



POLITECNICO DI MILANO

SOFTWARE ENGINEERING II PROJECT

**POWERENJOY**

---

# Requirements Analysis and Specifications Document

---

*Authors:*

Davide PIANTELLA  
Mario SCROCCA  
Moreno R. VENDRA

*Professor:*

Luca MOTTOLA

December 8, 2016

version 1.3

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Purpose of this document . . . . .	1
1.2	Actual system . . . . .	1
1.3	Scope . . . . .	1
1.3.1	Goals . . . . .	1
1.4	Glossary . . . . .	2
1.4.1	Definitions . . . . .	2
1.4.2	Acronyms . . . . .	3
1.4.3	Abbreviations . . . . .	3
1.5	Document overview . . . . .	3
<b>2</b>	<b>Overall description</b>	<b>5</b>
2.1	Product perspective . . . . .	5
2.1.1	System interfaces . . . . .	5
2.1.2	User interfaces . . . . .	7
2.1.3	Software interfaces . . . . .	7
2.2	User characteristics . . . . .	8
2.3	Domain assumption . . . . .	8
2.4	The World and the Machine . . . . .	9
<b>3</b>	<b>Specific Requirements</b>	<b>10</b>
3.1	Functional Requirements . . . . .	10
3.1.1	Goals . . . . .	10
3.2	Performance Requirements . . . . .	15
3.3	Software System Attributes . . . . .	15
3.3.1	Availability . . . . .	15
3.3.2	Security . . . . .	16
3.3.3	Portability . . . . .	16
<b>4</b>	<b>Use cases identification</b>	<b>17</b>
4.1	Scenarios . . . . .	17
4.1.1	Scenario 1 . . . . .	17
4.1.2	Scenario 2 . . . . .	17
4.1.3	Scenario 3 . . . . .	17
4.1.4	Scenario 4 . . . . .	17
4.1.5	Scenario 5 . . . . .	17
4.1.6	Scenario 6 . . . . .	18
4.2	Use case diagram . . . . .	19
4.3	Use cases description . . . . .	21
4.3.1	Registration . . . . .	21
4.3.2	Authentication . . . . .	23
4.3.3	View cars on the map . . . . .	25
4.3.4	Car reservation . . . . .	27
4.3.5	Car unlock . . . . .	28
4.3.6	Car rent . . . . .	30
4.3.7	Rent payment . . . . .	33
4.3.8	Money saving option . . . . .	36
4.3.9	Visualization of not available cars . . . . .	38

4.3.10	Tag a car as available . . . . .	40
4.3.11	Visualization of users information . . . . .	42
4.3.12	View users payments and rents history . . . . .	43
4.3.13	Mark or unmark a user as banned . . . . .	44
4.3.14	Tag a car as not available . . . . .	45
4.4	UML class diagram . . . . .	47
<b>Appendices</b>		<b>48</b>
<b>A Alloy model</b>		<b>48</b>
A.1	Source code . . . . .	48
A.2	Generated worlds . . . . .	56
<b>B Software and tools used</b>		<b>58</b>
<b>C Hours of work</b>		<b>58</b>
<b>D Changelog</b>		<b>58</b>

## List of Figures

1	Overview of system interfaces . . . . .	5
2	The World and the Machine . . . . .	9
3	Use case diagram . . . . .	19
4	<i>Registration</i> sequence diagram . . . . .	22
5	<i>Authentication</i> sequence diagram . . . . .	24
6	<i>View cars on the map</i> sequence diagram . . . . .	26
7	<i>Car unlock</i> sequence diagram . . . . .	29
8	<i>Car rent</i> sequence diagram . . . . .	31
9	<i>One Euro fee</i> sequence diagram . . . . .	31
10	Car status FSM . . . . .	32
11	<i>Rent payment</i> sequence diagram . . . . .	35
12	<i>Money saving option</i> sequence diagram . . . . .	37
13	<i>Visualization of not available cars</i> sequence diagram . . . . .	39
14	<i>Tag a car as available</i> sequence diagram . . . . .	41
15	<i>Tag a car as Not Available</i> sequence diagram . . . . .	46
16	UML class diagram . . . . .	47
17	Alloy execution result . . . . .	55
18	First alloy generated world . . . . .	56
19	Second alloy generated world . . . . .	57

## List of Tables

1	<i>Registration</i> use case description . . . . .	22
2	<i>Authentication</i> use case description . . . . .	23
3	<i>View cars on the map</i> use case description . . . . .	25
4	<i>Car reservation</i> use case description . . . . .	27
5	<i>Car unlock</i> use case description . . . . .	28
6	<i>Car rent</i> use case description . . . . .	30

7	<i>Rent payment</i> use case description . . . . .	34
8	<i>Money saving option</i> use case description . . . . .	36
9	<i>Visualization of not available cars</i> use case description . . . . .	38
10	<i>Tag a car as not available</i> use case description . . . . .	40
11	<i>Visualization of users information</i> use case description . . . . .	42
12	<i>View users payments and rents history</i> use case description . . . . .	43
13	<i>Mark or unmark a user as banned</i> use case description . . . . .	44
14	<i>Tag a car as not available</i> use case description . . . . .	45

# 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 behavior, and to their evolution over time and across software families.[2]

## 1.2 Actual system

The system we are to develop is brand new, there is no previous system.

## 1.3 Scope

PowerEnJoy is a car-sharing service that exclusively employs electric cars; we are going to develop a web-based software system that will provide the functionalities normally provided by car-sharing services, such as allowing the user to register to the system in order to access it, showing the cars available near a given location and allowing a user to reserve a car before picking it up. A screen located inside the car will show in real time the ride amount of money to the user. When the user reaches a predefined safe area and exits the car, the system will stop charging the user and will lock the car. The system will provide information about charging station location where the car can be plugged after the ride and incentivize virtuous behaviours of the users with discounts.[3]

### 1.3.1 Goals

- G1** Allow guest users to register to the system
- G2** Allow registered users to authenticate to the system
- G3** Provide logged users with the position of available cars
- G4** Notify maintenance service with a list of not available cars
- G5** Provide the maintenance service with a way to notify the system when a car is available again
- G6** Provide users with a way to report a damaged car
- G7** Provide a way to show to each user his rents and payments history
- G8** Provide customer service with a way to ban registered users in order to prevent them from reserving or using other cars, and enable them to use the service again
- G9** Allow a logged user to reserve a car, if available, and hold that reservation for an hour

- G10** Charge a user for 1€ in case he hasn't used the car he reserved after an hour from such reservation
- G11** Allow a logged user to perform a complete rent: reserving a car, using it and leaving it terminating the rent, accomplishing the payment procedure related to aforementioned rent
- G12** Calculate and charge the user for the correct amount of money he has to pay for his last ride, also considering the various discounts and fees applicable based on the ride
- G13** Allow a logged user to enable a money saving option which provides him with a charging station as destination of the ride to get a discount on the cost of the aforementioned ride

## 1.4 Glossary

### 1.4.1 Definitions

**System:** the PowerEnJoy software we are to develop

**Company:** the company we are developing the system for

**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

**Banned user:** a user that can not use the system, he can only contact the customer care service

**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

**Car:** an electric car owned by the company

**Available car:** the car can be reserved by a user

**Reserved car:** the car has been reserved by a user

**In use car:** a car is becomes in use when a user ignites the engine and stops being in use at the end of the rent

**Not available car:** the car can not be reserved by a user, a maintenance operator will deal with it

**Battery level critical:** battery level under 20%

**Charging station:** location where cars owned by the company can be charged using a provided plug

**Safe area:** area of the map where a rent can be terminated without the corresponding additional fee

**Payment procedure:** process which realizes the monetary transaction between the user and the system

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

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

**Base cost:** Ride cost calculated proportionally to the rent time

**Rent time:** Time period starting from the moment the engine was turned on, until the car is locked

#### 1.4.2 Acronyms

**RASD:** Requirements Analysis and Specification Document

**API:** Application Programming Interface

**GPS:** Global Position System

**DBMS:** Data Base Management System

**FSM:** Finite-State Machine

**GIS:** Geographic Information System

#### 1.4.3 Abbreviations

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

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

**i.d.:** id est

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

**e.g.:** exempli gratia

**etc.:** et cetera

### 1.5 Document overview

According to the IEEE standard [4], this document is structured as

1. **Introduction:** it provides an overview of this 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 system's functional and non-functional requirements

4. **Use cases identification:** it contains the usage scenarios of the system with the use case diagram, use cases descriptions and other diagrams
5. **Appendices:** it contains the Alloy model, software and tools used, hours of work per each team member



## 2 Overall description

### 2.1 Product perspective

#### 2.1.1 System interfaces

The system we are to develop will have some external interfaces (represented in [Figure 1](#)) to accomplish the [goals stated before](#).

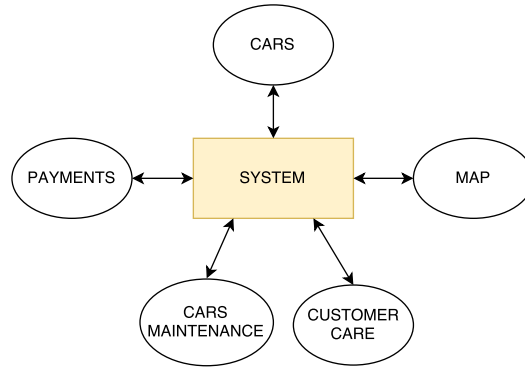


Figure 1: Overview of system interfaces

**Payments** When a payment is required (e.g. when a user ends his rent) the system sends a request with all the details needed to complete the payment (i.d. name and surname of the user, due amount, credit card number etc.) to an external payment handling system. Once the external system completes the payment process, it sends our system the payment outcome so that the system can take appropriate action.

**Customer care** Every time it is required, a PowerEnJoy customer care service operator can interact with a user. Customer care service operators can request and see all user details, their rents and payments history. Such operators can also mark or unmark users as banned from the system, mark cars as not available and, in general, provide assistance to users.

**Maintenance** The system will interact with a preexisting car maintenance service which already deals with other car sharing services. Our system will expose to the maintenance service a real time list of all the cars tagged as *not available* via a *restricted access API* which will also provides their GPS position and a brief description of their problems. The maintenance service takes care of reaching those cars, unlocks the doors, fixes the fault, locks the doors back and finally tags them as *available* using the aforementioned API provided by the system. See [cars section](#) for more details.

**Map** GPS position of cars and safe areas is displayed to all users, customer care operators and maintenance operators on a constantly updated map which relies on an external GIS.

**Cars** All cars provided by the customer are equipped with a communication system which ensures a continuous protected communication between the car and the system. All cars also have a module which provides a set of primitives that allow the system to retrieve information and to run commands to take actions on the car. A built-in user interface embedded with the modules shows some relevant information to the user.

Information retrieved by the system from the car include:

- unique car identifier
- GPS position
- engine status (on, off)
- current number of passengers
- maximum number of passengers
- battery level (percentage)
- charging status (in charge, not in charge)
- door locking status (locked, unlocked)
- door closing status (open, closed)

For each of these information the car provides a primitive to instantiate a listener which triggers a notification to the system whenever the observed parameter changes.

Information sent to the car by the system include:

- location of safe areas
- position of charging stations
- current time
- rent cost per hour

Commands runnable by the system include:

- lock doors
- unlock doors
- start rent timer

Information shown to the user by the embedded car interface include:

- current car position (also w.r.t. safe areas and charging stations)
- number of passengers
- battery level (percentage)
- current time

- rent time
- amount owed until now (based upon rent cost per hour)

This system provides, among other functionalities, a secure way to unlock and lock the doors of the car: it has a command which returns a software key which can be sent to the maintenance operators; they are able to unlock and lock the car with a smartphone client of the car's embedded system and the key.

In order to determine which cars are in charge in which charging station the system checks if the charging status of a car is set to *true* and its position is within a small distance from the charging station position.

The maximum number of passengers represents the maximum number of passengers that were detected by the car during its last ride (defined as the last period from engine on to engine off).

### 2.1.2 User interfaces

Using the interfaces of the system users can:

1. Register and log-in to the system
2. On the map they can view the position of
  - a) themselves
  - b) safe areas
  - c) available cars (with their current battery level)
  - d) charging stations
3. Reserve a car
4. View customer care contacts
5. Unlock the reserved car
6. View and edit personal information
7. View rents and payments history

### 2.1.3 Software interfaces

Databases and DBMSs are clearly required in order to store data about users, cars, charging stations, safe areas etc.

As mentioned before (see [system interfaces section](#)) the system needs to use external APIs and to expose interfaces in order to interact with other systems.

All vehicles have an embedded external software system, which is able to display all information described in [cars section](#).

## 2.2 User characteristics

Users can use our system when they want to rent a car.

Necessary conditions for the user in order to use the system are:

- He must have a smartphone and be able to use it
- He must be in the age of majority
- He must have a proper valid driving license
- He must be able to drive a car (i.d. he must be in both physical and mental health)

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

## 2.3 Domain assumption

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

- DA1** GPS position is supposed to be accurate (max error  $\pm 5m$ )
- DA2** GPS position of all cars is always obtainable
- DA3** The user who reserves the car will always be the person who drives it
- DA4** Users are legally allowed to drive cars (i.d. users have a proper driving license)
- DA5** Charging stations are always working correctly
- DA6** All information provided by users are correct and reliable
- DA7** All cars provided by the customer are equipped with a module which provides a set of primitives that allow the system to retrieve all the information it needs about the car and to run commands which allow the system to take actions on the car (see [cars section](#) for more details)
- DA8** Charging station can exclusively be used by PowerEnJoy cars
- DA9** The set of safe areas is pre-defined and is provided to our system by the customer
- DA10** The position of charging station is provided to our system by the customer
- DA11** All charging station are located inside safe areas
- DA12** The maps provided by the GIS are always up to date
- DA13** The commands sent to cars by the system are always executed correctly
- DA14** Information provided by the car are always correct and reliable
- DA15** Position of the user is always available when he uses our system
- DA16** Even if the car is left with no battery left, it is still able to communicate with the system

## 2.4 The World and the Machine

The world and the machine is a way of thinking about problems and phenomena relevant in the reality of the software system we are to develop. The world contains the phenomena that happens in reality but are not observable by our system; the machine instead contains the phenomena which take place inside the system and are not observable from outside of it. The intersection between these two sets of phenomena is the so called set of shared phenomena, which contains the phenomena that are controlled by the world and observed by the machine or controlled by the machine and observed by the world.

Goals are prescriptive assertions formulated in terms of world phenomena (not necessarily shared); domain properties/assumptions are descriptive assertions assumed to hold in the world; requirements are prescriptive assertions formulated in terms of shared phenomena.[5]

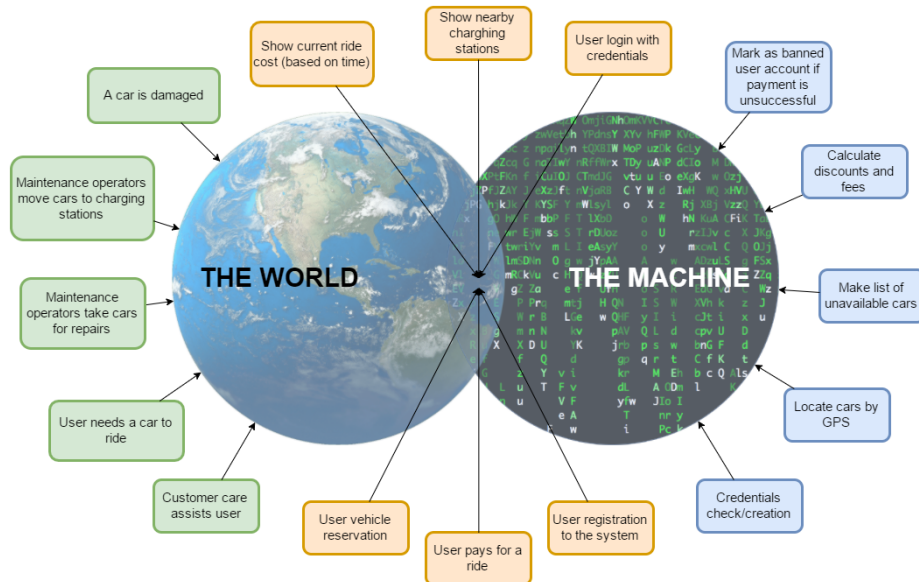


Figure 2: The World and the Machine

## 3 Specific Requirements

### 3.1 Functional Requirements

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

#### 3.1.1 Goals

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

- R1** The system must require the *guest* user to insert a username to identify him
- R2** The system must check that the username inserted by the *guest* user doesn't belong to another user already registered to the system
- R3** At the end of the registration phase the system must provide the *guest* user with a password bound to the username inserted by the *guest* user that can be used to access the system
- R4** The system must require the *guest* user to provide his driving license ID code during the registration phase
- R5** The system must check that the driving license ID inserted by the *guest* user doesn't belong to another user already registered to the system
- R6** The system must require the *guest* user to provide payment information during the registration phase
- R7** The system must require the *guest* user to provide an email address during the registration phase
- R8** The system must check that the email inserted by the *guest* user doesn't belong to another user already registered to the system
- R9** The system must check that the email inserted by the *guest* user exists and belongs to him
- R10** The system must require the *guest* user to insert his name, surname, birth date and place and current domicile in the registration phase
- R11** The system offers an interface to allow the user to modify or update his anagraphical information, payment information, driving license information, email and password (username can't be changed)

**G2** Allow registered users to authenticate to the system

- R12** The system must require the user to insert his username and password to authenticate to the system
- R13** The system must be able to check if the username and password pair correspond to a user correctly registered to the system
- R14** The system must allow access to a user if username and password inserted corresponds to a user correctly registered to the system and if the user has confirmed his own email address
- R15** The system must allow access to the services provided by the system only to authenticated users

**G3** Provide logged users with the position of available cars

- R16** The system must be able to identify each car unambiguously
- R17** The system must be able to retrieve the current position of each car
- R18** At each time the system must pair a car with one and only one state; possible states are *Available*, *Not Available*, *Reserved*, *In Use*
- R19** The system must be aware the current state of each car
- R20** The system must be able to know the exact amount of time the car has been in the current state
- R21** The system must be able to show a map with the position of *Available* cars
- R22** The system must be able to identify the position of the user and show it on a map
- R23** The system must be able to identify a position inserted by the user and show it on the map
- R24** The system must be able to calculate the distance of each car from a given position

**G4** Notify maintenance service with a list of not available cars

- R25** The system must be able to retrieve the current battery level of each car
- R26** If the state of a specific car is set to *Not Available* the system must prevent users from reserving or renting the aforementioned car
- R27** If the state of a specific car is set to *Not Available*, the car state must be paired with a brief description of why the car is not available
- R28** The system must set the state of a car from *Available* to *Not Available* if battery level is critical and the car is not on charge, stating that reason as description
- R29** The system must offer a restricted access API to retrieve the list of cars marked as *Not Available* along with the identifier used by the system to identify each car, the description of the problem paired with the current position of each car (*GPS coordinates*) and a software key to access each car

**G5** Provide the maintenance service with a way to notify the system when a car is available again

- R30** The system must be able to set a specific car state to *Available* in order to allow users to reserve and rent the aforementioned car
- R31** The system must offer a restricted access API to set the state of a specific car as *Available*
- R32** The system must be able to know if a specific car is locked or unlocked
- R33** When the system receives a request to set the state of a car to *Available* through the API, before processing the request the system must check that the car is locked and its state is set to *Not Available*

**G6** Provide users with a way to report a damaged car

**R34** The system must provide information about how to contact customer care service

**R35** The system must allow the customer service to set the state of a specific car to *Not Available*

**G7** Provide a way to show to each user his rents and payments history

**R36** The system must log an history of all rents and payments

**R37** User's rents history must include expired reservations in which the rent was not completed

**R38** Each record in the payment history of a user, which refers to a ride, must include the ride cost and the discounts or additional fees applied

**R39** User's payment history must include not completed payment procedures

**R40** The system must be able to show to the user his own history of rents and payments

**G8** Provide customer service with a way to ban registered users in order to prevent them from reserving or using other cars, and enable them to use the service again

**R41** The system must be able to mark and unmark a user as *banned*

**R42** The system must require a brief description of the reasons why the user is being marked as *banned*

**R43** The system must not allow a *banned* user to access the system but only provide him information about how to contact customer service

**R44** The system must allow customer service to access users' information (name, surname, birth date and place, current domicile, driving license information) eventually along with information about the car state the user is actually paired with

**R45** The system must allow customer service to access users' rents and payments histories

**R46** The system must allow the customer service to set the state of a specific user to *banned* or *not banned*

**G9** Allow a logged user to reserve a car, if available, and hold that reservation for an hour

**R47** The system must allow a user to select a specific car in order to reserve it (i.f.f its current state is *Available*), and set to *Reserved* the state of the aforementioned car

**R48** At each time a user can be paired with one single state of one single car

**R49** When the state of a specific car is set to *Reserved*, the car must be uniquely paired with the user who made the reservation for the aforementioned car, for the duration of the reservation



- R50** A car set to *Reserved* remains in this state exactly one hour after the user made the reservation, if the user doesn't pick it up before; after that time the reservation expires and the system must set the state of the aforementioned car to *Available*
- G10** Charge the user for 1€ in case he hasn't used the car he reserved after an hour from such reservation
- R51** The system must be able to carry out a payment procedure based on payment information provided by the user and on a specific amount of money
- R52** The system must be able to know if a payment procedure is successful or unsuccessful
- R53** The system must ban a user (set to *banned* user) if a payment procedure was unsuccessful and notify him that he has to contact customer service
- R54** The system must charge the user 1€ (through a payment procedure) if he reserved a car and the state *Reserved* of that car was paired with the aforementioned user for more than one hour and notify the user the reservation has expired
- G11** Allow a logged user to perform a complete rent: reserving a car, using it and leaving it terminating the rent, concluding successfully the payment procedure related to the aforementioned rent
- R55** The system must be able to lock and unlock each car
- R56** The system must be able to know the current engine state of each car (*on* or *off*)
- R57** The system must be able to know the current percentage of battery of each car
- R58** The system must be able to compute the distance between the GPS position of the user paired with the *Reserved* state of the car and the GPS position of the aforementioned car
- R59** The system must allow the user to ask for the unlocking of the car of the which *Reserved* state he is paired with
- R60** The system must unlock a car reserved by a user if the distance between the user's GPS position and the car GPS position is less than 5m and the user asks to the system to unlock the car
- R61** When the state of a specific car is set to *In Use*, the car must be uniquely paired with the user who is using the car
- R62** The system can set the state of a *Reserved* car to *In Use* i.f.f. the user paired with the *Reserved* state of the car has unlocked the car and he has ignited the car engine
- R63** The system must lock a car if no passengers are detected in the car, the car engine is *off* and the doors are closed
- R64** When locking an *In Use* car, the system must be able to activate a timer; only when that timer expires the system must calculate the cost of the last ride performed by the car and charge the user (through a payment procedure) of the calculated amount

- R65** When the timer that was activated while locking an *In Use* car expires the system must set the state of the aforementioned car from *In Use* to *Available*
- R66** The system must calculate the base cost of a ride proportionally to the time the car has been used by the aforementioned user (paired as *In Use* with the user)
- R67** When a car is set to *In Use* in every moment the system must show the current cost via the car display (to be payed by the user paired with the *In Use* state of the aforementioned car)
- R68** The system must be able to identify if a given position is or not inside the sets of safe areas
- R69** The system must be able to send to cars the sets of safe areas
- R70** The system must be able to know the position of all charging stations
- R71** The system must be able to send to cars the position of charging stations
- R72** When a user is paired with a car which is *In Use* in every moment the system must show him, via the car display, if the aforementioned car position is or isn't inside a safe area
- R73** The system must be able to know if a car is plugged in a specific charging station (see [cars section](#) for more details)
- G12** Calculate and charge the user for the correct amount of money he has to pay for his last ride, also considering the various discounts and fees applicable based on the ride
- R74** The system must not cumulate the discounts but must apply only the one with the highest percentage, calculated on the base cost
- R75** All applicable percentage based fees are calculated by the system on the base cost of the ride and then summed to obtain the total fee the system must add to the base cost
- R76** The system must be able to know how many passengers are detected on a car during a ride
- R77** If locking an *In Use* car the system detects that the car position is not inside a safe area, the system must charge the user paired with the *In Use* state of the aforementioned car for the cost of the ride plus an additional fee; that fee is composed by a fixed amount plus a variable amount proportional to the distance of the car from the nearest safe area
- R78** If a car is located outside of set of safe areas and its state is not *In Use* the system must set the car state to *Not Available* stating that reason as description
- R79** If during the time a car is set as *In Use* the system detects more than one passengers into the car, the system must apply to the user paired with the *In Use* state of the aforementioned car a discount of 10% of the cost of the last ride

- R80** If locking a *In Use* car the system detects a level of battery of the aforementioned car greater than 50%, the system must apply to the user paired with the *In Use* state of the aforementioned car a discount of 20% of the cost of the last ride
- R81** When the timer activated locking a *In Use* car expires if the system detects the car as plugged into the power grid of a charging station, the system must apply to the user paired with the *In Use* state of the aforementioned car a discount of 30% of the cost of the last ride
- R82** When the timer activated locking a *In Use* car expires if the system detects the car position is more than 3 KM away from the nearest charging station or the system detects a critical level of battery of the aforementioned car and the battery is not on charge, the system must charge to the user paired with the *In Use* state of the aforementioned car the 30% more on the last ride.
- G13** Allow a logged user to enable a money saving option which provides him with a charging station as destination of the ride to get a discount on the cost of the aforementioned ride
- R83** The system must know the total number of plugs for each charging station
- R84** The system must allow the user to enable the *money saving option*
- R85** If the *money saving option* is enabled the system must allow the user to insert his final destination and provide him information about a station where to leave the car to get a discount
- R86** The system must be able to determine the station suggested to the user by the *money saving option* in order to ensure a uniform distribution of cars in the city
- R87** The system must be able to determine the station suggested to the user by the *money saving option* taking into account the destination of the user and the availability of power plugs at the selected charging station
- R88** When the timer activated locking a *In Use* car expires if the system detects the car as plugged into the power grid of the charging station determined by the *money saving option* the system must apply to the user paired with the *In Use* state of the aforementioned car a discount on the cost of the current ride

## 3.2 Performance Requirements

The system should always respond to each interaction in at most 5 seconds. The system performances must scale w.r.t. the number of cars.

## 3.3 Software System Attributes

### 3.3.1 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.

**3.3.2 Security**

Users personal information and payment information are encrypted and must be protected during transmission. Restricted access APIs must check that who tries to use them is actually allowed to do so.

**3.3.3 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

Francesco wants to have a beer with his friend Vincenzo so Francesco logs in to system and searches for cars nearby. He notices that there are two cars available next to his house, he decides to reserve the one with more battery and after few minutes he reaches it. He starts to drive until he reaches Vincenzo's house, Vincenzo gets into the car and they arrive to the beer house where they terminate the rent.

#### 4.1.2 Scenario 2

Mirjana has been told by her friend Elisa that a new car sharing service is available in their city and so she decided to give it a try as she wants to go shopping in the city center. She registers to the system providing all information requested, she inserts the destination address and enables the money saving option. She is provided by the system with a charging station not far from the shopping center and, as it is a sunny day, she decided to take that location as destination in order to achieve a discount and reach the shopping center on foot.

#### 4.1.3 Scenario 3

Giovanni is really interested in electric cars so he decides to use the PowerEnJoy system. He wants to go to the museum in the afternoon so he reserves a car. After one hour he is notified by the system that his reservation is expired and he is charged of a 1€ fee. When he is ready to exit his house he notices that the same car is still available so he reserves it again, reaches it and starts driving. When he arrives at the destination he sees a charging station next to the museum so he decides to leave the car there plugging the charging cable in order to get a discount.

#### 4.1.4 Scenario 4

Dino reserves a car, he reaches it and unlock the doors. He starts driving but after few minutes the engine stops and a warning icon lights up in the dashboard. He contacts the customer care service that suggests him to reserve a different car which is nearby, the customer care operator then tags the first car as not available specifying a brief description of the fault. The maintenance service is now aware of the problem and they take care of resolving the issue: a maintenance operator is sent to the car, he unlocks it and fixes it. When the car is fully functional he tags it as available using a restricted access API of our system.

#### 4.1.5 Scenario 5

Stefania often uses PowerEnJoy service when she is coming back home after work. Before finish her work schedule she checks with the map if there are cars

nearby in order to reserve one of them: today she can see one from the window that is not present in the map because its battery is empty. After a while she checks again the map and she notices that the car is now located in a charging station nearby and it is available for a reservation.

#### 4.1.6 Scenario 6

Lorenzo is driving a PowerEnJoy car in order to reach Dino's house outside the safe area. As soon as he exists the safe area the car system notifies him with a message. When he is arrived he terminates the rent, the payment is executed with an extra fee and the car is tagged as not available.

## 4.2 Use case diagram

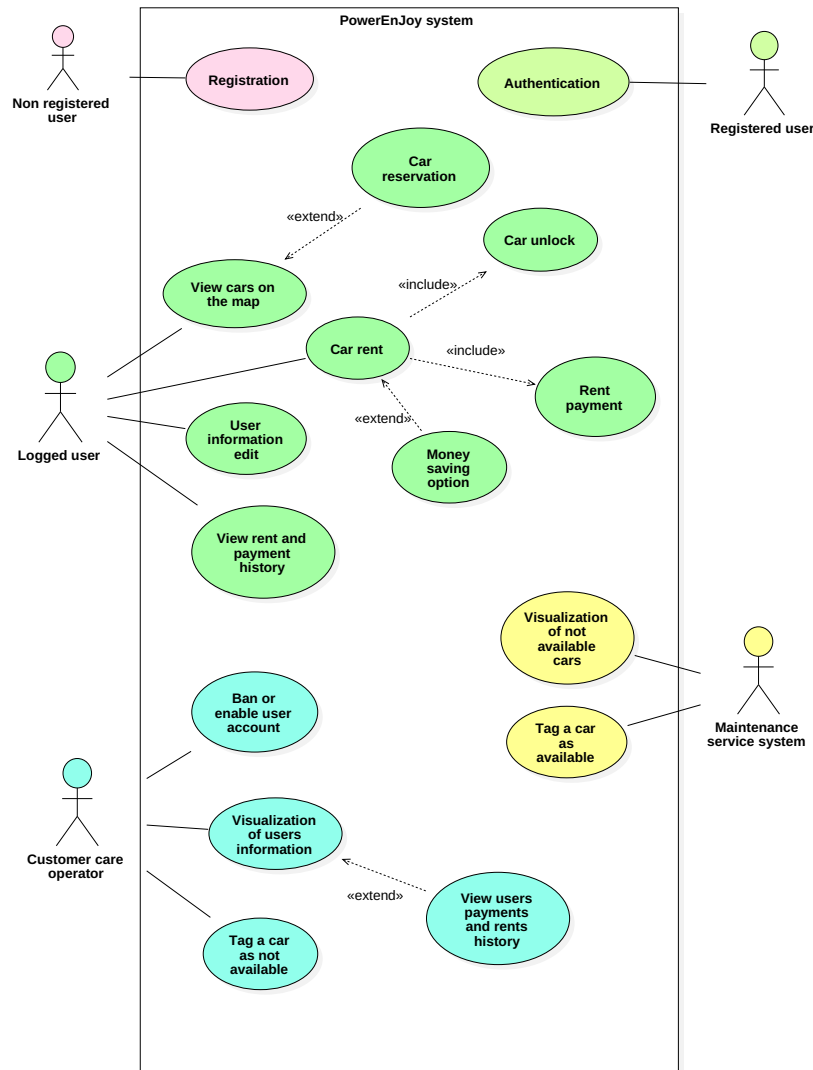


Figure 3: Use case diagram

**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

<b>Name</b>	<b>Registration</b>
<b>Actors</b>	Non registered user
<b>Entry conditions</b>	
<b>Flow of events</b>	<ol style="list-style-type: none"> <li>1. The user asks the system to register to its services</li> <li>2. The system shows the appropriate form to fill to register to the system</li> <li>3. The user inserts an username to be uniquely identified by the system</li> <li>4. The user inserts his own email address</li> <li>5. The user inserts his name, surname, birth date and place and current domicile</li> <li>6. The user inserts his driving license ID code</li> <li>7. The user inserts payment information</li> <li>8. The user confirms data inserted are correct e submit the form</li> <li>9. The system checks the username to be unique</li> <li>10. The system checks the email to be unique</li> <li>11. The system checks the driving license ID to be unique</li> <li>12. 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>13. The user clicking on the link received confirms his email address</li> <li>14. 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> </ol>
<b>Exit conditions</b>	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

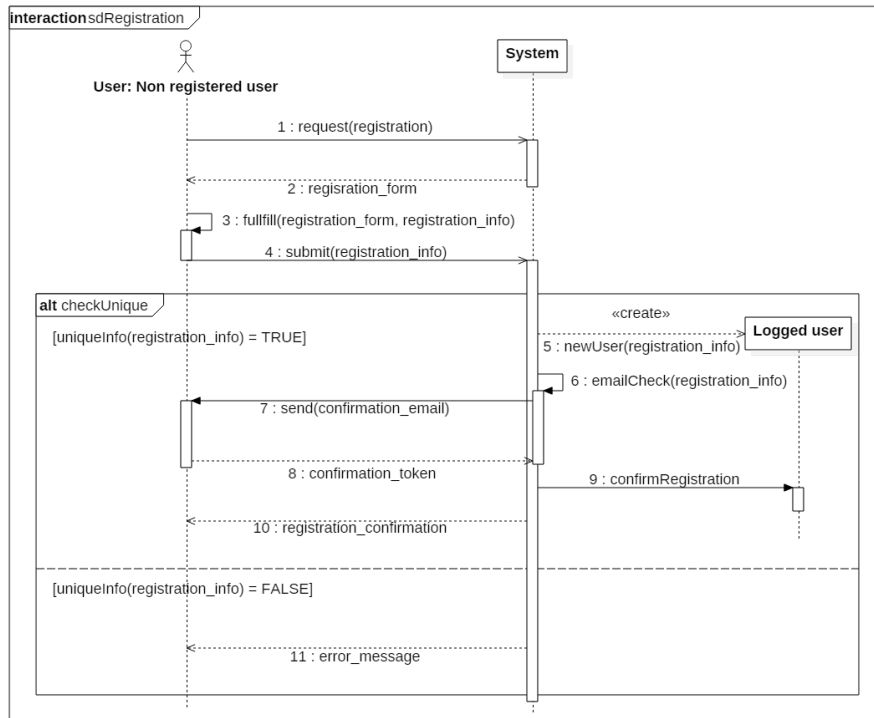
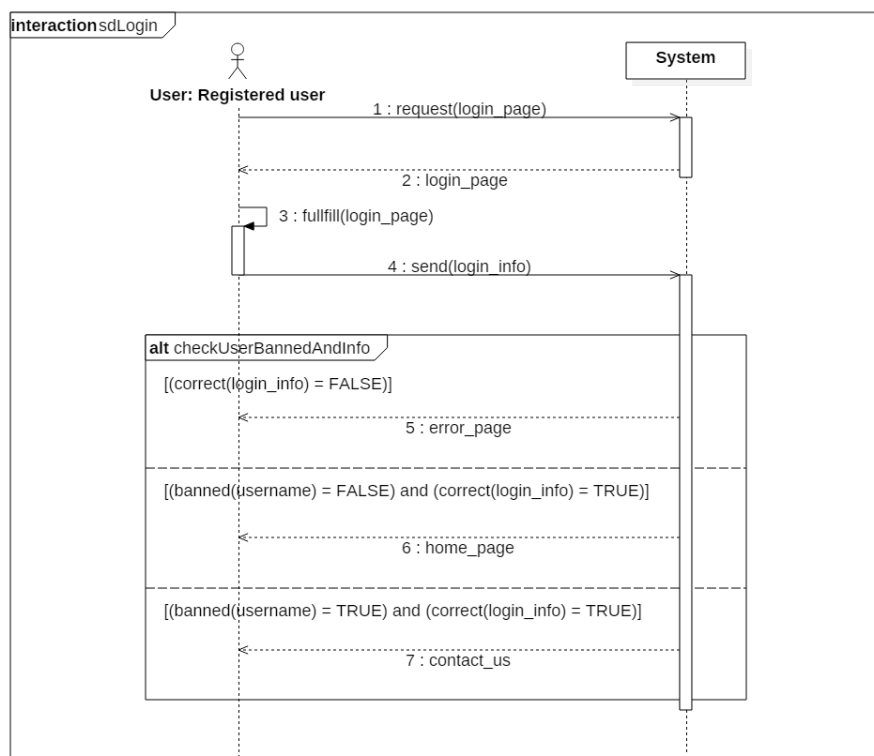


Figure 4: *Registration* sequence diagram

## 4.3.2 Authentication

<b>Name</b>	<b>Authentication</b>
<b>Actors</b>	Registered user
<b>Entry conditions</b>	The user must know his username and password
<b>Flow of events</b>	<ol style="list-style-type: none"> <li>1. The user inserts his username and password in the appropriate form and submit it</li> <li>2. The system validates the inserted credentials checking also if the user has confirmed his own email address</li> <li>3. The system checks if the user is banned</li> </ol>
<b>Exit conditions</b>	If the credential validation is successful and the user is not banned he is granted the proper privileges
<b>Exceptions</b>	<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>

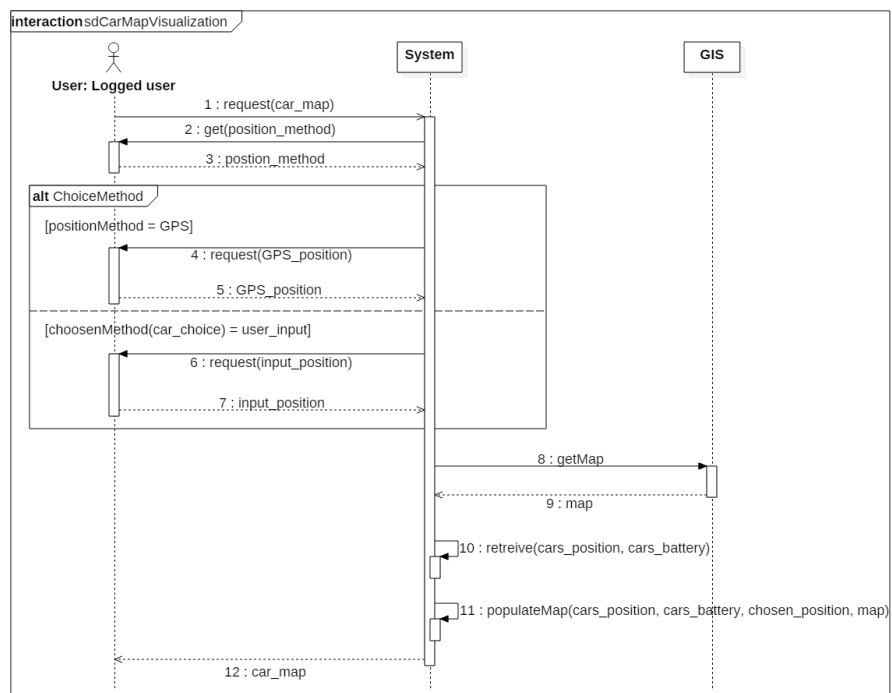
Table 2: *Authentication* use case description

Figure 5: *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>	<ol style="list-style-type: none"> <li>1. The user chooses if he wants to use his GPS position or insert a different one manually <ol style="list-style-type: none"> <li>a. The system retrieves the user's GPS position</li> <li>b. The user inserts a position</li> </ol> </li> <li>2. The system retrieves the position of all <i>Available</i> cars and their battery level percentage</li> <li>3. The system shows a map with all available cars near the position indicated by the user</li> <li>4. The user can click on a car on the map to see its battery level percentage</li> </ol>
<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 6: *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>	<ol style="list-style-type: none"> <li><b>1. View cars on the map</b></li> <li>The user selects the car he wants to reserve</li> <li>The user confirms he wants to reserve that car</li> </ol>
<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>	<ol style="list-style-type: none"> <li>1. The user asks the system to unlock the car he reserved</li> <li>2. The system checks if the user's position is at most 5 meters away from the position of the car he reserved</li> <li>3. The system unlocks the car with the state set as <i>Reserved</i> paired with the aforementioned user</li> <li>4. The system sends a message to the user, confirming that the car is unlocked</li> </ol>
<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



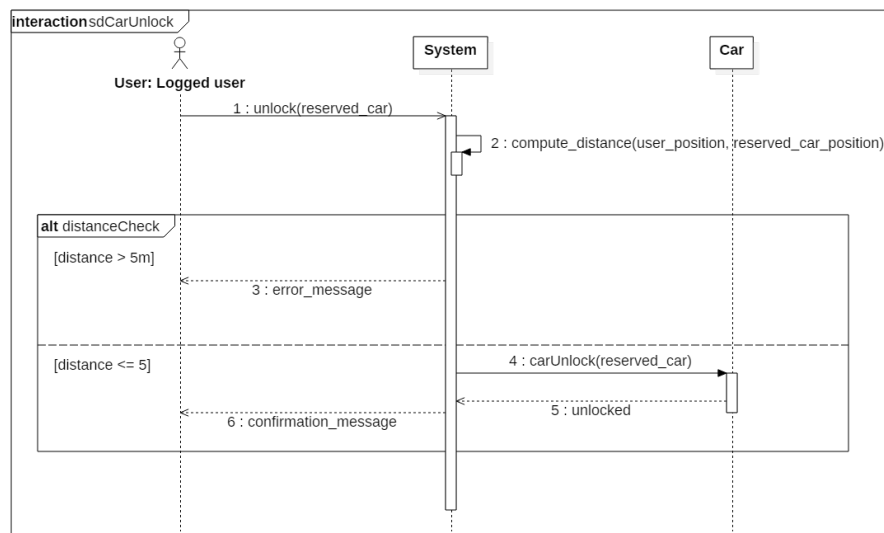
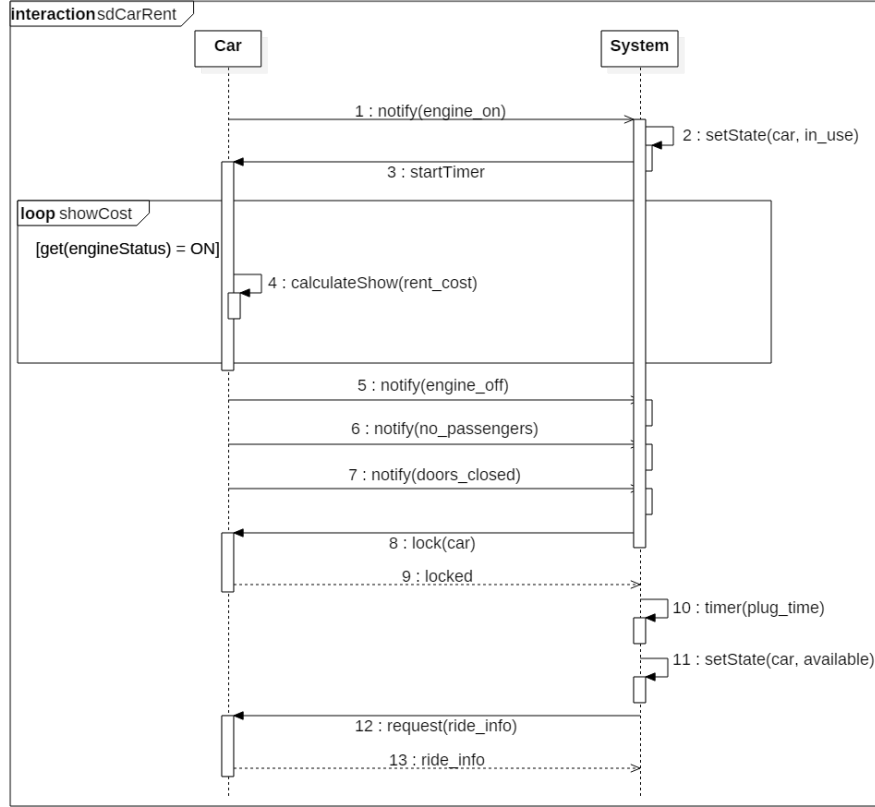
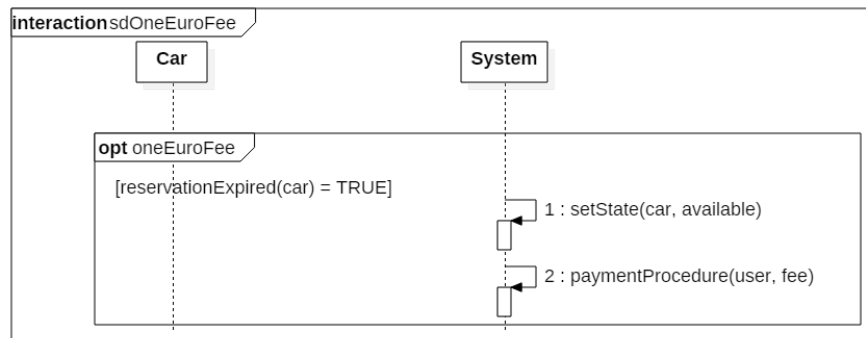


Figure 7: Car unlock sequence diagram

## 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>	<ol style="list-style-type: none"> <li>1. <b>Car unlock</b></li> <li>2. The user ignites the car engine</li> <li>3. The system sets the state of the <i>Reserved</i> car to <i>In Use</i> paired with the same user</li> <li>4. During the rent the user is informed about the current charge and whether he is or not inside a safe area</li> <li>5. The user leaves the car turning off the engine and closing the doors</li> <li>6. The system locks the car</li> <li>7. The system activates a timer to allow the user to plug the car into a charging station if it is near one of them</li> <li>8. When the timer expires: <ol style="list-style-type: none"> <li>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</li> <li>8.2 The system sets the car as <i>Available</i></li> </ol> </li> <li>9. <b>Rent payment</b></li> </ol>
<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 8: *Car rent* sequence diagramFigure 9: *One Euro fee* sequence diagram

The overall status of a car can be represented by the FSM in [Figure 10](#)

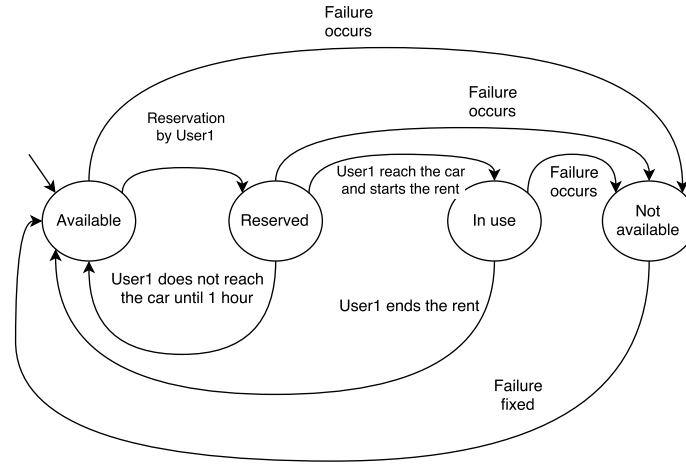


Figure 10: Car status FSM

**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 [R28](#)).

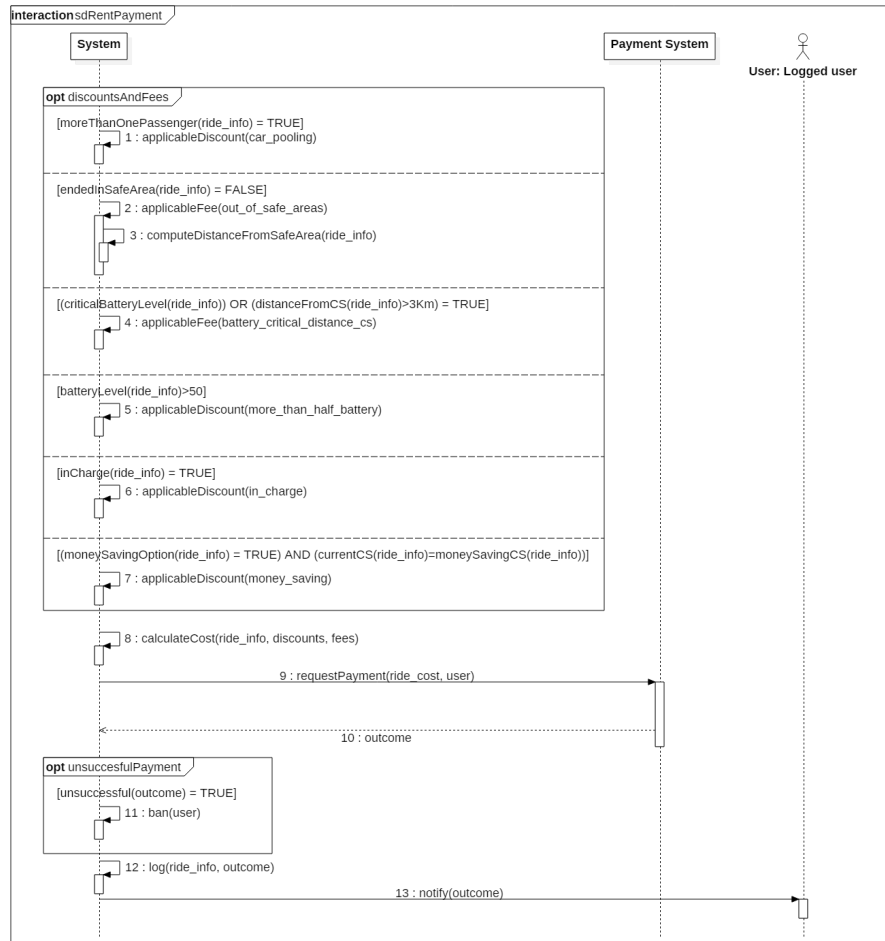
Even if the car is left with no battery left, it is still able to communicate with the system, so the rent can end normally and the maintenance service will take care the car (see [DA16](#)).

**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>	<ol style="list-style-type: none"> <li>1. The system checks if the car position is or is not inside a safe area</li> <li>2. The system checks if the car has detected more than one passenger during the rent</li> <li>3. The system checks the car battery percentage</li> <li>4. The system checks if the car is plugged on a charging station</li> <li>5. The system checks the distance of the car from the nearest charging station</li> <li>6. The system calculates the cost of the ride based on the rent time</li> <li>7. The system determines the applicable discounts/extra fee applying it to the cost of the ride</li> <li>8. The system starts a payment procedure with user's payment information using an external service</li> <li>9. The system waits a response from the external payment service</li> <li>10. The system logs data about the rent and the payment</li> <li>11. The system notifies the user about the result of the payment procedure and on discount/extra fees applied</li> </ol>

<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

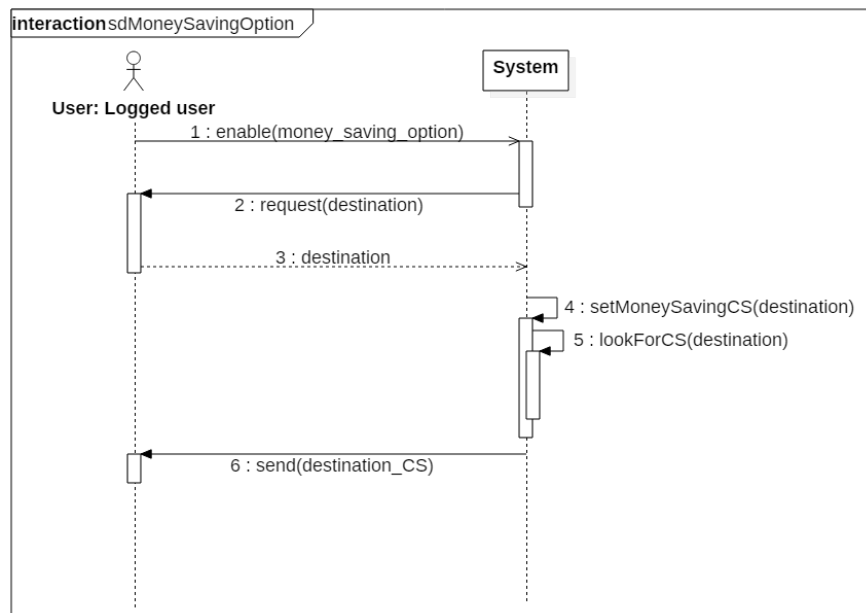
Figure 11: *Rent payment* sequence diagram

## 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>	<ol style="list-style-type: none"> <li>1. <b>Car Reservation</b></li> <li>2. The system asks the user to insert his destination</li> <li>3. The user inserts his destination</li> <li>4. The system searches for charging stations near the destination position inserted by the user with available plugs</li> <li>5. 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</li> <li>6. The system informs the user about the charging station to reach in order to obtain the discount</li> <li>7. <b>Car Rent</b> (<b>Car Reservation</b> already done)</li> </ol>
<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 12: *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	Maintenance service system must know the access token to be identified by the system
Flow of events	<ol style="list-style-type: none"> <li>1. 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>2. The system checks the access token</li> <li>3. 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>4. The system sends the information to the maintenance service system</li> </ol>
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

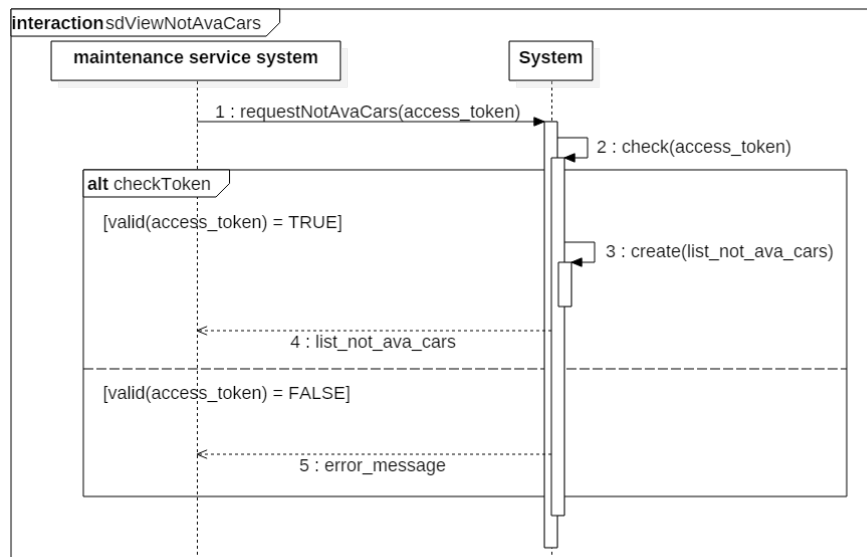
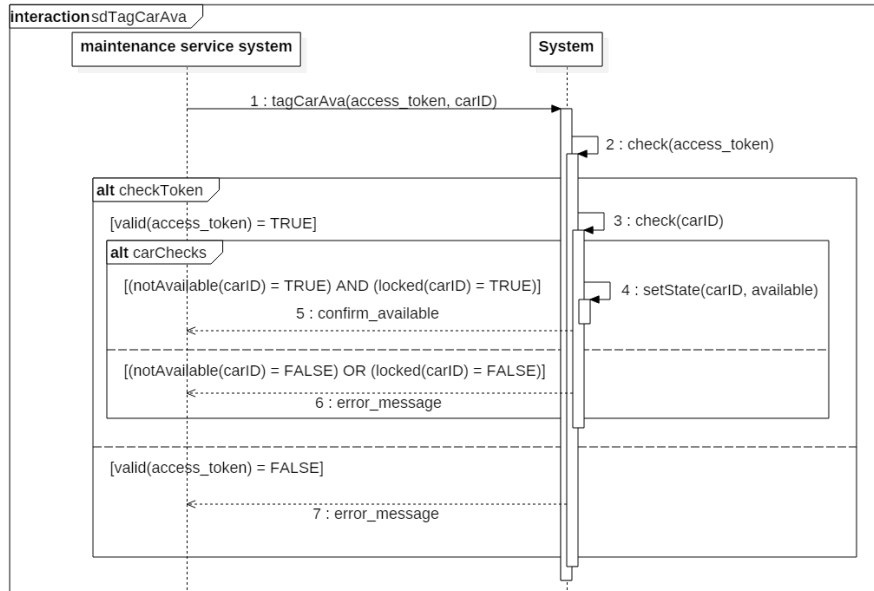


Figure 13: Visualization of not available cars sequence diagram

## 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>	<ol style="list-style-type: none"> <li>1. The maintenance service system asks to tag a car as Available sending the car identifier paired with the access token</li> <li>2. The system checks the access token sent by the maintenance service</li> <li>3. The system checks the identifier received corresponds to a car with state set as <i>Not Available</i></li> <li>4. The system checks if the car identified by the identifier received is locked</li> <li>5. The system set the state of the car identified by the aforementioned identifier as <i>Available</i></li> <li>6. The system sends to the maintenance service system a confirmation message the car state has been set as <i>Available</i></li> </ol>
<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 14: *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	<ol style="list-style-type: none"> <li>1. The customer care operator inserts the username or the mail of a registered user</li> <li>2. The system checks if the username or the mail correspond to a user registered to the system</li> <li>3. 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>4. The system shows to the customer care operator the info about the user</li> </ol>
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>	<ol style="list-style-type: none"> <li><b>Visualization of users information</b></li> <li>The customer care operator asks to view user's payments and rents history</li> <li>The system retrieves the list of user's payments (successful and unsuccessful)</li> <li>The system retrieves the list of user's rents</li> <li>The system shows to the customer care operator user's payments and rents history</li> </ol>
<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>	<ol style="list-style-type: none"> <li>1. The customer care operator inserts the username of a registered user</li> <li>2. 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>3. The system checks if the username corresponds to a user registered to the system</li> <li>4. The system marks or unmarks the user paired with the username as <i>banned</i></li> </ol>
<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>

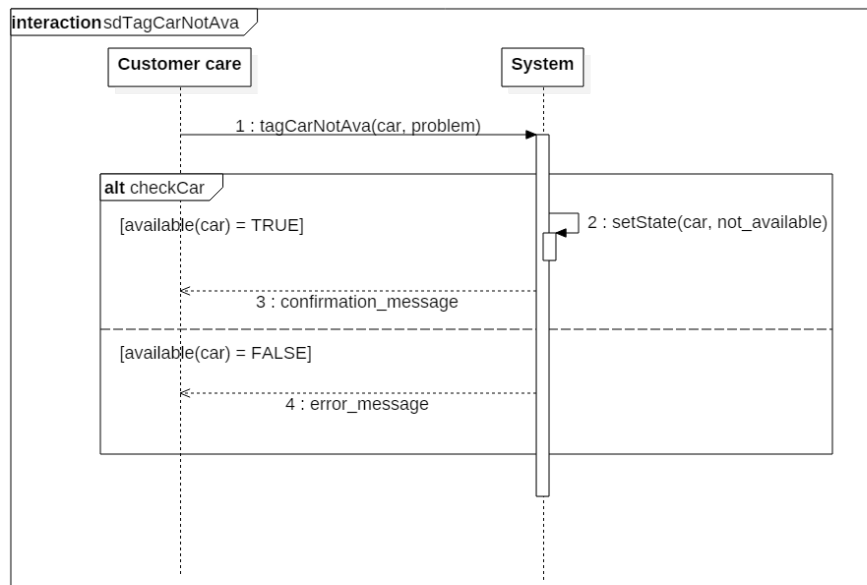
Table 13: *Mark or unmark a user as banned* use case description



## 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>	<ol style="list-style-type: none"> <li>1. The customer care operator inserts the identifier of the car</li> <li>2. The customer care operator asks to mark the car as <i>Not Available</i></li> <li>3. The customer care operator inserts a brief description of why the car state must be set as <i>Not Available</i></li> <li>4. The system checks the car identifier</li> <li>5. The system set the state of the car identified by the aforementioned identifier as <i>Not Available</i> paired with the description</li> <li>6. The system shows a confirmation message the car has been tagged as <i>Not Available</i></li> </ol>
<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 15: *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[6]. To ensure a better readability class attributes are not represented.

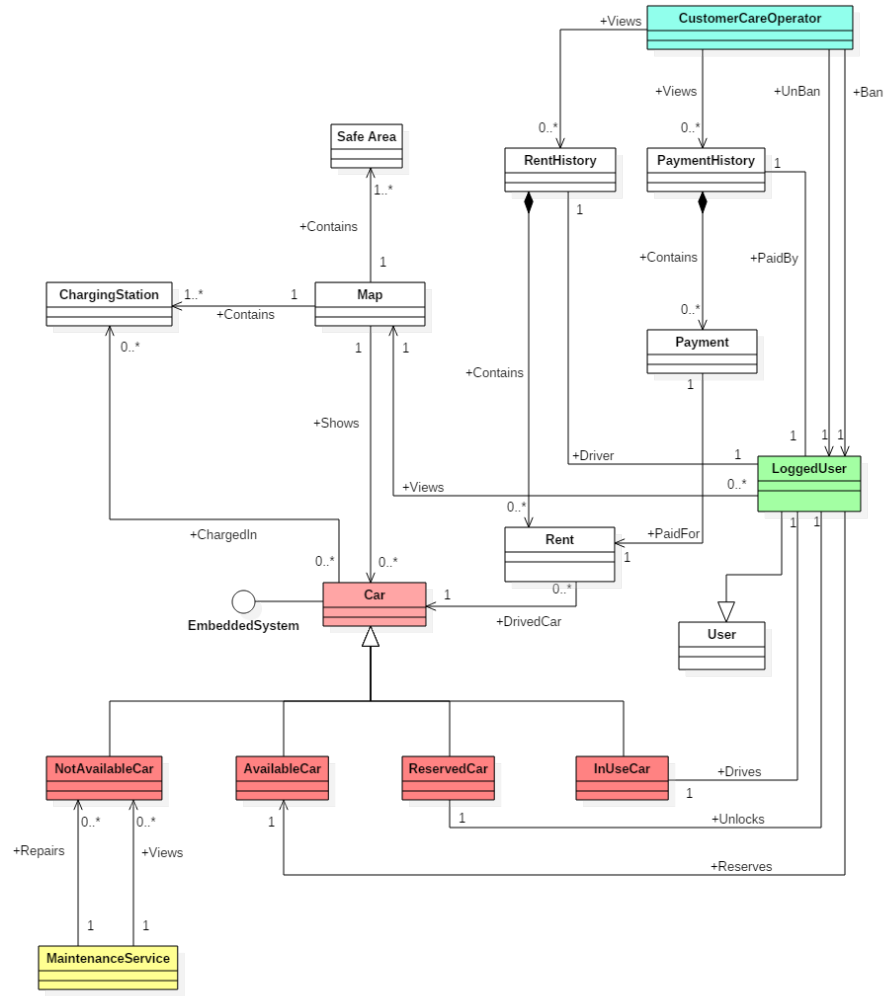


Figure 16: UML class diagram

# 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: NOType,
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 0-100%
21 abstract sig BatteryLevelPercentage{}
22 one sig Lower20Full extends BatteryLevelPercentage{}
23 one sig More50Full extends BatteryLevelPercentage{}
24 one sig From20to50Full extends BatteryLevelPercentage{}
25
26 //Number of passengers, we assume to deal with 5 passengers
   cars
27 abstract sig NOType{}
28 one sig Zero extends NOType{}
29 one sig One extends NOType{}
30 one sig Two extends NOType{}
31 one sig Three extends NOType{}
32 one sig Four extends NOType{}
33 one sig Five extends NOType{}
34
35 abstract sig User{}
36 sig LoggedUser extends User{
37   //personal information
38   //other parameters
39   banned: one Bool
40 }
41
42 sig ChargingStation{
43   charging: set Car
44 }
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
    corrispondent 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 NoUsersCanUseAndReserveDifferentCars{
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 in r.
        additionalFeeRent
179 }
180

```

```

181 //A reservation expired could not be outside safe area
182 fact NoReservationExpiredOutsideSafeArea{
183     no r:RentMade | r.reservationExpired = True and r.
        endSafeArea = False
184 }
185
186 //No discount are applicable if a reservation is expired
187 fact NoDiscountOrFeeIfReservationExpires{
188     all r:RentMade | r.reservationExpired = True implies r.
        discountApplicableRent = none
189 }
190
191 //No passengers can be detected during the ride if the
        reservation is expired
192 fact NoPassengersIfReservationExpires{
193     all r:RentMade | r.reservationExpired = True iff r.
        passengersDuringTheRide = Zero
194 }
195
196 //M2P discount must be applied iff there are at least two
        passengers detected during the ride
197 fact M1PDiscountAppliable{
198     all r:RentMade |( r.passengersDuringTheRide != Zero and r.
        passengersDuringTheRide != One)
        iff M1PD in r.discountApplicableRent
199 }
200
201
202 //BHF discount must be applied iff the car is left with more
        than 50 percent of battery
203 //at the end of the rent
204 fact BHFDiscnountAppliable{
205     all r:RentMade | r.endBatteryLevel = More50Full
        iff BHFD in r.discountApplicableRent
206 }
207
208
209 //CC discount must be applied iff the car is left on charge
        at the end of the ride
210 fact CCDiscnountAppliable{
211     all r:RentMade | r.onChargeAtTheEnd = True
        iff CCD in r.discountApplicableRent
212 }
213
214
215 //If a car is left on charge at the end of the ride it is
        located inside a safe area
216 fact AllCharginStationInSafeArea{
217     all r:RentMade | r.onChargeAtTheEnd = True implies r.
        endSafeArea = True
218 }
219
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
274 //outside safe area fee (OSAF)
275 //can not be applied because alla charging stations are
276 //inside a safe area
277 assert NoOSAFIfOnChargeAtTheEndRent{
278     no r:RentMade | r.onChargeAtTheEnd = True and OSAF in r.
279         additionalFeeRent
280 }
281 check NoOSAFIfOnChargeAtTheEndRent
282
283 //If CCD is applied A3BCF can not be applicable and
284 //viceversa
285 assert NoCCDAndA3BCF{
286     no r:RentMade | CCD in r.discountApplicableRent and A3BCF
287         in r.additionalFeeRent
288 }
289 check NoCCDAndA3BCF
290
291 //If CC discount is applied the end car position can not be
292 //more than 3km away
293 //from the nearest power grid
294 assert NoMSODMoreThan3km{
295     no r:RentMade | MSOD in r.discountApplicableRent and r.
296         endPosition = More3kmPowerGrid
297 }
298 check NoMSODMoreThan3km
299
300 //If MSOD is applied A3BCF can not be applicable and
301 //viceversa
302 assert NoMSODAndA3BCF{
303     no r:RentMade | MSOD in r.discountApplicableRent and A3BCF
304         in r.additionalFeeRent
305 }
306 check NoMSODAndA3BCF
307
308 pred show{#charging > 2 some u:LoggedUser | u.banned = True}
309 run show for 10 but exactly 2 ChargingStation, exactly 4 Car
310 , 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 17: Alloy execution result

## A.2 Generated worlds

Note that in [Figure 18](#) LoggedUser3 has been banned *after* completing Rent-Made0.

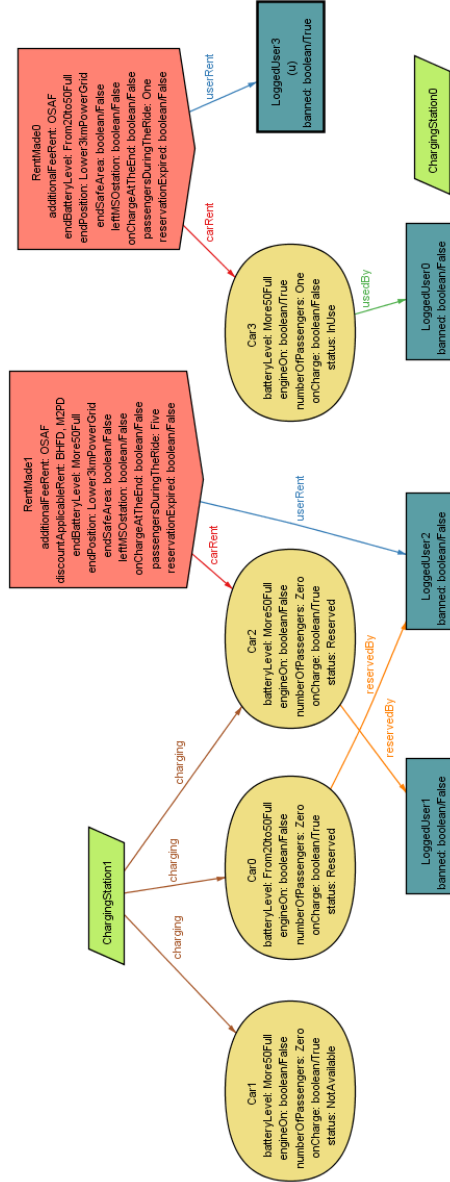


Figure 18: First alloy generated world

Note that in Figure 19 RentMade1 is actually a reservation expired of Car3 made by LoggedUser2. He now has reserved Car1.

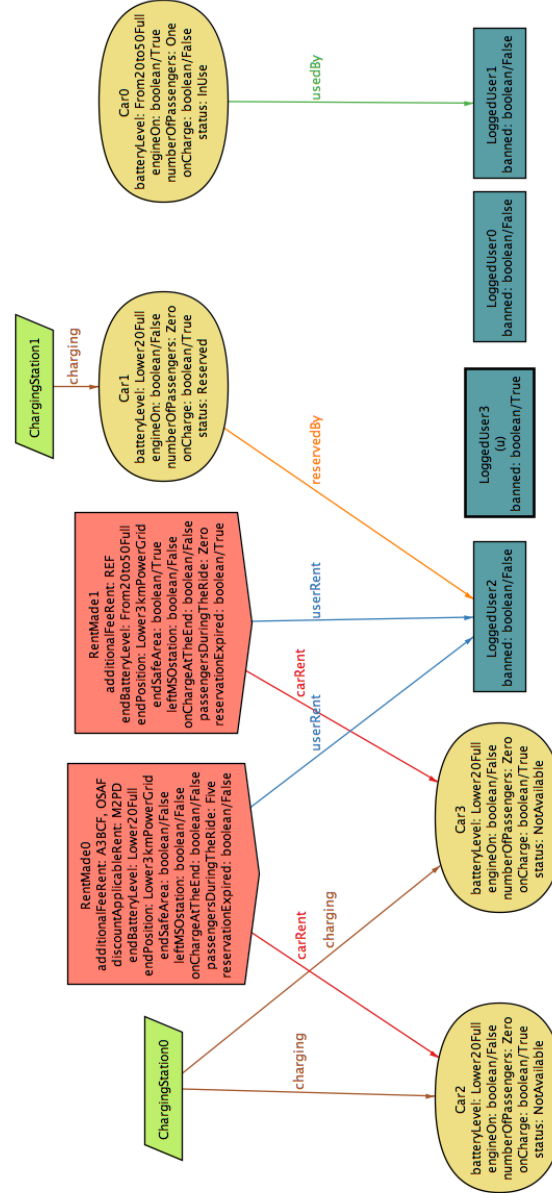


Figure 19: Second alloy generated world

## 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
- Git & GitHub as version control system
- Draw.io for graphs
- StarUML for diagrams
- Alloy as model analyzer

## C Hours of work

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

- Davide Piantella: ~ 48 hours
- Mario Scrocca: ~ 48 hours
- Moreno R. Vendra: ~ 45 hours

## D Changelog

- **v1.0** November 13, 2016
- **v1.1** November 23, 2016
  - Added notes to read the use case diagram w.r.t. external system interactions
  - Added notes to read the [FSM diagram](#) in order to clarify the system behaviour in case of car critical battery level
  - Improvements in [class diagram](#): cardinalities and compositions
  - Improvements in the definition of *Available* and *Not Available* car
  - Updated [R28](#) to avoid *Available* on charge cars to be set as *Not Available*
  - Added [DA16](#) to ensure communication even if the car has an empty battery
- **v1.2** November 30, 2016
  - Improvements in [DA6](#) to ensure all information provided by users are reliable
  - Split requirement about customer care access to user's data in [R44](#) and [R45](#)
  - Improvements to [R44](#) and related use case (*Visualization of users information*) to specify customer care could visualize the car state a user is eventually actually paired with

- **v1.3** December 8, 2016
  - Improvements **R4**
  - Add **R14** requirement to point out that user can not access to the system if he has not confirmed his own email address (also update *Authentication* use case)
  - Add **R5** to ensure driving license ID inserted by the user is unique
  - Update *Registration* use case to be coherent with last updates
  - Move **R28** from **G11** to **G4**

## 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, *Assignments Software Engineering 2*, AA 2016-2017
- [4] IEEE Std 830:1993, *IEEE Recommended Practice for Software Requirements Specifications*, 1993
- [5] M. Jackson, *The World and the Machine*, 1995
- [6] R. J. Abbot, *Textual (noun-verb) analysis*, 1983