

Trackme RASD

REQUIREMENTS ANALYSIS AND SPECIFICATION DOMAIN (RASD)

Release date: 11/11/2018

Version: 0.1 (usiamo 0.xx per indicare le bozze, la 1 sarà per la definitiva)

Come table of content propongo il sommario, che poi sarà pure quello che intende il prof. Come font propongo Georgia o Calibrì light (come quello del progetto di reti logiche), come tema il terzo da sinistra di office. Grazie ciao

Table of content

[Introduction 2](#_Toc529369590)

[Purpose 2](#_Toc529369591)

[Scope 2](#_Toc529369592)

[World phenomena 3](#_Toc529369593)

[Shared phenomena 3](#_Toc529369594)

[Machine phenomena 3](#_Toc529369595)

[Goals for the client 3](#_Toc529369596)

[Goals for the third party 4](#_Toc529369597)

[Definitions, acronyms, Abbreviations 4](#_Toc529369598)

[Definitions 4](#_Toc529369599)

[Abbreviations 4](#_Toc529369600)

[Revision history 4](#_Toc529369601)

[Reference Documents 4](#_Toc529369602)

[Document structure 4](#_Toc529369603)

[Overall description 5](#_Toc529369604)

[Product perspective 5](#_Toc529369605)

[Product functions 5](#_Toc529369606)

[User characteristics 5](#_Toc529369607)

[Actors 5](#_Toc529369608)

[Assumptions, dependencies and constraints 5](#_Toc529369609)

[Specific requirements 5](#_Toc529369610)

[External Interface Requirements 5](#_Toc529369611)

[User interfaces 5](#_Toc529369612)

[Hardware Interfaces 5](#_Toc529369613)

[Software Interfaces 5](#_Toc529369614)

[Communication Interfaces 5](#_Toc529369615)

[Functional Requirements 5](#_Toc529369616)

[[G1] Provide a form of unique identification (registration/login) of all patients using the application 5](#_Toc529369617)

[[G2] Prevent third parties from associating a single user to his data without his permission 6](#_Toc529369618)

[[G3] Whenever a patient is in danger of life, the application is working and there is internet connection, an ambulance is alerted 6](#_Toc529369619)

[[G4] If the patient’s health status is not expected the patient’s family is alerted within an hour 6](#_Toc529369620)

[Non-functional Requirements 6](#_Toc529369621)

[Performance 6](#_Toc529369622)

[Accuracy 7](#_Toc529369623)

[Availability and reliability 7](#_Toc529369624)

[Security 7](#_Toc529369625)

[Design Constraints 7](#_Toc529369626)

[Standards compliance 7](#_Toc529369627)

[Hardware limitations 7](#_Toc529369628)

[Any other constraint 8](#_Toc529369629)

[Scenarios 8](#_Toc529369630)

[UML modelling 8](#_Toc529369631)

[Formal analysis using alloy 8](#_Toc529369632)

[Effort spent 8](#_Toc529369633)

[References 8](#_Toc529369634)

# Introduction

## Purpose

## Scope

In this part we expose the phenomena we consider relevant in order to model the part of world of interest: they guided us to spot goals and requirements.

### World phenomena

* Diseases /absence of disease
* Emergency situations
* Ambulance moves and arrives
* Ambulance breakdown
* GPS does not work
* Server breakdown

### Shared phenomena

[Controlled by the world]

* Detection of health values
* Request for data from the patient or the third part
* Ambulance ack
* Confirmation of good health status by the patient
* Registration to the service by a user or a third party

[The following ones have been put here and not in machine phenomena because, in our modelling, they can be in some ways detected by the server or other components of our machine]

* Sensor breakdown
* Application breakdown
* Network breakdown

**[controlled by the machine]**

* Sending data to the third party
* Showing data to the patient
* Sending an alert to an ambulance
* asking the patient to confirm his health status

### Machine phenomena

* Database queries
* Database inserts
* Database creation
* Data analysis and comparation with thresholds
* Communication between the application and the server: i.e., sending and receiving messages between the app and the server
* Matching ambulances and emergencies
* Data elaboration for showing
* Data storing by the application

### Goals for patients

* [G1] Provide a form of unique identification (registration/login) of all users of the application;
  + [G1.1] Provide a form of unique identification (registration/login) of all patients using the application
  + [G1.2] Provide a form of unique identification (registration/login) of all patients using the application
* [G2] prevent third parties from associating a single user to his data without his permission;
* [G3] Whenever a user is in danger of life, the application is working and there is internet connection, an ambulance is alerted;
* [G4] If something is not working as expected (the sensor, the application, the network), the patient’s family is alerted within an hour;
* [G5] Allow the user to see, under request, reports on his vital parameters and data about his health;

### Goals for third parties

* [G6] Allow third parties to access data if and only if they could be anonymized;
* [G7] Allow third parties to access data to specific individuals’ data under their permission;
* [G8] Allow third parties to specify constrains in their researches;
* [G9] Allow third parties to subscribe to new data;

## Definitions, acronyms, Abbreviations

### Definitions

* “***Health status***”: when in the following parts we state “health status” we are meaning the following values:
  + Blood saturation: it’s an indicator of the status of lungs and of respiratory system in general (e.g. to detect suffocation)
  + Hearth rate: it’s an indicator of hearth diseases (to detect hearth attacks)
  + Blood pression: it hardly ever helps to detect an emergency, but it’s useful for third parties and statistics (blood pressure out of range can indicate/cause a huge number of chronical diseases)
  + Body temperature: it’s an indicator of fever
  + Patient’s falling: if the patient has suddenly fallen there could be various causes and effects that, though other values are not able to detect them, put in serious risk the patient’s life.
* ***“Data Anonymization”***: deleting the fiscal code associated to every data tuple obtained by the query;

### Abbreviations

* [G-n]: n-goal
* [D-n]: n-domain assumption
* [R-n]: n-functional requirement
* RASD: Requirements analysis and specification domain

## Revision history

## Reference Documents

* Specification Document “ A.Y. 2018-2019 Software Engineering 2 Mandatory project”

## Document structure

# Overall description

## Product perspective

(dobbiamo dire che il sistema

## 

## Product functions

## User characteristics

### Actors

* Patient: the person who uses the application, wearing the device and allowing the application to monitor his health status and to manage his data;
* Third party: a company which is interested in monitoring population’s health status and obtaining a useful resource of data (e.g. a health insurance, a pharmaceutical company, the government, an hospital);

## Assumptions, dependencies and constraints

### Domain Assumptions

* [D1] The user has correctly downloaded the application from the online store on his device (smartwatch, smartphone, etc) [i.e. he is not using a crack version]
* [D2] GPS always works properly indicating the patient’s position
* [D3] For every location, there is at least a third party
* [D4] The application knows the correct thresholds for each type of patient
* [D5] The emergency number is correct
* [D6] There is internet connection when the request is submitted

### Text Assumptions

The description of the problem appears to be incomplete: due to this, we made the following assumptions:

* The main advantage of registering to Data4Help for the patients is that in this way they can see reports about their health status. Otherwise, in fact, there is no clear advantage to register to the service (which is possible, but unlikely).
* When an emergency is reported, the system sends a notification to all third parties who are subscribed to AutomatedSOS; the first third party that responds to the alert is the one who takes charge of the emergency. When this happens, the emergency is marked as “handling” by the system, and the notification disappears from all the other third parties.
* All patients are identified through their fiscal code ( which is also their username), while all third parties are identified through their official email

# Specific requirements

## External Interface Requirements

### User interfaces

To give a generic idea of what the application will look like we deployed the following mock ups:

…….

### Hardware Interfaces

The sensor which detects data is the only hardware interface we need to deal with

### Software Interfaces

### Communication Interfaces

## Functional Requirements

### [G1] Provide a form of unique identification (registration/login) of all users of the application

* [R1] If the user does not insert username and password the application does not let the user access any functionality[login]
* [R2] If the user declares that it has not a valid username or password (i.e. it’s the first access), first the system shows him a registration form[registration]
* ;
* [R3] If the username provided in the registration form is already in use, the application refuses the registration
* [D1] The user has correctly downloaded the application from the online store on his device [i.e. he is not using a crack version]

#### [G1.1] Provide a form of unique identification (registration/login) of all patients using the application

* [R4] If the user does not fill the registration form with his fiscal code and all other personal data, the application refuses the registration

#### [G1.2] Provide a form of unique identification (registration/login) of all patients using the application

* [R5] If the third party does not fill the registration form with his official e-mail and all other public data, the system refuses the registration

### [G2] Prevent third parties from associating a single user to his data without his permission

* [R6] If a third part asks for data of a single user, data are shown if and only if he concedes his permission
* [R7] if a third part asks for data that involves less than 1000 people, the application refuses
* [R8] if a third part asks for data that involves more than 1000 people, the application anonymizes data before sending

### [G3] Whenever a patient is in danger of life, the application is working properly and there is internet connection, an ambulance is alerted

* [R9] If input data show a severe disease or the patient communicates that an emergency is occurring, the machine contacts the third party responsible for that location (with a notification containing the position and the health values)
* [D2] GPS always works properly indicating the patient’s position
* [D3] For every location, there is a third party which is responsible for that location
* [D4] The application knows the correct thresholds for each type of patient

### [G4] If the patient’s health status is not clear due to malfunctions, the patient’s family is alerted within an hour

* [R10] If the application does not read properly input data every 500 Ms, it informs the user that the sensor is not working as expected, suggests contacting the customer service as soon as possible and asks for confirmation of good health status.
* [R11] If the user does not respond to confirmation within 5 minutes, the machine calls the emergency number, provided through the registration form
* [R12] If the application does not send data for back up purpose every hour, the server sends a message to the emergency number
* [D5] The emergency number is correct
* [R4] If the user does not fill the registration form with his fiscal code and all other personal data, the application refuses the registration (R) (requirement taken from goal 1)

### [G5] Allow the patient to see, under request, reports on his vital parameters and data about his health

* + [D6] There is internet connection when the request is submitted
  + [R13] If the patient asks for a report, the machine shows data stored in the database

### [G6] Allow third parties to access data if and only if they could be anonymized

* [D6] There is internet connection when the request is submitted
* [R14] If the third party asks for data and the number of people involved is greater than 1000, the machine shows data stored in the database after having anonymized them
* [R15] if the third part asks for data and the number of people involved is less than 1000, the machine refuses

### [G8] Allow third parties to specify constrains in their researches

### [G9] Allow third parties to subscribe to new data

## Non-functional Requirements

Accuracy

This is the non-functional requirement we consider the most relevant. While assuming (here and in all other parts of RASD, cfr, *domain assumptions*) that GPS works properly, our biggest concern is about the sensor which detects values: there is a concrete risk of frequent false positives, caused by some little offsets. Such cases are particularly annoying because we can’t ignore the alarms but at the same time, they make us waste time, money and resources, threatening the correct working of our machine. We pointed out that there is a trade-off between this issue (which would request to wait for a lot of consecutive signals of emergency to be sure) and the issue of performance (which would request to react immediately). We decided to wait for 1,5 sec before alerting, which means, values below thresholds for three times in a row. However, provided that false positives are defined in statistics as *type one errors,* we state that the sensor must have prob (type I err) < 5%.

Performance

Of course, we need a fast reaction to emergency. Concretely, we state that the machine must guarantee a reaction time of less than 5 seconds from the time the parameters are below the thresholds. This means that the application should process, compares data and send a message to the server in less than 3,5 sec (provided that only three consecutive data below the threshold are a clear signal of severe disease and data are sent every 500 Ms).

In addition to this, 4G connection is required to ensure immediate communication with the server.

### Availability and reliability

* Concerning the server: We need a server available 24/7 to handle emergency messages as fast as possible because, among other reasons, there is no way for the app the handle an emergency without the server;
* Concerning the app: we also need availability for the app, but not (with so much relevance) reliability , due to the fact that it takes time to detect a disease ( the sensor does not send data in real time ecc..), in which there could be an app break down with no significative consequences for the service ( provided that recovery time is under 500 ms).

Security

Thinking of a market such as the American one, where health care is subject to negotiation between patients and companies, security of all sensitive information which could advantage malicious companies, is a very important concern for our application. Due to this reason, data encryption should be implemented in communications between the app and the server and the web apps.

## Design Constraints

### Standards compliance

### Hardware limitations

Our software needs 2 physical devices to work and communicate properly at the same time. In order to deal with this strong hardware limitation, we came up with some mechanisms of detection of breakdowns

* iOS or Android smartphone with 2G/3G/4G connection and Bluetooth connection
* 4G connection
* GPS connection
* Wearable device with Bluetooth connection

In alternative

* iOS or Android smartwatch
* 4G connection
* GPS connection

For visualizing data,

* Modern browser able to render graphs and statistical models

### Any other constraint

# Scenarios

## Scenario 1- Case of emergency

Gianni is a 76 years-old man and lives alone quite far from his daughter, Livia.

He suffers from hearts problems, so Livia decides to enrol him to “AutomatedSos”. Then she downloads the app on her father’s phone and buys him a smart bracelet to connect to the system.

When registering Livia indicates its number as emergency number and she indicates, beyond the basics, some details about heart problems that his father has had in the past.

There is no problem connecting to the internet because in the home of Gianni there has been a Wi-Fi network for some years. Gianni also recharges the device every afternoon during the visits of his daughter so that battery is fully charged when he is alone at home.

A day Gianni has a heart attack while alone in the house, and then his heart values fall sharply below the thresholds laid down for him by the application.

The system immediately sends an alarm to the companies offering the assistance service, together with the values of the heart rate and the position of Gianni’s home.

The Policlinic Hospital responds first to the warning transmitted from system and takes charge of the emergency, which is then marked as *"handling*”.

## Scenario 2-Application breakdown

Derek is a man in his fifties and for some years has installed on his smartwatch the application Data4Help, which helps him to keep an eye on his health.

One day a friend told him about the additional service offered by TrackMe, *AutomatedSoS,* which guarantees automated assistance, then Derek, feeling intrigued, decides to add AutomatedSos on his smartwatch.

He has already an account, so he has just to add a phone number to contact in case of emergency: he chooses his wife’s number.

During the week-end Derek descends to the cellar to help his son to repair his bike forgetting to set the app status manually "off": unfortunately, the cellar, being underground, is not covered by their home Wi-Fi network.

The application then fails to send the data every hour and the server, not getting the back-up, sends a message to the emergency number to notify that the application is not working properly.

The wife of Derek receives the message, so she decides to go to the cellar in order to check out if everything is ok and remembers her husband to turn the application’s status “off”.

## Scenario 3-.Sensor breakdown

Anna is an elderly lady who has recently retired. Instead of retiring too, her husband works all day outside home so convinces Anna to register to AutomatedSos to be safer when he is not at home.

So she buys a small smartwatch on which she installs the application. She provides her data and indicates her husband’s number as number of emergencies.

She wears the smartwatch every day when her husband is out and recharge it when he is at home.

One day she forgets to take it off before getting into the bath: a bit of water enters the smartwatch, causing a sensor breakdown. the sensor is no more able to send data correctly.

The application, not receiving data for more than 1 minute, sends a notification to Anna in order to know her health status.

Anna sees the message and confirms that she is okay but decides to manually disable the application, putting its status “off”, so that she can bring the smartwatch for repairing, without alerting the number of emergencies.

## Scenario 4-Data anonymization

The Saint Francis Medical Clinic would like to open a new geriatric ward then turns to external consultants to figure out if it is convenient, or to understand how many people they might have.

Therefore, the consultants decide to register to Data4Help to collect some prediction data concerning the population living near the clinic.

After registering with the mail at the company, they begin to gather information.

First, ask the average pression and heart rates of people between 70 and 90 years living within a radius of 20 km from the clinic. the application has the data of more than 1500 people, and then accepts the request by providing the media required by company, giving both the numerical data that some graphs that make it more understandable.

Then the company asks the number of falls recorded in the last year regarding persons over 60 years, always within 20 km from the clinic. Again, having been recorded more than 2000 falls more or less serious, the data is anonymized and is provided by the system.

The company requires then the number of people who have heart problems in their medical history but who live within a radius of 8 km from the clinic, but this time being that only a small number of users meets these criteria, the request is rejected by the system.

Finally, they ask the application the number of old people signed up to Data4Help who live near the clinic and, of course, who authorize the processing of their personal data. As many users agree to this option, the consultants suggest clinical administrators to exploit the application to monitor elderly patients without letting them get to the clinic, fixing a big inconvenience to them.

## Scenario 5-favourite queries

The municipal administration of Novate Milanese had a very positive impression about Data4Help before the last elections, finding some data very useful and interesting to get an idea on health of citizens.

In particular, they used the data provided by the application to propose some prevention programs or help for some diseases.

This year the Education Commissioner wants to allocate funds for a smoking-prevention program in all the schools of the municipality, because he is afraid that more and more kids start smoking during high school. Due to the fact that there is not enough money for all projects, and there is no clear evidence of a real increase of smokers between teenagers, his idea is abandoned.

Nonetheless, he decides to take advantage of Data4Help and indicates as “favourite query” data on blood saturation of teenagers between 14 the 18 years.

After 1 year the system notifies that the data regarding the “favourite queries” have changed. Therefore, he requires new data that indicate a decrease in blood saturation of that group of patients specified by the query. Consequently, he concludes that his fears were right.

After other 3 months the system notifies a further update in the data collected, so the Commissioner makes a new request of data and the result confirms the trend shown by the last request.

Thanks to these data, the Commissioner manages to convince the administration to invest some funds to sustain his program.

## Scenario 6-Personal Use

Betty has just begun a new fitness program, after being stopped for a few years. At the first lesson, the fitness coaches recommend using Data4Help to check whether the program is too stressful for her health.

Betty downloads the app on her smartphone and buys a device to connect to the application.

Betty enrolled the service providing her social fiscal code, basic information about herself (weight, height, gender) and her health (pre-existing conditions, chronical diseases, pathologies…).

Thanks to Data4Help, Betty everyday is able to control her health status and improvements that the fitness program has on her values.

The sponsors of the fitness program, who want to check out the real impact of their services, ask via Data4Help for her personal data. Betty receives the request on her smartphone, recognizes the company and accepts without any doubt. Data4Help finds and sends all kind of information it has from Betty’s profile stored in the database.

# UML modelling

# Formal analysis using alloy

# Effort spent

# References