SafeStreet
RASD document

Dario Miceli Pranio
Pierriccardo Olivieri

Academic year: 2019 - 2020

POLITECNICO
MILANO 1863

Contents

1 Introduction **2**

1.1 Purpose 2

1.2 Scope 2

1.2.1 World Phenomena 2

1.2.2 Shared Phenomena 3

1.2.3 Machine Phenomena 3

1.3 Definitions, acronyms, abbreviations 3

1.3.1 Definitions 3

1.3.2 Acronyms 3

1.3.3 Abbreviations 4

1.4 Revision History 4

1.5 Reference documents 4

1.6 Document Structure 4

2 Overall Description **4**

2.1 Product perspective 4

2.1.1 World Phenomena 4

2.1.2 Machine Phenomena 4

2.1.3 Shared Phenomena 4

2.2 Product functions 5

2.2.1 5

2.3 User characteristics 5

2.3.1 5

2.4 Assumption and Dependencies Constraints 5

2.4.1 Assumption 5

2.4.2 Dependencies 5

2.4.3 Constraints 5

3 Specific Requirements **6**

3.1 External Interface Requirements 6

3.1.1 User Interfaces 6

3.1.2 Hardware Interfaces 6

3.1.3 Software Interfaces 6

3.1.4 Communication Interfaces 6

3.2 Functional Requirements 6

3.3 Performance Requirements 6

3.4 Design Constraints 6

3.4.1 Standards compliance 6

3.4.2 Hardware limitations 6

3.5 Software System Attributes 6

3.5.1 Reliability 6

3.5.2 Availability 6

3.5.3 Security 6

3.5.4 Maintainability 6

3.5.5 Portability 6

4 Formal Analysis with Alloy **6**

5 Efforts **6**

1 Introduction

This is the RASD document for *SafeStreet*, it provides a general view about key aspects of the project. The purpose of this document is to formalize a description of the system's requirements both functional and non-funcional. In the following pages will be covered goals of the application with respect to phenomena. This document is addressed to developers as a guideline to implement the requirements that follows.

1.1 Purpose

SafeStreets is a service that aims to provide users with the possibility to notify authorities when traffic violations occur, and in particular parking violations. The application's goal is achieved by allowing users to share photo, position, date, time and type of violation and by enabling *Authorities* to request them.

Safestreets requires the users to create an account to access its services, the functionalities unlocked after registration depend on the type of account created.
If a user creates an account as *Citizen*, he/she must provide information about ID card on order to prove that he/she is a real person. Furthermore, he must provide an email with which he will be uniquely identified and a password. Once the account has been activated, user can finally start to report parking violation. The users can also see a summary of the streets with the highest frequency of violations.

On the other hand, an officer will create an account as *Authority* and he will need to provide his name, surname, work's Matricola, a password and as for *Citizen*, will be uniquely identified by an email. Once the Matricola has been verified and the account has been activated, the officer can retrieve the potential parking violations sent by *Citizen* that have not been taken into account yet by other officers, analyze them and, if it is the right case, generate traffic tickets. *Authorities* can also see a summary of the vehicles' license plate that commit the most violations.

From this brief description of the functionalities we may extract the following goals for SafeStreets:

- **[G1]**: allow users to be identified as a *Citizen* or as *Authority*;
- **[G2]**: allow *Citizens* to report parking violations;
- **[G3]**: *Citizen* has to be able to input information about the violation that he has reported;
- **[G4]**: must provide a visualization of the streets with high frequency of violations and vehicles' license plate that commit the most violations;
- **[G5]**: *Authority* can retrieve traffic violantions' data inserted by *Citizens*

1.2 Scope

Here we will describe all the relevant phenomena that may occur.

1.2.1 World Phenomena

Those are the events that may occur in the real word and are not affected by the Machine.
We identify:

- *Citizen* sees a parking violation and wants to report it;
- *Authorities* want to know about some violations that have been occurred;
- A *parking violation* occurs;

1.2.2 Shared Phenomena

Shared phenomena are the events based on the link beetween World Phenomena and Machine Phenomena. We can distinguish them in two types:
Controlled by the world observed by the machine:

- A Citizen take a photo of a violation;
- Users can enter data for registration/login;
- Users can request data;

Controlled by the machine observed by the world:

- track position of the violation;
- mark areas with an high rate of violations;
- System can fullfill data requests;

1.2.3 Machine Phenomena

The Machine Phenomena are the events that occur inside the machine and are not affected by the real world.
We identify:

- storing permanently collected data;
- encryption of sensitive data;
- retrieving data for a request;

1.3 Definitions, acronyms, abbreviations

1.3.1 Definitions

- user: can be either citizen or authorities

traffic violation: generic violation that can occur in a street parking violation: a violation caused by a bad parking violation: general violation, identity both traffic or parking violation unsafe areas: areas with an high rate of violations

1.3.2 Acronyms

Table with all acronyms used in document.

ACRONYM	COMPLETE NAME
RASD	Requirements Analysis and Specification Document
GPS	global positioning systems
ID	Identity document
S2B	Software to be
GDPR	General Data Protection Regulation

1.3.3 Abbreviations

1.4 Revision History

1.5 Reference documents

1.6 Document Structure

- **Chapter 2:**
- **Chapter 3:**
- **Chapter 4:**

2 Overall Description

2.1 Product perspective

This section aims to explain in more detail the World, Machine and Shared Phenomena described in the previous Chapter.

2.1.1 World Phenomena

2.1.2 Machine Phenomena

- **Storing permanently collected data:** The system needs to store, in a secure way, all the data submitted. In order to achive this purpose and guarantee the best service the system needs to use a DBMS.
- **Encryption of sensitive data:** Personal user's data and all the data relative to the violations that can only be seen by authorities need to be encrypted in order to proctect it from non-allowed third parties.
- **Retrieving data for a request:** System have to fullfill the data request from the users. Data requests can be of two types, a Citizen request who want to see statistics of a certain city area or data request by Authorities who want to receive the violation reports collected by SafeStreet

2.1.3 Shared Phenomena

Controlled by the Machine observed by the World

- **A Citizen take a photo of a violation:** Situation in which a Citizen spots a generic violation and wants to report it through the application. Using the phone camera he can take the photo of the violation.
- **User can enter data for registration/login:** A user decide to use the application and provides his personal in order to register if it's the first time he use the app, or to identify himself.
- **Users can request data:** In this phenomena we make a distinction between Citizen and Authorities. A Citizen or may want to see violation statistics of a certain area, or in the case of Authorities they can, request violation statistics and additional informations

Controlled by the World observed by the Machine

-

2.2 Product functions

2.2.1

2.3 User characteristics

Below we describe the convention used to identify the user of the application and the function that those users are allow to perform.

- **Guest:** A user that have donwload the application but is not registered yet. This type of user is not allowed to access the application functionalities.
- **Citizen:** is a generic user app not related to authorities, a common Citizen that want to use the application. After the registration process and the validation of the ID card provided He can log in the application and use the functionalities: - report a violation - request informations about the statistics of a certain area.
- **Authorities:** This user is associated to the local municipal police district, any traffic warden, once registered with is matricola number and logged in have access to those functionalities: - request informations about the statistics of a certain area. - request all the violations reported from Citizens.
- **User:** can be both a Citizen or Authority type, in this document this name is used when it's not necessary make a distinction between the two.

2.4 Assumption and Dependencies Constraints

2.4.1 Assumption

The following list present all the domain assumption made.

- **[D1]**: Users can't make more than one account.
- **[D2]**: The Citizen assumes all responsibility for misrepresentation.
- **[D3]**: Citizens who use the application are evenly distributed in any city area.
- **[D4]**: The ID card present by the Citizen during the registration is valid.
- **[D5]**: All the violantions reported are valid.
- **[D6]**: The S2B allows to take photos from the application.

2.4.2 Dependencies

This list below represent all the dependencies that S2B need in order to work properly.

- A internet connection.
- A Photocamera (with a minimum precision of 3Mp ?(non so se va messo, algoritmo può non riconoscere low quality foto))
- A GPS.
- A Trusted external Storage for violantions data

2.4.3 Constraints

- The S2B must guarantee the European data protection GDPR for user's sensitive data.
- The S2B will be used only in Italy due to personal data type like (fiscal code and police matricola).

3 Specific Requirements

3.1 External Interface Requirements

3.1.1 User Interfaces

3.1.2 Hardware Interfaces

3.1.3 Software Interfaces

3.1.4 Communication Interfaces

3.2 Functional Requirements

3.3 Performance Requirements

3.4 Design Constraints

3.4.1 Standards compliance

3.4.2 Hardware limitations

3.5 Software System Attributes

3.5.1 Reliability

3.5.2 Availability

3.5.3 Security

3.5.4 Maintainability

3.5.5 Portability

4 Formal Analysis with Alloy

5 Efforts