

Design Document

Document Version 1.5

Matteo Frosi (mat. 875393)
Luca Costa (mat. 808109)

Contents

1	Introduction	3
1.1	Purpose	3
1.2	Scope	3
1.3	Definitions, acronyms, abbreviations	3
1.4	Document structure	4
2	Architecture design	6
2.1	Overview	6
2.2	Overview of the car system	7
2.3	Components of the system	8
2.3.1	High level view	8
2.3.2	Detailed views	10
2.4	Deployment	13
2.5	Runtime diagrams	14
2.5.1	Login runtime diagram	14
2.5.2	Reservation runtime diagram - purpose of model -	16
2.5.3	End of service runtime diagram	18
2.5.4	Temporary stop by runtime diagram	20
2.5.5	Emergency handling runtime diagram	22
2.6	Component interfaces	23
2.7	Architectural styles and patterns	23
2.7.1	Overall architecture and comparison with other architectures	23
2.7.2	Protocols	24
3	Document further information	24
3.1	References	24
3.2	ChangeLog	24
3.3	Hours of work	25

1 Introduction

1.1 Purpose

This document, addressed mainly to developers, aims to go into further details regarding the specification of the project, described in the RASD. Here more technical features will be described, including:

- The high level architecture
- Some possible design patterns
- The description of the main components and their interaction (Runtime View)
- A brief description of the algorithms on which the software relies
- A more detailed overview of the user interfaces

Although these are the main topics of the document, other minor details will be touched and discussed, such as the architectural style and a brief comparison with other styles and the mapping between the requirements defined in the RASD and the designed elements described in this document.

1.2 Scope

PowerEnjoy is an electrical car sharing service, based on a mobile application. The targets of the service, intended as users, are people that needs to move from a place to another within a city and requires a conveyance to move (because they don't have their own or simply can't use it).

A user can make a reservation for a car, using the mobile app and his/her account, and check for the availability and status of all the cars within his/her position, identified using GPS localization, or a specific one, inserted manually by the user. As stated before, to access the service, the user must possess a private account, so a registration is needed.

The system provides the users a safe way (identification code) to access the cars, and the riding service and keeps trace of the status of all the cars.

Moreover, the system prizes or punishes a respectively good or bad behavior from the users, applying a discount or an overcharge on the cost of a ride. As example, if the user leaves the car without much battery, he/she will have to pay more than the standard cost of the ride, because the car will need to be charged and this operation has a cost. On the other hand, if a user plugs the car before ending the service, it receives a discount.

The system includes other functionality, such as GPS based maps available in every car, an emergency procedure in case an accident occur during a ride and the notification of a car status if the user requested it.

1.3 Definitions, acronyms, abbreviations

- RASD: document about the requirements analysis of the project.
- DD: document about the design choices and the components description of the project.
- GPS: global navigation satellite system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

- SMS: short message service; it is a notification sent to a mobile phone, we need a GSM gateway to use it.
- GMS gateway: device that allows SMS text messages to be sent and/or received by email, from Web pages or from other software applications by acquiring a unique identifier from the mobile phone's Subscriber Identity Module, or SIM card.
- Push notification/ push message: it is a notification sent to a smartphone using the mobile application.
- API: application programming interface; it is a common way to communicate with another system.
- REST: representational state transfer, it's one way of providing interoperability between computer systems on the Internet.
- RESTFul: REST with no session.
- UX: user experience design
- URL: uniform resource locator.
- MVC: model view controller, it's a design pattern.
- SOA: service oriented architecture, it's a style of software design where services are provided to the other components by application components, through a communication protocol over a network.
- Layer: way of organizing code in sections sharing a common goal. The highest partition includes Presentation Layer, Business or Logic Layer and Data Layer.
- Tier: physical deployment of layers.
- Safe area: it is a specific area where the electric cars of PowerEnjoy service can park. The set of safe areas is pre-defined and owned by the company/society that requested the management system for the service.
- Special safe area: it is a safe area where power grid stations are installed.
- Power grid station: it is an installation that allows the recharge of an electric car.
- Communication primitives: set of instructions and procedure that allow a communication between machines and devices over a network.
- Sensor data retrieval: procedure that consists in getting all the information collected by the sensors of the car.

1.4 Document structure

- Introduction: this section introduces the design document. It gives an overview on what topics will be covered and what aspects described in the RASD will be improved here.
- Architecture Design: this section is divided into different parts, each describing an aspect of the software design.
 - Overview: brief description of the division in tiers and layers of the application.

- Components and interaction: high level and detailed view of the components of the application and the way they communicate.
 - Deployment: view of the physical devices and the way they contains components
- Algorithm Design: this section describes some of the algorithms that the application will rely on. To focus on the algorithm idea and not the fine grained implementation, pseudo-code will be used.
- User Interface Design: this section presents mockups and user experience explained via UX diagrams.
- Requirements Traceability: this section aims to explain how the decisions taken in the RASD are linked to design elements.

2 Architecture design

2.1 Overview

PowerEnjoy relies on a three tier architecture. Referring to the proposed system architecture presented in section 2.3 of the RASD, the following figure represents the tier division of the system.

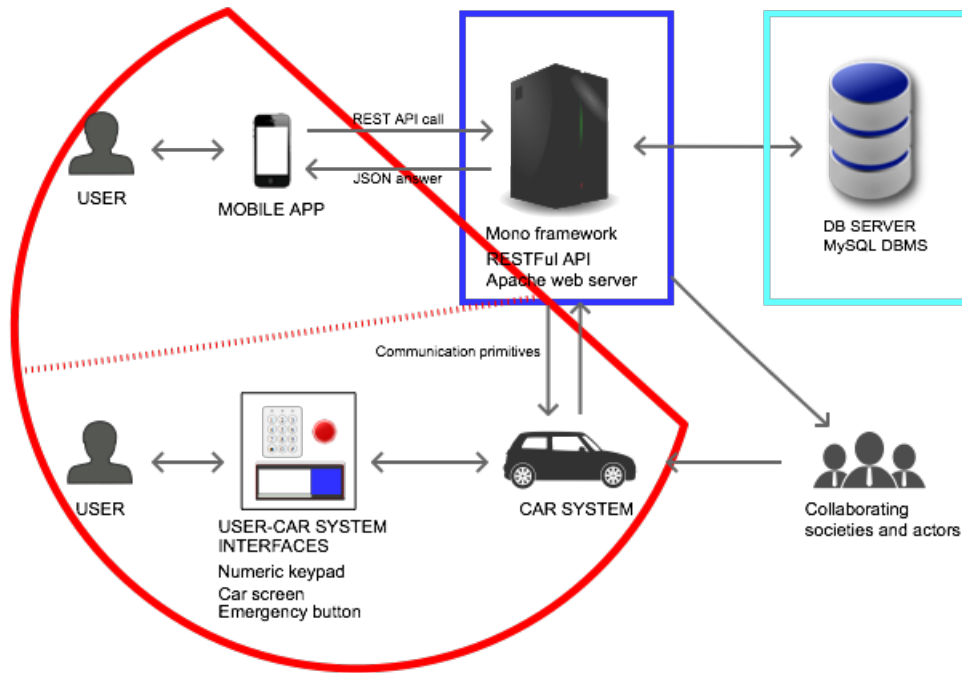


Figure 1: Proposed architecture, tier division - red: client, blue: server, azure: database

The client side includes all the possible ways by which a user can interact with the server (and the service), that are the mobile application and the car itself. The first represents the classical idea of client tier, including a GUI and a minimal amount of processing power that allows the user to have a connection with the rest of the tier, shown in a graphical way, that is more user friendly. The latter is, instead, a particular client tier that acts as a mini server, because it contains more logic than the mobile application. Here there is not a real graphic interface but multiple mechanical interfaces (MUI) can be detected, such as the numeric keypad that make the user able to unlock the car or end the service, the emergency button and the car screen, that is thought more towards an informative interface than an interactive interface. To better understand this concept, follow the same figure, this time divided in high level layers.

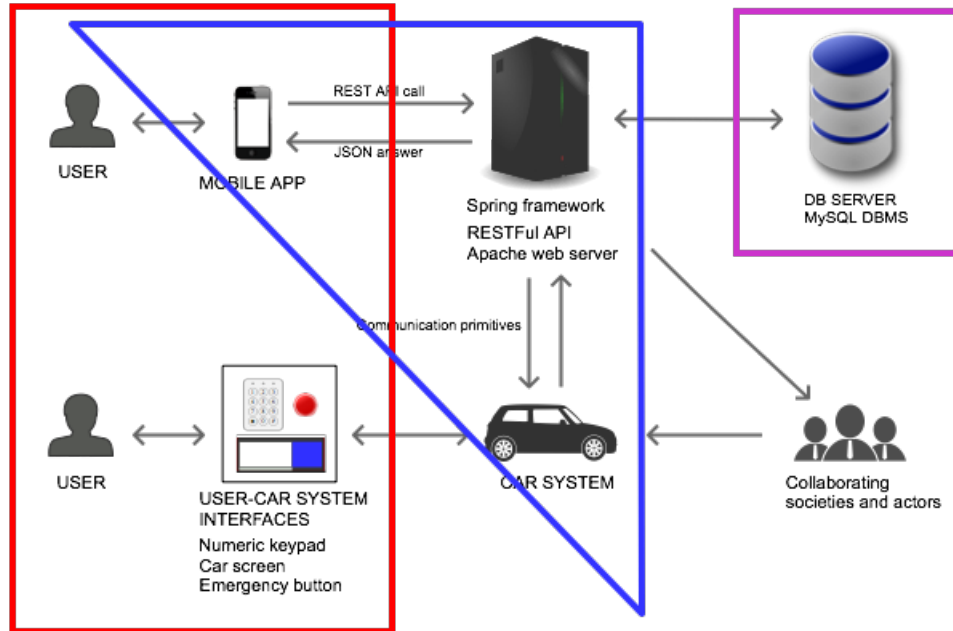


Figure 2: Proposed architecture, layer division - red: presentation, blue: logic/business, purple: data

The mobile application is also part of the logic layer because it can hold some immediate processes, instead of delegating them to the main server. An immediate example could be the elaboration of the GPS based map during the research of an available car.

2.2 Overview of the car system

It should be useful to spend some words to discuss more in detail the structure of the car and the way the user can interact with it, and consequentially with the server. Using multiple sensors, information about the car status can be retrieved, such as battery charge, number of passengers, degradation level of the car components, or even the localization data, obtained with GPS. Such data pool is interfaced with the car system, that resembles the shape of an application. The car app can be considered as a cluster of procedures and interfaces that allows user, car hardware and system to communicate and “know” about each other. Speaking in pattern terms, the car app emulates the controller entity in the MVC pattern, even if only partially. As said in the previous subsection, while the emergency button and the numeric keypad make the user interact with the car in an active way, the car screen acts as a passive element and is simply needed to inform the user of the car status and the service info. We can consider such feature as a way to diminish the interaction user-system to a very strict level, without changing the user perspective of the service. Such reduction lightens the logic needed in the car, making the project more achievable from a budget and complexity point of view.

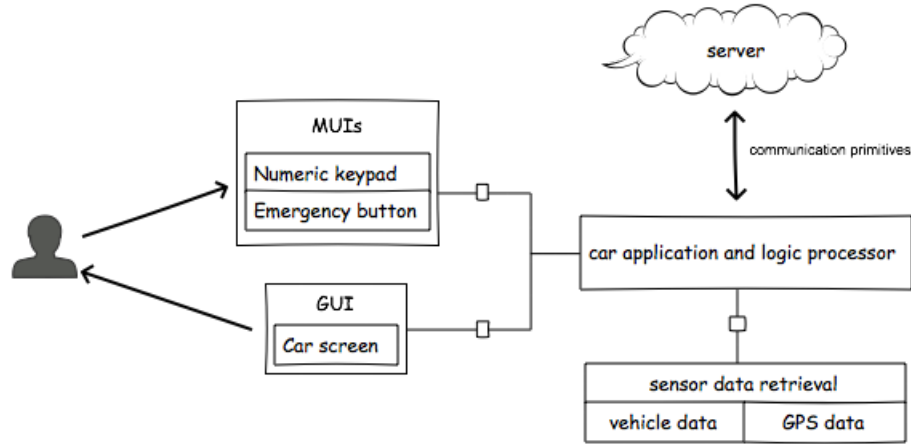


Figure 3: High level car system

2.3 Components of the system

2.3.1 High level view

From an high point of view, the system can be divided into four elements. The users can interact with the server, that is the main central where all the logic is concentrated, directly or with the support of the car. A user can initiate the interaction with the server using his/her mobile application. To proceed in using the service, the user must first be logged into the system and for every action he/she does (monitoring request, reservation request, take back of a reservation, code request and so on), he/she has to wait for the server response, informing the user that the request has been successful or not. Because of this sequentiality of actions, the communication directed from user to server has to follow synchronous rules when proceeding in a certain sequence and leave all the other non-interactive options as to be implemented in an asynchronous way. As example the user shouldn't be prohibited to search for an available car even if he/she already made a reservation, but he/she cannot made a code request if there is no reservation made. A clever way to implement the user-server relationship is to made all the communications asynchronous but thanks to particular patterns, MVC among them, denying the usage of particular services if certain conditions are not met.

The user can also interact indirectly with the server using the car - or it can be said that the car interacts with the server -. Some physical interfaces, such as the emergency button or the numeric keypad, allow the user to modify the condition of a car and, consequentially, of his/her service.

The server/central acts mainly as an elaborator, or referring to the chosen architecture, as a monolithic logic processor. Its job is to coordinate the requests from the users and the change of status of all the cars. As said before, the interaction between user and server can be described with a simple MVC pattern. From a very high view, the user makes an action, communicates it to the server, the server elaborates the request and confirms/rejects the will of the user. The server-car-user relationship is a bit more complex. Firstly, there is a continuous interaction between every car and the server, that follows this sequence:

1. Data retrieval
2. Car status update (car to server)
3. Database update (server to database)

4. [Optional] Car update (server to car), as example the lock following the end of the service

Moreover, to this sequence must be added the interaction with the user; that is both passive and active as said in the previous section.

The server communicates with all the other components using asynchronous messages, because it does not depend on their status but acts as the independent core of the software. Just referring to the user behavior, it would be unthinkable to have the server wait for a user decision, stated that the thinktime can be to long, and each communication would become a bottleneck for the whole system.

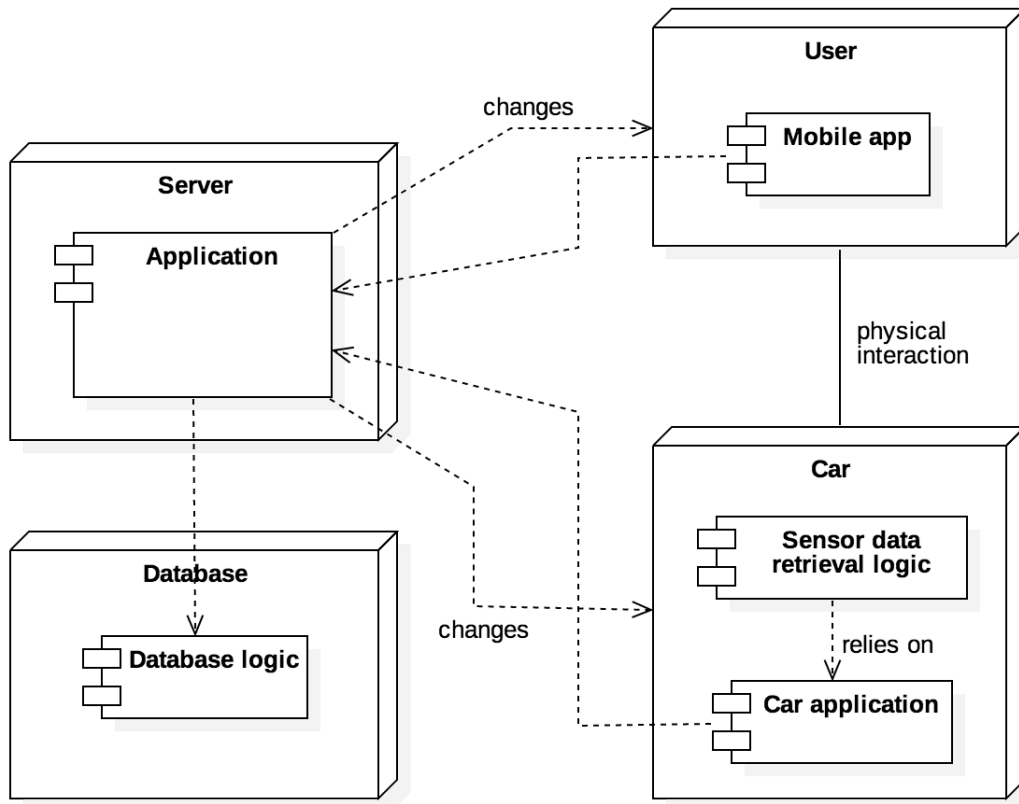


Figure 4: High level view of the components of the system

2.3.2 Detailed views

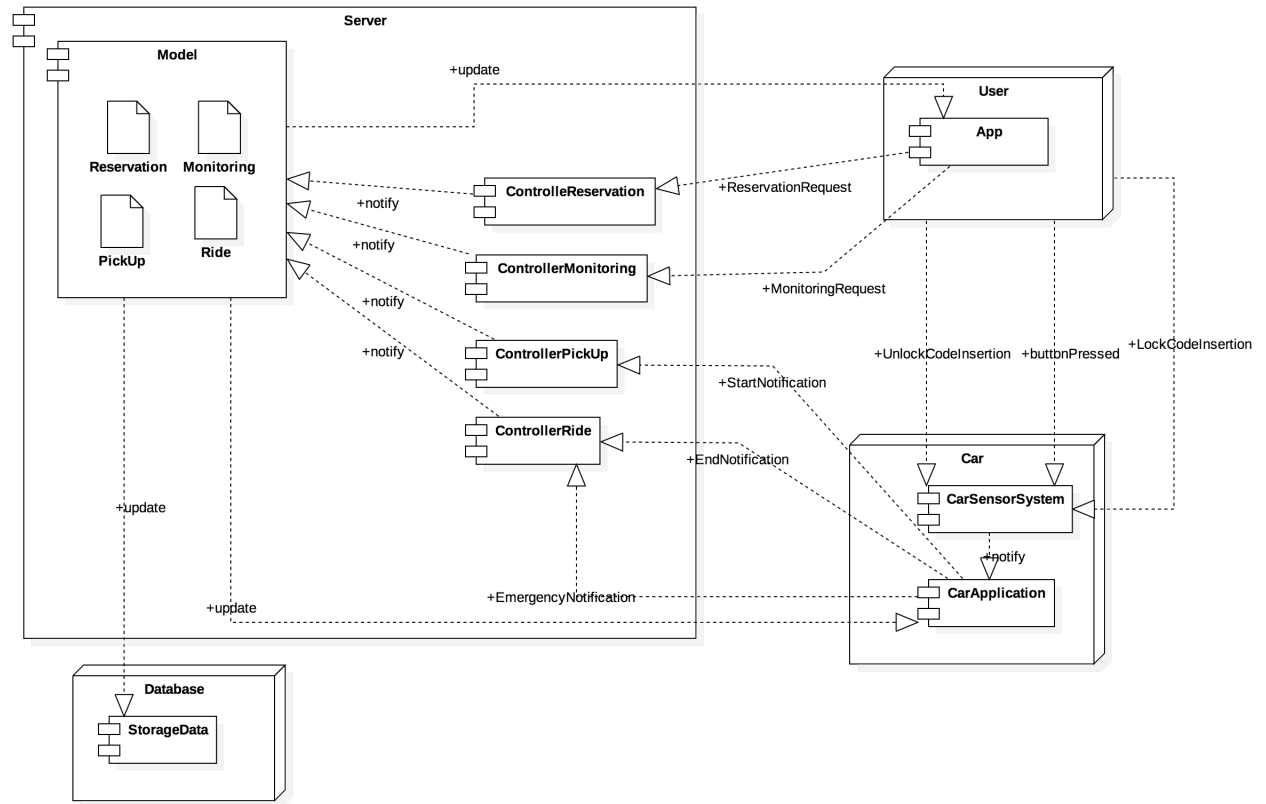


Figure 5: Deeper high level component diagram

Deepening the high level component diagram, each big node can be fragmented into smaller parts, each characterized by its functionality. As previously said, The user can interact directly with the main server/central using his/her mobile application, or, indirectly, using some of the car physical devices (the button and the numeric keypad). Focusing more on the server composition, multiple components to handle and manage every part of the service are needed. Purely from a topological point of view, the server consists of two big areas. One refers to all the structures and components that handles and addresses incoming data from and to the external world, while the other refers to all the functionality and procedures that allow the elaboration of an event and the consequent updates on the server itself, but also on the external world (database, clients or cars).

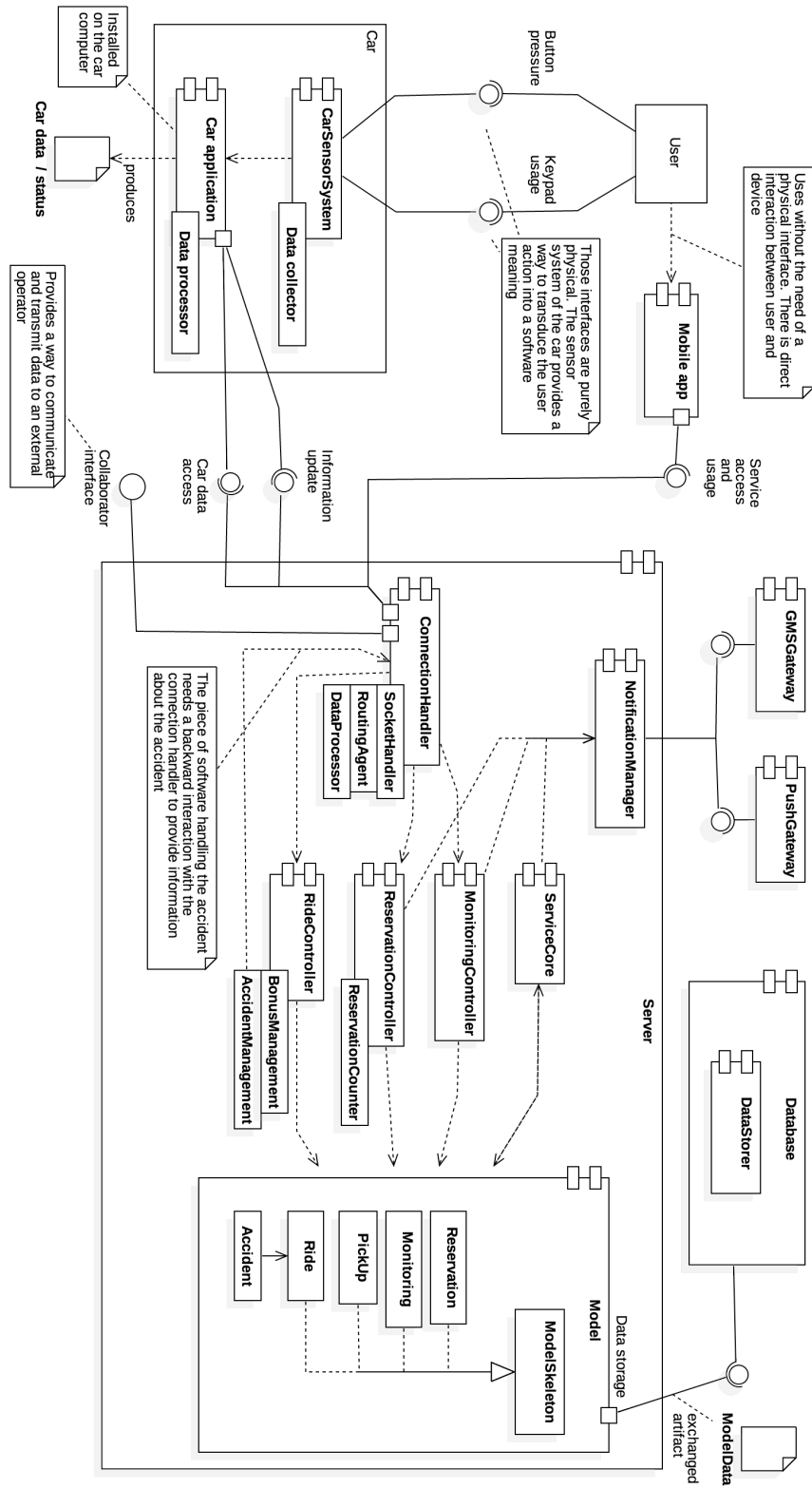


Figure 6: Detailed component diagram

Figure 6 represents an even more detailed component diagram, including sub components, interfaces, products (artifacts) and ports. One of the two area previously described can be seen as a mail office. The component ConnectionHandler, as the name suggests, handles the incoming and outgoing data, sorting it to the specific controller. The other area, composed by the Model and the ServiceCore interacts with the Database, providing it the information about the Model itself. The NotificationManager component takes care of the communication and interaction needed with the user's device. In detail:

- **GSMSGateway:** device that allows SMS text messages to be sent and/or received by email, from software applications.
- **PushGateway:** device(s) that manages push notifications.
- **NotificationManager:** component that takes care of the interaction with the user's device.
- **ConnectionHandler:** component that sorts incoming and outgoing messages (data transfer).
- **ServiceCore:** contains all the procedures supporting the software (algorithms, functions and so on).
- **ModelSkeleton:** representation of the analyzed world
- **CarApplication:** contains all the procedures that elaborates the data retrieved by the sensor system of the car and interacts with the server.
- **Database:** device used to store the model data

2.4 Deployment

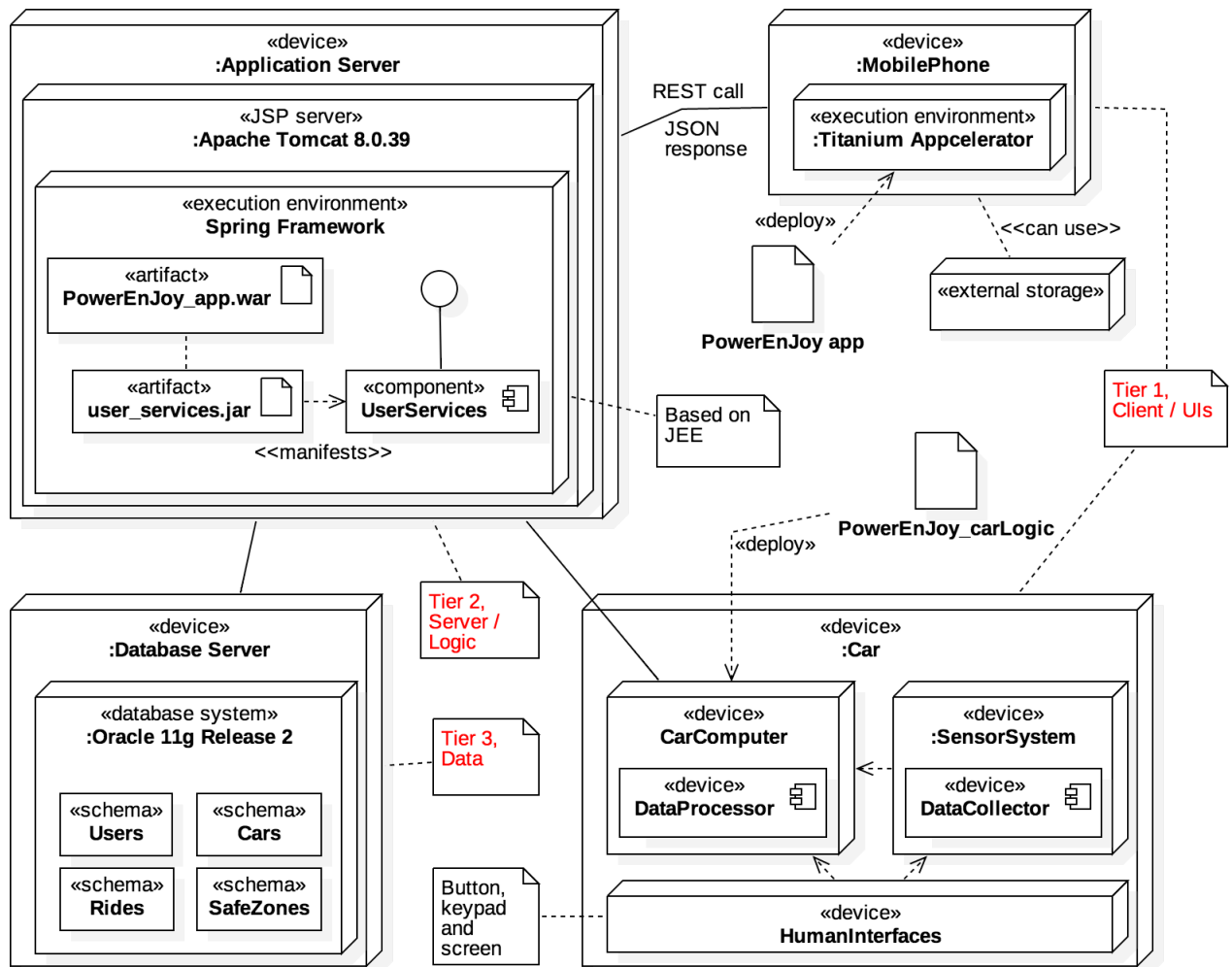


Figure 7: Deployment diagram

The PowerEnJoy software can be divided into three cores. The user-related core is deployed on the mobile device and in the same way the car-related core, which slightly differs from the first because it mainly takes care of the car logic and data elaboration, is deployed on the car processor / computer. The last core is obviously related to the logic tier of the whole software, deployed on the server machine(s). The Apache Tomcat server runs on the application server and the Spring framework, that provides a comprehensive programming and configuration model for modern Java-based enterprise applications - on any kind of deployment platform. A key element of Spring is infrastructural support at the application level. Moreover it provides foundational support for JDBC, allowing a simple and easy interaction with the main database.

2.5 Runtime diagrams

2.5.1 Login runtime diagram

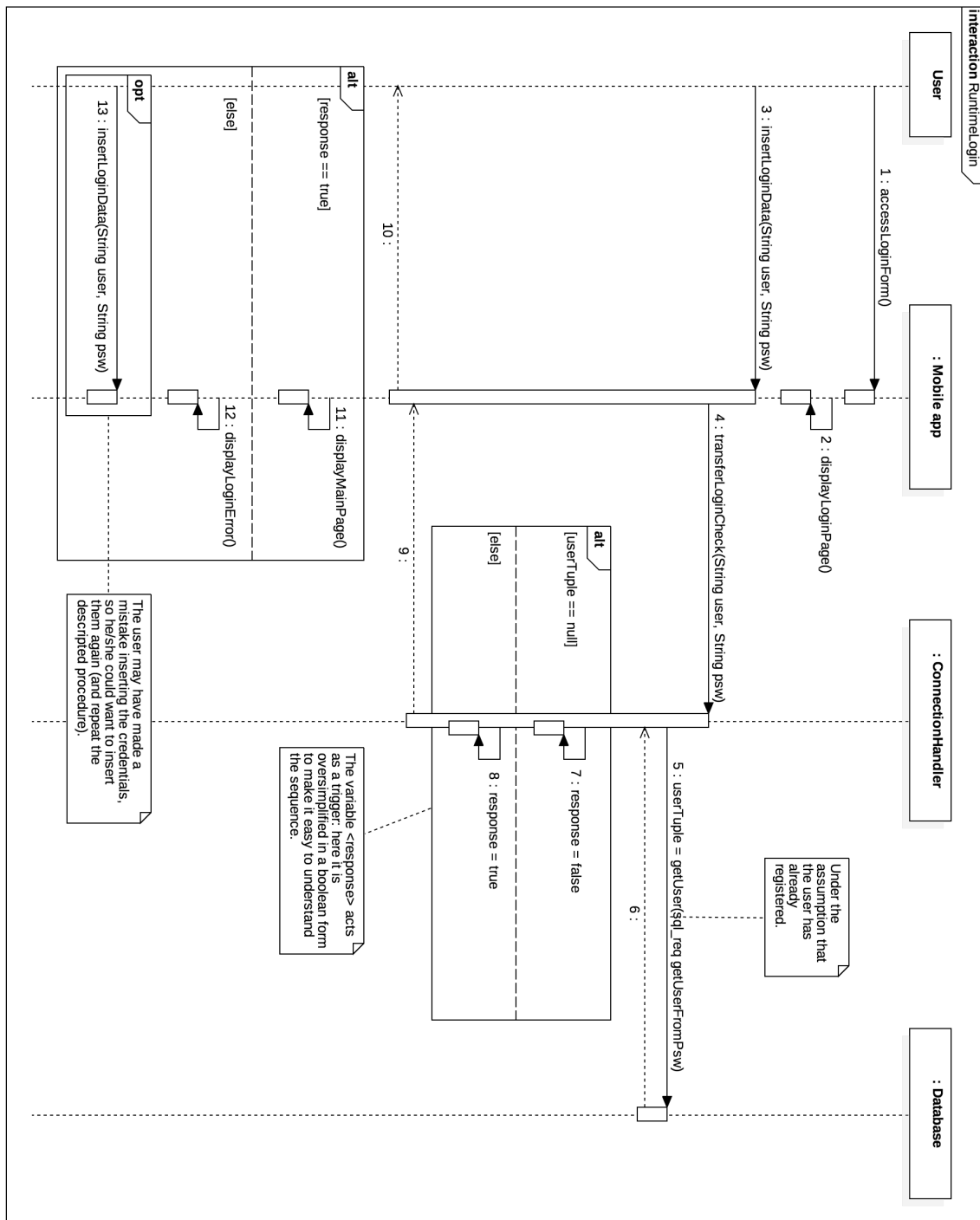


Figure 8: Login runtime sequence

This diagram describes, as the name implies, the interaction of some components during the login phase. After having accessed the login section on the mobile application, the user has to insert the login credentials. The app communicates with the server, thanks to the `ConnectionHandler` component, that makes a request on the database to retrieve the couple user/password. As the diagram represents the *use case description 1.1*, described in the RASD, it holds the assumption that the user has already registered. Otherwise a double check is needed: before searching for the couple user/password the server has to check if the user is in the database, meaning he/she already registered. The user may have inserted a wrong password, so he/she sees an error message on the screen, instead of the main page of the app.

2.5.2 Reservation runtime diagram - purpose of model -

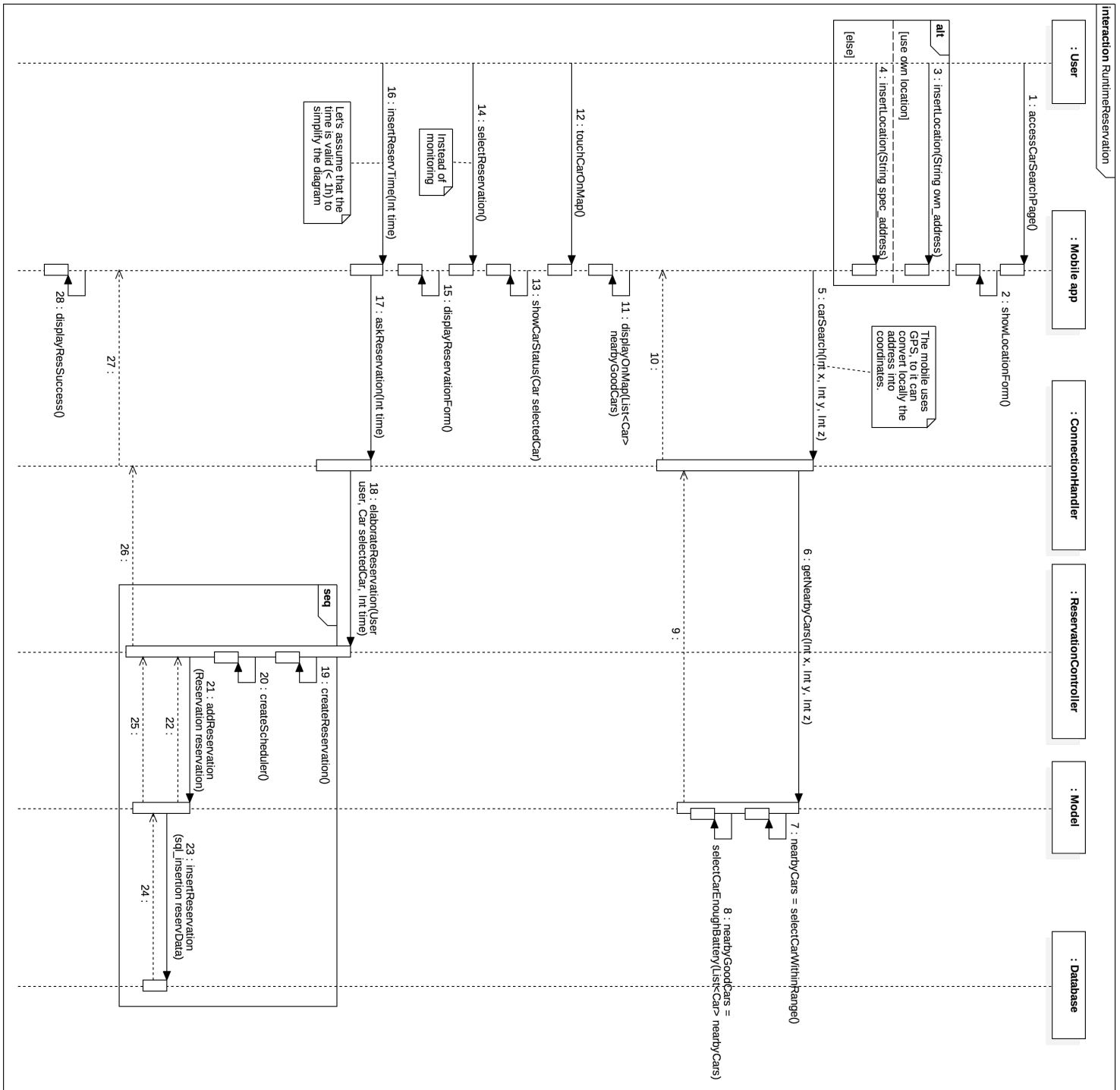


Figure 9: Reservation runtime sequence

The diagram represents the first part of the *use case description 1.2* in the RASD, not considering the pickup phase. The user accesses the car search section on the mobile app and can decide if using his/her own location or a specific address. The mobile app converts the address into coordinates (and this denotes a part of logic in the app, to lighten the server logic core) and communicates them to the server. The `ConnectionHandler` component interacts directly with the model. The model searches for the nearby cars, in a 5km range zone, and selects the ones with more than 20% of the battery.

Why the model and not the database? After having delayed the description of the model from the components description, it is necessary to explain the purpose of the model. It acts as a sort of cache: instead of interacting continuously with the database, the server contains, in the model, a bit chunk of information, such as car location and minimal status, user status of login and so on.

The server communicates then the list of cars to the mobile app, that displays it to the user. He/she can now select a car and make a reservation. After having informed the server of the reservation request, the `ReservationController` component handles the request, creating a timer (to count the expiring time before the reservation expires), the reservation object and updating Model and Database.

2.5.3 End of service runtime diagram

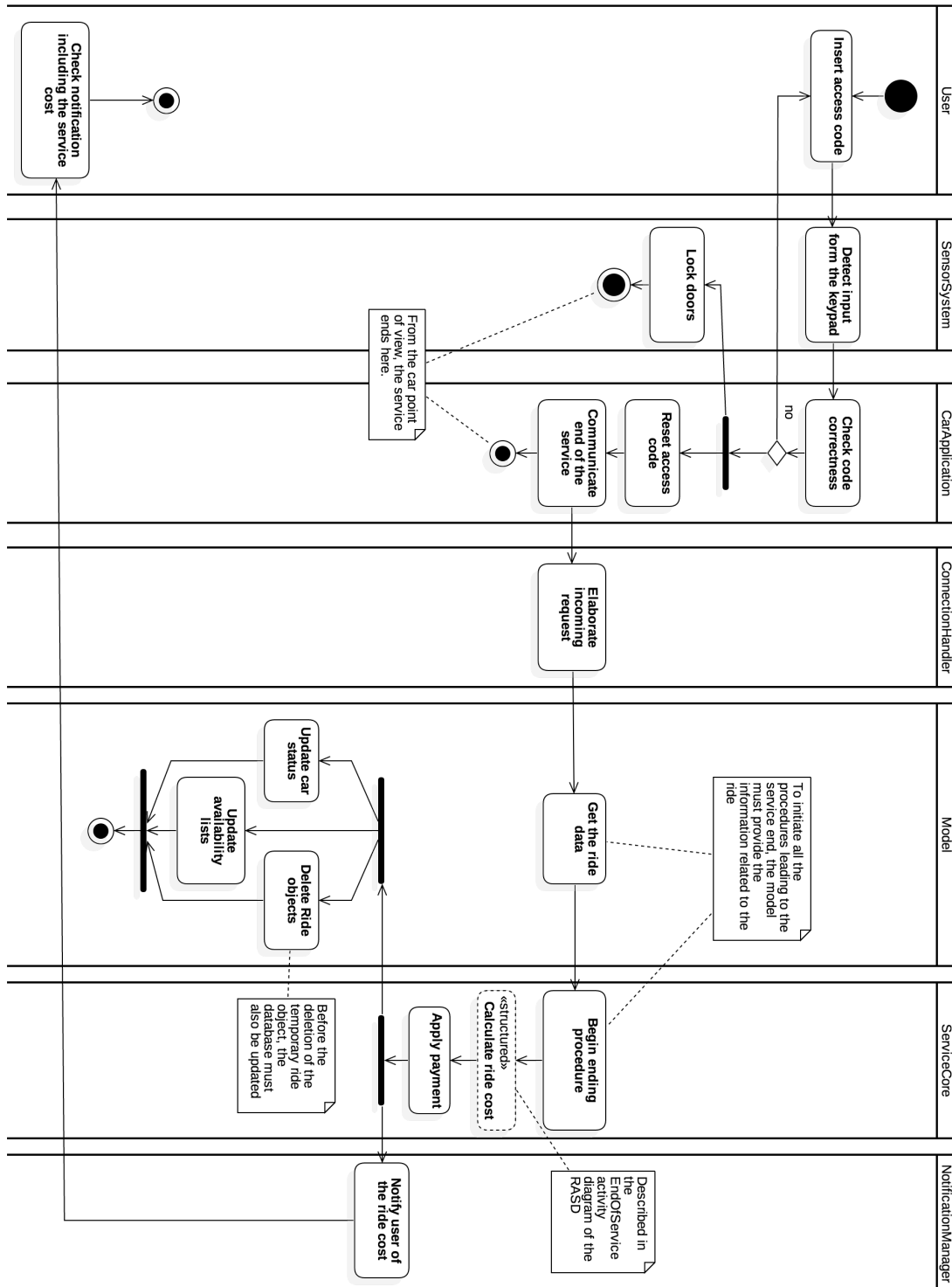


Figure 10: End of service runtime activities

The diagram describes, with some simplifications, the relations of the components during the end phase of the service, referring to the *use case description 5* of the RASD. The phase begins when the user inserts the access code of the service using the numeric keypad of the car. The latter detects that the service is going to end, so the code is reset (to avoid further uses of the car) and all the doors are locked. Meanwhile the server is informed of the end of the ride, so it collects from the model all the data about the ride and starts all the core functionality, in the ServiceCore component, concerning this phase, such as ride cost calculation, payment, and so on. The Model and the Database are updated (the model doesn't need to know the ride anymore, but the database does, for future usage of such data). The ServiceCore will also use the NotificationManager to notify the user of the service cost, through the PushGateway described in section 2.3.2.

2.5.4 Temporary stop by runtime diagram

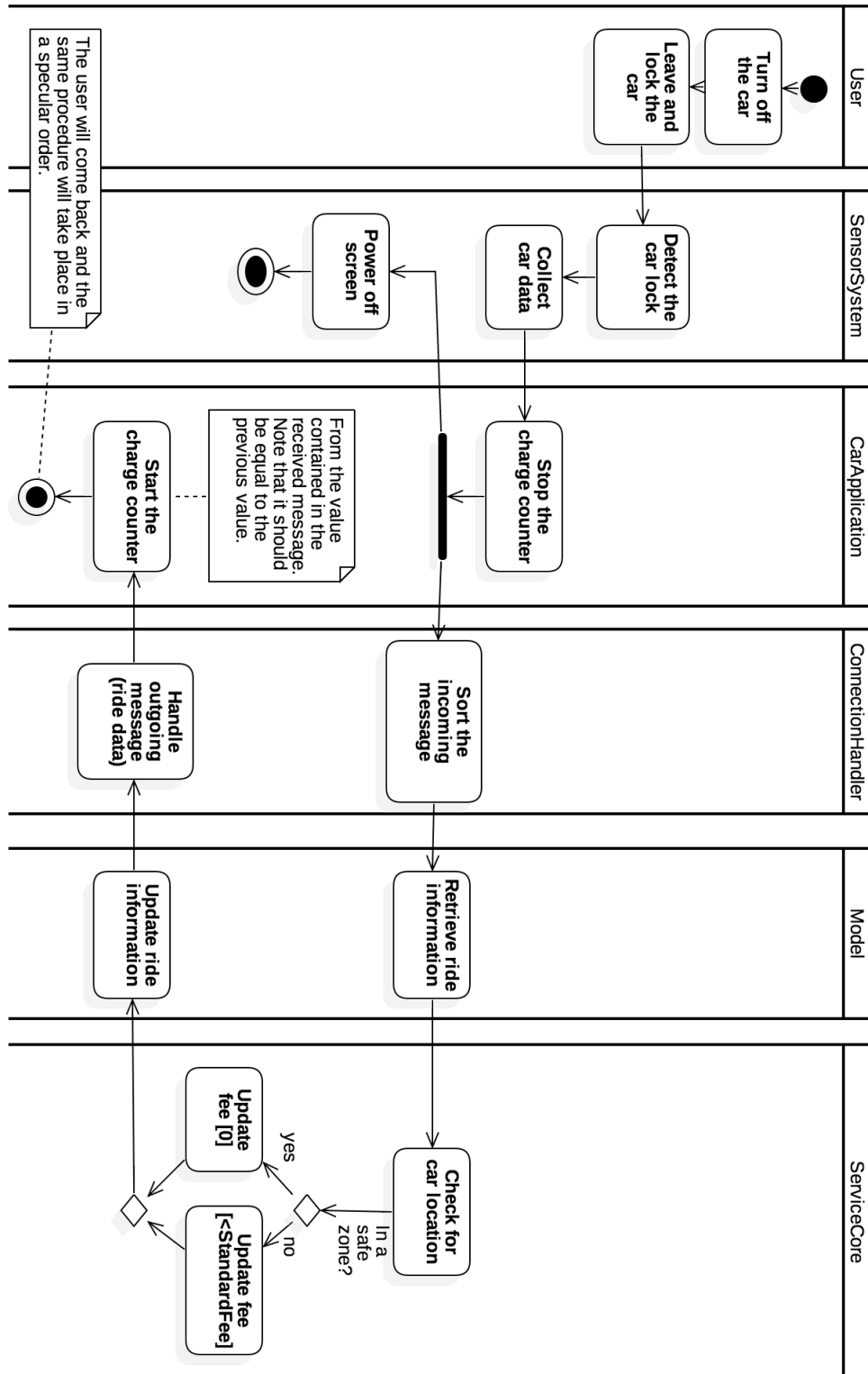


Figure 11: Temporary stop by runtime activities

The diagram describes the sequence of activities of the components of the system involved in the temporary stop by action, described partially in the *use case description 4* of the RASD. After having turned off and locked the car, the CarApplication stops the ride cost counter and powers off some of the car components, such as the dashboard, the internal lights and the screen - the user is gone, there is no need to waste energy -. The server receives information about the stop by action and calculates the new fee, operation done by the ServiceCore, using the data contained in the Model about the ride and the received data. This to check for the coherence of information, in fact the cost on the model should be the same of the cost calculated by the car - logic replica -. After the application of the new fee, the Model is updated and CarApplication is informed of it, ready to begin once again charging the user. Last thing to notice, and it's also written in the diagram, is that the value when the counter stopped and when it begins again, must be the same.

2.5.5 Emergency handling runtime diagram

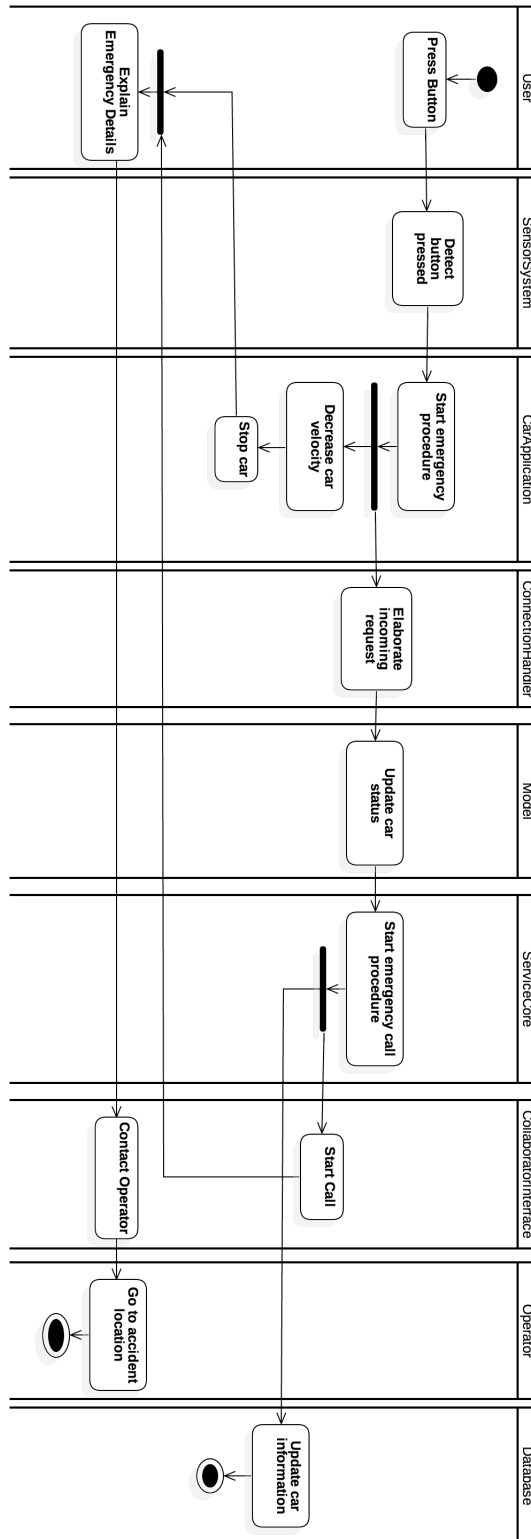


Figure 12: Emergency handling runtime diagram

2.6 Component interfaces

2.7 Architectural styles and patterns

2.7.1 Overall architecture and comparison with other architectures

As described in the introduction (Overview 2.1), PowerEnjoy software will be deployed following a 3-Tier architecture, composed of a database, a server and a client. The client consists of both the mobile app and the car (that is the other main actor, along with the user). Here some features of this architecture:

- Specialized (there is 1 tier dedicated to a certain task).
- Flexible: the server and the database are single points of failure of the system but acts independently. If a client “brakes” the other tiers will still continue to work.
- Secure: the client will not have direct access to the database, but each tier acts as a proxy to the next level.
- Deployed as a Monolith, so easier implementation of module interactions.
- Simple to test and deploy.

Before making a paragon with other architectures, here is made a compartmentalization between layers, already described in the previously said Overview:

- Client: contains an interface to the Business Logic Layer (BLL).
- Server, containing the biggest chunk of software logic: Business Logic Layer, that is separate from other tiers or layers, such as the data access layer or service layer.
- Database, containing the Data Access Layer (DAL).

3T vs Hexagonal The core of the hexagonal architecture is logic implemented by modules with attached several services using specific adapters. As the 3T it is also deployed as a Monolith and due to the modularity it is simple to test and deploy. However hexagonal architectures are more suitable for big and complex systems, dealing with multiple services and actors. The developing complexity is also higher, due to the implementation of more modules and adapters/interfaces than a 3T.

3T vs SOA The SOA, service oriented architecture, is a style of software design where services are provided to the other components by application components, through a communication protocol over a network. A service is a discrete unit of functionality that can be accessed remotely and acted upon and updated independently, such as retrieving a credit card statement online. SOA is:

- Scalable
- Reusable
- Flexible

SOA would not be a good idea for PowerEnjoy due to the heavy data exchange and the lack of the underlying idea of services: in the studied problem all the “services” are fragment and functionality provided by the same provider, such as the reservation request or the monitoring request.

3T vs Microservices The Microservices architecture is a specialization of and implementation approach for service oriented architectures (SOA) used to build flexible, independently deployable software systems. Services in a microservices architecture are processes that communicate with each other over a network in order to fulfill a goal and services should have a small granularity.

For the same reasons described in the paragraph, 3T vs SOA, also the Microservices architectures is not a good option in describing and developing the PoerEnJoy software, despite the better efficiency and the very low dependence factor.

2.7.2 Protocols

3 Document further information

3.1 References

- RASD, before Version 4.5
- Assignments AA 2016-2017.pdf
- <https://msdn.microsoft.com/en-us/library/ee658116.aspx>, containing some information about layers design
- <http://alistair.cockburn.us/Hexagonal+architecture>, contains some information about the Hexagonal architecture
- <https://www.nginx.com/blog/introduction-to-microservices/>, contains some information about the Microservices architecture
- <https://8thlight.com/blog/uncle-bob/2011/09/30/Screaming-Architecture.html>, contains some advices over the architecture choice and implementation
- <http://www.uxbooth.com/articles/8-must-see-ux-diagrams/>, contains some examples of user experience diagrams
- <https://projects.spring.io/spring-framework/>, contains some information about the Spring framework
- <http://www.agilemodeling.com/artifacts/componentDiagram.htm>. contains a brief description of the component diagrams from an AGILE point of view
- Sample Design Deliverable Discussed on Nov. 2.pdf
- Paper on the green move project.pdf
- Second paper on the green move project.pdf

3.2 ChangeLog

- [21/11/2016] [**Version 0.1**] :: Added first part of the document introduction, including preface, Purpose, Scope and Definitions. ChangeLog and Hours of work sections also introduced.
- [21/11/2016] [**Version 0.2**] :: Added the References and Document structure sections.

- [23/11/2016] [**Version 0.3**] :: Added the overview of the architecture of the project and a brief description of the car system, so subsections 2.1 and 2.2.
- [23/11/2016] [**Version 0.4**] :: Added the description of the different architectural styles that were considered and their brief comparison.
- [24/11/2016] [**Version 1.0**] :: Added high view of the components of the system with a detailed description, subsubsection 2.3.1.
- [24/11/2016] [**Version 1.1**] :: Added two detailed component diagrams, subsubsection 2.3.2.
- [25/11/2016] [**Version 1.2**] :: Added the deployment diagram and its description, subsection 2.4.
- [26-27/11/2016] [**Version 1.3**] :: Added three runtime views with the respective description (login, reservation and end of the service), subsubsections 2.5.1, 2.5.2, 2.5.3.
- [28/11/2016][**Version 1.4**] :: Added runtime diagram of the service temporarily stop by, subsubsection 2.5.4.
- [28/11/2016][**Version 1.5**] :: Added runtime diagram of an emergency handling, subsubsection 2.5.5 and rewriting of section 2.7, including the addition of Protocols subsubsection, 2.7.2.

3.3 Hours of work

Matteo Frosi

[Before 21/11/2016]: 3.00 hours (spent in analyzing well known architectures, to study and apply them at our problem).

[21/11/2016]: 2.00 hours (further analysis of an applicable architecture to our problem, alleging to the classic 3 Tier architectures).

[21/11/2016]: 1.00 hours (writing of the first part of the document).

[23/11/2016]: 2.00 hours (writing of the overview section of the document and drawing of architectures images)

[24/11/2016]: 2.00 hours (drawing up of the component view and writing of the component high view section)

[24/11/2016]: 2.30 hours (drawing of the component in a more detailed view)

[25/11/2016]: 1.00 hours (writing of the section about the detailed component diagrams)

[25/11/2016]: 3.00 hours (thinking, drawing and deploying the deployment diagram)

[26-27/11/2016]: 4.00 hours (thinking, drawing and describing three runtime views, of Version 1.3)

[28/11/2016]: 1.30 hours (addition of the fourth runtime diagram)

[28/11/2016]: 1.00 hours (rewriting of subsection 2.7 and addition of subsubsection 2.7.2)

TOTAL: 23.00 hours

Luca Costa

[Before 21/11/2016]: 2.30 hours (spent learning about the various architectures and apply them to our problem)

[22/11/16]: 1.00 hours (spent learning about a possible implementation of the different architecture styles)

[23/11/16]: 2.30 hours (spent writing comparison between architectures and informing about DD document in general)

[24/11/2016]: 2.00 hours (learning about how to draw a component diagram and its effective first drawing)

TOTAL: 8 hours