Position and Usage Monitoring of Help Aid

Adem Saran: elt13as1@student.lu.se
Mansoor Ashrati: elt13mas@student.lu.se

Department of Electrical and Information Technology
Lund University

Supervisors at EIT: Stefan Höst, Jonathan Sönnerup

Supervisors at Cybercom: Mahmoud Passikhani, Omid Asali

Examiner: Maria Kihl

2018-06-18

Printed in Sweden
Tryckeriet i E-huset, Lund

Popular science summary

The ever expanding world of Internet of things (IoT) solutions can be applied to many different areas. In the use case of help aid, this master's thesis aims to provide a solution that can reliably send out information about the usage and position of the help aids to the stakeholders.

The number of IoT devices are increasing and these devices are mainly used to collect data. An IoT device can be anything from a small sensor sending data once a day or be used in larger use cases, such as traffic safety or industry. The security in IoT devices are often not prioritized which has led to some major issues for the concerned parties. Also with the General Data Protection Regulation (GDPR) coming into effect on the 25th of May 2018, higher requirements on how the data that is collected can be stored and what data is allowed to be collected, will be enforced.

The three different help aids that are being monitored are, wheelchairs, walkers and TENS machines. These are lent out from hospitals in each county council in Sweden. Often these help aids are lost and never returned back to the hospitals. This is a unnecessary cost for the county councils, which also are the stakeholders in this project. Being able to monitor the help aids usage and position, reducing these unnecessary costs is possible. A comprehensive background research has been done on different components and earlier works and projects in the same problem area. The results from the research showed that there are no earlier solutions to this kind of monitoring problem but resources and components to create a solution, exists. The results from this thesis are therefore divided into an architectural proposal solution and a proof of concept solution.

In order to properly tackle the monitoring issue one must firstly define the aspect of what usage is for the three different types of help aids. Two other aspects that are essential are how the usage is going to be monitored and how the monitoring is performed.

The results from the architectural so-

lution and the proof of concept solution shows two solutions that are similar in many ways. Both solutions consider the monitoring aspects, security in the system and the implementation is in compliance to the GDPR and presentation of data. The usage monitoring of the wheelchair and the walker is done using three different sensors, hall effect sensor, pressure sensor and an accelerometer, since using one or two of them are not sufficient enough to ensure that they are being used. For the TENS machine, a circuit had been built, that senses conducting current through the wires from the TENS machine. The sensors and the circuit exchange data with an ESP8266, a popular device for IoT solutions. For the architectural proposal solution the position is determined with GPS and the communication between the ESP8266 to the Internet is done through the cellular network. For the proof of concept solution the position is determined with Geolocation and the communication to the Internet is done through the Wi-Fi network. The stored data is minimal, containing device id, coordinates and a time stamp. This together with encryption of the data ensures GDPR compliance. This data is presented in a web application.

The conclusions are that there is a solution to the issue of lost help aids. Both solutions given in the thesis are relevant and both are viable for further development. The architectural solution implements the most independent solution with regards to communication and positioning. This is then scaled down in to a proof of concept solution that focuses more on determining usage. The designed system could be used in other areas with similar monitoring issues. It could also be used by doctors to follow up a scheduled treatment, given out to patients etc.

Abstract

Internet of Things or IoT is an emerging field of technology that can be implemented in different use cases to collect and exchange data. Help aids such as wheelchairs, walkers and TENS machines, that are lent out by the county councils to private persons, are easily lost due to several factors and this is a problem. Using IoT to implement a system that can monitor the usage and the position of these help aids, could solve the problem. This Master's Thesis aims to provide an architectural proposal solution and a proof of concept solution on how to design the system from a hardware perspective and how to present of the collected data, with the main focus on how to monitor the position and usage of the help aids.

The thesis also introduces and discusses the implementation of the GDPR in the solution, which is highly relevant. Known from before, security in IoT solutions have not been highly prioritized. In this thesis, the security has been taken into consideration since sensitive data is being handled.

Keywords - Positioning, Usage, Wheelchair, Walker, TENS machine, IoT, Help aids, GDPR, Security

Acknowledgements

The authors of this thesis send our greatest gratitude to our supervisors Stefan Höst and Jonathan Sönnerup at EIT, as well as our supervisors Mahmoud Passikhani and Omid Asali at Cybercom for making this thesis possible. Special thanks go to Victor Remmo for his contributions and help.

Finally, we send thanks to our families and friends for their support.

Contents

List of Figures

List of Abbreviations

3GPP	3rd Generation Partnership Project
AP	Access Point
API	Application Programming Interface
BJT	Bipolar Junction Transistor
BSS	Basic Service Set
CA	Certification Authority
CEP	Circular Error Probability
CIA	Confidentiality, Integrity and Availability
CPU	Central Processing Unit
CSS	Chirp Spread Spectrum
DBPSK	Differential Binary Phase Shift
(E)DH	(Ephemeral) Diffie Hellman
ETSI	European Telecommunications Standards Institute
FSR	Force Sensitive Resistor
GDPR	General Data Protection Regulation
GFSK	Gaussian Frequency Shift Keying
GPRS	General Packet Radio Services
GPIO	General-purpose input/output
GPS	Global Positioning System
GSM	Groupe Spécial Mobile (Global System for Mobile Communications)
HTTP(S)	Hypertext Transfer Protocol (Secure)
I2C	Inter-Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunication Union
IP	Internet Protocol
ISP	Internet Service Provider
IoT	Internet of Things
JSON	JavaScript Object Notation
LPWAN	Low-Power Wide-Area Network
LTE	Long Term Evolution
MAC	Media Access Control

MITM	Man In The Middle
MOSFET	Metal Oxide Semiconductor Field Effect Transistor
NB-IoT	Narrowband IoT
NIST	National Institute of Standards and Technology
NFC	Near Field Communication
PFS	Perfect Forward Secrecy
PMOS	P-channel MOSFET
QPSK	Quadrature phase-shift keying
RDBMS	Relational Database Management System
REST	Representational State Transfer
SOC	System-on-a-Chip
SPI	Serial Peripheral Interface
SQL	Structured Query Language
TCP	Transmission Control Protocol
TENS	Transcutaneous Electrical Nerve Stimulation
UART	Universal Asynchronous Receiver/Transmitter
UNB	Ultra Narrow Band
WPA	Wi-Fi Protected Access

Chapter 1

Introduction

The research for this thesis has been conducted at Cybercom Group in cooperation with the Electrical and Information Technology department (EIT) at the Faculty of Engineering, Lund University. This chapter introduces the thesis with the problem background, goals with research questions and limitations and with an outline of the thesis.

1.1 Background

Locating objects and monitoring their usage is a challenge. When it comes to hospital equipment this is an increasing necessity due to the large number of help aids that are present and used. Many help aids are lost or disappear which introduces unnecessary costs and difficulties for the owners, which in Sweden are the county councils. These objects are often not returned to the owners due to various reasons. If these help aids are reliably monitored in terms of position and usage, they are known to be used and located. Solving this with modern and emerging technology, can be done by implementing an Internet of Things (IoT) solution. IoT is an increasingly used term describing a network of devices that can be used for collecting and sending data. IoT solutions can be used in many different applications and use cases in daily life.

In this thesis three types of help aids are examined; wheelchairs, walkers and TENS machines. Wheelchairs and walkers are very similar in their usage. However, TENS machines are used for stimulating nerves using electricity so they differ a bit in usage. This introduces two distinct usage problems to solve.

To do this type of positioning and measurement of the usage of these help aids, a communication with them is required which can be done in different ways, one is using the existing wireless and mobile networks.

Also, as a response to data scandals with more and more increasing severity, in the European Union the General Data Protection Regulation (GDPR) will come into effect on the 25th of May 2018, which all member states have to follow. This law introduces much stricter definitions on what is personal data, how it is stored and increases the rights of data subjects greatly. As of writing this thesis, the regulation hasn't come into effect and achieving compliance is a challenge for many data controllers. Due to the nature of collecting personal data related to health, this thesis will adapt to these regulations.

1.2 Goals

The goals of this thesis is to investigate and analyze how the three help aids are used and provide a definition for what usage is for the three use cases. From this definition an architectural solution proposal is presented that solves the usage, location, security and GDPR aspects. A proof of concept will then be implemented which focuses mostly on the usage and location aspects. To achieve this, some research questions and limitations that have been set up for this thesis.

1.2.1 Research questions

In order to achieve the goals in this thesis some research questions have been defined. Firstly, what is the best way to find if the help aid is used or not and what is the best way to monitor them in outdoor environments? Secondly, the question of if it is possible to provide a proof of concept solution where the position and usage is monitored for a help aid which is used by private persons? This solution must be based on requirements from the stakeholder, resources and within the time frame. This question is very relevant because the stakeholder requires an implemented solution and a proof of concept solution is assumed to be enough for providing that usage and position can be monitored.

With GDPR being relevant it is important to see if the implementation can be adapted to the GDPR. With this being stated, what data is relevant to be stored and provided for the stakeholder and how should the data be stored? Also, since IoT solutions can be versatile the question if this implementation can be used in different areas outside of the use case of this thesis is relevant.

1.2.2 Limitations

In order to limit the scope of the project, some limitations have been set. The proof of concept solution is not intended to be a finished product for the market. This would require a lot more focus on economics and other areas that are not of relevance in this work. The main focus of the thesis is the monitoring problem.

The solution to the monitoring problem opens the doors for possible management of the big issue of lost help aids. Other areas that will be considered but are not a major focus in this thesis, are the GDPR, energy efficiency and the security. This is due to the fact that the implementation should be secure, energy efficient and that the GDPR is highly relevant. The latency of the data transmission is not a focus of this thesis since the system has no requirements of the data transmission.

1.3 Related Work

Since IoT is such an large and coveted research area, there are many studies on it to examine. An IoT solution can vary in many ways, from its communication techniques, its security and its energy consumption depending on the use case of such a solution. M. Lauridsen et al. [1] in "*Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area*" for example discusses and compares the coverage of some of the more popular communication methods for IoT by conducting a series of experiments in northern Denmark. N. R. Potlapally et al. [2] in "*A study of the energy consumption characteristics of cryptographic algorithms and security protocols*" discusses the trade off between security and energy consumption in IoT devices. This is important because often the requirement of an IoT device is to be long lasting with low energy consumption. However depending on the use case, different levels of security is also required. For this thesis concerning medical data, this trade off is an important consideration.

Concerning the use case of this thesis i.e. monitioring usage and position of help aid, the study "*A Wheelchair Usage Monitoring/Logging System*" by D. Ding et al. [3] shows an implementation of a system that obtains data on distance traveled by the wheelchair, how long the user sits in various seating positions and importantly where the wheelchair has been. The latter mentioned part of this work is mostly relevant for this thesis. However, this isn't implemented as an IoT solution.

1.4 Outline of Thesis

Chapter 2 : This chapter introduces the usage and monitoring aspects. It also introduces the different help aids, defines the usage of the different help aids and how the usage is monitored and performed.

Chapter 3: This chapter introduces some basic concepts of the theory and softwares that are needed to understand the choices made for the architectural solution proposal and the proof of concept solution. The basics of the GDPR, security and network is introduced as well.

Chapter 4 : This chapter presents the architectural proposal solution. It shows how the problem should be solved for each help aid. Solutions on how the com-

munication, positioning, security and GDPR compliance should be done, are explained.

Chapter 5: This chapter contains the proof of concept solution for each help aid. Solutions on how the communication, positioning, security and GDPR compliance should be done, is explained. Also different observations and results are presented.

Chapter 6: This chapter evaluates the proof of concept solution and shows results from different test done on the system. The tests are done on the different proof of concept solutions but focuses on testing the usage and positioning.

Chapter 7: The results from the architectural solution proposal and proof of concept are discussed. A conclusion on whether the issues and research questions are fulfilled, is presented. Also, this chapter discusses how the project can be evolved in the future.

Chapter 2

Usage and Monitoring Aspects

This chapter explains what the different help aids are and whom they are used by. Also, usage is defined for each type of help aid, how usage is going to be monitored and how the monitoring is performed.

2.1 Wheelchair and Walker

Wheelchairs come in many different designs and sizes. Some are electrical and some are not, and they are mostly equipped with two big wheels combined with two small wheels. Usually wheelchairs are used due to the fact that walking is a difficulty caused from injuries or disabilities. The most common target audience is elderly people with walking difficulties due to age. In Sweden, wheelchairs are used permanently by 130 000 persons [4]. Wheelchairs are mostly used in outdoor environments but also in indoor environments.

Walkers often have the same design, four wheels with brakes and a basket. Its main field of application is to support the walking for people with walking difficulties. Walkers are mostly used by elderly people with walking difficulties caused by aging. It is estimated that 250 000 persons use walkers permanently in Sweden [4]. Walkers are often used in outdoor environments.

2.2 TENS Machine

TENS machines, or Transcutaneous Electrical Nerve Stimulation machine, is a device that stimulates nerves for therapeutic purposes by using electric current produced by the machine. Usually they are designed with two channels with 2 lead wires per channel. On each wire there are TENS plates hooked that will be placed on a part of the body. Electric current is sent through the channel from

one of the TENS plates, through the body and to the other TENS plate. TENS machines are mainly used by people with acute or chronic pain caused by any reasons. The TENS-machines are mostly used in indoor environments.

2.3 Usage

For the three different types of help aids considered in the report, the usage will have to be defined differently due to their different functionalities. In this section the following three main questions will be answered:

1. What is defined as usage?
2. How is usage monitored?
3. How is the monitoring performed?

2.3.1 What is defined as usage?

Defining usage can be done in different ways depending on the help aid that is being used. An important consideration is that each help aid needs to have usage defined clearly so that the choice of monitoring can be as accurate as possible.

A standard hand-driven wheelchair is used by one user who is seated. Usage for the wheelchair is reasonably defined as motion in a general direction propelled by either the user or somebody else pushing the wheelchair, e.g. a nurse or helper. This introduces an issue of the speed of the wheelchair. It must be assumed that the wheelchair moves at a reasonable speed. A walkers usage is defined in a similar way as for the wheelchair. Here, the major difference is that the user is not seated when the walker is moving. This means that seating is not an requirement for usage. Since both the wheelchair and walker are very similar with the only difference being whether the user is seated or not, the definition of usage depends mainly on the motion of the help aid. This definition is appropriate due to the fact that the help aids are used for helping disabled move around.

The TENS machine however differs a lot from the wheelchair and the walker. Because the machine is used indoors often, it can not be assumed to be in motion when being used. The user can e.g. be seated when using the machine. The machine can be turned on without any treatment running. This does not count as usage. The only time it is guaranteed to be used is when a treatment in the machine is running. This is an appropriate definition of usage.

2.3.2 How is usage monitored?

From the definitions of the usage for the three different help aids above, it is clear that peripheral devices are needed to fulfill the definitions. A single sensor for determining whether the wheelchair or the walker is used will not be sufficient. A sensor that senses motion in the form of speed or acceleration will only monitor and guarantee motion. The cause of the motion can be that the wheelchair or the walker is used as it supposed to be but it can also give false positives. The wheelchair or the walker could be transported in a vehicle etc. Similarly, having only a sensor that senses the spinning of the wheels, will only guarantee that the wheelchair or the walker has its wheels spinning. It will not in fact guarantee that someone actually is using it properly or that it moves in a reasonable speed. Having a sensor that senses that a person is seated on the wheelchair or the walker, will not guarantee that it is moving or even having its wheels spinning. The wheelchair is defined being used when the system can detect that there is someone seated on it, when it is moving in a reasonable speed and that its wheels are spinning. The walker is defined being used when the system can detect that the wheels on it are spinning and that it is moving in a reasonable speed.

In order to monitor the TENS machine and fulfill the definition of its usage, sensors that detect motion can be omitted. Focusing on the actual machine which is battery powered, it can be assumed that the machine is powered on when there is a loss in battery power. However, this does not in fact guarantee that the machine is used by a person because the machine can be powered on without the actual TENS treatments being used as stated before. Usage can instead be monitored by measuring the current through the wires to the TENS-plates and this guarantees that a treatment is running.

2.3.3 How is the monitoring performed?

For the wheelchair, monitoring has to be made on motion, spinning wheels and if the user is seated. This makes it clear that more than one sensor is needed. At least three sensors are required to monitor the usage. Motion can be detected with different types of sensors such as e.g. accelerometers and gyroscopes. Spinning wheels can be detected in various ways, but they all revolve around having a detector on the base of the wheelchair and a trigger on the wheel to detect one revolution. For example a hall-effect sensor together with a magnet on the wheel or a light with a detector together with a reflective surface on the wheel. To detect if a user is seated, a pressure sensor or a temperature sensor can be placed on the seat. For the walker the same implementation can be done, except for detecting if the user is seated.

For the TENS machine, monitoring has to be made on the current through the wires. This can be done in several ways. One way is to detect the magnetic field created by the current in the wire using a hall effect sensor or something similar

to a clamp meter. This has the benefit of not interfering with the wire. Another way is to build a circuit that detects current in the wire.

Chapter 3

Background

In order to have a good understanding of the problem and the choice of solution, background knowledge is important. This chapter will introduce basic background theory on different areas that are central in this thesis.

3.1 Internet of Things

The Internet of Things, or IoT, can be described as a network consisting of physical devices that can collect and exchange data using existing network infrastructure. These devices can be sensors, smart objects, wearables etc. Often, the main requirement for an IoT device is to be long lasting with low energy consumption.

IoT devices can be separated into two range categories: Short range and wide area. The former utilizes unlicensed radios with short range such as Wi-Fi or Bluetooth. The latter uses cellular connections such as GPRS, 3G/4G, NB-IoT and soon 5G.

Overall, the number of connected devices are expected to rise very drastically in the coming years. At the end of 2016 there was around 400 million IoT devices with cellular connection. By 2022 it is estimated that there will be around 18 billion IoT devices out of around 29 billion total connected devices [5].

IoT-solutions can be divided into two main categories: Massive and Critical IoT. Massive IoT consists of low power, low cost modules that update info with the cloud on a regular basis. Examples of this include sensors of various kinds. On the contrary, Critical IoT consists of high reliability and low latency devices. These are used in e.g. industry or traffic safety use cases. The problem in this thesis is considered to be a Massive IoT problem. This means that the solution faces the following challenges:

- Low cost of the device - Since IoT is applied in high volume applications, the cost of each device is significant.

- Long battery life - Many times, replacing batteries is not viable on the field.
- Large coverage - Depending on use case, the solution must have either good indoor connectivity or very good outdoor coverage for example in the transport field.
- Scalability - The network that supports the devices must be able to scale up from an initial limited number of devices to potentially support millions.
- Diversity - Connectivity, the network must be able to support different types of sensors and their different requirements on e.g. latency or throughput.

There are different types of technologies to enable IoT. Short-range techniques that enables IoT are Bluetooth, Near-field communications (NFC), Wi-Fi etc. Medium- and Long-range techniques that can enable IoT are LTE or NB-IoT for example.

3.2 Microcontroller

A microcontroller is a small computer on a single integrated circuit. Microcontrollers can be found in many products and devices such as remote controls etc. and they have at least one CPU, memory and programmable input/output peripherals. A microcontroller can for example control other devices and processes. Examples on well known microcontrollers are AVR, PIC, ESP8266 etc. [7].

The ESP8266 chip is integrated with a TCP/IP protocol stack and can give other microcontrollers access to Wi-Fi networks. The ESP8266 can run different operating systems, one of these are the NodeMCU.

3.3 NodeMCU

NodeMCU is an operating system for the ESP8266 chip based on the Lua programming language. It provides support for the use of advanced API's for hardware IO [8].

Some libraries in the NodeMCU software include [9]:

- `crypto` - Provides support for cryptographic algorithms.
- `gpio` - Provides access to the GPIO subsystem.
- `i2c` - For using the i^2c serial bus.
- `uart` - Allows for communication over the UART serial port
- `wifi` - For using WiFi-related features such as connecting to an AP or setting up the ESP as an AP.

Programming for the NodeMCU operating system can be done with Lua. Lua is a simple, lightweight, cross platform language. Lua was developed by a team at the Pontifical Catholic University of Rio de Janeiro, Brazil as a programming language primarily for embedded systems [10].

3.4 Sensors

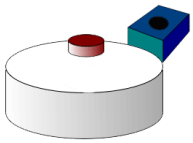
This section will introduce and explain some different types of sensors that can be used in the monitoring of the help aids.

3.4.1 Accelerometer

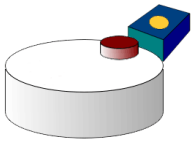
When an accelerometer measures acceleration on a body that is in rest, meaning the coordinate system where the body is stationary, it is called the proper acceleration. Different accelerometers have different properties, some measure proper acceleration in one axis and some in multiple axes. In general, capacitive plates are placed internally in accelerometers. These plates moves upon acceleration which makes the capacitance between them change. The acceleration can then be determined from the changes in capacitance. The acceleration can also be determined with accelerometers that uses piezoelectric materials. The piezoelectric material outputs an electrical charge when a mechanical stress is applied and the acceleration can be determined from this [11].

3.4.2 Hall-effect sensor

Hall-effect sensors are transducers, meaning they convert energy between two forms, from magnetic to electric energy. In the presence of a magnetic field, electrons in the metal placed inside hall-effect sensors, are deflected towards one edge. This produces a voltage gradient across one side of the metal. Figure 3.1 shows an example of the behavior of the hall-effect sensor when a magnet on a wheel passes by the sensor. The Figures 3.1a and 3.1b shows that the sensor detects the magnetic field, assumed that the magnetic field strength is high enough.



(a) Magnet outside the range of the hall-effect sensor.



(b) Magnet inside the range of the hall-effect sensor.

Figure 3.1: A wheel containing one magnet, passing by a hall-effect sensor.

It is known that current flowing in wires produces a magnetic field. The magnetic field strength for a straight wire can be determined with:

$$B = \frac{\mu_0 I}{2\pi r} \tag{3.1}$$

Where $\mu_0 = 4\pi \cdot 10^{-7}$ Tm/A is the permeability of free space, I is the current and r is the distance to the wire [12].

3.4.3 Pressure Sensor

Pressure is mostly stated as force per unit area. Pressure sensors usually acts as transducers. They are used in many different areas and come in various forms such as absolute pressure sensor, gauge pressure, vacuum pressure etc.

The Pressure-sensing technology can be divided into two categories of analog pressure sensors. The force collector types, which uses force collectors to measure deflection when force is applied on an area. The other category use density to determine the pressure of liquid and gas [13].

3.5 Interface Bus

An interface bus in computer architecture is a system that transfers data. This communication system can transfer data between components inside of a computer or between two computers. The buses can be divided into two groups, internal and external buses. The internal bus, also known as memory bus or system bus, connects the internal components such as the memory to the motherboard. The external bus, also known as expansion bus, connects different external devices such as modules, printers etc. to a computer. Inter-Intergrated Circuit (I^2C) and Serial Peripheral Interface Bus (SPI) are two different serial interface buses that are used by many modules and sensors.

I^2C is an invention by Philips Semiconductor. It is a multi-master/slave serial computer bus. Low-speed peripheral ICs attaches to processors and microcontrollers by applying I^2C [14].

The SPI is primarily used in embedded systems. The SPI is a synchronous serial communication interface for short distance communication. Motorola is the developer of the interface and SPI devices communicate in full duplex, which means that the communication can be done in both directions. Communication in both direction is achieved using a master-slave architecture with only one single master [15].

3.6 Positioning

In this section, the different methods of positioning objects will be mentioned. This section will also explain the technology behind each way of positioning. These different technologies are essential in this work in order to be able to position the different help aids.

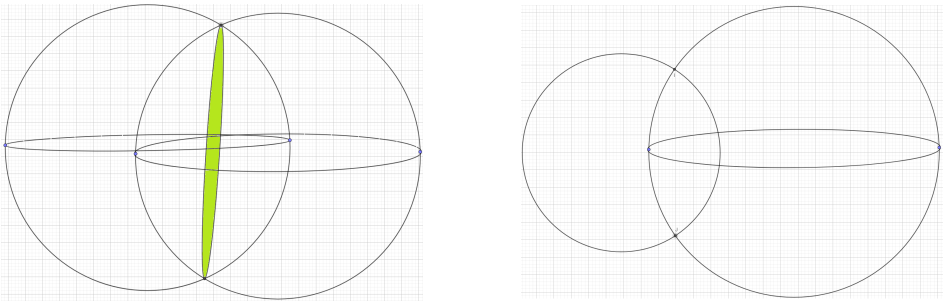
3.6.1 Global Positioning System (GPS)

The Global Positioning System (GPS) is a system that provides geolocation and time information. It was developed by the U.S. Department of Defense for military use. Civilians were allowed to use the system first in the 1980's. To determine a position, trilateration with satellites is used. Determining your position, GPS uses the signal from at least 4 satellites.

Each satellite has an atomic clock which is synchronized with the other satellites in the orbit. Each satellite continuously broadcasts its position and time. The device that is to be positioned with GPS, calculates the distance using:

$$d = c \times \Delta T \tag{3.2}$$

where d is the distance to the satellite from the receiver, c is the speed of light and ΔT is the time difference between the receiver and time broadcast by the satellite. Each satellite sends signals in outer space in the shape of spheres. When two spherical surfaces intersect, they create a shape of a ring which can be seen in Figure 3.2a. When the third spherical surface collides with the ring, they will intersect in two points which can be seen in Figure 3.2b. One of these points is more likely to be on the surface of the earth than the other, therefore it can be assumed to be the pending point. The fourth satellite is needed since the clock on our GPS receiver is not accurate [16].



(a) Two colliding spheres creating a ring surface (marked in green).

(b) The ring surface with the third sphere.

Figure 3.2: Colliding sphere surfaces from the GPS satellites.

3.6.2 Geolocation

Geolocation is a method of determining the location of an Internet host using its MAC or IP-addresses, hardware or software production numbers, GPS coordinates or other information. It works by mapping this information to factors such as:

- Country
- Region (city)
- Latitude/longitude
- ISP
- Domain name

When a device is requesting its location using a geolocation API, it will give a estimate of the devices physical address [17].

The Google Geolocation API

The Google Geolocation API returns a JSON formated object containing the location and accuracy radius from information given by a device. This information can contain both cell towers and/or Wi-Fi access points. These are sent as a JSON object called a request body. It contains the following optional fields:

- `homeMobileCountryCode`: The mobile country code for the device's home network.
- `homeMobileNetworkCode`: The mobile network code for the device's home network.
- `radioType`: The mobile radio type. Supported values are lte, gsm, cdma, and wcdma.
- `carrier`: The mobile carrier name.
- `considerIp`: Specifies whether to fall back to IP geolocation if Wi-Fi and cell tower signals are not available. Defaults to true.
- `cellTowers`: An array of cell tower objects.
- `wifiAccessPoints`: An array of Wi-Fi access point objects.

Furthermore, an `wifiAccessPoints` array contains the following elements, only `macAddress` is required [18]:

- `macAddress`: The MAC address of the Wi-Fi node.

- `signalStrength`: The current signal strength measured in dBm.
- `age`: The number of milliseconds since this access point was detected.
- `channel`: The channel over which the client is communicating with the access point.
- `signalToNoiseRatio`: The current signal to noise ratio measured in dB.

3.7 Wireless Communications

In this section, the different wireless communication technologies from mobile telecommunication technologies such as GSM to 4G LTE and a technology for local area networking such as Wi-Fi will be discussed and shortly introduced. According to H. Nguyen et al. [1] these are the most common technologies for IoT communications.

3.7.1 GSM

the Global System for Mobile Communication or GSM is the standard to describe the protocols for the second generation or 2G wireless telecommunication. The 2G network was developed to replace the 1G network which was analog. Originally the 2G was digital without any support for internet. With the GPRS introduced, the newer version of 2G also had access to internet but on theoretically speeds of 50 Kbit/s [19].

The GSM technology was commonly the time division multiple access or TDMA. TDMA is a method for shared-medium networks which allows multiple users utilize same frequency channel. Spreading the signal into different times slots, makes this possible.

3.7.2 General Packet Radio Service (GPRS)

The GPRS is service on the 2G and the 3G cellular communication system. The service is a packet oriented mobile data service which is a type of communication link sharing. The service is maintained by 3rd Generation Partnership Project (3GPP), but was originally standardized be the European Telecommunications Standards Institute (ETSI) [20].

3.7.3 3G

The third generation or 3G is the third generation of wireless telecommunication technology. The 3G is totally separate from the previous networks and provides Internet at faster speed around a few Mbit/s. 3G devices can not communicate with GSM towers since the 3G technology is different from the GSM technology. Therefor it is not backward compatible to the older GSM technology. This is a drawback since telecoms still have to maintain the older GSM technology.

The 3G technology uses a channel access method called Code-division multiple access or CDMA. The method employs spread spectrum technology in combination with a special coding scheme. What is different from this modulation and other modulation schemes is that the bandwidth is spread in the frequency domain, which results in a wider bandwidth. The advantages of this is an increased immunity against interference or jamming and multiple user access.

When it comes to security, the 3G networks uses KASUMI. KASUMI is a block cipher which is used to provide confidentiality and integrity. 3G networks offer greater security than GSM networks which uses the older A5/1 stream cipher [21].

3.7.4 4G

The broadband cellular network technology that succeeds 3G, is the 4G. The ITU specified the standard in the IMT-Advanced requirements. Two 4G systems were developed and are used commercially; WiMax and LTE. WiMax was standardized by IEEE and is currently the lesser used technology of the two. LTE, also known as Long Term Evolution is the more widespread. Both of these standards however do not fully comply with the IMT-Advanced requirements but are still accepted as 4G. One of the later versions of LTE called LTE Advanced, however fully complies with the IMT-Advanced requirements [22].

4G differs from the 3G standard in that it is developed firstly for Internet traffic. The 3G is however firstly developed for telephone traffic. LTE offers speeds of up to 100 Mbit/s and has been standardized by the 3GPP [23]. Some LTE solutions were specifically adapted for the use of IoT devices, such as NB-IoT.

NB-IoT

Narrowband IoT (NB-IoT) is a narrowband radio technology standardized by the 3GPP. It is a LPWAN developed that with the help of cellular telecommunication bands, enable a wide range of devices to be connected. NB-IoT focuses on long battery life and low cost, together with the use of many connected devices . The NB-IoT technology offers speeds around 250 Kbit/s [24, 25].

3.7.5 5G

Currently, the successor to the 4G networks are being developed for release in 2020. The 5G network is designed to handle many connected devices which are suitable for the projected rise of IoT devices worldwide. Some other goals with 5G are low latency and very high reliability. It must handle both high data rate applications such as mobile phone connectivity and low data rate applications such as machine to machine communication with IoT devices [22].

3.7.6 LoRa

LoRa is a wireless RF technology which is used in LPWANs for IoT applications. It was developed by Cycleo in Grenoble, France and acquired by Semtech in 2012. LoRa is based on chirp spread spectrum (CSS) technology which uses a chirp pulse consisting of a sinusoidal signal where the frequency increases or decreases over time. This pulse is used to encode and decode the sent packet. The goal with LoRa is to enable long communication distances with the help of CSS and enable low power consumption and low throughput communication of a maximum of 1 kbit/s. It also provides deep penetration in dense indoor regions.

When it comes to security in LoRa, it has end-to-end embedded encryption using AES which is a specification for encrypting data [26].

3.7.7 Sigfox

Sigfox is a French company that builds wireless networks. The Sigfox technology operates on the ISM radio band. It uses Ultra Narrow Band (UNB) technology which passes through solid objects freely and the required energy is little and therefor it is a LPWAN. Sigfox provides data transfers at speeds of 100 or 600 bit/s depending on the region. The Sigfox only allows 12-byte data payloads.

Together with the UNB technology, Sigfox uses the Differential Binary Phase Shift Keying (DBPSK) and Gaussian frequency-shift keying (GFSK) modulations. When the scheme depends om the difference between the successive phases, it is called DBPSK The GFSK is also a digital modulation that imparts the frequency of the carrier wave [27].

3.7.8 Wi-Fi

Wi-Fi is a certified trademark in use to describe the technology which allows the connection and use of most wireless networks, or WLANs. The technology is based mostly on the IEEE 802.11 standard, so the terms are used interchangeably in

most day to day speech. The WLANs can operate in two modes. In infrastructure mode, all units connect to a local network called a Basic Service Set (BSS). Each BCC uses access points or AP's to communicate via a router to the Internet. In a standard home network, the AP and router are integrated into the same device. However, in ad-hoc mode the units group together to form a BSS which has no AP and connection to the outside Internet. Here the units communicate directly with each other in a local network [28, 29].

In infrastructure mode the networks can either be configured as open networks where any unit can connect freely. Otherwise, the networks have some sort of access control. One way of doing this is using Wi-Fi Protected Access 2 (WPA2) [29]. WPA2 is however vulnerable to attacks such as KRACK which was announced in October 2017. This has led to WPA3 being introduced by the Wi-Fi Alliance [30].

3.8 Database

SQL which stands for *Structured Query Language*, is the the most common standardized language used to access databases [31]. MySQL is a relational database management system (RDBMS). This means that the data is stored in tables rather than all data put together in one space. The MySQL software is open source and should work in both client/server or embedded systems. It provides enough functions to make an implementation that is compatible with GDPR.

3.9 General Data Protection Regulation

To strengthen and unify the data protection for individuals within the European Union, the European Parliament has created the General Data Protection Regulation which will take effect the 25 May 2017. The goal for the regulation is primarily to give the control over personal data back to citizens. To implement and adapt for the regulation, there will be a challenge for most members in EU, but especially for Sweden. The current Data Protection Directive from the EU called PUL in Sweden, has so far been used at ease in Sweden compared to other countries in EU. For many companies, the regulation is a matter of money. This is due to the fact that those who do not follow the regulation, a fine of 20 million EUR or 4% of the annual worldwide turnover, whichever is greater, will be held [32]. This work will handle personal data that will be stored, therefore this is highly relevant for the thesis.

3.9.1 Personal Data

GDPR defines personal data in Article 4(1). It says that any identifiable natural person, also known as the *data subject* can be identified both directly and indirectly with personal data. Since the reason of the GDPR is to protect personal data and the regulation only applies to it, this definition is very important. Some examples of personal data include:

- Name
- Address
- Telephone number
- Email
- Identification number
- Location data
- Online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- Photos
- IP-addresses
- Cookies

Furthermore some data might be considered to be of higher importance which allows for a more comprehensive category of sensitive personal data [33, 34].

3.9.2 Sensitive Personal Data

Some data related to a persons personal identity requires stronger protection. GDPR defines sensitive personal data in Article 9(1). It strongly prohibits the processing of sensitive personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [35].

This means that processing data such as that concerning health is prohibited unless the person in question has given explicit consent unless Union or Member State law has prohibited the person to do so. This is defined in Article 9(2)(b). Consent is also defined further in Article 4(11) as any freely given indication of a data subjects wishes that they agree to the processing of personal data relating to them by a statement or by an other clear affirmative action [35].

3.9.3 Privacy By Design And Privacy By Default

GDPR recognizes the right of privacy by design. According to Article 25(1) [36], data controllers must "implement appropriate technical and organizational measures, such as pseudonymization." in design stages of all projects along with the life cycle of the relevant data process [37].

However, privacy by default as stated in Article 25(2) determines that the data that is collected is only used for the specific purpose for which the data is needed. This is not something new for data controllers as it was advisory before GDPR, but will now be mandatory. A way of implementing this is by minimizing the amount of data that is collected [37].

3.9.4 Pseudonymization of Data

GDPR introduces the concept of pseudonymous data which is personal data that has been altered in a way so that it is not directly traceable back to an individual without additional information. Hence, this means that the data has been for example hashed or encrypted so that it is unintelligible without the key, in the use case of e.g. encryption. The data will however still be considered to be personal data. Pseudonymization of data allows for certain relaxations from some provisions in the GDPR regarding breaches of data. It encourages the use of pseudonymization as a measure for privacy by design and for enhanced security [38].

3.9.5 GDPR and IoT

The use of IoT products introduces various difficulties and issues when trying to be compliant with the GDPR. This is due to the following regulations and definitions in it [39, 40]:

1. **Security breaches**: Due to the issues concerning IoT devices and security, some concerns have been put forward regarding security breaches and the fact that GDPR requires data controllers to report any breach within 72 hours of the incident occurring.
2. **Consent**: Since many IoT solutions are made for collecting data which can be connected to a person such as number of steps taken or position. Under GDPR this data will be considered to be personal data and the collection of it may therefore subject to consent from the users. The user must be able to opt-out i.e. withdraw consent from the data collection.

3. **Privacy by design and privacy by default**: Some existing IoT solutions may have been designed without privacy in mind and under the GDPR, data controllers must demonstrate their compliance with privacy by design and privacy by default.
4. **Enhanced data subject rights**: The data subjects under the GDPR, will enjoy expanded rights over their personal data. These rights include: the right to be forgotten, the right to object to automated decision making and data portability rights. IoT systems must be adapted to include these rights.
5. **Processing Personal Data relating to children**: Children under 13 can not consent on their personal behalf to data processing. This can be extended for children up to the age of 15 depending on individual member states legislation. IoT solutions must be adapted to allow for parents consent in these cases.

3.10 Security

This section introduces some security aspects that are used in the architectural solution proposal in Chapter 4.

3.10.1 Confidentiality, Integrity and Availability

Confidentiality, integrity and availability are three important terms used when designing and guiding security policies in an organization. They are also referred to as the CIA triad [41].

Confidentiality

Confidentiality, is the concept about stopping unauthorized users from reading the data that is being sent. This can be divided into two ways of for example concealing a document; either hiding it from unauthorized viewers or hiding the existence of it at all. It has two aspects known as privacy and secrecy. Privacy relates to the protection of personal data and secrecy about protecting data belonging to an organization. Confidentiality can be achieved with encryption or access control [29, 42].

Integrity

Integrity is related to writing of data. The message should be the same when arriving as when it was sent [42]. This includes both intentional alterations made

by an attacker and random transmission errors. D. Gollmann [29] defines integrity in the most common sense as:

> "In general, integrity is about making sure that everything is as it is supposed to be"

Integrity is achieved with different methods, for example hash functions [42].

Availability

Availability according to ISO 7498-2 defined as the property of being accessible and usable upon demand by an authorized entity [43]. This means that in order to achieve availability one must keep strict maintenance on hardware and keep conflict free software so that the system functions as good as possible [41].

3.10.2 Encryption

Encryption is a term describing an algorithm that is used for protecting data confidentiality. This algorithm E uses an cryptographic key k to encrypt a plaintext m into a ciphertext c. This ciphertext can be decrypted with a decryption algorithm D with the key k to retrieve the plaintext again. Encryption and decryption are shown in Equation (3.3) resp. (3.4).

$$c = E_k(m) \tag{3.3}$$

$$m = D_k(c) = D_k(E_k(m)) \tag{3.4}$$

Encryption can be divided into *symmetric encryption* and *asymmetric encryption* algorithms.

Symmetric encryption

Symmetric encryption algorithms use the same key for both encryption and decryption. This means that the sender and receiver share the key and that any malicious party observing the communication cannot read the message [29]. The key in symmetric encryption algorithms is referred to as the *secret key* by convention. Some commonly used symmetric encryption algorithms include AES, Blowfish and 3DES. Symmetric encryption algorithms are often used to encrypt data that is sent [45].

Asymmetric encryption

Asymmetric encryption algorithms, also known as *public key cryptography*, uses different keys for encryption and decryption. The encryption key can be made public but the other one must stay private. Is should not be possible to derive the private key from the public one. The key in asymmetric encryption algorithms is referred to as the *private key* by convention. This is to distinguish it from the *secret key* in symmetric encryption. Some commonly used asymmetric encryption algorithms include RSA, Diffie-Hellman Algorithm, DSA and Elliptic Curve Cryptography. Asymmetric encryption algorithms are often used in key establishment and are slower than symmetric encryption algorithms [29, 45].

For more detailed information about cryptography, consult the *Handbook of Applied Cryptography* [44].

3.10.3 Cryptographic Hash Functions

Cryptographic hash functions are mathematical algorithms that take data of arbitrary length and map this data into a string of fixed length. These functions are designed so that it is computationally easy to calculate the hash value from the plaintext but infeasible to invert the function i.e. calculate the plaintext from the hash value [29]. Cryptographic hash functions can be used to protect data such as passwords or in the case of the GDPR, data pseudonymization.

3.10.4 Key-exchange algorithms

Two parties that want to exchange encrypted messages, needs some type of key-exchange. In this thesis the device needs to send encrypted messages to the server that can only be read by the two parties. Any method in cryptography where cryptographic keys are exchanged between two parties, is called key exchange. In order for two parties to exchange encrypted messages, both must be able to decrypt and encrypt messages. The goal with key exchanging is that no one else can obtain a copy of the private key. To achieve this goal, Diffie-Hellman (DH) key exchange or Ephemeral Diffie-Hellman (EDH) can be used. Furthermore RSA key exchange can also be used. These are recommended by the National Institute of Standards and Technology (NIST) as key management [46].

Ephemeral Diffie-Hellman

Exchanging cryptographic keys over a public channel securely can be done with EDH key exchange. With zero knowledge of each other between two parties, a shared secret key can be established over an insecure channel. The EDH ensures

that each session key between the parties, is different. This enables Perfect Forward Secrecy or PFS [47].

The key exchange procedure is done by following:

1. Client: Requesting connection
2. Server: Suggest generator g and prime p
3. Client and Server: Computes $A = g^a \mod p$ and $B = g^b \mod p$ respectively. (a - Client secret value, b - server secret value)
4. Client and Server: Exchange of A and B - Handshake completed.
5. Client and Server: Computes $S = B^a \mod p$ and $S = A^b \mod p$ respectively - Shared secret key established.

For each new session, the values a and b are changed to ensure PFS is enabled [29]. PFS indicates that the secrecy of old session keys is taken forward into the future. It is important to know that any type of authentication is not provided with EDH, meaning that a Man-In-The-Middle attack is possible.

RSA

The RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem meaning that the encryption key is public and the decryption key is private and different from the encryption key. RSA is used for secure data transmissions and is used widely.

The client public and private key is determined by following:

1. Two large prime numbers are chosen, p and q.
2. The value n is calculated with $n = pq$.
3. The value t is calculated from $(p-1)(q-1) = t$.
4. Integer e is chosen from the conditions that $< t$ and a coprime with t.
5. d is found such that it is the multiplicative inverse of e modulo t.
6. The public key (e, n) is released and the private key (d, n) is kept.

When another party intends to communicate with the client, the message m is encrypted as $c = m^e \mod n$. The client decrypts the message by $m = c^d \mod n$.

The use of RSA ensures authentication since both parties know who they are communicating with [48].

3.10.5 Transport Layer Security

Transport Layer Security or TLS, is a protocol that provides communication security over the network. To provide privacy and integrity between two parties, TLS can be implemented. This means that the message can not be modified between senders and that the data is protected from unauthorized disclosure of information [42]. The protocol also provides with an optional protocol which is the handshake protocol. The handshake protocol provides authentication and key-exchange.

3.10.6 Threats

Threats and attacks come in many different shapes. Attacks can be perpetrated by someone outside or inside a organization. When a device is connected to a network, it will be liable to different threats. In order to understand where a system can be vulnerable, knowing the threats is vital. Below are some of the most common threats on a IoT system listed and explained.

For a list of the most common vulnerabilities with percentages, consult the *CVE Vulnerabilities* site [49].

Denial of Service Attacks

Denial of service attack (DoS attack) is a attack where the perpetrator wants to make a network resource or a machine, unavailable to the intendant users. When the target is flooded with requests, it can be overloaded and prevent legitimate request from being fulfilled. This happens because the victim is forced to perform a huge amount of computations. There are different defense techniques against DoS attacks such as sinkholing, IPS based prevention etc. [29].

Spoofing

The goal of a spoofing attack is to lure the victim to send important data such as for example passwords voluntarily by impersonating the other party that the victim wants to send the data to. An example of a spoofing attack is a program that shows a fake login screen for the victim when he or she tries to log on to a website. The victim enters his or hers credentials. The login screen then stops working and exits out to the real login credentials. The victim then inputs the credentials again, succeeds with login and most likely doesn't suspect any theft of the credentials. Some techniques to defend against spoofing include displaying the number of failed logins to the user, using a trusted path such as CTRL+ALT+DELETE in Windows or using mutual authentication where the system also needs to authenticate itself to the user [29].

Man-In-The-Middle Attack

A Man-In-The-Middle attack or MITM attack, is an attack where the attacker or malicious party gets access to the traffic between two parties by rerouting all traffic through the attacker. The attacker can eavesdrop which means that the attacker can listen to the private conversation of the two parties, without the knowledge of either, this illustrated in Figure 3.3. The only way for the attack to succeed is when the attacker can impersonate each endpoint. Protection to prevent MITM attack is done in most cryptographic protocols by including endpoint authentication [50].

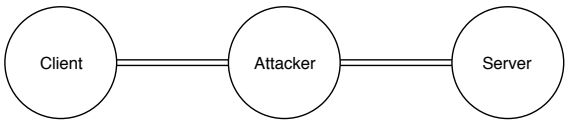


Figure 3.3: The connection during a Man-In-The-Middle attack.

Replay Attacks

In a replay attack, the malicious party impersonates the sender by reusing a compromised session key. The malicious party replays the original message to the receiver at a different time to e.g. authenticate itself as the original sender. To protect against replay attacks, *nonces* i.e. numbers that are used once for each session can be used or generating new keys for every session [51].

Code Injections

When code is introduced by a attacker into a vulnerable computer program to change the course of execution, it is called code injection. Usually, the outcomes of a code injection are disastrous such as corruption or loss of data, denial of access etc. Applications that are vulnerable to this type of attack, tend to send untrusted data to an interpreter. Flaws in applications can be found in SQL, NoSQL queries etc. Prevention against code injections are done in the application code.

A SQL injection is an attack where the attacker uses entry fields on the application to execute malicious SQL statements on the server side. SQL injection is one of the most common web hacking attacks and could destroy databases. Attackers could with the injection, spoof identity, tamper existing data etc [29].

Network Sniffing

Network Sniffing is an attack where the network communication is monitored or listened to by the attacker, this is illustrated in Figure 3.4. The attack can be done in different ways such as when a Wi-Fi is used which makes it possible for anyone to listen. Detecting and preventing this type of attacks is difficult [52].

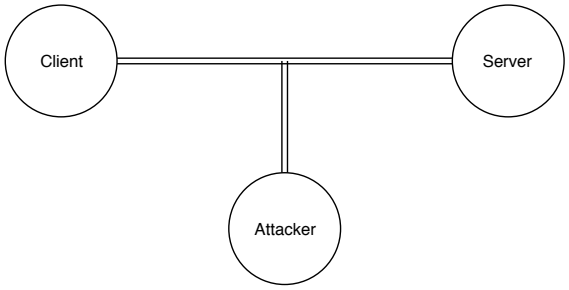


Figure 3.4: Network sniffing.

Brute force/Guessing Attack

When it comes to guessing passwords, the risk of an attacker guessing correctly, can never be completely eliminated. What can be done is to decrease the probability of that happening. In a for example, web application where sign in with credentials are required, this type of attacks are possible. A brute force attack is an attack where the attacker tries all possible combinations of valid symbols. Preventions against these type of attacks are many such as introducing password lengths, mixing all type of valid symbols, avoiding standard passwords, limit number of tries etc. [29].

Chapter 4

Architectural Solution Proposal

This chapter explains the best way in our terms, how to solve the problem of monitoring the usage and position using existing components, softwares and databases. Figure 4.1 shows a brief overview of the system and the flow of information from monitoring the data to collecting it in a database and displaying the information. Since this is the proposed architectural solution, some or most of these components have not been used in the proof of concept solution.

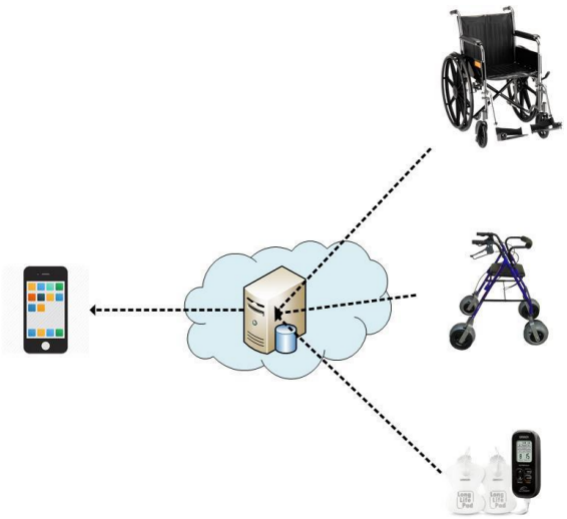


Figure 4.1: Brief overview of the system showing the flow of information.

4.1 Overview of Solution

The design of the architectural solution proposal with encryption and communication techniques is shown in Figure 4.2. The designed systems for the different help aids are approximately the same. The different systems have sensors or a small circuit to detect the usage. Each sensor has a different task to fulfill to ensure the usage, the hall effect sensor detects the wheels spinning, the accelerometer detects motion and the pressure sensor detects the pressure from a person sitting. The use of three sensors ensures that false positives are eliminated. To monitor the usage of the TENS machine, the main function of the circuit in Figure 4.4 is to detect current through the wires to the TENS pads. When the ESP8266, the main communication device, receives a notification from the sensors or the circuit, that the help aid is used, the position of the help aid will be given by the GPS. Positioning and cellular communication are handled by the SIM808 module which uses both GPS and GPRS.

The data containing the position and the device id, will thereafter be sent using mobile telecommunication to the Internet and to the server. Since the data that is sent to the server is considered as sensitive personal data under the GDPR, the solution will follow the concepts *privacy by design* and *privacy by default*. These are achieved by encrypting the database and minimizing the amount of data. Furthermore the patient will have to consent to the data processing. Privacy and integrity over the network is provided by the implementation of TLS. The presentation of the data on the website is the last step in the chain. At this stage the system can be vulnerable to different attacks such as MITM, SQL injections etc.

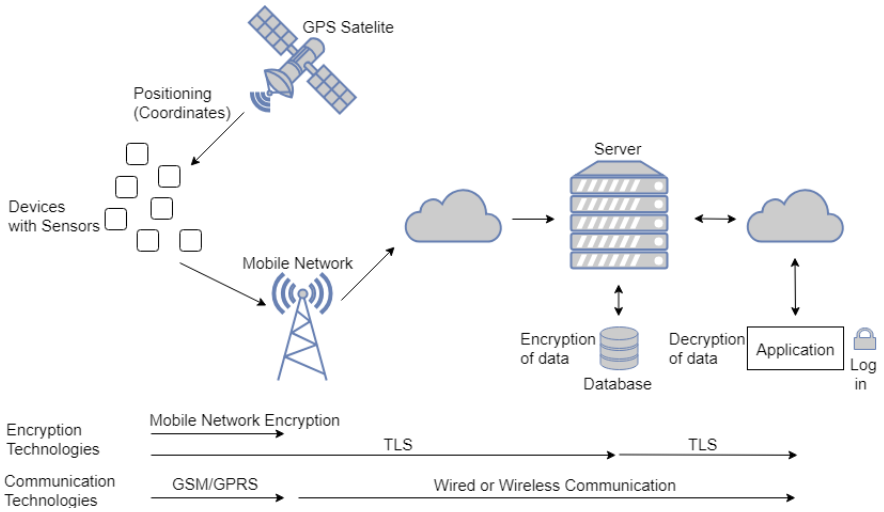


Figure 4.2: Overview of architectural solution proposal.

4.2 Communication

As Figure 4.2 shows, there is a need of reliable communication to every IoT device in the system. Since the system is used to determine if the help aid is used or not, the system is expected to send its information at the most once a day. This means that it is important that the data sent arrives to the database. The amount of data sent is the devices current location and its unique id. The size of the data can be assume to be at most one kilobyte knowing that it only contains the coordinates and the device id and this is not much data. It is also important that, since the device is on a help aid, that the communication is independent of the location of the help aid i.e. that the user can move around freely and that the communication to the database can be guaranteed.

The communication between the components, the outer world and the server can be done using many different techniques. To achieve this, the options from Section 3.7 about wireless communication are considered. These include: GSM/GPRS, 3G, 4G, 5G, NB-IoT, LoRa, Sigfox and Wi-Fi. All of these wireless communication technologies have their benefits and drawbacks. The 5G technology that is designed for IoT solutions is very interesting for this topic, is omitted from the discussion due to it still being in development and not available commercially at the time of writing this thesis. All of the technologies that are listed above provide good outdoor communication but differ in indoor communication, range, speed etc. From the study by M. Lauridsen et al. [1] the technologies GPRS, NB-IoT, LoRa and Sigfox have been compared regarding coverage. The study shows that all technologies have less than one percent outage for outdoor devices. When it comes to indoor coverage, the NB-IoT provides the best coverage. The drawback with the NB-IoT is that since it uses the same resources as LTE, it can experience interference. The drawback with Sigfox is the capacity problems [1]. From an energy consumption perspective, the 3G and 4G networks could be more energy consuming than the GSM/GPRS, NB-IoT, LoRa and Sigfox due to the higher speeds and in areas that lack coverage.

The Wi-Fi is mostly used indoors and works best in an indoor environment of the listed technologies. The range for the Wi-Fi is very limited and makes it unsuitable when the help aid is used in distance from the access point. Another problem with Wi-Fi networks is the connection establishment with the device. If the device could in an easy way connect to free opened secure Wi-Fi networks, it could be used when there is poor mobile coverage as a backup option.

For this system, the choice of communication system is the GSM/GPRS. Since there are no requirements on the system to transmit at high speed and have any latency, the GSM/GPRS is a good choice. It transmits at lower speeds than the 3G, 4G and the NB-IoT, but higher than the LoRa and Sigfox. From an energy consumption perspective it could be lower consuming in areas where 3G and 4G lack coverage and also due to the fact that it is transmitting at lower speeds. The GSM/GPRS provides very good outdoor coverage and a good enough indoor

coverage. The GSM/GPRS already has a good existing system with dense number of base stations.

4.3 Positioning

When it comes to positioning the different help aids, there are different technologies to use. The most common technology used for positioning and navigation is the GPS which should be used in the proposed architectural solution. The accuracy in outdoor environments is set to less than 2.5 m CEP which can be considered good enough. The only drawback is the indoor positioning which could be solved if the indoor positioning was done using peripheral devices or even the Wi-Fi network. Since positioning the help aids indoors is not relevant it is omitted.

4.4 Security and Attack Model

In most of todays IoT devices, the security has not been a priority. There are lots of different types of examples where the IoT devices lack security, such as hacked network-cameras. A system that is connected to the mobile networks or Internet, can be assumed to be in the risk of an attack. Attacks can be performed by a single individual with good knowledge, an organization, a group etc. Attacks are increasing and becoming more sophisticated. The system in this thesis will consider the attacker to be an individual with limited resources and government agencies will be omitted.

In order to keep an IoT system secure, it is important to know what data is necessary to be protected, where the system is vulnerable and what attacks that can be performed against it. It is also important that the system has enough security but not too much. Having too much security i.e. using keys that are too large will result in slow operations due to waste of CPU power for example when encrypting with large keys. This can weaken the user experience and the level of security with large e.g. 2048 bit key sizes is too large for this use case. The sensitive data that needs to be protected is the position of the device and the device id which also is the entire data being sent.

From an energy consumption perspective, there are several factors that can affect the battery life of an IoT device. Factors that matters are for example the size of transmitted data, encryption algorithms, key sizes etc. When determining the level of security and energy consumption, there is always a trade off. Low energy consumption is connected to low security level and high energy consumption is connected to high security level. N. R. Potlapally et al. [2] discusses the energy consumption characteristics of cryptographic algorithms and security protocols. It is for example mentioned that using key sizes of 512 bits instead of 1024 bits for the DH key exchange algorithm, can reduce the consumed energy in the key

generation with 77 percent and in the key exchange with 85 percent. This IoT system in comparison to an IoT system that measures for example the air humidity in a garden, requires a higher level of security due to the fact that sensitive data is transmitted. Therefore the security is more prioritized than the power consumption in this use case, although kept in mind.

Attacks on the system are possible in all steps in Figure 4.2. At the connection between the devices and the server, different types of network attacks are possible such as network sniffing, MITM, spoofing attacks, DoS attacks etc. Some of these attacks are harder to protect against and some are easier. Between the devices and the mobile network, there is mobile network encryption which protects against sniffing for example. To provide privacy and integrity between the devices and the server, TLS is to be implemented in two stages. Firstly, it is used in between each device and the server as shown in figure 4.2. TLS is a protocol that provides communication security over the network. In the implementation, symmetric cryptography e.g AES-128 which is recommended by NIST, will be used to encrypt the data, this will make the connection private and provide confidentiality. Symmetric cryptography is chosen because encrypting and decrypting with symmetric cryptography is faster than encrypting and decrypting with asymmetric cryptography. The keys for the symmetric encryption is done with EDH. This will protect from replay attacks and protect the data since each new session has a unique key. Integrity is provided because the TLS will include a message integrity check using a hash function. Protection against MITM attacks can be done by using TLS. Assuming that the certification authority or CA is trustworthy and that the server key is remained private, the connection can be assumed to be completely safe against MITM attacks. Assuming that the CA is trustworthy is very a bold assumption. In March 2018, Trustico's, a certificate reseller, CEO, transferred the private keys for 23,000 HTTPS certificates via email, which is a non-secure protocol. This implies that Trustico had violated the requirements for certificate authorities by storing these private keys [53]. Authentication is achieved by using public-key cryptography using e.g. RSA. The data is to be stored encrypted in the database in order to be in complaint with the GDPR.

At the second stage between the database and the application, the solution is still vulnerable to the attacks mentioned above, but also against different attacks for example code injections and brute force/guessing attacks. These attacks are possible to be attempted at the stage where requests to the database are made and at the log in stage to the application. In order to protect us in this stage of the system, same implementation as for the first part of the system, is used. Protection against the code injections are done with prepared statements in the code, preventing SQL injections to be executed at the database. Protection against brute force/guessing attacks are done by limiting number of attempts, introducing a password length and a mixing of valid symbols. The password length of eight characters plus a mix of valid symbols, is sufficient enough and follows same password policies as other trusted applications such as Outlook etc.

To make the system even more secure, introducing a multi-factor authentication could be implemented. For the system to be in line with the GDPR, the system

should have a log. Only necessary data should be logged, outdated data should be deleted and should only be accessed by authorized personnel. The log should register any attempt to access the sensitive data.

4.5 Privacy

Since the help aid is used by a patient, the data that is being collected will fall in between Personal Data and Sensitive Personal Data. Because the monitored data is the location of the device and if its being used, the data doesn't directly reveal any medical info but the device ID can be linked to a name in the hospital journals even though the purpose of the solution is to monitor a machine instead of a person. This places the solution in a grey-area where different interpretations of the GDPR laws can result in sanctions. Due to this, it is assumed that the solution handles only sensitive personal data.

In order to make the solution compliant with the GDPR, it must implement the concepts of privacy by design and default. Privacy by design is achieved with data pseudonymization in which all data in the database is encrypted. Privacy by default is achieved by only collecting the minimum data needed i.e. the location of the device and if the device is used. Data minimization is also implemented by only identifying the data with its unique ID and this is not directly linked to a person in the system. This link is found in other patient data systems.

Also, ideally some kind of data splitting is implemented by storing the values on different servers. The encryption should also be made using different keys for each server.

Furthermore, since consent is very important and required especially when dealing with sensitive personal data, any patient using the solution will have to consent to the data processing. The patient does have the right to withdraw consent when he/she so chooses. Also any child under the age of 13 will need parents consent. Also to allow for the right to be forgotten, the patient will get to have his/her entries removed from the database.

4.6 User interface

When data is collected and stored in the database, it must be presented easy and well. Ways to present the data can be either a mobile application, web application or both. The user interface should start fast, be easy to use in terms of navigation and have enough information, it should always be available for authenticated personnel after they login to the system using credentials etc. The application has to be safe and have some type of protection against attacks such as the ones

mentioned in Section 4.4. The presented data should at least show where and when a help aid has been used.

The target group for the user interface is an employee working for the stakeholder i.e. a help central in Sweden. Since there are no commercially available solutions for this use case, it has to be implemented. Implementing the interface in the existing journal system is not relevant due to the fact that only help aid needs to be monitored. Since medical journals contain sensitive personal data, this introduces difficulties concerning the GDPR.

4.7 Monitoring usage

This section describes the architectural solution proposal for the different help aids in detail.

4.7.1 Wheelchair and Walker

Monitoring the usage of the wheelchair and the walker, can be done in different ways using different sensors. To determine whether to use the accelerometer, hall-effect sensor, the pressure sensor or a combination of them, it had to be put to a test. Usage is defined in an earlier section as:

- Wheels spinning.
- A person seated (wheelchair).
- Movement in a reasonable speed.

Using only the hall-effect sensor to determine the usage, is not the most efficient way. The sensor only tells if the wheels are spinning, that does not imply that someone is in fact using the help aid. The wheel could be triggering the sensor just by moving it back and forth a few cm or it could even be someone that is transporting the help aid by pushing it from behind.

Using the pressure sensor only, will let us know if the breaks are released or if someone is sitting on the wheelchair. It wont in fact tell if its moving at all or if it is moving in reasonable speed.

If the accelerometer is used alone, it will only tell us that the object is moving and at what speed, but not if there is someone pushing it from behind, if it is transported in a car nor if someone actually sits on it.

To make sure that the help aid, is used to basis of the given definitions, a priority of the sensors have been introduced as in Figure 4.3 and as following:

1. The Hall-Effect sensor detecting spinning wheels.
2. Pressure sensor detecting a person being seated (wheelchair).
3. Accelerometer sensing a movement in reasonable speed.

The hall-effect sensor is tended to be placed at the metal holding the wheels and a magnet is attached to the wheel. Every turn of the wheel is then registered. The pressure sensor is placed on the seat/brakes and the accelerometer is placed at any optional spot.

4.7.2 TENS Machine

The TENS machine used in this project is an LT3011A from Clas Ohlson. The machine is programmed with many different programs for several different body areas. It also has modes for EMS and massage therapy. For this project only the TENS mode is considered. The specifications for the modes are shown in Appendix A.

From the table in Appendix A, several measurements were made on the machine in different modes so that each type of signal modulation was investigated. This was done in order to understand the behaviors of the different modes and to reliably select hardware. The measurements were made over an 1 $k\Omega$ resistor directly coupled to the TENS machines cables. Every pulse from the machine is a square wave and the following different signal modulations are introduced below:

- Simple modulated: The pulse width increases gradually over time.
- Hans: The pulse frequency changes in between 2 and 80 Hz.
- Continuous: The pulse is constant with a low frequency
- Amplitude modulated: The pulse width increases gradually over time.
- Pulse width modulated: The pulse width increases periodically over time.
- Synchronous: The pulse is constant but rises up to amplitude gradually.
- Asynchronous: Same as synchronous but the voltage level stops at an determined V_0 when rising and falling.
- Alternate Ramped burst: Similar to asynchronous but faster shifts between rise and fall.

All measured signal modulations are shown in Appendix B.

It is not that easy to assume that the TENS machine is used when the power is drawn from it. The TENS machine looses power by being turned on without actually running any program. Designing a circuit that measures the power level

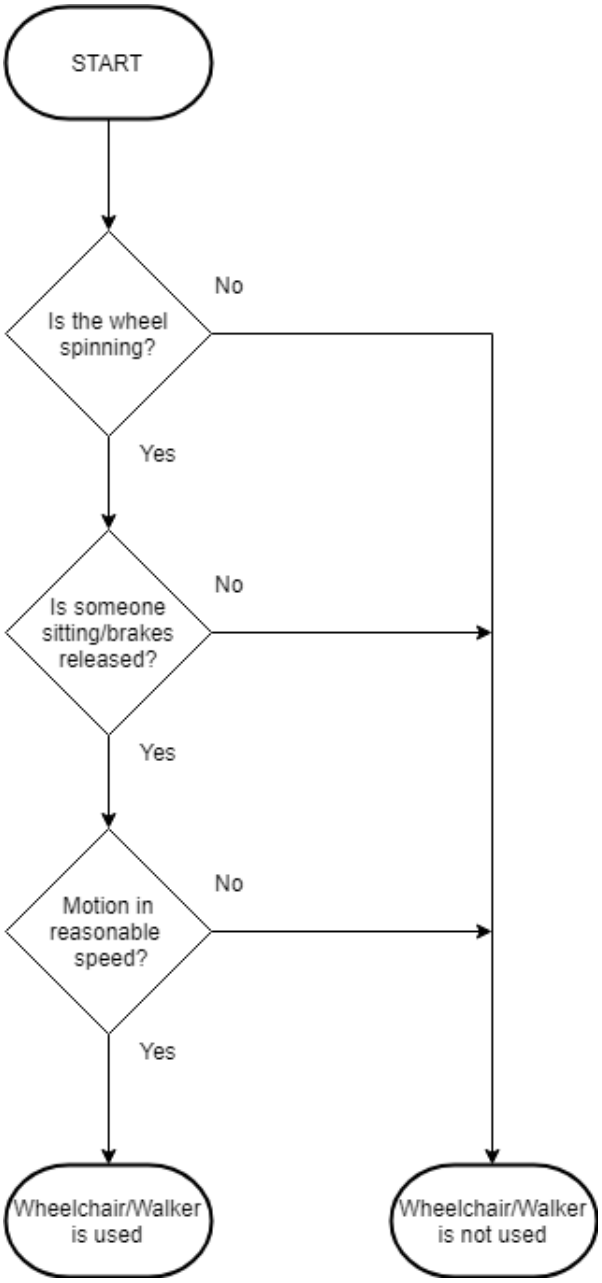


Figure 4.3: Priority flowchart of the sensors used for the wheelchair and walker solutions.

won't be enough to make sure it is actually used. It is only when current is conducted through the wires from the TENS machine to the TENS plates.

The wires from the TENS machine are male plugs to which the female plugs from the TENS plates are connected. Building the circuit in Figure 4.4 as an integrated circuit and using the construction as a bridge between the male and female plug. Each time the TENS machine sends a pulse through the wires, the circuit will detect the pulses, and signalize the ESP8266 by setting one of the pins on the ESP8266 to a digital one.

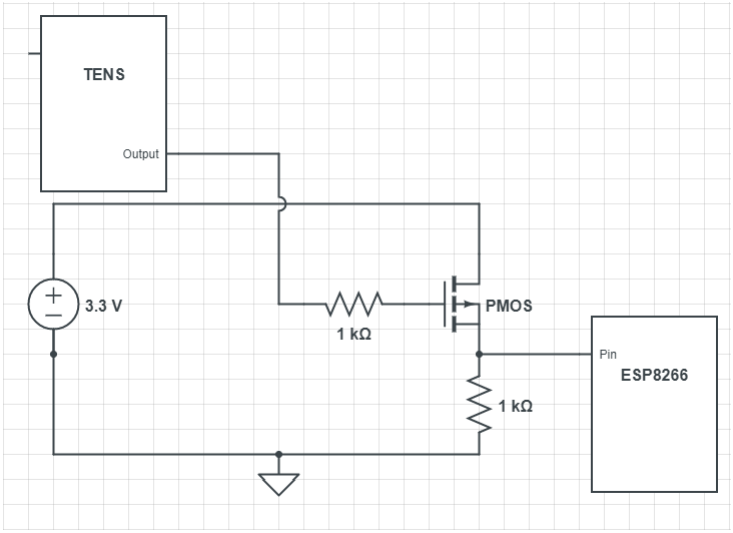


Figure 4.4: Bridge circuit detecting current through the wires from the TENS machine.

The circuit is built up with one a 3.3 V power supply, two resistors and one PMOS transistor. The transistor is a P-type metal-oxide-semiconductor or PMOS that uses the p-channel of a MOSFET. Creating a inversion layer or a p-channel in an n-type transistor body, lets PMOS transistors operate. The drawback with the PMOS is that it conducts when there is zero voltage at the gate. This can be either be solved with hardware or easily solved in the coding.

4.8 ESP8266

The ESP8266 module seen in Figure 4.5 can give microcontrollers access to Wi-Fi networks. It is a SOC with a full TCP/IP protocol stack [54]. It is provided with 16 GPIO's which through the firmware, can be assigned different functions.

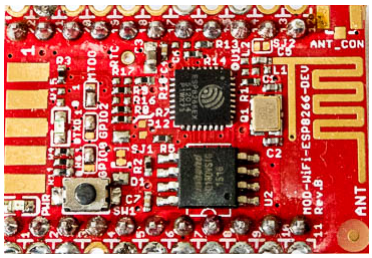


Figure 4.5: MOD-WIFI-ESP8266-DEV (ESP8266 module).

Technical features [55]:

- 802.11 b/g/n
- Wi-Fi Direct (P2P), soft-AP
- Integrated TCP/IP protocol stack
- Integrated TR switch, balun, LNA, power amplifier and matching network
- Integrated PLLs, regulators, DCXO and power management units
- +19.5 dBm output power in 802.11b mode
- Power down leakage current of $< 10\ \mu$A
- 1MB Flash Memory
- Integrated low power 32-bit CPU could be used as application processor
- SDIO 1.1 / 2.0, SPI, UART
- STBC, 1x1 MIMO, 2x1 MIMO
- A-MPDU & A-MSDU aggregation & 0.4 ms guard interval
- Wake up and transmit packets in < 2 ms
- Standby power consumption

The ESP8266 is a popular choice of module when it comes to IoT, mainly because of its size and functionality.

4.9 SIM808

Figure 4.6 shows the SIM808 which is a module providing a complete Quad-Band GPRS/GMS combined with GPS technology. This means the module can be used to send SMS, send data and even use satellite navigation.

Sending data through GPRS can be done at 85.6 kb/s and the accuracy for the GPS can be set to less than 2.5 m CEP. Circular error probability or CEP is a measure of a systems precision. It is defined as the radius centered on the mean, where the precision is expected to be at least 50 percent of the time. In this case, 50 percent of the time the accuracy for the GPS is less than 2.5 m [56].

Figure 4.6: The SIM808 module with GPS positioning and GPRS mobile communication.

The module is compatible with a AT cellular command interface. The AT cellular command interface has AT commands that are instructions to control a modem [57]. SIM808 also have optional interfaces such as SPI.

4.10 Sensors

This section describes the specific chosen components. These are going to be used to monitor the usage and the position.

4.10.1 Accelerometer

To measure acceleration from a rest frame, the LSM9DS1 is used which can be seen in Figure 4.7. Apart from 3 acceleration channels, the LSM9DS1 also provides 3 angular rate channels and 3 magnetic field channels. It has I^2C/SPI as serial interfaces [58].

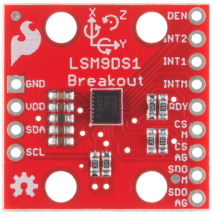


Figure 4.7: The LSM9DS1 accelerometer module.

4.10.2 Hall-effect sensor

The used hall-effect sensor is TLV4964-5TA which is a integrated hall-effect sensor. When the sensor detects a magnetic flux and the flux exceeds the set threshold, the sensor switches the output. By default the sensor switches from a digital one to zero. From an energy consumption point of view, this is not ideal, therefore an inverter was implemented to reduce the energy consumption [59]. Figure 4.8 shows the sensor from the bottom and from the side. The pin number 1 is the

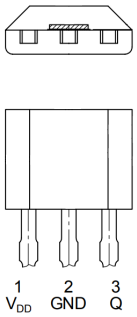


Figure 4.8: The hall-effect sensor and its pin layout.

V_{dd} which function as the supply voltage and pin number 2 is the ground. Pin number 3 which has the symbol Q, is the output. When the sensors is operating the sensitivity to sense is at 7.5 mT.

4.10.3 Pressure Sensor

The used pressure sensor is a force sensitive resistor (FSR) with a square sensing area. Depending on the force that is applied on the area, the resistance will vary. When there is no force on the area, the resistance is approximately 1 MΩ. The larger the force, the less resistance [60]. The FSR can bee seen in Figure 4.9.

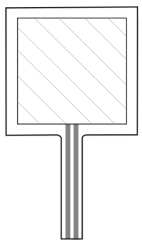


Figure 4.9: The force sensitive resistor.

There are two pins at the bottom of the sensor, where the one to the right is VCC and the one to the left is the GND.

Chapter 5

The proof of concept solution

This chapter introduces and explains the implementation of the proof of concept solution to the architectural solution proposal. The design of the proof of concept solution is shown in Figure 5.1. The difference from this solution and the architectural solution design, is the fact that the GPS and GSM/GPRS have have been omitted. Instead, the data is sent through the router to the Internet. The location of the help aid is given using Google Geolocation. Even though low energy consumption is often a requirement in an IoT system, it has been omitted in the proof of concept solution.

5.1 Assumptions

To solve this problem within the given time frame and other limitations, some assumptions had to be made in order to focus on the key issues. The main assumption considers the communication and positioning methods. It is assumed that each help aid is used in an environment with access to at least three AP's, one of which has a connection with the device on the help aid. The AP's exist in the Google Geolocation database. This allows for more focusing towards the usage monitoring issue and less on independent communication and positioning methods.

5.2 Overview of Solution

The design of the proof of concept solution is shown in Figure 5.1. The main difference between this solution and the architectural solution proposal, is the communication channels. Just like the architectural proposal solution, the proof of concept solution is implemented in the same way regarding on which sensors are used and why. When it comes to the solution for the TENS machine, the

proof of concept solution uses a NPN transistor instead of a PMOS transistor. When the ESP8266 that is connected to the Wi-Fi network, receives a notification from the sensors or the circuit that the help aid is used, the ESP8266 does a scan on access points nearby. The MAC-addresses and the signal strength from three access points are collected and sent to the Google Geolocation API, to determine the position of the help aid. The accuracy is good but not like when the position is determined with GPS. The data containing the device id and the position is sent to the server. The server is located locally on the local network and can only be accessed when being connected to the same network. This prevents many of the attacks mentioned in earlier chapters. The web application is also hosted locally and gives the user a opportunity to choose, which device it wants to get information about. The information received is the last position of the specific device on a map.

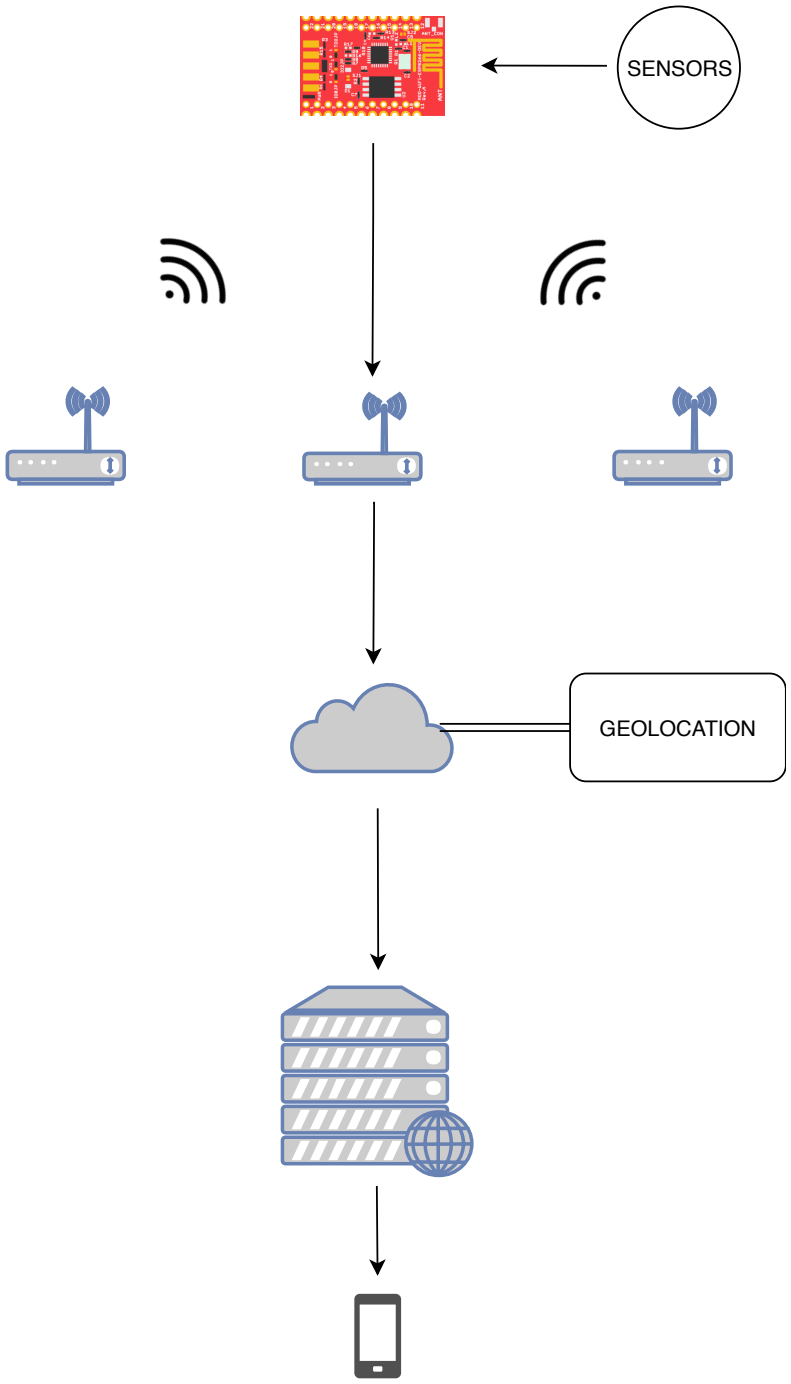


Figure 5.1: Overview of the proof of concept solution.

5.3 Communication

Since it is assumed that the proof of concept solution is set in a local environment and the ESP8266 has built in Wi-Fi chip, the communication to the Internet will be done with Wi-Fi. This allows us to focus more on the usage and positioning aspects of the problem in the proof of concept.

5.4 Positioning

Unlike for the ideal solution which uses GPS to locate itself, the proof of concept solution uses geolocation to achieve the same result. This solution uses an Google API which is open for everybody to use. As stated in Section 3.6.2, the API does require either some Cell Tower objects and/or some Wi-Fi access point objects as input. For the use case of this solution no cell tower information is sent due to the ESP8266's Wi-Fi only capability. This means that the following parameters are sent to the API and these are given in the list below:

- `considerIp: false`. Set to false to disable IP location due to high inaccuracy.
- `wifiAccessPoints`:
  - `macAddress`
  - `signalStrength`

The `considerIp` field is set to *false* due to high inaccuracy of IP location. This is used as default if the given AP's are not mapped in the Google database. This setting has the unfortunate effect of not giving any location data in that case, but since the proof of concept is set in an environment with access to already mapped AP's this is not an issue in this use case. The Wi-Fi access point objects are obtained using the `wifi.sta.getap()` function in NodeMCU which scans an AP list as an Lua table. This table is then formatted into a JSON object. Apart from the required MAC-addresses, the signal strengths of each AP are provided as well. An example of a request body sent to the Google Geolocation API is shown in Listing 5.1. Here three Wi-Fi access point objects are sent.

```
{
  "considerIp": "false",
  "wifiAccessPoints": [
    {
        "macAddress": "70:7d:b9:8b:54:22",
        "signalStrength": -59,
    },
    {
```

```
        "macAddress": "d8:9d:67:50:c5:11",
        "signalStrength": -79,
    },
    {
        "macAddress": "70:df:2f:1a:e1:a1",
        "signalStrength": -80,
    }
  ]
}
```

Listing 5.1: Example of an request body for the Google Geolocation API.

The API will then return an JSON object containing the latitude and longitude of the device, together with an accuracy radius in meters. An example of the JSON object is shown in Listing 5.2.

```
{
  "location": {
    "lat": 55.614254,
    "lng": 12.989117
  },
  "accuracy": 20
}
```

Listing 5.2: The response from the Google Geolocation API.

Geolocation provides a fairly accurate way of determining the location of the help aid and is considered to be sufficient for this proof of concept solution.

5.5 Security

To make the system safe, the application and the database for this system, has been implemented locally. This means that they are only reachable if and only if the user is connected to the local Wi-Fi network. When it comes to protection against attacks, password policies and logs, they have all been omitted due to the fact that they are not a center part of this solution.

5.6 Data handling, Database and GDPR

This section explains how the REST API is set up and how the database is set up with the GDPR in consideration.

5.6.1 REST API

In order to send data to the database a RESTful API has been set up. This API is based on the flask module for Python.

The data from the ESP8266 is sent as an JSON object containing the `lat` and `lng` location parameters from the Google Geolocation API in Section 5.4 and the `ID` parameter containing an unique id for each ESP8266. An example of the data sent is shown in Listing 5.3.

```
{
  "location": {
    "lat": 55.614254,
    "lng": 12.989117
  },
  "ID": XCDWSEOPFS3
}
```

Listing 5.3: The data sent from the ESP8266 to the API.

From this JSON object, the main parameters are extracted out and formatted for the database. The `lat` and `lng` parameters are combined into a `coordinates` parameter. Also, an time stamp of each entry is sent to the database.

5.6.2 Database and GDPR

The database is located at a virtual machine and is handled with MySQL. The database is hosted by Amazon web Services. One thing to have in mind is that Amazon web Services is vulnerable to Meltdown, which is a vulnerability that allows a rogue process to read all memory without being authorized to it [61]. The machine and database is built up with three separate structures containing information. The structures are built up as columns that contain the parameters: `ID`, `coordinates` and `time_stamp`. In order to comply with the GDPR, the `ID` column is stored encrypted in the database. This is an implementation of privacy by design with pseudonymization. This is done because only the `ID` field is linkable to a persons identity. Privacy by default is implemented with data minimization as in the ideal solution. However, due to the solution being a proof of concept, the consent rules are not being considered or implemented.

5.7 User interface

The collected data from the device is presented in a particularly easy manner. A website consisting of an input box and a map. After input in the box the

website provides the location of the help aid and what time it was monitored. This is sufficient enough to showcase the position and usage data to the owner. A screenshot of the website is shown in Figure 6.3.

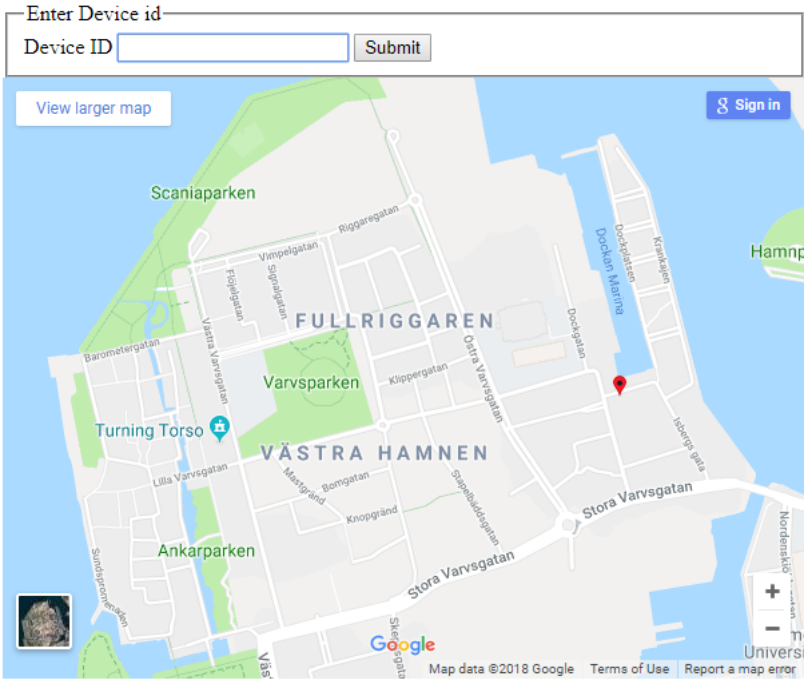


Figure 5.2: Screenshot of the web user interface.

5.8 Monitoring Usage

This section describes the proof of concept solution for the different help aids in detail. Here, any differences to the architectural solution proposal are also highlighted.

5.8.1 Wheelchair and Walker

The proof of concept solution have been implemented in the same way as in the architectural solution proposal. Since usage is the focus of the thesis, the most suitable solution has been implemented.

5.8.2 TENS Machine

Monitoring the usage of the TENS-machine is not a simple task and it can be done in different ways. Attempting to use the Hall-Effect sensor as a way to monitor the usage, failed. The magnetic field strength from Equation (3.1) in this case is:

$$B = \frac{4\pi \cdot 10^{-7} \cdot 10^{-3}}{2\pi \cdot 10^{-3}} = 0.2\ \mu\text{T}$$

which is sufficiently lower then the sensitivity on 7.5 mT. The sensor is not capable to detect the magnetic field created by the wires. This can depend on several factors, the current through the wires is not constant, the magnetic field is not strong enough to be detected by the sensor, the sensor needs better sensitivity, there is a plastic cover around the wire that weakens the field etc.

Another way to solve the problem is to build the circuit in Figure 5.3. The challenge with the TENS-machine is that its output tends to be different depending on what treatment the user chooses. What all the different treatments outputs have common is that the current out is low and the pulses are short. This is a problem for the transistor, since it wont be able to register anything at the gate. The used transistor is a BC647C transistor which is a NPN-transistor.

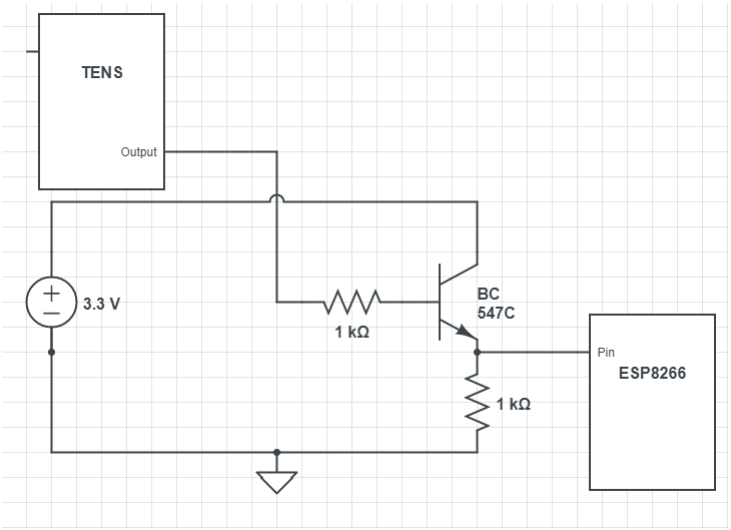


Figure 5.3: The designed circuit detecting conducted current.

A NPN-transistor is one form of a Bipolar Transistor or BJT. The NPN has the collector and the emitter negative and the gate positive which also can be seen in Figure 5.4. The NPN is the most commonly used transistor and they function as amplifiers or electronic switches [62]. The transistor in this case is used as a electronic switch to trigger a pin at the ESP8266, notifying it that the TENS-machine is in use.

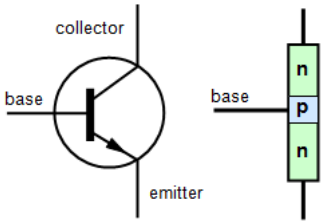


Figure 5.4: A NPN-transistor.

As mentioned earlier, the outputs from the TENS-machine differ. To help the transistor to register values at the gate, a small circuit is constructed at the gate. The output from the TENS-machine is connected to a resistor of 1 kΩ in series with a resistor of 1 MΩ and capacitor of 10 μF, which are in parallel. This circuit charges the capacitor with the output from the TENS-machine. The capacitor slowly discharges to the gate and makes sure the transistor has time to switch.

The solution is generally the same as in the architectural solution proposal. However the difference in the use of transistor is due to material constraints. The same result is still achieved with a BJT transistor. Also, the BJT conducts when the gate is a digital one instead of zero as in the PMOS transistor. This allows us to omit an inverter on the gate since we want to trigger the ESP8266 on signal in the wire.

Chapter 6

Evaluation of proof of concept solution

This chapter describes the different tests done on the different help aids and evaluates the outcome of the proof of concept solution with the focus on the usage and positioning.

6.1 Usage Evaluation of Wheelchair and Walker

Different tests on the wheelchair and walker has been done in order to monitor the usage. Testing the usage of the wheelchair and walker is done by attaching the sensors to their positions on the help aid as defined in Section 2.3.3. Then a series of tests were done with the help of an employee from Cybercom who used a wheelchair. These tests include sitting in the wheelchair while moving around in different speeds to examine if the system, with the priority of sensors works as defined in Figure 4.3.

Firstly, the detection property of the hall-effect sensor was tested by spinning the wheels of the wheelchair and walker in one direction at various speeds. A simple test was done inside the Cybercom office space. A distance of 20 m was measured out where the wheelchair was put into motion. The wheel diameter was measured to be 60 cm which results in a circumference of 2 m. This means that for a distance of 20 m there are $20/2 = 10$ revolutions. The expected result is that every revolution results in a hit in the sensor i.e. 10 hits for the distance. In Figure 6.1 the hit rates are shown for different speeds. The hitrates show the mean of five test runs per speed interval.

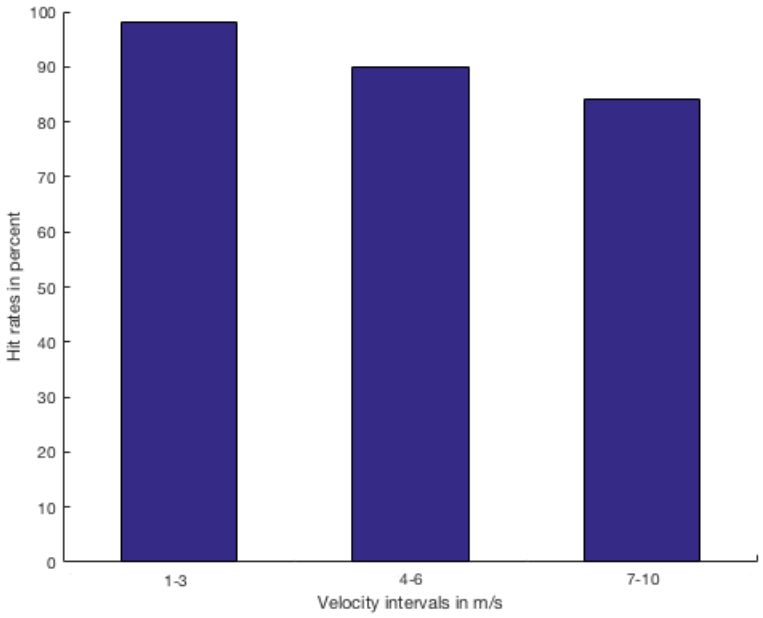


Figure 6.1: The mean hit rates of five test runs of wheelchair in different speed intervals.

The results from this test showed that the hall-effect sensor is very accurate at low speeds. This accuracy decreases marginally under higher speeds to about 85% which is still a very high accuracy.

The property of the pressure sensor was tested by placing the sensor on different spots at the seat. Since the sensor is very sensitive, it did sense pressure without any problems. The results showed that it could be placed almost anywhere on the seat, but recommended on the area around where the bottom is placed on the seat. The property of the accelerometer was tested with different methods. First it was calibrated when the help aid was not moving, in order to read zero acceleration. The results were as expected i.e. zero. Another test was set up to see if the accelerometer sensed movement in any horizontal direction. When moving the help aid around, the accelerometer sensed this and the output from the accelerometer was reasonable with both acceleration and direction. The results also showed that the accelerometer was very sensitive and any small movement was detected. Lastly, a test was made to ensure that the priority of sensors worked as defined in Figure 4.3. The test showed that the system worked accordingly to the priority setup in the figure and that any other priority order did not give any false positives.

6.2 Usage Evaluation of TENS Machine

In order to monitor the usage, several tests have been done on the TENS machine. All the different modulations in Appendix A have been studied in order to understand the signal outputs from the TENS machine. Results from test on the modulations are shown in Appendix B. All the different modulations are square pulses, making the design of the circuit less complex. The designed circuit detects each modulation on the lowest output on 1 mA easily. Higher outputs of 10 mA and maximum 30 mA are also easily detected by the circuit.

To make the test more practical, the TENS machine was tested by ten different men and women with different weights, as the usage was to be monitored. The results differ depending on the weight of the person and the distance between the TENS pads. The more weight the person has and the further the distance is between the TENS pads, the detection of the current through the wires was a little bit more difficult. With these results in hand, the tests were changed and performed at the biggest muscle area of the human body i.e. the back. The TENS pods were placed on the back with the biggest distance possible. This test showed that the circuit did detect every other pulse from the TENS machine with outputs being 1 mA from the TENS machine. First when the output was raised to 3 mA, every pulse was detected by the circuit.

These results are acceptable due to the fact that the circuit can detect pulses when the TENS pads are far distanced. Also from the results, we can see that the solution achieves good usage monitoring when tested on different persons with differing builds and physique.

6.3 Testing and evaluation of positioning

In order to show that the position of the help aid and that the usage is registered in the database full tests of the system were made. As stated before, every entry into the database guarantees usage of the help aid. Figure 6.2 shows a sample of five entries in the database. Here the `ID` column is a unique identifier for each help aid, `coordninates` show its position at the time of sending and the `time_stamp` shows when the entry has been made in the database.

ID	coordinates	time_stamp
XCDWSEOPFS3	55.614254,12.989117	2018-03-18 14:21:04
QRC53908AL	55.614468,12.989040	2018-03-19 11:11:54
RCOTM987CVL	55.613941,12.989281	2018-03-20 16:31:09
PVKDKM45SRG4	55.611814,12.980363	2018-03-22 10:52:43
XSSDF35MCKSO	55.608829,12.999363	2018-03-23 13:23:34

Figure 6.2: Screenshot of the database containing id, coordinates and time stamps.

The entries from Figure 6.2 are then shown in the user interface on a map. The entries from the example above are shown in Figure 6.3.

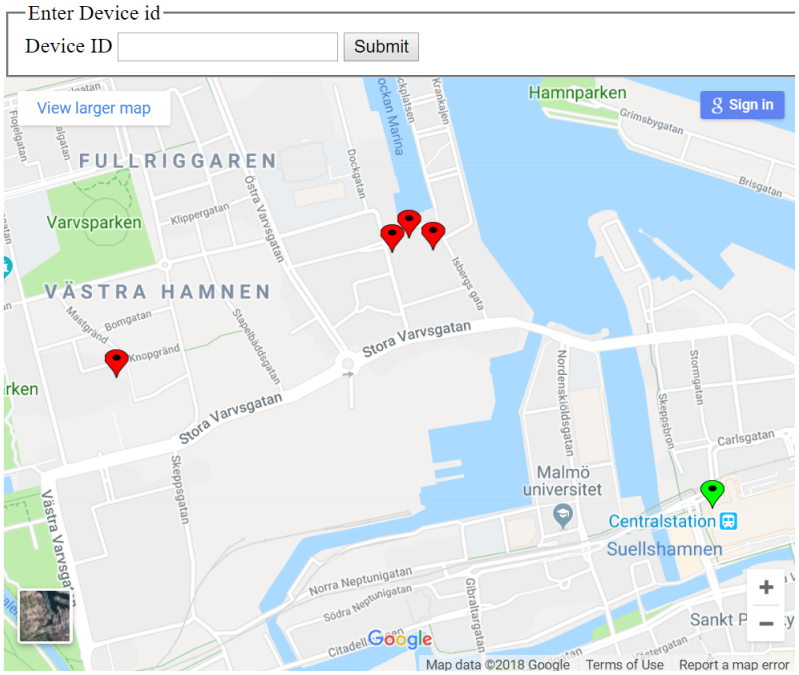


Figure 6.3: Screenshot of the map showing five different positions of the help aid.

Testing the accuracy of the Google Geolocation API was performed at different locations in the Malmö area where there was an open Wi-Fi network with at least three access points. The green pin in the figure shows a test where the access points could not be geolocated. Even though the help aid was located in the Cybercom offices the location was given at the Malmö central station about 700 meters away with an accuracy radius of 750 m. This means that the API defaulted to IP location which resulted in very low accuracy. Unlike as stated in Section 5.4, the `considerIp` field was set to *true* for the purposes of this test to show the inaccuracy of IP location. Every red pin is a correct location where the API managed to locate the help aid at an accuracy of around 20 m. These results can be assumed to be satisfactory but still not as good as the GPS accuracy.

Chapter 7

Conclusion

This chapter evaluates both the architectural proposal solution and the proof of concept solution. It answers the research questions in Section 1.2.1. The chapter also presents our thoughts on how this project could be evolved regarding the GDPR, security etc. in the future.

7.1 Comparison And Evaluation of Solutions

The reason behind the division between an architectural solution proposal and a proof of concept solution is to show a comprehensive design solution to the problem on how it should be solved and a solution that serves as a proof of concept. It also allows us to focus on the more important aspects of solving the problem i.e. the usage and location aspects of it.

The architectural solution proposal represents how we expect and think that this problem should be solved in the most optimal way. It also represents the best solution for the stakeholder of this project based on their requirements. The architectural solution proposal, with its GSM and GPS capabilities, allows for greater location and communication independence which is expected for a person using any one of the three help aids in the problem. Using Wi-Fi as the communication method over open networks is a big security issue and should not be used. Therefore, the use of GSM is preferred. Furthermore, the solution is assumed to be secure against the most common attacks that may affect an IoT system.

In this thesis, the proof of concept solution implements the architectural solution proposal scaled down to the minimum requirements for communication and location. the proof of concept is based on solving the objectives and the research questions within the limitations.

It has been shown in this thesis that it is possible to monitor the usage and the position of the help aids dependent on requirements. When it comes to the

wheelchair, it has been shown that using multiple sensors, is the best way to assure the usage. Both in the architectural solution proposal and the proof of concept the hall-effect sensor, pressure sensor and accelerometer were used. These sensors can be placed and will be placed differently depending on the design of the wheelchair. One can assume that the pressure sensor should be placed somewhere where it can detect force from a sitting person. The hall-effect sensor should be placed somewhere so that it can sense the magnetic field. The accelerometer can be placed freely somewhere on the wheelchair.

The solution for the walker has the same design thinking as the wheelchair except the fact that the pressure sensor might be unnecessary. As for the placement of the sensors, the hall effect should be placed at the wheels and the accelerometer can be placed freely.

For the TENS-machine, the best way is to build an integrated circuit that works as a bridge and that detects the current through the wires. It is also important to understand that the designs of the TENS-machines differ depending on the manufacturer. The pulses sent from the TENS-machines through the wires, can vary and that could change the selection of hardware in the circuit.

The implementations can in a sufficient way be adapted to the GDPR as shown in Section 4.5. In order to not have unnecessary data which can conflict with the design by default requirement in the GDPR, the collected data has been minimized. The data only contains id, location and time stamp. The collected data can be saved as it is done in the proof of concept solution but it is recommended to be saved as in the architectural solution proposal, mostly due to the GDPR. As of writing this thesis, the GDPR hasn't come into effect and there exists many parts of it that are open to interpretation. This means that our interpretation of what is GDPR compliant may be wrong and the data handling might need to be reworked.

7.2 Future work

The natural upcoming step in as future work is to implement the architectural solution proposal. Creating an independent device that can communicate to the server regardless of its location is important to be able to showcase it in a realistic environment. The finished system has to be secure from all mentioned attacks and be in compliance with the GDPR.

This solution can be used in other cases and the collected data can be valuable for doctors. They can use this to make sure their patients follows up with the treatments that are presented to them. However this might introduce new GDPR problems due to switching the monitoring from machines to their users. Since IoT solutions are on the rise today, any application that wants to monitor the usage and position of anything can use a similar scheme.

There are daily new attacks that could be used against a system like this. Therefore it is important to be updated with the latest information about security breaches.

Bibliography

[1] Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen and M. Sorensen, "Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area," 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, 2017, pp. 1-5. doi: 10.1109/VTCSpring.2017.8108182

[2] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," in IEEE Transactions on Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006. doi: 10.1109/TMC.2006.16

[3] D. Ding et al., "A Wheelchair Usage Monitoring/Logging System," 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference, Shanghai, 2005, pp. 6897-6899. doi: 10.1109/IEMBS.2005.1616091

[4] Funka. 'Funka statistik', 2018. Available: `https://www.funka.com/design-for-alla/tillganglighet/statistik/` [Accessed: 29 Mar 2018]

[5] Ericsson. 'Internet Of Things forecast', 2018. Available: `https://www.ericsson.com/en/mobility-report/internet-of-things-forecast` [Accessed: 16 Mar 2018]

[6] Ericsson. 'White Paper: Cellular networks for massive IoT', 2018. Available: `https://www.ericsson.com/assets/local/publications/white-papers/wp_iot.pdf` [Accessed: 16 Mar 2018]

[7] Heath, S. Embedded Systems Design. Oxford: Newnes, 2005

[8] L. K. P. Saputra and Y. Lukito, "Implementation of air conditioning control system using REST protocol based on NodeMCU ESP8266," 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), Yogyakarta, 2017, pp. 126-130. doi: 10.1109/ICON-SONICS.2017.8267834

[9] NodeMCU. 'NodeMCU Documentation', 2018. Available:
https://nodemcu.readthedocs.io/en/master/
[Accessed: 16 Mar 2018]

[10] Lua. 'About LUA', 2018. Available:
https://www.lua.org
[Accessed: 16 Mar 2018]

[11] Sparkfun. 'Accelerometer', 2018. Available:
https://learn.sparkfun.com/tutorials/accelerometer-basics
[Accessed: 16 Mar 2018]

[12] Wikipedia. 'Hall effect sensor', 2018. Available:
https://en.wikipedia.org/wiki/Hall_effect_sensor
[Accessed: 12 Apr 2018]

[13] Wikipedia. 'Pressure sensor', 2018. Available:
https://en.wikipedia.org/wiki/Pressure_sensor
[Accessed: 12 Apr 2018]

[14] NXP. 'UM10204 I2C-bus specification and user manual', 2014. Available:
https://www.nxp.com/docs/en/user-guide/UM10204.pdf
[Accessed: 29 Mar 2018]

[15] Sparkfun. 'Serial Peripheral Interface (SPI)', 2018. Available:
https://learn.sparkfun.com/tutorials/serial-peripheral-interface-spi
[Accessed: 29 Mar 2018]

[16] Wikipedia. 'Global Positioning System', 2018. Available:
https://en.wikipedia.org/wiki/Global_Positioning_System
[Accessed: 29 Mar 2018]

[17] Wikipedia. 'Geolocation', 2018. Available:
https://en.wikipedia.org/wiki/Geolocation
[Accessed: 13 Apr 2018]

[18] Google. 'Geolocation documentation', 2018. Available:
https://developers.google.com/maps/documentation/geolocation/intro
[Accessed: 01 Apr 2018]

[19] M. Rahnema, "Overview of the GSM system and protocol architecture," in IEEE Communications Magazine, vol. 31, no. 4, pp. 92-100, April 1993. doi: 10.1109/35.210402

[20] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen and M. Sorensen, "Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT," 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, 2017, pp. 1-5. doi: 10.1109/VTCSpring.2017.8108666

[21] E. Ezhilarasan and M. Dinakaran, "A Review on Mobile Technologies: 3G, 4G and 5G," 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), Tindivanam, 2017, pp. 369-373. doi: 10.1109/ICRTCCM.2017.90

[22] G. Stüber, Principles of Mobile Communication 4:th Edition. Atlanta: Springer, 2017

[23] M. Kihl, J. Andersson, Datakommunikation och nätverk. Lund: Studentlitteratur, 2014

[24] W. Ayoub, M. Mroue, F. Nouvel, A. E. Samhat and J. c. Prévotet, "Towards IP over LPWANs technologies: LoRaWAN, DASH7, NB-IoT," 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC), Beirut, Lebanon, 2018, pp. 43-47. doi: 10.1109/DINWC.2018.8356993

[25] A. Hoglund et al., "Overview of 3GPP Release 14 Enhanced NB-IoT," in IEEE Network, vol. 31, no. 6, pp. 16-22, November/December 2017. doi: 10.1109/MNET.2017.1700082

[26] Lora Alliance. 'Lora Alliance', 2018. Available: https://lora-alliance.org/ [Accessed: 16 May 2018]

[27] Sigfox. 'Sigfox Technology Overview', 2018. Available: https://www.sigfox.com/en/sigfox-iot-technology-overview [Accessed: 16 May 2018]

[28] J. Kurose, K. Ross, Computer Networking A Top-Down Approach. New York: Addison-Wesley, 2009, pp. 537-538.

[29] D. Gollmann, Computer security 3:rd edition. Chichester: Wiley, 2011.

[30] Wi-Fi Alliance. 'Wi-Fi Alliance introduces security enhancements', 2018. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements [Accessed: 16 May 2018]

[31] MySQL. 'MySQL', 2018. Available: https://dev.mysql.com/doc/refman/5.7/en/what-is-mysql.html [Accessed: 14 Mar 2018]

[32] Wikipedia. 'General Data Protection Regulation', 2017. Available: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation [Accessed: 19 Nov 2017]

[33] Intersoft Consulting. 'Art. 4 GDPR Definitions', 2018. Available: https://gdpr-info.eu/art-4-gdpr/ [Accessed: 19 Mar 2018]

[34] WhiteCase. 'Chapter 5: Key definitions – Unlocking the EU General Data Protection Regulation', 2017. Available: https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation [Accessed: 19 Mar 2018]

[35] Intersoft Consulting. 'Art. 9 GDPR Processing of special categories of personal data', 2018. Available:
https://gdpr-info.eu/art-9-gdpr/
[Accessed: 19 Mar 2018]

[36] Intersoft Consulting. 'Art. 25 GDPR Data protection by design and by default', 2018. Available:
https://gdpr-info.eu/art-25-gdpr/
[Accessed: 19 Mar 2018]

[37] PrivacyTrust. 'Privacy by Design GDPR', 2018. Available:
https://www.privacytrust.com/gdpr/privacy-by-design-gdpr.html
[Accessed: 27 Mar 2018]

[38] Fieldfisher. 'Getting to know the GDPR, Part 1 - You may be processing more personal information than you think', 2017. Available:
http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think/
[Accessed: 2 Apr 2018]

[39] Lexology. 'GDPR and the Internet of Things: 5 Things You Need to Know', 2016. Available:
https://www.lexology.com/library/detail.aspx?g=ba0b0d12-bae3-4e93-b832-85c15620b877
[Accessed: 19 Mar 2018]

[40] ComputerSweden. 'GDPR och internet of things – fem saker du behöver känna till', 2018. Available:
https://computersweden.idg.se/2.2683/1.697169/gdpr-och-iot
[Accessed: 19 Mar 2018]

[41] Whatis.com. 'confidentiality, integrity, and availability (CIA triad)', 2017. Available:
https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[Accessed: 12 Apr 2018]

[42] Föreläsning 1, Martin Hell, Lunds Tekniska Högskola, 2017-01-17
http://www.eit.lth.se/fileadmin/eit/courses/eit060/lect/Lect1.pdf
[Accessed: 1 Feb 2018]

[43] International Organization for Standardization. Basic Reference Model for Open Systems Interconnection (OSI) Part 2: Security Architecture. Geneva, Switzerland, 1989.

[44] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, Handbook of applied cryptography. Boca Raton: CRC Press, 1996.

Alfred J. Mendez, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. ISBN: 9780849385230. CRC Press, 1996.

[45] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), Antalya, 2017, pp. 1-7. doi: 10.1109/ICEngTechnol.2017.8308215

[46] Elaine Barker, National Institute of Standards and Technology, 'Recommendation for Key Management Part 1: General', 2016.
[Accessed: 1 May 2018]

[47] Föreläsning 8b-9a, Martin Hell, Lunds Tekniska Högskola, 2017-01-17
https://www.eit.lth.se/fileadmin/eit/courses/eita25/lect/Lect8b-9a.pdf
[Accessed: 9 Apr 2018]

[48] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM, 26(1), 1983, pp. 96-99.

[49] CVE, 'Vulnerabilities By Type', 2018. Available:
https://www.cvedetails.com/vulnerabilities-by-types.php
[Accessed: 19 May 2018]

[50] W. Stallings, Computer Security: Principles and Practices 5:th edition. New York: Pearson, 2010

[51] Wikipedia, 'Perfect Forward Secrecy', 2018. Available:
https://en.wikipedia.org/wiki/Forward_secrecy
[Accessed: 9 Apr 2018]

[52] S. Ansari, S. G. Rajeev and H. S. Chandrashekar, "Packet sniffing: a brief introduction," in IEEE Potentials, vol. 21, no. 5, pp. 17-19, Dec 2002/Jan 2003. doi: 10.1109/MP.2002.1166620

[53] Computing.co.uk. 'Trustico in the UK revoked due to security incident', 2018. Available:
https://www.computing.co.uk/ctg/news/3027713/23-000-digicert-ssl-certificates-issued-by-trustico-in-the-uk-revoked-due-to-security-incident
[Accessed: 2 Apr 2018]

[54] Sparkfun. 'ESP8266', 2017. Available:
https://www.sparkfun.com/products/13678
[Accessed: 12 Dec 2017]

[55] Espressif Smart Connectivity Platform. 12 Oct 2013. 'Espressif Smart Connectivity Platform: ESP8266'. Available:
https://cdn-shop.adafruit.com/datasheets/ESP8266_Specifications_English.pdf
[Accessed: 12 Dec 2017]

[56] SIMCom. 'SIM808', 2018. Available:
http://simcom.ee/modules/gsm-gprs-gnss/sim808/
[Accessed: 02 Apr 2018]

[57] Sparkfun. 'AT Commands Reference Guide', 2018. Available:
https://www.sparkfun.com/datasheets/Cellular%20Modules/AT_Commands_Reference_Guide_r0.pdf
[Accessed: 29 Mar 2018]

[58] Sparkfun. 'LSM9DS1', 2018. Available:
https://cdn.sparkfun.com/assets/learn_tutorials/3/7/3/LSM9DS1_Datasheet.pdf
[Accessed: 16 Mar 2018]

[59] Infineon. 'Hall-effect sensor', 2018. Available:
https://www.infineon.com/dgdl/Infineon-Infineon-TLV4964-5TAB_Hall_Switch-DS-v01_00-DS-v01_00-EN.pdf?fileId=5546d4624e765da5014ede55cc6a0bf6
[Accessed: 13 Mar 2018]

[60] Interlink Electronics. 'Force Sensing Resistor', 2018. Available:
https://www.interlinkelectronics.com/fsr-400
[Accessed: 29 Mar 2018]

[61] MeltdownAttack. 'Meltdown', 2018. Available:
https://meltdownattack.com/meltdown.pdf
[Accessed: 11 Apr 2018]

[62] NPN-Transistor. 'NPN', 2018. Available:
https://www.electronics-tutorials.ws/transistor/tran_2.html
[Accessed: 22 Mar 2018]

Appendix A

The specifications for the TENS modes

Program / Therapy part	P1			P2			U1 (Default)			Treatment time (min)
	Pulse rate (Hz)	Pulse width (μs)	Waveform	Pulse rate (Hz)	Pulse width (μs)	Waveform	Pulse rate (Hz)	Pulse width (μs)	Waveform	
SHOULDER	2~80	100~200	Simple modulated pulse	50	200	Synchronous	2~125	100~200	Simple modulated pulse	30
NECK	2	180	Continuous	80	70~180	Pulse width modulated	80	180	Continuous	
BACK	80/2	180	Hans	80	70/180	Hans	100	330/200	Amplitude modulated	
ELBOW	2	180	Continuous	80	70~180	Pulse width modulated	2~125	100~200	Simple modulated pulse	
HIP	100	330/200	Amplitude modulated	125	330/200	Amplitude modulated	80	330/200	Amplitude modulated	
ANKLE	2~60	100~200	Simple modulated pulse	2~8	300	Pulse rate modulated	2~40	100~200	Simple modulated pulse	
FOOT	80	70~180	Pulse width modulated	80	70/180	Hans	2~100	100~200	Simple modulated pulse	
WRIST	50	200	Synchronous	65	200	Synchronous	2~80	100~200	Simple modulated pulse	
KNEE	50	350	Asynchron-ous	2	180	Continuous	80	200	Alternate Ramped Burst	

Appendix B

The different signal modulations from the TENS machine

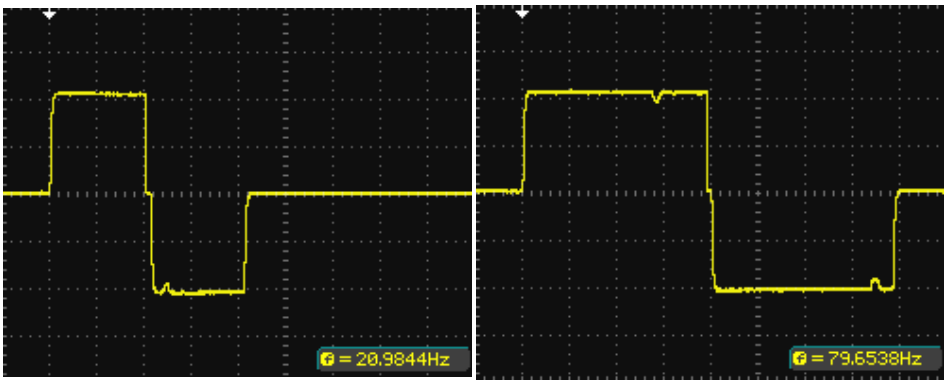


Figure B.1: The simple modulated waveform.

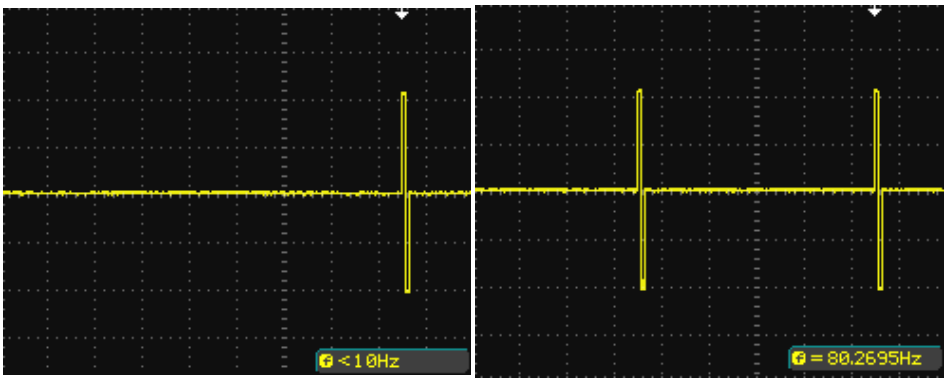


Figure B.2: The Hans waveform.

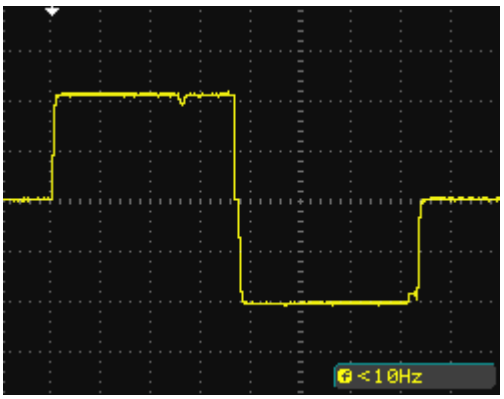


Figure B.3: The continuous waveform.

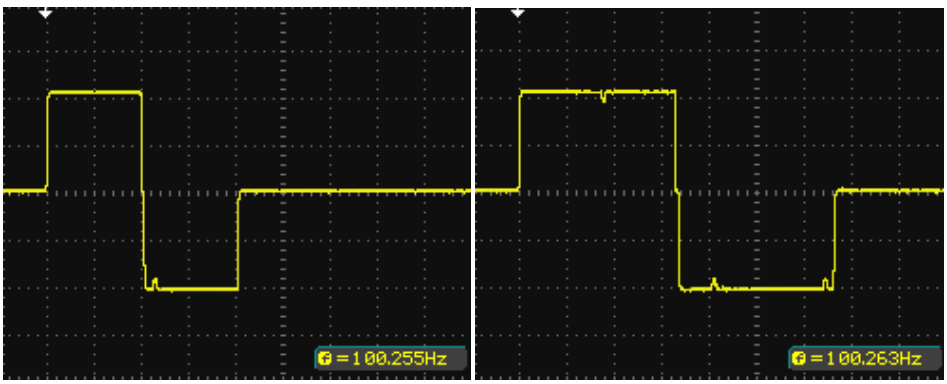


Figure B.4: The amplitude modulated waveform.

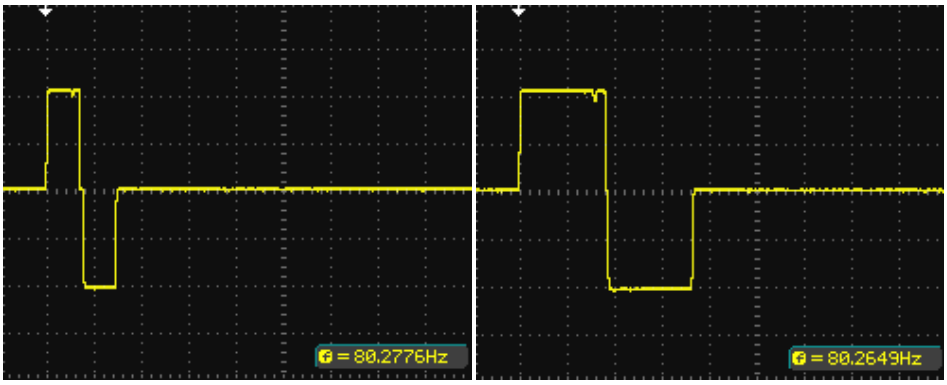
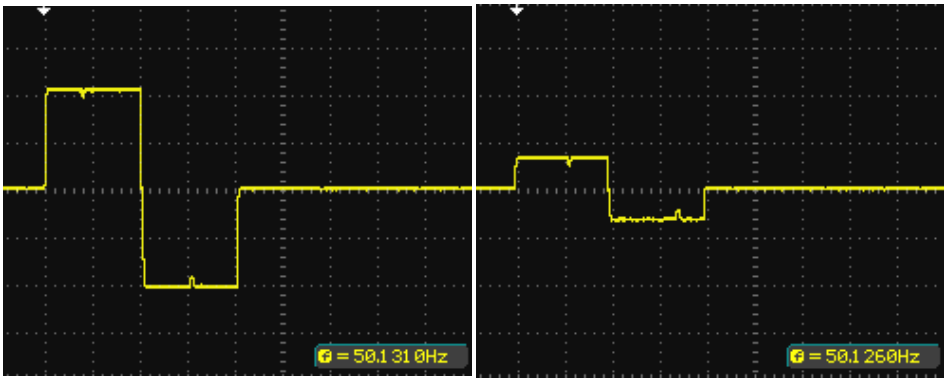


Figure B.5: The pulse width modulated waveform.



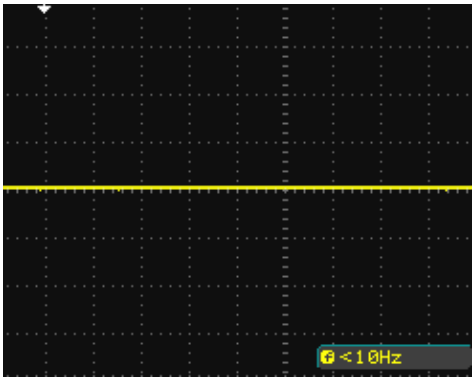


Figure B.6: The synchronous waveform.

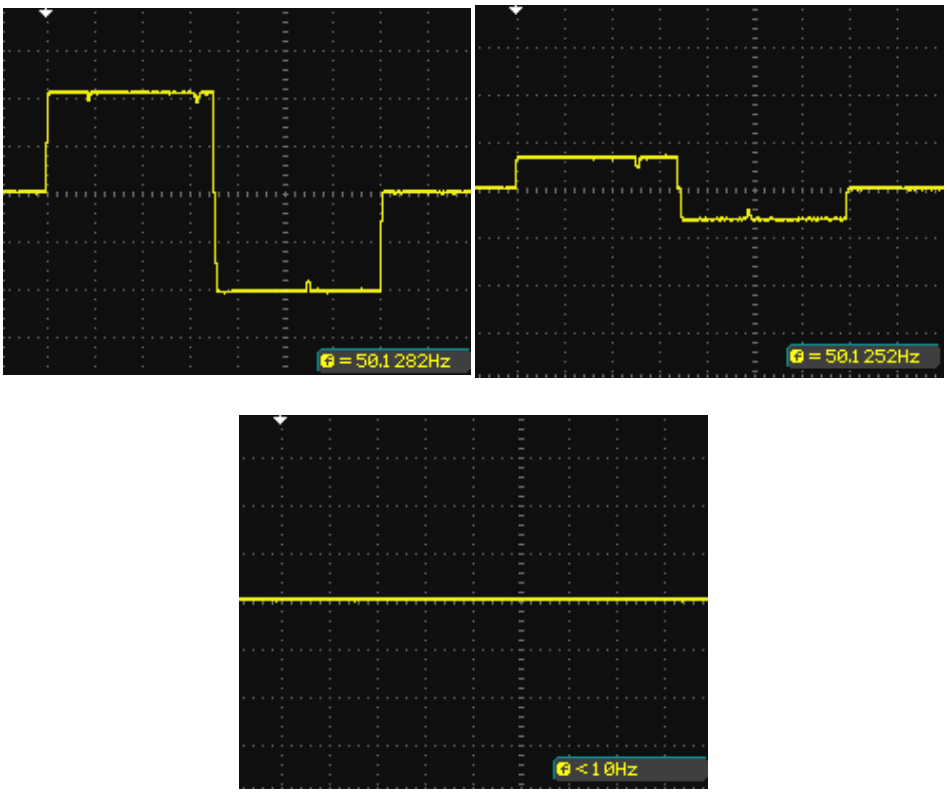


Figure B.7: The asynchronous and alternate ramped burst waveforms.

The Alternate Ramped Burst is the same as asynchronous only with faster rise and fall times.