Alexander Badju, Fredrik Helander, Jonathan Klingberg, Jonathan Knorn, David Lundberg, Niklas Sjöberg
7/12-14

Software Requirements Specification R2

Group F - Steve's Angels

Contents

List of Figures

1 Introduction

The car manufacturer LADA are worried about losing market shares and through their new product, a selfdriving car, they hope to maintain their position on the global car market. LADA themselves do not feel that they can produce a requirement specification to the quality standard they know is needed, which is why they have hired our company, Steve's Angels, to produce the requirements specification for the autonomous system called CRASH.

2 Background and goals

2.1 Main goals

The goal is to deliver an autonomous vehicle system to the car manufacturer LADA. As the car manufacturing industry develops, it is of great importance to keep up with the latest progress in terms of technology. Introducing new technology to the market is one way to maintain or expand market shares. The system we develop is LADA's answer to the current market situation.

The system must provide maximum traffic safety using the very latest achievements in the fields of navigation and anti-collision technology. This together with high passenger comfortability and excellent fuel economy will place LADA ahead of its competition.

3 Actors and their objectives

To get a better understanding of the actors and their objectives see the context diagram in figure 1 on page 2.

Passenger There are two types of passengers, a passive passenger or an authenticated passenger. Both can press the emergency stop button, but only the authenticated passenger can ride in the car alone.
Driver Can do anything that a passenger can. The driver can also drive the car manually, handle the voice control as well as choosing the destination.
Owner Can do anything that a driver can. The owner also handles user management. Which users are allowed to be drivers and passengers.
Administrator Can do anything that an owner can. The administrator can change the system settings as well as general admin management

4 Terminology

The system - Throughout this document we will use the term "The System" when referring to CRASH.
Autonomous car - An autonomous car is also known as a self driving car.
The system - The delivered product. When nothing else is stated, requirements are specified for autonomous driving mode.
Ecodriving - Ecodriving is a term used to describe energy efficient use of vehicles. It is a great and easy way to reduce fuel consumption from road transport

so that less fuel is used to travel the same distance.
Unsafe state - The unsafe state is the cars state when it does not fulfill Swedish car inspection regulations.
GPS - Global Positioning System based on space satellite communication.

The requirements are named in the following manner:

GoXX - Goal requirements
DoXX - Domain requirements
FPrXX - Functional Product requirements
DPrXX - Data Product requirements
DeXX - Design requirements
QuXX - Quality requirements

5 Context diagram

A context diagram of the system can be seen in Figure 1.

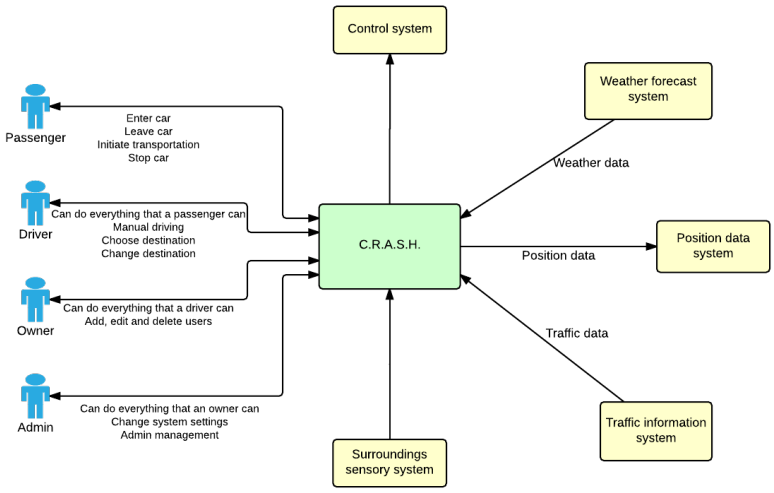


Figure 1: Context diagram with actors and key components within the system.

5.1 Context diagram description

Control system - A system that interprets data from the surroundings sensory systems, and identifies appropriate navigation paths, obstacles, traffic lights and signage.
Weather forecast system - A system that can provide weather forecasts that the car can download and use to warn about dangerous weather conditions along the current route.

Position data system - A system where the car can upload its current position. Used by the owner to locate the cars position and follow it along its path.
Traffic information system - A system that keeps track of the current traffic situation (e.g. accidents, queues etc).
Surroundings sensory system - A system that consists of several different sensors that senses the cars surroundings.

6 Scenarios

Scenarios are used to improve developer intuition. The described scenarios are so called vivid scenarios, they consist of a case story illustrating one or more user tasks. It is important to note that vivid scenarios are not suitable as test cases.

6.1 Scenario 1

Niklas Sjöberg is an owner of a CRASH-supported car and his football practice is over. He now remotely tells his car to pick him and his friends up at the football pitch, he uses his phone and the CRASH-application. The next step is that the car drives to pick up Niklas and his friends. When the car arrives, Niklas authenticates himself. When the authentication is done, Niklas and his friends enter the car and Niklas tells the car where to drive using voice control, when this is done, the car drives the passengers to the given addresses. One of Niklas' friends lives further away than Niklas himself and he is tired and he wants to be dropped off first. Since Niklas was the official "Driver" and now leaves the car, the passenger left in the car has to authenticate himself and thus becomes a authenticated passenger.

6.2 Scenario 2

Jonathan Klingberg is an Owner of a CRASH-supported car and he is at work when something very important has come up, which means that he cannot pick up his daughter at school as planned. Instead he uses his phone to remotely tell his car to pick up his child. The child receives a notification on her phone from the car that it is on its way for a pick up and how long it should take to arrive. When the car arrives, Jonathan's daughter authenticates herself and enters the car. The car drives the child home with the fathers predetermined route input.

6.3 Scenario 3

David Lundberg is at his local LADA dealership to purchase a new LADA with the inbuilt CRASH system. At the dealership David's fingerprint is configured and associated with the owner profile in the new car. The fingerprint is stored in LADA's database. David connects to his new car by scanning his fingerprint on his phone using the CRASH-application that he downloaded earlier. In the mobile application he assigns driver permissions to his son Alexander by letting him scan his fingerprint on David's phone. Alexander's fingerprint is stored in LADA's database and associated with David's car. Alexander authenticates

himself as well and enters David's car. David enters the car without authentication. David specifies a new destination to the car via voice command and the LADA car drives to the given destination.

7 Tasks

Tasks are, in contrast to vivid scenarios, suitable as test cases. A task should finish with a meaningful goal. It is important that completing the task makes the user feel that something as been achieved.

7.1 Task 1

Task: Authenticate user A.
Purpose: Authenticate A to retrieve user permissions.
Trigger: A presses the fingerprint verifier on mobile device or on vehicle.

Variants:
- 1a. A is admin
- 1b. A is owner
- 1c. A is driver
- 1d. A is passenger with special permissions
- 2. A is denied access

7.2 Task 2

Task: User A specifies a destination to CRASH.
Purpose: Tell the system to drive from one place to another.
Precondition: A is inside the vehicle. The vehicle has no specified destination.
Trigger: A gives a command via voice command or touch screen.

Variants:
- 1. Command accepted, CRASH confirms the destination and drives A to the requested destination.
- 2a. Command rejected, the requested destination does not exist.
- 2b. Command rejected, no one in the car is authorized.
- 2c. Command rejected, CRASH has no GPS connection.

7.3 Task 3

Task: User A specifies a new destination to CRASH.
Purpose: Tell the system to drive from one place to another.
Precondition: A is inside the vehicle. The vehicle already has a specified destination.
Trigger: A gives a command via voice command or touch screen.

Variants:

1 Command accepted, CRASH asks user for confirmation.
- 1a. A confirms, CRASH drives A to the requested destination.
- 1b. A rejects. CRASH will not change the destination.

2a. Command rejected, the requested destination does not exist.

2b. Command rejected, no one in the car is authorized.

2b. Command rejected, CRASH has no GPS connection.

7.4 Task 4

Task: User A attempts to drive the vehicle manually.
Purpose: A requests to drive the vehicle manually.
Precondition: The vehicle is not moving.
Trigger: A selects manual mode via touchscreen or voice command.

Subtasks:

1. A authenticates using fingerprint.
2. A uses the breathalyser.

Variants:

1. A is authenticated and gains access to manual control mode.

2a. A is denied access due to lack of manual control permission.

2b. A is denied access due to recent alcohol consumption.

7.5 Task 5

Task: User A specifies a destination from a distance.
Purpose: Request the system to drive from one place to another.
Precondition: A is outside the vehicle and has remote access permissions via mobile device.
Trigger: A starts the application on mobile device.

Subtasks:

1. A authenticates to mobile device using fingerprint.
2. A specifies a destination using voice command or touch screen on mobile device.

Variants:

1a. A is granted access to mobile application and CRASH accepts the given command.

1b. A is granted access to mobile application but voice command is not accepted.

2. A is denied access to mobile application due to lack of remote access permission.

7.6 Task 6

Task: The system adapts to- and informs user of current weather situation.
Purpose: Avoid danger caused by weather.
Precondition: The vehicle is not moving. User A has drive permissions.
Trigger: A specifies a new destination to the system using command.

Variants:
- 1a. The system accepts the command and drives to destination.
- 1b. The system informs A of dangerous weather conditions, however, command is still accepted.
- 2. The system informs A of dangerous weather conditions and rejects drive command.

8 Virtual Windows

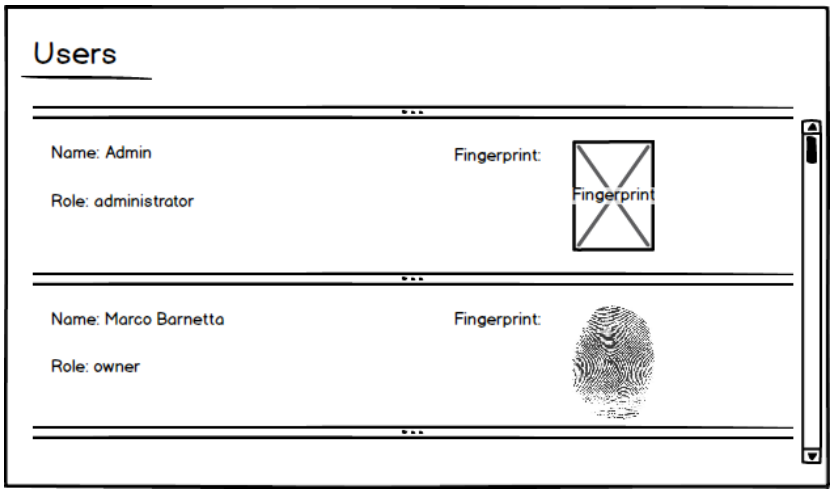


Figure 2: Virtual window that shows the data to be stored regarding users.

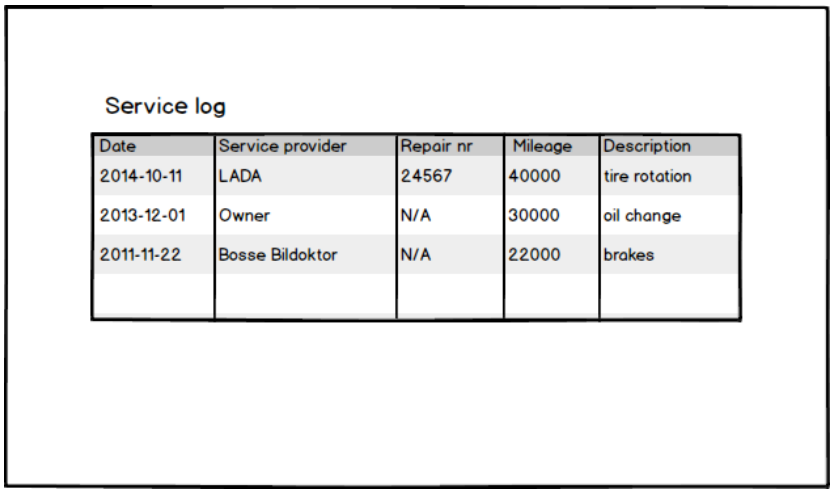
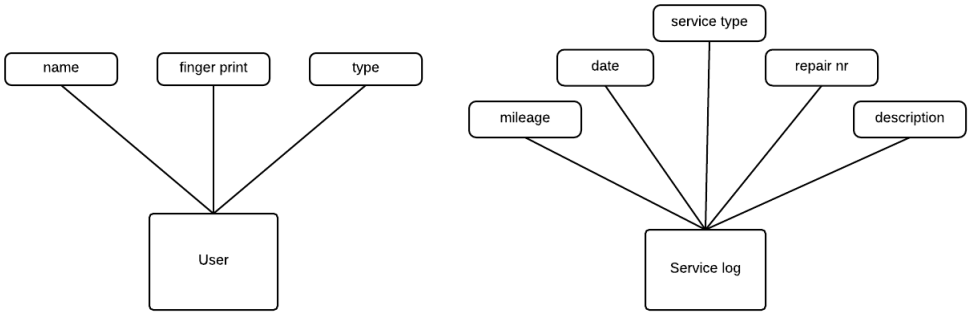


Figure 3: Virtual window that shows the data to be stored regarding service logs.

9 E/R diagram



(a) E/R diagram of the users table. (b) ER diagram of the service log table.

Figure 4: E/R diagrams of the database.

10 Domain requirements

```
Domain Do1
  Spec The system must adhere to Swedish traffic laws as long as an
       accident is not imminent
Domain Do2
```

```
  Spec If an accident can be avoided, the system may break traffic
      laws
Domain Do3
  Spec When the car is in an unsafe state the car must not be able/
      allowed to drive in automatic mode
Domain Do4
  Spec In the situation of an accident, the system must prioritize
      risks in the following order:
  Domain Do4a
    Spec Saving as many human lives as possible has top priority
  Domain Do4b
    Spec Protecting humans inside the car is prioritized over
        humans outside the car
Domain Do5
  Spec The system requires sensors for monitoring the road and
      surroundings
Domain Do6
  Spec The system requires a network connection
Domain Do7
  Spec The system requires a positioning instrument
Domain Do8
  Spec The system requires a intoxication measuring instrument
Domain Do9
  Spec The system requires an authentication sensor
Domain Do10
  Spec The system requires a voice input device
Domain Do11
  Spec The system functions without a GPS-signal once a route has
      been chosen
Domain Do12
  Spec The system needs a GPS-signal when starting on a new route
Domain Do13
  Spec The system must ecodrive when it is possible without risking
      safety
Domain Do14
  Spec All user interaction that is available in the system must be
      possible to enter remotely
Domain Do15
  Spec The system must support:
  Domain Do15a
    Spec Permanent user rights
  Domain Do15b
    Spec Temporary user rights
Domain Do16
  Spec The system must support the following authorized user types:
  Domain Do16a
    Spec Passenger
  Domain Do16b
    Spec Driver
  Domain Do16c
    Spec Owner
  Domain Do16d
    Spec Admin
Domain Do17
  Spec A driver must be able to choose & change destination
Domain Do18
```

Spec An owner has the same rights as a driver and must also be able to handle users

Domain Do19

Spec An admin must have the same rights as an owner and the admin must be able to change system settings

Domain Do20

Spec The system must support the functionality in the context diagram in figure 1

11 Quality requirements

Quality Qu1

Spec The system must query for new system and database updates at least once a day

Quality Qu2

Spec The system must query for new car inspection rules/ regulations online at least once a day

Quality Qu3

Spec System updates must only be performed when the car is parked

Quality Qu4

Spec Traffic and weather data must be fetched every minute when an Internet connection is available

Quality Qu5

Spec The car always needs to have fuel left in the tank to be able to drive to the nearest gas station when calculating the route the user has put in the system

Quality Qu6

Spec The system must respond to a potential accident before the accident is unavoidable

Quality Qu7

Spec The Internet connection must be fast enough to download the weather and traffic information within 1 minute

Quality Qu8

Spec When the emergency break is activated the system must start to process the request within 100 ms

Quality Qu9

Spec The sensors that monitor the road and surroundings must have a margin of error less than 0.01 %

Quality Qu10

Spec Ecodriving must be performed according to the current definition by Sveriges Trafikskolors Riksf rbund

Quality Qu11

Spec When a command is entered remotely, the system must send a confirmation to the user that sent the command

Quality Qu12

Spec Any dangerous weather conditions must be notified when a route is selected, before a route is commenced

Quality Qu13

Spec The service log must store data about date, service type, service provider, mileage and description from every service done on the car

Quality Qu14

Spec The margin of error for the voice control system must be lower than 1 %

Quality Qu15

Spec The GPS system must be precise to within 1 meter

Quality Qu16

Spec The system must query for updates to its maps once a day
Quality Qu17
Spec The maps must be precise, compared to the reality, to within 3 meters
Quality Qu18
Spec The dashboard control must be precise to within 0.5 mm from the touch point of the user
Quality Qu19
Spec The touch screen responsiveness must be instant
Quality Qu20
Spec The system response time must be lower than 100 ms

12 Product requirements

12.1 Functional product requirements

Product FPr1
Spec The system has to to retrieve current and future weather data from the Internet when a connection is available
Product FPr2
Spec The system must give a warning when dangerous weather conditions are predicted along the planned route
Product FPr3
Spec The system has to retrieve data of current and future traffic situations when an Internet connection is available
Product FPr4
Spec The system must always be possible to stop via an emergency-break
Product FPr5
Spec It must always be possible to request to turn off the autonomous system and drive the car manually
Product FPr6
Spec When manual driving has been requested, the car has to be standing still before the autonomous system is turned off
Product FPr7
Spec For a passenger to be able to drive the car manually, the person must pass the intoxication test
Product FPr8
Spec The intoxication test has to be configured according to Swedish traffic law
Product FPr9
Spec The system has to support voice controlled input
Product FPr10
Spec The system has to support input from the car's dashboard
Product FPr11
Spec The system has to be able to evaluate the car's status compared to current Swedish car inspection rules before driving off
Product FPr12
Spec The system has to order a towing service when it is in an unsafe state
Product FPr13
Spec When the system is in manual driving mode, the system must still be active and avoid accidents the same way as in autonomous mode

```
Product FPr14
  Spec When a command is entered feedback must be provided to the
      user
Product FPr15
  Spec The car must evaluate the amount of fuel left in the tank
Product FPr16
  Spec When the fuel level in the car reaches the level where it
      cannot make it to the second nearest gas station along the
      route, the car must drive to the nearest gas station and
      reload with fuel
Product FPr17
  Spec If the voice control system cannot interpret an incoming
      voice command, it must suggest to the user what it
      interpreted
Product FPr18
  Spec The system must be able to drive with its sensor when the
      GPS and maps don't align with the reality
Product FPr19
  Spec When the emergency break is activated the system must stop
      completely at the earliest possible place without risking an
      accident and stay still until a new command is provided by an
       authenticated user
Product FPr20
  Spec Traffic surroundings must be analyzed and taken into account
       in the decision making process
Product FPr21
  Spec Road irregularities must be analyzed to give the passengers
      a safe and comfortable ride
Product FPr22
  Spec To turn off the CRASH system the car must not be moving
Product FPr23
  Spec The positioning instrument must be used in the calculations
      for the route
Product FPr24
  Spec The positioning instrument must be used to remotely localize
       the car
Product FPr25
  Spec The authentication sensor must be used to authenticate the
      users
Product FPr26
  Spec The cars coordinates must be able to be pushed to a
      centralized server
Product FPr27
  Spec The system must be able to install stored future system
      updates at a given date
Product FPr28
  Spec The system is able to drive until the next connecting road
      without a GPS-signal
```

12.2 Data product requirements

```
Product DPr1
  Spec The system must store the following user data:
  Product DPr1a
    Spec Name
  Product DPr1b
    Spec User type
```

```
  Product DPr1c
    Spec Fingerprint
Product DPr2
  Spec The system must store route data
Product DPr3
  Spec The system must store a service log
Product DPr4
  Spec The system must be able to store future system updates
Product DPr5
  Spec The database must store current Swedish car inspection rules
       and regulations
Product DPr6
  Spec If there are users in the car, at least one needs to be
      authenticated
Product DPr7
  Spec The service log must contain the following data: date,
      repair nr, service provider, mileage, description
Product DPr8
  Spec The database must store the service log-entries in the way
      described in figure 3
Product DPr9
  Spec The database must store the user-entries in the way
      described in figure 2
```

13 Design requirements

```
Design De1
  Spec The touch screen must have brightness settings
Design De2
  Spec The touch screen must be easily readable
Design De3
  Spec The emergency break function must be easily accessible from
      all seats in the car
Design De4
  Spec The emergency break function must be easy to find
Design De5
  Spec The emergency break function must be easy to press
Design De6
  Spec The voice control system must be intuitive, resembling human
       communication
Design De7
  Spec Changing to manual mode must be easy
```

14 Goal requirements

```
Goal Go1
  Spec Autonomous car for Swedish traffic
Goal Go2
  Spec Reduce amount of traffic accidents on Swedish roads
Goal Go3
  Spec Maintain industry market shares
Goal Go4
  Spec Achieve maximal usability
Goal Go5
  Spec Avoid human deaths in traffic
Goal Go6
```

```
  Spec Achieve maximal security
Goal Go7
  Spec Expand to other markets than private use
Goal Go8
  Spec Achieve maximum comfort
Goal Go9
  Spec Reduce cars' negative impacts on the environment
```

References

[1] CRASH - Comfort, Reliability and Self Handling, Project Mission v2