D2.2 – Attack Modeling

Security Assurance Framework for Networked Vehicular Technology

Abstract

SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-I (V2I) communications aiming at improving the cyber-physical security ecosystem of "connected vehicles" in Europe. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related to Connected Vehicles and V2I systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics, services and integration with 3rd party components and applications. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

DX.X & Title:	**D2.2 Attack Modeling**
Work package:	WP2
Task:	T2.2 Threat Analysis and Attack Modeling
Due Date:	31 October 2017
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR	**DATE**
Matthieu Gay / CCS	08-11-2017
CONTRIBUTORS	**DATE**
Kostas Lambrinoudakis / UPRC	07-10-2017
Paul-Emmanuel Brun / CCS	31-05-2017
Gildas Koudessi / CCS	20-07-2017
Matthieu Gay / CCS	08-11-2017
Christos Kalloniatis / UPRC	30-10-2017
Athanasios Kanatas / UPRC	03-11-2017
Vasiliki Diamantopoulou / UPRC	30-10-2017
Konstantinos Maliatsos / UPRC	03-11-2017
REVIEWED BY	**DATE**
Sammy HADDAD / Oppida	06-11-2017
Panagiotis Pantazopoulos / ICCS	06-11-2017
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Document/Revision history

Version	Date	Partner	Description
V0.1	31/05/2017	CCS	First version with table of content
V0.2	20/07/2017	CCS	Update of the methodology and table of content
V0.3	20/10/2017	UPRC	Update methodology and use case description
V0.4	30/10/2017	UPRC	Update models in Use Cases
V1.0	03/11/2017	UPRC	Update Threat and Attack Models
V2.0	07/11/2017	UPRC	Incorporation of Internal Review Comments
V3.0	08/11/2017	CCS	Final Version
V4.0	04/02/2019	CCS & UPRC	• Justification of the lack of Attack Tree Analysis (ATA) in section 2.2 Secure Tropos Methodology page 18. • Explanation of the asset identification process and the usage of a questionnaire in section 5.2.1 Stage 1: identification of Assets page 57. • Explanation on the elicitation of threat agents, attack methods, threat sources and the completeness of the results in section 5.2.4 Stage 4: Threat and Attack Modelling page 69. • Addition of an appendix section page 90 to explain the usage of simulators.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

List of Figures

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Acronyms and abbreviations

Abbreviation	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Informations (National Cybersecurity Agency of France)
BMS	Bare Metal Server
CAM	Cooperative Awareness Message
CIAT	Confidentiality, Integrity, Availability, Tracability
C-ITS-S	Central Intelligent Transportation System Station
CSP	Cloud Service Provider
DENM	Decentralized Environmental Notification Message
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EKD	Enterprise Knowledge Development
ETSI	European Telecommunications Standards Institute
GNSS	Global Navigation Satellite System
HMI	Human-Machin Interface
ICT	Information and Communications Technology
ITS	Intelligent Transportation Systems
ITS-S	Intelligent Transportation System Station
LDM	Local Dynamique Map
LTE	Long-Term Evolution
LVI	Local Vehicle Information
OBU	(Vehicle) On Board Unit – ***This term is identical to V-ITS-S***
PriS	Privacy Safeguard
QoS	Quality of Service
R-ITS-S	Roadside Intelligent Transportation System Station
RSU	Roadside Unit -- ***This term is identical to R-ITS-S***
SPaT	Signal Phase and Time
TLC	Traffic Light Controller

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

TMC	Traffic Management Centre
ToE	Target of Evaluation
TVRA	Threat, Vulnerability and Risk Analysis
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
V-ITS-S	Vehicle Intelligent Transportation System Station
VM	Virtual Machine
VPN	Virtual Private Network

Table 1: List of Abbreviations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Executive Summary

In its objective of building a security assurance framework for connected vehicular technology, SAFERtec will address the safety, the security and the privacy of the handled data. A study has been carried out to identify the vulnerabilities, impacts, mitigation actions and respective security control. This deliverable, entitled "Attack Modelling" explains how these objectives will be fulfilled and part of achieved result.

To do so, this deliverable describes the work that has been carried out during the task T2.2 entitled "Threat Analysis and Attack Modelling". SAFERtec has developed a new methodology based on three other renowned methodologies namely EBIOS, Secure Tropos and PriS.

This document will present each methodology, their concepts and their implementations. Then, we will explain how we merged these three methodologies in a new 6-step-methodology which attempts to preserve the advantages of each one. For this occasion each step of the SAFERtec methodology will be described.

The ETSI Standards and more specifically the results of a Threat, Vulnerability and Risk Analysis (TVRA) study for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) for Intelligent Transportation Systems (ITS) has been used as a helpful tool for feeding the initial steps of the attack modelling method.

Although the entire methodology has been described, we will implement only the four first steps of the first use case called "Optimal Speed Driving" as a practical example. The full implementation of the SAFERtec methodology will be carried out on all considered use cases in the next deliverable D2.3 entitled "Vulnerability Analysis".

In the frame of this work package, we also developed simulators for the two radio interfaces used. These simulators will be used in the work packages 3 and 5 but all the details of their implementations are detailed in the appendix section.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

1. Introduction

One of the main SAFERtec goals is to provide a flexible and efficient assurance framework for the safety, security, privacy and trustworthiness of connected vehicles in Europe. More specifically the project aims to deliver innovative techniques, development methods and testing models for achieving assurance of the aforementioned requirements of ICT related Connected Vehicle and V2X systems. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

Assurance security evaluation methods always rely on the definition of a proper security target. This security target is the specification of the evaluation goal. Thus, it is an important aspect of the evaluation process to define a meaningful security target. It is often one of the most criticized parts of an evaluation, since there is no universal way to assess the relevance of such a document. But one thing that helps to gain confidence in this part of the evaluation is to have elements of proof that the system and the real threats associated to it are properly understood and justified. Here we provide formal and powerful tools to help designing relevant and convincing security target representing real world security objectives for ITS systems. This is one great step towards better and stronger security assurance framework.

1.1 Purpose of the Document

The document aims to present the results of the work carried out in task T2.2 entitled “Threat Analysis and Attack Modelling”.

1.2 Intended readership

In addition to the project reviewers, this deliverable is addressed to any interested reader (i.e., Public dissemination level).

1.3 Inputs from other projects

No input from other projects was considered during the compilation of this deliverable.

1.4 Relationship with other SAFERtec deliverables

This deliverable utilizes deliverables D2.1 “Connected Vehicle Use Cases and High Level Requirements” and D4.1 “Specifications of Connected Vehicle System”, as its principal inputs and will be used to carried out the work of the task T2.3 entitled “Vulnerability Analysis”.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

2. Risk Analysis and Modelling Methodologies

For the purpose of assessing cyber security risks on the retained use cases, the Safertec has to develop a methodology that enables an effective consideration of all security aspects for the designed architectures.

In this Chapter the three independent methodologies, namely EBIOS, SecureTropos and PriS, that will be integrated for the purposes of the modelling will be presented. More specifically the integrated SAFERtec methodology will be used for identifying the main assets (hardware, software, data, communication links) of the Connected Vehicle and V2X systems, eliciting the security, safety and privacy requirements, identifying threats and vulnerabilities and finally producing the threat and attack models of the system that is studied.

The resulting output (threat and attack models), in conjunction with specific test scenarios that will be developed, will be then used for evaluating the level at which the identified security, safety and privacy requirements are satisfied and thus facilitating the association of the connected vehicle system to an assurance level.

2.1 EBIOS methodology

EBIOS (English: Expression of needs and identification of security objectives) is the risk analysis methodology created by the french Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) (English: National Cybersecurity Agency of France). A risk analysis method identifies the critical part of the system and their corresponding threats in order to evaluate the risk for this assent and then the proper security objectives regarding the evaluated risks. EBIOS is composed of five steps and offers many advantages, particularly the flexibility, quickness besides the fact that it is a proven methodology that has been used in several risk assessments and that it is compatible with the ISO 27005 risk analysis phase.

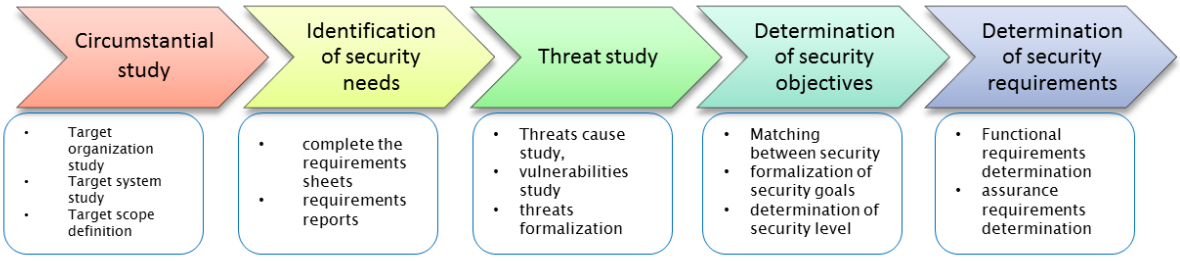

Figure 1: The five steps of EBIOS

To fully benefit from the swiftness of EBIOS, we will comply with the five classic steps of this methodology and we will use it for performing risk analysis for the use cases identified in Deliverable D2.1.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.1.1 Step 1: Circumstantial study

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 formalised (non-exhaustive list):

- Essentials assets in a connected vehicle 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 SAFERtec itself

At the end of this step, a clear vision of the components and the links between them will be formalised.

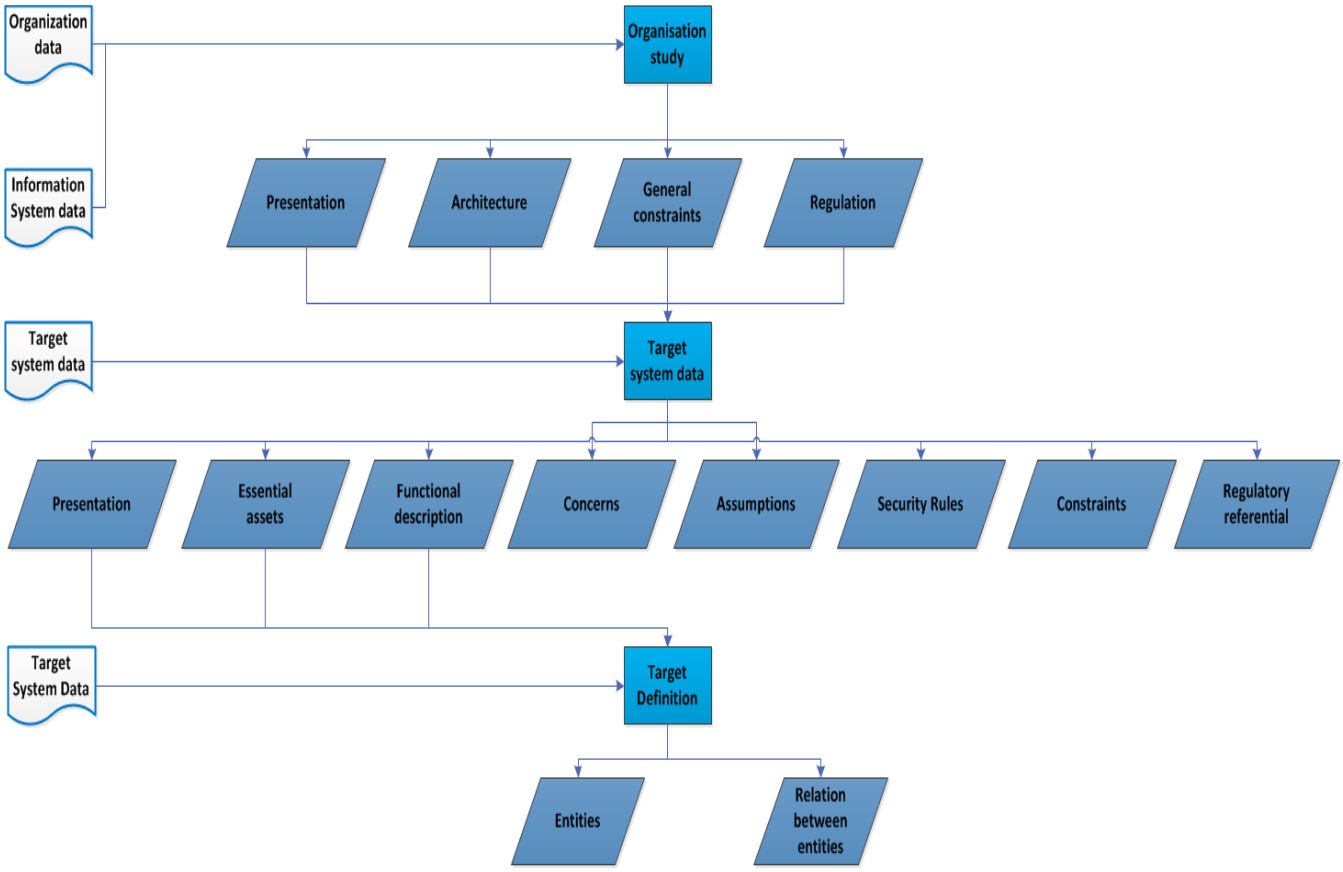

Figure 2: Circumstantial study

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.1.2 Step 2: Expression of security needs

This step will contribute to risk estimation and definition of risk criteria. The expression of security needs will be performed based on scale of needs. Security criteria and hypothetic impacts will be stated.

Security needs will be associated with each essential component by taking into account the security criteria.

A security needs report will be the output of this step.

2.1.3 Step 3: Threat study and modelling

At this stage, the threats affecting the connected vehicle systems will be studied. The threats are specific to the connected vehicles. There will be no dependencies between these threats and the security needs collected in the previous step.

The following activities will be performed:

- List the relevant attack methods (In collaboration with project partners - experts)
- Characterise the attack methods according to the security criteria they may be affected
- Characterise the threat agents for each attack method retained according to their type
- Add a value representing the attack methods with justifications
- Identify the vulnerabilities of the entities according to attack methods
- Estimate the vulnerability level
- Formulate the threats
- Assign priority in the threats according to the probability of their occurrence

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

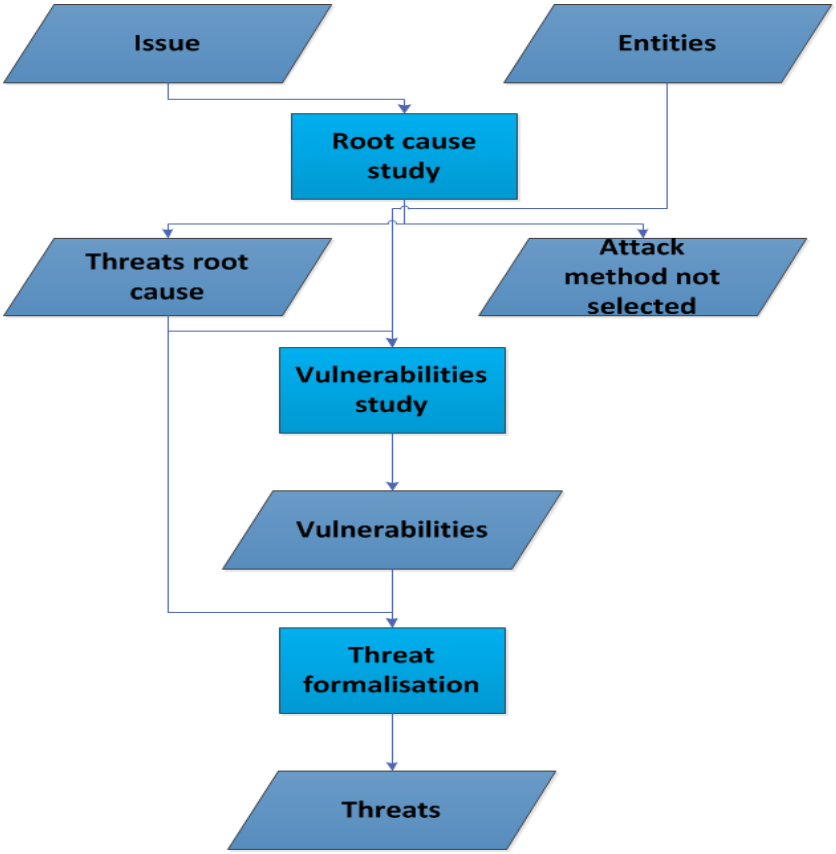

Figure 3: Threat study

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

On the basis of the identified security threats and attack types, Secure Tropos and PriS will be used to go deeper and formalise attack in the corresponding diagrams.

2.1.4 Step 4: Identification of security objectives

The purpose of this step is to evaluate the risks affecting the connected vehicle environment.

The security objective is highlighted by comparing the threats with security needs. The security objectives will contain the security requirements fulfilled in the development of secure connected vehicle system (or component).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

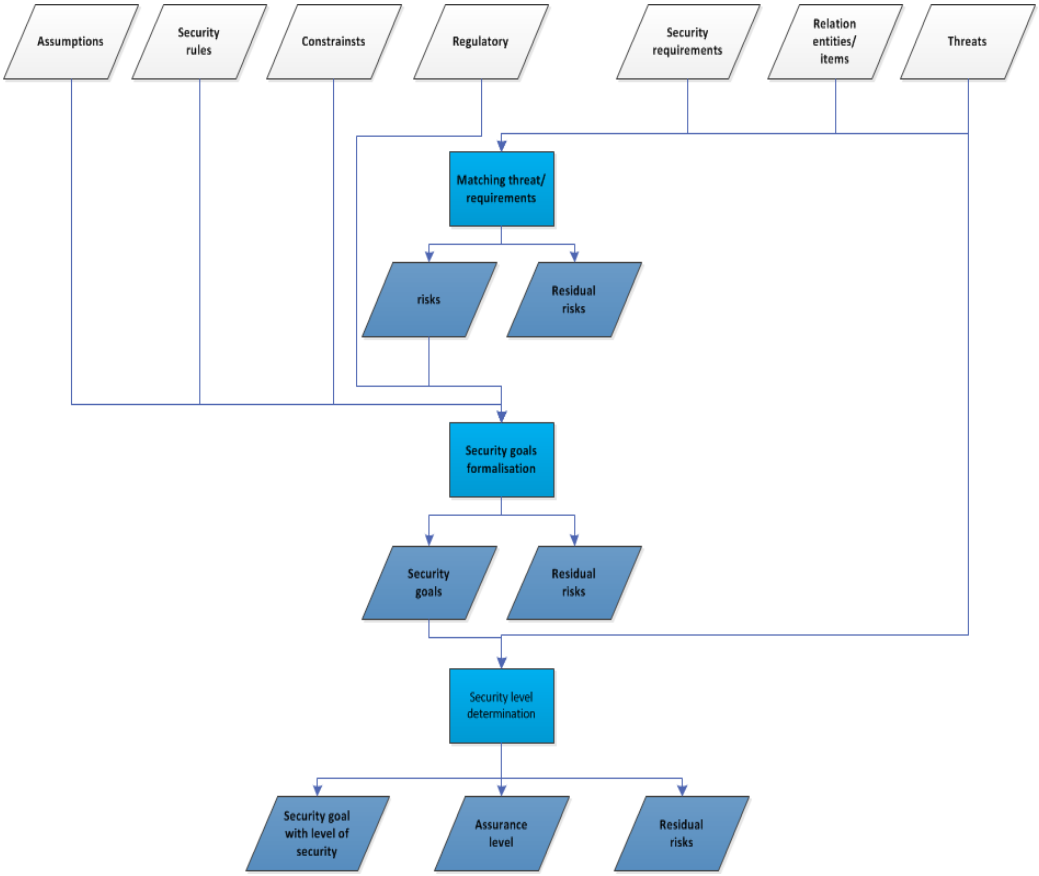

Figure 4: Identification of security objectives

The following actions will be considered when identifying security objectives:

- Determining the risks by comparing threats with security needs
- Formulate the risks explicitly
- Prioritise the risks according to the impact on the essential components and the threat probability
- Highlight the non-retained risks (residual risks), with justifications
- List the security objectives
- Justify the completeness of coverage, checking risks, assumptions and security rules are compatible with the constraints affecting the organisation and target system.
- Determine accurate strength level of each security objective

2.1.5 Step 5: Determination of security requirements

This step will bring an answer to the question how the security objectives will be achieved.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

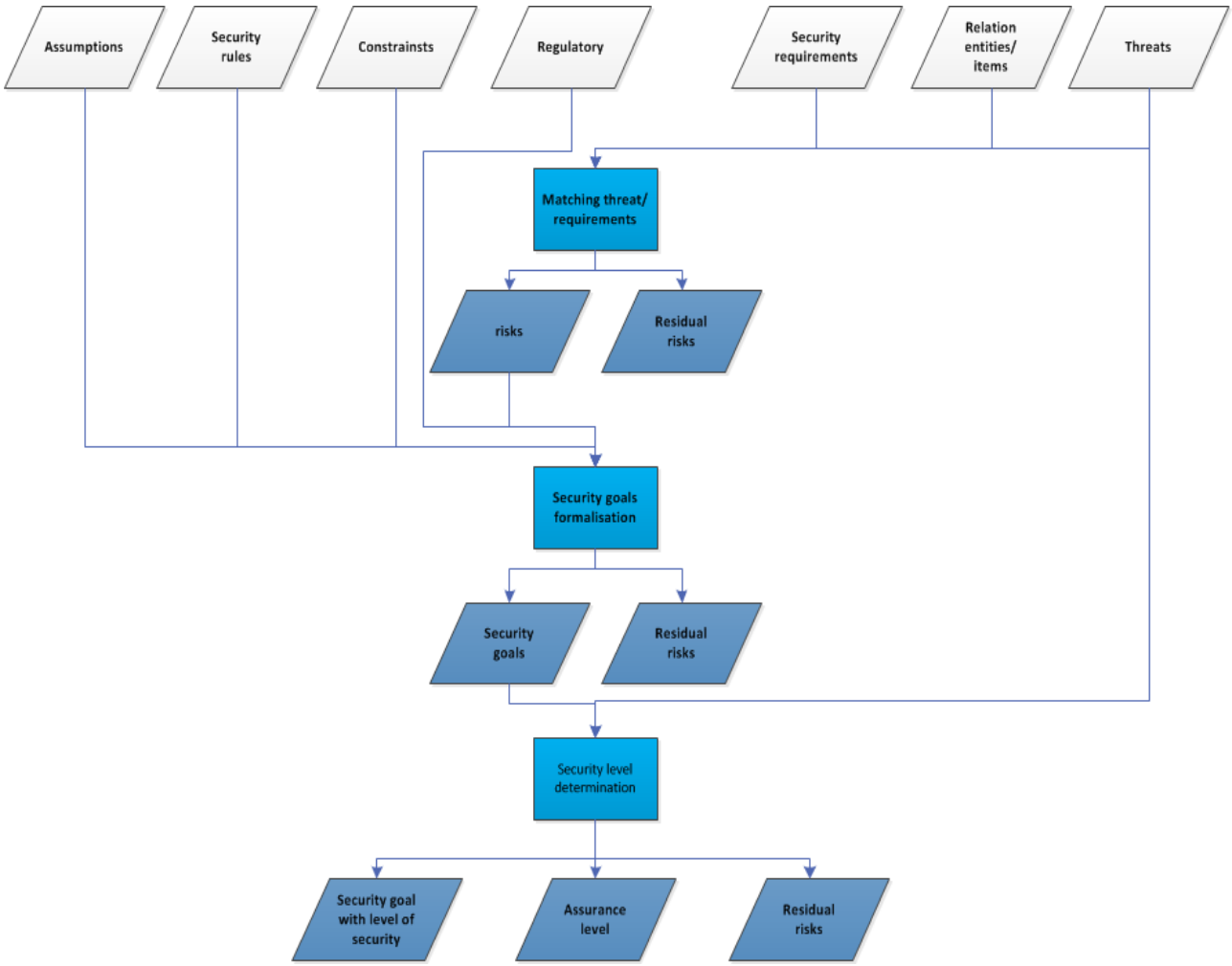

Figure 5: Determination of security requirements

- List the security functional requirements
- Justify the adequacy of coverage of the security objectives
- Highlight any coverage flaws (residual risks) with justifications.
- Classify the Security functional requirements into two categories:
  - Security functional requirements concerning the vehicle
  - Security functional requirements concerning the vehicle environments
- Where appropriate, justify the coverage of dependencies of security functional requirements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.2 Secure Tropos Methodology

Secure Tropos [1] is a security requirements engineering methodology that supports elicitation and analysis of security requirements. It is based on the principle that security should be analysed and considered from the early stages of the software system development process, and not added as an afterthought. To support that approach, the methodology provides a modelling language, a security-aware process, and a set of automated processes to support the analysis and consideration of security from the early stages of the development process. The Secure Tropos language consists of a set of concepts from the requirements engineering domain, and in particular Goal-Oriented Requirements Engineering [2, 3], such as actor, goal, plan, and dependency, which are enriched with concepts from security engineering, such as security constraint, secure plan, and attacks.

The use of Attack Tree Analysis (ATA), as envisaged in task 2.2 of the DoA, has been abandoned since Secure Tropos covers it in a much more complete and precise way. Attack tree is another modelling language which presents different possible attacks to an information system but they are incapable of representing some important aspects of information systems. In fact, the attack trees simply mention the different approaches to achieve a malicious goal without pointing to the assets, vulnerabilities, and security requirements and thus they do not provide enough information for the software engineers to avoid the probable risks, something that can be achieved through Secure Tropos.

The Secure Tropos methodology closely follows the software development life-cycle, i.e. capturing of early requirements, late requirements, architectural design, detailed design, and finally, implementation. Thus, it allows the developer to create and refine models, starting from the system-as-it-is, in order to finally develop the system-to-be, during the analysis and design stage [4].

2.2.1 Concepts Description

Secure Tropos combines concepts from requirements engineering for representing general concepts and security engineering for representing security-oriented concepts [5].

A (hard) ***Goal*** represents a condition in the world that an actor would like to achieve [6]. In other words, goals represent actors' strategic interests. In Tropos, the concept of a hard-goal (simply goal hereafter) is differentiated from the concept of soft-goal.

A **Soft-Goal** is used to capture non-functional requirements of the system, and unlike a (hard) goal, it does not have clear criteria for deciding whether it is satisfied or not and therefore it is subject to interpretation [6]. For instance, an example of a soft-goal is "the system should be scalable". According to Chung et al. [7], the difference between a goal and a soft-goal is underlined by saying that goals are satisfied whereas soft-goals are satisfied under specific circumstances.

An **Actor** represents an entity that has intentionality and strategic goals within the multi-agent system or within its organisational setting. An actor can be human, a system, or an organisation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

A **Plan** represents, at an abstract level, a way of doing something [8]. The fulfilment of a task can be a mean for satisfying a goal, or for contributing towards the satisfying of a soft-goal. In Tropos different (alternative) tasks, that actors might employ to achieve their goals, are modelled. Therefore, developers can reason about the different ways that actors can achieve their goals and choose the best one.

A **Resource** presents a physical or informational entity that one of the actors requires [8]. The main concern when dealing with resources is whether the resource is available and who is responsible for its delivery.

A **Dependency** between two actors represents that one actor depends on the other to attain some goal, execute a task, or deliver a resource [6]. The depending actor is called the depender and the actor who is depended upon is called the dependee. The type of the dependency describes the nature of an agreement (called dependum) between dependee and depender. Goal dependencies represent delegation of responsibility for fulfilling a goal. Soft-goal dependencies are similar to goal dependencies, but their fulfilment cannot be defined precisely whereas task dependencies are used in situations where the dependee is required to perform a given activity. Resource dependencies require the dependee to provide a resource to the depender. By depending on the dependee for the dependum, the depender is able to achieve goals that it is otherwise unable to achieve on their own, or not as easily or not as well [6]. On the other hand, the depender becomes vulnerable, since if the dependee fails to deliver the dependum, the depender is affected in their aim to achieve their goals.

A **Secure Dependency** introduces one or more Security Constraint(s) that must be fulfilled for the dependency to be valid [9]. In the Secure Tropos methodology we distinguish among three types of secure dependencies: dependee secure dependency, depender secure dependency, and double secure dependency. In terms of the modelling language, different Secure Dependency types are defined using depender and dependee attributes of Security Constraints.

A **Security Constraint** is the main concept introduced by Secure Tropos. Security Constraints are used, in the Secure Tropos methodology, to represent security requirements [29]. A Security Constraint is a specialisation of the concept of constraint. In the context of software engineering, a constraint is usually defined as a restriction that can influence the analysis and design of a software system under development by restricting some alternative design solutions, by conflicting with some of the requirements of the system, or by refining some of the systems objectives. In other words, constraints can represent a set of restrictions that do not permit specific actions to be taken or prevent certain objectives from being achieved. Constraints are often integrated in the specification of existing textual descriptions. However, this approach can often lead to misunderstandings and an unclear definition of a constraint and its role in the development process. Consequently, this results in errors in the very early development stages that propagate to the later stages of the development process causing many problems when discovered; if they are discovered. Therefore, in the Secure Tropos modelling language we handle security constraints, as a separate concept. To this end, the concept of security constraint has been defined within the context of Secure Tropos as: A security condition imposed to an actor that restricts achievement of an actor's goals, execution of plans or availability of resources. Security constraints are outside the control of an actor. This means that,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

differently than goals, security constraints are not conditions that an actor wishes to introduce but it is forced to introduce.

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 [9]. 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 [9].

Threats can be operationalised by different attack methods, each exploiting a number of system vulnerabilities.

An **Attack Method** in Secure Tropos is an action aiming to cause a potential violation of security in the system [10].

Security Mechanisms represent standard security methods for helping towards the satisfaction of the security objectives [10]. Some of these methods are able to prevent security attacks, whereas others are able only to detect security breaches. It must be noted that furthered analysis of some security mechanisms is required to allow developers to identify possible security sub-mechanisms. A security sub-mechanism represents a specific way of achieving a security mechanism. For instance, authentication denotes a security mechanism for the fulfilment of a protection objective such as authorisation. However, authentication can be achieved by sub-mechanisms such as passwords, digital signatures and biometrics.

2.2.2 Secure Tropos Model Views

The Secure Tropos produces models that contain security and privacy requirements analysis, but with the support of the corresponding tool, namely SecTro [11], the information is grouped according to three perspectives (views), i) the Organisational view, ii) the Requirements view and iii) the Attacks view. Each view provides specific focus of the system under analysis.

Organisational view: This view represents the organisational architecture allowing a developer to understand the requirements of the organisation and any interactions between the organisation and external actors or systems. In addition, it displays the organisations' boundaries, where organisational actors reside; any external actors are modelled outside of this boundary. Organisational view represents the system-as-it-is.

Requirements view: This view provides a detailed representation of the organisational view. There, system actors and their goals are designed including the security and privacy analysis concepts. The modelling activity focuses on the responsibilities of the system and other actors, as well as the interaction of actors with the system itself. Requirements view represents the system-to-be.

Attacks View: This view allows the evaluation of the system security and privacy against various attacks. The attack modelling takes place by analysing and checking whether security and privacy threats, which have already been introduced in the Requirements View, are mitigated by the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

security mechanisms and privacy enhancing technologies, respectively, available within the system. If the developer identifies any inability of the system to mitigate these threats, they follow an iterative process, going back to the Requirements View, and adjust the design accordingly.

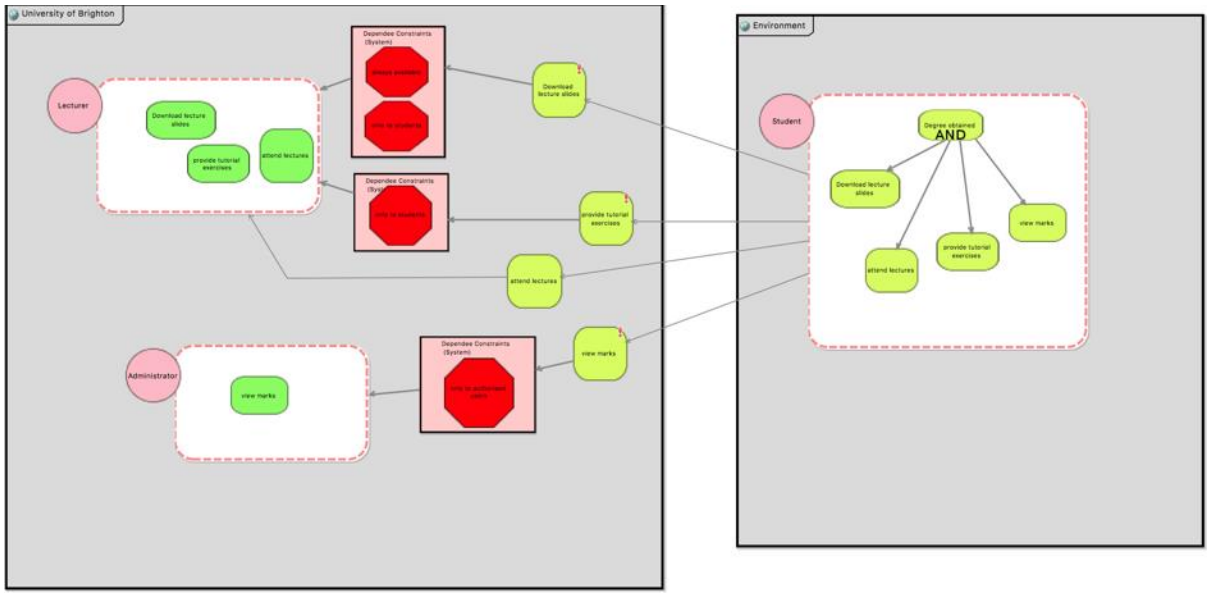

Figure 6: Organisational View

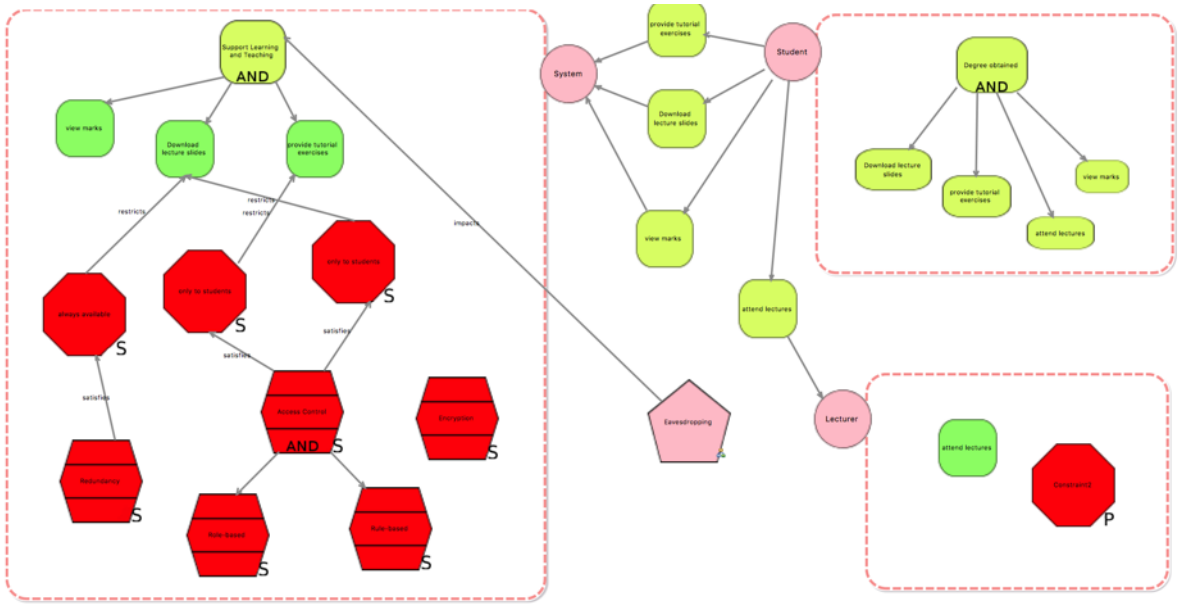

Figure 7: Requirements View

Attacks View: This view allows the evaluation of the system security and privacy against various attacks. The attack modelling takes place by analysing and checking whether security and privacy threats, which have already been introduced in the Requirements View, are mitigated by the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

security mechanisms and privacy enhancing technologies, respectively, available within the system. If the developer identifies any inability of the system to mitigate these threats, they follow an iterative process, going back to the Requirements View, and adjust the design accordingly.

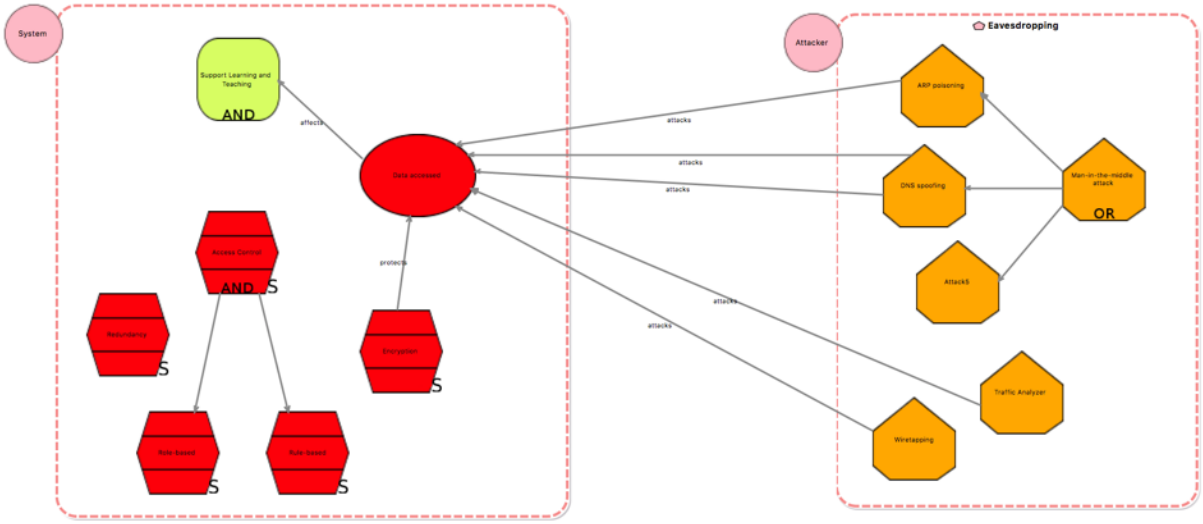

Figure 8: Attacks View

2.2.3 Secure Tropos Process

Using the different modelling views supported by the SecTro tool, security-related features of the system can be analysed from a variety of perspectives. The process is not strictly sequential, as the developer can return to a preview view to enhance or alter their model.

Step 1: Organisational modelling

During the first step, the designer, alongside the stakeholders of the system, identifies:

- The Actors of the system
- The Goals (hard and soft) that these actors have
- The Plans and the Resources that are required for the realisation of the Goals
- The Dependencies that one Actor might have on another Actor, for the achievement/realisation of a Goal, a Plan or a Resource
- The security and privacy requirements of the system, which are presented in the form of Security and Privacy Constraints

Step 2: Security Requirements Modelling

It provides a more detailed representation of the security aspects of the system. More specifically, this step contains:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Description of the relationship between attacks expected and mitigation mechanisms for any identified threat.
- Introduction of a number of resources, which represent various assets that are either created from or required for the achievement of each of the modelled goals.
- Introduction of plans that indicate activities required for the achievement of certain system goals.
- Modelling of threats of the systems that impact different goals and resources
- Introduction of security and privacy mechanisms that protect the system against each of the identified vulnerabilities

Step 3: Security Attacks Modelling:

This step allows the refinement of threats, by modelling attackers and ways to mitigate attacks on vulnerabilities. Here, the designer demonstrates how each threat can impact the system.

- Identification of the attack methods that a threat can utilise
- Identification of the vulnerabilities that the above attack methods can exploit
- Identification of the system resources and goals that the above vulnerabilities can affect.

2.3 PriS Methodology

PriS is a privacy requirements engineering methodology, which provides a set of concepts for modelling privacy requirements in the organisation domain and a systematic way-of-working for translating these requirements into system models.

PriS, initially introduced in [12,13,14], is a privacy requirements engineering method developed for assisting designers on eliciting, modeling, designing privacy requirements of the system to be and also providing guidance to the developers on selecting the appropriate implementation techniques that best fit the organisation's privacy requirements. PriS is a privacy requirements engineering methodology, which provides a set of concepts for modelling privacy requirements in the organisation domain and a systematic way-of-working for translating these requirements into system models. PriS identifies privacy as a multifaceted concept and defines it in the context of eight technical privacy requirements (such as anonymity and unlinkability) and adopts the use of process patterns as a way to: (a) describe the effect of privacy requirements on business processes; and (b) facilitate the identification of the system architecture that best supports the privacy-related business processes.

PriS was designed for supporting the realisation of privacy-aware information systems on traditional environments and not for the cloud. Cloud environments introduced a number of new privacy related concepts that along with the ones already stated form a new set of concepts that need to be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

considered when designing privacy-aware services over the cloud. Thus, extended versions of PriS were introduced [15, 16] for assisting designers to reason about privacy concerns in cloud environments as well.

2.3.1 PriS Conceptual Model

The conceptual model used in PriS is based on the Enterprise Knowledge Development (EKD) framework [17, 18], which is a systematic approach to developing and documenting enterprise knowledge, helping enterprises to consciously develop schemes for implementing changes (e.g., the introduction of a new software system); an enterprise is defined as the organisation about which the proposed software system is to provide some service.

Modelling of organisational knowledge in EKD is achieved through the modelling of:

(a) organisational goals, that expresses the intentional objectives that control and govern its operation,

(b) the 'physical' processes, that collaboratively operationalise organisational goals and

(c) the software systems, that support the above processes. EKD adopts a goal-oriented approach to software engineering.

The EKD generic schema is shown in the following figure. The processes represent WHAT needs to be done, goals justify WHY the associated processes exist, while systems describe HOW processes can be implemented in terms of appropriate system architectures. In this way, a connection between system purpose and system structure is established.

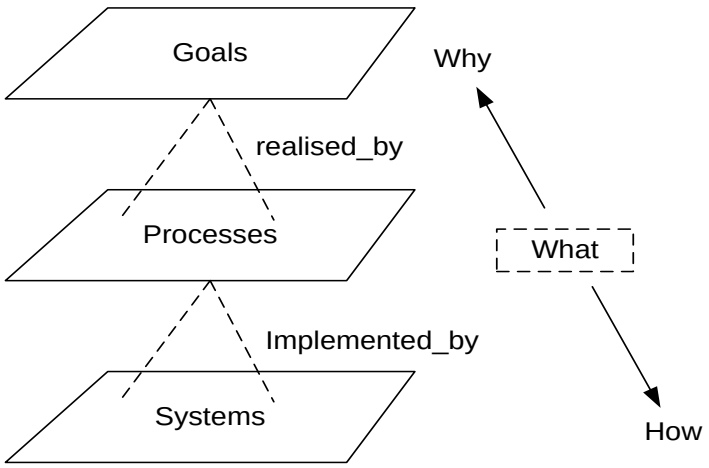

Figure 9. The EKD Schema

The conceptual model of PriS is presented in the following figure.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

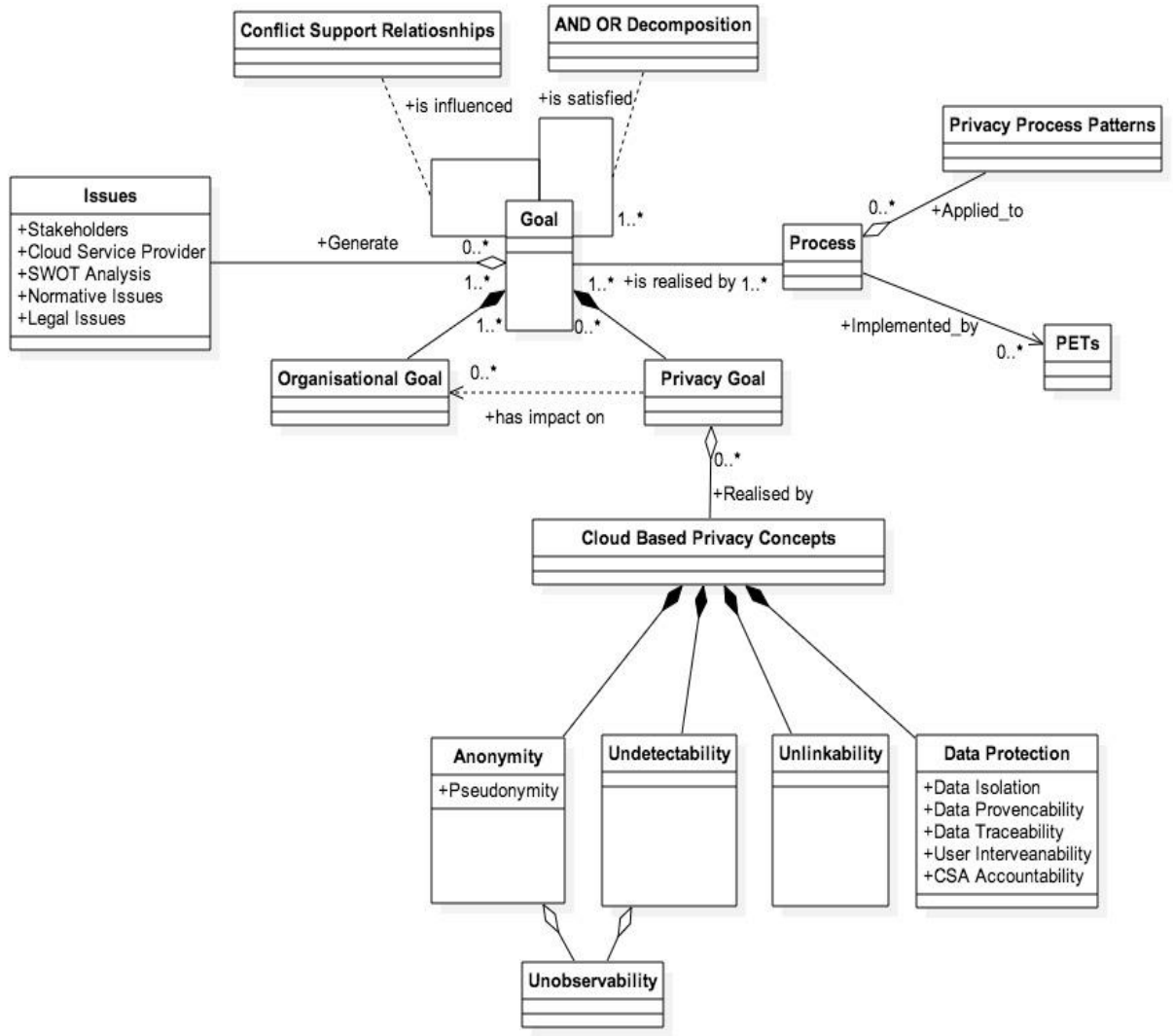

Figure 10. PriS Conceptual Model

The conceptual model uses the concept of **goal** as the central and most important concept as shown in figure 10. Goals are desired state of affairs that need to be attained. Goals concern stakeholders, i.e. anyone that has as interest in the system design and usage. Also, goals are generated because of **issues**. An issue is a statement of a **strength, weakness, opportunity or threat** that leads to the formation of the goal. **Cloud Service Providers (CSPs)** constraint the functionality of the developed system or service due to the technologies they use, the policies they follow, the contractual requirements with third parties, etc. Thus, the CSP may provide requirements that designers need to take under consideration during the realisation of the system. Protection of users' privacy is stated in many European and national **legislations** through the form of laws, policies, directives, best practices etc. All these sources need to be taken under consideration during the identification of functional and non-functional requirements for traditional and cloud-based systems. Thus, goal

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

identification needs to take under consideration all these elements before further analysis is conducted.

As shown in figure 10 there are two types of goals namely **organisational goals** and **privacy goals**. Organisational goals express the main organisation objectives that need to be satisfied by the system into consideration. Organisational goals will lead to the realisation of system's functional requirements. In parallel, privacy goals are introduced because of specific cloud based privacy related concepts namely **anonymity, pseudonymity, unlinkability, undetectability and data protection**. **Unobservability** is realised if the system sufficiently realises undetectability among the respective assets and anonymity of the user accessing them. Thus it is not accomplished directly but indirectly through the realisation of the respective two concepts. Finally, the concepts of **isolation, provenanceability, traceability, interveanability and accountability** are related to data protection of user's or systems data over the cloud as it was explained previously. Thus, all these concepts are grouped under the data protection class. Privacy goals may have an impact on organisational goals. In general, a privacy goal may cause the improvement/ adaptation of organisational goals or the introduction of new ones. In this way, privacy issues are incorporated into the system's design.

Goals are realised by **processes**. However, goals cannot be mapped directly onto processes. The transition process from goals to processes includes the causal transformation of general goals into one or more subgoals that form the means for achieving desired ends. During this process, in every step new goals are introduced and linked to the original one through causal relations thus forming a hierarchy of goals. Every subgoal may contribute to the achievement to more than one goals, thus the resulting structure is a graph rather than a hierarchy. As it can be seen from the figure the satisfaction relationships between original goals and their subgoals, in the goal graph, are of the **AND/OR type**.

Besides the satisfaction type relationship between a goal and its successor goals another relationship type exists. **The influencing relation type**, which is based on two subtypes namely goal support relationship and goal conflict relationship. A support relationship between two goals means that the achievement of one goal assists the achievement of the other; however, the opposite is not necessarily true. Finally, the conflict relationship between two goals implies that the achievement of one goal hinders the achievement of the second one.

As it was mention before goals are realised by processes. PriS uses a set of **privacy process patterns** as a more robust way of bringing the gap between the design and the implementation phase. Privacy process patterns are usually generalised process models, which include activities and flows connecting them, presenting how a business should be run in a specific domain. Privacy process patterns are applied on privacy related processes in order to specify the way that the respective privacy issues will be realised through a specific number of steps. This assists also the developer who can understand in a better and specific way, how to implement the aforementioned privacy concepts. Privacy process patterns are also used for identifying a number of **Privacy Enhancing Technologies (PETs)** already available for implementing the system's privacy requirements. In this way the developer can choose the most appropriate technology based on the privacy process patterns applied on every privacy-related process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.3.2 PriS Way of Working

Step 1: Elicit Privacy Related Goals

The first step concerns the elicitation of the privacy goals that are relevant to the specific organisation. This task usually involves a number of stakeholders and decision makers (managers, policy makers, system developers, system users, etc.). Therefore, elicitation of privacy goals is performed through the following activities: perform stakeholder analysis and organise stakeholder workshop; identify privacy issues; and agree on a structures set of privacy goals. Identifying privacy issues is guided by the basic privacy concerns in collaboration with any risk analysis or threat elicitation technique. The aim is to interpret the general privacy requirements with respect to the specific application context into consideration.

Step 2: Analyse the impact of privacy goals on business processes

The second step is to analyse the impact of these privacy goals on processes and related support systems. Answering this question involves the following tasks: identify the influence of privacy goals on organisational goals and analyse the impact on processes.

A summary of this process is shown in figure 11. For each privacy goal, PriS identifies the impact it may have on other organisational goals. This impact may lead to the introduction of new goals or to the improvement / adaptation of existing goals. Introduction of new goals may lead to the introduction of new processes while improvement / adaptation of goals may lead to the adaptation of associated processes accordingly. Repeating this process for every privacy goal and its associated organisational goals leads to the identification of alternative ways for resolving privacy requirements. The result of this process modelled in the spirit of and extended AND/OR goal graph.

Step 3: Model affected processes using privacy process patterns

Having identified the privacy-related processes these are modelled based on respective privacy patterns. Also, through the pattern analysis, PriS is able to suggest the proper implementation technique(s) that best support/implement these processes.

For every privacy-related concept introduced in the conceptual model of PriS a respective process pattern does exist. Patterns are expressed in the form of a generalised activity diagram as the one presented in figure 12.

Step 4: Identify the technique(s) that best support/implement the above processes

The last step is to define the system architecture that best supports the privacy-related process identified in the previous step. It should be mentioned that alternative system implementation architectures may be used depending on the privacy requirement that one wishes to achieve. Therefore, instead of prescribing a single solution PriS identifies and suggests a number of implementation techniques and architectures that best support the realisation of each privacy-related process in the system's development phase. The developer is then responsible for choosing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

which architecture is best for the developing system based on organisation's priorities such as, cost, systems efficiency etc.

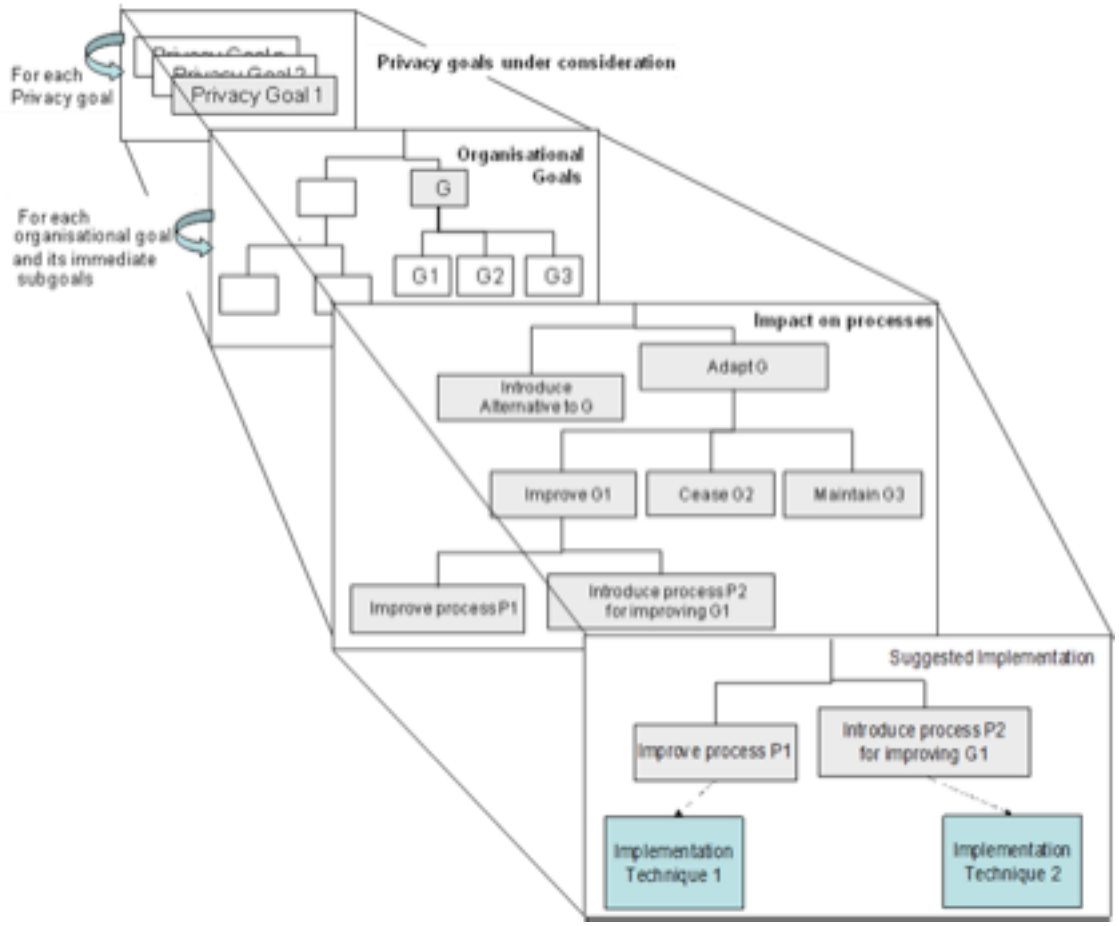

Figure 11. Analyse the impact of privacy requirements on business processes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

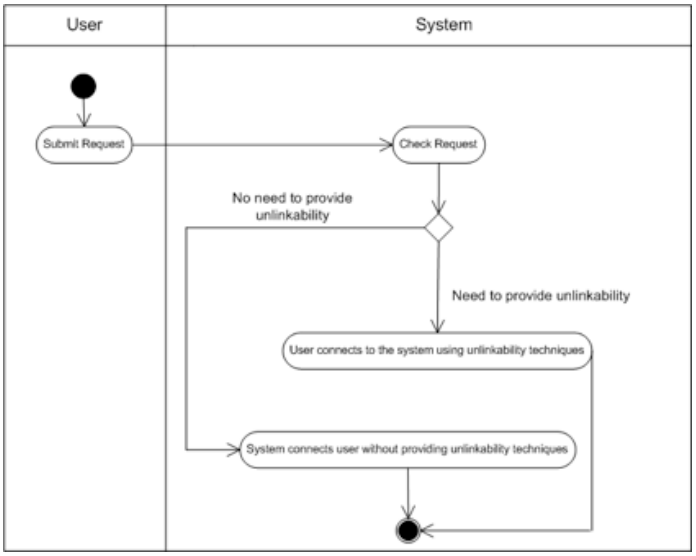

Figure 12. Unlinkability Process Pattern

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3. SAFERtec Attack Modelling Methodology

A generic approach combining the three methodologies (EBIOS-Secure Tropos-PriS) is presented below. We want a methodology that helps to get from the system description and threats knowledge a detailed, clearly justified and well-structured set of security requirements covering the threats. EBIOS is a very good tool to start the study and to help the methodology user by guiding him in the first steps the system and its security objectives definition, to then use those results as input for the second step of the methodology helping to derive "formally" the adequate security requirements for the different element of the system. Also, PriS provides an extra focus on privacy which is a very important topic in the field of ITS security, since we do not want vehicles to be trackable by anyone in the world. This is why, during the proposed process, a number of steps, deliberately include all three methodologies.

In order to provide a more efficient design of the unified methodology an alignment of the EBIOS concepts with the concepts of Secure Tropos and PriS was important in order to identify any conceptual conflicts or any similarities in the terms used. The alignment of the concepts is presented in table 1. Since Secure Tropos and PriS have their origins from the Software Engineering world there was no need to align their concepts as well. The necessary alignment was between EBIOS and the two other methods.

Table 2: EBIOS Concepts and Alignment with Secure Tropos and PriS

Concept	Meaning	Example	Concept Alignment with Secure Tropos and PriS
Entities	Main organization elements	Hardware, Software, Network, etc.	Resources (Assets) Actors
Essential Elements	Functions and information providing added value to the entities. They are linked to the Entities	A computational parameter is an essential element that is linked with the computer A and Software Process B	
Sensitivity	Security criteria that constraint an essential element. Avoiding the coverage of a security criterion there will be an impact on the organization through the linked entity.	Integrity, Availability, Confidentiality	Security Constraint Privacy Constraint

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Concept	Meaning	Example	Concept Alignment with Secure Tropos and PriS
Threat Agents	Natural, human, environmental threats, either accidental or deliberate	Earthquake, loss of password	Threat
Attack Methods	The knowledge derived by the combination of the sensitivity of the organization and the respective threat agents	Availability and denial of service attack	Attack method
Vulnerability	Each entity has a number of vulnerabilities that can be exploited by threat agents using attack methods	A denial of service attack (attack method) exploited by a malicious actor (threat agent) on the web server (entity) due to lack of cryptographic protocol usage (vulnerability)	Vulnerability
Security Objectives	The way that vulnerabilities are reduced thus reducing the potential risk on the entities	Protect the integrity of users' data in order to avoid unauthorized alterations from malicious parties.	Security Objectives Privacy Objectives
Security Requirements	The transformation of security objectives into security functionalities that are translated into functional requirements		Security Process patterns and plans Privacy Process patterns and plans
Assurance Requirements	Specific requirements that will guarantee the required level of		Security Measure Privacy Measure

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Concept	Meaning	Example	Concept Alignment with Secure Tropos and PriS
	confidence for the realization of the security requirements expressed as functional requirements		(Security mechanisms)

3.1 Stage 1: identification of Assets

- Stage Description

During this step EBIOS will be introduced in order to proceed with the identification of the respective entities that correspond to the main players of the system to be. In parallel with the significant entities the essential elements will be identified. Essential elements play a key role in the threat and attack modelling process since they represent functions and information providing added value to the entities. Entities and the respective essential elements will provide the first mapping of the system to be.

- Steps

Step 1.1 Identification of the respective Entities

Step 1.2 Identification of the respective Essential Elements

- Input:

Interview results with the stakeholders, Policy Statements, Project generic requirements

- Output:

List of Entities, List of Essential Elements

- Methods Involved: EBIOS

3.2 Stage 2: Organisational Domain Mapping

- Stage Description

During the second stage, it is essential to map the organisational context following the results of stage 1. Thus, the aim of this step is to understand the current organisational structure and based on the identification of the entities and the essential elements from stage 1 to identify entities like actors, organisational goals, plans, resources, services and infrastructure. This leads

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

to an efficient organisational analysis (in our case an efficient mapping of every use case) which is a mandatory prerequisite for the threat and attack modelling activities in the following steps.

- Steps

Step 2.1 Identify the list of Actors

Step 2.2 Identify Existing Organizational Goals

Step 2.3 Create the initial Organizational View Diagram

- Input:
  List of Entities and Essential Elements

- Output:

Actors, Organisational Goals, Plans, Resources, Infrastructure Components, Organisational View Diagram

- Methods Involved: Secure Tropos, PriS

3.3 Stage 3: Security and Privacy Constraints Elicitation

- Stage Description

Once the organisational needs have been identified, the next stage involves the identification of security and privacy constraints related to the organisational needs. Security and privacy needs are identified based on the security and privacy concerns that the organisation has. Thus it is important to identify, initially, the security concerns of the organisation and understand their linkage with the identified organizational goals. Identification of sensitivities will provide the first set of candidate security and privacy concerns per use case. Then, through Secure Tropos and PriS, the refinement of the sensitivities will occur considering the rest of the identified entities from the previous steps and the list of security and privacy constraints will be provided as output. These constraints will be the set of concerns that should be fulfilled along with every identified functional requirement.

It should be also mentioned that the input source for identifying the system's sensitivities and constraint lists can also be the organisation's policy. Relevant laws and regulations can also be considered to identify the set of security and privacy goals. It is important to note that the aim is not to ''blindly'' use any security and privacy constraint that the literature has captured but to identify those that are relevant to the organisational parts that are considered for deployment per project's use case.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Steps

Step 3.1 Identify the sensitivities

Step 3.2 Enhance the Security Constraints List

Step 3.3 Define the Privacy Constraint List

- Input:

Security Policy, Organisational Goals, Organisational View Diagram, Constraint Lists

- Output:

List of Sensitivities, List of Security Constraints, List of Privacy Constraints, Relationships between organisational goals and constraints

- Methods Involved: EBIOS, Secure Tropos, PriS

3.4 Stage 4: Threat and Attack Modelling

- Stage Description

During this stage, the threat analysis will be performed following the EBIOS process along with the methodology of the ETSI standard as it was described in section 3. During this stage, the identification of every threat per organisational goal will be conducted. Threat elicitation is of vital importance for capturing the external and internal sources that can cause harm to the assets of the system but also for validating that the identified security and privacy constraint lists are complete. Attack models will also be constructed for every identified threat per security and privacy constraint for every functional goal (organisational goal). Upon the completion of the specific step the Threat and Attack Models will be constructed representing all necessary knowledge in order to be combined with the vulnerability analysis and security and privacy requirements elicitation in the following step.

- Steps

Step 4.1 Identify Threat Agents and Attack Methods

Step 4.2 Create the Attack model Diagram

- Input:

  List of Sensitivities, List of Security Constraints, List of Privacy Constraints, Relationships between organisational goals and constraints

- Output:

  Attack Model Diagram, Threat Agent List, Attack Methods

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Methods Involved: EBIOS, Secure Tropos, PriS

3.5 Stage 5: Security and Privacy Requirements Elicitation

- Stage Description

The identification of the respective threat agents and the attack methods that can be deployed to the proposed system leads to the identification of the vulnerabilities that will be defined in the specific 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 realisation of the identified objectives. This step is critical since the security and privacy requirements list will have to satisfy the identified objectives in accordance with the security and privacy constraint list and the attack models described above. Finally, in the cases were measurable indexes can be established for examining the efficient implementation of the security or privacy requirements along with other parameters (e.g. safety) step 5.4 will contribute to this direction where the identification of the proper metrics for every security and privacy requirements will be conducted.

- Steps

Step 5.1 Define Security and Privacy Vulnerabilities

Step 5.2 Define Security and Privacy Objectives

Step 5.3 Define Security and Privacy Requirements

Step 5.4 Define Security and Privacy Metrics

- Input:
  Threat Model Diagram, Attack Model Diagram, Threat Agent List, Attack Methods

- Output:
  Security and Privacy Vulnerability and Objectives List, Security and Privacy Requirements List and the respective metrics when applicable.

- Methods Involved: EBIOS, Secure Tropos, PriS

3.6 Stage 6: Security and Privacy Requirements Analysis

- Stage Description

The final stage of the unified process is the security and privacy requirements analysis. The specific stage is of vital importance since all the information collected from the previous stages

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

will be modelled under a unified model in order to proceed in the identification of possible conflicts among security and privacy, obstacle recognition and avoidance, threat mitigation and vulnerability satisfaction, etc. Also, the identification of possible implementation scenarios for every security and privacy requirement will be realised in order for the stakeholders and the developers to select the most appropriate solution per use case.

- Steps

Step 6.1 Analyse Security and Privacy Requirements

Step 6.2 Identify possible Implementation Techniques

- Input:
  Security and Privacy Vulnerability and Objectives List, Security and Privacy Requirements List and the respective metrics

- Output:
  Enhanced Models, Implementation Scenarios, Conflict Reports

- Methods Involved: Secure Tropos, PriS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

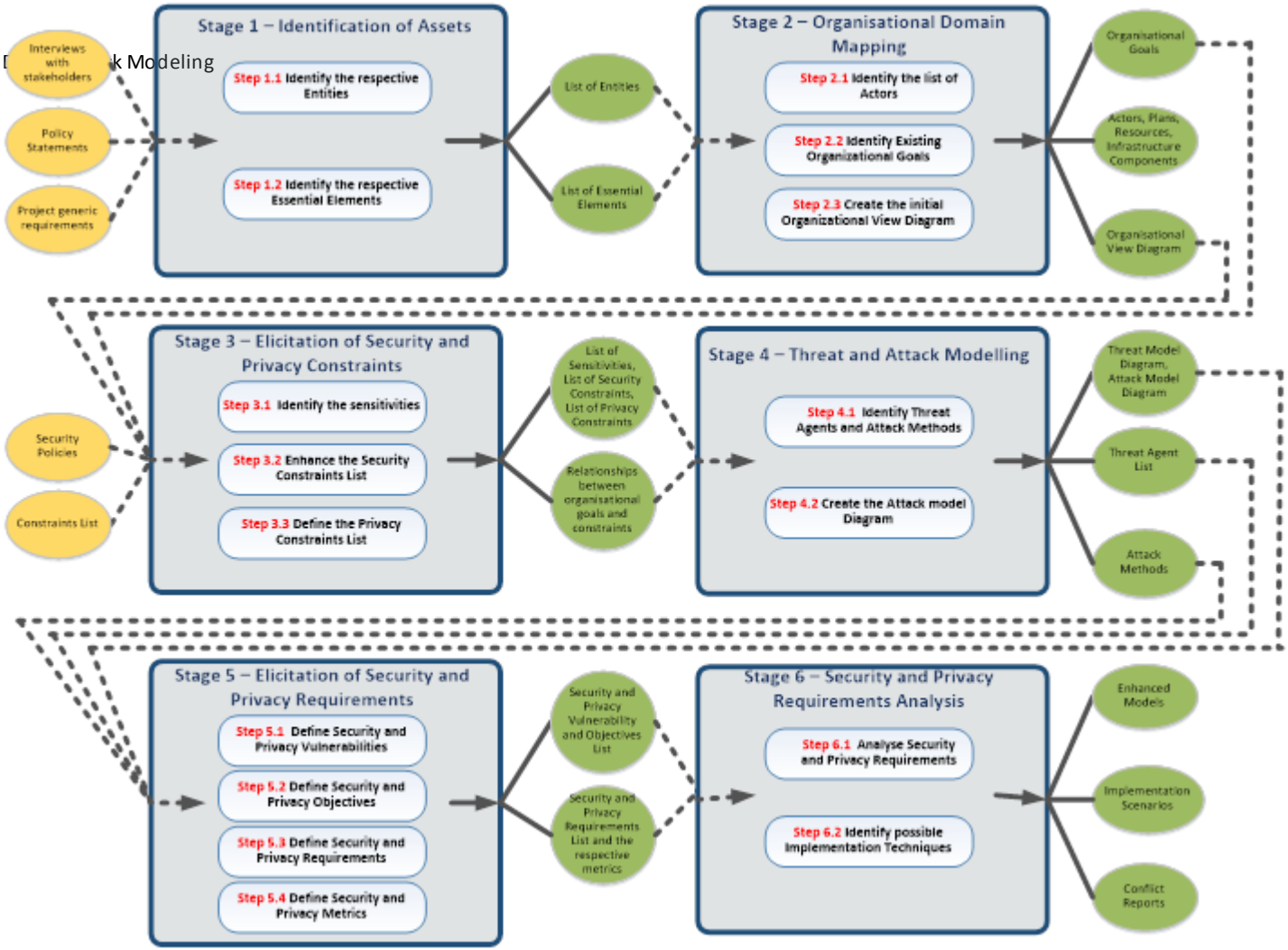

Figure 13. SAFERtec Attack Modelling Process

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4. Threat Elicitation based on ETSI Standard

In this section we present the application of ETSI standard as an initial mean of eliciting threats and essential functional assets for the SAFERtec project. The current threat elicitation has been conducted in all major SAFERtec use cases in order for the research team to be able to identify the following specific concepts per use case:

- Threats
- Attacks
- Targets of Evaluation
- System Assets (Functional and Data) for the main ITS components
- Security Objectives
- Privacy Objectives
- Reliability Objectives

The aforementioned concepts are derived from ETSI terminology. In any case ETSI cannot support the detailed elicitation process described in section 3. However, it is a valuable source of input for specific types of data for every use case and a valuable method for feeding the initial steps of the attack modelling method.

In the following sections a description of the ETSI standard and the elicitation of the respective concepts for the SAFERtec project use cases are described.

4.1 The ETSI Standard

In [19], the European Telecommunications Standards Institute published a technical report that summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) study for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) for Intelligent Transportation Systems (ITS) in 5.9GHz, i.e. using the ITS-G5 radio standard.

The specific document can be used as a guide and reference for the respective works and studies conducted within SAFERtec. However, it must be noted that the modelling work in SAFERtec has more generic features, since it considers a wide range of software and hardware components, functional units, networking and radio access protocols and data sources for end-to-end application scenarios. More specifically,

- The ETSI TVRA considers only vehicle to roadside unit (R-ITS-S) communication for V2I scenarios.
- The ETSI TVRA focuses on the on-board-unit (OBU) and its links for V2V and V2I. Entities like the Central ITS Station (C-ITS-S) or the Traffic Management Centre (TMC) are out of scope. However, in SAFERtec a holistic evaluation of the ITS framework is performed. This means that the level of complexity is increased significantly.
- The ETSI TVRA focus on security, while SAFERtec also deals with reliability and privacy concerns.
- SAFERtec includes cloud-enabled ITS services.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- SAFERtec supports multiple air interfaces, i.e. ITS messages may be exchanged either using ITS-G5 or conventional, legacy cellular networks (e.g. LTE).
- SAFERtec focuses on the V2I paradigm. Nevertheless, it is noted that the analysis results can be applied also in V2V systems.

Despite the differences, the ETSI TVRA can be used as a guide for the development of the SAFERtec models. In this section, an attempt to use the modelling and analysis principles provided in [19] is made. In order to properly modify the ETSI methodology to fit the SAFERtec objectives, extensions are proposed that are able to include the requirement set in terms of security, reliability and privacy for the end-to-end ITS architecture.

4.2 Determining the ITS application class and features

The specification of objectives, requirements and assets in terms of reliability, security and privacy depends on the type of ITS application under evaluation. The ITS reliability/security/safety architecture should cover the ITS Station (ITS-S) assets and software/hardware components, as well as the means of communication among ITS entities for a given application. The importance and criticality of each specified requirement depends on the application class. Thus, as a first step, the definition of an application class profile is necessary. In SAFERtec, several use cases are defined in [22]. As an example, we focus on the first three use cases. Each use case can be classified in an application class defined in [21]:

1. USE CASE 1: Traffic light optimal speed advisory – Application Class: Cooperative traffic efficiency – Application: Cooperative speed management.
2. USE CASE 2: Roadwork Warning / Traffic Condition Warning – Application Class: Active Road Safety – Application: Driving Assistance, Road hazard warning.
3. USE CASE 3: Emergency vehicle warning: - Application class: Active road safety – Application: Driving assistance Cooperative Awareness.

For each use case, a communication profile is specified. Each communication profile is vulnerable to different threats and attacks. More specifically:

USE CASE 1:

- Broadcast messages in ITS level.
- I2V link only, i.e. there is no need to investigate the vehicle as an information source.
- No session is established during communication (i.e. no acknowledgment in packet reception, or handshake is necessary in radio level)
- ITS messages are broadcasted with medium frequency
- Multi-hops (relays) are allowed.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

USE CASE 2:

- Broadcast messages in ITS level.
- Low frequency of messages.
- I2V for roadworks – Bidirectional broadcast communication for traffic conditions.
- Multi-hops are allowed
- No session established.

USE CASE 3:

- Broadcast messages
- High frequency of messages (during the emergency vehicle crossing).
- No session established.
- Single-hop, no relaying is allowed.
- All possible V2X directions may be considered.

The short profiles defined using the definitions in [19] and [21] cover the V2X communication counterpart, however, the backend of the use cases that includes communication of other relevant entities (e.g R-ITS-S, C-ITS-S, TMC links) is not defined.

4.3 Targets of Evaluation

In [19], each large scale, high level asset of the system is defined as a Target of Evaluation (ToE). Each ToE contains multiple functional and data assets. The identification of the potential ToEs is resulted by the architectural description of the use cases in [22] and [23]. It is clear that since SAFERtec should offer an end-to-end assessment approach, the number of ToEs increases.

Based on [19], the ToEs are analysed using the following assumptions:

- ToEs may be defined as two distinct functional units although, in practice, they may be manufactured as a single physical device comprising both functionalities.
- All communication and actions within the ToE are performed within the boundaries of a trust domain and are, therefore, secure.
- All ITS stations have connectivity to a proper respective network.
- The ITS services are amongst the defined basic set of possible applications.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Restricted data is only transmitted to authorized parties. Consequently, a station needs to have the ability to validate the identity and authority of the recipient before sending restricted data.
- The vehicles always know on which logical channels safety messages are sent and received at a given point in time (i.e. the vehicles have a validated network, medium access and facility layer).
- An ITS station has the ability to determine trustworthiness of received information (i.e. correctness of information).

Moreover, the following assumptions are considered for the ToE environment:

- Communication over interfaces on different ToEs are considered secure, when evaluating a specific interface.
- There is no 5.9GHz communication between roadside units or the cloud and the ITSs.
- Broadcast messages are not protected and assumed always to carry non-sensitive information (and as a consequence they should never carry personal data).
- Application and security parameter updates to an ITS-S may be made either using a direct, fixed interface or indirectly using a wireless (e.g. ITS-G5) interface.

It is noted that unlike [19], communication between ITS-S and the end user is in the scope of the SAFERtec framework.

As high-level assets of the use cases identified in [22], the following modules are identified:

- The vehicle ITS-S including all hardware, software and networking modules installed on the vehicle, or any other device carried on it.
- The R-ITS-S (also mentioned as RSU). For some application classes, The R-ITS-S acts as a gateway between the C-ITS-S and the vehicles. Both R-ITS-S and vehicle ITS-S are also considered in [1].
- The Central ITS-S (C-ITS-S) is considered as a central component of the ITS application. The C-ITS-S is responsible for the provision of accurate information to the vehicles and the R-ITS-Ss. It also maintains a registry of connected vehicles for a given area of control. C-ITS-S is also connected with a higher management entity, i.e. the TMC. Generally, it can be assumed that the TMC is the main source of officially validated data. However, since the C-ITS-S has the ability to communicate with all modules of the ITS chain, it also acts as a concentrator and evaluator of heterogeneous data originated from various sources. Based on the provided definition, the C-ITS-S is a typical example of a system that can be implemented using a shared pool of configurable resources (e.g. networks, servers, databases, storage devices). Moreover, it is based on a distributed system architecture (based on geonetworking criteria, service and application sets or providers etc.). Therefore, in the SAFERtec context, the C-ITS-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

S is a cloud computing system. The C-ITS-S services and applications may be hosted by either a private or public cloud. In the private cloud, the service provider also has the management and physical control of the resources that create the cloud. On the other hand, in a public cloud all data and computing resources are maintained and managed by an external cloud provider.

The C-ITS-S resources are interconnected using proprietary wired network infrastructure or using secured virtual private networks and tunnels. Through the same network infrastructure or instantiation of virtual networking, the C-ITS-S cloud communicates with the TMC. On the other end, the virtual servers of C-ITS-S are available to authorized ITS-S (roadside units or vehicles) through IP-based links established over the internet (most possibly using VPNs). As the information flows from the C-ITS-S virtual servers and data centers, radio access may be used (cellular 3G/4G connections) to establish connectivity with vehicles and R-ITS-S without wired network infrastructure.

The C-ITS-S may contain multiple functional components depending on the applications and services provided. The functional components may include a) collection, processing and storage of real-time traffic data from vehicles, b) dissemination of traffic/road conditions and incident information, c) dissemination of location-specific, situation-relevant information at R-ITS-S including traffic light management and control, d) distribution of customer-tailored traveler information (e.g. weather, lodging, parking and many more), e) collection and evaluation of data from R-ITS-S situation monitoring or data originating from sensors and measurement equipment positioned on the road network.

- The TT Cloud entity is also an ITS cloud service/application provider. In SAFERtec, the distinction between C-ITS-S and the TT cloud has been made in order to separate services offered by different SAFERtec partners (SWARCO and TomTom respectively). However, both ToEs can be modelled assuming similar functional and data assets. In practice, the differences between the two modules can be summarized in the following points:
    - The TT cloud operation depends on collecting data from the users. On the other hand, the C-ITS-S uses the TMC as the main source of information.
    - The TT cloud does not interact with the roadside units. It basically provides cloud-based services directly to the vehicles.
    - Depending on the use case, the TT cloud may extract information from the C-ITS-S.
- The Traffic Management Centre is considered to be the control and management entity of the authority that regulates the road network in a given area. Moreover, the TMC is responsible for the dissemination of officially validated data, thus, the TMC is the main source of information for the C-ITS-S. It contains various functional components, namely:
    - It collects and monitors data from traffic sensors and surveillance equipment.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- It fuses traffic and traveller information from other data centres. For example, the TMC may use information originating from cloud service providers (e.g. the TT cloud or the C-ITS-S)
- It disseminates traffic and road condition information (including incident information, driver information etc.)

In many cases, the TMC is considered to be the main executive agent of the ITS application. However, in SAFERtec use cases, the TMC actions are limited to data dissemination and update. Executive actions (e.g. dynamic message signs, dynamic speed limits, traffic light patterns and phases) are generally applied by the C-ITS-S services.

The TMC communicates with the C-ITS-S cloud services and applications through wired proprietary infrastructure and/or virtual private networks over public network resources. TMC also maintain connections with many information sources. However, the investigation of the specific interfaces is out of SAFERtec scope.

TMC can be implemented either as a conventional data center or as a cloud computing system. In the analysis presented in this document, the TMC is considered a data center or data farm constituted of proprietary bare metal servers properly interconnected through a local area network.

- The Traffic Light Controller (TLC) is an ITS entity that is responsible to control traffic light phases and patterns based on prioritization requests made by vehicular ITS-S. As an entity, the TLC can be seen as a service hosted by the R-ITS-S. The TLC is involved in use case 2.1.3 since it collects priority requests and performs respective actions by accepting or rejecting each incoming request. In several cases, the TLC is considered as a tool for collecting requests and applying specific actions, while request processing is performed and granted by a respective service executed by the TMC. In all cases, it is not necessary to model the TLC separately, as long as it is considered a subset of services that runs on the R-ITS-S and the TMC.

Communication between the defined ToEs is performed through specific interfaces and links. The ToE links and interfaces specified for the SAFERtec use cases is presented in the following figure. The specified links/interfaces are:

- The (A) V2V link (ITS-G5) between vehicular ITS-S's participating in the network. Link (A) is defined in [19].
- The (B) V2I/I2V link (ITS-G5) between R-ITS-S's and vehicles. Link (B) is also defined in [19].
- The (C_1) and (C_2) links for direct communication of cloud services with ITS-S through cellular networks. It is noted that links (C_1) and (C_2) share the same network connection and resources. However, they are defined as different links, since they may have different requirements, security mechanisms and protection profiles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- The (J) link, i.e. a wired or wireless IP connection (probably VPN) between the C-ITS-S and the R-ITS-S. Link (J) is also defined in [19].
- The (K) link between the TMC and the cloud service provider. The link is established through proprietary wired infrastructure or secure virtual networking.
- The (I) link between ITS clouds from different providers or application classes.

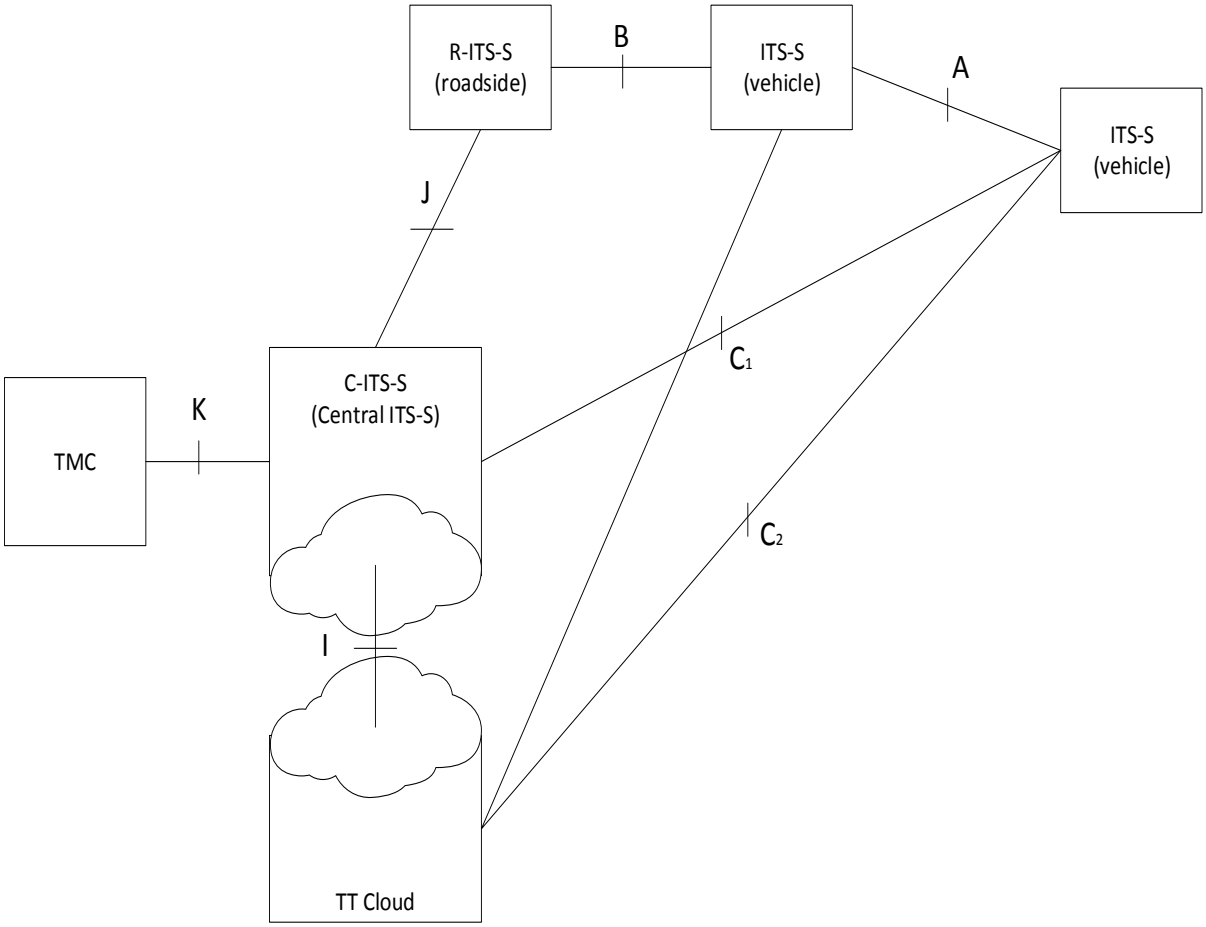

Figure 14: ToEs and interfaces/links for the SAFERtec ITS application set

In some cases, the link between the ITS-S and an external device carried by a passenger may be considered as part of the link/interface set of the ITS scheme However, based on the aforementioned definition of ToEs, these devices are considered as internal functional assets of the ITS-S system.

In SAFERtec, modelling and analysis should be performed for all identified ToEs and the corresponding links and interfaces per ToE. It is noted that all defined links are bi-directional. However, depending on the investigated application, some links may be one-way.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.4 System Assets (Functional and Data)

Each ITS functional entity contains a number of functional and data elements, called assets. In [19], it is proposed to define the functional and data assets for each ToE and determine all possible ways the set of assets interact with each other and with external entities (through the specified in put-output interfaces). In the following section, an attempt to model the high-level assets using the same approach is performed.

In the following figure the vehicular ITS-S system assets are presented. The specific block diagram extends the schematic presented in [19] in order to include all functionalities adopted in the SAFERtec use cases. The system assets are separated in functional assets and data assets.

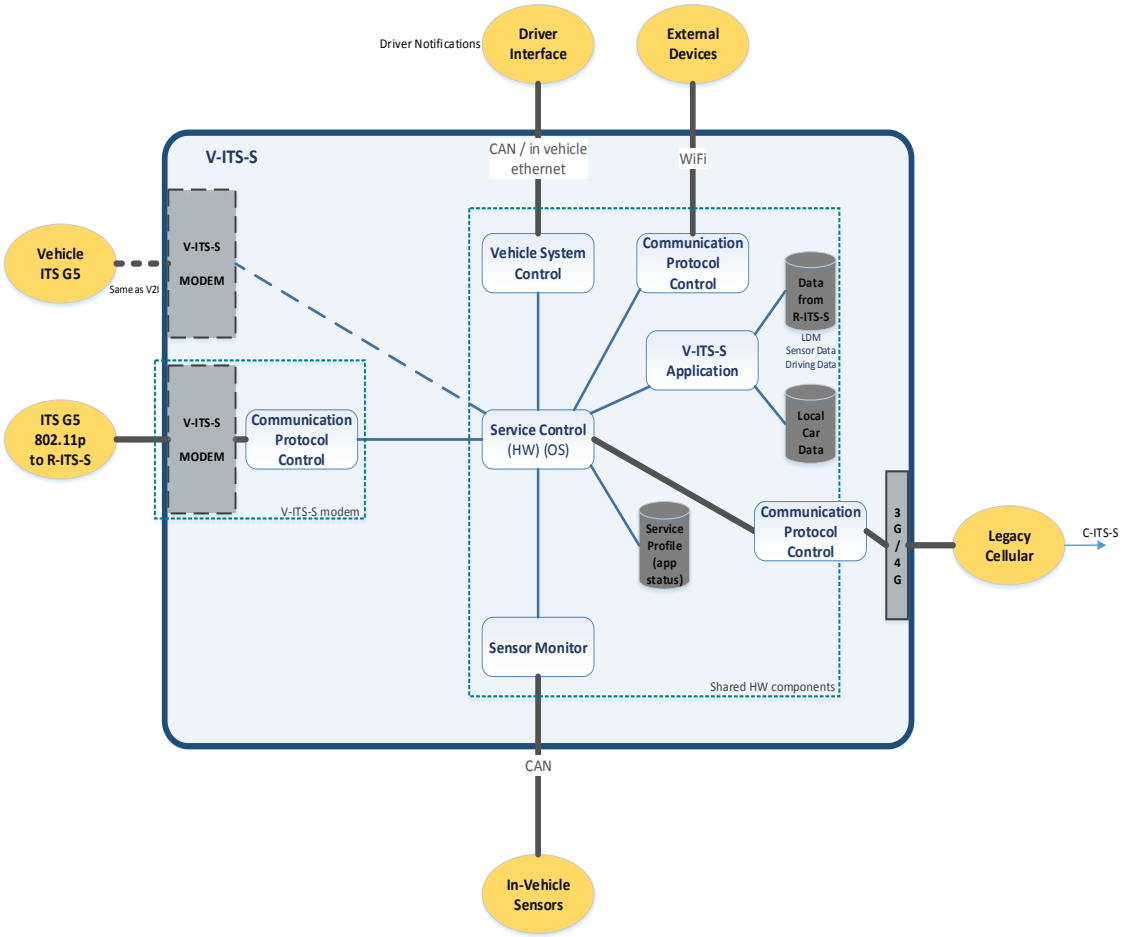

Figure 15: Vehicle ITS-S assets

4.4.1 ITS-S Functional Assets

1. *Protocol control*: With protocol control, the network/radio access/transmission techniques are considered. An appropriate message protocol for outgoing messages is selected and the message propagates through the protocol stack, until transmission. The respective inverse procedure is performed for incoming messages. The protocol control assets include the following links:

    - Interface (A) links between vehicles. V2V communication is enabled through the ITS-G5 protocol.

    - Interface (B) links between the ITS-S and the roadside unit. It includes all ad-hoc V2I/I2B messages between the vehicle and roadside infrastructure.

    - Interface (C) messages between the vehicle and the cloud services. The link is enabled through 3G/4G/5G radio access. Messages propagate through the core network of the network provider and through VPNs established over the internet, the vehicle can access the cloud-based service set.

    - An internal wireless network interface, the local in-vehicle WiFi network or possible Bluetooth links, that allow the interaction of the vehicle with devices carried by the driver or passengers (e.g. tablets, smartphones, notebooks, etc.)

2. *Service control*: It includes all assets that manage inter-process communications between assets without altering the content of communications. Service control is responsible for handling and managing:

- The hardware resources and the respective interfaces and networks that are shared into the vehicle.

- It manages all the services and defines all access rules that manage the interaction between assets.

- The list of applications installed and activated for transmission

- The list of applications installed and activated for reception.

- The list of applications installed but not activated.

- It implements an information exchange scheme between assets (e.g. a publisher-subscriber scheme).

Service control may originate messages for ITS-G5 transmission as heartbeats/beacons in order to maintain the ability to use a service and maintain a service profile.

3. *Applications*: It includes all assets/applications that evaluate and process ITS data for local use and determine when and how to initiate communications with other stations. Some examples of functionalities include:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Local Dynamic Map (LDM) maintenance.
- Evaluation of SPAT, DENM and CAM messages in order to, for example, propose an optimal speed (use case 2.1.1).
- Notify users (or impose specific actions) for incident or e.g., a near-by emergency vehicle.

An ITS application may originate messages for transmission using a communication interface (protocol control asset). Information exchange is enabled through the service control assets that manages all interactions.

4. *Sensor Monitor*: It includes assets that provide relevant environmental data to the Service Control for distribution to the other functional assets of the ITS-S. Different vehicles may contain different implementations of sensor monitor. The end-user may originate messages for transmission across the V2X or cellular links using the Sensor Monitor. Examples of sensor monitor information available to the vehicle include:

- GNSS data
- Vehicle telematics including speed, acceleration, steering angle, bearing, braking force etc.
- Tyre tread state, amount of fuel remaining etc.
- Human input received from a proper user interface.
- Radar measurements and other ITS-relevant data not collected through a cooperative ITS scheme.

5. *Vehicle System Control*: This asset allows other functional assets to access the vehicle control systems via service control. It includes notification/alarm actions like:

- Playing sounds or activating alarms during an event/incident.
- Providing information to driver only; to passengers only; to both driver and passengers through Human-Machine Interfaces (HMI).

It may also include more invasive actions like:

- Reconfiguring vehicle to reduce/prevent damages caused by imminent collision.
- Taking direct control of certain driving actuators.

4.4.2 ITS-S Data Assets

With the term Data Assets, we describe all sources of data that are available in the vehicle. Generally, it includes the following data sets/databases:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- *The Local Dynamic Map*: The LDM is an in-vehicle dynamically updated repository of data related to local driving conditions. It includes:
- Sensor data from all available vehicle sensors and modules that offer real-time information for the driving and vehicle status.
- Data and information extracted from the received ITS messages (SPaT, CAM, DENM etc.).
- Data from the cloud or the internet that may be used for route planning or driving/travel assistance.
- *The Local Vehicle Information*: It contains data that relates with the vehicle but that may not be immediately relevant to real-time driving decision. However, LVI data may be used for maintenance or may influence driving strategy. LVI may include: identification data (Vehicle Identification Number, license plate), manufacturer and model id's, inventory of components on the vehicle, known physical damages, service and maintenance status. LVI may also hold private information for the driver/vehicle owner such as: name, address, contact details, toll subscriber identity, credit card number etc.
- *Service Profile*: It contains all data that are used to define a certain service profile and a certain service control functionality. For example, it maintains a list of applications installed and activated for the vehicle and more over it contains data for access control and references to security parameters related to each application.

It is noted that the definition of assets is based on an operational perspective. This means that the identified assets may share common hardware resources. Thus, for SAFERtec, three different modems are used to provide software control. However, Service control, ITS Applications and data assets are implemented in a shared pool of resources that includes one or more processing units, an Ethernet and a CAN bus. More information for the respective hardware of the connected vehicle is presented in [23].

4.4.3 R-ITS-S Functional and Data Assets

The functional assets of the roadside unit are presented in the following figure. Similarly, to the vehicular ITS-S, the functional assets include protocol control, service control and ITS application modules. The basic definitions and principles of the functional assets remain the same. Thus, only the differences in the specification of the R-ITS-S vs. the vehicular ITS-S are highlighted:

- There is no protocol control asset for connectivity with local external devices (e.g. WiFi or Bluetooth). However, there are two possibilities regarding the implementation of link (J). Thus, it can be implemented either through wired infrastructure of proprietary or public network (and the possible establishment of a VPN), or through a cellular link using a legacy network.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Despite the fact that it is not prohibited, no use case imposes the need for direct communication among roadside units. Thus, no such link is defined.
- The Sensor Monitor mostly contains external environmental data such as temperature, humidity, rain, road slipperiness, ambient light level etc. It also provides information from cameras or other road/traffic monitoring equipment. The Sensor Monitor module also provides an interface for direct connection to the roadside unit by an authorized operator.
- The Display Control asset manages the information sent to external presentation devices. These include road signs, traffic lights, and other displays intended for use by an operator. The Display Control may be used by any other asset, if the specific action is accepted by the Service Control asset. When requested to display a message, Display Control will pass the information to the presentation device without regard of the content of the message.
- Data assets for the R-ITS-S are similar with those defined for vehicular ITS-S. The R-ITS-S also contains an LDM with locally collected data from telematics and sensors, as well as data extracted from ITS messages (coming either from vehicles or the cloud). It also contains road surface condition data and information about the physical environment.
- LVI is transformed to Local Station Information (LSI). It can be easily concluded that LSI contains a smaller set of information compared to the LVI.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

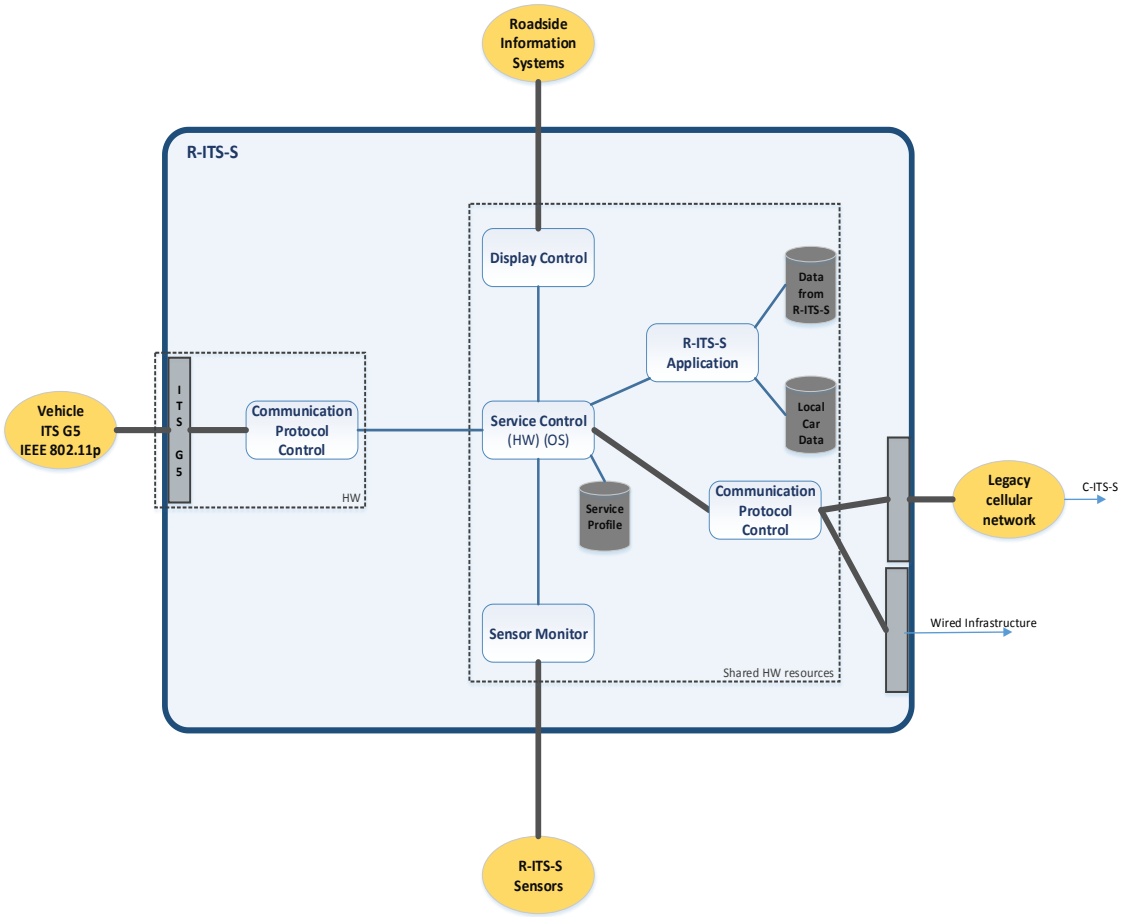

Figure 16: Roadside ITS station assets

4.4.4 C-ITS-S Assets / TT cloud Assets

As mentioned before, despite of their differences, both cloud service providers (C-ITS-S and TT) can be modelled using the same approach. The C-ITS-S model is presented in the following figure. An attempt was made to combine the modelling perspective of the ITS-S's and the common cloud computing modelling approach that defines the Infrastructure cloud, the Platform cloud and the Application cloud.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

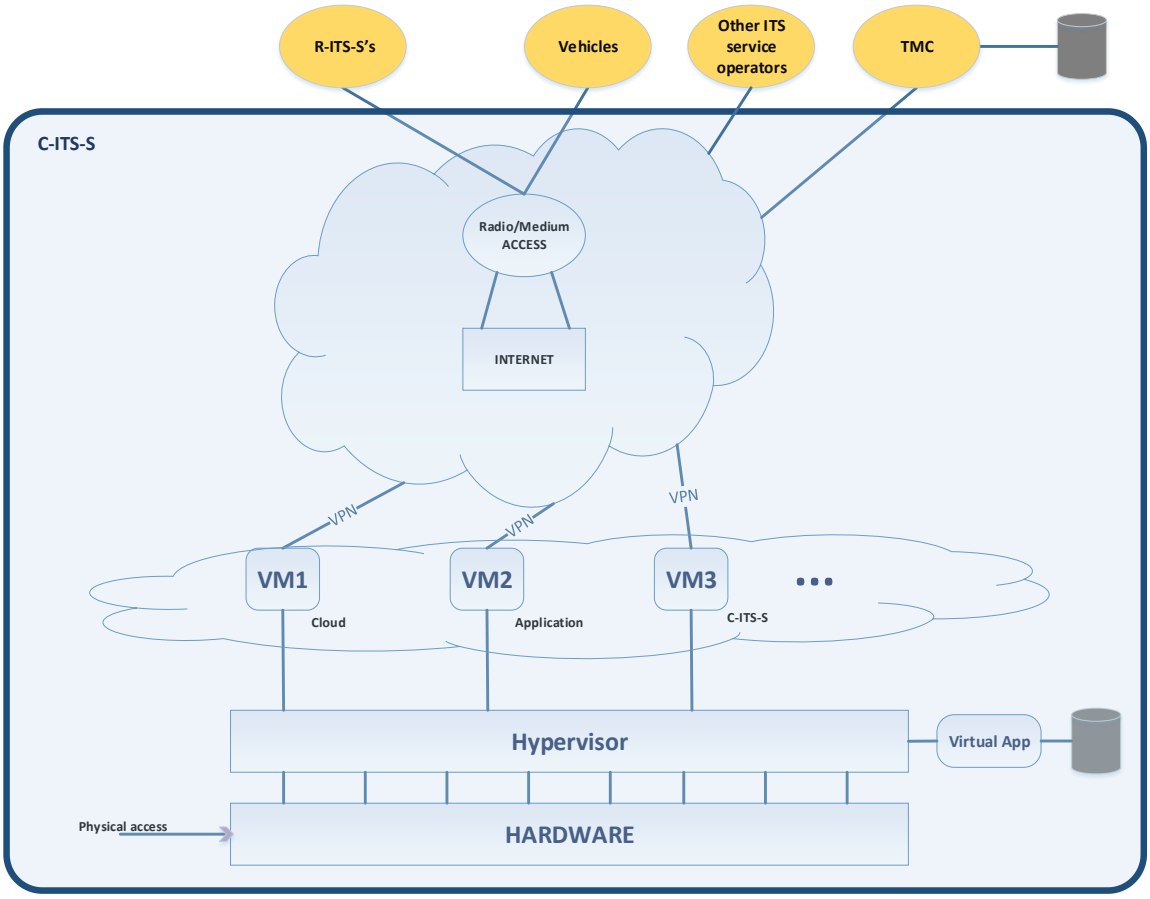

Figure 17: The Central ITS station assets

Based on this approach the following assets are defined:

- The Bare Metal Servers (BMS), i.e. the hardware that is used in order to implement the cloud. In private clouds, usually the BMS are located in specific areas (data centre, data/server farms). On the other hand, in public (or extended private) cloud architectures the BMS that share their computing resources may be located in many different places around the world. BMS have limited functional value in the C-ITS-S operation. However, they are considered as functional assets because more than 40% of cloud related failures are caused due to hardware failures and insecure interfaces. As far as insecure interfaces are concerned, it is noted that the BMS offer physical access interfaces to operators and users.
- The Hypervisor entity plays a role similar to the Service Control in the previous ToE analysis. However, it has now a far more complicated role, since it has the responsibility to manage the available BMC and coordinate and allocate the resources into Virtual Machines (VMs).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

It manages and distributes the platform resources (computational and network) and controls the application and service sets that are executed on the VMs.

- The VMs are the virtual servers that offer specific ITS services. Each VM may contain an ITS application. In many cases, a specific application is implemented with the distributed operation of multiple VMs. The VMs are able to exchange information (when allowed by the hypervisor). In correspondence with the previous analysis, the VMs provide similar functionalities with the ITS application blocks.
- The implementation of the cloud computing subsystem implies the existence of network resources that are used from the hypervisor to allocate resources to VMs and to monitor quality of service, as well as from the VMs to communicate with each other or the TMC, and, most importantly, to provide cloud based ITS services to vehicles and R-ITS-Ss. Since the existence of the underlying network is required, no protocol control is defined as a common functional asset. Practically, each BMS or VM has physical or virtual protocol control functional assets, however, these assets are considered an internal feature of the physical or virtual machine.
- Network-wise, all ITS actors are considered interconnected through an IP-based network infrastructure (most probably the internet). It is noted, that cloud-based services can be offered to vehicular nodes only through radio access with the use of legacy 3G/4G services.
- Depending on the offered cloud-based services, data assets that contain all the required, collected and processed data are maintained. These data repository can be physically or virtually distributed among the available resources. In order to simplify the analysis, we assume that the C-ITS-S maintains one extended LDM with data coming from multiple sources through ITS messages and one service data repository that is used from the hypervisor for logging, maintaining and improving the cloud functionalities.

4.4.5 TMC Assets

As mentioned in a previous section, the TMC may be implemented as a cloud computing system. In this case, the TMC should be modelled similarly with the C-ITS-S (with some minor modifications). Nevertheless, in this document, it is assumed that the TMC is a single cyber-physical system, that is defined with the guidelines used in the vehicular ITS-S's and R-ITS-S's.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

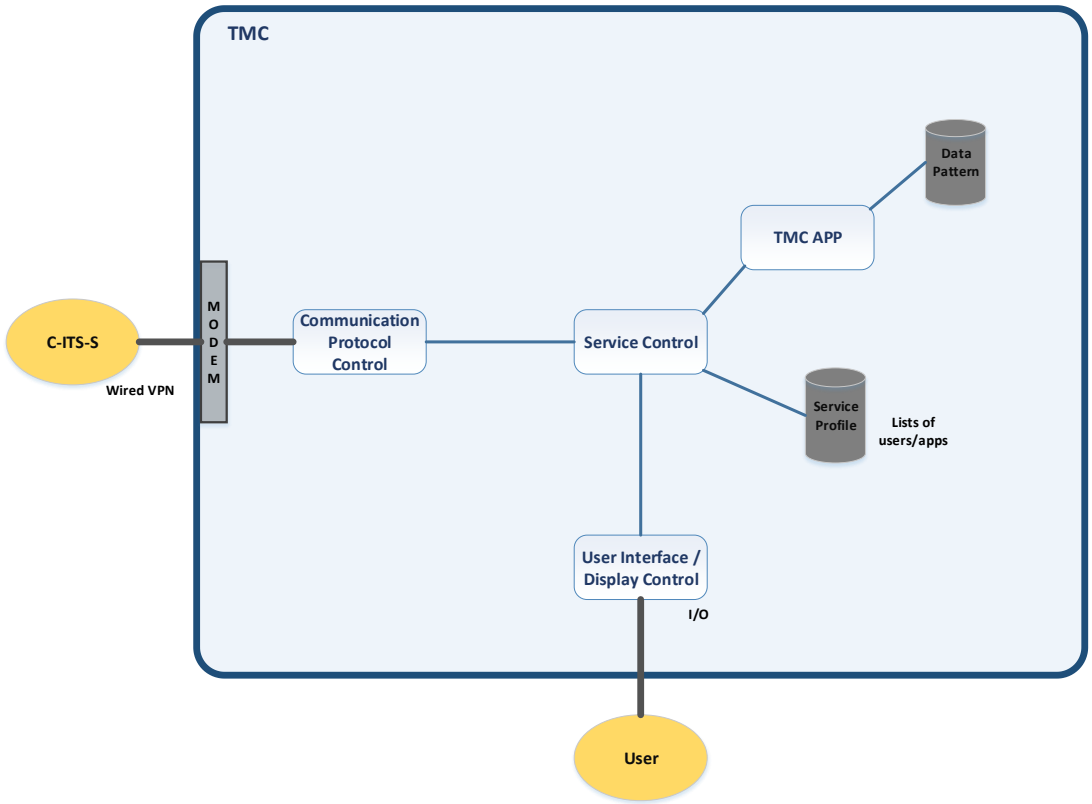

Figure 18: TMC assets

The TMC has a single protocol control asset that provides the (K) interface that implements the link with the C-ITS-S. It has no Sensor Monitor assets, since it does not directly measure any parameter values from its direct environment.

The TMC provides Input-Output interfaces for direct or indirect connection of an operator with the TMC system. The User Interface/Display Control functional asset provides all conventional input-output devices that may be used from any computer system.

The TMC also maintains two data assets: a) an extended Dynamic Map that contains data (any ITS-relevant information) for all areas controlled and monitored by the TMC. The size of the Dynamic Map may be extremely large depending on the TMC service area. These data are accessed and updated by the TMC applications that run on the TMC. b) the service profile data asset that contains all data used from certain service profile and a certain service control functionality.

Finally, it should be noted that the TMC model is simplified, since it does not contain links and data sources that are used to timely update the content of the Dynamic Map. This simplification is made, since SAFERtec will not be able to model, analyse and assess the specific TMC aspects, since no real-world TMC implementation will be used by the project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.5 Security, Privacy and Reliability Objectives

4.5.1 Security

The definition of requirements/objectives in terms of security is based on the analysis provided in [19], properly extended to cover all aspects of the SAFERtec paradigm. Thus, the security requirements are summarized as follows:

A. Confidentiality

i. Confidentiality of communications: Information exchanged should not be revealed to unauthorized entities.
ii. Confidentiality of application/service contained data: Information held within the ITS node should be protected by unauthorized access.
iii. Details relating to identity, services and capabilities of the ITS-S should not be revealed to unauthorized third parties.
iv. Confidentiality of management data exchange /signaling /coordination.
v. Location confidentiality in the communication links. ITS services carry various localization data in the messages. Unauthorized deduction of location should be prevented.
vi. Same with (v) for the route of the ITS subject.

B. Integrity:

i. Integrity of service – application: No malicious modification or deletion of data held and managed from the ITS.
ii. Integrity of communication: No malicious data modification/manipulation through transmit or receive paths from the ITS.
iii. Integrity of management data.
iv. Integrity of management data exchange /signaling /coordination.

It is interesting that the ETSI document distinguishes data/communication integrity and confidentiality between management and application data – indicating that each set of data has different impact in system security.

C. Availability

Access to the ITS services is not prevented by malicious activities.

D. Accountability

It describes the need to log, review and revert possible changes on an ITS application or service (updates, additions and deletions). It is a system that assigns accountability of actions for changes in the security parameters.

E. Authenticity:

i. It is not possible to act as an ITS-S (vehicular, R-ITS-S, C-ITS-S) without proper authentication.
ii. ITS-S's should not accept management and configuration information from unauthorized sources.
iii. Restricted ITS services (e.g. Use case 3) are only available for special authorized users.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.5.2 Privacy

As far as privacy is concerned, the confidentiality requirements identified in the security objectives can be also applied. Moreover, the following privacy-related requirement are identified:

A. ***Minimization of the Personal Information*** collected by the system. The system should only collect and use information relevant to its purposes.

B. ***Consent***: All entities that collect Personal Information from source systems or third parties should support a method of tracking consent when appropriate.

C. ***Redress***: When some individual disputes the accuracy of Personal Information or any output based on the disputed information, the system shall maintain a flag indicating that the information is in dispute.

D. ***Location/ Driver Privacy***: The location or/and identity of the driver should not be revealed even if the data transmitted between the car and the infrastructure are not utilized (e.g. through the car's number plates).

The aforementioned short profile description for the operation mode of the V2X/X2V communication subsystem should be repeated for all possible targets/assets/links in each use case.

4.5.3 Safety – Reliability

The following points indicate requirements in terms of reliability-safety, i.e. failures that may occur as a result of poor design.

A. Reliability:

It is the ability of the ITS-S to provide reliable services to the end user. ITS reliability may concern:

i. Reliability in communications, including acceptable Bit Error Rates /Packet Error Rates for given radio channel and interference conditions, as well as the incorporation of means (e.g. diversity scheme) to improve connectivity.
ii. Reliability in application/service level, i.e. that the application or service produces reliable and validated results.

B. Accessibility:

An ITS-S station will be granted access in the available resources in order to provide a service that has to follow specific requirements. Resources may be:

i. Network/Radio access resources (spectrum, time slots) that may suffer from congestion.
ii. Hardware/computer resources that may not be allocated properly and as a result an application fails.

C. Coverage and capacity:

This is strictly a communication-related objective. The network service should provide the required capacity and coverage to support ALL ITS services coexisting in the specific location.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

D. Quality of Service:

The main QoS metric that concerns the ITS systems is latency. Latency objectives are distinguished as follows:

i. Low-latency communications, that will ensure that the ITS message will arrive timely and serve its purpose.
ii. Low-latency services and applications, that will quickly decide on specific actions or produce warning messages etc.

E. Prioritization:

There are certain ITS users and vehicles (e.g. emergency vehicles) or roadside units that should be treated specially with the offering of special services. This is also the reason why:

i. A distinction between control and service channels is performed.
ii. EDCA function is used with prioritized queues during transmission.

Prioritization among messages (management or plain data) should also exist. It is emphasized that all safety-related objectives reflect on a given ITS service (i.e. the studied use case), however, it may be caused due to the fact that other ITS services share the same finite network/computational resources.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5. Modelling of the "Optimal Speed Driving" Use Case

5.1 Description of the Use Case

For the identification of threats and vulnerabilities that may threaten and affect a connected vehicle system, a case study has been performed, focusing on the main elements of the examined ecosystem, and the way the necessary information is transmitted.

This case study, named *Optimal speed driving*, aims at providing a speed advice to the driver who will be able to cross junctions without stopping at a traffic light if he decides to follow it. Consequently, the driver adjusts the vehicle's speed, either accelerating or slowing down, or keeping it steady, with never reaching a traffic light being 'red'. This scenario involves specific elements (components) which have been described in detail in Section 4, each of whom is responsible for transmitting the required information. In this scenario, the V-ITS-S of the vehicle communicates with the R-ITS-S in order to receive the necessary information and to display it to the driver, after the appropriate processing.

More specifically, the V-ITS-S Sensors Monitor collects the sensors data, which are distributed inside the vehicle, converts them in a suitable for the applications form and sends them to the V-ITS-S Service Control. The V-ITS-S Service Control is responsible for the processing of these data, alongside with the data it receives from i) the R-ITS-S, ii) Cellular data, which are sent from the C-ITS-S, and iii) data from external devices. After this processing, Service Control delivers the necessary LVI and LDM data, which are then sent to the V-ITS-S Application. V-ITS-S application stores this data to the respective LVI and LDM databases and finally transmits it to the driver interface, advising them accordingly, in order to optimise the driving speed. The communication among the V-ITS-S and the R-ITS-S system is achieved through ITS G5 802.11p, where a Communication Protocol Control is required.

5.2 Attack Modelling

This section describes the modelling of the Optimal Speed Driving Use Case following both the input from the elicitation conducted with ETSI and the reasoning made by the application of the proposed methodology in section 3. Since the scope of the deliverable is the threat elicitation and attack modelling, the proposed method is applied up to stage 4. In D.2.3 the identification of the respective vulnerabilities and the analysis of the identified security and privacy requirements (steps 5 and 6) will follow. Thus, the specific subsection will demonstrate the results from the application of the first four stages of the proposed integrated SAFERtec method.

5.2.1 Stage 1: identification of Assets

Step 1.1 Identification of the respective Entities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The scope of this step is to initiate the risk analysis phase. To identify respective assets in the architecture, CCS has constructed and shared questionnaires about what is typically important in terms of safety and privacy in the architecture for the given use cases. The questions adopted were focusing on the identification of assets, based on the use case description presented in D2.1, but also on the security and privacy concerns (in a generic level), functionalities, data, infrastructure and other related categories that could lead to the identification of valuable information. Although the questions that were addressed to, and answered by, the stakeholders (project partners) have a degree of subjectivity, as is always the case in the risk analysis process, they have fully utilized the expertise and experience of the project partners as well as the ETSI TVRA standard (section 4.1). The objective was to gather precise information and at the same time ensure that no crucial information will be omitted.

The following Table presents a sample of questions that have been used during the early stage of the risk analysis of each use case. These questions helped security experts to understand the use cases down to the very last detail and make sure that no ambiguity left. As mentioned before, these questions have been defined on the basis of the information already available (use case description of D2.1 and connected vehicle system specifications of D4.1), on the provision of the ETSI standard, and of course on the experience of the security experts.

Table 3 Sample Questions for Asset Elicitation

Number	Questions
1	Where are personal data stored? Which kind of data is personal?
2	What are privacy primary requirement?
3	Which data are critical for the vehicle safety?
4	Considering safety requirement, what are critical data stored, and exchanged between entities?
5	Where the critical data are being processed/stored?
6	Will the telematics (acceleration, pedal position, vehicle speed) data be exchanged between V-ITS-S and R-ITS-S?
7	Which functionalities are critical for the vehicle safety?
8	Which functionalities are critical for the privacy?
9	Which critical data are stored? Where?
10	What packet filtering (firewall) equipment for the data circulating on can bus?
11	What is the processing flow that leads to data displayed/communicated? (e.g. input data, processing functions, output data descriptions)
12	SAFETY Related APPLICATION: Where data are being processed? Where are they coming from?
13	Which packet filtering (e.g. firewall) for IP communications between V2X and Cloud?
14	What is V2X Transmission Mean defined in the interfaces excel sheet? (ITS G5 ?)
15	What are the specifications for R-ITS-S software, in-vehicle software, cloud based software?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Number	Questions
16	How are telematics data being processed, stored and transmitted between V-ITS-S and peripheral system? Are there persistent in memory?
17	Are data being exchanged always signed during transmissions, processing, storage phases? How?
18	Which other integrity check features is in place for data transmission between V-ITS-S, R-ITS-S, Cloud
19	Which confidentiality means are in place for data transmission between V-ITS-S, R-ITS-S, and Cloud
20	What are functionalities, interfaces, data accessed?
21	Which data will be displayed?
22	Which applications will be installed? What are the features expected from the HMI? What is the difference with the other HMI android?

Step 1.2 Identification of the respective Essential Elements

The only essential asset on optimal driving speed use case is the GLOSA Service providing the driver with the optimal speed driving such as he reaches the traffic light when it turn to green.

Table 4 List of Essential Elements

Essential asset	Description
GLOSA service	Service providing the driver with the optimal speed driving

Table 5 List of Support Assets

REF ID	Support assets	TYPE
SA-01	V2X On Board Unit	DEVICE
SA-02	HMI On Board Unit	DEVICE
SA-03	Smartphone HMI	DEVICE
SA-04	CAN Gateway	DEVICE
SA-05	Ethernet Gateway	DEVICE
SA-06	Safety Application V-ITS-S	DEVICE
SA-07	Wired communication link (R-ITS-S - Cloud)	DEVICE
SA-08	R-ITS-S	DEVICE
SA-09	Wi-Fi communication link	MEDIUM
SA-10	Mobile communication link	MEDIUM
SA-11	V2X communication link	MEDIUM
SA-12	C-ITS-S	DEVICE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5.2.2 Stage 2: Organisational Domain Mapping

Step 2.1 Identify the list of Actors

According to the aforementioned analysis, the main identified actors are the V-ITS-S, the R-ITS-S, the C-ITS-S and the TMC. However, due to the high complexity of the examined case, we decided to approach V-ITS-S and R-ITS-S entities as a system, which are further analysed to the following actors:

- For the V-ITS-S, the actors that we identified are the i) Service Control, ii) Sensors Monitor, iii) V-ITS-S Application, iv) Driver interface, v) three communication interfaces, the first responsible for the communication with the R-ITS-S via ITS G5 802.11p, the second responsible for the communication with the external devices, via in-car WiFi, and the third supports cellular communication.
- For the R-ITS-S, the actors that we identified are similar to the ones of the V-ITS-S. There we have i) Service Control, ii) Sensors Monitor, iii) R-ITS-S Application, iv) Display control, v) four communication interfaces, the first responsible for the communication with the V-ITS-S via ITS G5 802.11p, the second responsible for the communication with the external devices, the third for the cellular and the C-ITS-S communication, and the fourth interface supports the wired communication.

Step 2.2 Identify Existing Organizational Goals

Each actor has specific organisational goals that he has to fulfil.

Starting from the system of the V-ITS-S, we identified the following goals which are related with each actor.

- Service Control: Its ultimate goal is to "Acquire and transmit data". This goal is decomposed in the following subgoals: "Receive sensors' data from Sensors Monitor", "Receive data from R-ITS-S", "Process data for V-ITS-S Application", "Send LVI and LDM to V-ITS-S Application", "Send data to R-ITS-S", "Send data to external devices", and "Send data to cellular".
- Sensor Monitor: The ultimate goal is to "Handle sensors' data". This goal is decomposed in the following subgoals: "Collect sensors' data", "Convert sensors' data applicable for applications", and "Send sensors' data to Service Control".
- V-ITS-S Application: The ultimate goal is the "Local Vehicle data manipulation". This goal is decomposed in the following subgoals: "Receive data", "Store data", "Process LDM", and "Send LDM to Driver Interface".
- Driver Interface: This actor has one goal which is to "Display data" so as the driver to receive the necessary information.
- The three communication interfaces have the same goals and subgoals, since their functionalities are the same. Thus, their goal is to "Communicate data through [the specific way of communication, i.e. ITS G5 802.11p, in-car WiFi, and cellular, respectively]", which is decomposed in the subgoals "Broadcast vehicle data" and "Receive data [to/from the specific system that each interface communicates with, i.e. R-ITS-S, external devices, and cellular, respectively]".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Then the actors of the R-ITS-S have the following goals:

- Service Control: Its ultimate goal is to "Acquire and transmit data". This goal is decomposed in subgoals: "Receive sensors' data from Sensors Monitor", "Receive data from V-ITS-S", "Process data for R-ITS-S Application", "Send LVI and LDM to R-ITS-S Application", "Send data to V-ITS-S", "Send data to external devices", "Send data to cellular", and "Send data to wired interface".
- Sensors Monitor: The ultimate goal is to "Handle sensors' data". This goal is decomposed in the following subgoals: "Collect environmental data", "Convert sensors' data applicable for Applications", and "Send sensors' data to Service Control".
- R-ITS-S Application: The ultimate goal is the "R-ITS-S data manipulation". This goal is decomposed in the following subgoals: "Receive data from Service Control", "Store data", "Process LDM", and "Send LDM to Display Control".
- Display Control: This actor has one goal which is to "Display data".
- The four communication interfaces that facilitate the communication of the R-ITS-S with the other entities have the same goals and subgoals, since their functionalities are the same. Thus, their goal is to "Communicate data through [the specific way of communication, i.e. ITS G5 802.11p, in-car WiFi, cellular, and wired, respectively]", which is decomposed in the subgoals "Broadcast R-ITS-S data" and "Receive data [to/from the specific system that each interface communicates with].

Regarding the C-ITS-S actor, its ultimate goal is to "Manage and Coordinate communication" which is decomposed to the following subgoals: "Collect V-ITS-S data", "Process V-ITS-S data", "Store V-ITS-S data", "Distribute data to R-ITS-S, "Distribute data to TMC", "Distribute data to V-ITS-S", "Collect R-ITS-S data", and "Evaluate R-ITS-S data".

Finally, for the TMC, we have two ultimate goals, the first is "Acquire and transmit data" which is decomposed to the subgoals "Collect data", and "Distribute data" and the second is "Process data" which is decomposed to the subgoals "Process data", and "Fuse data".

Step 2.3 Create the initial Organizational View Diagram

Based on the analysis conducted in Step 2.2, in this step the organisational diagrams of the main subsystems namely V-ITS-S, R-ITS-S and C-ITS are constructed for showing every goal and subgoal than needs to be fulfilled, along with the respective resources as well as the internal and external connections in and out of every subsystem.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

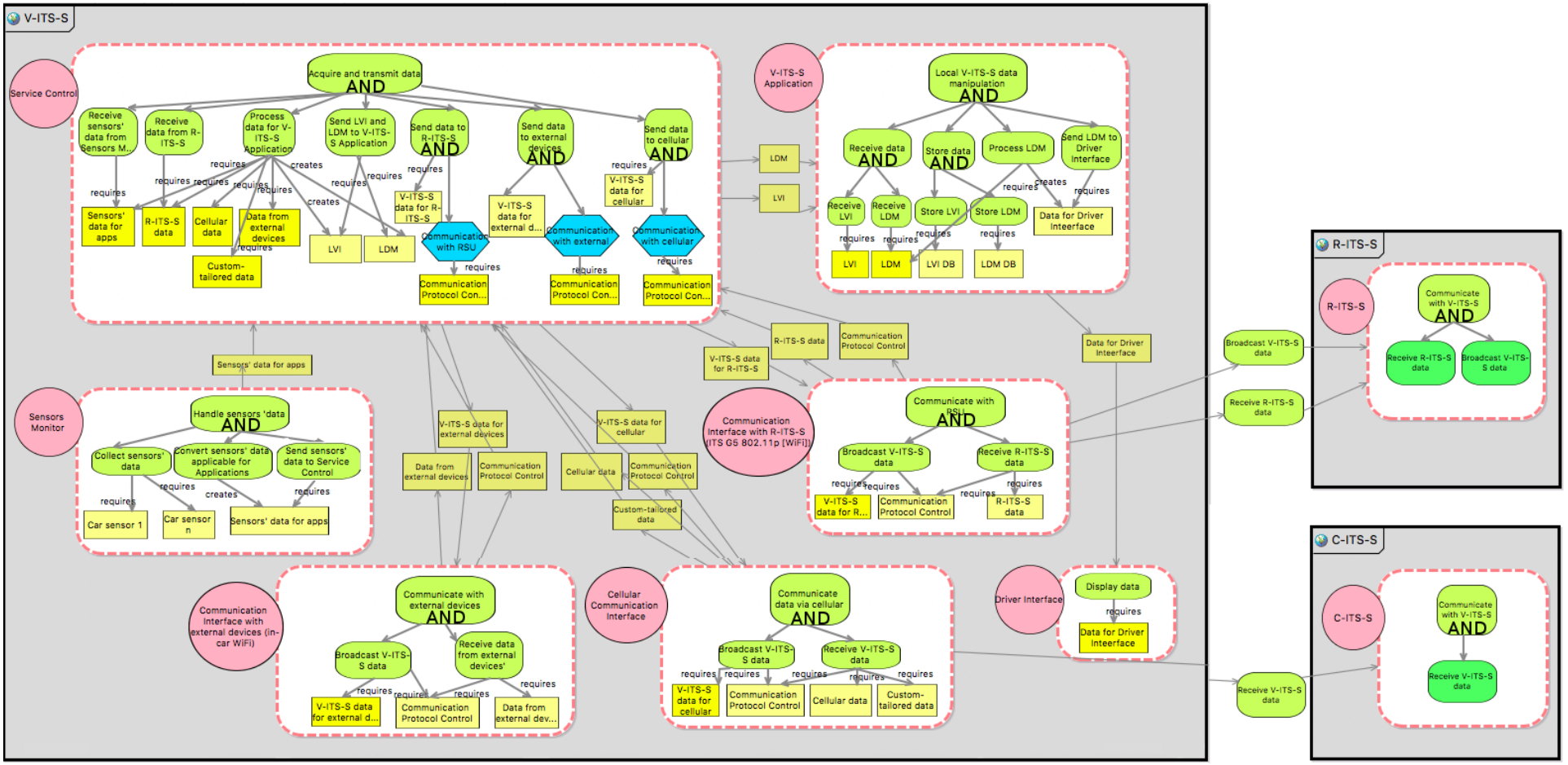

Figure 19: The V-ITS-S Organizational View model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

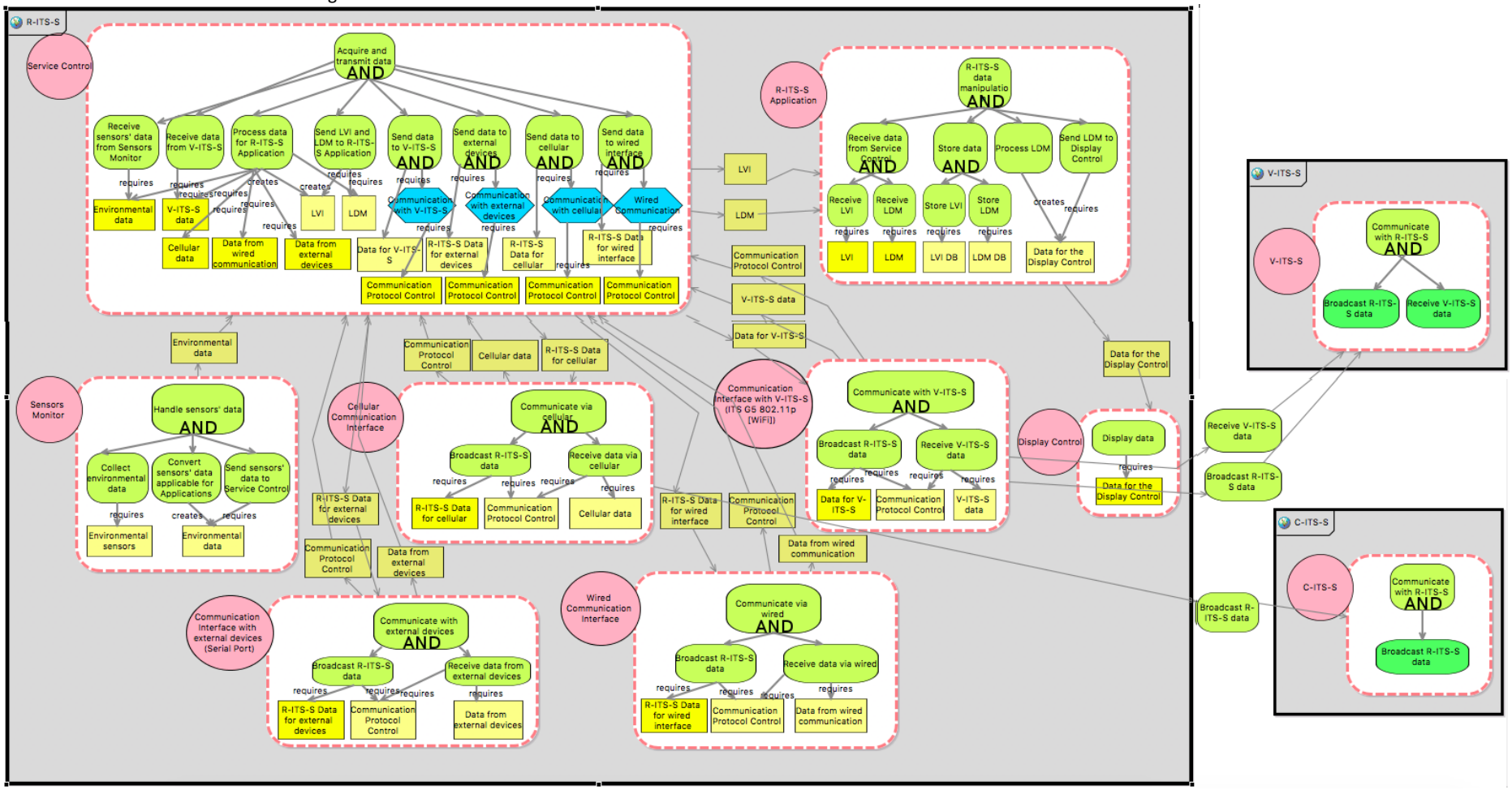

Figure 20: The R-ITS-S Organizational View model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

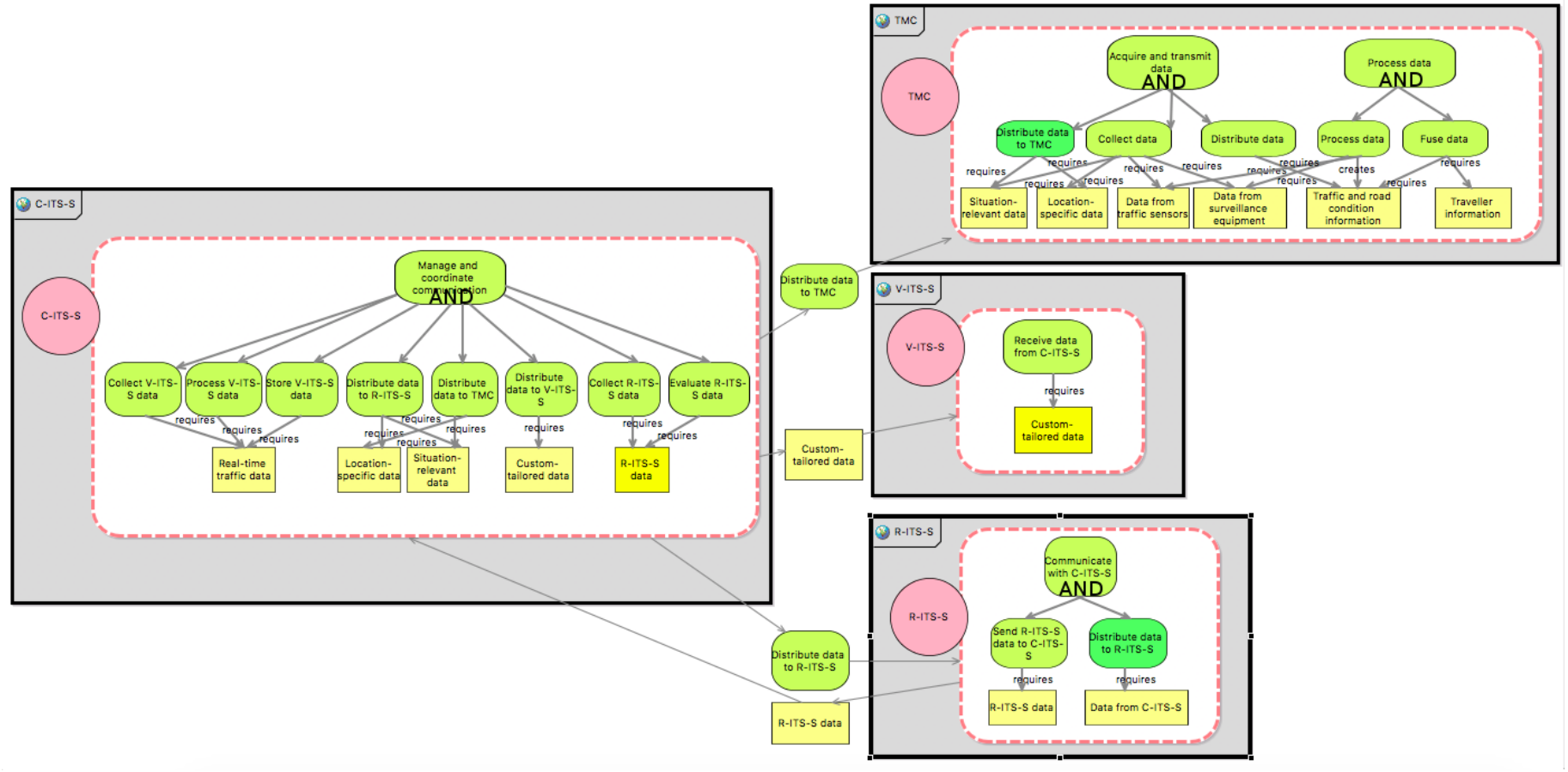

Figure 21: The C-ITS and TMC Organizational View model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5.2.3 Stage 3: Security and Privacy Constraints Elicitation

Having identified the main functionality of the "optimal speed driving" scenario together with the main entities / assets involved, it is necessary to proceed with the elicitation of the safety, security and privacy requirements.

Step 3.1 Identify the sensitivities

For the specific uses case the main safety issue is to ensure that the information presented to the driver is accurate, thus related to the security (integrity) constraints presented to step 3.2. Taking into account that the information has only an informative role and that it does not intervene with other car systems, it can be deduced that safety issues are not critical.

Step 3.2 Enhance the Security Constraints List

For the "optimal speed driving" scenario the main security constraints are related to the integrity and availability of the information communicated to the car. More specifically:

- Integrity, in terms of accuracy, of the information transmitted from the C-ITS to the R-ITS-S
- Similarly, integrity of the information broadcasted from the R-ITS-Ss to the cars.
- The availability of the service is not prevented by malicious actors at the C-ITS or/and R-ITS-S
- The availability of the service is not prevented by problems in the communication links between C-ITS-S and R-ITS-S as well as R-ITS-S and car.
- The authenticity of the C-ITS and R-ITS-S must be ensured.

The aforementioned constraints apply to both:

- The communication links between C-ITS-S and R-ITS-S as well as R-ITS-S and car.

The application and service control of the involved entities.

Step 3.3 Define the Privacy Constraint List

In the specific Use case, no personal (driver or vehicle) information is communicated and thus there are no privacy issues involved. However, since the models that we have developed capture most of the functionalities of each actor, we have identified privacy constraints that affect the data related with the owner of the vehicle.

The three following Figures, partially present the security and privacy constraints of the V-ITS-S, R-ITS-S and C-ITS-S actors, respectively.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

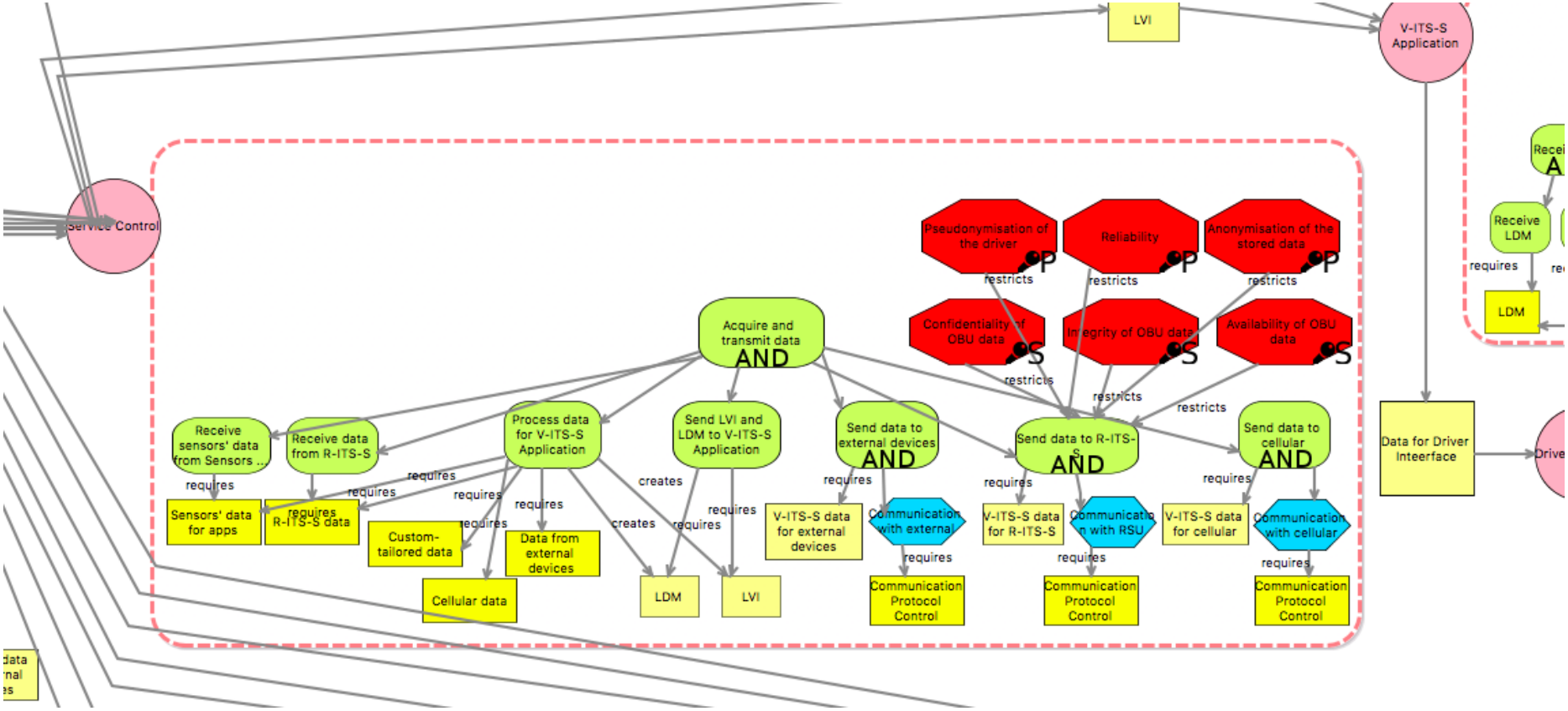

Figure 22: Partial View of the V-ITS-S Security Constraints View model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

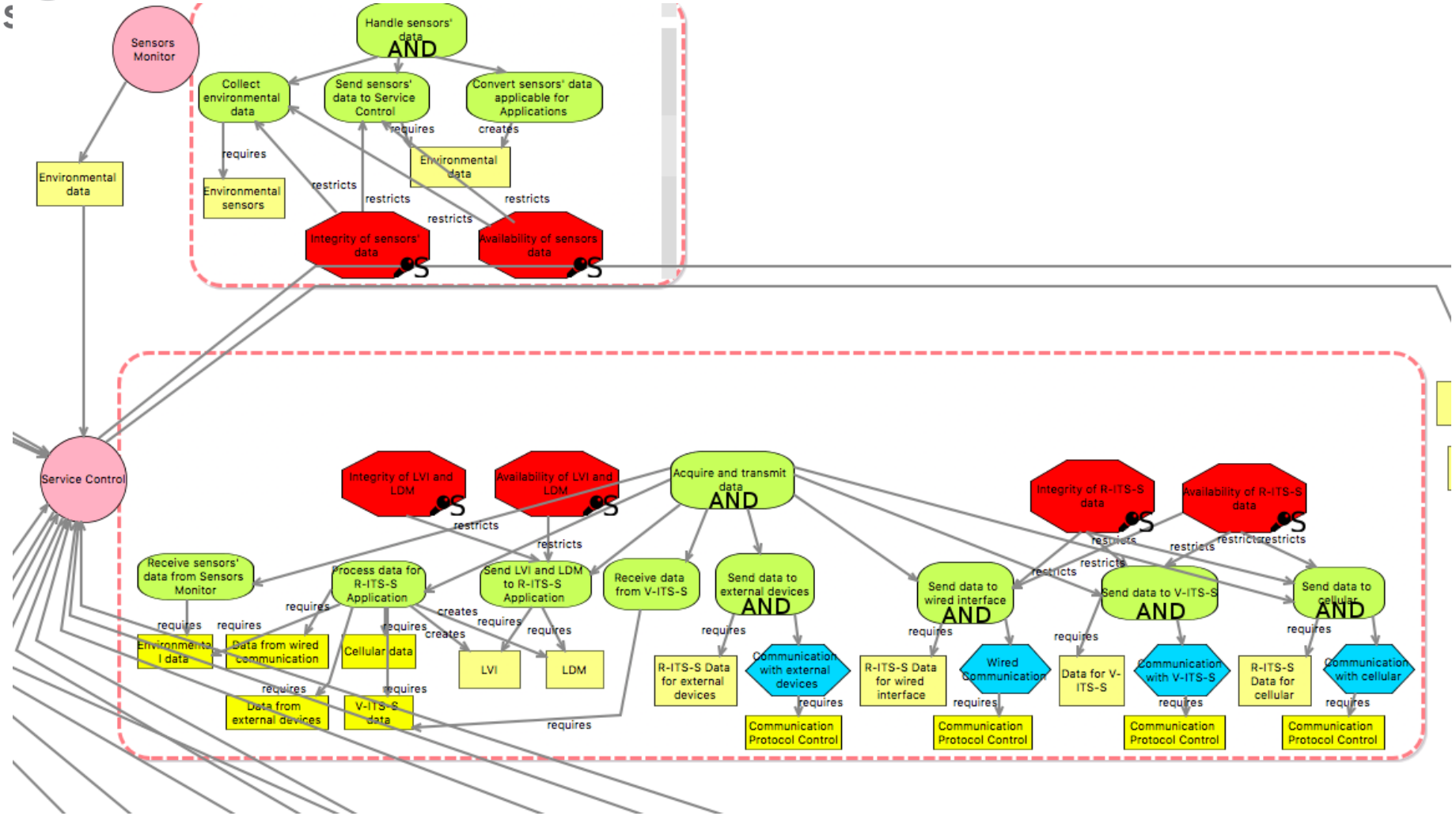

Figure 23: Partial view of the R-ITS-S Security Constraints View model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

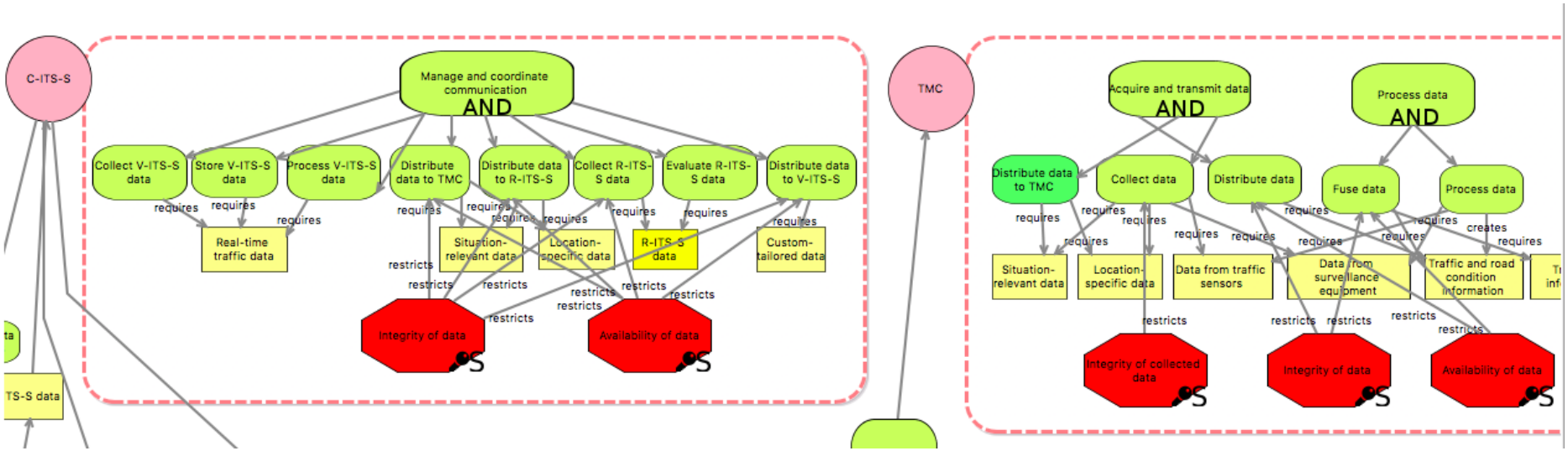

Figure 24: Partial view of the C-ITS-S and TMC Security Constraints View model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5.2.4 Stage 4: Threat and Attack Modelling

Step 4.1 Identify Threat Agents and Attack Methods

In this step the respective threats for the specific use case are identified. For raising the readability of the deliverable, the threats are presented per identified asset. The following table lists the threats (for each asset) that have been retained for the optimal speed driving use case. They may affect devices, software/systems or communication links.

Threat ID	Threat	Observation	TYPE
TH-01	Radio Jamming	Intentional disturbance of the communication link layer by decreasing the signal-to-noise ratio.	MEDIUM
TH-02	Link layer flooding	Denial of service attack which consists in sending a large amount of useless frames making the network unusable.	MEDIUM
TH-03	Equipment spoofing	Impersonation of a legitimate equipment.	MEDIUM
TH-04	Man-in-the-middle attack (Data manipulation)	Secretly relaying and possibly altering the communication between two parties who believes they are directly communicating with each other.	MEDIUM
TH-05	Communication Eavesdropping	Secretly listening a private communication.	MEDIUM
TH-06	Electromagnetic interference disturbance (unintentional)	Unintentional disturbance of the communication link layer generated by external source.	MEDIUM
TH-07	Sabotage	Deterioration or destruction of the medium.	MEDIUM
TH-08	Firmware alteration	Alteration of the low level firmware such as the equipment changes its behaviour.	DEVICE
TH-09	Firmware erasing	Alteration of the low level firmware such as the equipment cannot run properly anymore.	DEVICE
TH-10	Firmware reverse engineering	Firmware analysis for vulnerability detection.	DEVICE
TH-11	Degradation due to impact	Physical degradation of an equipment due to a weighty impact.	DEVICE
TH-12	Degradation du to bad weather	Physical degradation of an equipment due to bad weather.	DEVICE
TH-13	Electromagnetic interference disturbance	Unintentional disturbance generated by an external source that affects an electrical circuit.	DEVICE
TH-14	Sabotage	Untentional deterioration or destruction of an equipment.	DEVICE
TH-15	Extreme solicitation	Denial of service attack which consists in sending a large amount of requests to a listenning service making it unavailable.	SOFTWARE/SYSTEM
TH-16	Malicious code injection	Malicious code injection through a communication link.	SOFTWARE/SYSTEM
TH-17	Malformated frame injection	Malformated frame injection through a communication link.	SOFTWARE/SYSTEM
TH-18	System alteration after unauthorized access to maintenance port	Accessing a maintenace port without authorisation and taking advantage of the high privilege to altere the system.	SOFTWARE/SYSTEM

Table 6: List of Threats considered on all use cases

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The identified threats, listed in the previous Table, are the outcome of the ETSI TVRA standard (section 4.1) and the interviews conducted with various stakeholders and experts related to the project (section 5.2.1). The answers received were post processed to extract the threats that are the most relevant to the chosen use cases. This list is complete taking into account the type of threats known today. Evidently, it is not possible to consider threats that are unknown today but may appear in the following years. Although the industry needs a kind of certificate that could guarantee that a system is unbreakable, this is not possible. The system can only be protected until a certain level, meaning that it will resist to attacker(s) with certain knowledge.

Considering the list of threats of Table 6 and the list of threat sources of Table 7, it can be assured that the security level of the considered system will be high enough to meet the security objectives of an ITS system and this will be confirmed during the test phases of the project in the following work packages.

The list of threat "sources" is listed below.

ID THSR	Threats sources	Cause	Origin	Capability	Retained
THSR_01	Animal activity	Non-human	External	Weak	Yes
THSR_02	Vehicle crash	Non-human	External	Medium	Yes
THSR_03	Meteorological phenomena	Non-human	External	Unlimited	Yes
THSR_04	Script-kiddies	Human	External	Weak	Yes
THSR_05	Vandal, terrorist	Human	External	Unlimited	Yes
THSR_06	Hobbyist	Human	External	Medium	Yes
THSR_07	Competitor	Human	External	Medium	Yes
THSR_08	Criminal organization	Human	External	Unlimited	Yes
THSR_09	Foreign state	Human	External	Unlimited	Yes
THSR_10	Ex-employee	Human	External	Medium	Yes
THSR_11	Administrator	Human	Internal	Unlimited	Yes
THSR_12	Developer	Human	Internal	Medium	Yes
THSR_13	Maintenance/Support	Human	Internal	Weak	Yes
THSR_14	ISP	Human	External	Medium	No
THSR_15	External radio source	Non-human	External	Medium	Yes
THSR_16	Power failure	Non-human	External	Weak	Yes

Table 7: List of Threat Sources

In the following table, a list of attack methods is defined. This set contains all identified attack methods that may implement or facilitate a threat contained in Table 9 to Table 18.

Table 8: List of Attack Methods applied to SAFERtec use cases

Attack Method	Attack Types	Description
Denial of Service (DoS)	- Message saturation, Denial of access to incoming messages.	The availability of network or system applications, resources and services are

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	- Protocol alteration/misuse - Denial of access to outgoing messages. - Denial of access to system resources. - Denial of access to data sources. - Denial of transmission. - Denial of data receipt.	compromised. In wireless networks, this type of attack is typically accomplished by disabling one of the interacting entities in the data exchange. A common method is to create a greedy user that does not unfairly occupies the access medium or resource pool, preventing other users of using it.
Jamming (Ja)	- Provocation of interference with noisy signals, electromagnetic disturbance.	The disruption of a communications system such as a wireless network through the intentional use of electromagnetic interference. Jamming blocks a signal or message between two interacting. An attacker sends a signal with a significantly greater signal strength relative to normal signal levels in the system to flood the channel. Thus, jamming is effectively a simple but effective form of DoS attack. Jamming can be performed by a single attacker or multiple attackers working together.
Masquerading (Mq)	- Eavesdropping - Impersonation attacks - Acquisition of personal information. - Acquisition of behavioral details. - Acquisition of location information, GNSS tracking.	An attacker impersonates an authorized entity to gain access to network applications, resources, or services
Man in The Middle (MiTM)	- Eavesdropping + MM - Infrastructure spoofing - DNS spoofing - Circumvention of mutual authentication - Sybil attack (multiple fake identities)	Man-in-the-middle attacks involve a double masquerade, where the attacker convinces the sender that she is the authorized recipient of a message on one hand, and convinces the recipient that she is the authorized sender of the message on the other. Man-in-the-middle is the most common method for radio communication interception.
Malware Injection (MI)	- Message Injection -Injection of false messages - Bogus Information or Forgery Attack - Worm, Trojan, blended threat infection.	Equipment posing as genuine ITS-S (vehicle) sending false information in ITS messages that are otherwise valid

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Message Modification (MM)	- Modification or deletion of transmitted information. - Modification or deletion of published information. - Modification of stored information	An attacker alters packets by inserting changes into them, deleting information from them, reordering them, or delaying them. Usually combined with MiTM or MI attacks.
Replay attack (Re)	- Replay of expired messages. - Wormhole attack - Relay attack (in conjunction with MiTM) - Pre-play attacks	Equipment posing as genuine ITS-S sending "expired"-outdated-misleading information in ITS messages that are otherwise valid.
Routing attack (Ro)	- Routing table poisoning - Packet mistreating attacks - Router hit & run or persistent attacks - Router spoofing	Interference with the correct routing of packets through a network. Corruption of scheduling schemes that prevent access to resources. Several different types of routing attacks can be carried out at the network layer, including spoofed, altered, or replayed routing information. These attacks can create routing loops, extend or shorten intended routing paths, generate bogus error messages, and increase end-to-end latency, thereby compromising availability.
Side Channel (SC)	- Cache attack - Timing attack - Wireshark-monitoring attack - Electromagnetic and power monitoring attack - Differential fault analysis - Data remanence	A side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. Side channel attacks are attacks based on Side Channel Information. Side channel information can be retrieved from the investigated device by observing behaviors and patterns, with neither the plaintext to be encrypted nor the ciphertext resulting from the encryption process.
Co-Residence (CR)	- Information gathering. - Misuse of shared physical resources. - Perform DoS	A co-resident attack targets the virtualisation level, i.e. it is a cloud-specific attack. In this type of attack, the attacker has a clear set of target virtual machines (VMs). By co-locating the attack VMs with the target VMs on the same physical servers, the attacker intends to degrade the target VM performance by misusing shared resources,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

		extract private information of the victim, perform DoS attacks etc.
Physical attack (Ph)	- Vandalism. - Sabotage. - Hands-on intervention to shut down, restart, cause general failure to a system resource.	It includes all attacks that require physical access and action to an asset, e.g. an attack implemented with the destroying of an asset or a resource.

As a next step, the identified attack methods were assigned to each threat per asset. The threats and corresponding attacks per asset are presented in the following tables. Methodologically, identification of attack methods is performed with the following three-step procedure:

1. Determination of threats per asset.
2. Identification of active interfaces that may allow access to the asset and implement a threat.
3. Identification of attack methods that could implement a threat through the available interfaces.

Table 9: Threats/Attacks on asset: V2X On Board Unit

Threat	Type	CIA	Attack
TH-08: Firmware alteration	DEVICE	I	MI
TH-09: Firmware erasing	DEVICE	A	MI
TH-10: Firmware reverse engineering	DEVICE	(AI)	MI, Mq, CRC
TH-11: Degradation due to impact	DEVICE	A	Ph
TH-12: Degradation due to bad weather	DEVICE	A	Ph
TH-13: Electromagnetic interference disturbance	DEVICE	A	Ja
TH-14: Sabotage of device	DEVICE	A	Ph
TH-15: Extreme solicitation	SOFTWARE/SYSTEM	A	DoS
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS

Table 10: Threats/Attacks on asset: CAN Gateway

Threat	Type	CIA	Attack
TH-08: Firmware alteration	DEVICE	I	MI
TH-09: Firmware erasing	DEVICE	A	MI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

TH-10: Firmware reverse engineering	DEVICE	(AI)	MI, Mq, CRC
TH-11: Degradation due to impact	DEVICE	A	Ph
TH-12: Degradation due to bad weather	DEVICE	A	Ph
TH-13: Electromagnetic interference disturbance	DEVICE	A	Ja
TH-14: Sabotage of device	DEVICE	A	Ph
TH-15: Extreme solicitation	SOFTWARE/SYSTEM	A	DoS
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS

Table 11: Threats/Attacks on asset: Ethernet Gateway

Threat	Type	CIA	Attack
TH-08: Firmware alteration	DEVICE	I	MM
TH-09: Firmware erasing	DEVICE	A	MI
TH-10: Firmware reverse engineering	DEVICE	(AI)	MI, Mq, CRC
TH-11: Degradation due to impact	DEVICE	A	Ph
TH-12: Degradation due to bad weather	DEVICE	A	Ph
TH-13: Electromagnetic interference disturbance	DEVICE	A	Ja
TH-14: Sabotage of device	DEVICE	A	Ph
TH-15: Extreme solicitation	SOFTWARE/SYSTEM	A	DoS
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS

Table 12: Threats/Attacks on asset: HMI On board Unit

Threat	Type	CIA	Attack
TH-08: Firmware alteration	DEVICE	I	MI, MM
TH-09: Firmware erasing	DEVICE	A	MI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

TH-10: Firmware reverse engineering	DEVICE	(AI)	MI, Mq, CRC
TH-11: Degradation due to impact	DEVICE	A	Ph
TH-12: Degradation due to bad weather	DEVICE	A	Ph
TH-13: Electromagnetic interference disturbance	DEVICE	A	Ja
TH-14: Sabotage of device	DEVICE	A	Ph
TH-15: Extreme solicitation	SOFTWARE/SYSTEM	A	DoS
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS

Table 13: Threats/Attacks on asset: Mobile communication link

Threat	Type	CIA	Attack
TH-01: Radio Jamming	MEDIUM	A	Ja
TH-02: Link layer flooding	MEDIUM	A	DoS, Re
TH-03: Equipment spoofing	MEDIUM	I	MiTM, MM, Ro
TH-04: Man-in-the-middle attack (Data manipulation)	MEDIUM	I	Mq, MiTM, Re, MM, Mi
TH-05: Communication Eavesdropping	MEDIUM	C	Mq
TH-06: Electromagnetic interference disturbance (unintentional)	MEDIUM	A	Ja

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 14: Threats/Attacks on asset: R-ITS-S

Threat	Type	CIA	Attack
TH-08: Firmware alteration	DEVICE	I	MI, MM
TH-09: Firmware erasing	DEVICE	A	MI
TH-10: Firmware reverse engineering	DEVICE	(AI)	MI, Mq, CRC
TH-11: Degradation due to impact	DEVICE	A	Ph
TH-12: Degradation due to bad weather	DEVICE	A	Ph
TH-13: Electromagnetic interference disturbance	DEVICE	A	Ja
TH-14: Sabotage of device	DEVICE	A	Ph
TH-15: Extreme solicitation	SOFTWARE/SYSTEM	A	DoS
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS
TH-18: System alteration after unauthorized access to maintenance port	SOFTWARE/SYSTEM	AI	MM, MI

Table 15 : Threats/Attacks on asset: Safety Application V-ITS-S

Threat	Type	CIA	Attack
TH-08: Firmware alteration	DEVICE	I	MI, MM
TH-09: Firmware erasing	DEVICE	A	MI
TH-10: Firmware reverse engineering	DEVICE	(AI)	MI, Mq, CRC
TH-11: Degradation due to impact	DEVICE	A	Ph
TH-12: Degradation due to bad weather	DEVICE	A	Ph
TH-13: Electromagnetic interference disturbance	DEVICE	A	Ja
TH-14: Sabotage of device	DEVICE	A	Ph
TH-15: Extreme solicitation	SOFTWARE/SYSTEM	A	DoS
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 16: Threats/Attacks on asset: V2X communication link

Threat	Type	CIA	Attack
TH-01: Radio Jamming	MEDIUM	A	Ja
TH-02: Link layer flooding	MEDIUM	A	DoS, Re
TH-03: Equipment spoofing	MEDIUM	I	MiTM, MM, Ro
TH-04: Man-in-the-middle attack (Data manipulation)	MEDIUM	I	Mq, MiTM
TH-05: Communication Eavesdropping	MEDIUM	C	Mq
TH-06: Electromagnetic interference disturbance (unintentional)	MEDIUM	A	Ja

Table 17: Threats/Attacks on asset: Wi-Fi communication link

Threat	Type	CIA	Attack
TH-01: Radio Jamming	MEDIUM	A	Ja
TH-02: Link layer flooding	MEDIUM	A	DoS, Re
TH-03: Equipment spoofing	MEDIUM	I	MiTM, MM, Ro
TH-04: Man-in-the-middle attack (Data manipulation)	MEDIUM	I	Mq, MiTM
TH-05: Communication Eavesdropping	MEDIUM	I	MiTN, Mq,
TH-06: Electromagnetic interference disturbance (unintentional)	MEDIUM	A	Ja

Table 18: Threats/Attacks on asset: Wired com. Link

Threat	Type	CIA	Attack
TH-02: Link layer flooding	MEDIUM	A	DoS, Re
TH-03: Equipment spoofing	MEDIUM	I	MiTM, MM, Ro
TH-04: Man-in-the-middle attack (Data manipulation)	MEDIUM	I	Mq, MiTM
TH-05: Communication Eavesdropping	MEDIUM	I	MiTN, Mq,
TH-06: Electromagnetic interference disturbance (unintentional)	MEDIUM	A	Ja
TH-07: Sabotage of medium	MEDIUM	A	Ph

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 19: Threats/Attacks on asset: Cloud (C-ITS-S)

Threat	Type	CIA	Attack
TH-16: Malicious code injection	SOFTWARE/SYSTEM	(AI)	MI, Mq, DoS
TH-17: Malformed frame injection (DoS)	SOFTWARE/SYSTEM	(AI)	Mq, MI, MiTM, DoS
TH-18: System alteration after unauthorized access to maintenance port	SOFTWARE/SYSTEM	(CIA)	MI, Mq, MiTM
Data breaches	SOFTWARE	C	MI, MM, Mq, MiTM, SC,CRC
Weak identity credential and access management	SOFTWARE	(CIA)	Mq, MiTM
Insecure interfaces and APIs	SOFTWARE	(CIA)	Mq, MiTM
Account hijacking	SOFTWARE	(CIA)	MI, Mq, MiTM
Advanced persistence threats	SOFTWARE	(CIA)	DoS, MI
System and application vulnerability	SOFTWARE	(CIA)	DoS, MI
Abuse of cloud services	SOFTWARE	(CIA)	DoS, MI, CRC
Data loss	SOFTWARE	(CIA)	MI, MM, SC, CRC
Malicious Insider	SOFTWARE	(CIA)	Ph

Reliability – Safety Threats

If the case of malicious attacks is excluded, the performance of a system component may be affected by internal or external factors, which, despite the fact that they were not caused by a malicious counterpart, can cause failures. The specific set of threats is associated with the Reliability-Safety objectives and requirements of the cyber physical system. In the following matrices, failure threats per asset and corresponding failure reasons are identified, similarly to the aforementioned security/privacy-related threat-attack pairs.

The identified generalized failure reasons can be summarized in the following table:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 20: List of failure reasons in respect to system reliability

Overestimation of possibilities / overutilization of resources	The tasks/responsibilities assigned to the component overcome its abilities and available resources, causing degradation of performance and/or failure.
System Design Error	The specific system module is unable to fulfill specific operational requirements due to poor design.
Extreme functional/operational Conditions	During its operation, a system module has to deal with unusual demand or has to consume an abnormally high number of system resources, causing degradation of performance and/or failure.
Environmental conditions	Specific environmental conditions will cause a system module failure.
Hardware flaw	A hardware component poorly designed/constructed/attached will cause system module failure.
Random-circumstantial special condition	A random and unexpected event, i.e. an outlier, may cause temporary operational failure (quite common for wireless communication systems).
Insufficient unit testing/ debugging	The system module was not sufficiently tested to deal with all possible conditions/combination of events. As a result, systematic errors-bugs occur.
Operator/user error	The functional/operational error caused by user setting selection or handing

As a next step, the identified failure reasons are assigned to safety-reliability threats per asset.

Table 21 Reliability Threat to supports asset: V2X On Board Unit

Requirement	Threat	Reason
Accessibility	Congestion of applications	Overestimation of possibilities / overutilization of resources
Quality of service	Increased latency / processing delay	System Design Error, Extreme functional conditions, overutilization of resources
Accessibility	Poor / unreasonable use of resources	System Design Error
Accessibility	Poor scheduling	System Design Error, Extreme functional conditions, overutilization of resources
Prioritization	Inability to prioritize for available resources	System Design Error
Reliability	Failure due to extreme temperature/humidity/dust etc.	Random-circumstantial special condition, Environmental conditions
Accessibility, Reliability	Erroneous setting and configuration	Operator/user error
Reliability	General hardware failure	Hardware flaw, Environmental conditions
Reliability	Software bug	Insufficient unit testing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 22 Reliability Threat to supports asset: CAN gateway

Requirement	Threat	Reason
Accessibility	Congestion of connections	Overestimation of possibilities / overutilization of resources
Quality of service	Increased latency / processing delay	System Design Error, Extreme functional conditions, overutilization of resources
Accessibility	Poor / unreasonable use of resources	System Design Error
Accessibility	Poor scheduling	System Design Error, Extreme functional conditions, overutilization of resources
Prioritization	Inability to prioritize for available resources	System Design Error
Reliability	Failure due to extreme temperature/humidity/dust etc.	Random-circumstantial special condition, Environmental conditions
Accessibility, Reliability	Erroneous setting and configuration	Operator/user error
Reliability	General hardware failure	Hardware flaw, Environmental conditions
Reliability	Software bug	Insufficient unit testing

Table 23 Reliability Threat to supports asset: Ethernet gateway

Requirement	Threat	Reason
Accessibility	Congestion of connections	Overestimation of possibilities / overutilization of resources
Quality of service	Increased latency / processing delay	System Design Error, Extreme functional conditions, overutilization of resources
Accessibility	Poor / unreasonable use of resources	System Design Error
Accessibility	Poor scheduling	System Design Error, Extreme functional conditions, overutilization of resources
Prioritization	Inability to prioritize for available resources	System Design Error
Reliability	Failure due to extreme temperature/humidity/dust etc.	Random-circumstantial special condition, Environmental conditions
Accessibility, Reliability	Erroneous setting and configuration	Operator/user error
Reliability	General hardware failure	Hardware flaw, Environmental conditions
Reliability	Software bug	Insufficient unit testing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 24 Reliability Threat to supports asset: HMI On board unit

Requirement	Threat	Reason
Reliability	Failure due to extreme temperature/humidity/dust etc.	Random-circumstantial special condition, Environmental conditions
Accessibility, Reliability	Erroneous setting and configuration	Operator/user error
Reliability	General hardware failure	Hardware flaw, Environmental conditions
Reliability	Software bug	Insufficient unit testing

Table 25 Reliability Threat to supports asset: Mobile communication link

Requirement	Threat	Reason
Coverage and capacity	Insufficient network coverage	System Design Error, Environmental conditions
Coverage and capacity, Reliability	Hidden terminal	Random-circumstantial special condition, Environmental conditions
Reliability, Quality of service	Low Signal to Interference ratio	System Design Error, Extreme functional conditions, Environmental conditions
Accessibility	Poor scheduling	System Design Error, Extreme functional conditions, overutilization of resources
Quality of service	Increased latency	System Design Error, Extreme functional conditions, overutilization of resources
Accessibility, Reliability	Lack of radio resources	Overestimation of possibilities / overutilization of resources
Prioritization	Inability to prioritize in resource allocation	System Design Error

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 26 Reliability Threat to supports asset: RSU

Requirement	Threat	Reason
Accessibility	Congestion of applications	Overestimation of possibilities / overutilization of resources
Quality of service	Increased latency / processing delay	System Design Error, Extreme functional conditions, overutilization of resources
Accessibility	Poor / unreasonable use of resources	System Design Error
Accessibility	Poor scheduling	System Design Error, Extreme functional conditions, overutilization of resources
Prioritization	Inability to prioritize for available resources	System Design Error
Reliability	Failure due to extreme temperature/humidity/dust etc.	Random-circumstantial special condition, Environmental conditions
Accessibility, Reliability	Erroneous setting and configuration	Operator/user error
Reliability	General hardware failure	Hardware flaw, Environmental conditions
Reliability	Software bug	Insufficient unit testing

Table 27 Reliability Threat to supports asset: Safety Application on board Unit

Requirement	Threat	Reason
Quality of service	Increased latency / processing delay	System Design Error, Extreme functional conditions
Accessibility	Poor / unreasonable use of resources	System Design Error
Prioritization	Inability to prioritize for available resources	System Design Error
Accessibility, Reliability	Erroneous setting and configuration	Operator/user error
Reliability	Software bug	Insufficient unit testing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table 28 Reliability Threat to supports asset: V2X communication link

Requirement	Threat	Reason
Coverage and capacity	Insufficient network coverage	System Design Error, Environmental conditions
Coverage and capacity, Reliability	Hidden terminal	Random-circumstantial special condition, Environmental conditions
Reliability, Quality of service	Low Signal to Interference ratio	System Design Error, Extreme functional conditions, Environmental conditions
Accessibility, Reliability	Abnormalities due to relays	System Design Error, Extreme functional conditions.
Quality of service	Increased latency	System Design Error, Extreme functional conditions, overutilization of resources
Accessibility, Reliability	Lack of radio resources	Overestimation of possibilities / overutilization of resources
Prioritization	Inability to prioritize in resource allocation	System Design Error

Table 29 Reliability Threat to supports asset: V2X communication link

Requirement	Threat	Reason
Reliability	Detachment of cabling	Hardware flaw

Step 4.2 Create the Attack Model diagram

Through this step, we have a holistic view of the system and the elements that are affected by each threat. These diagrams add value on the project since they integrate in a holistic way the analysis that has been conducted so far in the previous steps, moving beyond the narrow limits that the previous analysis offer, which examines each specific actor and asset solely. The benefit is that at this point, we have threat related information escaping an actor's boundaries. Hence, our aim is to identify the relationships that create paths which affect the actors' goals, resources and plans, and to proceed with the necessary conflict resolutions, in the resources level, if it is necessary. Also, we can examine if there are threats that affect not only a specific actor, but also the ones that we have identified that there are dependences (from stage 2 of our methodology) on. This analysis gives us the confidence that each attack is finally mitigated, through specific security and privacy mechanisms.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Moreover, we realise if some threats are repeated or if affect the same constraint, from various perspectives. If so, we will be able to identify the necessary plans and resources that will be used during the implementation phase, later on. Consequently, the analysis of steps 1-4 will be used as input in step 5, in order to identify the requirements of the system.

For the development of the Attacks Model diagrams of each actor, the first step is to capture the threats that impact the actors, negatively affecting their ability to fulfil their goals. Thus, after the identification of the threats in Table 9 to Table 18, we proceded with the development of the relevant threat models. In Figures 25 and 26, a partial view of each threat model is presented, containing the affected actors of the V-ITS-S and the R-ITS-S system, respectively. Next, after the elicitation of the attack methods that affect the threats, we further decompose each threat. In Figure 27 we present an indicative example of Security Attacks view (in this view, the actor "cellular communication interface" is affected by the threat "TH-04: Man-in-the-Middle attack - Data Manipulation" ---- in Figure 27 appearing as "Arbitrary data injections"---- and only four of the attack methods that realize this specific threat are displayed; namely: "Replay", "Man-in-the-Middle", "Message modification" and "Malware Injection"). As we mentioned in the beginning of this report, the analysis of the system stops here. Consequently, the vulnerabilities that these attack methods exploit will be determined in the Deliverable 2.3. However, this is an iterative process. After the elicitation of the vulnerabilities of the system, we will examine the system again, providing the necessary security mechanisms and privacy enhancing technologies that will mitigate the identified attacks and ensure the satisfaction of security and privacy requirements, delivering, thus, a secure and protected system.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

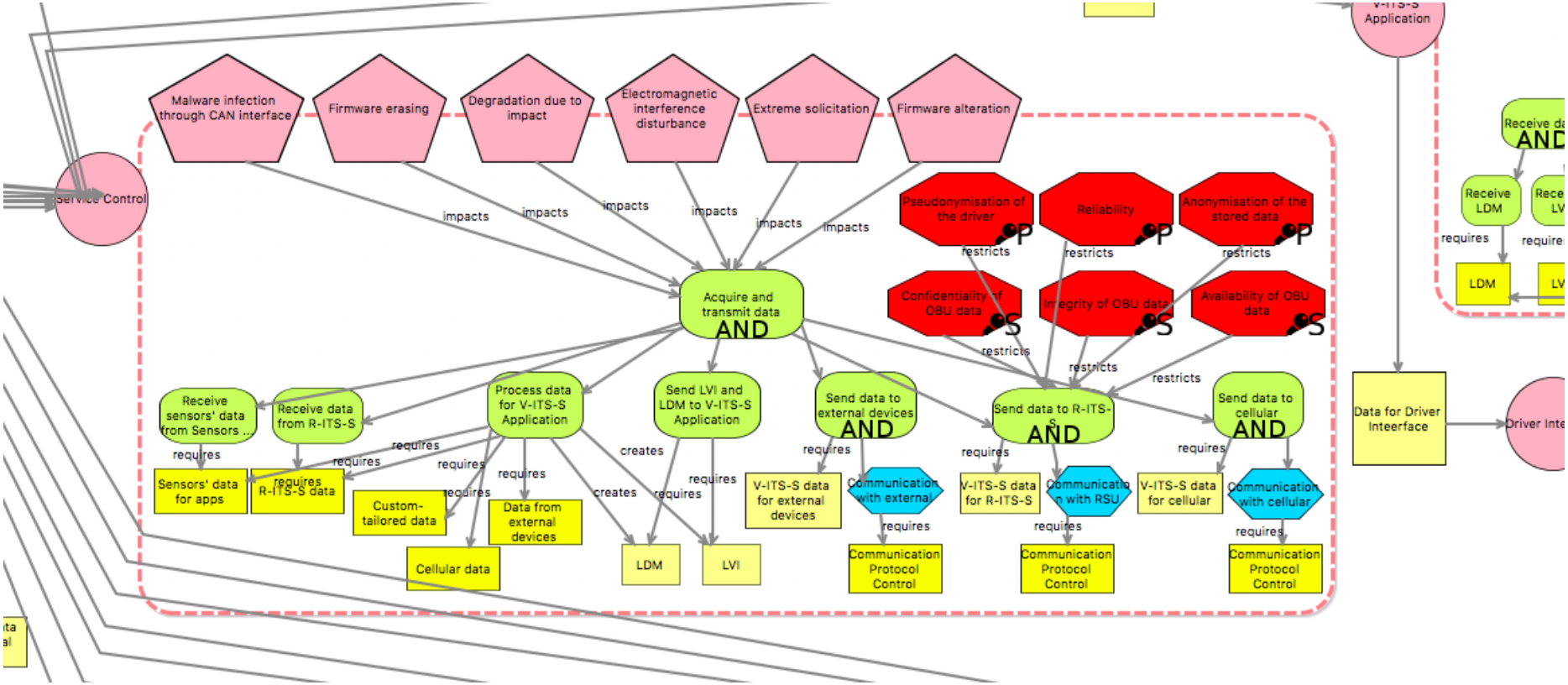

Figure 25: Partial view of the threat model of the V-ITS-S system

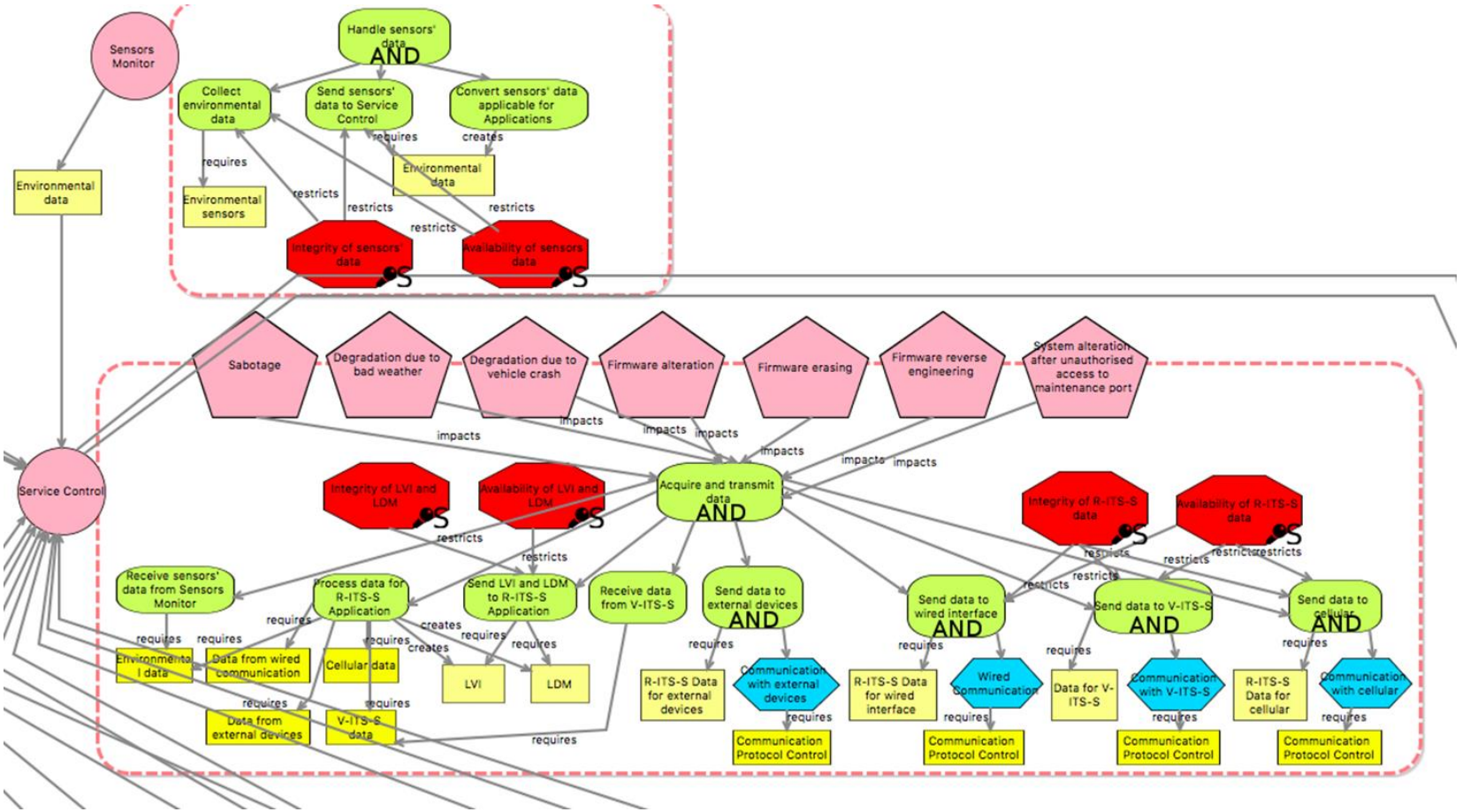

Figure 26: Partial view of the threat model of the R-ITS-S system

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

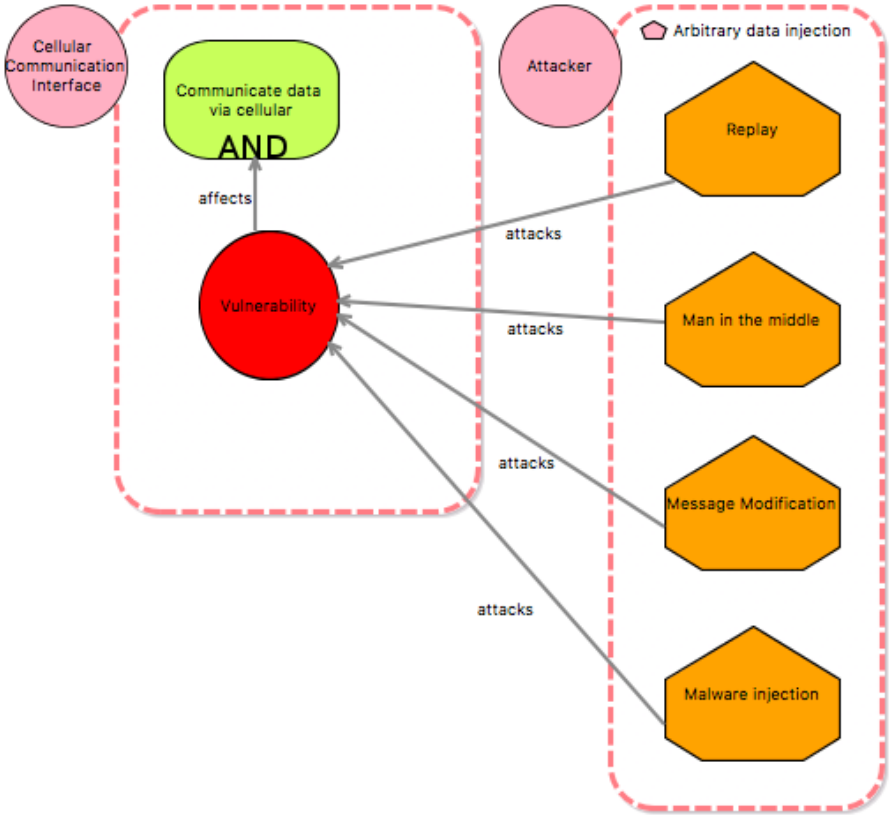

Figure 27: Attack model for "Arbitrary data injection" threat

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

References

[1] Mouratidis, H., Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17(2), 285–309 (2007)

[2] Van Lamsweerde, A.: Goal-oriented requirements engineering: A guided tour. In: Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on. pp. 249–262. IEEE (2001)

[3] Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., Mylopoulos, J.: Tropos: An agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems 8(3), 203–236 (2004)

[4] Diamantopoulou,V., Pavlidis, M., Mouratidis, H.: "Evaluation of a security and privacy requirements methodology using the physics of notation," in ESORICS SECPRE Workshop. Springer (2017).

[5] Mouratidis, H.: A security oriented approach in the development of multiagent systems: applied to the management of the health and social care needs of older people in England. PhD Thesis, University of Sheffield, UK (2004)

[6] Yu, E.: Modelling strategic relationships for process reengineering. Ph.D. thesis, Department of Computer Science, University of Toronto, Canada (1995)

[7] Chung, L., Nixon B.: Dealing with Non-Functional Requirements: Three Experimental Studies of a Process-Oriented Approach. In: 17th International Conference on Software Engineering, pp. 25{37. ACM (1995)

[8] Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., Mylopoulos, J.: Tropos: An agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems, 8(3), 203{236 (2004)

[9] Mouratidis, H., Islam S., Kalloniatis C., Gritzalis S.: A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software 86(9), 2276{2293 (2013)

[10] Mouratidis, H.: Secure software systems engineering: The Secure Tropos approach. Journal of Software, 6(3), 331{339 (2011)

[11] Pavlidis, M., Islam, S.: Sectro: A case tool for modelling security in requirements engineering using secure tropos. In: CAiSE Forum. pp. 89–96 (2011)

[12] Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: The PriS method. Requirements Engineering Journal 13(3), 241-255, 2008

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

[13] Kalloniatis, C., Kavakli, E., Kontellis, E.: PriS Tool: A Case Tool for Privacy-Oriented RE, Proceedings of the MCIS 2009 4th Mediterranean Conference on Information Systems, pp.913-925 (e-version), G. Doukidis et al. (Eds.), September 2009, Athens Greece

[14] Kalloniatis, C., Kavakli, E., Gritzalis, S.: 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, J. Mylopoulos, G. Spafford (Eds.) Paris, France, August 2005, IEEE CPS Conference Publishing Services, 2005.

[15] C. Kalloniatis, "Designing Privacy-Aware Systems in the Cloud", *Proceedings of the TRUSTBUS 2015 12th International Conference on Trust Privacy and Security in Digital Business,* S. Hubner, C. Lambrinoudakis (eds), September 2015, Valencia, Spain, Springer LNCS Lecture Notes in Computer Science.

[16] C. Kalloniatis (2017) "Incorporating Privacy in the Design of Cloud-Based Systems: A Conceptual Metamodel", *Information and Computer Security Journal*, Emerald https://doi.org/10.1108/ICS-06-2016-0044

[17] Loucopoulos, P., Kavakli, V. (1999) "Enterprise Knowledge Management and Conceptual Modelling", LNCS Vol. 1565, Springer, pp. 123-143.

[18] Loucopoulos, P. (2000), "From Information Modelling to Enterprise Modelling", In: Information Systems Engineering: State of the Art and Research Themes, Springer-Verlag, Berlin Heidelberg New York, pp. 67-78.

[19] ETSI TR 102 893 V1.2.1 (2017-03): Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA).

[20] ETSI EN 302 663 V1.2.0 (2012-11) Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band

[21] ETSI TR 102 638: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions.

[22] SAFERtec D2.1 Connected Vehicle Use Cases and High-Level Requirements

[23] SAFERtec D4.1 Specification of Connected Vehicle System

[24] K. Shi and E. Serpedin, "Coarse frame and carrier synchronization of OFDM systems: a new metric and comparison," IEEE Transactions on in Wireless Communications, vol. 3, no. 4, pp. 1271-1284, Jul July 2004.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Appendices

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Contents

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

A.1 Development of Simulators for Radio Interfaces

In the course of WP2, simulators for the two currently used radio interfaces for vehicular communications and ITS applications were developed. The simulators can be used to implement threats and attacks in the radio access network level (mainly Denial-of-Service) and more significantly test, validate and evaluate countermeasures improving system availability.
It is noted that while the simulator development was part of WP2, it was decided that the application of the simulators for test, validation and evaluation will be part of the work done in tasks 3.3 (Assurance Framework Testing) and 5.2 (Simulation based evaluation), that are the tasks that mainly include testing procedures.

A.2 IEEE 802.11p/ITS-G5 Simulator

In the context of T2.2, a simulation platform implementing the ITS-G5/IEEE 802.11p standard, which is considered as the underlying protocol for IVC has been realized. This platform may be used to test, evaluate, and examine the PHY and medium access control (MAC) layers of V2V/V2I links. The simulator is developed from UPRC. Initial development was done in the course of the H2020-ROADART project and it was extended and updated during SAFERtec.

A.2.1 Physical Layer

The following block-diagram depicts the simulator system structure. The system model is divided into three main parts, transmitter, receiver, and channel.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

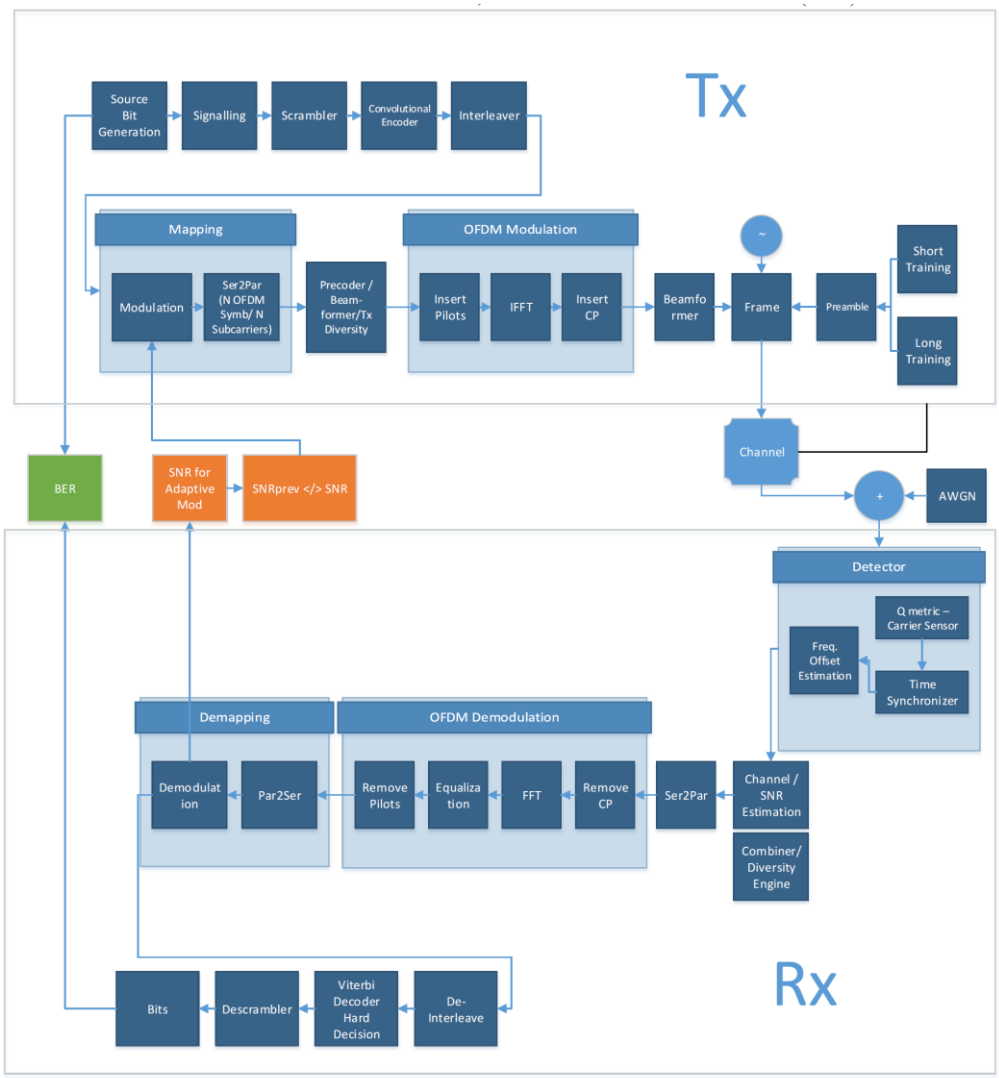

Figure 28: ITS-G5 simulator model

The simulator is built using an object-oriented approach, where an instantiation for each of the main simulator parts is created. In addition, the objects share a common library of functions, like Fast Fourier transform (FFT), Inverse FFT (IFFT), cross-correlators etc.

The transmitter class includes adaptive modulation and coding mechanism, supporting 4 types of modulations and three coding rates. Moreover, scrambling and interleaving functions are available. Data symbols are modulated through orthogonal frequency division multiplexing (OFDM). Furthermore, short training preamble, long training preamble and signaling data are created and pilot symbols are inserted, as specified at IEEE802.11p standard.

The Receiver class, on the other hand, consists of the transmitter's "mirror" functions, such as de-mapper, de-modulator, etc. In addition, the Receiver includes non-standardized essential functions like: signal sensing and acquisition (implemented from reaped correlations of the short preamble), the coarse-synchronization and frequency offset estimation function (based primarily on the Shi-Serpedin proposed algorithm [23]), fine-synchronization, frequency error

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

compensation, channel estimation (where the Channel State Information is extracted by the long preamble and tracked by the pilot symbols) and finally channel equalization.

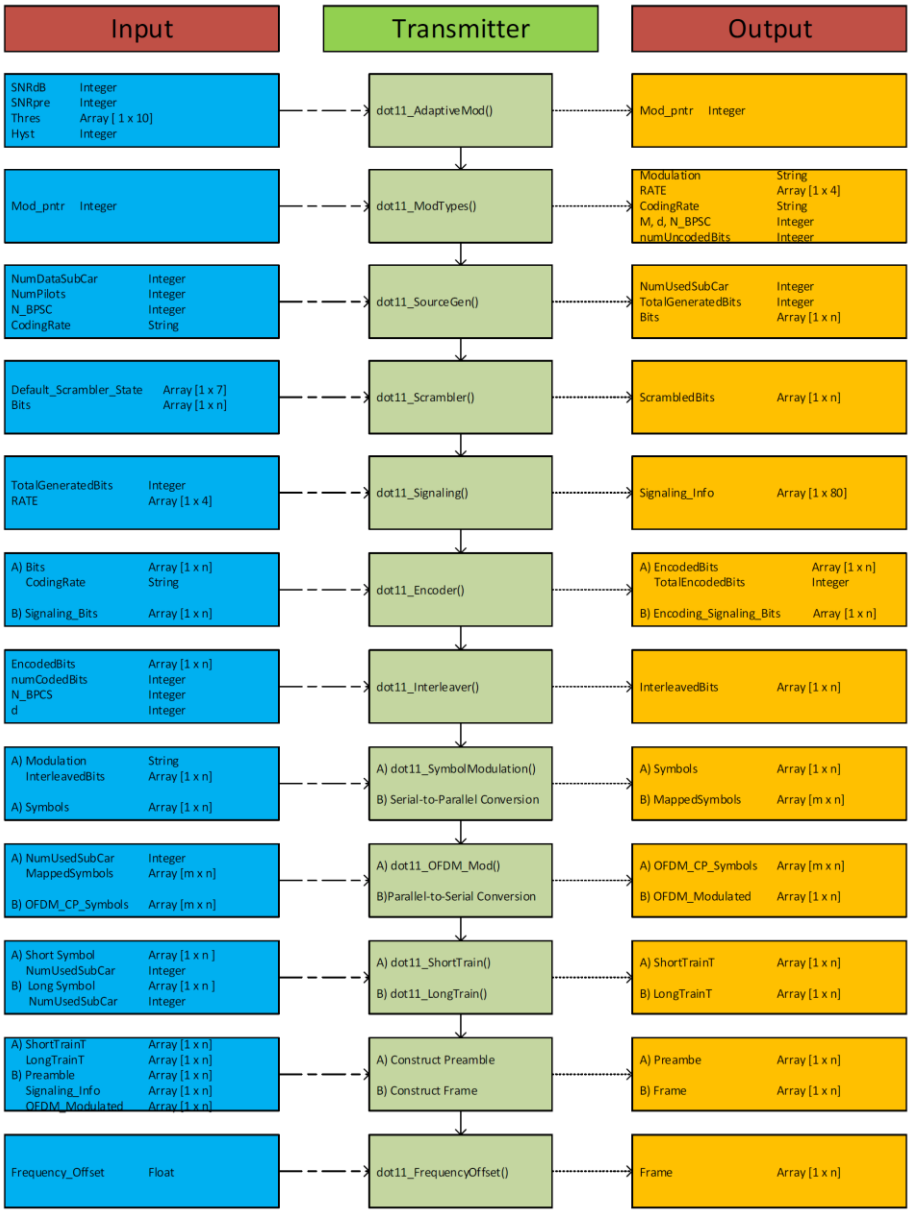

Figure 29: Transmitter class structure and Input-Output

The software diagrams shown in Figure 29 and Figure 30 offer a more vivid image of the transmitter and receiver functions. Note that, when a vector is followed by a [1 x n] notation, is one-dimensional, where [m x n] denotes an mxn matrix.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

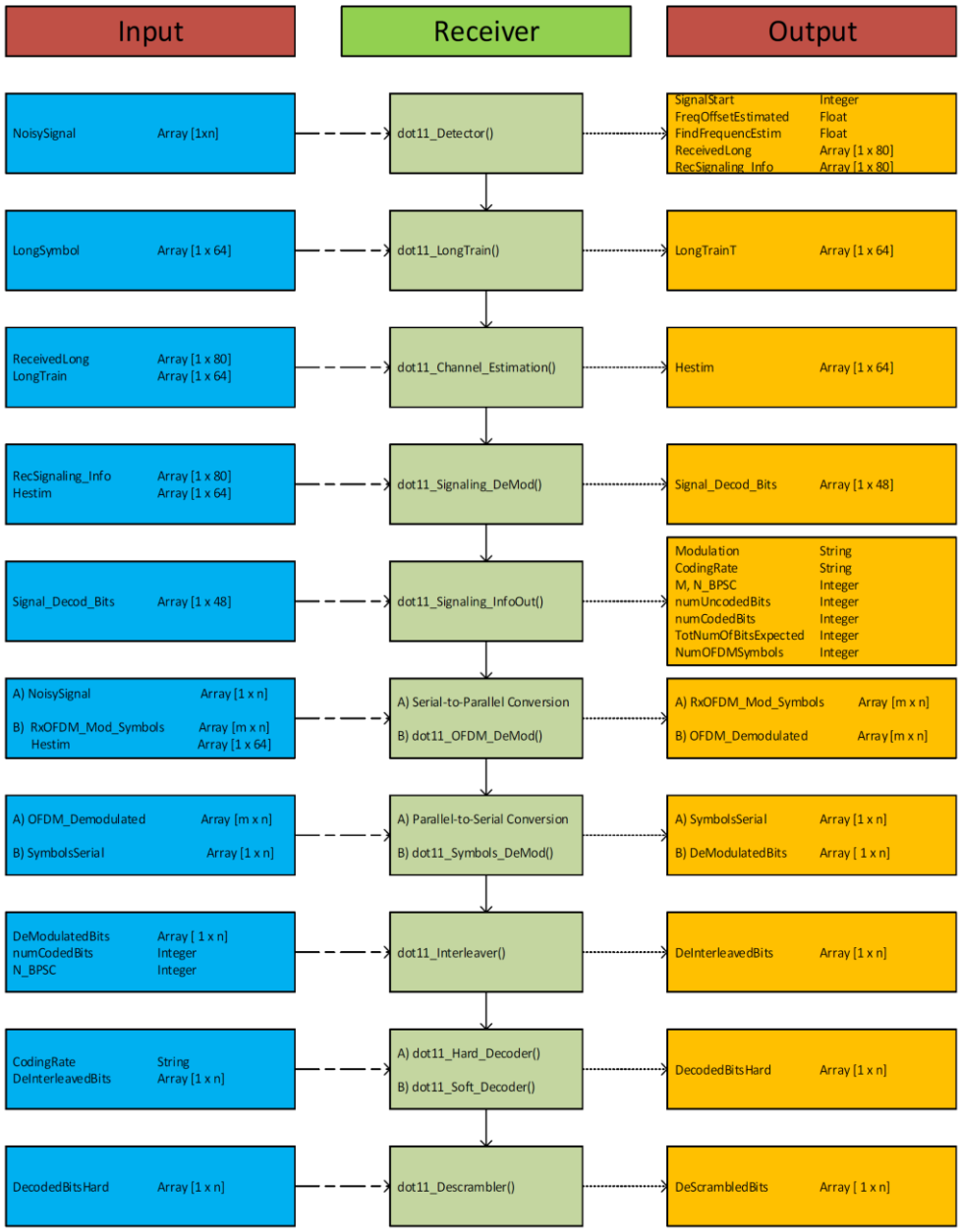

Figure 30: Receiver class structure and Input-Output

A.2.2 Medium Access Control

A description of the developed MAC simulator is presented in this paragraph. The basic operations of the MAC sublayer in IEEE 802.11p is summarized in the flow diagram of Figure 31. ITS-G5 is based on IEEE 802.11p, a random-access protocol that uses carrier sense multiple access with collision avoidance (CSMA/CA) technique. Distributed radio access is implemented using the enhanced distributed channel access (EDCA) function.
The simulator is implemented in MATLAB with an object-oriented approach. Five main classes are defined:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

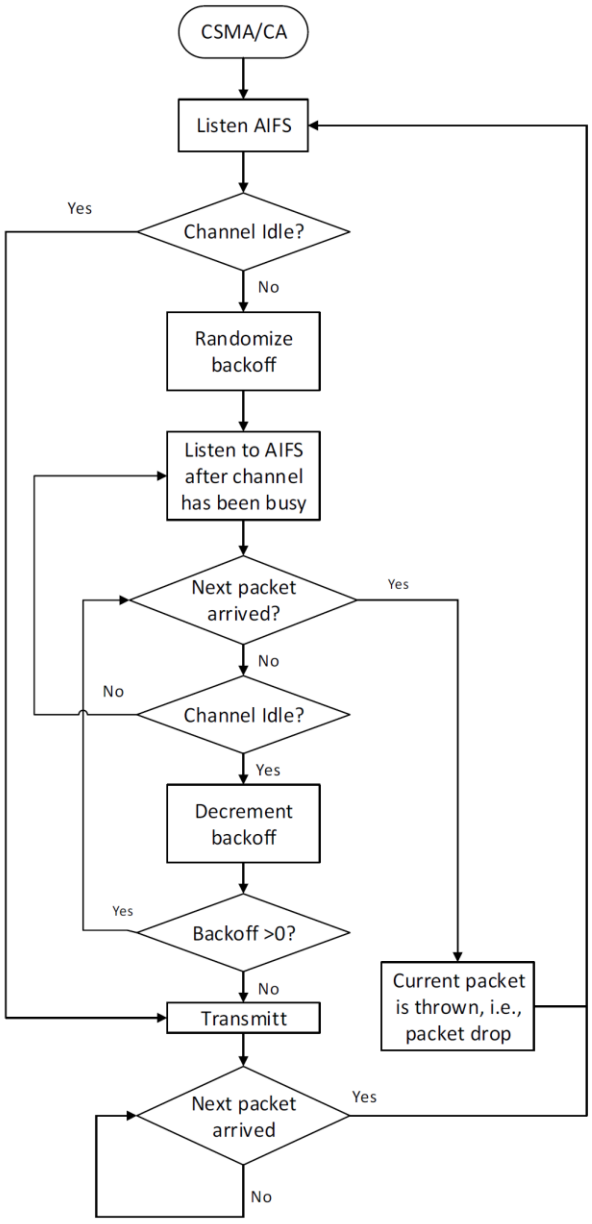

Figure 31: CSMA/CA implementation in IEEE 802.11p

1. The ITSG5_MAC class that initialize global properties for the MAC layer of all network nodes.
2. The ITSG5_Simulator class that implements the functionality of an ITSG5 network with multiple network nodes. The ITSG5_simulator_loop method implements the main simulator actions. The ITSG5_Simulator contains and manages the simulator clock, i.e., the simulated time line for the network operation
3. The ITSG5_Tranceiver class implements the PHY and MAC procedures per network node. Each network node in the simulator uses an instance of the ITSG5_Transceiver class. The ITSG5_Transceiver inherits properties from the ITSG5_MAC class.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4. The ITSG5_Transmitter is a class-property for the ITSG5_Transceiver. ITSG5_Transmitter implements all the PHY functions and operations as described in the previous paragraph for transmitter operation. ITSG5_Transceiver controls MAC operation and assigns transmitting operation to its ITSG5_Transmitter property
5. The ITSG5_Receiver is a class-property for the ITSG5_Transceiver. ITSG5_Receiver implements all the PHY functions and operations as described in Subsection 2.1 for receiving operation. ITSG5_Transceiver controls MAC operation and assigns receiving operation to its ITSG5_Receiver property

During the simulator initialization stage, one ITSG5_Simulator instance is produced that performs the main network/simulator tasks. Moreover, based on the selected user generation procedure (implemented as a method in the simulator class), new network nodes are generated either in the initialization stage or continuously during the simulator loop. New network nodes are generated with new ITSG5_Transceiver instances. Each ITSG5_Transceiver instance retains as properties one ITSG5_Transmitter instance and one ITSG5_Receiver instance. At all times, each ITSG5_Transmitter uses either the receiver or transmitter operation.

The following five transmission types are supported:

- Broadcast – i.e., a transceiver gains access to the medium and broadcasts a QoS data frame. No ACK is expected.
- Multicast – i.e., a transceiver gains access to the medium and sends a QoS data frame to a group of users. No ACK is expected
- Unicast without ACK – i.e., the transceiver sends directly a QoS data frame to a specified destination but it does not require an ACK
- Unicast with ACK – i.e. the transceiver sends directly a QoS data frame to a specified destination and an ACK is expected as a response
- RTS-CTS Unicast with ACK – i.e. the transceiver sends an RTS (ready to send) frame towards a destination. A CTS (clear to send) response is expected. When the CTS is received, then a QoS data frame is send with an expected ACK as a response. RTS-CTS type of transmission is expected for frames with MPDU size greater than 1Kbyte

The simulator supports the following types of Frames:

- Management frames:
  - Action frames
  - Time advertisement frames
- Control Frames
  - RTS
  - CTS
  - ACK
- Data Frames
  - QoS data (since EDCA is used)
  - Null (without practical use for the simulator)

The following status are defined per network node:

0. Idle – Sensing.
1. Waiting to Tx (transmitter) – Sensing.
2. Transmitting (data or ACK).
3. Waiting to transmit ACK.
4. Receiving.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5. Waiting to receive ACK.

In order to simulate the slotted operation of CSMA/CA, the simulator implements a time line in nano-seconds. The time line is updated with the use of a "while" loop (until the end of the simulation). The time line is increased using the following rationale:

- Simulator global time increases in slot duration steps, where slot duration is the MAC slot time duration in nanoseconds. The exception in this procedure is the existence of an event at a time instance less than the current slot duration. The existence of an event is specified by a number of counters retained by each network node that participates in the simulator
- Each network node (user) retains the following counters:
    - Timers that count short interframe spacing (SIFS), arbitration interframe space (AIFS), or extended interframe space (EIFS) duration. (AIFS, SIFS, and EIFS counters – AIFS counter is a 4-vector, since four QoS queues are defined by the standard).
    - Timers that implement the contention procedure for each node and each priority group of data (contention window (CW) timers).
    - Timers that count the duration of the currently transmitted packet from other sources (information acquired with demodulation of the NAV field).
    - Timer that counts the remaining time for transmission for a packet originating by the transceiver (Tx Timer)

All counters are initialized (based on an event) and continuously reduced until reaching zeros. Zeroing of a timer constitutes an event. The simulator All counters are initialized (based on an event) and continuously reduced until reaching zeros. Zeroing of a timer constitutes an event. The simulator time controller is depicted in Figure 32. The general flow of the simulator is described in Figure 33.

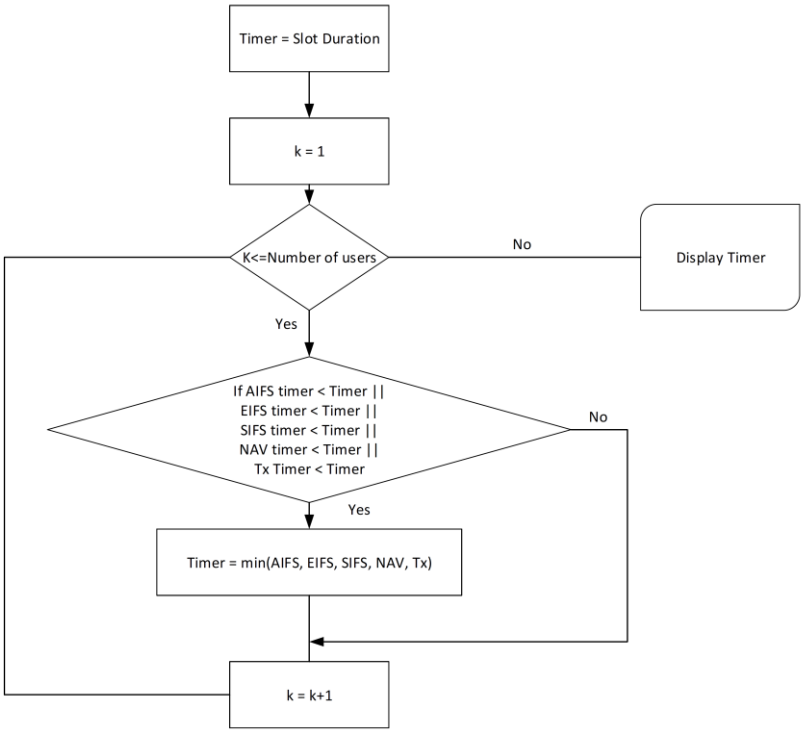

Figure 32: Simulator time controller

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

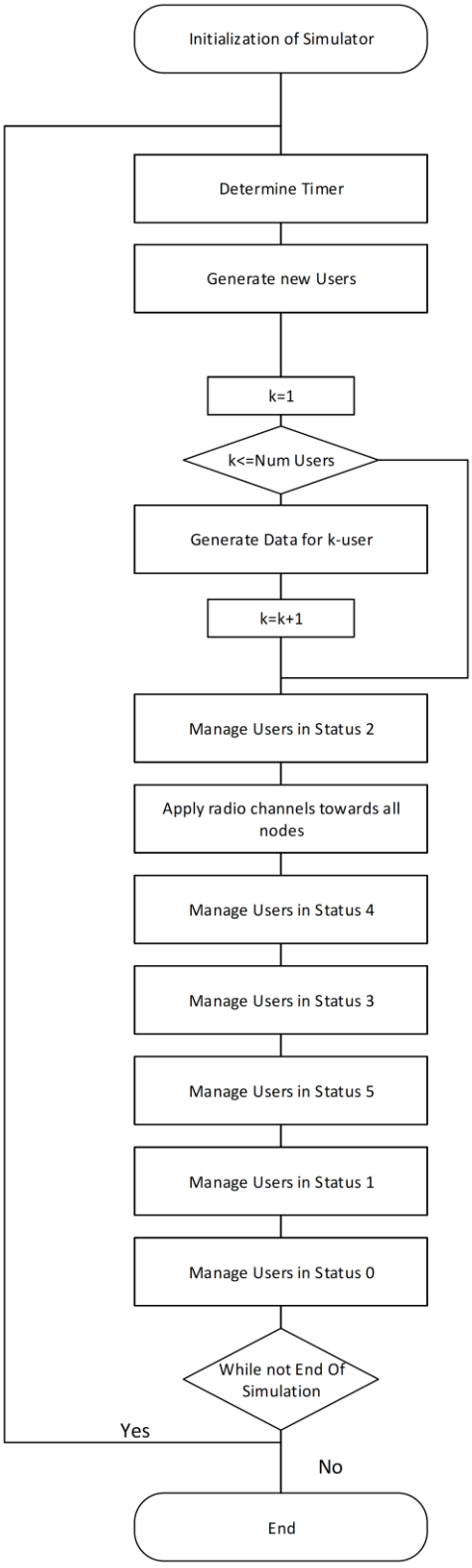

Figure 33: Basic flow of the simulator loop

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Initialization of Users:

Each generated user initially has:

- No data to send
- No information about adjacent network nodes

Therefore, no a-priori knowledge is available at each transmitter.

Data Generation Procedure:

Initially, each user has no data. Based on a predefined method, new data are produced stochastically with a certain rate during each time progression step. Data are produced with a different rate for each QoS data queue of each transceiver. Moreover, the size of the currently produced data frame is stochastically determined. Therefore, the current data frame size is determined randomly between 200 bytes up to 4Kbytes. The data generation procedure is depicted in Figure 34.

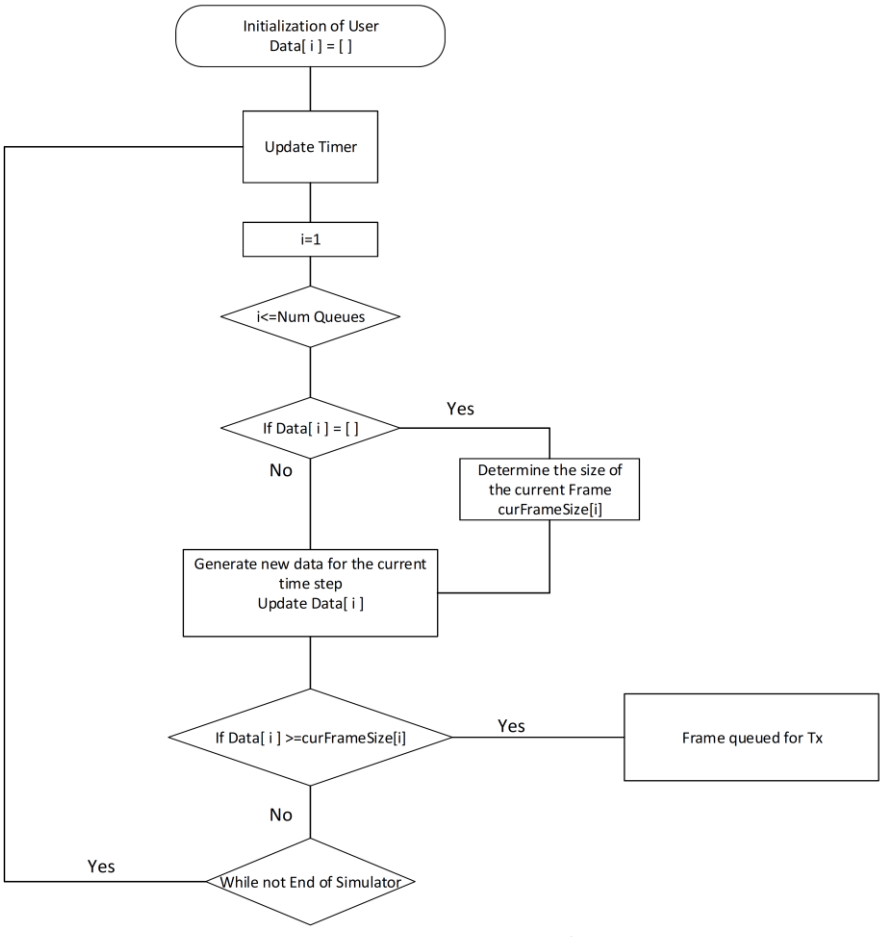

Figure 34:Data generation procedure

Simulator Actions per Status:

Status 0: When a node is in status 0, then:

- There are no available data into the QoS data queues to compose a full frame

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- The node operates as a receiver, sensing the medium
- The node is operating as a receiver performing carrier sense.
- New data are created during each time step. When the data in one or multiple queues are enough to compose a full frame, then the node moves to Status 1.

The receiving operation produces a decision regarding the medium status. If medium status is busy, then the receiver demodulates the headers in order to:

- Update NAV counters and determine the end of the transmission
- Decide if the node is the destination for the specific frame. In this case, the node is moving to State 4 and demodulates.

Status 1: When a node is in status 1, then:

- There are available data into the QoS data queues to compose a full frame
- The node has initialized and it continuously updates
  - AIFS counters
  - CW counters (if a collision has been already sensed in previous instances)
- The node operates as a receiver, sensing the medium
- If during the sensing procedure, a signal is sensed
  - The node reinitializes all AIFS counters
  - The node pauses all CW counters
  - It remains in State 1, and it tries to extract Destination and NAV information.

If the identified destination is the ID of the node, then the node moves to State 4 and demodulates the signal. If no signal is sensed, and AIFS and CW counters are zeroed, then the node will transmit data and it moves in State 2. If more than on AIFS/CW counter are zeroed simultaneously, then internal collision is detected. The queue with the highest priority is qualified, while Back-off procedure and AIFS counters are reinitialized for the rest of the queues.

Status 2: When a node is in status 2, then:

- The node is in transmitter node
- The frame with the highest order from the queue that won contention is transmitted
- If during the current time period, transmission is not completed (indicated by the Tx timer), then the node remains at State 2 until completion
- If Tx timer is zeroed (i.e., transmission is completed), the basic transmission scheme is used (i.e. no ACK) and the node has more data to send then it moves to State 1. If no other data are available, then the node moves to State 0
- If Tx timer is zeroed (i.e., transmission is completed) and ACK or CTS is needed, then the node moves to State 3

Status 3:
When a node is in status 3, then:

- The node is waiting to receive an ACK for a frame send during its previous state
- The node will wait for duration EIFS for ACK

During the EIFS waiting period, the medium should be determined as busy. If EIFS expires with no reception of an ACK, then the node determines that a collision occurred since no response from the destination was received.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

If the medium is sensed as busy, then the node moves to Receiver node. After de modulation of the received signal, the node will determine if the desired ACK was received (successful transmission) or a different signal was received (collision detected).

Status 4: When a node is in status 4, then:

- The node receives and demodulates the signal
- It is assumed that the node has identified itself as a destination of the signal

If the NAV timer for the received frame has not yet expired, then reception continues and the node remains at State 4.
If data reception is completed then:

- If no ACK is needed, then it moves in State 0 or State 1 depending on the availability of data.
- If no ACK is needed, however CRC does not check and collision is detected, CW timers are properly updated.
- If ACK is needed and collision is detected, then the node moves in State 0 or State 1 depending on the availability of data with proper adjustment of CW timers.
- If ACK is needed and no collision is detected, then the node moves in State 5 (waiting to transmit an ACK).

Status 5: When a node is in status 5, then it waits SIFS duration and then transmits an ACK for a frame received during its previous state that needs acknowledgement. If SIFS expires and the medium is considered free, then the node moves to Transmitting Mode State 2 and it sends the ACK. If during SIFS, the medium status changes to busy, then collision is detected and the node moves either to State 0 (no data available) or State 1 (data available – with necessary CW timer adjustment).

In this section, the MATLAB/OCTAVE simulator for both PHY and MAC layers of ITS-G5 standard that was developed is presented. In particular, all the functionalities of the PHY and MAC layers have been developed, based on the latest releases of this standard.

A.3 LTE-4G Simulator

The aim of this paragraph is to analyze an LTE simulator which could be used in V2X use cases scenarios. LTE simulator provides high functionality for designing, constructing, simulating, extracting and analyzing outcomes from a plethora of different configurations among vehicle communications. This simulator makes use of LTE algorithms and the knowledge of physical layer conditions to generate end-to-end communication links in which data will be transmitted through. The LTE simulator supports both legacy/cellular operation, as well as adhoc V2X operation (PC5 mode).

In the first stages of LTE and in legacy cellular-based uplink/downlink Radio Access Networks, the data exchange between two UEs had to traverse the LTE eNB. After the 3GPP Release 12, 3GPP introduced the sidelink LTE feature which enabled the direct communication between two proximal UEs, without the need of eNB, by using PC5 interface. Releases 13 and 14 have enriched D2D communication with numerous features and recently with V2X operations. D2D communications is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

closely related and applicable with V2X scenarios and this simulator provides, except of the standard LTE features, also a variety of tools for the implementation of the sidelink feature for the V2V and V2I communications.

In particular, LTE simulator provides the implementation of physical signals, physical downlink and uplink channels, sidelink channels, logical and transport channels, control information, OFDM modulation, and radio resources allocation operations based on the 3GPP standard. Some typical, supported by the simulator, features are indicated below.

- End-to-end uplink, downlink and sidelink link simulation.
- Uplink, downlink and sidelink waveform generation.
- Subframe creation, loading and time-domain transformation.
- Receiver functionality for waveforms:
  - Time-synchronization.
  - Frequency-offset estimation and compensation.
  - Channel estimation and equalization.
  - Signal demodulation/decoding.

- Basic transceiver operations: CRC, Coding, Rate Matching, Modulation, Transform Precoding, Interleaving, Golden Sequence.

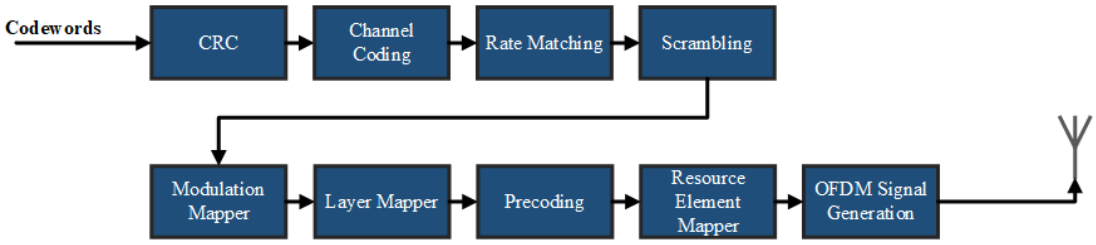

Figure 35: Channel and Signal Development

- Construction of downlink physical channels (PBCH, PDSCH, PDCCH, PCFICH, PHICH and EPDCCH) for transmission and reception.
- Construction of uplink physical channels (PSSCH, PUCCH formats 1, 2, and 3 and PRACH) for transmission and reception.
- Construction of sidelink physical channels (PDSCH, PSDCH DRMS) for transmission and reception.

- Generate, encode, and decode downlink transport channels (BCH, DL-SCH).
- Generate, encode, and decode uplink transport channels (UL-SCH and PUSCH).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Generate, encode, and decode sidelink transport channels (SL-BCH, PSBCH, PSSCH, and PSCCH).

- Downlink synchronization signals (PSS and SSS) and reference signals (CRS, DM-RS, CSI-RS and PRS).
- Uplink demodulation reference signals for PUSCH and PUCCH formats 1, 2, and 3 and demodulation reference signals.
- Sidelink synchronization signals (PSSS and SSSS) and demodulation reference signals.

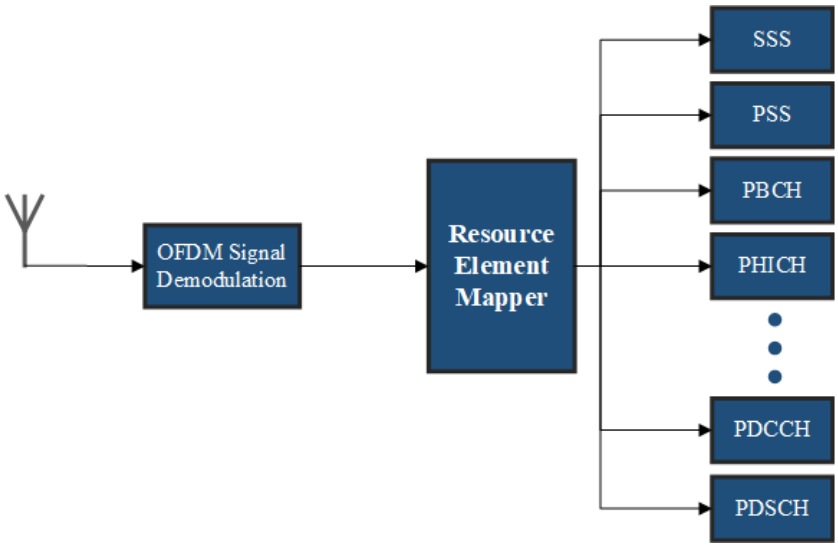

Figure 36: Receiver's DL Development

- Perform OFDM modulation and demodulation for the downlink scheme.
- Perform SC-FDMA modulation and demodulation for the uplink scheme.
- Perform SC-FDMA modulation and demodulation for the sidelink scheme.

- Construction of downlink physical signals and channels for Control Signaling: Downlink Control Information (DCI) and Control Format Indication (CFI)
- Construction of uplink physical signals and channels for Control Signaling: Uplink Control Information (UCI), Channel Quality Indicator (CQI) and Rank Indicator (RI).
- Construction of sidelink physical signals and channels for Control Signaling: SCI Format 0, PSCCH, SL-SCH, PSSCH, PSCCH DMRS.

- Especially for V2X communication mode:
    - Construction of physical Signals and channels for L1 signaling: SCI Format 1 (V2V), PSCCH, PSCCH DMRS.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Construction of physical signals and channels for Payload: V2X PSSCH, PSSCH DMRS.
- Subframe/PRB pool formation & UE-specific resource allocation for V2X communication.

To conclude, it is known that the deployment of a network especially considered for vehicular communications is facing a variety of different and new challenges in contrast with the common networks. For instance, in vehicular communications, the channel state is changing very fast due to the mobility of the distributed users which leads to degradation of the systems. Challenges like those must be taken into consideration for the proper construction of the network. So, it is of highly importance to analyze and counter as many as possible factors that play significant roles on the grade of service of the systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319