatively, the CitySCAPE partners will notably have to:

- choose the appropriate measures among those available (i.e., within the 'state of the art')
- consider the cost of implementation
- consider the specific risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing
- Note that, when making the above assessment and considering specific measures, the factors relating to the state of the art of available technology and relating to the cost of implementation must not be interpreted in such a way that the measures chosen do not sufficiently mitigate existing risks and the resulting protection is not adequate. It should however be noted that less extensive measures may be required in case e.g. the extent of a certain processing activity is very limited and is considered to constitute a low risk to the rights and freedoms of individuals.

8.8.2 The Data protection principles

Without being exhaustive, this subsection includes a checklist to ensure compliance of the CitySCAPE platform with the data protection principles and the main GDPR requirements.

- Is the processing recorded / logged so as to be able to identify misuse of the data? If so, is the recording/log tamper-proof?
- In case personal data are automatically (or otherwise, e.g. on request) anonymised or pseudonymised the following criteria should be addressed: when that happens (timing), on what parameter does the decision to anonymise or pseudonymise personal data depend? How are pseudonymous data secured against too-easy re-identification?
- Are measures taken to avoid the creation of temporary shadow files (e.g. through unnecessary logging)? If such temporary shadow files are needed, how well are they protected against unauthorized access?
- If data are (intended to be) passed on to other controllers (or processors), are measures taken to filter out data that are not needed by the recipients?

- Are data disclosed internally only to those who need access and how is this ensured?
- Will any third party recipients be informed that they should only use the data for the purpose(s) for which they are provided? Are they asked to warrant that they will do so? Are such warranties binding? Can they be invoked by the data subjects?
- Is there a guarantee that all personal data, the actual personal data used and any back-ups, are erased or de-identified (really anonymised) when they are no longer needed for the purpose for which they were held? How is this done and verified?
- Can data that is no longer needed for the original purpose, but that cannot be erased due to retention rules (e.g. documentary reasons, tax regulations etc.) be blocked or otherwise excluded from regular processing?
- Which steps are taken to ensure that personal data that are inaccurate are erased or rectified without delay?
- What technical and organizational measures will be implemented to be able to demonstrate that processing is performed in accordance with the GDPR?
- Has an internal accountability file been created allowing the CitySCAPE partners to document and demonstrate GDPR compliance? The accountability file should contain, among others, records of processing activities, a list of IT systems, a list of data processors (and related contracts), an inventory of security measures, a data breach handling policy, requests from and responses to individuals, the information provided to individuals (policies) and any privacy-related risk assessments.
- Are risk assessments (such as DPIAs) conducted whenever required under the GDPR and are these risk assessments documented?

8.8.3 Meeting other GDPR requirements

This subsection provides a list of key questions that will support the CitySCAPE partners to implement the appropriate safeguards, into the envisaged processing activities, and thus ensure compliance with the most important GDPR requirements.

8.8.3.1 Legal Ground for Processing

- Is it ensured that the legal basis for the processing of personal data (informed consent for the CitySCAPE case) is explicitly explained to (and asked by) the data subjects?
- If so: Does the consent meets the associated legal requirements? This means that consent is (i) freely given, (ii) sufficiently specific,

by setting out the purpose(s) of the various phases of the processing, (iii) informed, and (iv) unambiguously given by way of a statement or a clear affirmative action of the data subject?

- Where appropriate, are separate consents obtained for distinct processing purposes?
- How will it be demonstrated that the data subject has consented to the processing of his/her personal data?
- How is it ensured that consent can be withdrawn just as easily as it can be given?
- Is it ensured, when relying on legitimate interests, that decision-making in relation to the balance between the interests of the controllers (or relevant third party) and the rights of data subjects, is documented?

8.8.3.2 Transparency: privacy notice

- Is transparency, in respect of the data subjects, ensured with regard to the data processing (e.g. where appropriate data flow, data location, ways of transmission etc.)?
- Is an informative, up-to-date and understandable, well-indexed and/or searchable privacy notice in place, containing a description of CitySCAPE and the processing activities conducted in the context thereof? Is it simple to access the privacy notice? How will this be updated?
- Is the basic concept underpinning service clearly set out?
- Is there a privacy notice that provides sufficient information on relevant privacy issues resulting from the use of CitySCAPE (including e.g. use of cookies, processing of IP addresses)?
- Does the privacy notice provide specific and meaningful information about the processing of personal data instead of mere blanket confirmations of legal compliance?
- Is the concept of "highlight notices" (providing some high-level information at a glance) used?
- Is the privacy notice available in one or multiple languages?
- Has the personal data been obtained directly from the individuals (data subjects) or not? If so: has all the information appearing in the left column of Table 17 been provided to the data subjects? If not: has all the information appearing in the right column of Table 17 been provided to the data subjects?
- Is the information provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language?
- Where possible, is the information provided in combination with (standardised) icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing?

- Are there special measures to enhance transparency? Can specific processing steps be clarified to the individual?
- Does the privacy notice inform about all relevant aspects of the processing activities as required under Article 13 or 14 GDPR (see table below)?

Information to be provided	Data obtained from data subject	Data not obtained from data subject
Identity and contact details of controller, representative and DPO if any	<input type="checkbox"/>	<input type="checkbox"/>
Purposes and legal basis of the processing	<input type="checkbox"/>	<input type="checkbox"/>
Categories of personal data concerned		<input type="checkbox"/>
Any recipients / categories of recipients	<input type="checkbox"/>	<input type="checkbox"/>
The source and, if applicable, whether it came from publicly accessible sources		<input type="checkbox"/>
The existence of each of the data subject rights	<input type="checkbox"/>	<input type="checkbox"/>
The right to complain to a supervisory authority	<input type="checkbox"/>	<input type="checkbox"/>
Details of any transfers to a third country and safeguards	<input type="checkbox"/>	<input type="checkbox"/>
Retention periods or criteria used to determine retention	<input type="checkbox"/>	<input type="checkbox"/>
The right to withdraw consent at any time (where relevant)	<input type="checkbox"/>	<input type="checkbox"/>
The legitimate interests pursued by the controller or third party (where relevant)	<input type="checkbox"/>	<input type="checkbox"/>
Whether the provision of data is a statutory or contractual requirement, whether the data subject is obliged to provide it, the consequences of not providing it	<input type="checkbox"/>	
The existence of automated decision making, information about the logic involved, its significance and envisaged consequences	<input type="checkbox"/>	<input type="checkbox"/>

Table 17: Information per case

8.8.3.3 Data Subjects' Rights

- Has an internal procedure been established to handle data subject requests?
- Has it been assessed how to authenticate the data subject's identity, as well as when and how to verify such identity?
- Are there template for responses to access requests from data subjects?
- Are there procedures that allow the data subject to exercise their rights? Has this been verified for each of the different rights?
- Has it been assessed whether CitySCAPE needs a central system for dealing with data subject requests such as a dedicated email

address or web page, and if so, has it been ensured that data subjects are informed thereof in the privacy policy?

8.8.3.4 Contractual Relations

- Has it been ensured that CitySCAPE data processors (if any) provide sufficient guarantees to comply with the GDPR?
- Where necessary, has a data processing agreement (containing at least the mandatory minimum content) been concluded with all service providers that will be acting as data processors?
- Where necessary, has an agreement of joint controllers been concluded?

8.8.3.5 International Transfers

- In case an international data transfer is conducted to an organization established in a third country not ensuring an adequate level of protection, are SCCs foreseen / put in place and is the Schrems II decision taken into account?

8.9 Privacy and data Protection methodology

8.9.1 Description of the framework

UPRC has proposed and adopted a flexible and efficient GDPR Compliant Personal Data Management methodology in order to ensure the security, safety and privacy aspects. The Framework ensures that GDPR principles, such as purpose limitation, data minimization, accuracy, accountability, the lawfulness of processing, the user consent, are fully satisfied. In this regard, the system will respect all the data owners' rights, such as their rights to object to the storage/processing of their information, their right to be forgotten, their right to restriction of processing, while it will enforce the obligations of the intermediate users (in general all the professional profiles) that manage the system and potentially exploit all the data generated. Finally, all necessary technical, organizational and procedural measures for the satisfaction of the elicited security and privacy requirements are considered, thus enhancing confidence and trust among all stakeholders. It comprises of the following four stages, pictured in Figure 18:

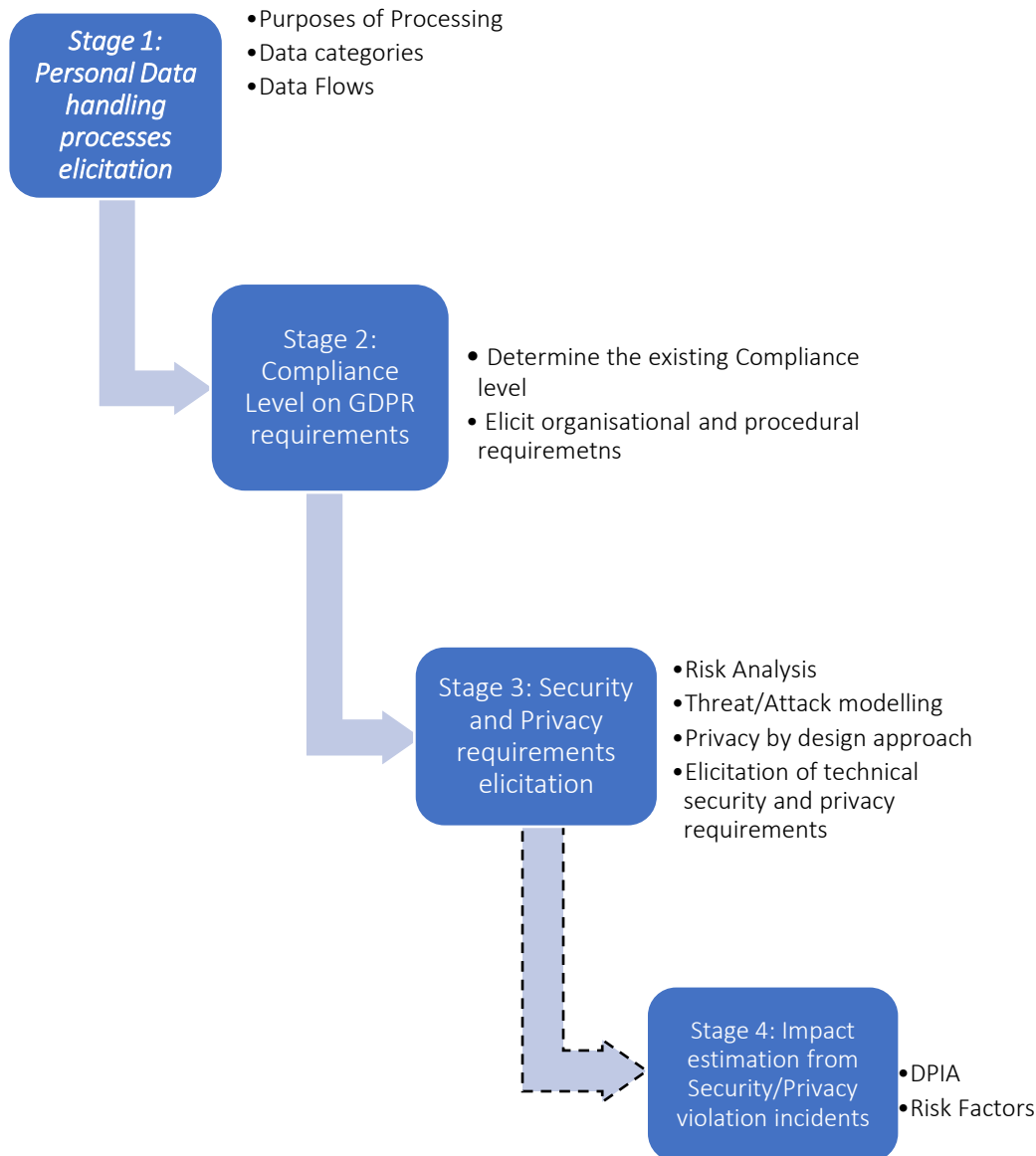


Figure 18. GDPR Compliant Personal Data Management Methodology

8.9.1.1 Stage 1: Personal Data handling processes elicitation

The purpose of this step is to define the perimeter of the Personal Data handling processes, by capturing, reviewing and formalizing the following issues:

- The categories of the personal data processed.
- The categories of the data subjects
- The purposes of each processing activity
- The identification of high risk data processing activities
- The legal basis of each processing activity (e.g. contract and/or consent and/or legitimate interest and/or statutory obligation)

- The categories of recipients to whom the personal data are disclosed
- The envisaged time limits for erasure of the different categories of data – if they exist
- The existing technical and organizational measures for the protection of personal data.

To this end, it is necessary to identify, through a systematic procedure, the following information for each purpose of data processing separately.

- Short Description for the purpose of processing
- Legal Basis for the purpose of processing, including the subcategories a) Law, b) User consent, c) Contract
- The data involved in serving the specific purpose of processing, including the subcategories a) General Data, b) Personal Data, c) Special categories of Personal Data
- The necessity of the involved data for serving the specific purpose of processing
- The sources of collected data
- The transmission of personal data to third parties
- The processing of automated decision-making, including profiling

Therefore its main output concerns the listing of the Purposes of Processing and the Personal Data Categories.

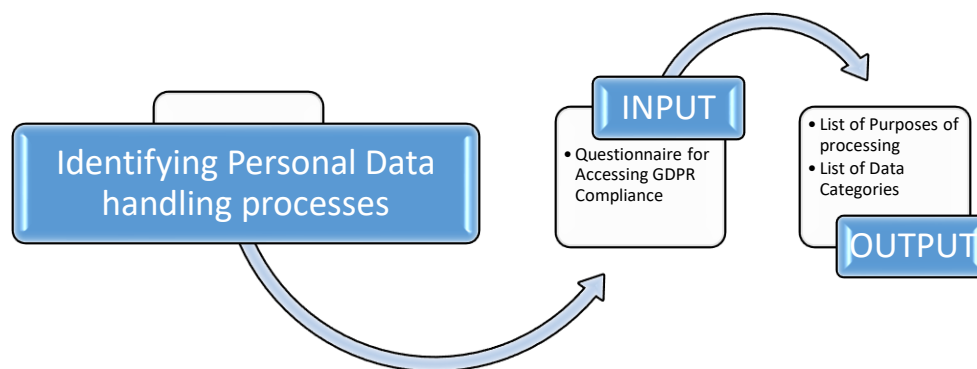


Figure 19. Output of Stage 1

8.9.1.2 Stage 2: Compliance Level on GDPR requirements

During the second stage, it is essential to map the organizational context following the results of stage 1. Therefore, when the above list of information has been compiled, the processing of each personal data category is being reviewed against the GDPR requirements to deduce the existing compliance level, through a GDPR gap analysis. Topics that are examined are presented indicatively as following:

- lawfulness, fairness and transparency of the personal data processing
- the processing purpose limitation, the data minimization,

- the consent of the data subjects,
- the personal data storage limitation
- the measures for personal data protection
- integrity and confidentiality
- The readiness of the involved stakeholders to respond to the data subjects' rights' is examined, such as the 'right of access', the 'right to rectification', the 'right to be forgotten', the right to restriction of processing', the 'right to data portability', the 'right to object'.
- Information to be provided where personal data have not been obtained from the data subject
- Automated individual decision-making, including profiling
- Data protection by design and by default
- Joint controllers
- Security of processing
- Processing under the authority of the controller or processor
- Tasks of the data protection officer
- Transfers on the basis of an adequacy decision

Moreover, the readiness of the organization to respond to the data subjects' rights' will be examined. Indicatively the 'right of access' , the 'right to rectification', the 'right to be forgotten', the 'right to restriction of processing', the 'right to data portability', 'right to object'.

Indicative activities that will be performed during the gap analysis include:

- Review of legal basis on which the organization processes Personal Information.
- Review the necessary retention periods per category of Personal Information, for various reasons such as for compliance with a legal obligation, for inquiries of auditing authorities, for legal claims, for public interest etc.
- Review of Privacy Notices.
- Review of the legal basis for marketing services.
- Legal review of all defined internal Personal Information Protection Policies and Procedures.
- Legal Review of sample employment contracts and updating with necessary legal language to allow the processing of employees Personal Information for legitimate business purposes.
- Review of standard consent forms used to collect and record data subject consent for the processing of Personal Information.
- Legal review of standard Intra- and Third-Party contracts, Procurement contracts and Supply Contracts to identify any contractual gaps in relation to Data Protection relevant clauses. If no standard contracts are used, the review will cover key activities, which should at least include all contracts related to identified high risk processing activities.

- Understand the operational policies and procedures for the IT systems
- Access the efficiency of the organization to protect the data (data protection measures)
- IT and Security Governance review
- Network architecture review

The main output of this stage concerns a set of GDPR Compliance Requirements for each identified purpose of Processing.

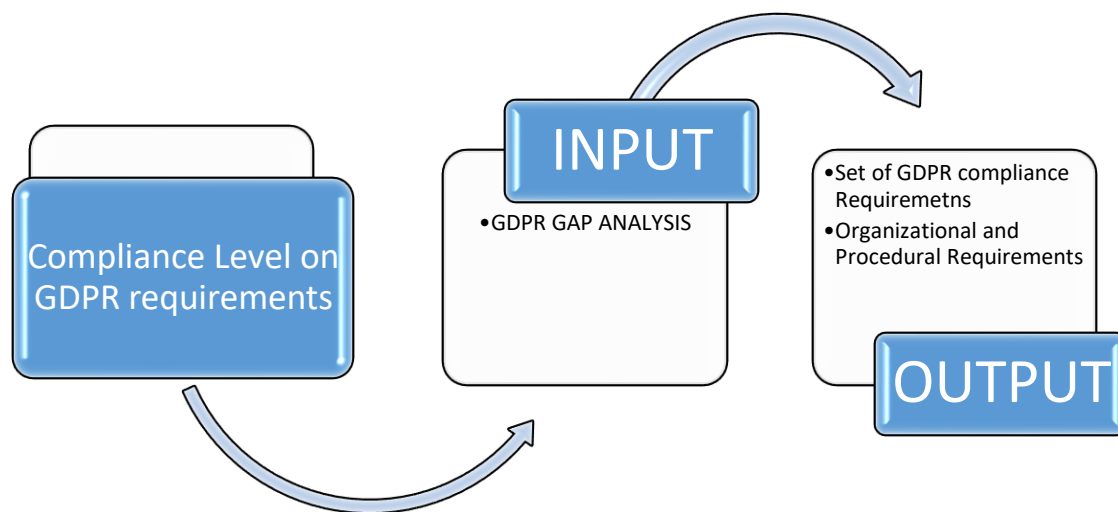


Figure 20. Output of Stage 2

In order to facilitate the process a small auxiliary service has been implemented, that can be embedded as a webservice or can be used with an excel file that is currently available at CitySCAPE repositories and it is going to be integrated at the CitySCAPE platform in WP5. Currently, the file is distributed by UPRC on request.

8.9.2 Stage 3: Security and Privacy requirements elicitation

Security is protection against intended incidents, i.e., incidents that happen due to a result of deliberate or planned act. Security concerns the protection of assets from threats, where these are categorised as “the potential for abuse of protected assets”. Whereas privacy concerns the protection of the assets’ owner identity from users that do not have the owner’s consent to view/process their data. Risk analysis or equivalently Risk Assessment is the methodology where an IT infrastructure and/or interconnection between computational devices is methodically analysed and the corresponding Security/Privacy threats are identified as long with the specific vulnerabilities and/or potential failures may cause them. Moreover, the goal of a security assessment, is to ensure that necessary security and privacy objectives are integrated into the design and implementation of an architecture. A Vulnerability is defined as a weakness, in terms of security

and privacy, that exists in from a resource, an actor and/or a goal (Zhou et al., 2015). Vulnerabilities are exploited by threats, as an attack or incident within a specific context. A Threat represents circumstances that have the potential to cause loss; or a problem that can put in danger the security features of the system (Mouratidis et al. 2013).

In Stage 3, a Risk analysis, identifying threats, vulnerabilities, data, should be conducted in order to deduce attack modelling and threat propagation. The need for such analysis results directly from the GDPR principle of accountability. The analysis assists in the identification and assessment of security and privacy risks and thus in the selection of the appropriate measures to reduce these risks and as such reduce the potential impact of the risks on the data subjects, the risk of non-compliance, legal actions and operational risk.

The proposed steps for implementing stage 3 can be described as follows:

Substep1: Identify System Assets and Stakeholders

The purpose of this step is to define the perimeter (boundaries) of the study. A global vision of the components and communications between components will be clarified. At this step, the following data will be collected and formalized:

- Essentials assets of the system.
- Functional description of components and relations between components.
- Security issues that need to be addressed by the study.
- Assumptions made if appropriate.
- Existing security rules (law and regulation, existing rules in other studies).
- Constraints (internal or external) from system itself.

At the end of this step, a clear vision of the components and the links between them will be formalized that are going to be used as input for the risk analysis method.

Substep2: Identify Potential Security and Privacy Threats and related System Vulnerabilities

The security/privacy threats and vulnerabilities affecting the system will be studied as outcome from a dedicated risk analysis. The threats and vulnerabilities are going to be specific for the system's infrastructure components.

The following activities will be performed:

- List the relevant attack methods against security and privacy.
- Characterize the threat agents for each attack method retained according to their type.
- Identify the security and privacy vulnerabilities of the entities according to attack methods.

- Estimate the vulnerability level.
- Formulate the security and privacy threats.
- Assign priority in the security and privacy threats according to the probability of their occurrence.

The list of the pertinent security and privacy threats and the type of attacks will be the main outputs of this step.

Substep3: Security and Privacy Requirements Analysis

From the previous step, the identification of the respective threats and the attack methods that can be deployed to the proposed system leads to the identification of the system's vulnerabilities. At this stage, Security and Privacy vulnerabilities detection will lead to the identification of the security and privacy objectives, which are the way that vulnerabilities are reduced thus reducing the potential risk on the identified entities. The next step of the specific stage is the definition of the security and privacy requirements that basically describe in a specific way the realization of the identified security and privacy objectives.

The following actions will be considered when identifying security and privacy requirements:

- List the security and privacy functional requirements
- Justify the adequacy of coverage of the security and privacy objectives
- Highlight any coverage flaws (residual risks) with justifications.
- Classify the Security and privacy requirements for each use case.
- Where appropriate, justify the coverage of dependencies of security and privacy requirements

The main output of this stage concerns a) a List of Threats and Attacks, b) the provision of Legal and Organizational Measures and c) the elicitation of the appropriate security and privacy requirements.

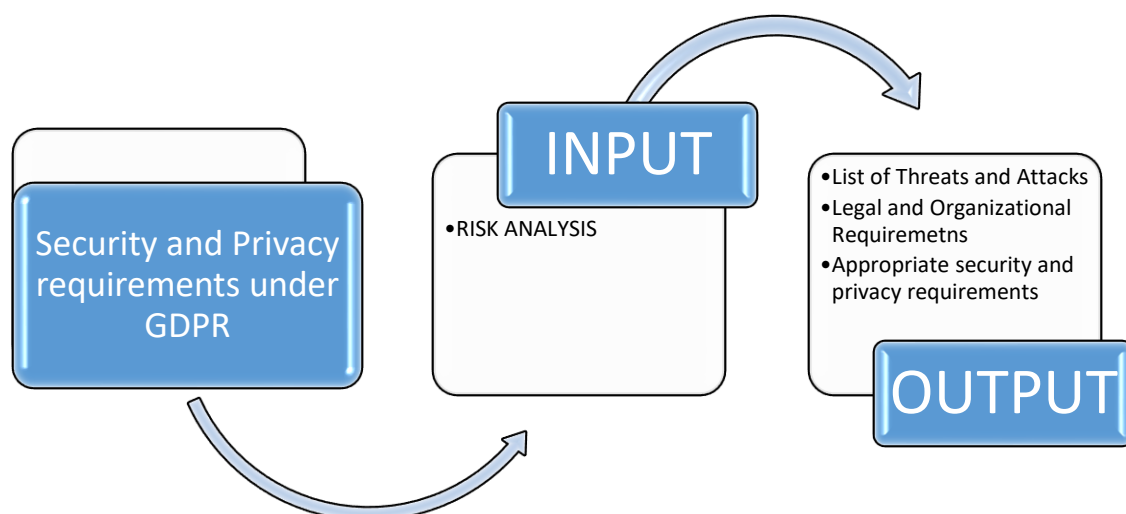


Figure 21. Output of Stage 3

Therefore, it can be concluded that the context of Stage 3 is actually implemented by the Risk Modelling and Analysis process described in Sections 1 to 7 in the current deliverable and will be implemented as part of the CitySCAPE RITA engine in WP5. The execution of the risk analysis from the tool is equivalent to the implementation of Stage 3.

8.9.3 Stage 4: Data Protection Impact Assessment

According to the Regulation (EC) 2016/679 of the European Parliament and of the Council of 27th April 2016 for the protection of natural persons with regard to processing of personal data and on the free movement of such data, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Taking into account the continuous evolution of the system and threats, risk management “necessitates” the identification of appropriate controls. The processing of personal data, the hierarchy and management of risks has to be examined in a way that optimises the cost and contributes to the most suitable decision making, aiming at protecting personal data. Impact assessment contributes to the application of privacy principles, in a way that the data subjects are able to preserve control of their personal data.

A data protection impact assessment, and hence, the criticality of data shall (in accordance with Regulation (EC) 2016/679 of the European Parliament and of the Council) particularly be required in the case of:

- a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g., user profiling by web search activity monitoring for targeted advertising and promotion of products and services (hotels, restaurants, etc.),
- b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10 (e.g., processing of patients’ medical records (special category of personal data) from healthcare organisations, including medical history, illnesses, and patient care, etc.) or
- c) a systematic monitoring of a publicly accessible area on a large scale (e.g., traffic monitoring for informing drivers of the fastest route, residence entries’ monitoring, public transport entrance, etc.).

Moreover, the assessment shall contain, in accordance with Regulation (EC) 2016/679 of the European Parliament and of the Council, at least:

- a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- c) an assessment of the risks to the rights and freedoms of data subjects;
- d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

This privacy impact assessment is based on a robust conceptual framework related to personal data and data subject protection, to the processing of this data by Information Systems or non-automated means, as well as to an impact analysis of possible incidents of personal data for the data subjects they belong to.

Impact assessment aims at the protection of personal data, according to the definition provided by the GDPR, during its processing, as well as the protection of elements that support their processing and are recognised as **Assets**. The value of such assets is equal to the **Impact** brought upon by a possible **violation** of individuals' privacy. A Feared Event is the illegitimate access to personal data, unwanted modification of personal data, as well as the data disappearance. The violation of Information Systems needs the existence of **Vulnerability** and the appearance of a relevant **Threat** coming from a **Risk source**. Summarising, we note that a Threat exploits a vulnerability of an Information System and can have as a result an incident of data protection breach, inflicting some **Impact** on data subjects.

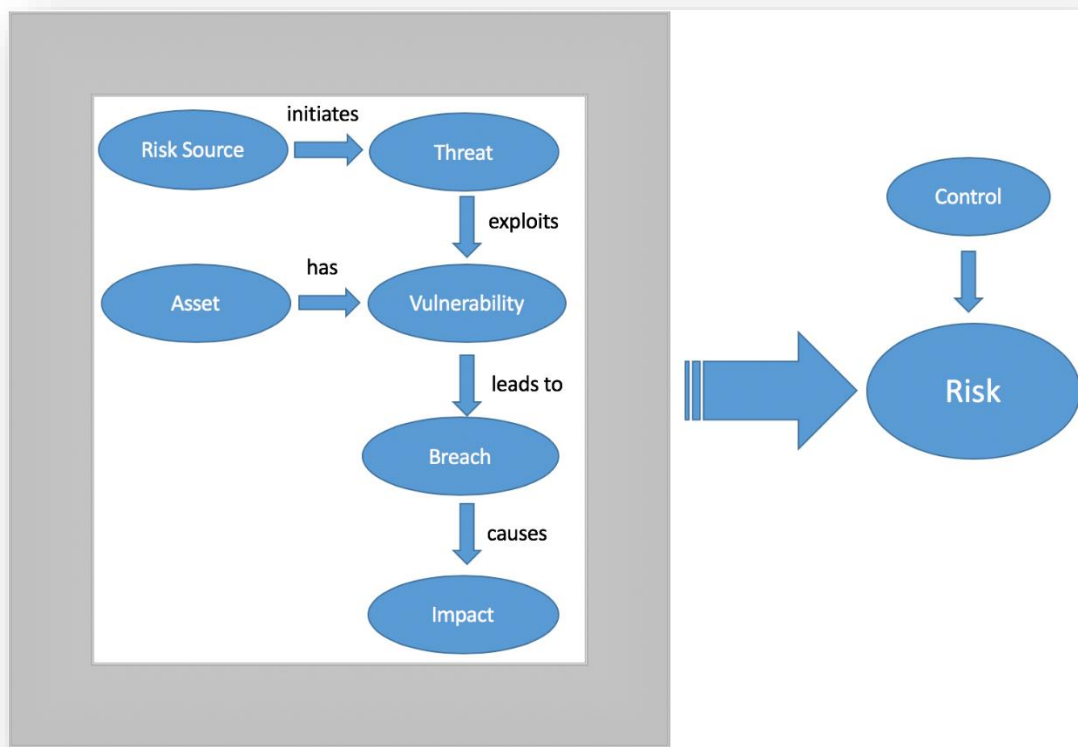


Figure 22. Conceptual Framework of Impact Assessment

A **Risk** is a hypothetical scenario that describes:

- how **Risk Sources** (e.g., an employee bribed by a competitor)
- could exploit the vulnerabilities in **personal data supporting assets** (e.g., the file management system that allows the manipulation of data)
- in a context of **threats** (e.g., misuse by sending emails)
- and allow **feared events** to occur (e.g., illegitimate access to personal data)
- on personal data (e.g., customer file)
- thus, generating **potential impacts** on the privacy of data subjects (e.g., unwanted solicitations, feelings of invasion of privacy, etc.).

The following figure summarizes all the concepts above:

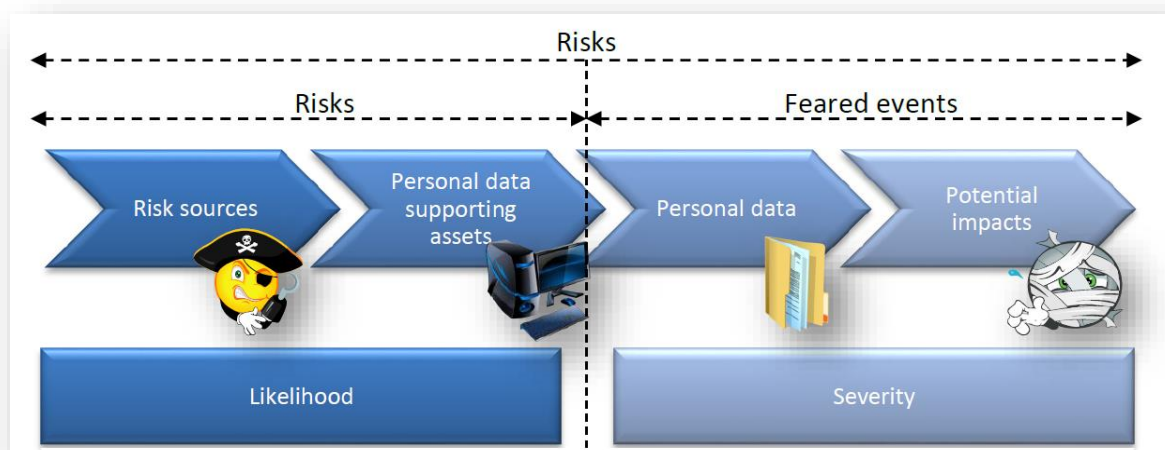


Figure 23. Risks and Feared events

The risk level is estimated in terms of severity, which represents the magnitude of a risk. It essentially depends on the prejudicial effect of the potential impacts, and likelihood, which represents the possibility for a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing threats and the level of capabilities of the risk sources to exploit them as shown below.

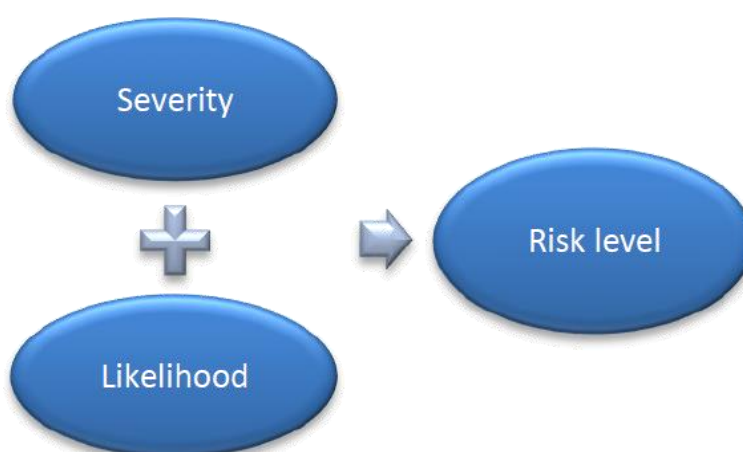


Figure 24. Factors used to estimate risks

In this stage a data protection impact assessment (DPIA) method should be applied in order to identify the severity and likelihood of any possible privacy violation incidents. During this stage all security and privacy requirements elicited in stage 3 will be evaluated in order to eliminate any possible conflicts prior to the selection of the security and privacy countermeasures. In parallel the DPIA will assist in the identification and assessment of privacy risks and thus in the selection of the appropriate measures to reduce these risks and as such reduce the potential impact of the risks on the data

subjects, the risk of non-compliance, legal actions and operational risk. Then the appropriate technical countermeasures for the satisfaction of each requirement will be identified. This information will facilitate the developers to select and proceed with the most suitable implementation techniques for ensuring the security (confidentiality, integrity and availability) of the data processed, as well as the protection of the users' privacy (user consent on data processing and data transmission, satisfaction of user rights etc.).

For conducting the DPIA it is necessary to consider both the output of stage 2 regarding the organizational and legal requirements as they are derived from the Gap analysis as well as the output of stage 3 regarding the technical security and privacy requirements derived from the risk/threat analysis and the privacy by design approach.

The main output of this stage concerns a) the severity of the privacy violations incidents and b) the likelihood of the privacy violations incidents. The following figure presents the input and output of stage 4.

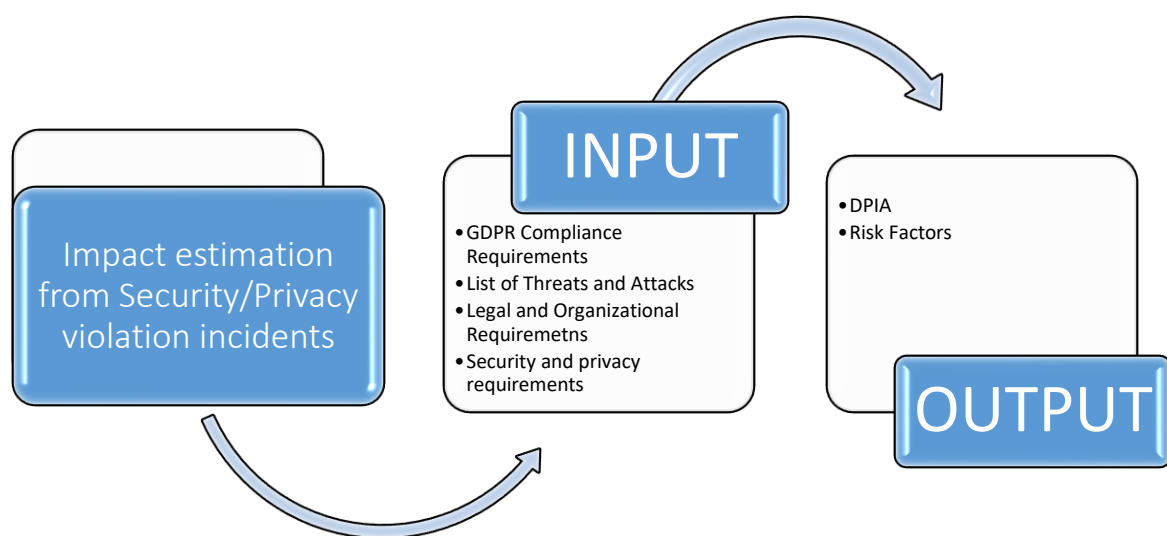


Figure 25. Output of Stage 4

The output of stage 4 will enable the developers to select and proceed with the most suitable implementation techniques for ensuring the security (e.g. confidentiality, integrity and availability) of the data processed, as well as the protection of the users' privacy (e.g. user consent on data processing and data transmission, satisfaction of user rights) under GDPR principles. In the following sections the analysis of each stage is described in more detail.

9. CONCLUSIONS

In WP2, the Use case definition and risk analysis/modelling was performed. The main results of the performed risk analysis and modelling work are presented in this deliverable, as well as in D2.4 with the proposal of a cascading threat methodology. In this report, the following issues were addressed:

- The proposal of a new conceptual model as a basis of a novel risk analysis approach tailored based for the multimodal transport ecosystem.
- Extraction of the system architecture, identification of system assets and decomposition of the system (composite) assets to basic assets.
- Identification of the threats was performed based on the composite system assets – with application of inheritance of threats from basic assets to composite assets.
- Identification of a generic set of vulnerabilities and association of the vulnerabilities with the identified threats and assets.
- Definition of a new modelling methodology based on fault tree analysis, called modified Fault Trees for Threat Analysis (mFTTA), that will be used as a software engineering approach for the implementation of cascading threats in the RITA engine of the CitySCAPE project.
- Development of a dynamic risk analysis system based on the conceptual model that can be updated in real-time by external sources. The dynamic risk analysis approach will be implemented as part of the RITA engine of the CitySCAPE project.
- Investigation of GDPR requirements and compliance with respect to the rights of data owners for the multimodal transport eco-system.

CitySCAPE aims at the development of a dynamic framework that will significantly enhance the security for the multimodal transport use cases. Under this perspective, the work presented in this deliverable focuses on the creation of a) a hierarchical modelling architecture, b) a knowledgebase of assets, threats and vulnerabilities, and c) the development of a dynamic risk modelling scheme – rather than a static use case-specific risk analysis with no reusability.

10. REFERENCES

ANSSI. (n.d.). *Agence nationale de la sécurité des systèmes d'information*. Retrieved from EBIOS Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_ebios.html

- CAPEC. (2021, June 28). *New to CAPEC?* Retrieved August 31, 2021, from https://capec.mitre.org/about/new_to_capec.html
- CASES. (2020, June 10). *MONARC Method Guide*. Retrieved from <https://www.monarc.lu>
- CASES. (2021, September 9). *MOSP*. Retrieved from <https://objects.monarc.lu/schema/14>
- CVE. (2021, March 03). *Frequently asked questions*. Retrieved August 31, 2021, from <https://cve.mitre.org/about/faqs.html>
- CWE. (2020, August 19). *Frequently Asked Questions*. Retrieved August 31, 2021, from <https://cwe.mitre.org/about/faq.html>
- CWE. (2021, July 20). *287: Improper Authentication*. Retrieved September 2021, from <http://cwe.mitre.org/data/definitions/287.html>
- CWE. (2021, July 20). *416: Use After Free*. Retrieved September 2021, from <http://cwe.mitre.org/data/definitions/416.html>
- ENISA. (17, December 2013). *Smart Grid Threat Landscape and Good Practice Guide*. Retrieved from <https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide>
- ENISA. (2009, November 20). *Cloud Computing Risk Assessment*. Retrieved from <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>
- ENISA. (2010, December 10). *Smartphones: Information security risks, opportunities and recommendations for users*. Retrieved from <https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users>
- ENISA. (2017, November 20). *Baseline Security Recommendations for IoT*. Retrieved from <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>
- ENISA. (2019, November 25). *ENISA good practices for security of Smart Cars*. Retrieved from <https://www.enisa.europa.eu/publications/smart-cars>
- ENISA. (2019, November 26). *Port Cybersecurity - Good practices for cybersecurity in the maritime sector*. Retrieved from <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>
- ENISA. (2020, December 14). *ENISA Threat Landscape for 5G Networks Report*. Retrieved from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/>
- Fisher, D., Markscheffel, B., Frosch, S., & Buettner, D. (2012). A survey of threats and security measures for data transmission over GSM/UMTS networks. *2012 International Conference for Internet Technology and Secured Transactions* (pp. 447-482). London: IEEE.
- J. Sokolowski, C. B. (2010). *Modeling and Simulation Fundamentals: Theoretical Underpinnings and Practical Domains*. Wiley .
- Kalloniatis, C. K. (2005). *PriS Methodology: Incorporating Privacy Requirements into the System Design Process*. *Proceedings of the 13th IEEE International Requirements Engineering Conference – SREIS 2005 Symposium on Requirements Engineering for Information Security*. IEEE CPS Conference Publishing Services.

- López, D., Pastor, O., & L. Villalba, G. (2013). Dynamic risk assessment in information systems: state-of-the-art. *6th International Conference on Information Technology*, (pp. 8-10). Amman.
- Marvin Rausand, A. H. (2004). *System Reliability Theory Models, Statistical Methods, and Applications, Second Edition*. Wiley.
- Mouratidis, H. (2011, Mouratidis, H.: . *Journal of Software*, 6(3), 331{339 (2011)). Secure software systems engineering: The Secure Tropos approach. *Journal of Software*, 6(3), 331-339.
- NIST. (2021, September 10). *CVEs and the NVD Process*. Retrieved August 31, 2021, from <https://nvd.nist.gov/general/cve-process>
- NIST. (2021, September 7). *National Vulnerability Database*. Retrieved from CVE-2021-0430 Detail: <https://nvd.nist.gov/vuln/detail/CVE-2021-0430#VulnChangeHistorySection>
- NIST. (2021, September 10). *NVD - General Information*. Retrieved August 31, 2021, from <https://nvd.nist.gov/general>
- NIST. (2021, June 6). *NVD: CVE-2017-3167 Detail*. Retrieved September 2021, from <https://nvd.nist.gov/vuln/detail/CVE-2017-3167#vulnConfigurationsArea>
- NIST. (2021, March 4). *NVD: CVE-2020-16119 Detail*. Retrieved September 2021, from <https://nvd.nist.gov/vuln/detail/CVE-2020-16119#match-6369650>
- NIST. (2021, May 4). *NVD: CVE-2021-0430 Detail*. Retrieved September 2021, from CVE-2021-0430 Detail: <https://nvd.nist.gov/vuln/detail/CVE-2021-0430#VulnChangeHistorySection>
- Riesco, R., & Villagrà, V. A. (2019). Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal of Information Security*, 715-739.
- SaferTEC, H. (2017, Oct). *D2.2 – Attack Modeling* . Retrieved from www.safertec-project.eu/wp-content/uploads/2019/06/D2.2-Attack_modelling-v4.0-final-1.pdf