

Politecnico di Milano
AA 2018-2019
Computer Science and Engineering
Software Engineering 2 Project
Requirement Analysis and Specification
Document

Gargano Jacopo Pio, Giannetti Cristian, Haag Federico

2018-11-11

Contents

1	Introduction	3
1.1	Purpose	3
1.1.1	Goals	3
1.2	Scope	5
1.2.1	Analysis of shared phenomena	6
1.3	Definitions, Acronyms, Abbreviations	6
1.3.1	Definitions	6
1.3.2	Acronyms	7
1.3.3	Abbreviations	7
1.4	Revision history	7
1.5	Reference Documents	7
1.6	Document Structure	7
2	Overall description	8
2.1	Product perspective	8
2.2	Product perspective	8
2.3	Product functions	8
2.3.1	Data4Help	8
2.4	User characteristics	10
2.4.1	Data4Help	10
2.4.2	AutomatedSOS	10
2.4.3	Track4Run	10
2.5	Assumptions, Dependencies and Constraints	10
2.5.1	Domain Assumptions	10
3	Specific requirements	12
3.1	External Interface Requirements	12
3.1.1	User Interfaces	12
3.1.2	Hardware Interfaces	12
3.1.3	Software Interfaces	12
3.1.4	Communication Interfaces	12
3.2	Functional Requirements	12
3.3	Performance Requirements	12

3.4	Design Constraints	13
3.4.1	Standards compliance	13
3.4.2	Hardware limitations	13
3.4.3	Any other constraint	13
3.5	Software System Attributes	13
3.5.1	Reliability	13
3.5.2	Availability	13
3.5.3	Security	13
3.5.4	Maintainability	13
3.5.5	Portability	13
4	Formal analysis using Alloy	14
5	Effort spent	15
6	References	16

Chapter 1

Introduction

1.1 Purpose

TrackMe offers a basic B2B service named "Data4Help" on top of which are built two B2C services named "AutomatedSOS" and "Track4Run".

Data4Help: It's a service that TrackMe company is willing to develop. The basic idea is allowing third parties to monitor the location and health status of individuals through many sensors. The service is based on the retrieval of data sent by registered users. Every user has one or more sensor that sends the information to TrackMe. Then, data can be directly sent to a third party client that pays for the service and had obtained the authorization of the user, or can contribute to a anonymous dataset (composed by at least a thousands people due to company policy). Users sending data are rewarded.

AutomatedSOS: It's a service that guarantees (within a certain amount of time - 5 seconds according company policy) the call of an ambulance if the health data that is received is under a given threshold.

Track4Run: It's a service that it can be used during a running competition: organizers can define a path and runners can enroll to it enabling spectators to track them in a map.

1.1.1 Goals

- G₁ Allow a person to register as Individual after his agreement of acquirement of data by TrackMe.
- G₂ Allow a person or a company to register as third party of Data4Help.
- G₃ Manage individual request of a third party.

- G_{3.1} Allow a third party to select a person whom want to access data through his fiscal code or his social security number.
- G_{3.2} Allow the individual to accept or refuse the request.
- G_{3.3} If the Individual accept the request, his data are sent to the third party which made the request.
- G_{3.4} If the Individual does not accept the request, the third party which made the request is not able to see his data.
- G₄ Manage groups of individuals request of a third party.
 - G_{4.1} Allow a third party to select a group of people linked by one or more data.
 - G_{4.2} If the request refers to 1000 individuals or more, the request is accepted and the data are anonymized before being sent to the third party which made the request.
 - G_{4.3} If the request refers to less than 1000 individuals, the request is refused and the third party is not able to access to the data.
- G₅ Allow to a third party to access to data of individuals of whom it have permission as soon as they are produced.
- G₆ Allow to an Individual to revoke the availability of his data to a specific Third Party that has access to them.
- G₇ Allow to elderly Individuals to subscribe to AutomatedSOS.
- G₈ Monitor with smart devices the health parameters of Individuals registered to AutomatedSOS.
- G₉ Send an ambulance to the position of an Individual registered to AutomatedSOS with health parameters beyond certain intervals.
 - G_{9.1} If the health parameters registered of an Individual are beyond certain intervals, the system checks the position of the device.
 - G_{9.2} The system makes an emergency call to the local emergency number explaining the position of the Individual and the values of his non-regular health parameters.
 - G_{9.3} The emergency call is initiated within five seconds of the detection of the non-regular parameters.
- WORK IN PROGRESS

1.2 Scope

TrackMe offers its services in a world where technology and health are taking huge strides forward every day and innovation is commonplace.

Nowadays, people use smart devices such as smartphones and smart wearables more than any other object that they own. This means that any activity they perform already is or can be integrated with these devices.

TrackMe, with the introduction of Data4Help, offers the possibility to monitor users' location and health data and allows third parties to register in the system to acquire these data.

When it comes to personal data acquisition, privacy is a fundamental issue that TrackMe needs to consider. Privacy is, in fact, regulated by several laws: there are many restrictions on how user's data is acquired and stored. Therefore, TrackMe is concerned with users' consent to transferring data to TrackMe itself and to third parties for individual specific analysis. Moreover, TrackMe guarantees that anonymized data of groups of individuals are properly anonymized by checking specific constraints.

Over the course of their daily routine, users perform several actions during which their data can be analyzed to provide them with insights. For instance, they might want to monitor their heart rate while sleeping or to keep track of the distance they have walked during their day and the places they have been to.

People with a potential need for immediate assistance have always been a huge concern for their relatives and for technology makers. These may include old people with limited movement and a high chance to need urgent assistance, anyone who has a specific disease, but also a healthy individual who can suffer from a sudden heart failure. Until now, the only practical way to receive help has been to call for help, either by using a cell phone or by pushing an SOS button on a dedicated device. TrackMe proposes to automatize the step of calling for help through AutomatedSOS. In fact, when determined health values will no more be considered as normal, the system will automatically send a request for help.

Moreover, a considerable percentage of people work out on a daily basis or simply enjoy being fit through some physical exercise sporadically. Personal trainers can be helpful in providing tips and work out routines that people can follow. Doctors should periodically monitor an individual's health status, especially if they exercise. However, these not only are expensive but also, most importantly, aren't always available.

A sport practiced and loved by many is running. Organizing a run requires several steps to be taken such as defining a path, getting athletes to participate and spectators to watch it. TrackMe proposes to simplify the organization of a run, by introducing Track4Run. This service will allow the definition of a path, easy enrollment for participants and a real-time tracking of each runner's

position on a map.

1.2.1 Analysis of shared phenomena

TO DO LIST OF SHARED PHENOMENA

1. users move (or run in Track4Run)
2. users can have health problems
3. sensors collect data
4. sensors communication
5. sensors break
6. third parties collect data from the system
7. third parties registration to Data4Help
8. user grant direct usage of personal data
9. user registration (Data4Help and/or services built on top of it)
10. organizers of run define path
11. participants of run enroll to it
12. run spectators see on a map the position of runners

1.3 Definitions, Acronyms, Abbreviations

1.3.1 Definitions

Data-senders : people using Track4Help sending data from device(s)

Third parties : companies or private persons retrieving data from TrackMe

Organizers : companies or private persons organizing running competitions

Spectators : people participating as spectators to running competitions

Participants : people running in running competitions

User data : user's health data and location acquired by Data4Help and stored in a database

Smart wearables : smart devices that can be worn on the body as accessories. These devices are required to have specific sensors for data acquisition, to be compatible with the system to be (see [add reference to requirements for smart wearables](#)). The adjective 'smart' refers to the possibility of connecting them to an external device, such as a smartphone, and to the ability of operating autonomously even if not connected.

1.3.2 Acronyms

B2B : Business to Business

B2C : Business to Consumer

GPS : Global Positioning Service

1.3.3 Abbreviations

G_n : nth goal

D_n : nth domain assumption

R_n : nth requirement

1.4 Revision history

1. v. 1.0

1.5 Reference Documents

TO DO DURING THE WRITING OF THIS DOCUMENT

1.6 Document Structure

WORK IN PROGRESS

Chapter 2

Overall description

2.1 Product perspective

WORK IN PROGRESS

2.2 Product perspective

WORK IN PROGRESS

2.3 Product functions

2.3.1 Data4Help

User Registration

Data4Help will allow users to register. These will register by entering all the required information (see [R_x] [add reference to Requirements where we specify User info for registration](#)). When registering to Data4Help, a user will first declare to have read the privacy statement and second they will have to accept the terms and conditions, which specifically include their consent to the acquisition and processing of their data, including sensitive ones, by TrackMe.

The user registration process will be carried out on the user dedicated application (see [add reference to where we are going to specify the user interface - probably section User Interface \(mobile app\)](#), maybe add also reference to user registration scenario / use case).

Unregistered users will not be able to use Data4Help. ([maybe this is a requirement and it is not necessary to put it here](#))

Third Party Registration

A third party will be automatically registered to Data4Help once the ([add name of contract between third parties and TrackMe, both here and in the definitions](#))

contract has been agreed upon and signed by both TrackMe and the third party itself.

Third party registration is required for using the service: an unregistered third party must not be able to access users data. (maybe this is a requirement and it is not necessary to put it here)

User Data Acquisition

Data4Help will acquire users data through smart wearables.

Users must give consent to the acquisition of their data when registering to Data4Help.

Data acquisition frequency can be changed according to users or third parties needs. For instance, if a user wants to save their smart wearable battery, frequency can be reduced. On the other hand, if a third party would like to track more accurately a user's position, a higher location acquisition frequency can be requested.

Third Parties Data Access

Once a third party is registered to Data4Help, it can request access to users data acquired through Data4Help and stored by TrackMe. Third parties may request data that refers either to a specific individual or to a group of users.

Consent to individual data access is left to the specific user, who can either allow or deny a third party request.

Data on groups of individuals will be shared with third parties as long as TrackMe will be able to anonymize it properly (see R_X include reference to requirement about anonymized data (1000 users satisfy request)).

Data Management and Privacy

All data acquired through Data4Help will be stored on a database accessible only by TrackMe. Each piece of users data will have a list of parties to whom access was granted. At any time, a user will be able to revoke the previously given consent to any third party or to TrackMe. Moreover, a user may exercise their right to data portability, which means that TrackMe will have to provide them with all the collected data regarding them. Finally, users may ask the deletion of all their data stored by TrackMe. might want to list the requirements that relate to this

By guaranteeing these functions, Data4Help will respect existing general regulations on privacy (e.g. EU GDPR).

2.4 User characteristics

2.4.1 Data4Help

Data-senders: People having at least one device with a sensor connected to internet, willing to share the collected data with TrackMe to take advantage of the company rewards and eventually use the services built on top of Data4Help service.

Third parties: Companies or private persons willing, for any reasons, to collect bulk data. Usually the data is used for building services on top of it; in this case it is very important that data is transferred real time. Sometimes it is used just for statistics analysis. In both cases, third parties need that the data is correct and precise.

2.4.2 AutomatedSOS

Data-senders: People (mainly elderly) having some disease or high risk of disorder willing to monitor own health parameters and conditions in order to prevent and possibly avoid crisis.

2.4.3 Track4Run

Participants: People participating in running competition. Need to have small device and with no interaction during the run to avoid distractions.

Organizers: Companies or private persons organizing running competitions willing to better engage the spectators giving the possibility to track in real-time the position of all participants. Need to provide the service easily to ensure spectators are not prevented in using it.

Spectators: People participating as spectators to running competitions, willing to better engage the event by tracking the runners during all the run. Want it to be easy without needed particular devices or applications. Usually it is a "one-time usage".

2.5 Assumptions, Dependencies and Constraints

2.5.1 Domain Assumptions

- D₁ Personal data inserted by the user during the registration correspond to his real data
- D₂ Data collected and sent by the GPS and the sensors at a certain instant correspond to the status of the user at that time

D₃ User is logged in one device at a time

D₄ The maps used faithfully represent the streets that can be traveled

WORK IN PROGRESS

Chapter 3

Specific requirements

3.1 External Interface Requirements

3.1.1 User Interfaces

WORK IN PROGRESS

3.1.2 Hardware Interfaces

WORK IN PROGRESS

3.1.3 Software Interfaces

WORK IN PROGRESS

3.1.4 Communication Interfaces

WORK IN PROGRESS

3.2 Functional Requirements

WORK IN PROGRESS

3.3 Performance Requirements

WORK IN PROGRESS

3.4 Design Constraints

3.4.1 Standards compliance

WORK IN PROGRESS

3.4.2 Hardware limitations

WORK IN PROGRESS

3.4.3 Any other constraint

WORK IN PROGRESS

3.5 Software System Attributes

3.5.1 Reliability

WORK IN PROGRESS

3.5.2 Availability

WORK IN PROGRESS

3.5.3 Security

WORK IN PROGRESS

3.5.4 Maintainability

WORK IN PROGRESS

3.5.5 Portability

WORK IN PROGRESS

Chapter 4

Formal analysis using Alloy

WORK IN PROGRESS

Chapter 5

Effort spent

WORK IN PROGRESS

Chapter 6

References

WORK IN PROGRESS