



POLITECNICO DI MILANO

SOFTWARE ENGINEERING II PROJECT

**SAFESTREETS**

---

# Requirements Analysis and Specifications Document

---

*Authors:*

Mattia CALABRESE  
Federico CAPACCIO  
Amedeo CAVALLO

*Professor:*

Elisabetta DI NITTO

October 23, 2019

version 1.0

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Purpose of this document . . . . .	1
1.2	Scope . . . . .	1
1.2.1	Goals . . . . .	1
1.3	Glossary . . . . .	2
1.3.1	Definitions . . . . .	2
1.3.2	Acronyms . . . . .	2
1.3.3	Abbreviations . . . . .	3
1.4	Document overview . . . . .	3
<b>2</b>	<b>Overall Description</b>	<b>4</b>
2.1	Product Perspective . . . . .	4
2.1.1	System Interfaces . . . . .	4
2.1.2	User Interfaces . . . . .	5
2.1.3	Hardware Interfaces . . . . .	6
2.1.4	Software Interfaces . . . . .	6
2.1.5	Communication Interfaces . . . . .	6
2.2	Product Functions . . . . .	6
2.3	User Characteristics . . . . .	9
2.4	Constraints . . . . .	9
2.5	Assumptions . . . . .	9
<b>3</b>	<b>Specific Requirements</b>	<b>10</b>
3.1	External Interfaces . . . . .	10
3.1.1	System Interfaces . . . . .	10
3.1.2	User Interfaces . . . . .	12
3.1.3	Hardware Interfaces . . . . .	12
3.1.4	Software Interfaces . . . . .	12
3.1.5	Communication Interfaces . . . . .	12
3.2	Functional Requirements . . . . .	12
3.3	Performance Requirements . . . . .	12
3.4	Logical Database Requirements . . . . .	12
3.5	Design Constraints . . . . .	12
3.5.1	Standards Compliance . . . . .	12
3.5.2	Hardware Limitations . . . . .	12
3.5.3	Other? . . . . .	12
3.6	Software System Attributes . . . . .	12
3.6.1	Reliability . . . . .	12
3.6.2	Availability . . . . .	12
3.6.3	Security . . . . .	12
3.6.4	Maintainability . . . . .	12
3.6.5	Portability . . . . .	12
3.7	Functional Requirements . . . . .	12
3.7.1	Goals . . . . .	12
3.8	Performance Requirements . . . . .	14
3.9	Software System Attributes . . . . .	15
3.9.1	Availability . . . . .	15
3.9.2	Security . . . . .	15

3.9.3	Portability . . . . .	15
<b>4</b>	<b>Use cases identification</b>	<b>16</b>
4.1	Scenarios . . . . .	16
4.1.1	Scenario 1 . . . . .	16
4.1.2	Scenario 2 . . . . .	16
4.1.3	Scenario 3 . . . . .	16
4.1.4	Scenario 4 . . . . .	16
4.1.5	Scenario 5 . . . . .	16
4.1.6	Scenario 6 . . . . .	16
4.2	Use case diagram . . . . .	17
4.3	Use cases description . . . . .	19
4.3.1	Registration . . . . .	19
4.3.2	Authentication . . . . .	21
4.3.3	View cars on the map . . . . .	23
4.3.4	Car reservation . . . . .	25
4.3.5	Car unlock . . . . .	26
4.3.6	Car rent . . . . .	28
4.3.7	Rent payment . . . . .	31
4.3.8	Money saving option . . . . .	34
4.3.9	Visualization of not available cars . . . . .	36
4.3.10	Tag a car as available . . . . .	38
4.3.11	Visualization of users information . . . . .	40
4.3.12	View users payments and rents history . . . . .	41
4.3.13	Mark or unmark a user as banned . . . . .	42
4.3.14	Tag a car as not available . . . . .	43
4.4	UML class diagram . . . . .	45
	<b>Appendices</b>	<b>46</b>
<b>A</b>	<b>Alloy model</b>	<b>46</b>
A.1	Source code . . . . .	46
A.2	Generated worlds . . . . .	54
<b>B</b>	<b>Software and tools used</b>	<b>56</b>
<b>C</b>	<b>Hours of Work</b>	<b>56</b>
<b>D</b>	<b>Changelog</b>	<b>56</b>

## List of Figures

1	SafeStreets Class Diagram CHANGE HANDLER + GIS Request	4
2	Overview of system interfaces . . . . .	4
3	Violation Upload Process . . . . .	7
4	Retrieve Data From Municipality . . . . .	7
5	Show Information and Statistics . . . . .	8
6	Restricted access API . . . . .	8
7	GIS Interaction Diagram . . . . .	11
8	Use case diagram . . . . .	17

9	<i>Registration</i> sequence diagram . . . . .	20
10	<i>Authentication</i> sequence diagram . . . . .	22
11	<i>View cars on the map</i> sequence diagram . . . . .	24
12	<i>Car unlock</i> sequence diagram . . . . .	27
13	<i>Car rent</i> sequence diagram . . . . .	29
14	<i>One Euro fee</i> sequence diagram . . . . .	29
15	Car status FSM . . . . .	30
16	<i>Rent payment</i> sequence diagram . . . . .	33
17	<i>Money saving option</i> sequence diagram . . . . .	35
18	<i>Visualization of not available cars</i> sequence diagram . . . . .	37
19	<i>Tag a car as available</i> sequence diagram . . . . .	39
20	<i>Tag a car as Not Available</i> sequence diagram . . . . .	44
21	UML class diagram . . . . .	45
22	Alloy execution result . . . . .	53
23	First alloy generated world . . . . .	54
24	Second alloy generated world . . . . .	55

## List of Tables

1	<i>Registration</i> use case description . . . . .	20
2	<i>Authentication</i> use case description . . . . .	21
3	<i>View cars on the map</i> use case description . . . . .	23
4	<i>Car reservation</i> use case description . . . . .	25
5	<i>Car unlock</i> use case description . . . . .	26
6	<i>Car rent</i> use case description . . . . .	28
7	<i>Rent payment</i> use case description . . . . .	32
8	<i>Money saving option</i> use case description . . . . .	34
9	<i>Visualization of not available cars</i> use case description . . . . .	36
10	<i>Tag a car as not available</i> use case description . . . . .	38
11	<i>Visualization of users information</i> use case description . . . . .	40
12	<i>View users payments and rents history</i> use case description . . . . .	41
13	<i>Mark or unmark a user as banned</i> use case description . . . . .	42
14	<i>Tag a car as not available</i> use case description . . . . .	43

# 1 Introduction

## 1.1 Purpose of this document

The purpose of a **Requirement Analysis and Specifications Document** is the process of discovering the purpose for which a software system was intended, by identifying stakeholders and their needs, and documenting these in a form that is amenable to analysis, communication, and subsequent implementation. [1] It is also concerned with the relationship of software's factors such as goals, functions and constraints to precise specifications of software behaviour, and to their evolution over time and across software families. [2]

## 1.2 Scope

SafeStreets is a crowd-sourced application that intends to provide users with the possibility to notify authorities when traffic violations occur, and in particular parking violations.

The system allows users to send pictures of violations, including suitable metadata, to authorities. Examples of violations are vehicles parked in the middle of bike lanes or in places reserved for people with disabilities, double parking, and so on. In addition, the system allows users to mine the previously stored information, for example by highlighting the streets (and the areas) with the highest frequency of violations, or by showing statistics regarding the vehicles that commit the most violations.

The system will also provide a communication interface to the municipality's provided service to create a secure bridge for data transfer. This connection will enable SafeStreets to cross its data with municipality's to make analysis and build different types of statistics. Moreover the system will offer back to the municipality the possibility to retrieve information about the violations in order to generate traffic tickets from it and receive suggestions on possible interventions. [3]

### 1.2.1 Goals

- G1** Allow guest users to register to the system
- G2** Allow registered users to authenticate to the system
- G3** Allow users to transfer data to the system describing occurred violations, including the suitable metadata to describe the submitted violation
- G4** Ensure that the chain of custody of the information provided by the users is never broken, and the information is never altered or manipulated
- G5** Allow the system to retrieve data about the accidents that occur on the territory and data about issued tickets via the municipality provided service
- G6** Allow the system to cross the information submitted by the users and the information retrieved from the municipality to build statistics

**G7** Allow users to consult a map highlighting the streets (and the areas) with the highest frequency of violations, the identified potentially unsafe areas and view statistics about previously stored violations

**G8** Allow municipality to consult the system data and receive suggestions on possible interventions via a restrict access API

## 1.3 Glossary

### 1.3.1 Definitions

**System *or* Product:** the SafeStreets software we are to develop

**Municipality:** a city, a town or a village, or a small group of them

**Local authorities *or* authorities:** the local authorities of the municipality for example the local police

**Guest *or* Guest user:** person who access the system as non logged user

**Logged user *or* Authenticated user:** authenticated person who is interfacing with the system

**User:** guest user or logged user

**Registration:** interaction between a non registered user and the system in which the user, providing all of the information required by the system for the creation of an account, receives from the system the credentials needed to authenticate to the system

**Authentication *or* Login:** interaction between guests and the system that grants authenticated user's privileges to a guest user

**Upload procedure:** process which realises the transfer of data between the user and the system

**Restricted access API:** API that can be used only by authorised person or system through an access token

**GPS Coordinates:** GPS coordinates are a unique identifier of a precise geographic location on the earth

**Chain of Custody *or* Chain of Evidence:** process of validating how any kind of evidence has been gathered, tracked, and protected on its way to a court of law. It guarantees that the data presented is "as originally acquired" and has not been tampered with and is authentic prior to admission into evidence. [4]

### 1.3.2 Acronyms

**RASD:** Requirements Analysis and Specification Document

**API:** Application Programming Interface

**GPS:** Global Position System

**DBMS:** Data Base Management System

**GIS:** Geographic Information System

**UML:** Unified Modelling Language

### 1.3.3 Abbreviations

**m:** meters (with multiples and submultiples)

**w.r.t.:** with respect to

**i.f.f.:** if and only if

**i.e.:** in example

**etc.:** et cetera

## 1.4 Document overview

According to the IEEE standard [5], this document is structured as

1. **Introduction:** it provides an overview of the entire document and product goals
2. **Overall Description:** it describes general factors that affect the product providing the background for system requirements
3. **Specific Requirements:** it contains all the software requirements to a level of detail sufficient to enable designers to design a system to satisfy those requirements, and testers to test that the system satisfies those requirements
4. **Formal Analysis using Alloy:** includes a brief presentation of the main objectives driving the formal modelling activity, as well as a description of the model itself, and what can be proved with it

## 2 Overall Description

### 2.1 Product Perspective

The product is not independent nor totally self-contained but defines a component of a larger system. This subsection relates the requirements of that larger system to functionality of the software and identifies interfaces between that system and the software.

A class diagram in UML that describes the general structure of the system showing the system's classes, their attributes, operations (or methods), and the relationships among objects is represented in Figure 1. To ensure a better readability not all class attributes and operations are represented.

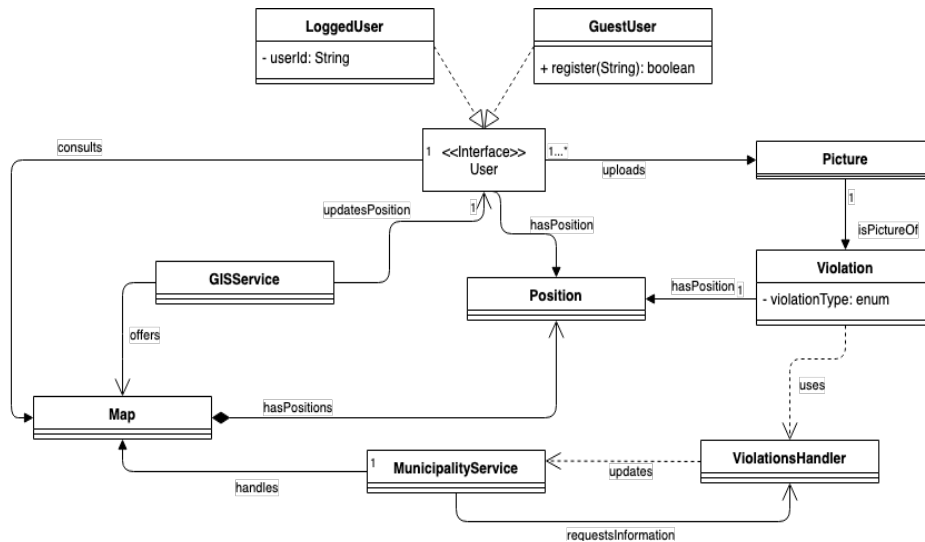


Figure 1: SafeStreets Class Diagram CHANGE HANDLER + GIS Request

#### 2.1.1 System Interfaces

The system requires some external interfaces (represented in Figure 2) to accomplish the goals stated before.

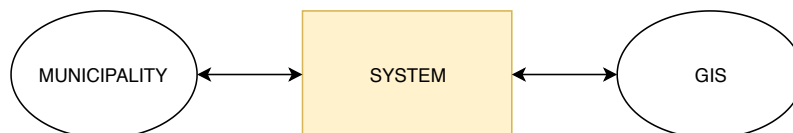


Figure 2: Overview of system interfaces



**Municipality Data Exchange** The system will interact with municipalities. The system will retrieve the information about the accidents that occur on the territory of the municipality and cross this information with its own data to identify potentially unsafe areas. It will also retrieve the information about issued tickets from the municipalities to build statistics, for example about the most egregious offenders, or the effectiveness of the SafeStreets initiative (e.g., by looking for trends in the issuing of tickets). In addition, our system will expose via a *restricted access API* the stored information about the violations to the municipalities, so that the local authorities can generate traffic tickets from it, and receive suggestions for possible interventions (e.g., add a barrier between the bike lane and the part of the road for motorised vehicles to prevent unsafe parking). [3]

**Geographic Information System** The system will interact with an external GIS. Our system will map the spatial location of stored violations and visualise the spatial relationships among them. The external GIS will map quantities, such as where the most and least number of violations occurred, to find places that meet the user requested criteria inside an area of interest. This can be accomplished mapping concentrations, or a quantity normalised by area or total number. The system can map the change in a specific geographic area to visualise statistics, or to evaluate the results of the SafeStreets initiative.

### 2.1.2 User Interfaces

The system requires a user interface as the access point where users interact with the system. As the user interface design can dramatically affect the usability and user experience of the system, the layout of the user interface will be clearly set out so that elements can be found in a logical position, in a way that users will be able to find the the information and services they are looking for.

**Guest User** Using the user interfaces of the system guest users can:

- Register to the system
- Authenticate and log-in to the system

**Logged User** Using the user interfaces of the system logged users can:

- Submit a violation with all the required and optional metadata
- Consult a map through an external GIS visualising specific data based on a selected criteria
- Consult different statistics generated upon the system and the municipality collected data
- View and edit personal information

### 2.1.3 Hardware Interfaces

The system will interact with the user's device hardware interfaces.

- Telephony and other wireless connections are leveraged for the communication between the user and the system
- Full access to the user's device camera hardware is needed for the user to capture a photo
- The geomagnetic field sensor and the proximity hardware-based sensor are leveraged to determine the position of the user's device

### 2.1.4 Software Interfaces

In order to accomplish the [goals stated before](#) the system requires to interface with Databases and DBMSs, required in order to store data about users, violations, and the corresponding metadata. These interfaces are also required to guarantee the ability to input queries to the database in order to satisfy the system required capabilities.

### 2.1.5 Communication Interfaces

The system requires secure communication within the involved entities in a way not susceptible to eavesdropping or interception. Secure communication includes means by which the system can share information that third parties cannot intercept or alter. For these reasons communication encryption methods must be implemented in a way that guarantees the use of encryption, i.e. if encrypted communication is impossible then no traffic is sent.

## 2.2 Product Functions

**Violation Upload Procedure** Provide logged users with the ability to notify authorities when traffic violations occur and, in particular, parking violations. The application allows users to send pictures of violations, including the suitable required metadata. In particular, when it receives a picture, it runs an algorithm to read the license plate number (the user can help with the recognition via an optional form) and it stores the retrieved information with the violation, including also the type of the violation (submitted by the user) and the street where the violation occurred. [3]

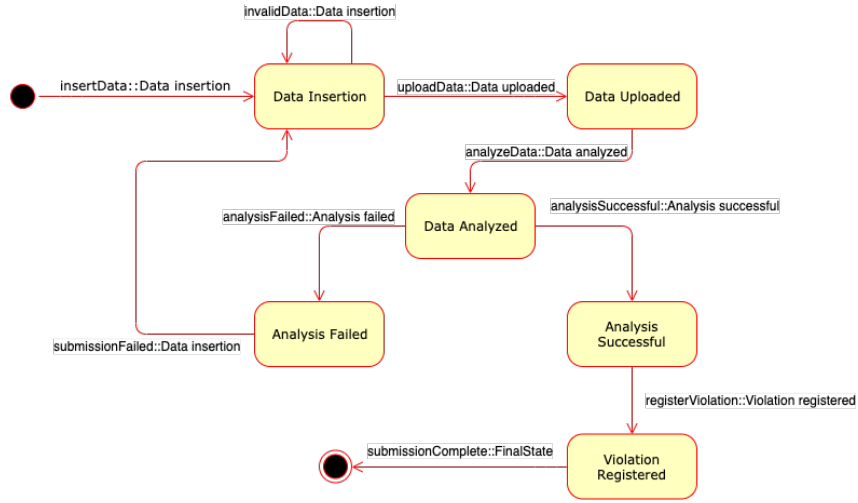


Figure 3: Violation Upload Process

**Retrieve Data from Municipality** Retrieve the information about the accidents that occur on the territory and the issued tickets using the service offered by the municipalities and cross this data with SafeStreets data to identify potentially unsafe areas and build different types of statistics. This will also allow the system to understand which violations are more likely to cause accidents in a particular zone and elaborate suggestions on possible interventions, later communicated to the municipality via a *restricted access API* provided to them. [3]

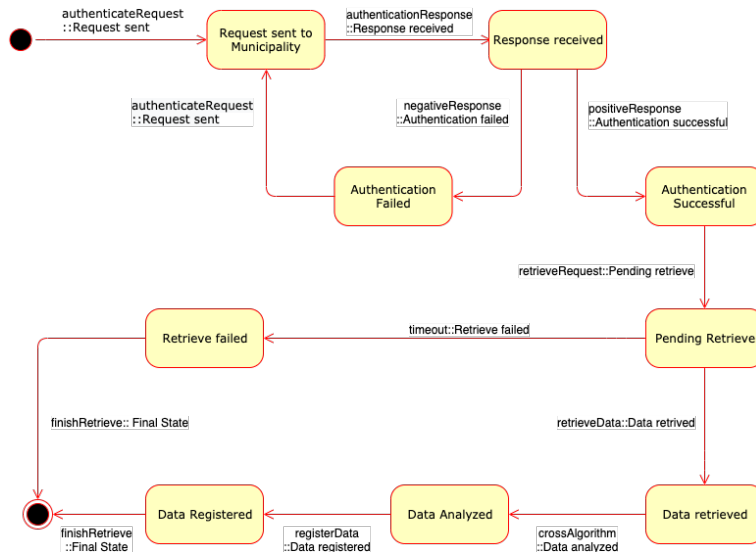


Figure 4: Retrieve Data From Municipality

**Show Information and Statistics** The application allows logged users to mine the information that has been received, highlighting the streets (or the areas) with the highest frequency of violations, considered unsafe areas, or the vehicles that commit the most violations. In addition, statistics about issued tickets, about the most egregious offenders, or the effectiveness of the SafeStreets initiative, are shown to the user if requested. [3]

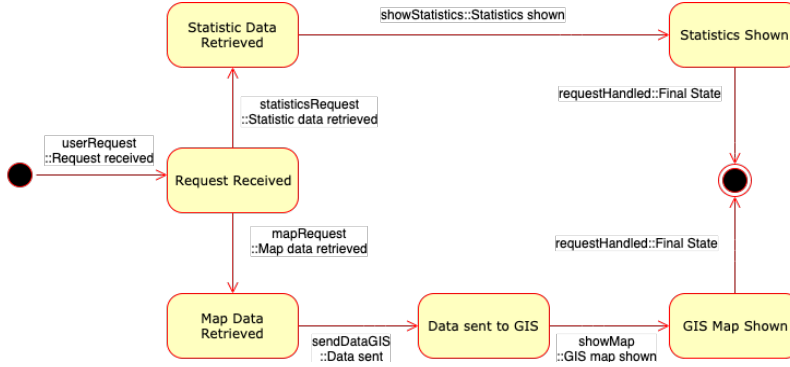


Figure 5: Show Information and Statistics

**Restricted Access API** The system will expose via a *restricted access API* the stored information about the violations to the municipalities, so that the local authorities can generate traffic tickets from it and receive suggestions for possible interventions to carry out (e.g., add a barrier between the bike lane and the part of the road for motorised vehicles to prevent unsafe parking), in order to decrease the risk of those areas, increasing their safety. [3]

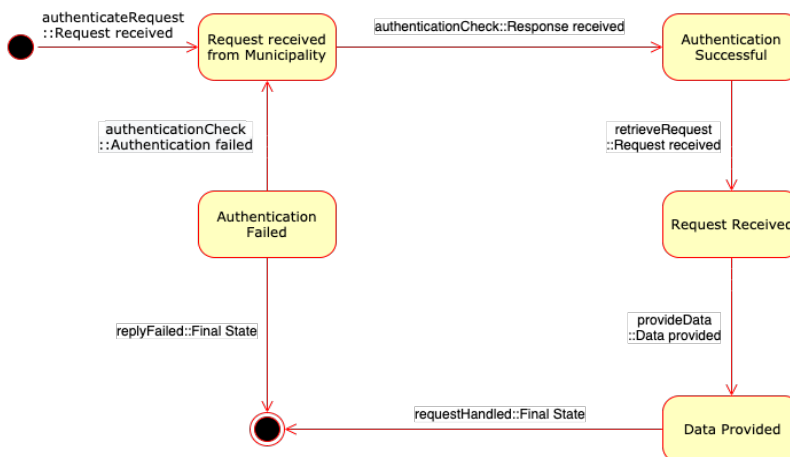


Figure 6: Restricted access API

### 2.3 User Characteristics

Users can use our system when they notice a violation and want to communicate it to the authorities. Necessary conditions for the user in order to use the system are:

- The user must have a smartphone with a working connection to the internet and must be able to functionally use the provided services
- The user must be in the age of majority in order to decrease the cases of wrong reports caused by user's inexperience on the topic
- A direct consequence of the previous item is that the user must be able to identify violations and the different types of violations

The user agrees to these conditions during the registration to the system.

### 2.4 Constraints

We assume that these constraints are always met:

- C1** GPS position is supposed to be accurate (max error  $\pm 5m$ )
- C2** The quality of the picture is sufficient to recognise the plate number (min resolution 320x240)
- C3** Internet connection must be strong enough to allow the upload of the picture in a reasonable amount of time (supported technologies are 3G, 4G and 5G due to the performance requirement)

### 2.5 Assumptions

We assume that these assumptions hold true in the domain of our system

- DA1** GPS position of all users is always obtainable
- DA2** Internet connection always works correctly
- DA3** Municipality services are always reachable
- DA4** The maps provided by the GIS are always reachable and up to date
- DA5** The DBMS always works properly and the information in the DB are always accessible

## 3 Specific Requirements

### 3.1 External Interfaces

#### 3.1.1 System Interfaces

**Municipality Data Exchange** The definition of the municipality data exchange interface is dependent to the corresponding SafeStreet's interface required to be offered to the municipalities. The municipality is required to offer the following functionalities to the system:

- guarantee a secure authentication to the municipalities' system using a provided *restricted access API*
- provide a secure transfer of data related to accidents occurred in the territory of the municipality
- provide a secure transfer of data related to local authorities' issued tickets

Leveraging the retrieved municipality data the system is required to cross this information with the system previously stored data. In addition, the system is required to perform the following functions on the crossed data:

- build statistics on the frequency of violations
- build statistics on the vehicles that commit the most violations
- build statistics on the most egregious offenders leveraging the issued tickets data
- build statistics on the effectiveness of the SafeStreets initiative by looking for trends in the issuing of tickets
- identify potentially unsafe areas and store this new generated information
- identify possible interventions to be suggested to the municipalities and store this new generated information

To fulfil the bidirectional data exchange the system is required to offer the following functionalities to the municipalities:

- guarantee a secure authentication to the system using a provided *restricted access API*
- provide a secure transfer of data related to user uploaded violations and all the corresponding metadata
- provide a secure transfer of data related to possible interventions suggestions

**Geographic Information System** The definition of the external GIS interface is GIS dependant and will be described in a functionality-based way. The system is required to perform the following functions:

- load and filter data based on the user requested criteria
- cache retrieved data for the most common user requested criteria
- communicate the loaded and filtered data to the external GIS with the final goal of presenting the requested map to the user via the user interfaces

The system via the external GIS is required to be capable of handling the following data visualisations:

- visualise the spatial location of stored violations inside a specific geographic area requested by the user
- visualise the spatial location of stored violations inside a specific geographic area and a specific time range requested by the user
- visualise the distinction between possible safe and unsafe areas identified by the system
- map quantities and concentrations, such as where the most and least number of violations occurred, highlighting the streets (and areas) with the highest frequency of violations
- map the change of quantities and concentrations inside a specific geographic area and a specific time range requested by the user

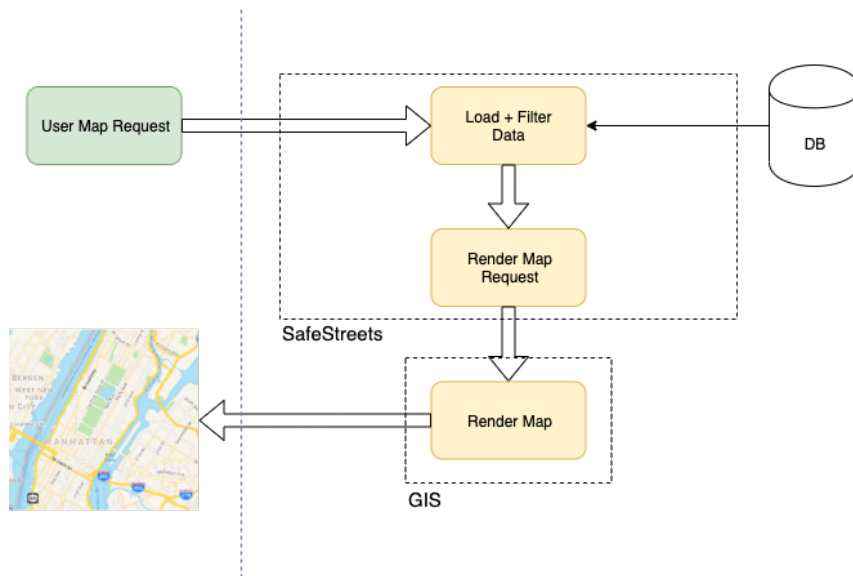


Figure 7: GIS Interaction Diagram

**3.1.2 User Interfaces****3.1.3 Hardware Interfaces****3.1.4 Software Interfaces****3.1.5 Communication Interfaces****3.2 Functional Requirements**

Definition of use case diagrams, use cases and associated sequence/activity diagrams, and mapping on requirements

**3.3 Performance Requirements****3.4 Logical Database Requirements****3.5 Design Constraints****3.5.1 Standards Compliance****3.5.2 Hardware Limitations****3.5.3 Other?****3.6 Software System Attributes****3.6.1 Reliability****3.6.2 Availability****3.6.3 Security****3.6.4 Maintainability****3.6.5 Portability****3.7 Functional Requirements**

The following requirements are derived in order to achieve the specified goals.

**3.7.1 Goals**

**G1** Allow guest users to register to the system

**R1** The system must require the *guest* user to insert his fiscal code, a username, a valid e-mail and a password to identify him

**R2** The system must check that the validity of the data inserted by the *guest* user namely avoid duplicates, invalid fiscal codes and too weak passwords



- R3** The system must send an e-mail to the *guest* user to verify the e-mail address given during the registration
- DA2** Internet connection always works correctly
- DA6** The smartphone of the user runs iOS (9 or later) or Android (Jelly Bean or later)
- G2** Allow registered users to authenticate to the system
  - R4** The system must require the user to insert his username and password to authenticate to the system
  - R5** The system must be able to check if the username and password pair correspond to a user correctly registered to the system and grant the access to that user
  - DA2** Internet connection always works correctly
  - DA5** The DBMS always works properly so that the information in the DB are always accessible
- G3** Allow users to transfer data to the system describing occurred violations, including the suitable metadata to describe the submitted violation
  - R6** The system must allow the user to take a picture of the violation and the plate from the mobile application
  - R7** The system must allow the user to manually insert the license plate number in order to help the recognition algorithm
  - R8** The system must be able to retrieve the license plate of the vehicle running an algorithm to recognise it
  - R9** The system must be able to verify that the license plate number is valid and registered to a vehicle
  - R10** The system must require the user to specify the type of violation
  - R11** The system must allow the user to provide the location of the violation, manually specifying the address, picking it up from the map or using the GPS of the device
  - C2** The quality of the picture is sufficient to recognise the plate number (min resolution 320x240)
  - C3** Internet connection must be strong enough to allow the upload of the picture in a reasonable amount of time (supported technologies are 3G, 4G and 5G due to the performance requirement)
  - DA1** GPS position of all users is always obtainable
  - DA2** Internet connection always works correctly
- G4** Ensure that the chain of custody of the information provided by the users is never broken, and the information is never altered or manipulated
  - R12** The system must provide a secure channel to communicate with the users
  - R13** The system must encrypt the connection with the users in order to protect the process of providing data
  - R14** The system must adopt security measures to prevent malicious accesses and to protect sensible data

**R15** Questo davvero non lo so mori miei

**G5** Allow the system to retrieve data about the accidents that occur on the territory and data about issued tickets via the municipality provided service

**R16** The system must be able to retrieve data about accidents from municipality systems

**R17** The system must be able to process data retrieved from municipality

**R18** The system must be able to elaborate accidents and violations information to extract data about unsafe areas

**R19** The system must be able to provide data to municipality systems to suggest possible interventions to increase safety in a specific area

**DA2** Internet connection always works correctly

**DA3** Municipality services are always reachable

**G6** Allow the system to cross the information submitted by the users and the information retrieved from the municipality to build statistics

**R20**

**G7** Allow users to consult a map highlighting the streets (and the areas) with the highest frequency of violations, the identified potentially unsafe areas and view statistics about previously stored violations

**R21** The system must be able to retrieve data about tickets issued by the municipality

**R22** The system must be able to process data retrieved from municipality

**R23** The system must be able to elaborate issued tickets information to generate statistics about useful violations provided by users

**G8** Allow municipality to consult the system data and receive suggestions on possible interventions via a restrict access API

**R24** The system must be able to retrieve data about tickets issued by the municipality

**R25** The system must be able to process data retrieved from municipality

**R26** The system must be able to elaborate issued tickets information to generate statistics about useful violations provided by users

### 3.8 Performance Requirements

The system should ensure acceptable response times in the interactions with the user, which strictly depends on the number of concurrent users and the connection speed.

The processes of providing data and loading the map of safe and unsafe areas shouldn't be too slow.

### **3.9 Software System Attributes**

#### **3.9.1 Availability**

The system must be available 99,9% of the time (up to 8,76 hours per year of downtime). The system should be accessible 24 hours per day.

#### **3.9.2 Security**

Users personal information and payment information are encrypted and must be protected during transmission, as already stated the PTPP protocol will be used to ensure encryption through the network. Restricted access APIs must check that who tries to use them is actually allowed to do so.

#### **3.9.3 Portability**

The system must be also accessible by the most common mobile platforms (iOS and Android devices).

## 4 Use cases identification

### 4.1 Scenarios

Here are some scenarios that describe the usage of the system.

#### 4.1.1 Scenario 1

Davide is walking down the street and notices a car parked over the crosswalks. He opens the SafeStreets app, registers to the system with his fiscal code, and takes a picture from the in-app camera. Before uploading he adds information such as the type of violation (i.e. "Bad Parking") and the street in which the violation occurred. As soon as SafeStreet processes the uploaded data the authorities are alerted.

#### 4.1.2 Scenario 2

Carlo wants to teach his son to drive and wants to find the safest area of Milan in order to avoid exposing him to difficult situations in his first drives. He opens the SafeStreets app and consult the map with the streets that have the greatest number of incidents and violations, and will try to avoid them allowing his son to have a safe drive.

#### 4.1.3 Scenario 3

SafeStreets automatically retrieves data from the municipality's service, and after a while notices that extremely frequently cars are parked in a restricted area of Milan. After further analysis and with the help of the users they come to the conclusion that don't realise that they can't park in that area because of a misleading signal, so they contact the municipality and offer a possible solution to the problem.

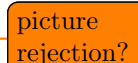
#### 4.1.4 Scenario 4

After receiving a notification of "Dangerously parked car" with the picture showing a car parked in such a way that could risk a possible collision with the tram line, SafeStreets alerts the authorities in order to facilitate the process of car removal and the consequential ticket generation.

#### 4.1.5 Scenario 5

#### 4.1.6 Scenario 6

Non so more ce ne verranno altri



picture  
rejection?

## 4.2 Use case diagram

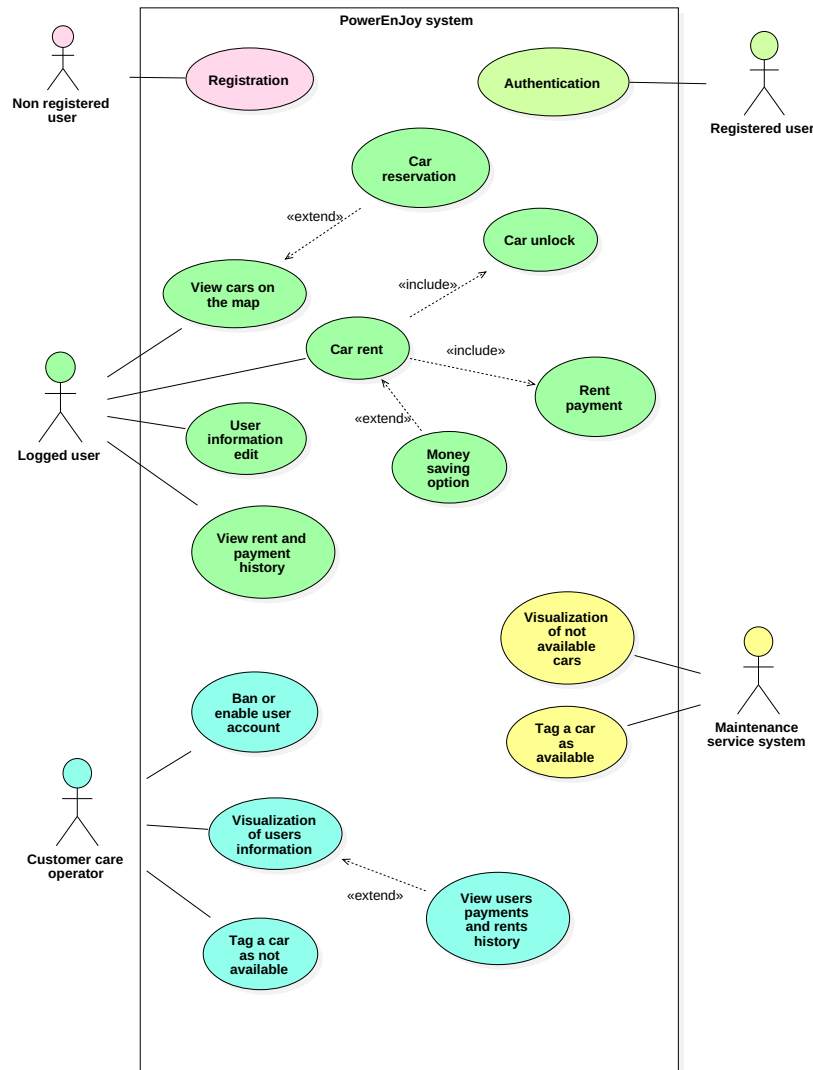


Figure 8: Use case diagram

**Notes to read the diagram** The use case diagram represents the possible interactions of actors with the system and the different use cases in which the actors are involved.

The "Maintenance service system" is an external software which the system-to-be needs to interact with.

We do not consider the external payment handling system an actor since it does not start any interaction with our system, it simply reacts when our system requests its services; this interaction is encapsulated as sub-procedure in the flow of events of the "Rent payment" use case.

We do not consider the car an actor for the same reason, moreover the only interactions started by the car are trigger events which are very simple interactions, which we do not consider use cases.

### 4.3 Use cases description

#### 4.3.1 Registration

Name	Registration
Actors	Non registered user
Entry conditions	
Flow of events	<ul style="list-style-type: none"> <li>(a) The user asks the system to register to its services</li> <li>(b) The system shows the appropriate form to fill to register to the system</li> <li>(c) The user inserts an username to be uniquely identified by the system</li> <li>(d) The user inserts his own email address</li> <li>(e) The user inserts his name, surname, birth date and place and current domicile</li> <li>(f) The user inserts his driving license ID code</li> <li>(g) The user inserts payment information</li> <li>(h) The user confirms data inserted are correct e submit the form</li> <li>(i) The system checks the username to be unique</li> <li>(j) The system checks the email to be unique</li> <li>(k) The system checks the driving license ID to be unique</li> <li>(l) The system sends an email to the user with a unique link to verify the email address inserted by the user really belongs to him</li> <li>(m) The user clicking on the link received confirms his email address</li> <li>(n) The user is notified by mail the registration procedure is correctly completed and provided with a password bound to his username to access the system</li> </ul>
Exit conditions	The user is able to authenticate to the system as <i>registered</i> user with its own credentials

### Exceptions

- If the username inserted by the user is already used by another user, the system displays an error message asking the user to insert another username
- If the mail inserted by the user is already used by another user, the system displays an error message asking the user to insert another mail
- If the user notices to have entered wrong informations he could edit them at the end of the process of registration in his personal page

Table 1: *Registration* use case description

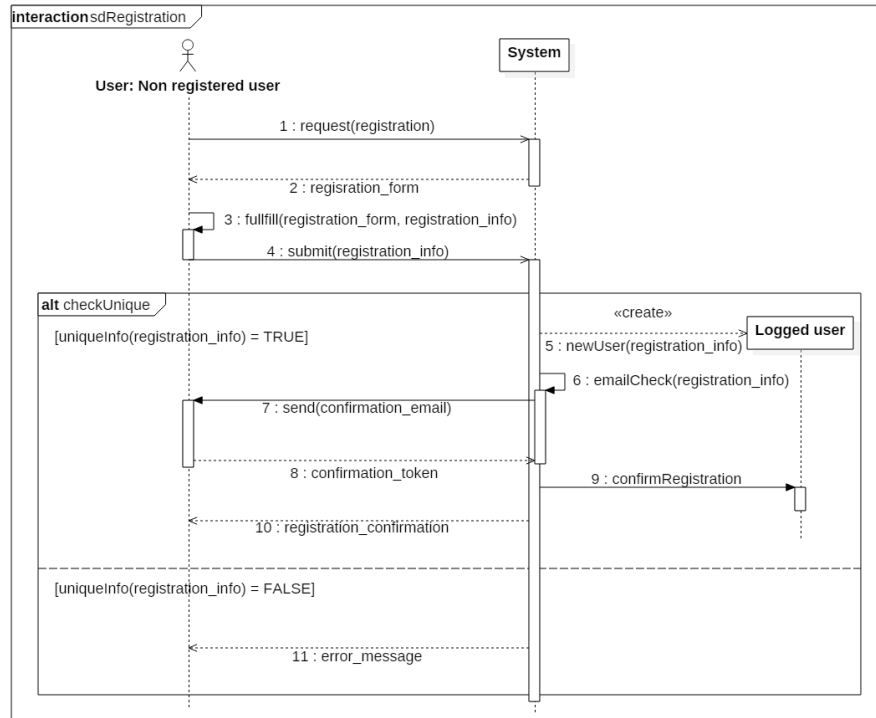


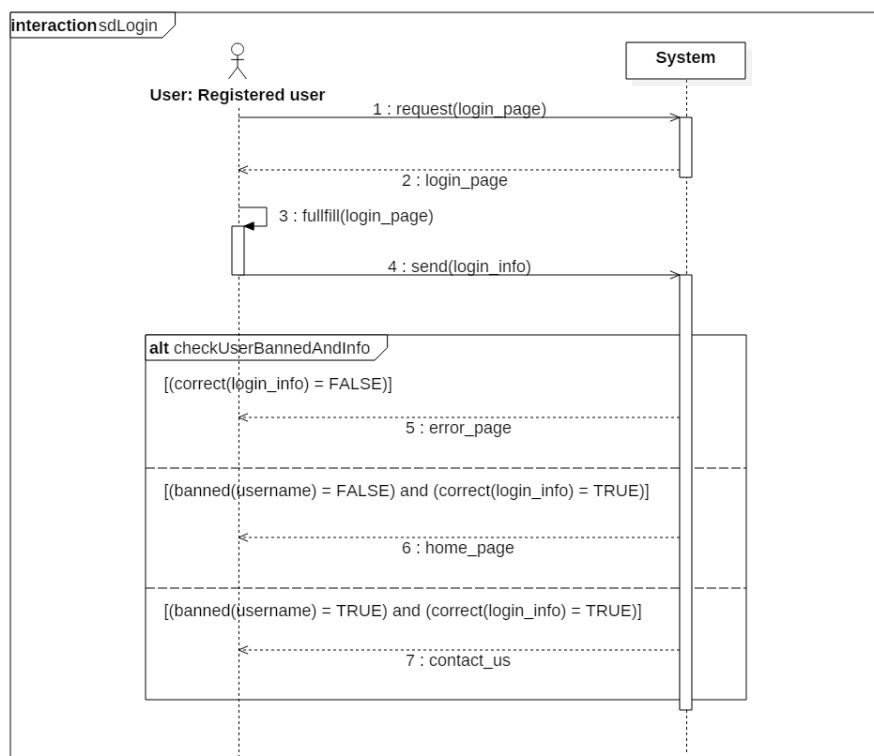
Figure 9: *Registration* sequence diagram



## 4.3.2 Authentication

Name		Authentication
Actors		Registered user
Entry conditions	condi-	The user must know his username and password
Flow of events		
<ul style="list-style-type: none"> <li>(a) The user inserts his username and password in the appropriate form and submit it</li> <li>(b) The system validates the inserted credentials checking also if the user has confirmed his own email address</li> <li>(c) The system checks if the user is banned</li> </ul>		
Exit conditions		If the credential validation is successful and the user is not banned he is granted the proper privileges
Exceptions		
<ul style="list-style-type: none"> <li>• If the credential validation failed an error message is displayed</li> <li>• If the credential validation is successful and the user is banned a message providing assistance is displayed and the system doesn't allows the user to access to the system</li> </ul>		

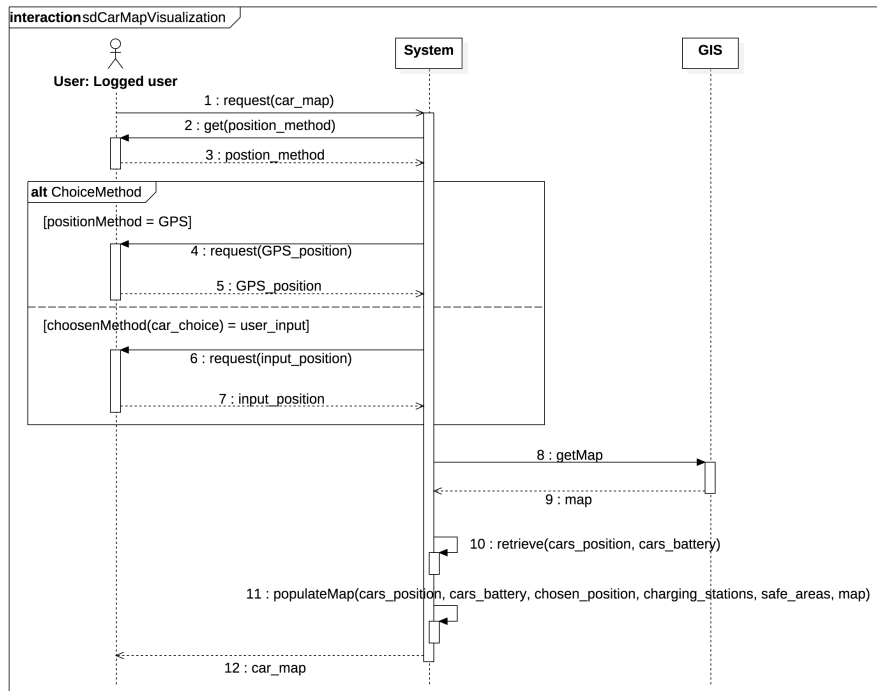
Table 2: *Authentication* use case description

Figure 10: *Authentication* sequence diagram

## 4.3.3 View cars on the map

<b>Name</b>	<b>View cars on the map</b>
<b>Actors</b>	Logged user
<b>Entry conditions</b>	
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) The user chooses if he wants to use his GPS position or insert a different one manually <ul style="list-style-type: none"> <li>a. The system retrieves the user's GPS position</li> <li>b. The user inserts a position</li> </ul> </li> <li>(b) The system retrieves the position of all <i>Available</i> cars and their battery level percentage</li> <li>(c) The system shows a map with all available cars, charging stations position and safe areas near the position indicated</li> <li>(d) The user can click on a car on the map to see its battery level percentage</li> </ul>
<b>Exit conditions</b>	The user can navigate a map with all available cars near the position indicated by him
<b>Exceptions</b>	If the position inserted by the user is not correct an error message is displayed

Table 3: *View cars on the map* use case description

Figure 11: *View cars on the map* sequence diagram

## 4.3.4 Car reservation

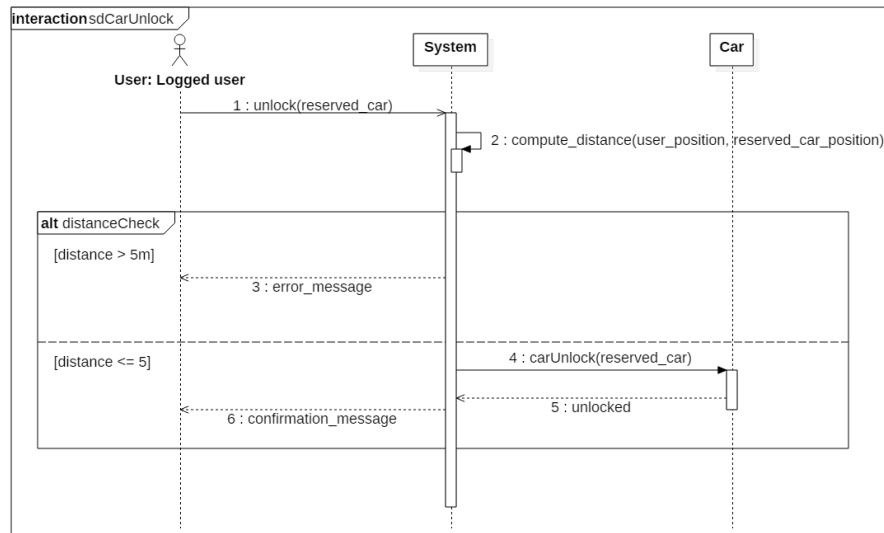
<b>Name</b>	<b>Car reservation</b>
<b>Actors</b>	Logged user
<b>Entry conditions</b>	
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) <b>View cars on the map</b></li> <li>(b) The user selects the car he wants to reserve</li> <li>(c) The user confirms he wants to reserve that car</li> </ul>
<b>Exit conditions</b>	The system set the state of the chosen car as <i>Reserved</i> paired with the user who made the reservation
<b>Exceptions</b>	If the user has already reserved a car, the system shows an error message and doesn't allow him to reserve another car

Table 4: *Car reservation* use case description

## 4.3.5 Car unlock

<b>Name</b>	<b>Car unlock</b>
<b>Actors</b>	Logged user
<b>Entry conditions</b>	The user reserved car
<b>Flow of events</b>	
	<ul style="list-style-type: none"> <li>(a) The user asks the system to unlock the car he reserved</li> <li>(b) The system checks if the user's position is at most 5 meters away from the position of the car he reserved</li> <li>(c) The system unlocks the car with the state set as <i>Reserved</i> paired with the aforementioned user</li> <li>(d) The system sends a message to the user, confirming that the car is unlocked</li> </ul>
<b>Exit conditions</b>	The car is unlocked and the user can pick it up
<b>Exceptions</b>	
	<ul style="list-style-type: none"> <li>• If the position of the user is not at most 5 meters away from the position of the car he reserved the system displays an error message</li> </ul>

Table 5: *Car unlock* use case description

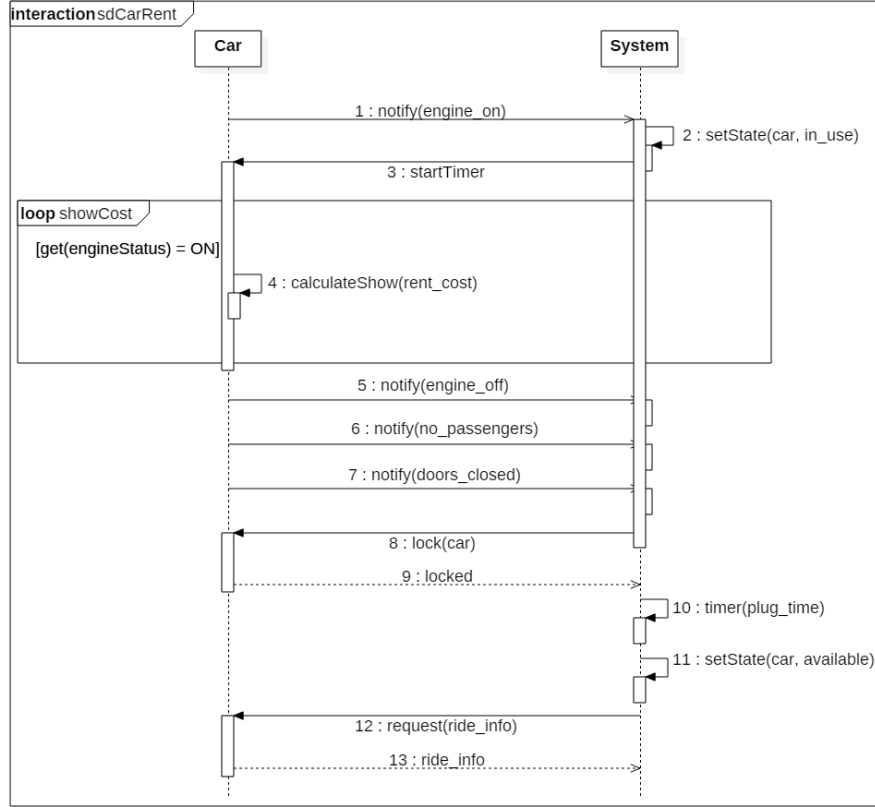
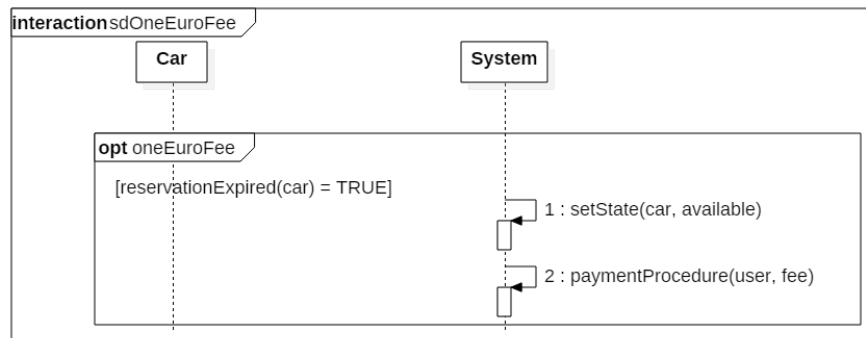
Figure 12: *Car unlock* sequence diagram

## 4.3.6 Car rent

<b>Name</b>	<b>Car rent</b>
<b>Actors</b>	Logged user
<b>Entry conditions</b>	The user is paired with the <i>Reserved</i> state of a car
<b>Flow of events</b>	<p>(a) <b>Car unlock</b></p> <p>(b) The user ignites the car engine</p> <p>(c) The system sets the state of the <i>Reserved</i> car to <i>In Use</i> paired with the same user</p> <p>(d) During the rent the user is informed about the current charge and whether he is or not inside a safe area</p> <p>(e) The user leaves the car turning off the engine and closing the doors</p> <p>(f) The system locks the car</p> <p>(g) The system activates a timer to allow the user to plug the car into a charging station if it is near one of them</p> <p>(h) When the timer expires:</p> <p>8.1 The system retrieves informations about the ride from the car: number of passengers detected during the ride, position of the car and battery level at the end of the ride and if the car is or not on charge</p> <p>8.2 The system sets the car as <i>Available</i></p> <p>(i) <b>Rent payment</b></p>
<b>Exit conditions</b>	The user is charged of the correct amount for the ride and at anytime could perform another rent, the car is available again
<b>Exceptions</b>	<ul style="list-style-type: none"> <li>• If the user doesn't start the engine up to one hour after the reservation, he is charged of 1€(through a payment procedure), the car state is set as <i>Available</i> and the user is notified his reservation is expired</li> </ul>

Table 6: *Car rent* use case description



Figure 13: *Car rent* sequence diagramFigure 14: *One Euro fee* sequence diagram

The overall status of a car can be represented by the FSM in [Figure 15](#)

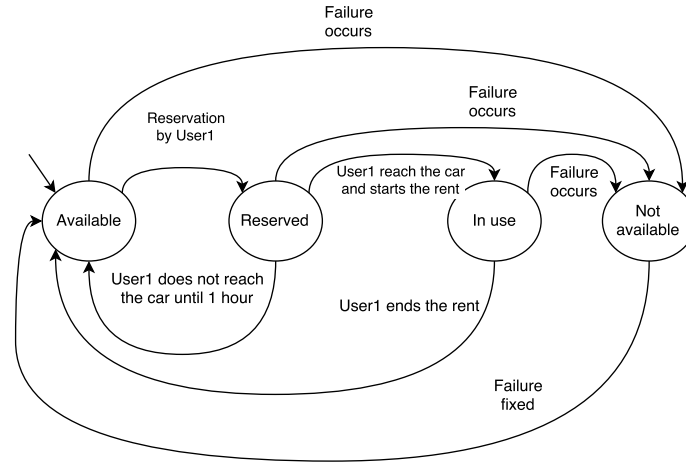


Figure 15: Car status FSM

**Notes to read the diagram** The *Not Available* state includes the cases in which the car is either broken or a user left it with a critical battery level and not on charge.

The system changes the state of a car from *Available* to *Not Available* when its battery level is critical and the car is not on charge (see ??).

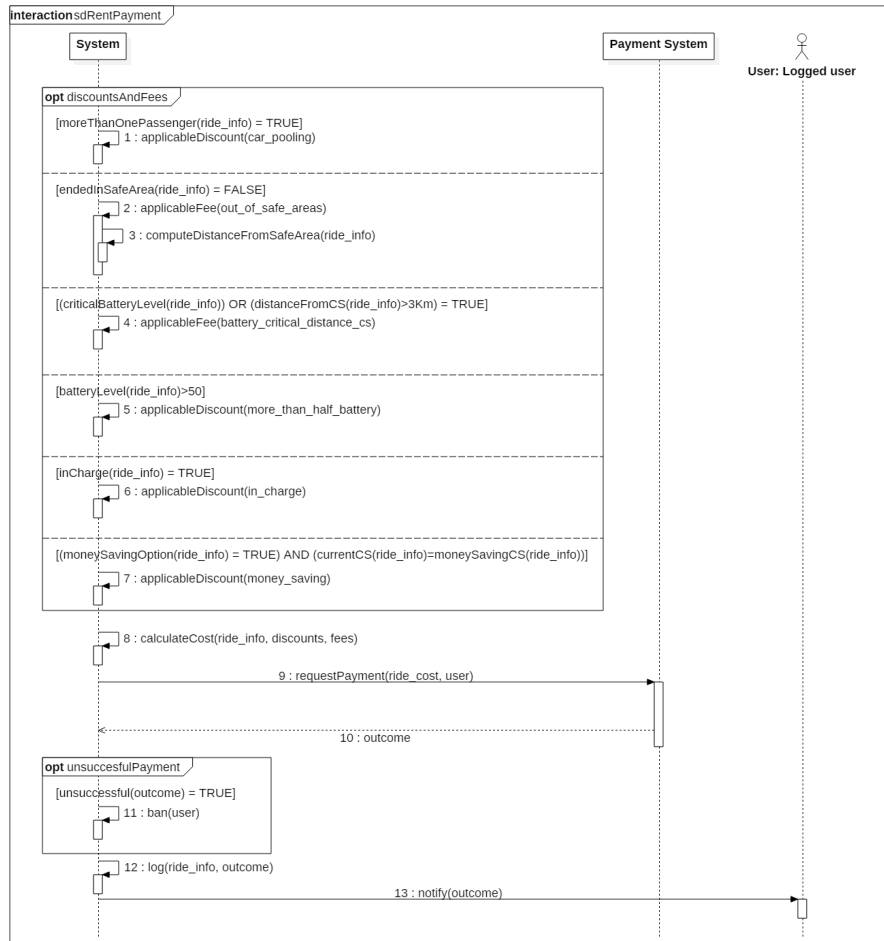
Even if the car is left with no battery left, it is still able to communicate with the system, so the rent can end normally and the maintenance service will take care the car (see ??).

**4.3.7 Rent payment**

<b>Name</b>	<b>Rent payment</b>
<b>Actors</b>	Logged user
<b>Entry conditions</b>	The user must have completed a rent shutting off the engine and exiting the car. The system has retrieved information about the ride from the car.
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) The system checks if the car position is or is not inside a safe area</li> <li>(b) The system checks if the car has detected more than one passenger during the rent</li> <li>(c) The system checks the car battery percentage</li> <li>(d) The system checks if the car is plugged on a charging station</li> <li>(e) The system checks the distance of the car from the nearest charging station</li> <li>(f) The system calculates the cost of the ride based on the rent time</li> <li>(g) The system determines the applicable discounts/extra fee applying it to the cost of the ride</li> <li>(h) The system starts a payment procedure with user's payment information using an external service</li> <li>(i) The system waits a response from the external payment service</li> <li>(j) The system logs data about the rent and the payment</li> <li>(k) The system notifies the user about the result of the payment procedure and on discount/extra fees applied</li> </ul>

<b>Alternative flow</b>	Flow of events as specified upon from 1 to 7
	8 a. The system detects the user has enabled the <i>money saving option</i>
	8 b. The system checks if the car is currently on charge on the charge station determined by the system at the begin of the rent
	8 c. The system determines the applicable discounts/extra fee applying it to the cost of the ride eventually also taking in account the <i>money saving option</i> discount if the car is currently on charge on the charge station determined by the system at the begin of the rent
	Flow of events as specified upon from 9 to 12
<b>Exit conditions</b>	The user is charged of the correct amount for the ride
<b>Exceptions</b>	<ul style="list-style-type: none"> <li>• If the payment procedure is not correctly completed the user is banned, rent information is stored, the payment suspended and the user is informed to contact the customer service.</li> </ul>

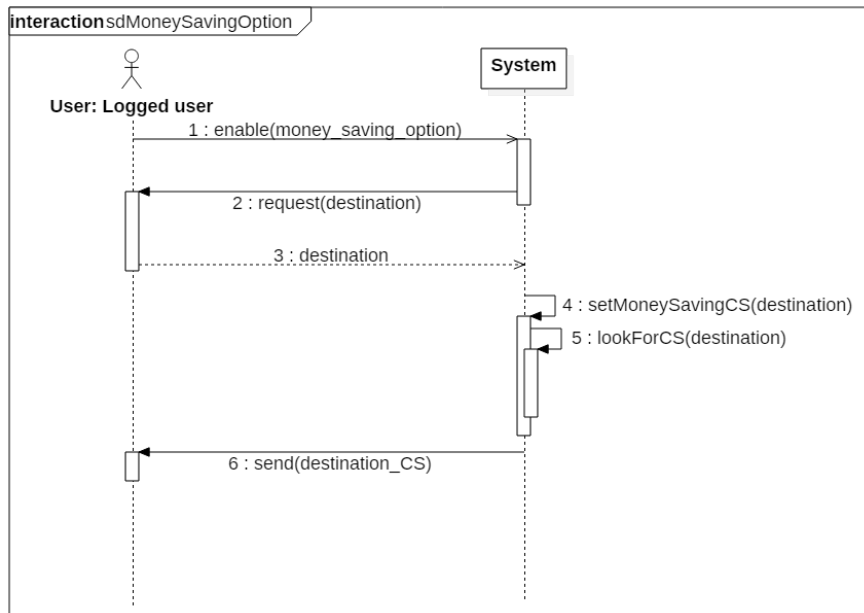
Table 7: *Rent payment* use case description

Figure 16: *Rent payment* sequence diagram

## 4.3.8 Money saving option

<b>Name</b>	<b>Money saving option</b>
<b>Actors</b>	Logged user
<b>Entry conditions</b>	The user should have enabled the <i>money saving option</i>
<b>Flow of events</b>	<p>(a) <b>Car Reservation</b></p> <p>(b) The system asks the user to insert his destination</p> <p>(c) The user inserts his destination</p> <p>(d) The system searches for charging stations near the destination position inserted by the user with available plugs</p> <p>(e) The system chooses a charging station in order to ensure a uniform distribution of cars in the city and taking in account the destination of the user</p> <p>(f) The system informs the user about the charging station to reach in order to obtain the discount</p> <p>(g) <b>Car Rent</b> (<b>Car Reservation</b> already done)</p>
<b>Exit conditions</b>	<ul style="list-style-type: none"> <li>• If the user has left the car plugged in the charging station suggested by the <i>money saving option</i> he has obtained the correct discount</li> <li>• The user can any time perform another rent</li> <li>• Car is again available</li> </ul>
<b>Exceptions</b>	<ul style="list-style-type: none"> <li>• If the user doesn't leave the car in the charging station suggested by the <i>money saving option</i> he doesn't obtain the related discount</li> </ul>

Table 8: *Money saving option* use case description

Figure 17: *Money saving option* sequence diagram

## 4.3.9 Visualization of not available cars

Name		Visualization of not available cars
Actors		Maintenance service system
Entry conditions	condi-	Maintenance service system must know the access token to be identified by the system
Flow of events		
<ul style="list-style-type: none"> <li>(a) The maintenance service system asks for the list of car with state set as <i>Not Available</i> sending the request paired with the access token</li> <li>(b) The system checks the access token</li> <li>(c) The system retrieves the list of car with state set as <i>Not Available</i> along with the identifier used by the system to identify each car, the GPS position of each car, the description of the problem of each car and the software key to access each car</li> <li>(d) The system sends the information to the maintenance service system</li> </ul>		
Exit conditions		The maintenance service system receives the list of cars with state set as <i>Not Available</i>
Exceptions		
<ul style="list-style-type: none"> <li>• If the access token sent by the maintenance service system is not recognized, the system sent to the maintenance service system an error message</li> </ul>		

Table 9: *Visualization of not available cars* use case description



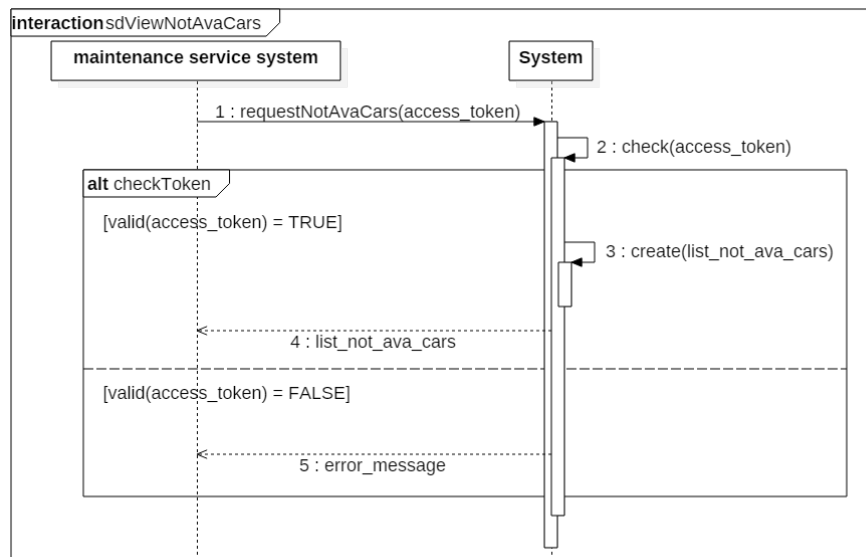
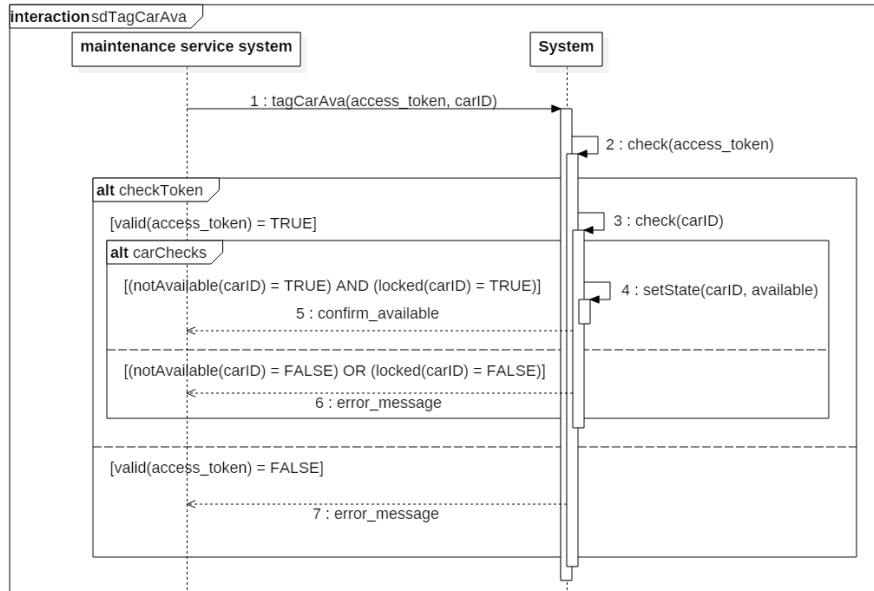


Figure 18: Visualization of not available cars sequence diagram

## 4.3.10 Tag a car as available

<b>Name</b>	<b>Tag a car as available</b>
<b>Actors</b>	Maintenance service system
<b>Entry conditions</b>	Maintenance service system must know the access token to be identified by the system
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) The maintenance service system asks to tag a car as Available sending the car identifier paired with the access token</li> <li>(b) The system checks the access token sent by the maintenance service</li> <li>(c) The system checks the identifier received corresponds to a car with state set as <i>Not Available</i></li> <li>(d) The system checks if the car identified by the identifier received is locked</li> <li>(e) The system set the state of the car identified by the aforementioned identifier as <i>Available</i></li> <li>(f) The system sends to the maintenance service system a confirmation message the car state has been set as <i>Available</i></li> </ul>
<b>Exit conditions</b>	The car state is set as <i>Available</i>
<b>Exceptions</b>	<ul style="list-style-type: none"> <li>• If the access token sent by the maintenance service system is not recognized, the system sends to the maintenance service system an error message</li> <li>• If the car identifier sent by the maintenance service system is not recognized or doesn't correspond to a car set as <i>Not Available</i>, the system sends to the maintenance service system an error message</li> <li>• If the car identifier sent by the maintenance service system corresponds to a car not locked, the system sends to the maintenance service system an error message</li> </ul>

Table 10: *Tag a car as not available* use case description

Figure 19: *Tag a car as available* sequence diagram

## 4.3.11 Visualization of users information

Name	Visualization of users information
Actors	Customer care operator
Entry conditions	
Flow of events	<ul style="list-style-type: none"> <li>(a) The customer care operator inserts the username or the mail of a registered user</li> <li>(b) The system checks if the username or the mail correspond to a user registered to the system</li> <li>(c) The system retrieves user's data (name, surname, birth date and place, current domicile and driving license information) along with information about the car state the user is actually paired with</li> <li>(d) The system shows to the customer care operator the info about the user</li> </ul>
Exit conditions	The customer care operator can view the information required about the user
Exceptions	<ul style="list-style-type: none"> <li>• If no users are found according to the parameters inserted by the customer care operator the system shows an error message</li> </ul>

Table 11: *Visualization of users information* use case description

## 4.3.12 View users payments and rents history

<b>Name</b>	<b>View users payments and rents history</b>
<b>Actors</b>	Customer care operator
<b>Entry conditions</b>	
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) <b>Visualization of users information</b></li> <li>(b) The customer care operator asks to view user's payments and rents history</li> <li>(c) The system retrieves the list of user's payments (successful and unsuccessful)</li> <li>(d) The system retrieves the list of user's rents</li> <li>(e) The system shows to the customer care operator user's payments and rents history</li> </ul>
<b>Exit conditions</b>	The customer care operator can view the information required about the user
<b>Exceptions</b>	

Table 12: *View users payments and rents history* use case description

## 4.3.13 Mark or unmark a user as banned

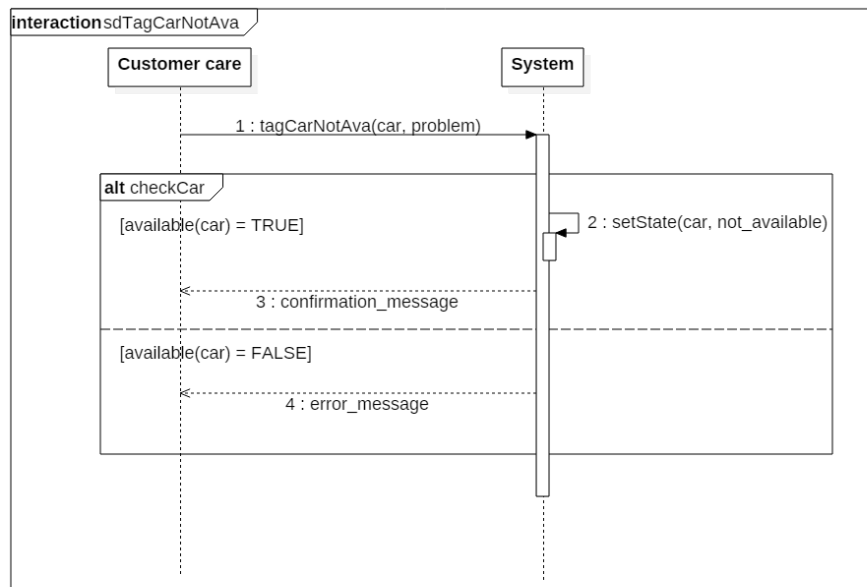
<b>Name</b>	<b>Mark or unmark a user as banned</b>
<b>Actors</b>	Customer care operator
<b>Entry conditions</b>	
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) The customer care operator inserts the username of a registered user</li> <li>(b) The customer care operator asks to ban or to enable the registered user paired with the inserted username <ul style="list-style-type: none"> <li>• If the operator wants to mark a user as <i>banned</i> he must insert a brief description of reasons why</li> </ul> </li> <li>(c) The system checks if the username corresponds to a user registered to the system</li> <li>(d) The system marks or unmarks the user paired with the username as <i>banned</i></li> </ul>
<b>Exit conditions</b>	The state of the user is updated
<b>Exceptions</b>	<ul style="list-style-type: none"> <li>• If the username inserted by the customer car operator is not recognized, the system shows an error message</li> </ul>

Table 13: *Mark or unmark a user as banned* use case description

## 4.3.14 Tag a car as not available

<b>Name</b>	<b>Tag a car as not available</b>
<b>Actors</b>	Customer care operator
<b>Entry conditions</b>	
<b>Flow of events</b>	<ul style="list-style-type: none"> <li>(a) The customer care operator inserts the identifier of the car</li> <li>(b) The customer care operator asks to mark the car as <i>Not Available</i></li> <li>(c) The customer care operator inserts a brief description of why the car state must be set as <i>Not Available</i></li> <li>(d) The system checks the car identifier</li> <li>(e) The system set the state of the car identified by the aforementioned identifier as <i>Not Available</i> paired with the description</li> <li>(f) The system shows a confirmation message the car has been tagged as <i>Not Available</i></li> </ul>
<b>Exit conditions</b>	The state of the car is setted as <i>Not Available</i>
<b>Exceptions</b>	<ul style="list-style-type: none"> <li>• If car identifier sent by the customer care operator is not recognized, the system displays an error message</li> </ul>

Table 14: *Tag a car as not available* use case description

Figure 20: *Tag a car as Not Available* sequence diagram



#### 4.4 UML class diagram

Based on collected scenarios and on the identified use cases we have developed the following requirements-level class diagram[?]. To ensure a better readability class attributes are not represented.

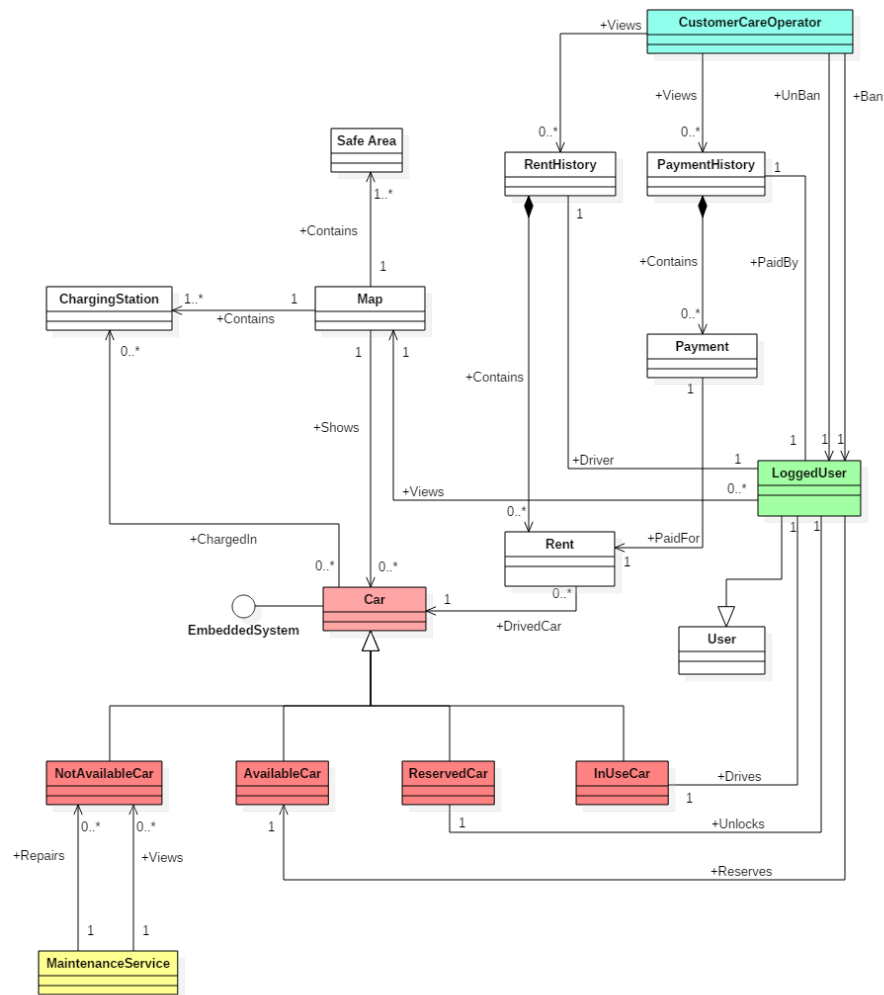


Figure 21: UML class diagram

# Appendices

## A Alloy model

### A.1 Source code

```

1  open util/boolean
2
3  sig Car{
4    batteryLevel: one BatteryLevelPercentage,
5    status: one CarStatus,
6    usedBy: lone LoggedUser,
7    reservedBy: lone LoggedUser,
8    numberOfPassengers: NOPTYPE,
9    onCharge: one Bool,
10   engineOn: one Bool
11 }
12
13 //Car statuses
14 abstract sig CarStatus{}
15 one sig Available extends CarStatus{}
16 one sig Reserved extends CarStatus{}
17 one sig InUse extends CarStatus{}
18 one sig NotAvailable extends CarStatus{}
19
20 //Battery level percentage: should be a percentage
21 //    0-100%
22 abstract sig BatteryLevelPercentage{}
23 one sig Lower20Full extends BatteryLevelPercentage{}
24 one sig More50Full extends BatteryLevelPercentage{}
25 one sig From20to50Full extends BatteryLevelPercentage{}
26
27 //Number of passengers, we assume to deal with 5
28 //    passengers cars
29 abstract sig NOPTYPE{}
30 one sig Zero extends NOPTYPE{}
31 one sig One extends NOPTYPE{}
32 one sig Two extends NOPTYPE{}
33 one sig Three extends NOPTYPE{}
34 one sig Four extends NOPTYPE{}
35 one sig Five extends NOPTYPE{}
36
37 abstract sig User{}
38 sig LoggedUser extends User{
39   //personal information
40   //other parameters
41   banned: one Bool
42 }
43
44 sig ChargingStation{
45   charging: set Car
46 }
```

```

45
46 //A RentMade models a rent made in the past, so, for
    example, in the world created
47 //the user who made the rent can be banned or the car
    used for the rent can be NotAvailable
48
49 //If a RentMade corresponds to a reservation expired the
    correspondent fee is assigned but
50 //others parameters regarding the end of the rent are
    set to default acceptable values
51
52 //leftMSOstation: true iff money saving option enabled
    and auto left on charge
53 //in the station determined by MSO
54
55 //Choice of discount to be applied is not modeled
56 sig RentMade{
57     userRent: one LoggedUser,
58     carRent: one Car,
59     endPosition: one PositionWrtPowerGrid,
60     endSafeArea: one Bool,
61     reservationExpired: one Bool,
62     endBatteryLevel: one BatteryLevelPercentage,
63     onChargeAtTheEnd: one Bool,
64     passengersDuringTheRide: one NOPType,
65     discountApplicableRent: set Discount,
66     additionalFeeRent: set Fee,
67     leftMSOstation: one Bool
68 }
69
70 abstract sig PositionWrtPowerGrid{}
71 one sig More3kmPowerGrid extends PositionWrtPowerGrid{}
72 one sig Lower3kmPowerGrid extends PositionWrtPowerGrid{}
73
74 //M1PD = MoreThan1PassengerDiscount
75 //BHFD = BatteryHalfFullDiscount
76 //CCD = CarOnChargeDiscount
77 //MSOD = MoneySavingOptionDiscount
78 abstract sig Discount{}
79 one sig M1PD extends Discount{}
80 one sig BHFD extends Discount{}
81 one sig CCD extends Discount{}
82 one sig MSOD extends Discount{}
83
84 //REF =ReservationExpiredFee
85 //OSAF =OutSafeAreaFee
86 //A3BCF =Away3kmOrCSBatteryCriticalFee
87 abstract sig Fee{}
88 one sig REF extends Fee{}
89 one sig OSAF extends Fee{}
90 one sig A3BCF extends Fee{}
91
92 //A user can be only in one car at a given time
93 fact OneUserCanBeInOneCarAtSameTime{

```

```

94   no disjoint c1,c2:Car | c1.usedBy = c2.usedBy and c1.
    usedBy != none
95 }
96
97 //A user can reserve only one car at a given time
98 fact ACarReservedByOnlyOneUser{
99   no disjoint c1,c2:Car | c1.reservedBy = c2.reservedBy
    and c1.reservedBy != none
100 }
101
102 //A car in use cannot be reserved
103 fact ACarInUseCannotBeReserved{
104   all c:Car | c.usedBy != none implies c.reservedBy =
    none
105 }
106
107 //A user cannot use one car and reserve another car at a
    given time
108 fact NoUsersCanUseAndReservedDifferentCars{
109   no disjoint c1,c2:Car | c1.usedBy = c2.reservedBy and
    c1.usedBy != none and c2.reservedBy != none
110 }
111
112 //Cars set as Available cannot be used or reserved at a
    given time
113 fact AvailableCarsCantBeReservedOrUsed{
114   no c:Car | c.status = Available and (c.usedBy != none
    or c.reservedBy != none)
115 }
116
117 //Cars set as Not Available cannot be used or reserved
    at a given time
118 fact NotAvailableCarsCantBeReservedOrUsed{
119   no c:Car | c.status = NotAvailable and (c.usedBy !=
    none or c.reservedBy != none)
120 }
121
122 //Reserved statuts must be paired with only one user
123 fact ReservedStatusMustBePairedWithOneUser{
124   all c:Car | c.status = Reserved implies (c.reservedBy
    != none and c.usedBy = none)
125 }
126
127 //In Use statuts must be paired with only one user
128 fact InUseStatusMustBePairedWithOneUser{
129   all c:Car | c.status = InUse implies (c.reservedBy =
    none and c.usedBy != none)
130 }
131
132 //Car with battery percentage lower than 20 percent full
    must be set as Not Available
133 fact CarWithBatteryPercentageLower20FullNotAvailable{
134   all c:Car | (c.batteryLevel = Lower20Full and c.
    onCharge = False) implies c.status = NotAvailable

```

```

135 }
136
137 //A car not in use can not detect number of passengers
    greater than zero
138 fact PassengersOnlyOnInUseCars{
139     no c:Car | c.status != InUse and c.numberOfPassengers
        != Zero
140 }
141
142 //A car In Use must detect at least one passenger
143 fact AtLeastOnePassengerOnInUseCars{
144     no c:Car | c.status = InUse and c.numberOfPassengers =
        Zero
145 }
146
147 //A car In Use has the engine turned on
148 //Note that a In Use car can have the engine turned off
149 fact OnlyInUseCarEngineOn{
150     all c:Car | c.engineOn = True implies c.status = InUse
151 }
152
153 //A car In Use can not be on charge
154 fact InUseCarNotOnCharge{
155     all c:Car | c.status = InUse implies c.onCharge =
        False
156 }
157
158 // A car is charging when connected to a charging
    station
159 fact CarIsChargingWhenConnected{
160     all s:ChargingStation, c:Car | c in s.charging implies
        c.onCharge = True
161     all c:Car | some s:ChargingStation | c.onCharge = True
        implies c in s.charging
162 }
163
164 // At most one charging station connected to a car
165 fact NoMoreOneCSForOneCar{
166     all disjoint s1,s2:ChargingStation | s1.charging & s2.
        charging = none
167 }
168
169 //Banned users cannot deal with cars
170 fact NoBannedUsersDealingWithCars{
171     no u:User | some c:Car | u.banned = True and ( c.
        usedBy = u or c.reservedBy = u )
172 }
173
174 //A REF is applicable if the reservation is expired
175 //No other fee are applicable if the reservation is
    expired
176 fact ReservationExpiredFeeApplicable{
177     all r:RentMade | r.reservationExpired = True iff (REF
        in r.additionalFeeRent and #r.additionalFeeRent = 1)

```

```

178   no r:RentMade | r.reservationExpired = False and REF
179       in r.additionalFeeRent
180   }
181   //A reservation expired could not be outside safe area
182   fact NoReservationExpiredOutsideSafeArea{
183       no r:RentMade | r.reservationExpired = True and r.
184           endSafeArea = False
185   }
186   //No discount are applicable if a reservation is expired
187   fact NoDiscountOrFeeIfReservationExpires{
188       all r:RentMade | r.reservationExpired = True implies r
189           .discountApplicableRent = none
190   }
191   //No passengers can be detected during the ride if the
192       reservation is expired
193   fact NoPassengersIfReservationExpires{
194       all r:RentMade | r.reservationExpired = True iff r.
195           passengersDuringTheRide = Zero
196   }
197   //M2P discount must be applied iff there are at least
198       two passengers detected during the ride
199   fact M1PDiscountApplicable{
200       all r:RentMade |( r.passengersDuringTheRide != Zero
201           and r.passengersDuringTheRide != One)
202           iff M1PD in r.discountApplicableRent
203   }
204   //BHF discount must be applied iff the car is left with
205       more than 50 percent of battery
206   //at the end of the rent
207   fact BHFDDiscountApplicable{
208       all r:RentMade | r.endBatteryLevel = More50Full
209           iff BHFD in r.discountApplicableRent
210   }
211   //CC discount must be applied iff the car is left on
212       charge at the end of the ride
213   fact CCDDiscountApplicable{
214       all r:RentMade | r.onChargeAtTheEnd = True
215           iff CCD in r.discountApplicableRent
216   }
217   //If a car is left on charge at the end of the ride it
218       is located inside a safe area
219   fact AllCharginStationInSafeArea{
220       all r:RentMade | r.onChargeAtTheEnd = True implies r.
221           endSafeArea = True
222   }

```

```

220 //If a car is left in the charge station determined by
    the MSO at the end of the
221 //ride, it is on charge at the end of the ride
222 fact IfLeftMSOStationIsOnCharge{
223     all r:RentMade | r.leftMSOstation = True implies r.
        onChargeAtTheEnd = True
224 }
225
226 //MSO discount must be applied iff the car is left in
    the charging station
227 //determined by the MSO
228 fact MSODiscountApplicable{
229     all r:RentMade | r.leftMSOstation = True iff MSOD in r
        .discountApplicableRent
230 }
231
232 //OSA fee must be applied iff the car is left outside a
    safe area at the end of the rent
233 fact OSAFeeMustBeAdded{
234     all r:RentMade | r.endSafeArea = False
235         iff OSAF in r.additionalFeeRent
236 }
237
238 //A3BC fee must be applied if the car is left more than
    3km away from the nearest
239 //charging station or with battery percentage lower than
    20 percent
240 fact A3BCFeeMustBeAdded{
241     all r:RentMade | r.endPosition = More3kmPowerGrid
242         implies A3BCF in r.additionalFeeRent
243     all r:RentMade | r.endBatteryLevel = Lower20Full
244         implies A3BCF in r.additionalFeeRent
245     all r:RentMade | A3BCF in r.additionalFeeRent
246         implies (r.endPosition = More3kmPowerGrid or r.
            endBatteryLevel = Lower20Full)
247 }
248
249 //A3BC fee cannot be applied if the car is left on
    charge
250 fact NoA3BCFeeIfOnCharge{
251     no r:RentMade | r.onChargeAtTheEnd = True and A3BCF
        in r.additionalFeeRent
252 }
253
254 //If CC discount is applied the end car position can not
    be more than 3km away
255 //from the nearest power grid
256 fact NoCCDMoreThan3km{
257     no r:RentMade | CCD in r.discountApplicableRent and r.
        endPosition = More3kmPowerGrid
258 }
259
260 // Assertions
261 //Can not exists reserved car with engine turned on

```

```

262 assert NoReservedCarWithEngineOn{
263   no c:Car | c.engineOn = True and c.status = Reserved
264 }
265 check NoReservedCarWithEngineOn
266
267 //Can not exists a car in charge with engine turned on
268 assert NoCarInChargeWithEngineOn{
269   no c:Car | c.engineOn = True and c.onCharge = True
270 }
271 check NoCarInChargeWithEngineOn
272
273 //If a car is left on charge at the end of the rent the
    outside safe area fee (OSAF)
274 //can not be applied because alla charging stations are
    inside a safe area
275 assert NoOSAFIfOnChargeAtTheEndRent{
276   no r:RentMade | r.onChargeAtTheEnd = True and OSAF
    in r.additionalFeeRent
277 }
278 check NoOSAFIfOnChargeAtTheEndRent
279
280 //If CCD is applied A3BCF can not be applicable and
    viceversa
281 assert NoCCDAndA3BCF{
282   no r:RentMade | CCD in r.discountApplicableRent and
    A3BCF in r.additionalFeeRent
283 }
284 check NoCCDAndA3BCF
285
286 //If CC discount is applied the end car position can not
    be more than 3km away
287 //from the nearest power grid
288 assert NoMSODMoreThan3km{
289   no r:RentMade | MSOD in r.discountApplicableRent and r
    .endPosition = More3kmPowerGrid
290 }
291 check NoMSODMoreThan3km
292
293 //If MSOD is applied A3BCF can not be applicable and
    viceversa
294 assert NoMSODAndA3BCF{
295   no r:RentMade | MSOD in r.discountApplicableRent and
    A3BCF in r.additionalFeeRent
296 }
297 check NoMSODAndA3BCF
298
299 pred show{#charging > 2 some u:LoggedUser | u.banned =
    True}
300 run show for 10 but exactly 2 ChargingStation, exactly 4
    Car, exactly 4 LoggedUser, exactly 2 RentMade

```



**7 commands were executed. The results are:**

#1: No counterexample found. NoReservedCarWithEngineOn may be valid.  
#2: No counterexample found. NoCarInChargeWithEngineOn may be valid.  
#3: No counterexample found. NoOSAFIfOnChargeAtTheEndRent may be valid.  
#4: No counterexample found. NoCCDAndA3BCF may be valid.  
#5: No counterexample found. NoMSODMoreThan3km may be valid.  
#6: No counterexample found. NoMSODAndA3BCF may be valid.  
#7: **Instance found.** show is consistent.

Figure 22: Alloy execution result

## A.2 Generated worlds

Note that in [Figure 23](#) `LoggedUser3` has been banned *after* completing `RentMade0`.

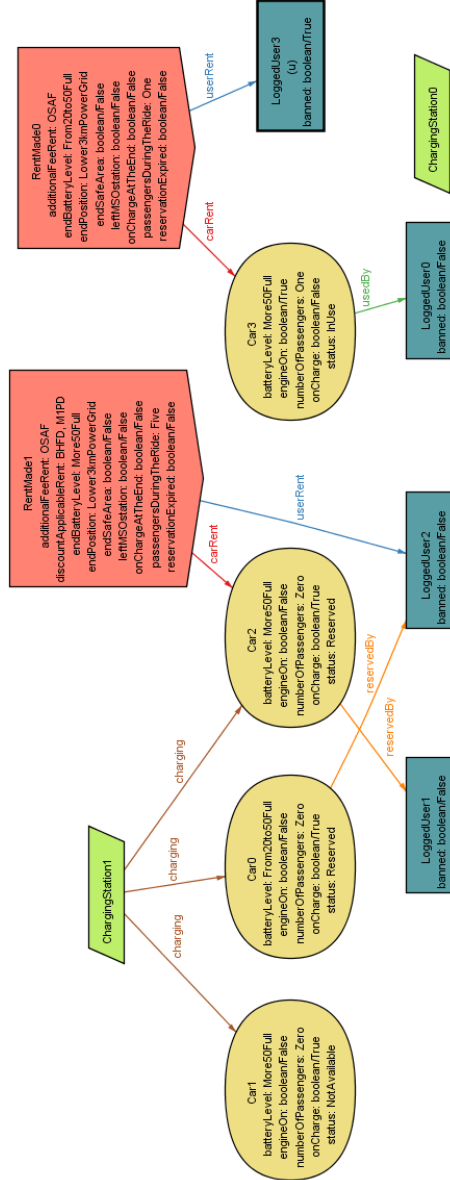


Figure 23: First alloy generated world

Note that in Figure 24 RentMade1 is actually a reservation expired of Car3 made by LoggedUser2. He now has reserved Car1.

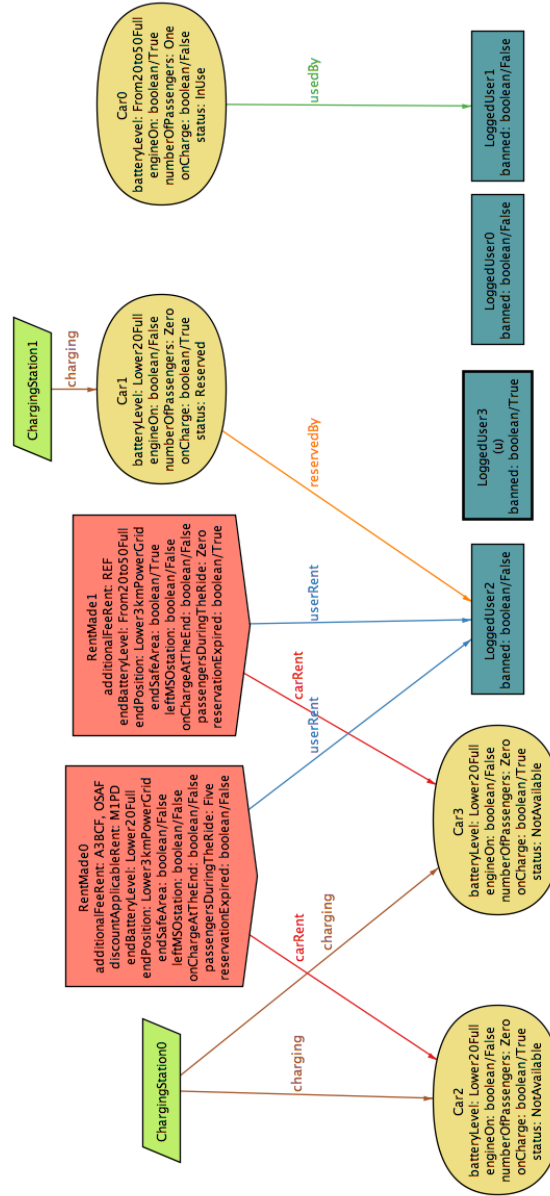


Figure 24: Second alloy generated world

## B Software and tools used

For the development of this document we used

- L<sup>A</sup>T<sub>E</sub>X as document preparation system
- GitHub as version control system
- Draw.io for graphs

## C Hours of Work

This is the amount of time spent to redact this document:

- **Section 1 - Introduction**
  - Amedeo Cavallo - 2 hours
  - Mattia Calabrese - 1 hour
  - Federico Capaccio - 1 hour

## D Changelog

- **v1.0** October 23, 2019
  - Initial RASD document structuring and redaction
  - Introduction (Purpose and Scope sections)

## References

- [1] B. Nuseibeh, S. Easterbrook, *Requirements Engineering: A Roadmap*, 2000
- [2] P. Zave, *Classification of Research Efforts in Requirements Engineering*, ACM Computing Surveys, 1997
- [3] E. Di Nitto, L. Mottola, *Software Engineering 2 Assignment*, AA 2019-2020
- [4] A. Stone, “Chain of custody: How to ensure digital evidence stands up in court,” September 2015
- [5] IEEE Std 830:1993, *IEEE Recommended Practice for Software Requirements Specifications*, 1993