

Software Engineering 2

A.Y. 2019/2020

**SafeStreets**

RASD – Requirement Analysis and Specification Document

Version 1.0

**Authors:**

Daniele Comi 10528029 - 944534  
Anton Ghobryal 10501942 - 945577

**Professor:**

Elisabetta Di Nitto

Contents

[1. Introduction 3](#_Toc22478870)

[1.1 Purpose 3](#_Toc22478871)

[1.2 Scope 3](#_Toc22478872)

[1.3 Definitions, Acronyms, Abbreviations 3](#_Toc22478873)

[1.4 Revision history 3](#_Toc22478874)

[1.5 Reference Documents 3](#_Toc22478875)

[1.6 Document Structure 3](#_Toc22478876)

[2. Overall description 3](#_Toc22478877)

[2.1 Product perspective 3](#_Toc22478878)

[2.2 Product functions 3](#_Toc22478879)

[2.3 User characteristics 3](#_Toc22478880)

[2.4 Assumptions, dependencies and constraints 3](#_Toc22478881)

[3. Specific requirements 4](#_Toc22478882)

[3.1 External Interface Requirements 4](#_Toc22478883)

[3.1.1 User interfaces 4](#_Toc22478884)

[3.1.2 Hardware Interfaces 4](#_Toc22478885)

[3.1.3 Software Interfaces 4](#_Toc22478886)

[3.1.4 Communication Interfaces 4](#_Toc22478887)

[3.2 Functional Requirements 4](#_Toc22478888)

[3.3 Performance Requirements 4](#_Toc22478889)

[3.4 Design Constraints 4](#_Toc22478890)

[3.4.1 Standards compliance 4](#_Toc22478891)

[3.4.2 Hardware limitations 4](#_Toc22478892)

[3.4.3 Any other constraint 4](#_Toc22478893)

[3.5 Software System Attributes 4](#_Toc22478894)

[3.5.1 Availability 4](#_Toc22478895)

[3.5.2 Security 4](#_Toc22478896)

[3.5.3 Maintainability 4](#_Toc22478897)

[3.5.4 Portability 4](#_Toc22478898)

[4. Formal Analysis using Alloy 4](#_Toc22478899)

[5. Effort spent 4](#_Toc22478900)

[6. References 4](#_Toc22478901)

# Introduction

## Purpose

### 1.1.1 General Purpose

SafeStreets is a crowded-sourced application that intends to provide users with the possibility to notify authorities when traffic violations occur, specifically parking violations. The application allows users to send pictures of violations, including their date, time, and position, to authorities. The main purpose of SafeStreets is to reduce the number of accidents that may be caused by certain violations that can be avoided easily. The following examples may illustrate and visualize the type of violations that may be captured and notified to the authorities:

* Double parking
* Expiry of the parking time limit
* No parking area
* Parking in places reserved to people with disabilities
* Parking in the middle of bike lanes
* Parking near bus stops
* Parking on crosswalk
* Parking on residents reserved spots
* Parking ticket missing
* Possible vehicles damage by third parties (e.g. broken glass)

SafeStreets stores the information provided by the users, completing it with suitable metadata. In particular, when it receives a picture, it runs an algorithm to read the licence plate and stores the retrieved information with the violation, including also the type of violation (input by the user) and the name of the street where the violation occurred (which can be retrieved from the geographical position of the violation). In addition, the application allows both end users and authorities to mine the information that has been received, for example by highlighting the streets (or the areas) with the highest frequency of violations, or the vehicles that commit the most violations. Of course, different levels of visibility are offered to different roles, for example the authorities can see the licence plate numbers of the vehicles that commit any violation while the end user cannot see that.

Moreover, there’s another functionality that can be provided by SafeStreets. If the municipality offers a service that allows users to retrieve the information about accidents that occur on the territory of the municipality, SafeStreets can cross that information with its own data to identify potentially unsafe areas, hence suggest possible interventions depending of the type of the most committed violation in that area. The following examples show which intervention could be suggested depending on the preceding examples of violations presented earlier in this paragraph:

* Add a barrier between the bike lane and the part of the road for motorized vehicles
* Install a towaway zone sign
* Increase parking slots
* Increase local police controls

The main purpose of this functionality is that SafeStreets also identifies areas with critical number of accidents and reports suggestions as a possible solution as an automatized method to engage with the problem. Thus, it could help the authorities to highlight where the interventions should be provided, and this functionality should make it easier to point out the areas with critical statistics. So, if the municipality provide the needed information, it helps with the traceability of the main problem, therefore handling it providing also a higher measurement on local security.

### 1.1.2 Goals

Taking the abstraction as an outcome of the “real-world” only, we should be able to define the goals as a part of the requirement engineering of an S2B to satisfy the stakeholders’ requests:

* [G1] Every registered user should be able to notify violations
* [G2] Every recognized authority should be able to access the application
* [G3] Every recognized authority should be able to receive any violation that has been pointed out by a registered user
* [G4] Every communication from the user must include a violation that has been committed by a recognizable vehicle
* [G5] Every registered end user should be able to mine general information about the violations committed in a certain area
* [G6] Every recognized authority must be able to verify the notified violations by the registered users
* [G7] Every recognized authority must be able to receive suggestions about improving the local security

Reading these goals, we should acknowledge the fact that the system considers two most end users: the normal user and the authorities. They’ll be defined later on.

## 1.2 Scope



SafeStreets is meant to help authorities to identify some serious violations, traffic and parking violations, that may cause accidents in the future being. Thus, as it’s been called, it’s intended for making streets safer. Also, this application will increase the efficiency on reporting violations with the help of a common citizen. In order to report a violation, citizens won’t have to go to a police station (that might be far from the current position of the violation), they won’t even have to search where they are in order to report formally the committed violation. There are also some assumptions made in order to satisfy the goals of the S2B and the fundamental requirements that would help the lower level to easily realize the implementation part without considering the research on some tech already defined and available for use, also for higher level perspectives, for future improvements; thus it will be easier to integrate some new tech inherent to the domain of the application.

SafeStreets allow users to report a violation to the authorities when they spot one. In order to obtain the ability of using SafeStreets the user will have to register himself into the application system. Users have two different modes to register themselves into the system: the first one is the proprietary authentication and the second one consists of SPID authentication. Generally, they will have to subscribe with their full name and fiscal code since they’re mandatory to be able to fill certain reports. Registered Users obtain points that indicate their integrity through their continuous voluntaristic participation in order to provide the possibility of achieving the goal of making the streets safer. These points are called integrity points. Initially, users, who have registered with SPID, have more integrity points than the proprietary authentication (according to demonstrating more integrity into the society verifying his own identity through a public system of digital authentication). Moreover, when a report is verified by the authorities, integrity points of the notifier increase. Users can see also, through a map, the security level of a zone. Actually, allowing users to mine general information about notified violations doesn’t violate the privacy of the reporting user according to the Legislative Decree 196/03 and the regulation 2016/679 given since they aren’t authorized to access other users’ private information such as fiscal code, name, surname etc. Security level is calculated being based on the statistics of the types of violations committed in the interested area.

As it is in the specification of the S2B, Reports are composed of date, time, position, a note (with a maximum fixed number of characters) and a clear picture of the committed violation in which the licence plate should be included, but it isn’t a restricted requirement because, in the worst case, there are two possible situations: in the first one the licence plate isn’t clear (e.g. poor quality or blurry image) the user is allowed to do one out of two possible actions that consist of re-take the picture of the violation or modify the licence plate number, and if the user chooses to do the second action, the system shall recognize the report as one, instead, with a modified licence plate number and this induces minor level of credibility; instead, in the second situation, if the system doesn’t recognize a vehicle in the taken picture it will take an immediate action to discard this picture and it will eventually ask the user to take a new clearer picture to be able to proceed, and that precludes the fact that user might send pictures that are not in accordance with the domain of the application (e.g. photos that don’t contain a vehicle such as selfies).

Since the violation must be notified in real-time domain, the user is not allowed to upload a picture at all. So that, situations as creating a false violation or manipulating data of a certain violation. For the same reason the user is not allowed to modify a photo. If the user notices something that should be mentioned, there’s a note that he can fill in briefly with possible observations. Also, the user must have a stable active connection to be able to submit the violation.

A report should satisfy the application domain before it becomes in hands of authorities and in order to realize this fact a report should include the preconditions described earlier. When a report is filled in completely the authorities must be able to receive it through the application. Within this context, the authorities are defined as Italy’s law enforcement agencies. The authorities, interested in the application willing to use it for increasing local security, must have a valid digital certificate provided by the police forces through the Ministry of the Interior. An authority must register to be able to use the application. The registration process requires a valid digital certificate. Once an authority is registered, it’s able to receive notifications about the committed violations. Registered authorities have the maximum authorization to access all the data notified by users. They also have access to all normal user functionalities, thus the capability of reporting violations. The authorities can also verify and validate the visualized reports depending on the veracity of the notified violations.

Either the registration process or the reports made and of the user who carried it out are respects the terms established by the Legislative Decree 196/03 and the regulation 2016/679.

SafeStreets offers also the possibility to be an important participant as an independent entity which can provide suggestions to the improvement of a certain area. In order to realize such a functionality, SafeStreets should have access to accident records of the applied areas. Interested municipalities, in order to apply this functionality, must guarantee access to those data records because it helps the application to cross the provided data about accidents with its own data to provide suitable suggestions depending on the identified situation.

## Definitions, Acronyms, Abbreviations

### Definitions

* **Violation**: a subset of anything that is classified as a traffic violation by the Traffic regulation and laws document. This subset is composed of:
* Double parking
* Expiry of the parking time limit
* No parking area
* Parking in places reserved to people with disabilities
* Parking in the middle of bike lanes
* Parking near bus stops
* Parking on crosswalk
* Parking on residents reserved spots
* Parking ticket missing
* Possible vehicles damage by third parties (e.g. broken glass)
* **Vehicle**: any terrestrial identifiable vehicle subject to Traffic regulation and laws document, like cars, motorbikes, tirs, etc…
* **User**: any citizen registered in the system who is using any of SafeStreets functionalities.
* **Authority**: any registered law enforcement using SafeStreets application alongside its authority-restricted functionalities
* **Reliability score**: score assigned to any user account which gives a sense of how much a user I reliable in giving information regarding violations.
* **Safe area**: a low radius geographical area where violations are lower than a certain threshold or lower than other areas.
* **Suggestion**: an automatically inferred hint given to the authorities by SafeStreets regarding how they could improve, with the help and permission of their municipality, area marked as high-risk area due to a high correlation of violations and incidents reported from the same municipality.
* **Galileo**: Global localization system based on a network of 24 satellites commissioned by European Union and ESA (European Space Agency)
* **SPID**: is the unique system of access with digital identity to the online services of the Italian public administration and of private members: citizens and companies can access services with a unique digital identity in a secured way

### Acronyms

* S2B: Software to Be
* GPS: Global Positioning System
* API: Application Programming Interface
* UI: User Interface
* SPID: Public Digital Identity System
* D.L.: Legislative Decree
* DCPM: Decree of the President of the Council of Ministers of the Italian Republic
* GDPR: General Data Protection Regulation
* IEEE: Institute of Electrical and Electronics Engineers

### Abbreviations

• Gn = nth goal

• Dn = nth domain assumption

• Rn = nth requirement

## 1.4 Revision history

## 1.5 Reference Documents

* D.L. 196 del 2003 (196/03) <https://www.camera.it/parlam/leggi/deleghe/Testi/03196dl.htm>
* General Data Protection Regulation (EU) 2016/679 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>
* IEEE 830-1998 - IEEE Recommended Practice for Software Requirements Specifications <https://standards.ieee.org/standard/830-1998.html>
* IEEE 29148-2018 - ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes -- Requirements engineering <https://standards.ieee.org/standard/29148-2018.html>
* Specification document “Mandatory Project Assignment AY 2018-2019” <https://polimi365-my.sharepoint.com/:b:/g/personal/10528029_polimi_it/EXR1gN6gBoxJgMC86Ow45gMBFwZzkRSWuoaf5K7t1wZutA?e=SPnVkI>
* Ministry of the Interior and digital certificates released <http://politichepersonale.interno.it/itaindex.php?IdMat=1&IdSot=35&IdNot=386>
* Traffic regulation and laws <http://www.aci.it/i-servizi/normative/codice-della-strada.html>

## 1.6 Document Structure

* Chapter 1 is an introduction: it describes the purpose of the system informally and also by making use of the list of goals which the application has to reach. Moreover, it defines the scope, where the aim of the project is defined in greater detail and the application domain and the most important shared phenomena are shown.
* Chapter 2 offers an overall description of the project. Here the actors involved in the application’s usage lifecycle are identified and the boundaries of the project are defined, listing all the necessary assumptions. Furthermore, a class diagram is provided, aid to better understanding the general structure of the project, with all the related entities. Then some state diagrams are listed to make 10 the evolution of the crucial objects clear. Finally, the functions offered by the system are here more clearly specified, with respect to the previously listed goals.
* Chapter 3 represents the body of the document. It contains the interface requirements, which are: user interfaces, hardware interfaces and software interfaces. It then lists some scenarios to show how the system acts in real world situations, followed by the description of the functional requirements, using use cases and sequence diagrams. All the requirements necessary in order to reach the goals are given, linked with the related domain assumptions. Lastly, the non-functional requirements are defined through performance requirements, design constraints and software system attributes.
* Chapter 4 contains the Alloy model of some critical aspects with all the related comments and documentation in order to show how the project has been modelled and represented through the language.
* Chapter 5 shows the effort which each member of the group spent working on the project.

# Overall description

## Product perspective

In the below figure 2 is shown the main structure of the SafeStreets application, actually only the main parts without going too deep in the actual SafeStreets structure which is not a topic for this document.  
One of the main objectives is security. To offer two type of different authentications, an authentication manager will have as its duty to offer these two authentications as transparent as possible, of course SPID authentication will have to communicate with different server than the ones of SafeStreets. SPID servers and its authentication process will follow its documentations.  
User data has to be secured in the best way possible following directives imposed by D.L. 196/03 and the General Data Protection Regulation 2016/679, so even if not shown, for clarity reasons, in the class diagram data will indeed have to be decrypted to be seen from the application and has to be crypted when memorized in the database through SafeStreets servers to guarantee.  
A user will not ever be able to access other user restricted information, SafeStreets will grant him only the permission to explore violations signalled. Contraposed to the authority which has the legal rights to see every user data, expect obviously the authentication related ones.  
An authority to access this data will have to let its previous asked digital certificate be verified in every application session to use even just one of the main three restricted functions.

SafeStreets needs to be as fast as possible, considering the requirement to have always an available Internet connection, SafeStreets computing servers will be used for peculiar sub functionalities like live statistics computation on violations data or like the violation image validity recognizer which will be featured with the use of a Convolutional Neural Network helping authorities to have as many as possible valid violations.

Concerning valid violations to also ensure no misuse of any localization spoofing service, to upload to SafeStreets servers a new violation it will be needed that three different locations taken from GPS/Galileo system, Internet localization system and mobile cell approximate location will have to coincide within a few kilometres radius.

SafeStreets needs to be as autonomous as possible to prohibit any misuse of its violations reporting system. Indeed, even when an user needs to modify the license plate autonomously read in case of a wrong reading, the application through ViolationControl will have to lower the quality attribute of this violation due to this needed modification made by the user, even if it will result right.

Expect some note that a user can write about some violation and obviously the type of violations, editing the license, at the cost of a notified lower quality, is the only allowed edit for a violation that can be made by the user.



*Figure 2 – SafeStreets Descriptive Class Diagram*

## Product functions

In this section the most important functions and requirements are listed and explained with few more details

* Violations signaller:  
  This functionality allows the user to create a new violation record to be sent through Internet to SafeStreets server which will safely and securely memorize it in the databases.  
  The violations signaller asks to the user just to take a picture of the identifiable vehicle committing, at most of his knowledge, a violation or more precisely from one to up to three of the violations which are listed by SafeStreets.  
  The user will also need to compose a small note containing a text which length is up to 140 characters, its function is to clarify at user’s best capabilities the current situation which will eventually be controlled by authorities.  
  Any other data will be automatically filled by SafeStreets application. Like the violation position, its timestamp, vehicle license plate and the violation quality which actually depends on the latter : if a user thinks the automated license plate reading system did a wrong read due to bad angled images or other issues which could compromise OCR accuracy, he will be able to edit the license plate field at the cost of reducing violation quality for security reason.
* Safeness areas map:  
  This functionality is one of the main reasons SafeStreets idea was born. Allowing users to know how safe a certain geographically area by using every data collected about violations with the help of authority verification. Any user will be able just to open inside SafeStreets this map to have him pinpointed every area in his surroundings with its safety level regarding street traffic.  
  This will allow to make eventually, in a certain time period, streets safer and safer with a decreasing number of incidents caused by traffic violations and a constant increase of citizens happiness regarding how traffic and traffic services are managed by their municipality.  
  Of course, all this can be possible with the intervention of the authorities which will also be discussed in the following functionality how
* Suggestion inferring system:  
  This functionality is another very important one for SafeStreets: it allows authority to know which solutions they should apply, and propose to municipality council, to reduce the amount of violations committed which led to incidents reported by municipality data.  
  There will be a list of possible suggestions and they will be inferred completely autonomously by taking in account violations data notified by the users of SafeStreets and, as said before, municipality data regarding incidents.
* Automated violation validity control:  
  To help authorities doing a better job and to give them the least work possible regarding violation notified through SafeStreets, an autonomously violation validation system will be present to check if a currently composing violation notification actually a traffic violation and not something else like any other type of uncorrelated violations or anything which does not involve any violations at all, either an error or not done by the user. It will be able to recognize if the image is containing an actual identifiable vehicle and it will be able to read its license plate.
* User reliability score improvement:  
  An important functionality to improve SafeStreets efficiency in doing what’s was designed for, a reliability score is assigned to each user indicating how much a user is reliable in signalling violations. Authority can increase or decrease this score by verifying it, but it will be also done autonomously in case of multiple bad composed violation notifications.  
  A better imposed user base will improve SafeStreets purpose fulfilment.

## 2.3 User characteristics

SafeStreets requires some fundamental actors who could help in order to exploit the possibility to use all the possible functionalities to accomplish what is built for as described earlier. Those actors belong to two different categories: a normal user or a citizen and the authorities (mainly, local police). Their characteristics will be described as follows:

* User: a person who registers to SafeStreets, a citizen of the community, a passer-by who may spot a violation while he’s walking around the streets, having the possibility to report it via the application, simply taking a photo of the violation, and filling in the required data. He may register through the proprietary authentication or SPID. Data as his full name and his fiscal code are restrictedly required. He has access to his own profile on which, in addition to his own data, there will be all the violation notified followed by an integrity score which describes the credibility of the reports provided by him. He’s also allowed to make queries about other violations (obviously, without violating other users’ privacy accordingly with the terms established by the Legislative Decree 196/03 and the regulation 2016/679). He’s also allowed to visualize, through a map, the security level of a certain area and the statistics on the type committed violations.
* Authority: mainly, the authority is represented by the local police (in the domain of the application). Authorities are recognizable through a valid digital certificate which is provided by the police forces through the Ministry of the Interior, usable according to D.P.C.M. of 30.10.2014 N.193 art.21 and art.22. Once they access, they have the maximum authority to access data of the violations made respecting the terms established by the Legislative Decree 196/03 and the regulation 2016/679. They should act based on the information provided by a violation. They also receive suggestions on how to decrease the number of violations and, consequently, increase the local security. They also have access to the same functionalities as the normal users

## 2.4 Assumptions, dependencies and constraints

2.4.1 Assumptions

* + - D1: Users can identify a violation
    - D2: Authorities possess valid digital certificates provided by the police forces through the Ministry of the Interior
    - D3: Users decide to modify the licence number providing the right one if and only if the recognized licence number, through the application, isn’t the correct one
    - D4: Users have an available internet connection for the whole process of reporting a violation
    - D5: Every considered geographical area is covered by a satellite location system (e.g. GPS and Galileo)
    - D6: authority acts based on notifications about violations or suggestions about security improvement
    - D7: SafeStreets crosses data with incidents’ records based on the quantity of both its own data and data provided by the municipality

2.4.2 Dependencies

2.4.3 Constraints

# 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

[G1] Every registered user should be able to notify violations

* [R1] The user must be registered to use the application
* [R2] The user can register, and access, through two different authentication methods: SPID and proprietary authentication
* [R3] The user registered with SPID has a higher initial integrity score than a registered user with proprietary authentication
* [R4] Each user has an integrity score
* [R5] Each user can access the details of his own and view his data, integrity score and reports made
* [R6] Each registration made by a user follows the indications imposed by the Legislative Decree 196/03 and the Regulation 2016/679, which are shown to the user

[G2] Every recognized authority should be able to access the application

* [R7] Each authority can access the application through its pre-given credentials and its digital certificate provided by the police forces through the Ministry of the Interior
* [R8] Every authority can make reports
* [R9] Each authority can have access to the application features available for users without privileged access

[G3] Every recognized authority should be able to receive any violation that has been pointed out by a registered user

* [R10] Each authority has full access to the reports made
* [R11] Each authority can access the details of the report made and of the user who carried it out according to the terms established by the Legislative Decree 196/03 and the regulation 2016/679

[G4] Every communication from the user must include a violation that has been committed by a recognizable vehicle

* [R12] A report must consist of an image, date, time, location and metadata
* [R13] The metadata of a report is the type of report, the quality of the report and the notes entered by the user
* [R14] The notes entered by the user cannot be longer than 140 characters
* [R15] Date, time and location must be added automatically via the Internet and GPS/Galileo satellites
* [R16] The user can proceed with the signalling if the GPS location, if present, is inside the location through the Internet and the location through mobile network cells
* [R17] It is possible to report in the presence of an Internet connection only
* [R18] User reporting image is recognized as valid for reporting only if it contains a vehicle that can be identified through the license plate
* [R19] The system must be able to recognize the vehicle registration number
* [R20] The user can decide to modify the result of the reading of the license plate made by the system
* [R21] A warning in which the user has modified the vehicle registration number will have reported a lower quality

[G5] Every registered end user should be able to mine general information about the violations committed in a certain area

* [R22] Each user can access a map showing the security level in certain areas
* [R23] Each user can have limited access to reports by viewing information that does not violate the privacy of the reporting user according to the Legislative Decree 196/03 and the regulation 2016/679
* [R24] Each user can view statistics based on reports made in certain areas

[G6] Every recognized authority must be able to verify the notified violations by the registered users

* [R25] Authorities can indicate an alert as verified through the application
* [R26] Each alert verified by an authority will give the user who has indicated it a higher reliability score

[G7] Every recognized authority must be able to receive suggestions about improving the local security

* [R27] The system must be able to access the accident data present in a specific municipal area if present
* [R28] The system must analyse accidents and violations data to produce a suggestion to be notified to the authority to improve road safety

## 3.3 Performance Requirements

## 3.4 Design Constraints

### 3.4.1 Standards compliance

### 3.4.2 Hardware limitations

### 3.4.3 Any other constraint

## 3.5 Software System Attributes

### 3.5.1 Availability

### 3.5.2 Security

### 3.5.3 Maintainability

### 3.5.4 Portability

# Formal Analysis using Alloy

# Effort spent

# References