D2.4 Cascading Risks in the Multimodal Transportation Platforms

Work Package	WP2 Use-cases and Vulnerabilities modelling
Task	T2.3 Mechanisms of cascading threats (across multimodal ecosystem)
Authors	Christos Lyvas, Kostas Maliatsos, Costas Lambrinoudakis, Athanasios Kanatas, Andreas Menegatos, Thrasyvoulos Giannakopoulos, Christos Kalloniatis
Dissemination Level	PU
Status	Final
Due Date	31/07/2021
Document Date	31/07/2021
Version Number	1.0

Quality Control

	Name	Organisation	Date
Editor	Konstantinos Maliatsos	UPRC	22/07/2021
Peer review 1	Liivar Luts / Andrew James Roberts	TALLINN / TALTECH	29/07/2021
Peer review 2	Sammy Haddad	OPPIDA	29/07/2021
Authorised by (Technical Coordinator)	Jason Sioutis	ICCS	28/07/2021
Authorised by (Quality Manager)	Panagiotis Lytrivis	ICCS	28/07/2021
Submitted by (Project Coordinator)	Angelos Amditis	ICCS	31/07/2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Contributors

Name	Organisation	Date
Konstantinos Maliatsos	UPRC	22/05/2021
Christos Kalloniatis	UPRC	10/06/2021
Costas Lambrinoudakis	UPRC	20/06/2021
Athanasios Kanatas	UPRC	01/07/2021
Christos Kalloniatis	UPRC	10/06/2021
Andreas Menegatos	UPRC	10/07/2021
Thrasyvoulos Giannakopoulos	UPRC	10/07/2021
Christos Lyvas	UPRC	14/07/2021
Costas Lambrinoudakis	UPRC	23/07/2021
Konstantinos Maliatsos	UPRC	27/07/2021

Document Revision History

Version	Date	Modification	Partner
0.01	22/05/2021	Draft Release with Table of Contents	UPRC
0.1	10/06/2021	Draft with use cases	UPRC
0.2	15/06/2021	Draft with notes from plenary	UPRC
0..3	21/06/2021	Draft with architecture	UPRC
0.4	30/06/2021	Draft with preliminary threat table	UPRC
0.5	14/07/2021	Draft – updated matrices	UPRC
0.6	23/07/2021	Draft – Cascading threats methodology	UPRC
0.7	26/07/2021	Draft – Fault trees	UPRC
0.9	27/07/2021	Final Draft for review	UPRC
1.0	31/07/2021	Final Document for submission	UPRC

Legal Disclaimer

CitySCAPE is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No. 883321.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

List of Figures

List of Tables

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
ITS	Intelligent Transport Systems
LTE	Long Term Evolution
MaaS	Mobility-As-A-Service
NFC	Near-Field Communication
OS	Operating System
RSU	Road-Side Unit
SMS	Short Message Service
SW	Software
TST	Threat Sequence and Transformation graph

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Executive Summary

This deliverable presents the results of the work carried out during Task 2.3 entitled "Mechanisms of cascading threats (across multimodal ecosystem)". The main objective of the task is to develop a new methodology for analysis of interconnections and interdependencies between systems, assets and critical infrastructures, that will help model and accurately evaluate the infrastructure behaviour due to the propagation of cascading threats.

In the initial project plan, this deliverable followed the completed risk and threat analysis conducted during Task 2.2. However, during the first stages of the analysis it was concluded that the methodology for analysis and modelling of cascading threats should be included in the final version of the risk analysis. Therefore, with the approval of the project coordinator and the project officer, it was decided that the results on cascading threat methodology should precede the final CitySCAPE risk and threat analysis results.

Therefore, D2.4 "Cascading Risks in the Multimodal Transportation Platforms" can be considered as is Part 1 of the complete CitySCAPE Risk and threat analysis focusing on cascading threats for interdependent systems. In order to carry out the development of the new methodology, during this task:

- the assets for the CPaaS system architectures were identified based on the use case definition from Task 2.1 of the CitySCAPE project,
- the interfaces allowing access to the assets (entry points) and the possible interdependencies among them were extracted,
- the composite system assets were further analysed in basic assets, based on the implementation information extracted by D2.1. As composite assets, we define high-level assets of the composite system, composed by various types of components and subsystems, that can be furtherly decomposed in more detailed basic generic assets
- the cyber threats related to the basic assets and consequently the composite CPaaS assets were identified,
- the analysis of the system allowed the investigation of interdependencies leading to a new methodology for cascading threat analysis,

The results of D2.4 will be integrated into the complete risk and threat analysis methodology that is currently developed in Task 2.2 "Cross-domain threat analysis". The developed methodology will be applied on the CitySCAPE CPaaS architectures and use cases.

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 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.

WP2 unfolds activities related to the use-cases, risk analysis and threats in the multimodal transport domain. Initial use-cases will be further detailed and updated, while an exhaustive threat analysis taking into high consideration GDPR will be developed. WP2 outcomes will set the basis for the articulation of the two CitySCAPE pilots planned, as well as a major contributor for the development objectives of the CitySCAPE toolkit.

1.2 Deliverable Purpose

The purpose of this document is to initiate threat analysis ofthe CitySCAPE use cases, and introduce and propose a novel methodology to analyse cascading threats and their propagation and transformation through interdependent assets of a system, or interdependent systems, or interdependent infrastructures.

The document is provided in M11 of the project so that it can facilitate the final steps of the risk analysis process conducted in Task 2.2 (Cross-domain threat analysis) and integrate into the risk analysis process, the cascading threats methodology. Furthermore, the document aims to facilitate the efforts in user and system requirements elicitation of WP3 (User/system requirements & architecture) and the initial development tasks of WP5 (CitySCAPE security layer implementation) and particularly Task 5.5.

1.3 Intended Audience

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 project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

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 and cascading threat methodology can be used to model interdependent systems and critical infrastructures for any of the NIS directive essential services domains.
The deliverables outcomes have direct relevance to the following CitySCAPE tasks:

Table 1: Tasks related to the deliverable

Task	Relationship
T2.2 Cross-domain threat analysis	The deliverable introduces a new methodology for analysis of cascading threats that will be used by the risk analysis performed in the course of T2.2. The results will be documented by the deliverable D2.3.
T2.4 Security assurance methodology and tools	The deliverable provides lists of assets, threats 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 architectural views of the systems described in the use cases, a breakdown of assets to basic components, a list of relevant/applicable threats and provides a way to study threat propagation. 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 a feature with significant added value for the risk analysis, that will be implemented as inference engine in T5.5.

1.4 Inputs from other projects

The development of the new cascading threats 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 propagation approach were evaluated.

1.5 Outline of the Document

The document is structured as follows:

- Chapter 2:
  - Asset analysis of the multimodal transport ecosystem that includes:
    - Brief use case overview,
    - Basic asset definition,
    - Identification of system (composite) assets and their breakdown to basic assets.
- Chapter 3:
  - Identified threats relevant to the system operation,
- Chapter 4:
  - A new methodology for cascading threat analysis is proposed.
  - The concept of Threat Sequence and Transformation (TST) graph is introduced.
- Chapter 5:
  - The derived conclusions are presented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

2 CITYSCAPE MULTIMODAL TRANSPORT ECOSYSTEM ASSETS

2.1 Use Cases – Brief Description

The CitySCAPE consortium includes two public transportation authorities from two European cities, Genoa (Italy) and Tallinn (Estonia). The CPaaS platform from the two cities will be the project's playground for experimentation, development and validation. The CitySCAPE use cases have been defined during T2.1 and can be found in (CitySCAPE, 2021). In the following paragraph, a brief summary of the use cases is provided.

The use cases have been defined with the following goals:

- They should involve multimodal transport scenarios,
- They should include real-world situations – depicting realistic and practical interactions between the transport user and the platform during a journey.
- They should include various assets, users and stakeholders involved in the transportation scenario – like user data, ticketing systems, payment systems, live-tracking, etc.
- They should be compatible with current and future architectures of the transportation platform (CPaaS). The use case must enable solutions that have future applicability.
- They should match the goals and objectives of the CitySCAPE project, meaning that they should be suitable for investigation, development and evaluation of cybersecurity methods and technologies.

Tallinn Use Case:

The Tallinn use case focuses on two basic scenarios:

- Mobility as a Service (MaaS) and,
- Adaptive Traffic Control.

For each scenario, several "micro"- use cases have been defined that focus on very specific situations.

The general view of the operations and workflows of the MaaS scenario (including the Last Mile Extension) as a whole, is presented in Figure 1, from which the involved assets and stakeholders can be extracted. The MaaS scenario can be divided in the following micro-use cases:

- Journey Planning: the process of planning a transportation journey using the electronic means provided by the city of Tallinn.
- Ticket Validation: the process of purchase and validation of a ticket by a user using ICT-supported/enabled services.

- Real-time information: the process of journey tracking or guidance in real-time using available electronic means.
- Last-mile extension: The process enabling the passenger to switch between the city transportation mode onto the last-mile services (AV Shuttle, e-scooter) seamlessly. This scenario includes an automated vehicle, which introduces cooperative, connected and automated mobility into the project.

Figure 1: Operations and Workflow for the Tallinn MaaS scenario

For the Adaptive Traffic Control use case, an Intelligent Transportation System (ITS) solution is investigated, since an ITS-supported street junction is considered. Conventional connected public transport vehicles, as well as autonomous vehicle shuttles are managed by an ITS application and an ITS-enabled roadside unit. This use case is decomposed in two micro-use cases:

- The ITS platform gives priority to an automated vehicle to pass the junction.
- The ITS platform decides to stop the autonomous vehicle giving priority to a public bus.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

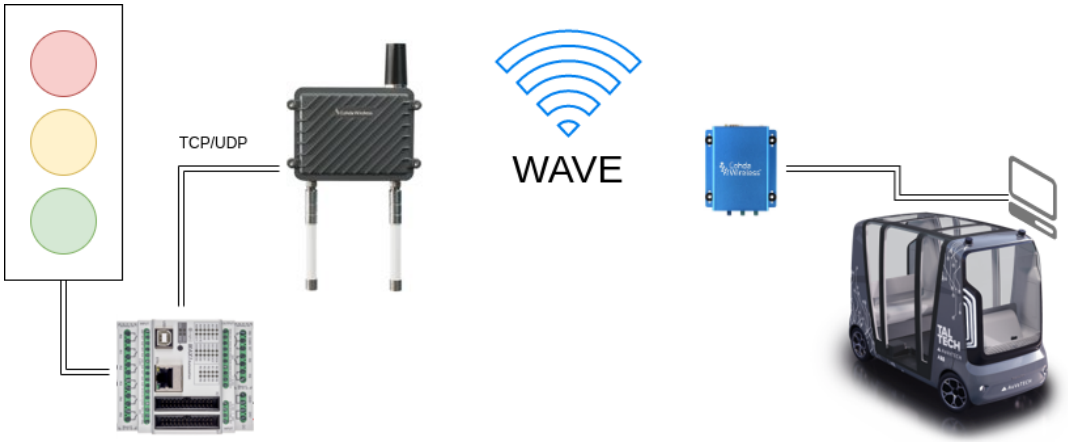

Figure 2: Communication of the roadside unit with the vehicle in the Adaptive Traffic Control Scenario

Genoa use case:

The Genoa use case focuses on two transport scenarios:

- Information to passengers (infomobility),
- Electronic and mobile ticketing,

In general, the Genoa use case focuses on the electronic services (e.g., from website or mobile application) offered to the public transport users. The high-level structure of the Genoa CPaaS architecture is provided in Figure 3.

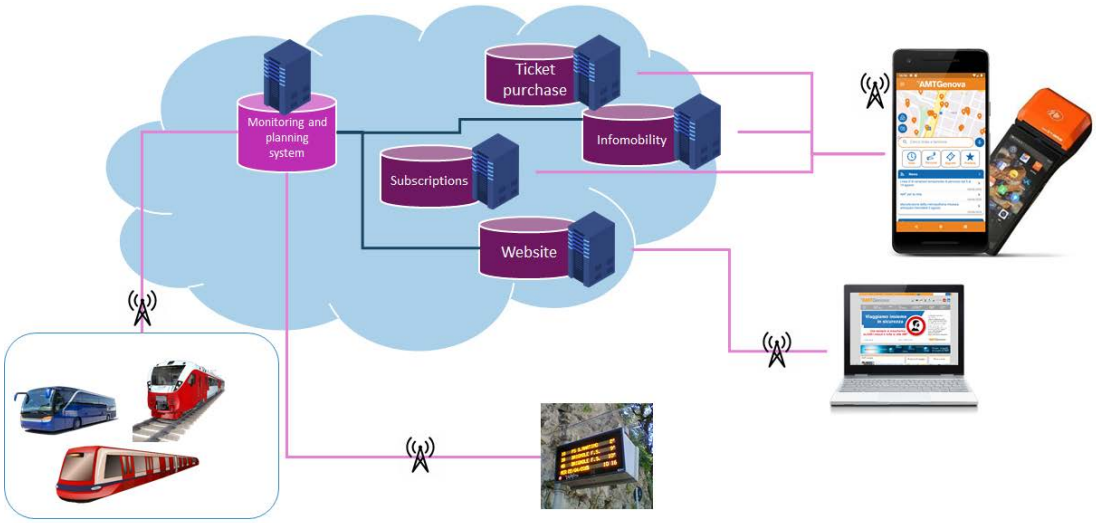

Figure 3: Genoa CPaaS high level structure

As for the Tallinn use case, for each scenario, several micro- use cases have been defined that focus on very specific situations. The micro-use cases for the Infomobility use case are:

- *Waiting time at the stop*: the means provided to a passenger to get this information when (arriving) at the stop.
- *Service schedule*: the available means for a passenger to access information regarding the service schedule, when not necessarily in the station.

- *Waiting time of the next train*: the process of providing information for the next arriving train at a station before the passenger reaches the specific station.
- *Metro Station infomobility*: the available ways of interaction and communication with passengers when inside the metro station, not actively interacting with any part of the transport system.
- *Notifications to passengers on service update*: the process of notifying the passengers of a service update through available electronic and communication means.

For the Electronic and Mobile ticketing scenario, the micro use-casesare:

- *Ticket from the mobile app*: the process of a passenger purchasing ticket from the mobile application.
- *Validating a mobile ticket*: the process for a validator to verify a ticket from its device (with the validators dedicated application).
- *Ticketing - CityPass subscription*: the process for a passenger to get a CityPass subscription from the mobile application.
- *Validating a CityPass subscription ticket*: the process for a validator to verify the subscription.
- *Ticketing Using Urban Train*: A multi-modal, multi-company scenario where a passenger wants to use the urban train transport with its CityPass subscription.

Two macro-scenarios combining all the micro-use cases have been defined:

1. All the steps for the transport of a passenger from their home in Genoa to Casella using public transportation (cf. Figure 4).
2. Re-plan scenario – during her trip, an event of a “technical problem” disrupts the provided service, so the passenger has to reschedule.

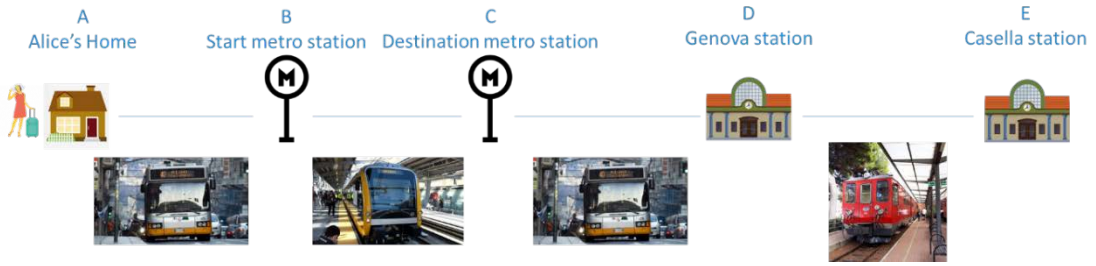

Figure 4: All considered steps for the Genoa-Casella station trip through multiple modes of public transport

2.2 Identified Basic Assets

CitySCAPE introduces a dynamic model for risk and threat analysis, where new threats and vulnerabilities can be introduced in an agile and repeatable manner to validate the assumptions made in threat analysis and updated risk analysis results.

The following assertions are made:

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

- An asset-based risk analysis and modelling approach is used. This means that threats, vulnerabilities and impacts are evaluated through asset security requirements and objectives.
- In order to create a dynamic risk model with high reuse value for other transport ecosystems or critical infrastructures, the ability to continuously include new threats and vulnerabilities is a desirable property. However, due to the fact that the system assets may be application-specific, custom, composite hardware/software/networking entities, it is practically almost impossible to expect to find external threat or vulnerability feeds for such very specific and unique systems as the ticketing system used specifically by the city of Genoa and may contain customizations that fit the needs of the transport operator. This means that a different approach should be investigated.
- In order to achieve the goal of exploiting existed threat and vulnerability feeds and knowledgebases for the set of composite application-specific assets defined in the use-cases, a hierarchical view of the assets is considered. This means that:
    - A set of basic assets is identified. These are generic asset types that are generally found in ICT platforms.
    - Relationships are defined between basic assets.
    - We can now decompose all system assets to a set of basic assets interconnected through the defined relationships. For example, "Data are generated by the Application" (Blue colour indicates basic assets, while the orange colour indicates the relationships).
    - If a system asset cannot be decomposed into basic assets, then it should be included as a basic asset.
    - Due to the generic nature of the basic assets, common third-party threat and vulnerability feeds that can be linked with the basic assets through the system components can be utilized by the risk model. Generally, assets can be of different type and may have vulnerabilities (leaving unprotected entry points for malicious acts or failures) or may be linked to vulnerabilities of system components (making them exploitable from a malicious user).
    - 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". A vulnerability of its operating system, is also a vulnerability for the server (Red colour indicates the composite asset).

Following this rationale for the CitySCAPE use cases briefly discussed in Sec. 2.1 and described in detail in (CitySCAPE, 2021) including an extensive description of the systems components and assets, the following set of basic assets was identified and additionally classified into asset groups. This CitySCAPE asset taxonomy is presented in Table 2.

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 (3rd 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 2 Basic Assets List

From this analysis we are able to define composite assets, that can fully describe each use case architecture from a high-level point of view. This is a new taxonomy, where:

a) each composite asset is composed by several basic assets, and
b) each composite asset may combine several assets identified in D2.1 (CitySCAPE, 2021) by the transport operators.

The obtained Tallinn use case Composite Assets list is provided in Table 3.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

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 3 Tallinn Composite Asset List

While for the Genoa use case, the list of Composite Assets is given in Table 4.

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

Table 4 Genoa Tallinn Composite Asset List

2.3 High-level Architecture for the two Environments

As a next step, the high-level architecture for each use case is defined using as architectural blocks the composite assets defined in Sec. 2.2. It is noted that with the use of the composite assets:

- We can provide a simplified overview of the system when considering the scenarios of the specific use case.
- All micro and macro scenarios of the use case are covered through the extracted high-level architecture.

2.3.1 Tallinn Architecture High Level Overview

The high-level architectural overview of the Tallinn use case using the extracted composite assets as building blocks is provided in Figure 5.

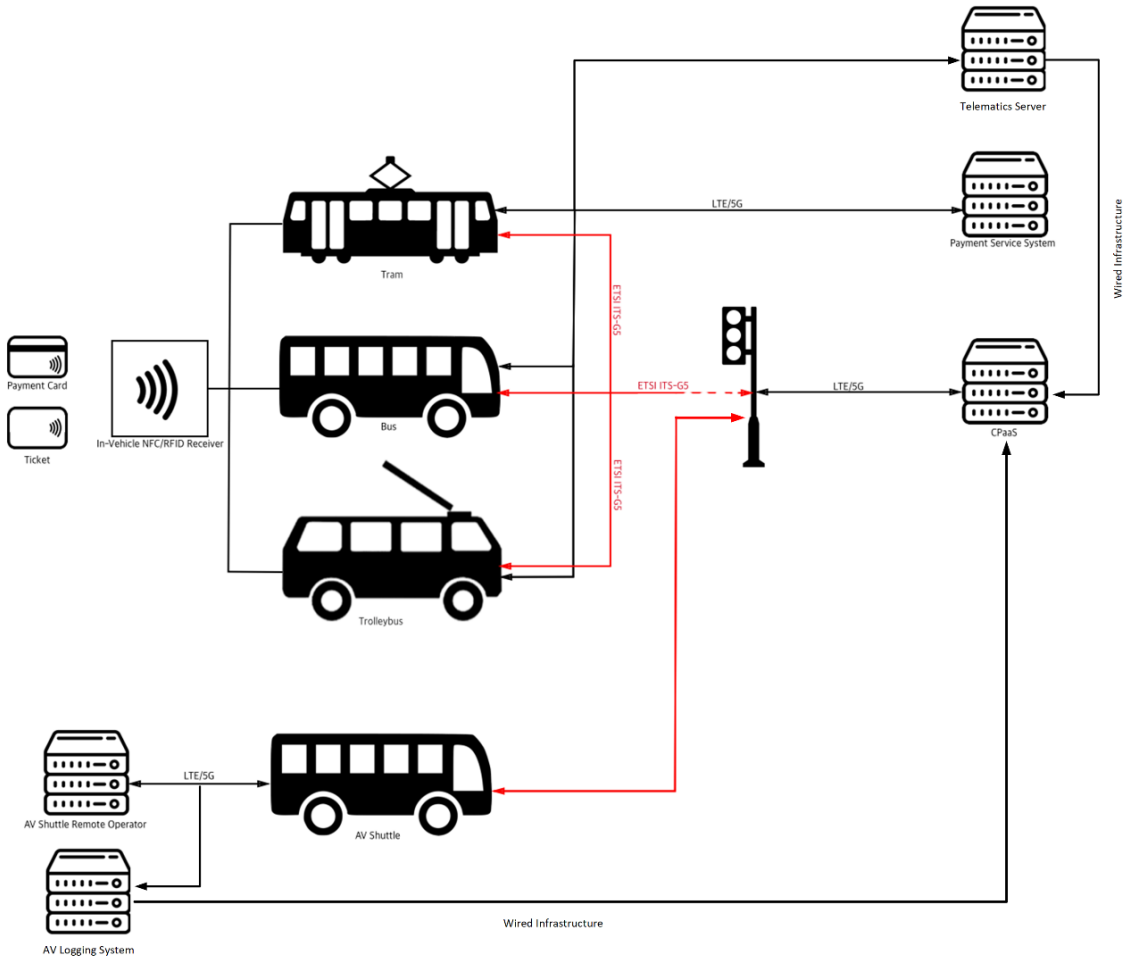

Figure 5 Tallinn Architecture High Level Overview

It is noted that the system architecture is subjected to changes as the risk modelling process of Task 2.2 is moving forward and the CPaaS implementation details of WP4 are clarified. A revised version of the architecture for both use-cases will be provided in D2.3. Some clarifications on Figure 5 are the following:

- The link between public transport vehicles and the RSU is depicted with dashed line to indicate that it is not implemented but will be used in the future.
- The CPaaS entity represents a super entity regarded as the basic coordinator-manager of the use case providing multiple services.
- The considered Tallinn use-case architecture does not focus on the interaction of passengers with mobile applications and web sites offered by the transportation authority. On the contrary, these interactions are considered objectives of the Genoa use case (Figure 6).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

The next step is to decompose each composite asset of the Tallinn architecture into basic assets based on the details provided by (CitySCAPE, 2021). This will allow us to introduce a hierarchical process for the assignment of threats, vulnerabilities and impacts for each system asset.

2.3.2 Identification of Tallinn Architecture Composite Assets

In Table 5, the public transport vehicle is investigated as an ICT platform and decomposed into basic assets. The breakdown is based on implementation details provided in D2.1 (CitySCAPE, 2021).

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
HW 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

Table 5 Basic Assets of Tram, Bus and Trolleybus Composite Assets

In Table 6, all basic components of the considered roadside unit in the Tallinn use case are presented. The breakdown is based on implementation details provided in the asset tables in D2.1 (CitySCAPE, 2021).

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
HW Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
HSM	Computational Device	AS-HW-03
Actuator	Sensors/Actuators Hardware	AS-HW-01
Sensor	Sensors/Actuators Hardware	AS-HW-01
Camera	I/O Devices	AS-HW-05
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

Table 6 Basic Assets of the Roadside Unit (RSU) Composite Asset

In Table 7, we focus on the Autonomous vehicle. It should be noted that the vehicle itself is an “extended IoT” device containing various automations. In our approach, we use the generic term sensor and actuator to describe any possible sensor or actuator installed in the vehicle and accessed by the vehicle on-board unit.

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

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

HSM Interface	Operating System	AS-OS-04
Firmware and Drivers	Operating System	AS-OS-04
HW Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
HSM	Computational Device	AS-HW-03
Actuator	Sensors/Actuators Hardware	AS-HW-01
Sensor	Sensors/Actuators Hardware	AS-HW-01
Camera	I/O Devices	AS-HW-05
HMI	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
CAN bus network interface	Network Interfaces	AS-NE-02
In-vehicle ethernet	Network Interfaces	AS-NE-02

Table 7 Basic Assets of the Autonomous Vehicle (AV) Shuttle Composite Asset

In Table 8, the remote-control system for the autonomous vehicle, the logging system and the payment service system are considered and decomposed into basic assets. It is noted that while the systems are functionally completely different, due to the fact that they provide a remote secure service, their basic/generic asset breakdown is considered identical.

Basic Asset Name	Basic Asset Type	Asset ID
Web API	Web-Based Services	AS-SO-01
Application Keys	Operation Data / Application Data	AS-DA-03
Application Data	Operation Data / Application Data	AS-DA-03
Web Service	Web-Based Services	AS-SO-01
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
HW Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
Storage	Storage	AS-HW-06
Network Controller	Network Controller (HW)	AS-NE-03
Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04

Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02

Table 8 Basic Assets of the Autonomous Vehicle (AV) Shuttle Remote Operator, AV logging System, and Payment Service System Composite Assets

In Table 9, the composite asset that is considered as the "server" for the provision of data and information for the MaaS functionalities is considered. The general term "CPaaS" is used to describe such a server. If multiple servers are considered for the full implementation of the system, multiple instantiations of the composite asset can be used – i.e., the Telemetry server can be included.

Basic Asset Name	Basic Asset Type	Asset ID
Web API	Web-Based Services	AS-SO-01
Application Keys	Operation Data / Application Data	AS-DA-03
Application Data	Operation Data / Application Data	AS-DA-03
Web Service	Web-Based Services	AS-SO-01
Application Database	Database Management Systems	AS-SO-03
Native API	Native API	AS-OS-02
VM Management Interface	Web-Based Services	AS-SO-01
Hypervisor	Operating System	AS-OS-04
OS	Operating System	AS-OS-04
OS Services	Operating System	AS-OS-04
OS Data	System Data	AS-DA-04
HW Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
Storage	Storage	AS-HW-06
Network Controller	Network Controller (HW)	AS-NE-03
Network Stack (TCP-UDP/IP)	Network Stack (SW)	AS-NE-04
Network Interface Wired (TCP-UDP /IP)	Network Interfaces	AS-NE-02

Table 9 Basic Assets of the Communications Platform-as-a-Service (CPaaS) Composite Asset and Telemetry Server

Finally, in Table 10, the communication technologies considered for the use case are presented.

Basic Asset Name	Basic Asset Type	Asset ID
LTE (4G)	Communication Technologies	AS-NE-01
5G	Communication Technologies	AS-NE-01
NFC	Communication Technologies	AS-NE-01
Ethernet (TCP-UDP/IP)	Communication Technologies	AS-NE-01
ITS-G5	Communication Technologies	AS-NE-01
CAN	Communication Technologies	AS-NE-01

Table 10 Communications Protocols of Tallinn Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

2.3.3 Genoa Architecture High Level Overview

The high-level architectural overview of the Genoa use case using the extracted composite assets as building blocks is provided in Figure 6.

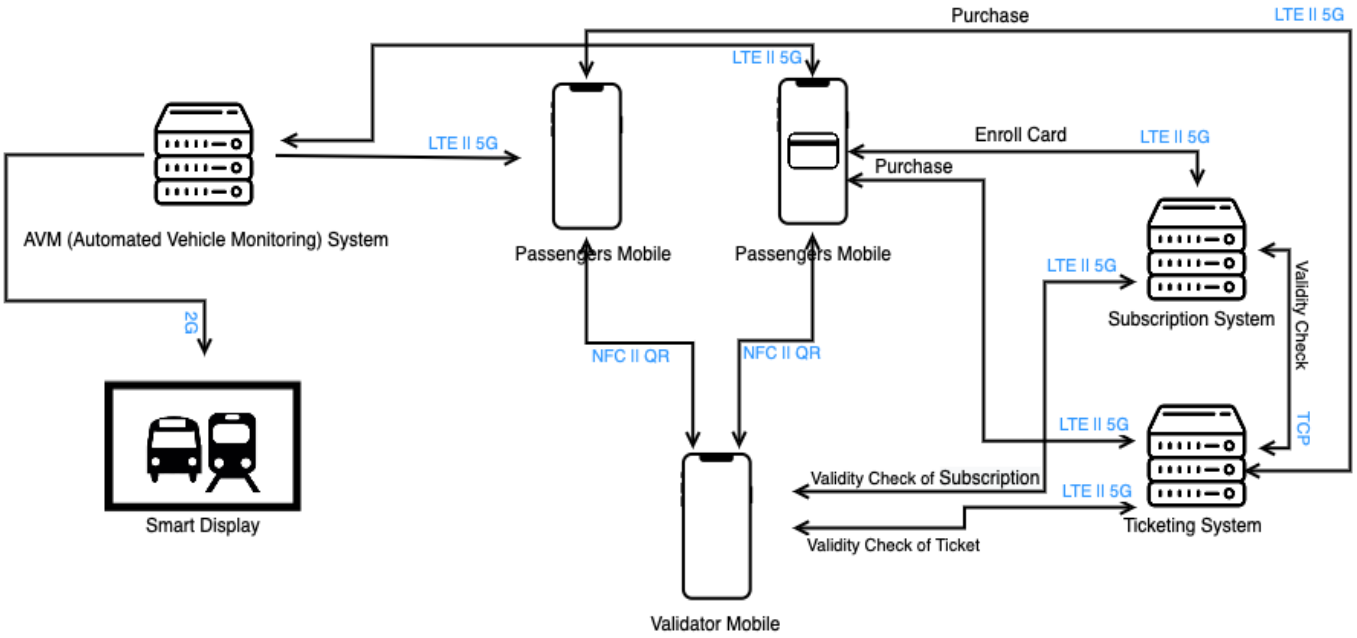

Figure 6 Genoa Architecture High Level Overview

2.3.4 Identification of Genoa Architecture Composite Assets

In Table 11, the passenger mobile device is presented as a composite asset. It is noted that while we are interested mostly in the mobile application used for the Genoa public transportation system, the risk model will take into account other aspects of the mobile device (e.g., the hosting operating system), since threats and vulnerabilities against the device components will also through propagating effects the system security.

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
HW 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

Table 11 Basic Assets of the Passenger Mobile Device Composite Asset

In Table 12, the mobile validator device is presented as a composite asset. The same modelling notes/assumptions with the passenger mobile device are also considered.

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
HW Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
Camera	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

Table 12 Basic Assets of the Validator Mobile Device Composite Asset

In Table 13, the Genoa use case servers are decomposed into basic assets. It is noted that there is no high-level operational difference between the Ticketing System, the AVM System and the Subscription System servers. Their functional difference is instantiated in the Web service and application data basic assets.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Basic Asset Name	Basic Asset Type	Asset ID
Web API	Web-Based Services	AS-SO-01
Application Keys	Operation Data / Application Data	AS-DA-03
Application Data	Operation Data / Application Data	AS-DA-03
Web Service	Web-Based Services	AS-SO-01
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
HW Interface	HW Interface	AS-HW-04
Computational Device	Computational Device	AS-HW-03
Storage	Storage	AS-HW-06
Network Controller	Network Controller (HW)	AS-NE-03
Network Stack Wired (TCP/IP)	Network Stack (SW)	AS-NE-04
Network Interface Wired (TCP/IP)	Network Interfaces	AS-NE-02

Table 13 Basic Assets of Genoa's Ticketing System, AVM (Automated Vehicle Monitoring) System and Subscription System Composite Assets

In Table 14, the Genoa smart displays are analysed as composite assets. It is noted that any notification device with computational system support besides smart displays can be modelled using the same decomposition.

Basic Asset Name	Basic Asset Type	Asset ID
Native Application	Application Software	AS-SO-02
Application Data	Operation Data / Application Data	AS-DA-03
Native API	Native API	AS-OS-02
OS	Embedded Systems Firmware	AS-OS-01
OS Services	Embedded Systems Firmware	AS-OS-01
OS Data	System Data	AS-DA-04
HW 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 GSM (2G)	Network Stack (SW)	AS-NE-04
Network Interface GSM (2G)	Network Interfaces	AS-NE-02

Table 14 Basic Assets of the Smart Display Composite Asset

Finally, in Table 15, the communication protocols considered for the use case are presented.

Basic Asset Name	Basic Asset Type	Asset ID
LTE (4G)	Communication Technologies	AS-NE-01

5G	Communication Technologies	AS-NE-01
Wired TCP/IP	Communication Technologies	AS-NE-01
NFC	Communication Technologies	AS-NE-01
GSM (2G)	Communication Technologies	AS-NE-01

Table 15 Communications Protocols of Genoa Architecture

2.4 The Asset Correlation Table – Interfaces

The decomposition of assets into basic components will allow us to investigate and model the propagation of threats and risks inside a composite asset. For example, we will be able to take into account the risks introduced by a threat-vulnerability pair at the operating system in the application or service operation.

However, the cascading threats provide more insight when we investigate their propagation between different systems (i.e., composite assets) or even entities composed as groups of composite assets. In order to be able to consider the possibility for a cascading threat, the interconnections between the various composite assets/systems should be identified and taken into account.

The Asset Correlation or Transition (AT) matrix is a data structure (see Table 16 and Table 17) that essentially represents the various feasible ways/interconnections to outreach from one asset to another. The system architecture determines those ways (see Figure 5 and Figure 6 and will be furtherly analysed by the vulnerability analysis contained in D2.3 that follow), i.e., allowing only the transitions that are accommodated by the underling available communication links (e.g., in-vehicle network, V2X short-range communication links, cellular communication links, wired networks, etc.) established in the setting defined by the use cases.

Given a realisation of a threat in any system asset (shown as AS-xx, where xx is the asset's identifier) in the yellow column of Table 16 and Table 17, we identify all other system assets (light blue row) which can be affected. In the AT matrix, a connection between assets (therefore a potential threat propagation) is represented by an interface code, while the absence of connection with (-). It is noted that the Asset Transition Matrix Table 16 and Table 17 represent a specific instantiation of the system architecture. This means that a different Asset Transition matrix may be investigated without changing the followed algorithmic approach.
A number of assumptions have been adopted to derive certain entries of the above matrix. Those are summarised in the following points:

- The considered software instances (appearing in numerous locations across the CitySCAPE ecosystem) cannot harm the underlying hardware.
- Chain transitions should be considered when 'traversing' matrix i.e., asset A may reach asset C through asset

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Composite Asset ID	COM-TAL-AS-01	COM-TAL-AS-02	COM-TAL-AS-03	COM-TAL-AS-04	COM-TAL-AS-05	COM-TAL-AS-06	COM-TAL-AS-07	COM-TAL-AS-08	COM-TAL-AS-09	COM-TAL-AS-010
COM-TAL-AS-01	-	3G/LTE/5G	-	-	ETSI-ITS-G5	ETSI-ITS-G5	ETSI-ITS-G5	ETSI-ITS-G5	3G/LTE/5G	-
COM-TAL-AS-02	3G/LTE/5G	-	-	-	-	-	-	-	-	
COM-TAL-AS-03	-	-	-	-	3G/LTE/5G	-	-	-	Wired infrastructure	Wired infrastructure
COM-TAL-AS-04	-	-	-	-	-	3G/LTE/5G	3G/LTE/5G	3G/LTE/5G	-	-
COM-TAL-AS-05	ETSI-ITS-G5	-	3G/LTE/5G	-	-	ETSI-ITS-G5	ETSI-ITS-G5	ETSI-ITS-G5	-	-
COM-TAL-AS-06	ETSI-ITS-G5	-	-	3G/LTE/5G	-		ETSI-ITS-G5	ETSI-ITS-G5	-	3G/LTE/5G
COM-TAL-AS-07	ETSI-ITS-G5	-	-	3G/LTE/5G	-	ETSI-ITS-G5	-	ETSI-ITS-G5	-	3G/LTE/5G
COM-TAL-AS-08	ETSI-ITS-G5	-	-	3G/LTE/5G	-	ETSI-ITS-G5	ETSI-ITS-G5	-	-	3G/LTE/5G
COM-TAL-AS-09	3G/LTE/5G	-	Wired infrastructure	-	-	-	-	-	-	-
COM-TAL-AS-10	-	-	Wired infrastructure	-	-	3G/LTE/5G	3G/LTE/5G	3G/LTE/5G	-	-

Table 16 Tallinn Composite Assets Interconnections via Network Interfaces

Composite Asset ID	COM-GEN-AS-01	COM-GEN-AS-02	COM-GEN-AS-03	COM-GEN-AS-04	COM-GEN-AS-05	COM-GEN-AS-06
COM-GEN-AS-01	-	3G/LTE/5G	2G	-	-	3G/LTE/5G
COM-GEN-AS-02	3G/LTE/5G	-	-	3G/LTE/5G	3G/LTE/5G	NFC or QR
COM-GEN-AS-03	2G	-	-	-	-	-
COM-GEN-AS-04	-	3G/LTE/5G	-	-	TCP/IP	3G/LTE/5G
COM-GEN-AS-05	-	3G/LTE/5G	-	TCP/IP	-	3G/LTE/5G
COM-GEN-AS-06	-	NFC or QR	-	3G/LTE/5G	3G/LTE/5G	-

Table 17 Genoa Composite Assets Interconnections via Network and Other Interfaces

3 THREAT ANALYSIS

To assess cybersecurity risks on the relevant use cases of CitySCAPE architectures, a set of threats mostly from ENISA (Ross, et al., 2017; Hogben & Dekker, 2010; Perilli, et al., 2009; Lourenço, Marinos, & Patseas, 2020; Marinos, 2013; ENISA, 2019) and other sources (Fischer, Markscheffel, Frosch, & D. Buettner, 2012) were used.

The threat analysis results also took into account the cross-domain, generic threat investigation presented at CitySCAPE deliverable D2.2 ("Analysis NIS directive Cross-domain threats and proof of concepts"). It is noted that the associations and correlations between threats and assets (basic or composite) are not presented in this deliverable, but are part of the complete risk and threat analysis performed in the context of D2.3 ("Multimodal Transport System: System Modelling, Risk Analysis and Management, GDPR Compliance"). The threats in the current document are presented in order to support the cascading threat methodology presented in Sec. 4. It is also noted that, the list contains threats that are not relevant to cyber-security (e.g., natural disaster) and may be considered out of scope. Nevertheless, the unavailability of a resource or component from e.g., a physical attack may be a traceable event for the CitySCAPE platform.

The identified threats of the Genoa and Tallinn architectures cover several categories, as Table 18 shows, such as network, software, hardware, and physical threats. Besides the threats and their description, their possible impact on Confidentiality, Integrity or Availability (represented by columns C, I and A in the table) is identified and denoted.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

3.1 Identification of Threats

Type	Threat ID	Threat	Impact			Description
			C	I	A	
SW	TH-01	Malware Injection	X	X	X	Software programs are designed to carry out unwanted and unauthorised actions on a system without the consent of the user, resulting in damage, corruption, or information theft. Its impact can be high.
SW/NET	TH-02	Denial of Service			X	Multiple systems attack a single target in order to saturate it and make it crash. This can be done by making many connections, flooding a communication channel, or replaying the same communications over and over.
DATA	TH-03	Modification of Information / Data Manipulation	X	X	X	In this case, the objective is not to damage the devices, but to manipulate the information in order to cause chaos or acquire monetary gains. Or the objective is to manipulate the data in order to modify data, cause the failure of the software, or acquire monetary gains. By accessing the operation data of the system, an attacker may modify them to alter the operation of the application for malicious purposes
NET	TH-04	Man in the Middle	X	X	X	Active eavesdropping attack, in which the attacker relays messages from one victim to another, in order to make them believe that they are talking directly to each other

NET	TH-05	Interception of Information	X			Unauthorised interception (and sometimes modification) of private communication, such as phone calls, instant messages, e-mail communications and network transactions.
NET	TH-06	Replay of Messages		X	X	This attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.
NET	TH-07	Network Outage			X	Interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected, and on the time required to recover, the importance of this threat ranges from high to critical.
HW	TH-08	Failures of Devices			X	Threat of failure or malfunction of hardware devices
SW/NET	TH-09	Failure of System			X	Threat of failure of software services or applications
NET	TH-10	Loss of Support Services			X	Unavailability of support services required for proper operation of the information system
SW/NET	TH-11	Software Exploitation / Malicious Code Injection	X	X	X	The most common devices are often vulnerable due to weak/default passwords, software bugs, and configuration errors, posing a risk to the network. This threat is usually connected to others, like exploit kits, and it is considered crucial.
HW	TH-12	Natural Disaster			X	These include floods, heavy winds, heavy snows, and landslides, among other natural disasters, which could physically damage the devices.
HW	TH-13	Environmental Disaster			X	Disasters in the deployment environments of ~~IoT~~ equipment and causing their inoperability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

HW/SW	TH-14	Device Modification	X	X	X	Tampering a device by, for example, taking advantage of the bad configuration of ports, exploiting those left open.
HW	TH-15	Device Destruction (Sabotage)			X	Incidents such as devices theft, bomb attacks, vandalism or sabotage could damage devices
HW	TH-16	Device Loss or Theft	X			The device is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.
DATA	TH-17	Unintentional Disclosure of Data	X			The smartphone user unintentionally discloses data on the smartphone.
HW	TH-18	Attacks on Decommissioned Device	X			The smartphone is decommissioned improperly allowing an attacker access to the data on the device.
NET	TH-19	Phishing Attacks	X	X	X	An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.
NET	TH-20	Network Spoofing	X	X	X	An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.
SW/NET	TH-21	Resource Exhaustion/Lack of resources			X	Cloud services are on-demand services [see Cloud computing - working definition]. Therefore, there is a level of calculated risk in allocating all the resources of a cloud service because resources are allocated according to statistical projections.

SW	TH-22	Isolation/Virtualization Abuse	X	X	X	Multi-tenancy and shared resources are two of the defining characteristics of cloud computing environments. Computing capacity, storage, and network are shared between multiple users. This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure (e.g., so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks).
SW/NET	TH-23	Management Interface Compromise	X	X	X	The management interfaces of the cloud infrastructures are usually Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.
HW/SW/NET	TH-24	Unauthorized Access to Premises	X	X	X	–
SW/NET	TH-25	Abuse of Authorization / Privilege Escalation	X	X	X	Abuse of authorised access systems that support the infrastructure, making it possible to modify the version of the software and the tools during the process of software. The threat of unauthorised manipulation of hardware and software that can be used to modify source code for malicious purposes, posing threats such as bomb injections, backdoor generation, or the destruction of source code. An unauthorised modification of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

						configuration data could cause the system to work incorrectly, or the security measures implemented may not act correctly, allowing attacks against the system. Unauthorised modification of code or data, attacking its integrity. In this case, it can result in the manipulation of information, unauthorised access to confidential information, and access to source code.
DATA	TH-26	Abuse of Authorization / Privilege Escalation	X		X	Loss of Source code, Configuration data, Test data, Production data, Documentation, Backup Data, Third-Party Data, Training data
SW/NET	TH-27	Abuse of Authentication	X	X	X	Authentication traffic spikes or Abuse of user authentication/authorisation data by third parties' personnel or Abuse of the application management function (AMF) authentication and key agreement procedure or abuse the credentials of existing accounts
SW/NET	TH-28	Identity Theft	X	X		An attacker can use, deliberately, the identity of a person involved in the transport ecosystem, through for example the stealing of credentials, to obtain financial gain, critical information, unauthorised access to a system, etc. The "fake president" fraud, using the identity of powerful people in the ecosystem, can have a serious impact.

SW/NET	TH-29	Social Engineering	X	X	X	An attacker can use human interaction to obtain or compromise information about the transport system and transport processes: by asking questions, by pretending to be another person, the attacker can piece together information he needs to infiltrate the port systems. The attacker can ask several sources by relying on the information he can get from the first source to add to his credibility or sending malicious links. Phishing attacks are the most common social engineering attack: hackers use email or malicious websites to solicit personal information by posing as a trustworthy organisation. Other forms exist: vishing attack (though voice communication), smishing attack (exploitation of SMS, text, messages containing malicious link, etc.)

Table 18 List of Identified Threats of Genoa and Tallinn Architectures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

4 A NOVEL METHODOLOGY FOR CASCADING THREATS

4.1 Risk management approach

Everyone takes and manages risks all the time, balancing potential rewards against uncertain losses. Risk management remains nevertheless a very difficult process. It requires combining the hard-science approach, who treats risks as something that can be objectively measured, with the view of the soft- and social- science who argues that risk is a fuzzy concept and the propensity to take risks is in part culturally constructed.

Risk is the effect of uncertainty on objects (ISO/IEC 27000, 2018). It is the chance of something going wrong as a result of a hazard or a threat which has an impact on operations. Risks arise out of uncertainty. A risk is measured in terms of its likelihood of happening and the consequences if it should happen.

Risk management is the coordinated activity to direct and control an organisation with regard to risk (ISO/IEC 27000, 2018). It is balancing the cost of avoiding, reducing, transferring or accepting a risk with the consequences that can be expected from taking the risk. The term risk management is used in a wide variety of disciplines, and itself also combines concepts and techniques from a range of fields like statistics, economics, operations research and decision theory.

Unfortunately, there are no standards for defining vulnerabilities and threat-sources, assigning and combining impact and probability ratings, or introducing the impact of controls in the field of information security related risk management. Generally, vulnerabilities and threats may be unique to specific implementations and environment and it may be impossible to identify and classify them all. Under this perspective and due to many implementation differences, it is not easy to get consensus in order to pursue standardization.

Recent standards and recommendations on the management of information systems and organising the protection of information security within an organisation widely recognise the importance of information security related risk management.
There is a variety of views and descriptions of the processes that risk management involves, the way it should be conducted and what is aimed at. As defined by NIST: 800-53 (2020) and ISO/IEC 27001 (2013), we adopt a model for the risk management process which includes three risk management stages: initiation, risk analysis and risk mitigation.

Figure 7: Risk Management stages

The stage of **initiation** aims mainly at:

- defining the context of the risk management process;
- at setting the scope of the analysis; in other words, the information system that is the target of the evaluation, its boundaries and environment and
- at establishing the risk management team.

The characterisation of the information system must be as complete as possible and most often includes the following elements:

- Hardware (e.g., servers, workstations, network equipment);
- Software (e.g., operating systems, system services, application software);
- Connectivity (internal and external);
- The information system's mission;
- The information that is managed by the system and its requirements regarding availability, integrity and confidentiality;
- Support staff and users; and
- Existing controls: technical controls (e.g., user identification and authentication equipment, encryption hardware and software), management controls (e.g. security policy, acceptable use policy), operational controls (e.g. backup and contingency operations, off-site storage, user account creation and deletion procedures), physical security environment (e.g. site security, data centre policies), environmental security (e.g. controls for power, temperature, humidity).

During this stage the appropriate risk management methodology is also selected.

Risk analysis (or risk assessment since these terms are considered synonymous), which comprises three processes: risk identification, risk estimation and risk evaluation as shown in Figure 2.

Risk identification refers to the process of identifying risks that pose threats to the assets that need to be safeguarded. Therefore, it is necessary, at this phase, to identify the assets to be protected, possible associate threats to these assets and identify their vulnerabilities.

Risk identification is followed by *risk estimation* which is the process of quantifying – putting values on – the risks that have been identified. Commonly, risks are quantified

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

by measuring the probability of their occurrence (P) and estimating their possible business impact or cost (C); thus, in the risk analysis process, the risk is calculated as: R = P * C.

Finally, during the *risk evaluation* process, options for the treatment of the risks are identified and the level of tolerance is determined. Possible options include risk transfer (transfer risk to third parties), risk acceptance (no control of the risk), risk avoidance (if applicable, the asset is not exposed to the risk) and risk reduction (selection of appropriate control measures) (ISO/IEC 27001, 2013).

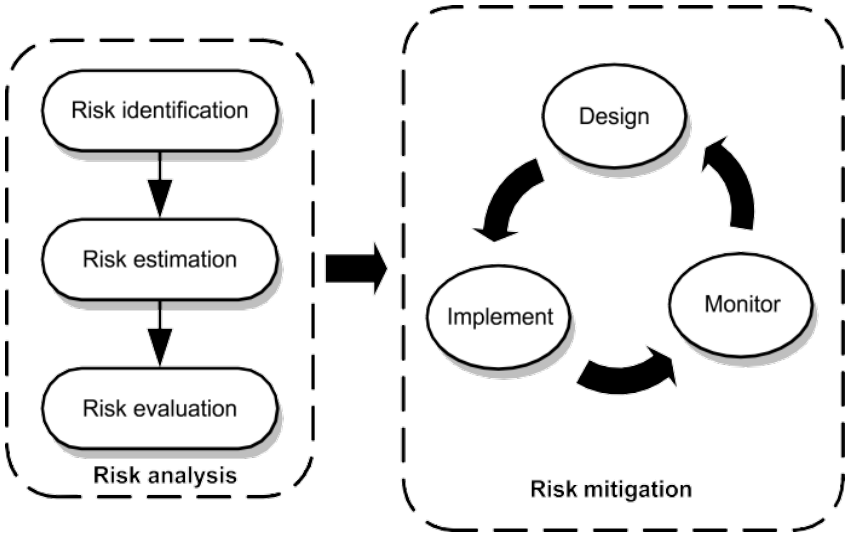

Figure 8: Risk analysis steps and risk mitigation circle

Based on the system and context description available at the end of the previous step, the vulnerabilities that apply to the target of the evaluation are identified. A *vulnerability* is a weakness of an asset or control that can be exploited by one or more threats (ISO/IEC 27000, 2018). It can be expressed as any flaw or weakness in the design of a system, in its implementation or in the controls that are in place to protect it and that can result in damage when it is accidentally triggered or intentionally exploited.

A *threat-source* is either the combination of the intent and the means to intentionally exploit a vulnerability (e.g., a thief, a disgruntled employee) or a situation that may accidentally trigger a vulnerability (e.g., an earthquake, a sloppy user). A *threat* is a potential cause of an unwanted incident, which may result in harm to a system or organisation (ISO/IEC 27000, 2018). It is the potential for a threat-source to accidentally trigger or intentionally exploit vulnerability. When for a given vulnerability there is no threat-source that has the technical ability or motivation to exploit it, there is no threat. Likewise, when there is no vulnerability present for which a given threat-source has the necessary skills, time and budget, this threat source poses no threat.

Each threat is, after that, matched with the list of controls that were identified in the first phase, and that mitigate the likelihood of a vulnerability being exercised or reduce the impact of such an adverse event when it occurs.

The risks that were identified, must be further analysed, so that the minor, acceptable risks can be separated from the major risks which must absolutely be eliminated or reduced. This involves deriving for each risk an overall likelihood rating that indicates the probability that the vulnerability may be exercised by the corresponding threat-source. The second element in risk assessment is trying to rate the adverse impact of the vulnerability when it was to be exercised. This rating will be based on an evaluation of the loss or degradation of integrity, availability, and confidentiality of the information that is threatened by the vulnerability.

When determining the probability and impact of a threat, the existing controls that reduce the likelihood or impact and their adequacy have to be taken into account. The combination of probability and impact will finally be translated into a single level of risk to the information system.

Risk mitigation, the final stage of the risk management process, involves prioritising, evaluating, and implementing the appropriate risk-reducing controls that have been identified during the risk analysis process. Risk mitigation also includes the processes of monitoring and evaluating the effectiveness of risk controls (ISO/IEC 27001, 2013). Three tasks are included in the stage of risk mitigation:

- design;
- implement; and
- monitor (Figure 2).

These three tasks are individually discussed in more detail in the following.

- Design. The process of risk mitigation includes the specification of security objectives and the establishment of security policies and processes relevant to controlling risk. Currently applied countermeasures and policies, if any, are identified and evaluated in comparison to the results of risk analysis (e.g., the emergence of new risks). If required, additional control measures are specified and designed, accompanied by the timeframe over which they should be implemented.
- Implement. The task of implementation involves the application of the selected control measures and procedures. It also includes the management of resources required for implementing these measures (people, time, money, operations). Security awareness programs are also included in this process, aiming at fostering an appropriate risk and security culture.
- Monitor. The process of monitoring follows the implementation of the selected countermeasures. Its purpose is to ensure that the control measures are operating effectively and as intended. It includes:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

- processes for the prompt detection of errors and security incidents,
- mechanisms that examine whether documented procedures are being followed; and
- reviews aiming at the evaluation of implemented controls' efficiency.

It also includes the reassessment of the level of residual risk, after considering possible changes that might occur to the organisational processes or the business objectives.

Risks can be handled in a number of ways:

- Risk Avoidance: This means simply not performing the activity that carries the risk. Unfortunately, this also typically means losing out on the potential gain that performing the activity might have produced.
- Risk Reduction: This involves approaches that reduce the probability of the vulnerability being triggered or reduce the impact when the vulnerability is triggered. Reducing a risk most often involves putting in place controls.
- Risk Transfer: This means passing the risk on to another party that is willing to accept the risk, typically by contract or by hedging. Insurance is an example of risk transfer using contracts.
- Risk Acceptance: This means accepting the loss when it occurs. Risk acceptance is a viable strategy for small-impact risks where the cost of insuring against the risk would be greater over time than the total losses sustained. Also, all risks that are not avoided nor transferred, and that one does not can or wish to reduce any further, automatically fall under this category. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible.

The combination of methods used to handle each of the risks that were identified, analysed and treated, leads to a risk management plan that must then be implemented. Risk management can be performed once for a given system, for instance before it comes in operation, and then periodically updated during the lifetime of the system. The back coupling is in this case not permanent but rather periodically triggered. Risks management can however also be conceived as a continuous process and influence decision-making at all instances through the life of the system.

4.2 Cascading Threats in Critical Infrastructures (Threat Modelling)

The modelling and analysis of interdependencies between critical infrastructure elements is a very important field of study (P. Pederson, 2006). Much effort is currently being spent to develop models that accurately model simulate critical infrastructure behavior and identify interdependencies and vulnerabilities. The results of these models are used by private companies, government agencies, military, and communities to plan for expansion, reduce costs, enhance redundancy, improve traffic flow, and to prepare for and respond to emergencies.

Modern infrastructures are often depended on other infrastructures to function properly, or even locally in one infrastructure, one information system depends on the correct operation of some other. This necessity has led to the development of complex networks of interdependent infrastructures. These dependency graphs reveal information on what will happen if a failure occurs; in other words, they are as safe as their most critical path of interdependencies and as exposed as their most dangerous node. For example, as far as the dangers of interdependent infrastructures are concerned, Rinaldi, Peerenboom and Kelly in (S. M. Rinaldi, 2001) provide a visual presentation of the well-known electric failure scenario of California which is a real-case example of a multi-order dependency between CIs. The electric power disruptions in California caused cross-sectoral cascading effects, as power disruptions affected natural gas production, operation of petroleum product pipelines transporting gasoline and jet fuel along with the operation of massive water pumps for crop irrigation.

Concerning software and its dangers in Critical Infrastructure information systems, one should look no further than the incident with the security worm, Stuxnet. The Stuxnet incident was a typical example of software being able to misuse functionality in machinery and manifest catastrophic failures across multiple infrastructures. Many Critical Infrastructures use Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) as control locations, in order to handle the machinery and functionality of an infrastructure (e.g., valves, sensors, breakers, etc.). Thus, a failure on any one of them may affect the operation of the entire infrastructure and start a cascading event, where multiple CIs fail due to their dependencies.

When industrial SCADA systems started to be connected with the Internet, these control systems were exposed to various vulnerabilities and threats (Krutz, 2005). Built as standalone, isolated control systems, they lacked the proper security measures needed to support a robust and safe functionality over the Internet. For example, an over-the-Internet, man-in-the-middle attack on a green diesel generator that led to a total meltdown has been presented in the literature (Alcaraz, 2011) .

Therefore, it is clear that to take into account the cascading threats, the risk identification process performed during the risk analysis (as described above) should not be restricted to the independent risks/threat sources against stand-alone assets. It should consider all potential threat-sources, globally for the system and not only for each specific asset. These threat-sources may be internal or external (coming from some other CI). In case that a threat-source pauses a risk to any part (asset) of the system and achieves to exploit a vulnerability (intentionally or accidentally), thus causing an incident that will harm (have some kind of impact) the organisation, it is necessary to investigate if the caused impact will become a new threat-source for other components of the system.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

The combination of methods used to handle each of the risks that were identified, analysed and treated, leads to a risk management plan that must then be implemented. Risk management can be performed once for a given system, for instance before it comes into operation, and then periodically updated during the lifetime of the system. The back coupling is in this case not permanent but rather periodically triggered. Risks management can however also be conceived as a continuous process and influence decision-making at all instances through the life of the system.

To work towards this direction and take into account the potential cascading effect of threats or of the consequences that an incident may have caused, we have identified, through the use cases of Tallinn and Genoa, a set of "***Primary Threats***" (Table 18), i.e., threats that they are standalone and may appear without requiring any conditions (prerequisites) to have been met.

4.2.1 Threat Sequence and Transformation (TST) graph

The CitySCAPE use cases TST graph relies on the identified threats of Sec. 3. The graph includes all possible paths of threat propagation. Each threat is represented by a red node in Figure 9 and its potential evolution to another one is depicted with directional arrows (practical example: the threat of Unauthorized Access to premises can be evolved in the threat Device Destruction – Sabotage).

Those transitions are determined in line with typical cyber-security engineering practices. In certain cases, there are green rectangles that offer a logical justification in terms of impact, for a number of transitions; those yellow boxes are only used for the sake of clarity rather than any kind of calculation. The arrows suggest a certain sequence of transitions that finally reach "absorbing" nodes/states (*e.g.*, Denial of Service). Along these lines, certain threats, such as the Targeted Cyber Attacks may trigger multiple other threats (*e.g.*, Manipulation of Information, Denial of Service, Malware).

The TST is a CitySCAPE novelty and it is composed of nodes and arrows. There are three kinds of nodes:

- Primary threats – depicted as red circles,
- Primary threats with repeated occurrence due to their correlation with several impacts – depicted as orange circles,
- Impacts (relevant to the cascading threats) – depicted as green rectangular.

There are two kinds of arrows:

- Black arrows indicating evolution of threats or correlation of threats and impacts.
- Orange arrows indicating transformation of impacts.

Given an initial threat occurrence, all the (potentially) emerging threats can be identified by traversing the graph. In parallel, the aforementioned green rectangles of the TST graph suggest the potential impact on the system, if a threat is realised. Two impact types are identified:

- Direct impact from threats (*e.g.*, Man in the Middle attack causes Loss of Transmitted Data)
- Indirect impact from other impacts (*e.g.*, Loss of Transmitted Data causes Loss/Unavailability of Stored Data), represented by the yellow arrows.

On a more general note, the threat propagation model itself is system-agnostic; although tailored for the needs of the CitySCAPE multimodal ecosystem and validated for the CitySCAPE use-cases, the graph can find applicability to all assets across a variety of IT systems.

Going back to the definition of primary threats, they are depicted in the following figure as the Red Circles. As already mentioned, each of those threats can appear independently but at the same time it can be noticed that there are also chains of Threats, in the sense that the appearance of a specific threat can generate secondary threats that may harm the system. *As an example, consider the Threat of a "Natural Disaster". This is clearly a threat that can occur at any time without any preconditions. A natural disaster can trigger a secondary threat which is "Failure of Devices" that will certainly affect the operation of the system. However, the "Failure of Devices", as a primary threat, can also occur independently of a natural disaster. Thus, each primary threat, either independently or as part of a Threats' chain, should be considered in terms of the impact that it could potentially cause to the system.*

In order to support the identification of the potential consequences that an incident may cause to the system, Table 20 lists the impact that each threat may have on the assets it can impact. Clearly, the impact concerns the availability, integrity and confidentiality of processed/stored/transmitted data, as well as the availability of the offered services. In the following figure, the impact caused by a threat/chain of threats is depicted in rectangles.

The fact that an incident's impact may also affect an asset that is not directly connected to the threat that has caused the incident (due to cascading effect) is also modelled in Figure 9 by orange arrows. For instance, the "Man-in-the-Middle" threat over a communication protocol, may have an impact of "Modification of Transmitted Information". Clearly this will also affect the integrity of the data that will be stored in the destination asset. Thus, the initial threat, against the communication protocol, has propagated and affected a different asset (i.e., a database). This cascading effect also applies when disclosure of transmitted data may lead to partial leakage of the generated, processed, or stored data of the component that transmits them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Finally, it is important to note that the aforementioned concept of cascading effects applies both internally to an information system (from one asset to another asset) and from one critical infrastructure to another. So, it can apply to cases where the consequences of an incident on a critical infrastructure affect the operation of another critical one. Using the same principles as described in the previous paragraph (how a threat, through its impacts, can affect another asset), we can model the impact that a transmitted data sent to an external system can have and so how the consequences of the original Threat propagate to another potentially critical infrastructure.

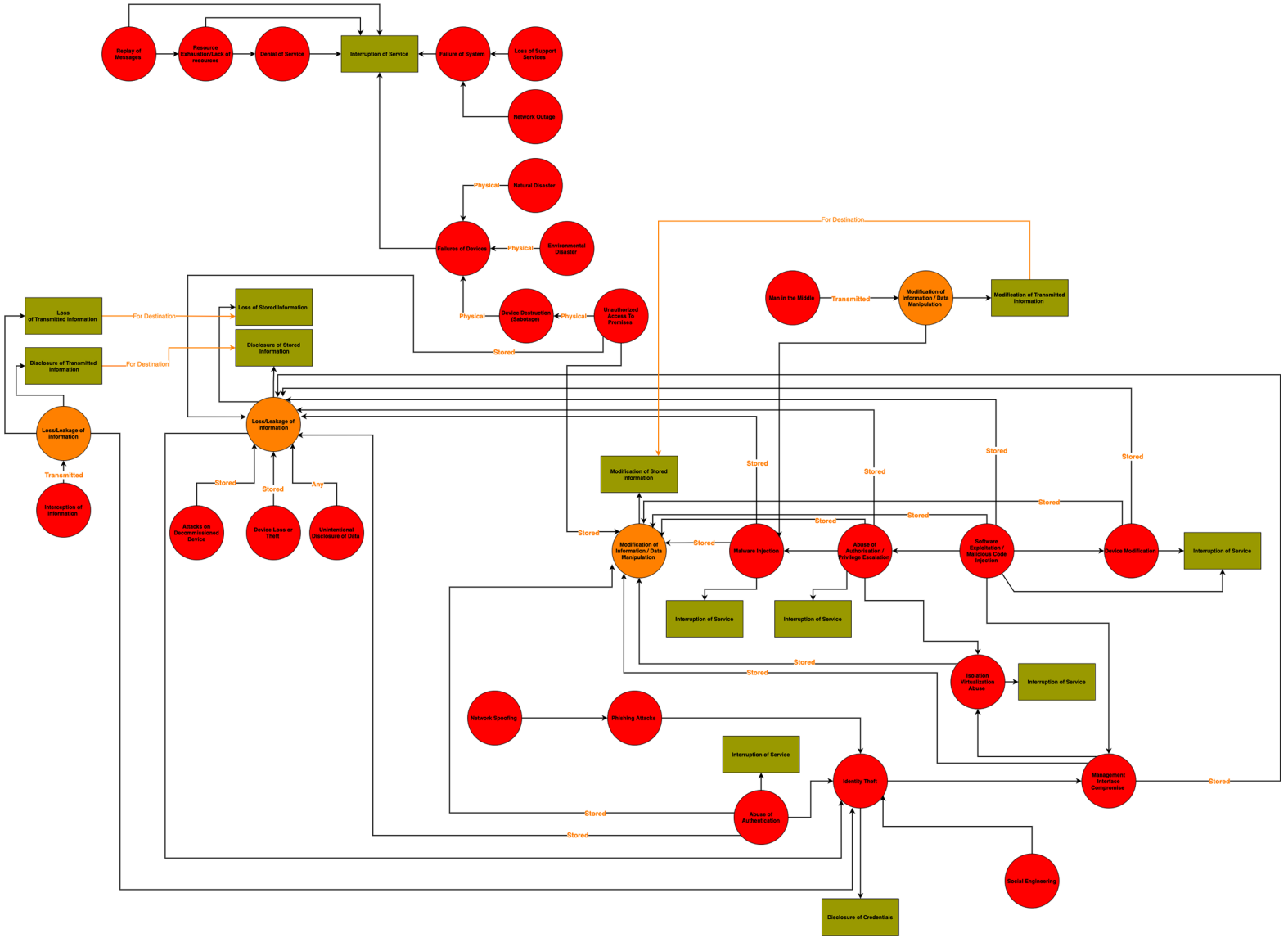

Figure 9: Cascading Threats of CitySCAPE Architectures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

4.3 Interconnected Threats and Impacts

The following matrices provide a lookup table that can be used to investigate and examine the instantiation of the cascading threat methodology depicted in Figure 9 for the CitySCAPE use cases

First of all, in Table 19, the set of Impacts that are identified as a cause/transformation for threat propagation are presented. The following notes can be made:

- A threat may also cause other additional impacts. However, for the CitySCAPE use cases, only the impacts in the following list can cause a cascading threat phenomenon.
- In Figure 9, there is a "specialization" of the impacts in stored or transmitted information in order to indicate data in move or rest, and how the propagation mechanism works. Thus, the loss of transmitted data for a component/asset will be "transformed" to loss of received or stored data for the destination.

Impact ID	Impact
IM-01	Disclosure of Information
IM-02	Modification of Information
IM-03	Loss of Information
IM-04	Interruption of Service
IM-05	Disclosure of Credentials

Table 19 Identified Impacts of CitySCAPE Architectures

In Table 20, the association between the threats and the cascading-threat-causing impacts is presented.

Table 20: Correlations of CitySCAPE Threats with Impacts

Threat ID	Threat	Impact ID	Impact
TH-01	Malware Injection	IM-03	Loss of Information
		IM-01	Disclosure of Information
		IM-02	Modification of Information
TH-02	Denial of Service	IM-04	Interruption of Service
TH-03	Modification of Information / Data Manipulation	IM-02	Modification of Information
TH-04	Man in the Middle	IM-03	Loss of Information
		IM-02	Modification of Information
TH-05	Interception of Information	IM-01	Disclosure of Information
TH-06	Replay of Messages	IM-04	Interruption of Service
TH-07	Network Outage	IM-04	Interruption of Service

TH-08	Failures of Devices	IM-04	Interruption of Service
TH-09	Failure of System	IM-04	Interruption of Service
TH-10	Loss of Support Services	IM-04	Interruption of Service
TH-18	Data / Sensitive Information Leakage		
TH-11	Software Exploitation / Malicious Code Injection	IM-01	Disclosure of Information
		IM-02	Modification of Information
		IM-04	Interruption of Service
		IM-03	Loss of Information
TH-12	Natural Disaster	IM-04	Interruption of Service
TH-13	Environmental Disaster	IM-04	Interruption of Service
TH-14	Device Modification	IM-01	Disclosure of Information
		IM-02	Modification of Information
		IM-04	Interruption of Service
		IM-03	Loss of Information
TH-15	Device Destruction (Sabotage)	IM-03	Interruption of Service
TH-16	Device Loss or Theft	IM-01	Disclosure of Information
TH-17	Unintentional Disclosure of Data	IM-01	Disclosure of Information
TH-18	Attacks on Decommissioned Device	IM-01	Disclosure of Information
TH-19	Phishing Attacks	IM-05	Disclosure of Credentials
TH-20	Network Spoofing	IM-01	Disclosure of Information
		IM-02	Modification of Information
TH-21	Resource Exhaustion/Lack of resources	IM-04	Interruption of Service
TH-22	Isolation/Virtualization Abuse	IM-01	Disclosure of Information
		IM-02	Modification of Information
		IM-04	Interruption of Service
		IM-03	Loss of Information
TH-23	Management Interface Compromise	IM-01	Disclosure of Information
		IM-02	Modification of Information
		IM-04	Interruption of Service
		IM-02	Loss of Information
TH-24	Unauthorized Access To Premises	IM-01	Disclosure of Information
		IM-02	Modification of Information
		IM-04	Interruption of Service
		IM-03	Loss of Information
TH-25	Abuse of Authorisation / Privilege Escalation	IM-01	Disclosure of Information
		IM-02	Modification of Information

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

		IM-04	Interruption of Service
		IM-03	Loss of Information
TH-26	Loss/Leakage of information	IM-01	Disclosure of Information
TH-27	Abuse of Authentication	IM-01	Disclosure of Information
		IM-02	Modification of Information
		IM-03	Loss of Information
TH-28	Identity Theft	IM-05	Disclosure of Credentials
TH-29	Social Engineering	IM-05	Disclosure of Credentials

Now that we have the correlation table is defined and the threat propagation analysis for CitySCAPE is concluded, Let's go back to our threat modelling process.
Generally, the cascading threat modelling and analysis process can be expressed with the following steps (note: the security controls and countermeasures are not in the scope of this deliverable – the relevant blocks in Figure 10 are presented with orange color):

1. Check if a threat is implemented on an asset.
2. Check if a security measure protects from exploitation of possible vulnerabilities.
3. Check if there are interfaces that are affected by the threat and may be used to propagate the threat. This can be done by checking the network/interface connections of the assets from the system architecture views of Figure 5 and Figure 6.
4. Check if the asset is interconnected with a different asset. This can be done from the Asset Transition matrix in Table 16 and Table 17 for Tallinn and Genoa use cases respectively. If so, the interconnected asset is denoted as the second asset.
5. Check if the implementation of a threat on the first asset has an impact on the first asset. This is done by the matrix of Table 20.
6. Check if the implementation of the threat on the first asset, correlates with impact or threat for the second asset that was identified. This is done using the TST graph of Figure 9.
7. If so, a cascading threat is identified.
8. However, a threat does not translate into risk or failure unless there is a vulnerability that can be exposed.
9. If there is such a vulnerability, check if there are countermeasures to protect the second asset.
10. If there are no security controls, or if the effectiveness of the security control is low, then we have a cascading risk.

The cascading threat methodology is integrated into the Risk Analysis process and the results will be reported on D2.3, where CitySCAPE-specific cascading threats/risks will be identified.

It is noted that as the risk modeling and threat analysis evolves, certain changes at the content of Table 18, Table 19, Table 20 and Figure 9 may occur. These changes, if any, will be reported on D2.3.

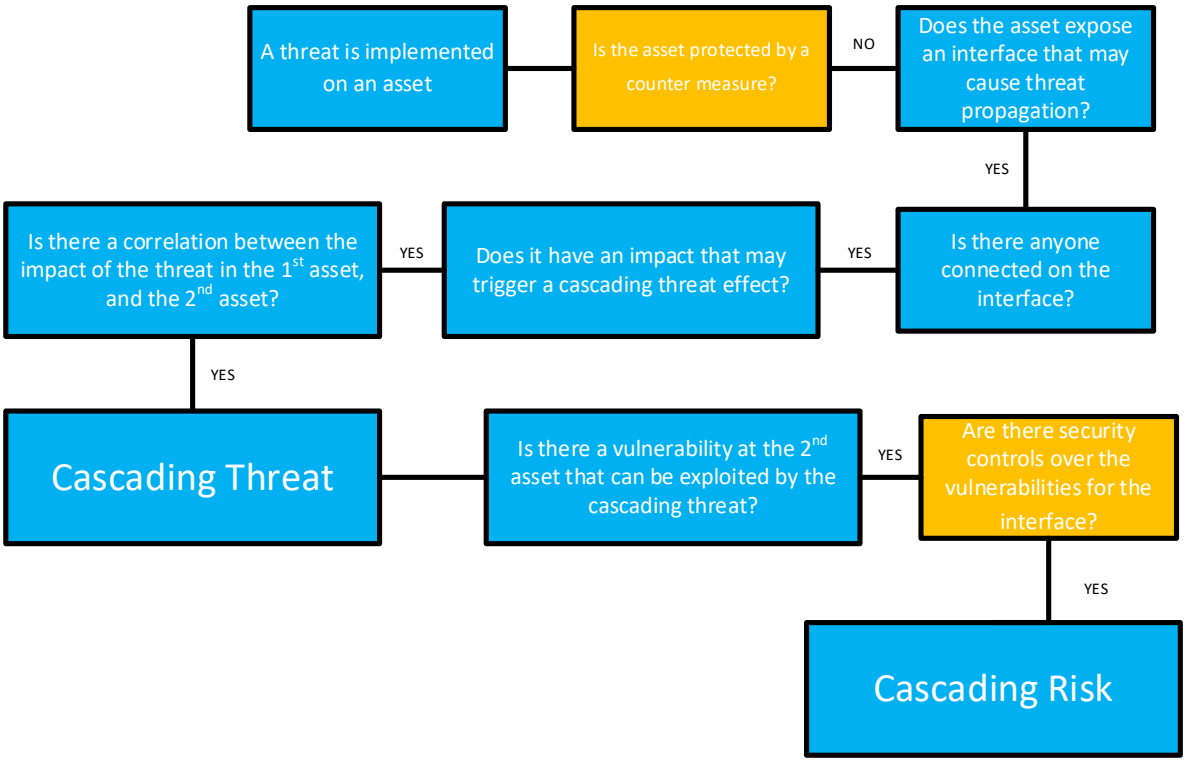

Figure 10: Logical flow for cascading threat and risk identification

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

5 CONCLUSIONS

The main goal of this deliverable is the development of a new methodology for analysis of interconnections and interdependencies between systems, assets and critical infrastructures, that will help model and accurately evaluate the infrastructure behaviour due to the propagation of cascading threats.

The deliverable can be considered as is Part 1 of the complete CitySCAPE Risk and threat analysis that will be concluded in D2.3 “Multimodal Transport System: System Modelling, Risk Analysis and Management, GDPR Compliance”, since in order to achieve the goal of modelling cascading threats for interdependent systems, a number of risk and threat analysis steps were performed having as reference the CitySCAPE use cases described in D2.1. Thus, in this report:

- Reference architectures of the CitySCAPE use cases were derived in order to be used for modelling and analysis.
- The assets for the CPaaS system architectures were identified and re-examined as “composite assets”, i.e., application-specific, customized, complex system components-entities.
- A set of basic/generic assets was defined in order to be able to decompose the composite systems into manageable basic sub-systems.
- The composite system assets were further analysed in basic assets, based on the implementation information extracted by D2.1.
- The cyber threats related to the basic assets and consequently the composite CPaaS assets were identified – using the study of D2.2 as a reference and by introducing a new taxonomy that fits CitySCAPE objectives.
- the analysis of the system allowed the investigation of interdependencies leading to a new methodology for cascading threat analysis with the introduction of the TST graph and the Asset Transition matrix.

The results of D2.4 will be integrated into the complete risk and threat analysis methodology that is currently developed in Task 2.2 “Cross-domain threat analysis”.

BIBLIOGRAPHY

Alcaraz, C. ,. (2011). Secure SCADA framework for the protection of energy control systems. *Concurrency Comput. Pract. Experience*, 23(12), 1414–1430.

CitySCAPE, H. (2021). *D2.1 CitySCAPE use cases.*

ENISA. (2019). *Good Practices for Security of Smart Cars.* ENISA.

Fischer, D., Markscheffel, B., Frosch, S., & D. Buettner. (2012). A survey of threats and security measures for data transmission over GSM/UMTS networks. *2012 International Conference for Internet Technology and Secured Transactions.* IEEE.

Hogben, G., & Dekker, M. (2010). *Smartphones: Information security risks, opportunities and recommendations for users.* ENISA.

Krutz, R. (2005). Securing SCADA Systems. *Wiley, Indianapolis.*

Lourenço, M. B., Marinos, L., & Patseas, L. (2020). *Threat Landscape For 5G Networks* . ENISA.

Marinos, L. (2013). *Smart Grid Threat Landscape and Good Practice Guide.* ENISA.

P. Pederson, D. D. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research.*

Perilli, A., Manieri, A., Algom, A., Balding, C., Bunker, G., Rhoton, J., . . . Pascoe, S. (2009). *Cloud Computing: Benefits, risks and recommendations for information security.*

Ross, M., Tschofenig, H., Jara, A. J., Valderrama, C., Cosenza, A., Zolotnikov, V., . . . Greer, C. (2017). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.* ENISA.

S. M. Rinaldi, J. P. (2001). *Identifying, understanding, and analyzing critical infrastructure interdependencies.* IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25.