UNIVERSITY OF MORATUWA, SRI LANKA

Faculty of Engineering

Department of Electronic and Telecommunication Engineering

Semester 4 (Intake 2020)

EN2160 - Electronic Design Realization

Portable GSM Signal Jammer

A. A. H. Pramuditha – 200476P

This report is submitted as a partial fulfillment for the module EN2160 - Electronic Design Realization, Department of Electronic and Telecommunication Engineering, University of Moratuwa.

ABSTRACT

As a result of technological advancements in the mobile phone industry, mobile phones have emerged as a crucial communication device, encompassing various end-user applications. These applications include but are not limited to games, online videos, e-commerce, and social media platforms such as Facebook, WhatsApp, and Twitter. Consequently, the ubiquitous use of mobile phones has led to disruptive situations in various contexts, such as during prayer, studying, meetings, courtrooms, driving and examination rooms.

The primary objective of this project was to design and construct a system capable of blocking the usage of mobile phones by transmitting radio waves on the same frequencies as those used by the mobile phone itself. This interference would disrupt the connection between the mobile phone and Base transceiver Station (BTS), resulting in the display of "No Network on the mobile phone screen". The system was intended for installation in locations where mobile phone usage is prohibited. While different cellular systems employ distinct signal processing methods, all cell-phone networks utilize radio signals that can be interrupted or interfered with. GSM technology, employed in digital cellular and PCS-based (Personal Communication Service) systems, operates within the frequency bands of 900 MHz, 1800 MHz, and 2100 MHz (WCDMA) in Europe and Asia, and 1900 MHz in the United States. These networks, including WCDMA, GSM, and DCS, can be effectively targeted by jammers capable of broadcasting on any mobile network frequency.

This project encompasses a comprehensive discussion on the design and development of a GSM Signal jammer, which offers a potential solution to the aforementioned issues. Extensive research was conducted to derive appropriate designs for the system, followed by the construction and integration of various system components into a cohesive unit. Finally, the system underwent functionality testing, yielding results that demonstrated its efficacy in jamming mobile phone signals by transmitting signals on the same frequency as those emanating from the Base Transceiver Station.

BACKGROUND

As of today, due to the advanced improvements in technology, mobile phones have become a vital and necessary device with several end user applications embedded. For instance, mobile games, e-business and e-commerce, social media platforms etc.

But this has resulted in creating disruptive conditions on some occasions and some places, namely studying, praying, driving, in courtroom, in meeting room, in examination rooms etc. For such occasions and places, it is necessary to take precautions to mitigate this disruptiveness created by mobile phones.

However, in most countries these kinds of activities without proper supervision are prohibited (apart from some special situations). Since this project doesn't meet the national regulations and requirements, it should be stated that this project is solely done for educational purposes in the University of Moratuwa. There is no intention to manufacture and distribute such device among public in Sri Lanka. Yet, this device can be employed in a few specific occasions when properly supervised by the appropriate authorities.

MAIN OBJECTIVE

The main objective of this project is to come up with a system which has the capability to transmit radio waves causing interference between the mobile phone and the base transceiver station (Simply, make the mobile phone switch to “NO NETWORK” condition).

There are several ways to jam an RF device. The three most common techniques can be specified as follows.

1. **Spoofing:**

   Under this technique, the mobile phone will be forced to turn off itself. Implementation of this technique is very difficult since first, it must detect the presence of a mobile phone and then send a signal to disable that specific phone. Sometimes, it will detect a nearby mobile phone and sends a message to tell the user to switch off his/her phone. This technique is called Intelligent Beacon Disablers.

2. **Shielding Attacks**

   This technique is also known as EMF shielding, and it requires closing a particular area in a faraday cage so that the RF devices in this cage cannot receive any signal from outside of the cage.

3. **Denial of Service (DOS)**

   We are using this technique on our device. In this technique, the device transmits a noise signal that has the same frequency as the mobile phone signal to reduce the SNR (signal-to-noise ratio) value.

Since the down-link frequencies utilize less power than the up-link frequencies, in this project, only the down-link frequencies were considered using the Global System for Mobile Communications (GSM) frequency band of 900 MHz (800-1000 MHz).

GSM is the abbreviation for Global System for Mobile Communications. It accounts for about 70% of the global mobile market which uses time division multiple access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA).

METHODOLOGY AND FEATURES

A mobile signal jammer will transmit an RF signal at the same frequency as the mobile phone signal, with enough power so that two signals will collide and cancel each other out or reduce the power of the mobile signal. To do that, all we need is a device that broadcasts on the correct frequencies.

Basically, GSM (Global System for Mobile Communication) operates in the 900 MHz and 1800 MHz bands in Europe, Asia, and Africa.

So, our jamming device transmits on the same radio frequency, which is 900 MHz, thereby disrupting the communication between the cell phone and the base transceiver station in the town (denial of service).

When designing this system, there are some key areas to which much attention should be paid.

- There are three main sections that should be included on this system. They are the power supply unit, the IF (intermediate frequency) section, and the RF (radio frequency) section. Apart from that a method of transmission is needed.

- Since this device is designed to be portable, the power source should not be a complex mechanism or a fixed one. To make the device more portable, 9V batteries or rechargeable batteries are included to the system, as they can be replaced and very convenient to use (no need to use the domestic AC power supply).

- The intermediate frequency section will generate the tuning frequency signal that will be fed to the RF section.

- The RF section will generate the RF signal with the help of the above tuning frequency signal, which would interfere with the signal from the base station to the mobile phone.

- Basically, this device will generate signals in the 900 MHz radio frequency band. But it can be integrated to increase or decrease the frequency band it's working on. So, a mechanism is included to change the jamming frequency band it's operating on (an extra feature). This will be implemented both in the RF section.

- Since this device is a portable device, it's not our intention to implement a separate power generation and regulation unit powered by a domestic AC power supply.

SYSTEM DESIGN AND SIMULATION

When designing the system and enclosure for the product, several brainstorm sessions were conducted among our peer groups (Conceptual Design Stage) and several methodologies and enclosure designs were suggested for the final product. After reviewing the pros and cons of these designs, a single design was selected for the final product.

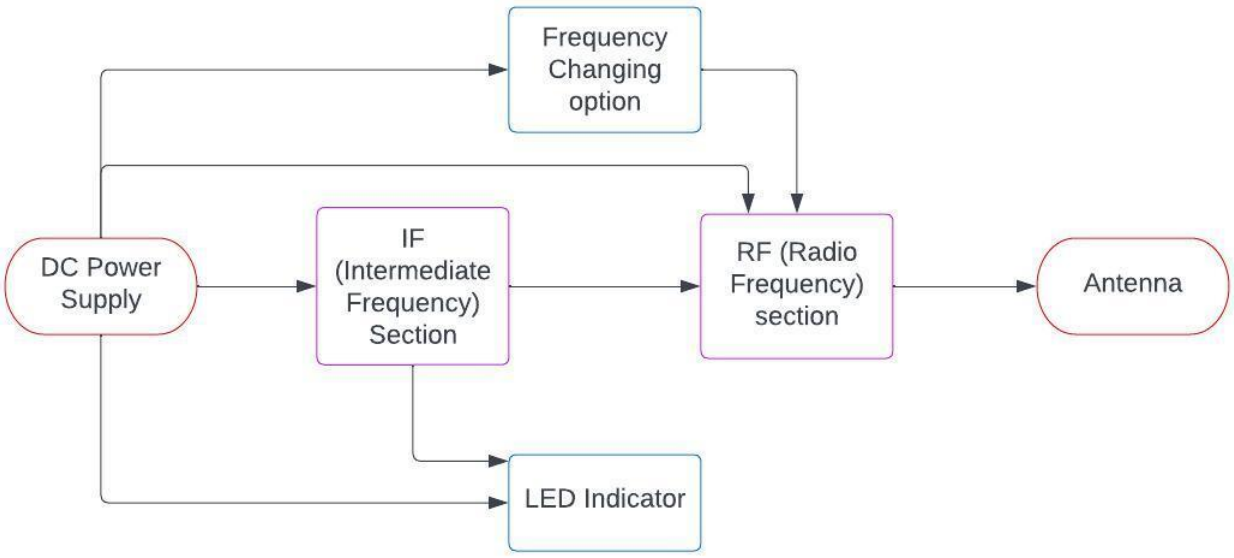
In conceptual design stage, it is the main goal to develop concepts and make prototypes for a particular product by considering different circuits, different enclosures, different functional parts, combining different ideas to make a complete solution.

After that those underlying ideas are grouped and presented using free hand sketches to get an optimal solution.

Design-driven innovation, which is also known as radical product innovation is another design methodology that can be used to add creativity to the product.

With design-driven innovation, the manufacturer's creative vision for the product will be presented to the consumers rather than addressing existing user demands for the product. These newer concepts will be presented by an interpreter for the consumer society.

When it comes to the process of the system, several system block diagrams were designed based on the basic functionality of the product by the group members to decide an optimal functional design for the product. Among those block diagrams, one block diagram was selected to implement for the product.



Proposed Block Diagram for the Product

When it comes to the system design, as stated earlier, this device consists of three main sections namely,

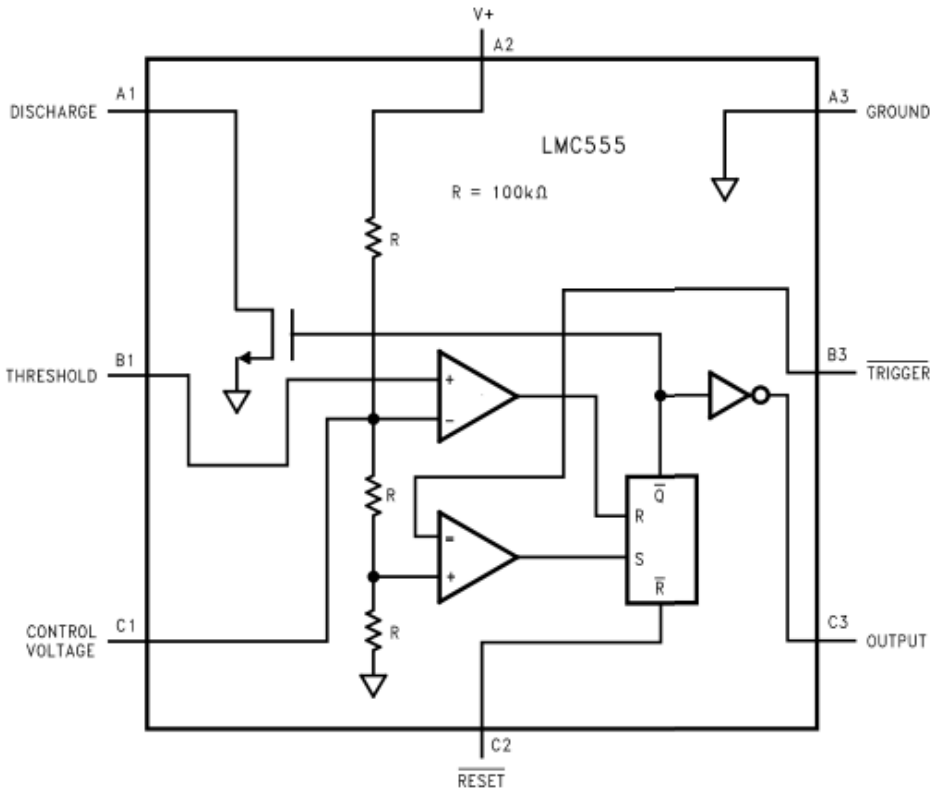
1. The power supply unit
2. The IF (Intermediate Frequency) section
3. The RF (Radio Frequency) section

THE POWER SUPPLY UNIT

In this section, the main goal is to use a simple, convenient power supply solution to make the product more portable. Also, when considering an option for the power supply, it is necessary to ensure whether the power requirements of the system components are fulfilled by this unit. Considering all these requirements, a 9V DC voltage source was included as the main power source. Since the main signal generating source of the system (timer IC) is able to produce a reasonable output under a supply voltage range of 4.5V to 15V, it is enough to use a 9V DC voltage source (9V battery) for the system.

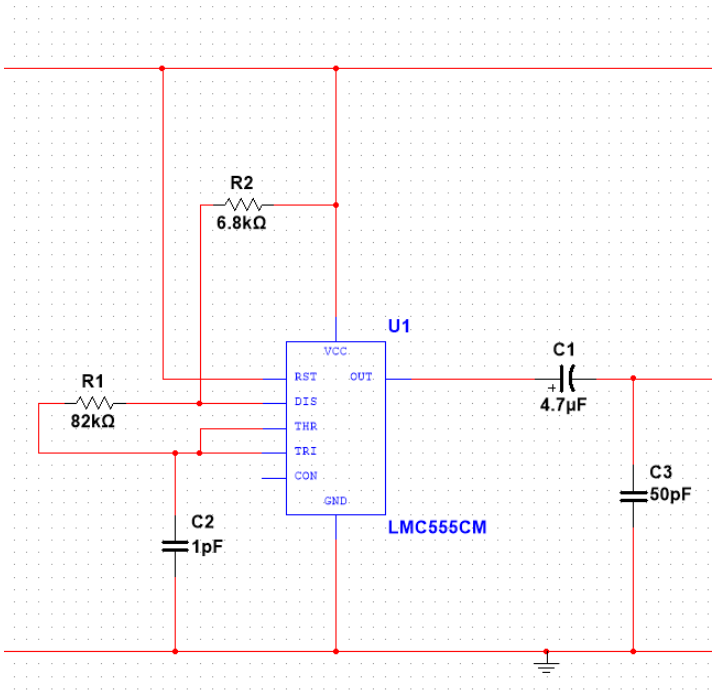
THE IF (INTERMEDIATE FREQUENCY) SECTION

The main functionality of this section is to produce a tuning signal which will then be mixed with the desired frequency. To generate the tuning signal with a sufficient frequency value, LMC555 CMOS timer IC was used in the system.



Internal Structure of the LMC555 CMOS Timer IC

To generate the required oscillating signal, the above-mentioned timer was configured into astable mode of operation by implementing standard astable timer IC configuration and the values of the components (resistors, capacitors) were calculated and selected to obtain a frequency value around 8 MHz.



IF Section of the System

To obtain the above-mentioned frequency, calculations were done to decide the values for R1, R2 resistors and C2 capacitor according to the equations listed below.

$$t1 = 0.693(R1 + R2) * C2$$

$$t2 = 0.693(R1) * C2$$

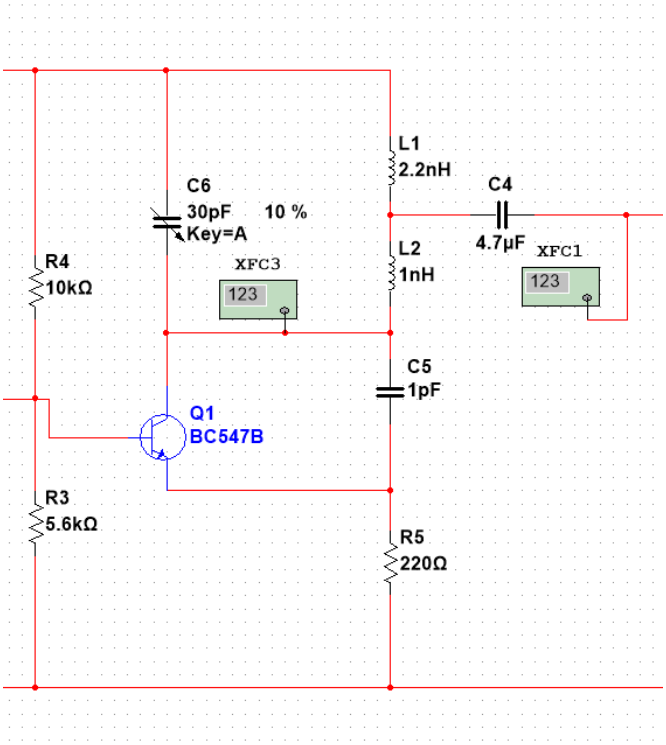
$$T_{total} = t1 + t2$$

$$F(frequency) = \frac{1}{T}$$

Decreasing the values of R1 and R2 will give us a short period of time and small percentage of duty cycle and higher frequency than the output values I was expecting, and similar effect can be seen when increasing the values of R1 and R2.

THE RF (RADIO FREQUENCY) SECTION

The output astable clock pulse of IF section will be given to the RF section which consists of BF495 transistor, 30pF trimmer capacitor, inductors, biasing resistors and capacitors, and an antenna.



RF Section of the System

The oscillator circuit, consisting of C6 trimmer capacitor, L1 and L2 inductors, will generate the resonance frequency which suits the desired frequency band (GSM band). The output of the IF section will be fed to the base of the Q1 transistor (BC547B), which amplifies the signal for the given common emitter configuration. The values of R3 and R4 were calculated to get the required amplification.

After going through the resonator circuit, the final signal will be given to the antenna for the transmission. Initially, 23 SWG copper wire was used to build this antenna by winding it nearly 15-20 turns. But lately, to achieve a precise transmission, GSM right angled antenna was used with an SMA connector cable.

The following formula was used to obtain the coil length and the number of turns for the inductors to achieve desired inductances.

$$L = \frac{d^2 + n^2}{18d + 40l}$$

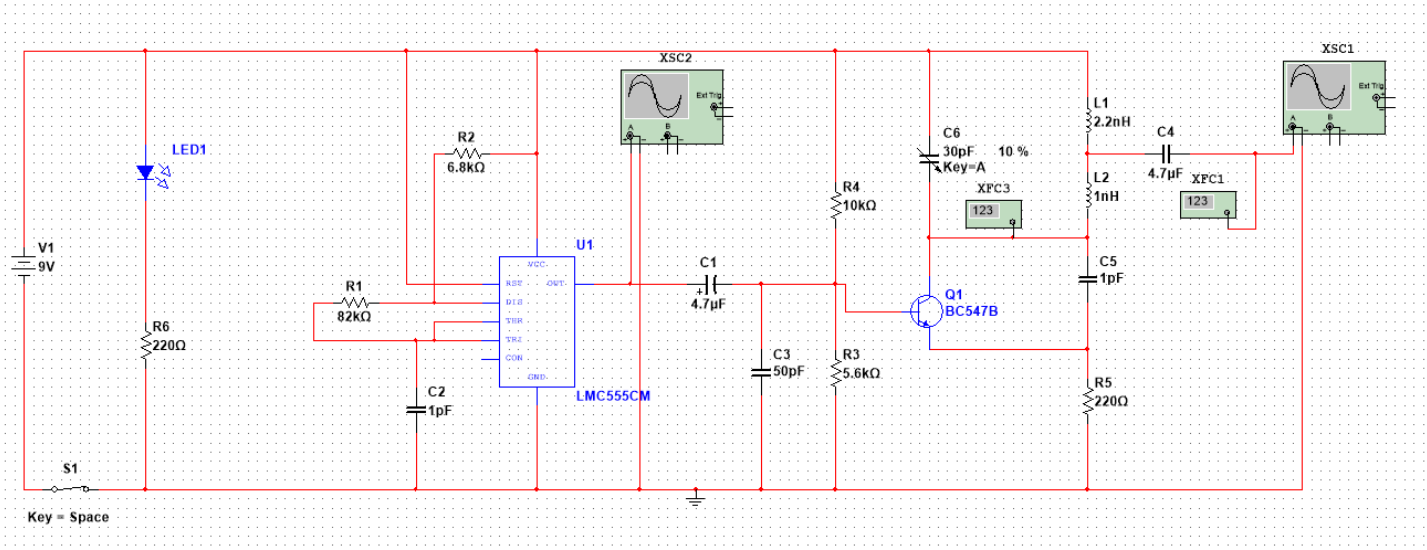
L = inductance in micro henrys

D = Coil diameter in inches

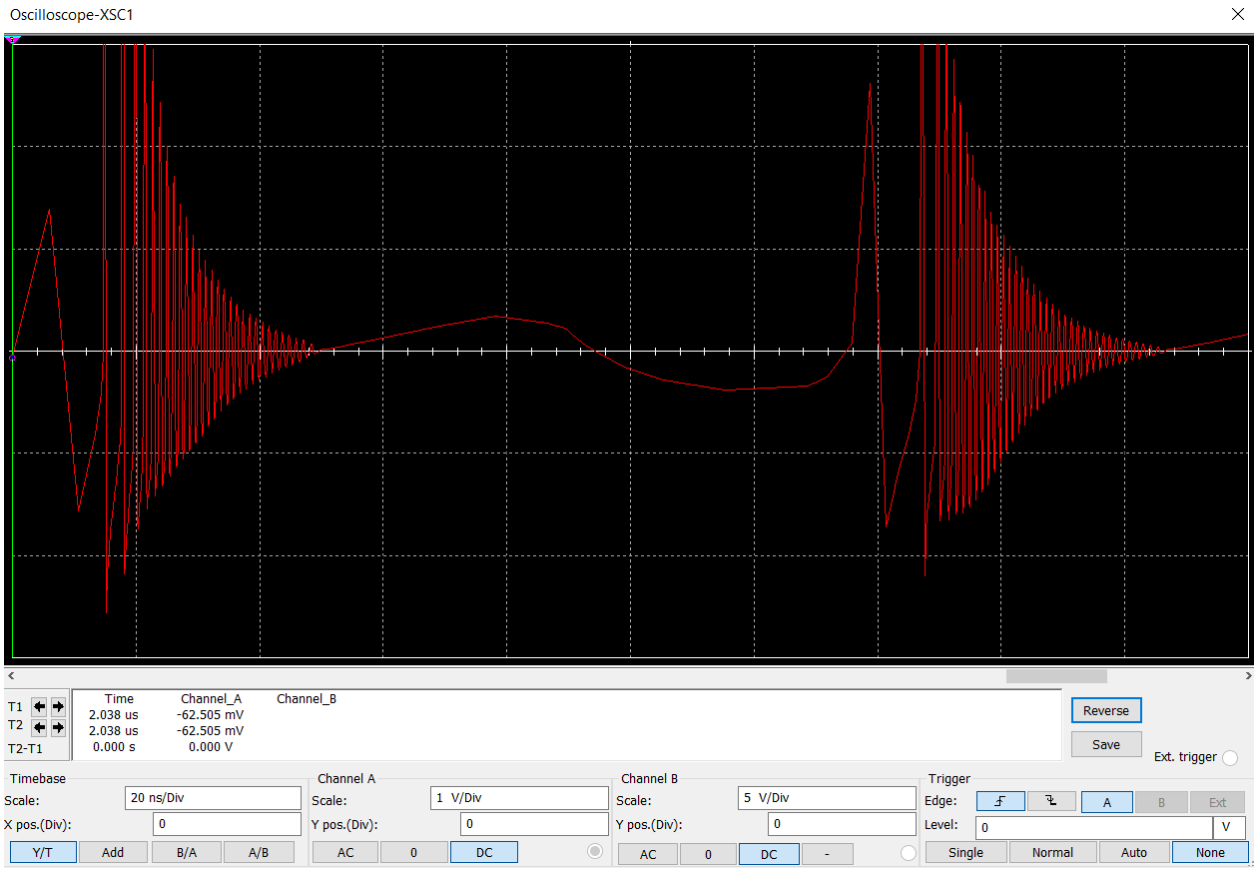
L = coil length in inches

N = number of turns

Based on the above design methodology of the system, simulation design was built using Multisim software tool to verify the operation of the system.



The signals generated in IF and RF stages were observed by using virtual oscilloscopes and the frequencies of the signals were measured by placing several frequency counters. The waveform of the final transmitting signal was obtained as follows.

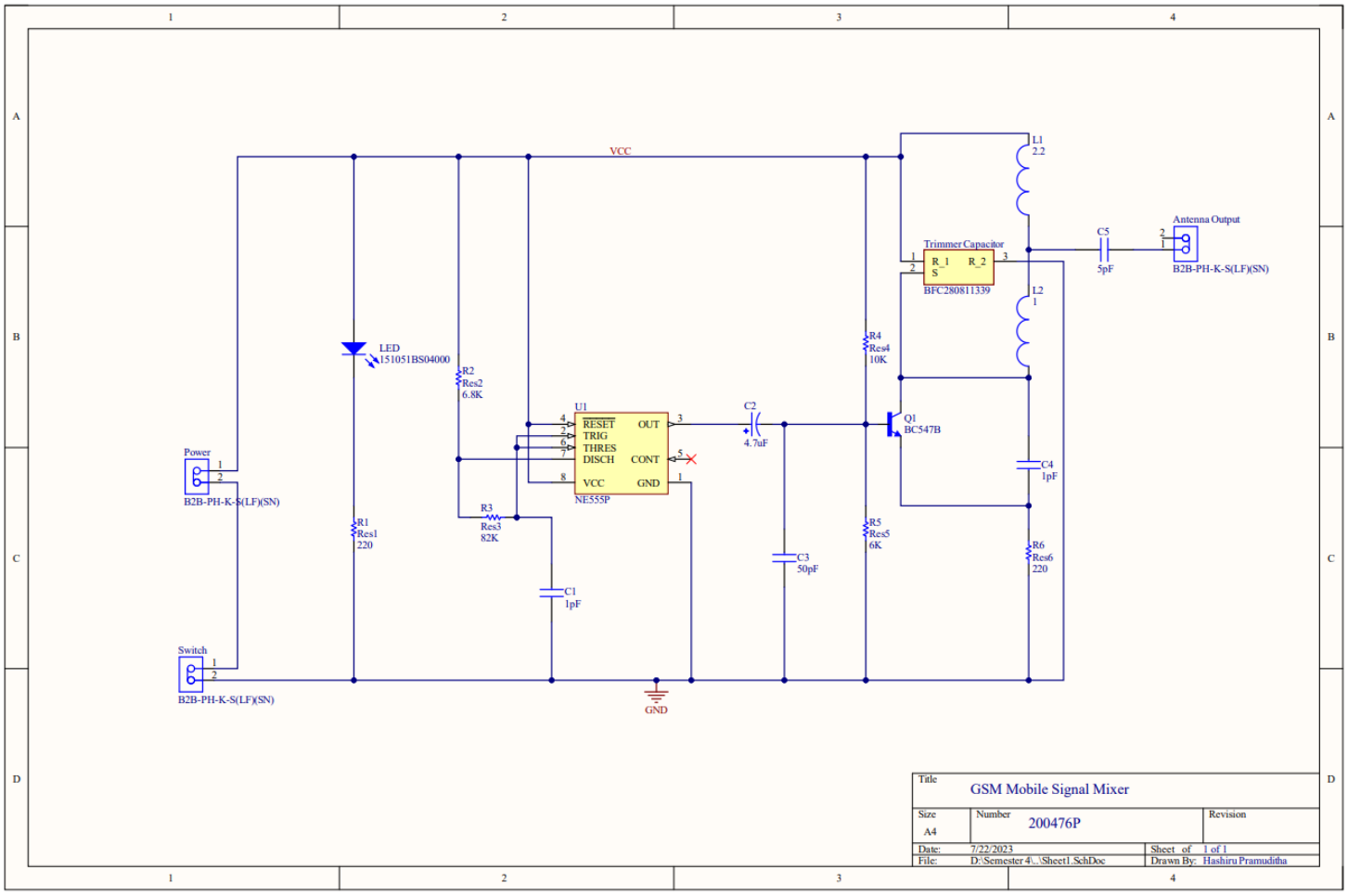


SCHEMATIC & PCB DESIGN

After the completion of the system design and simulation stage, schematic and PCB design were made to the circuit system using Altium Designer tool.

SCHEMATIC DESIGN

The schematic was designed in two stages by improving and changing some features of the first stage. The final schematic is shown below.

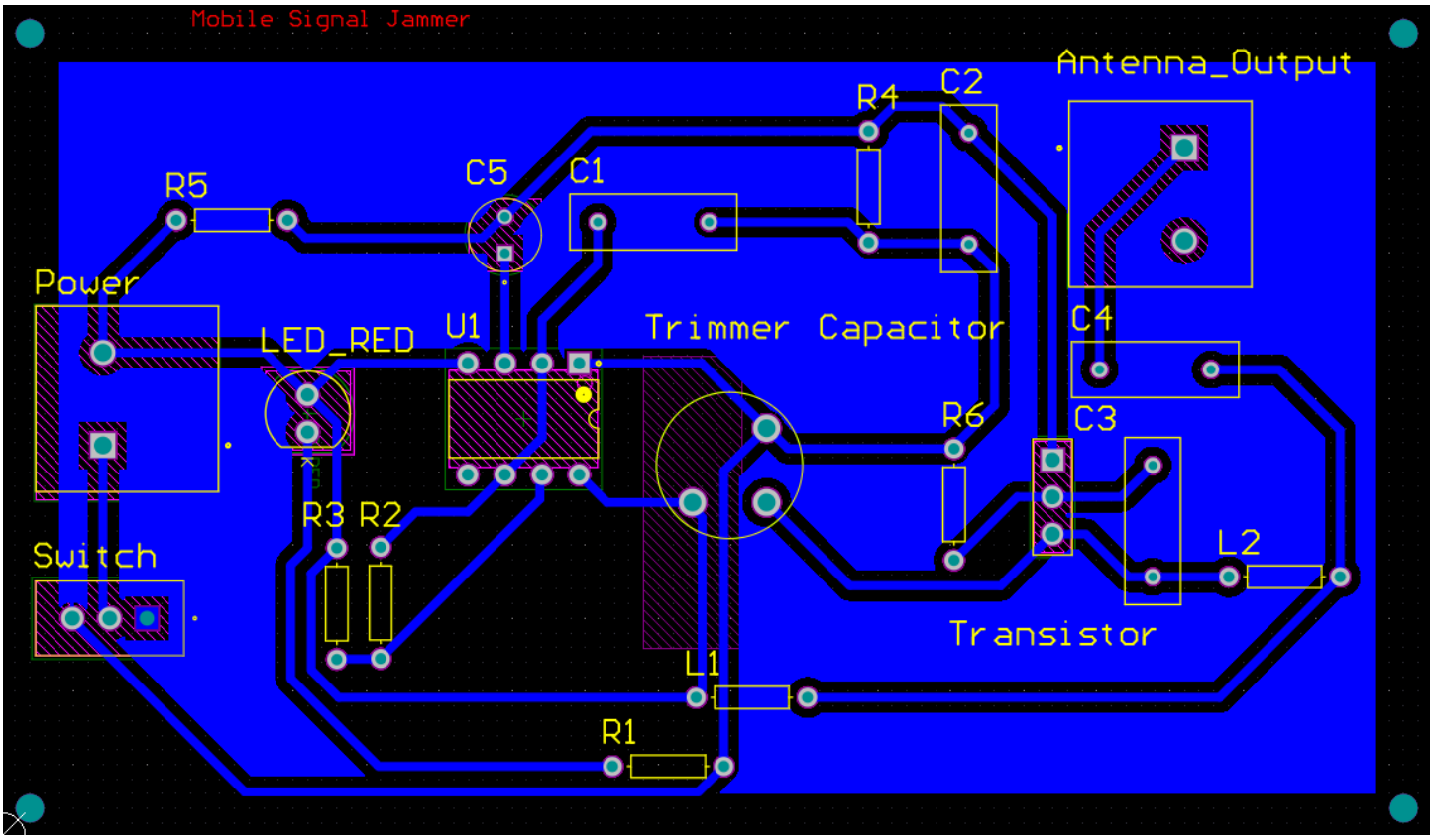


GSM Signal Jammer – Schematic Design

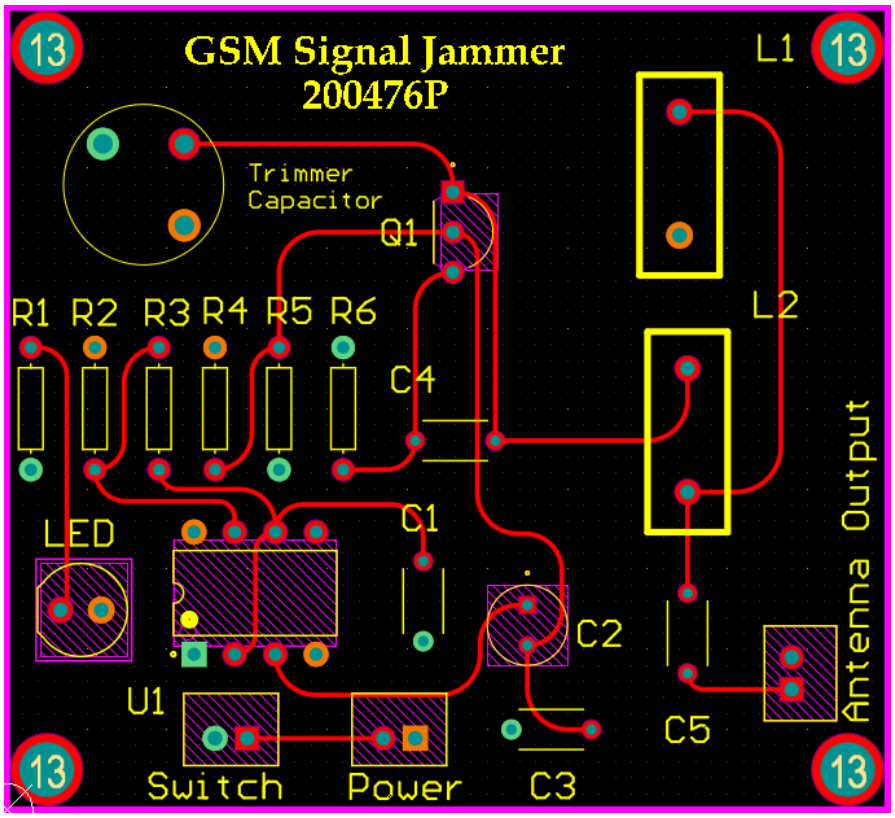
Symbols and footprints for most of the components were obtained from the standard Altium Vault. For some components (inductors), custom symbols and footprints were designed and integrated to the project as a single PCB and Schematic library.

PCB DESIGN

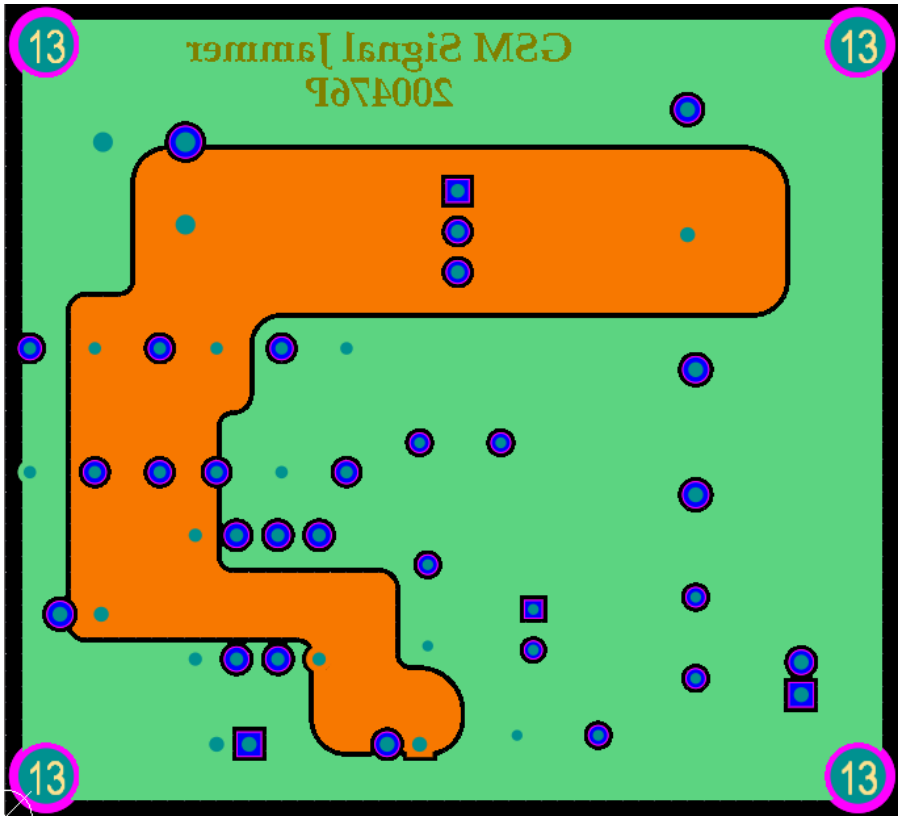
After validating the components placement and the routing of the schematic, footprints were generated to design the PCB. PCB designing was also done in two stages. In the second stage, some design rules and ethics of RF circuit design and routing were followed, and the PCB was designed based on the standard design rules of JLC PCB Design Rules since they are the ones who were chosen to manufacture the PCB board.



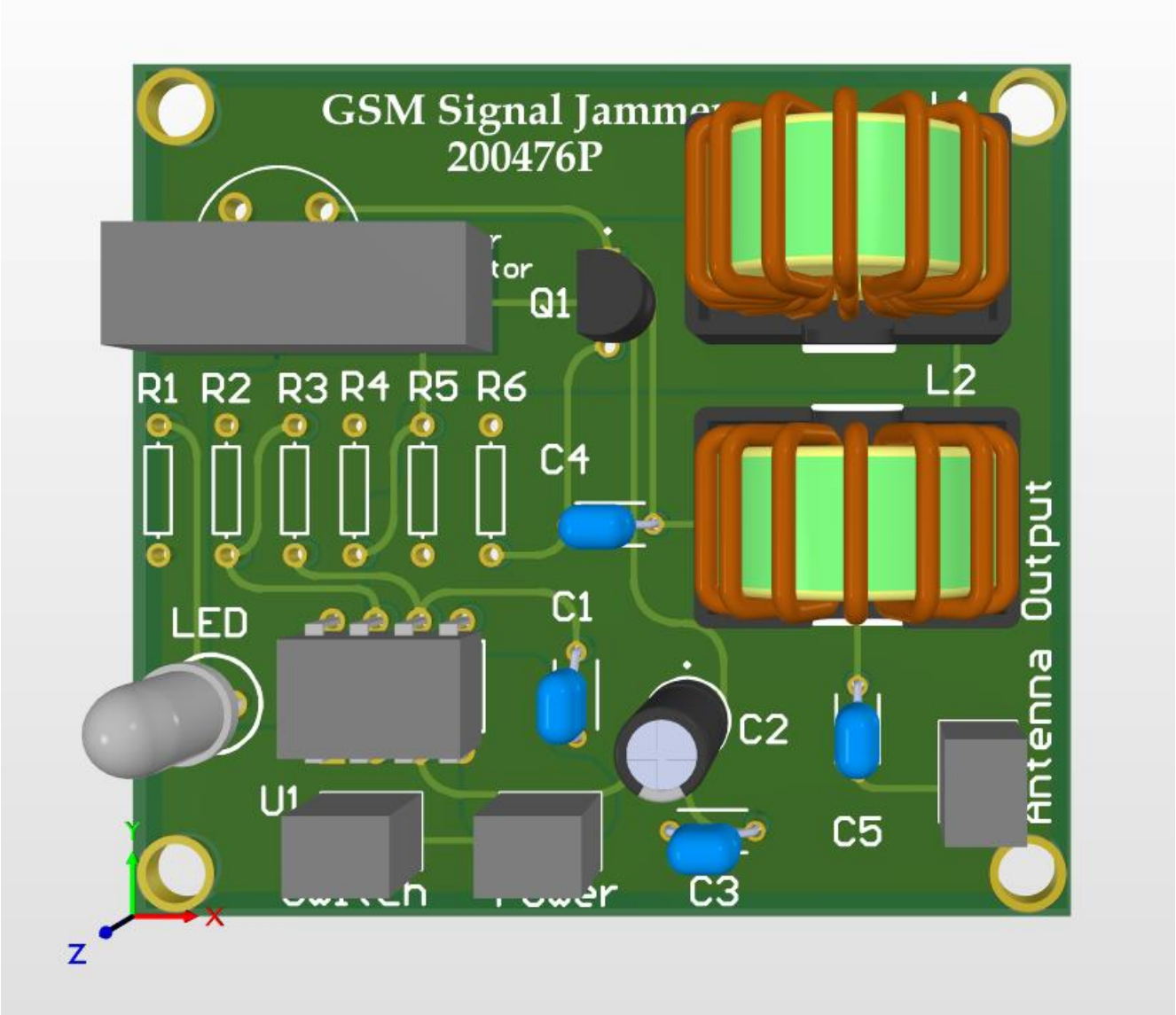
1st Stage: Single Layer PCB design



2nd Stage: Double Layer PCB Design – Top layer



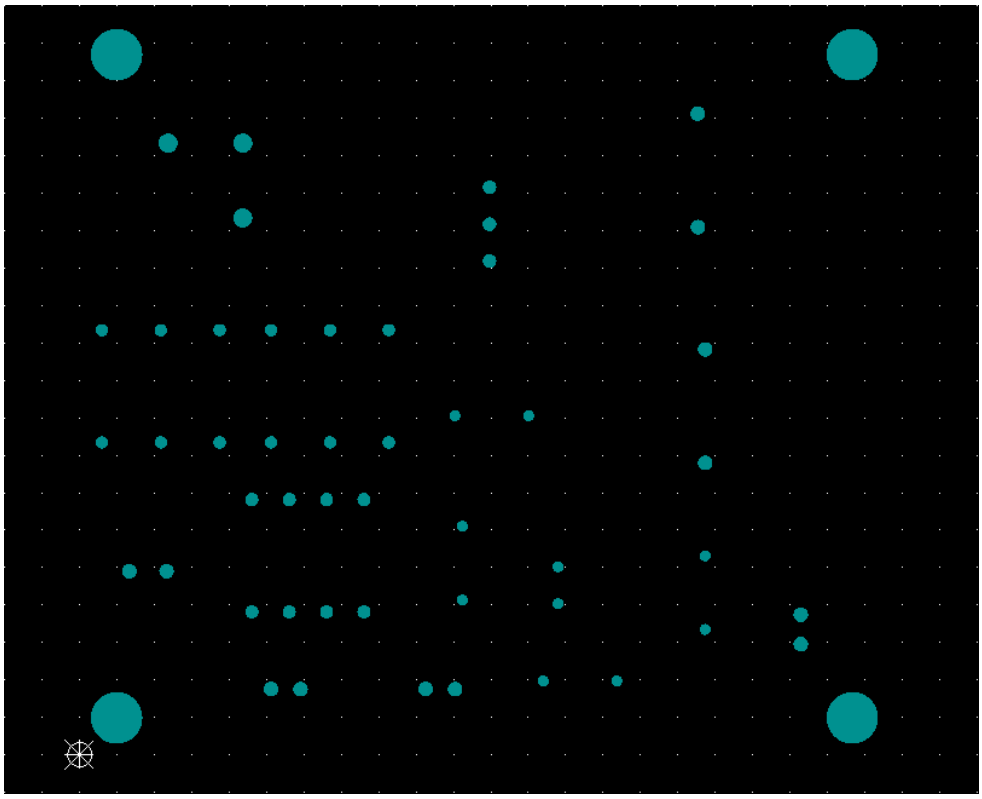
2nd Stage: Double Layer PCB Design – Bottom layer

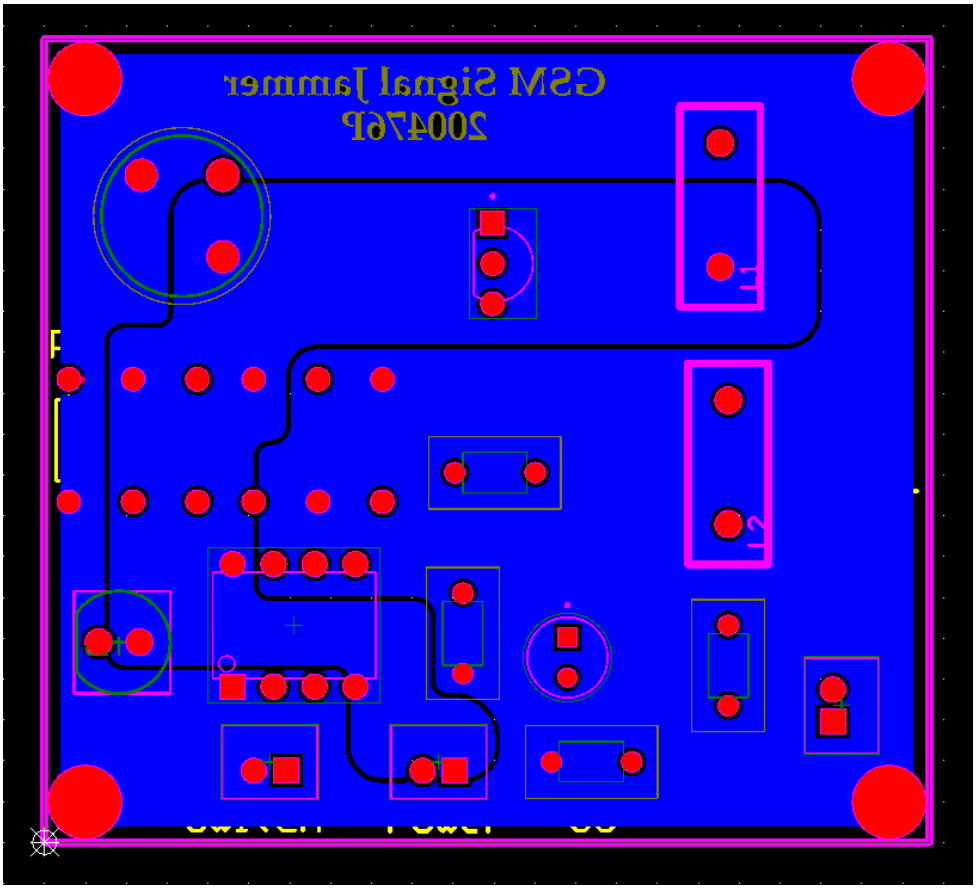


2nd Stage: Double Layer PCB Design – 3D View

Since there are high frequency signals (above 1 MHz) flowing through the PCB, traces were made without applying sudden turns (using curved turns on paths) and power and ground traces were separated from the signal paths (By applying two polygon pours for VCC and GND using whole bottom layer, only the signal traces are on the top layer).

After routing the whole PCB, design rule check was implemented to check any erroneous points in the design. Then Gerber files and NC drill files were generated to send for the manufacturer to manufacture the PCB.





Gerber Files and NC Drill Files

BOM – BILL OF MATERIALS

All the components included in the schematic can be listed as follows.

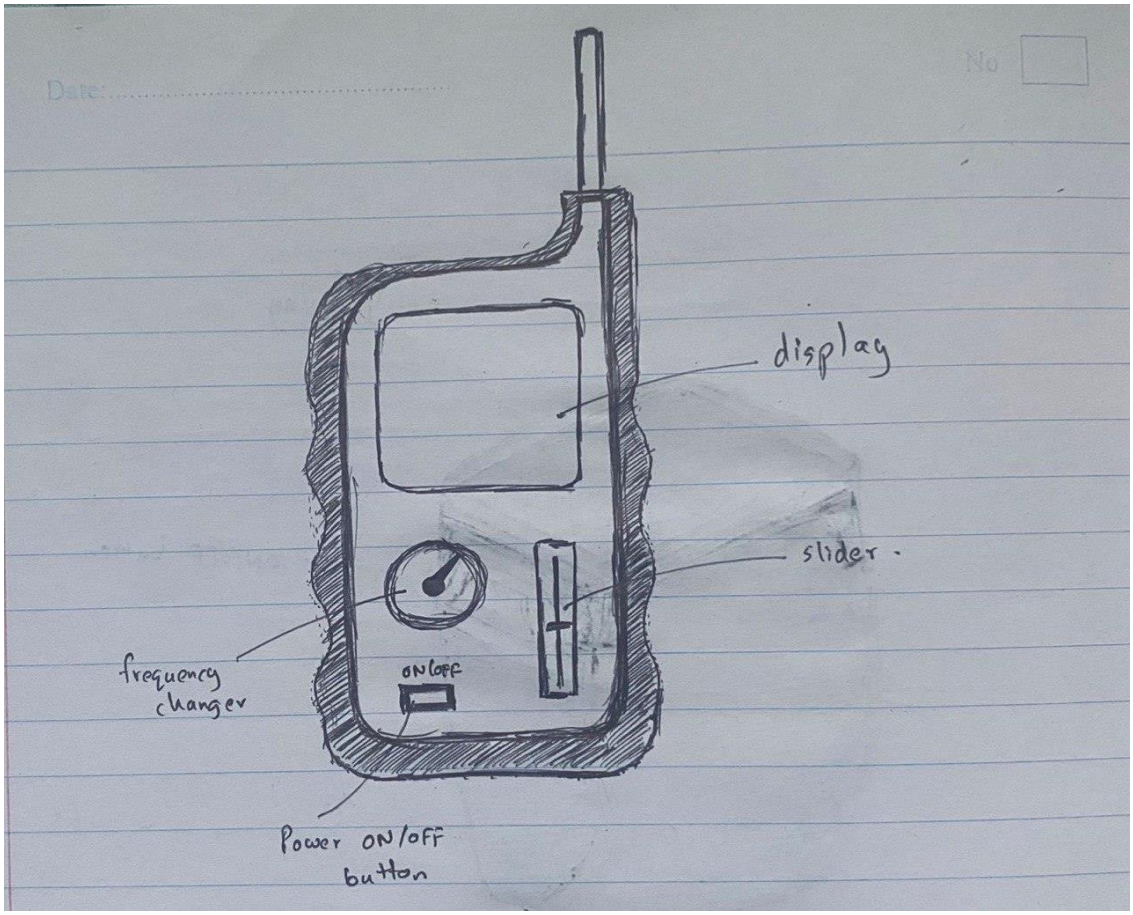
Comment	Description	Designator	Footprint	LibRef	Quantity
B2B-PH-K-S(LF)(SN)	Male Header, Pitch 2 mm, 1 x 2 Position, Height 6 mm, Tail Length 3.4 mm, -25 to 85 degC, RoHS, Bulk	Antenna Output, Power, Switch	JST-B2B-PH-K-S_V	CMP-2000-05162-1	3
1pF	Capacitor L=4.0mm W=3.5mm T=2.5mm	C1, C4	RDE5C1H330J0M1H03A	RDE5C1H1R0C0M1H03A	2
4.7uF	10ÂµF 63V Aluminum Electrolytic Capacitors Radial, Can 5000 Hrs @ 105Â°C	C2	CAPPRD250W50D500H1100	EEUEB1J100SH	1
50pF	Capacitor L=4.0mm W=3.5mm T=2.5mm	C3	RDE5C1H330J0M1H03A	RDE5C1H1R0C0M1H03A	1
5pF	Capacitor L=4.0mm W=3.5mm T=2.5mm	C5	RDE5C1H330J0M1H03A	RDE5C1H5R0C0K1H03B	1
2.2		L1	Inductor Coil TH	Inductor	1
1		L2	Inductor Coil TH	Inductor	1
151051BS04000	THT LED round mono-color color lens, WL-TMRW, Blue	LED	Type 5mm	CMP-1488-00009-1	1
BC547B	Bipolar (BJT) TransistÃ¶r NPN 45 V 100 mA 300MHz 625 mW Delikten TO-92 (TO-226)	Q1	TO92250P510H770-3	BC547B	1
Res1	Resistor	R1	AXIAL-0.3	Res1	1
Res2	Resistor	R2	AXIAL-0.3	Res1	1
Res3	Resistor	R3	AXIAL-0.3	Res1	1
Res4	Resistor	R4	AXIAL-0.3	Res1	1
Res5	Resistor	R5	AXIAL-0.3	Res1	1
Res6	Resistor	R6	AXIAL-0.3	Res1	1
BFC280811339	CAP TRIMMER 3-33PF 250V TH	Trimmer Capacitor	BFC280811339	BFC280811339	1
NE555P	Precision Timer, 4.5 to 16 V, 0 to 70 degC, 8-Pin DIP, Pb-Free, Tube	U1	P0008A	CMP-2000-04954-1	1

ENCLOSURE DESIGN & MANUFACTURING

When selecting a proper enclosure for the selected product, several discussions were made among peer groups and several designs were designed and suggested in this process. So, the enclosure is also designed in two stages.

In the first stage, simple enclosure design was made without considering any user requirements or following proper designing cycles. In the second stage, some methods and principles associated with the product design domain were followed.

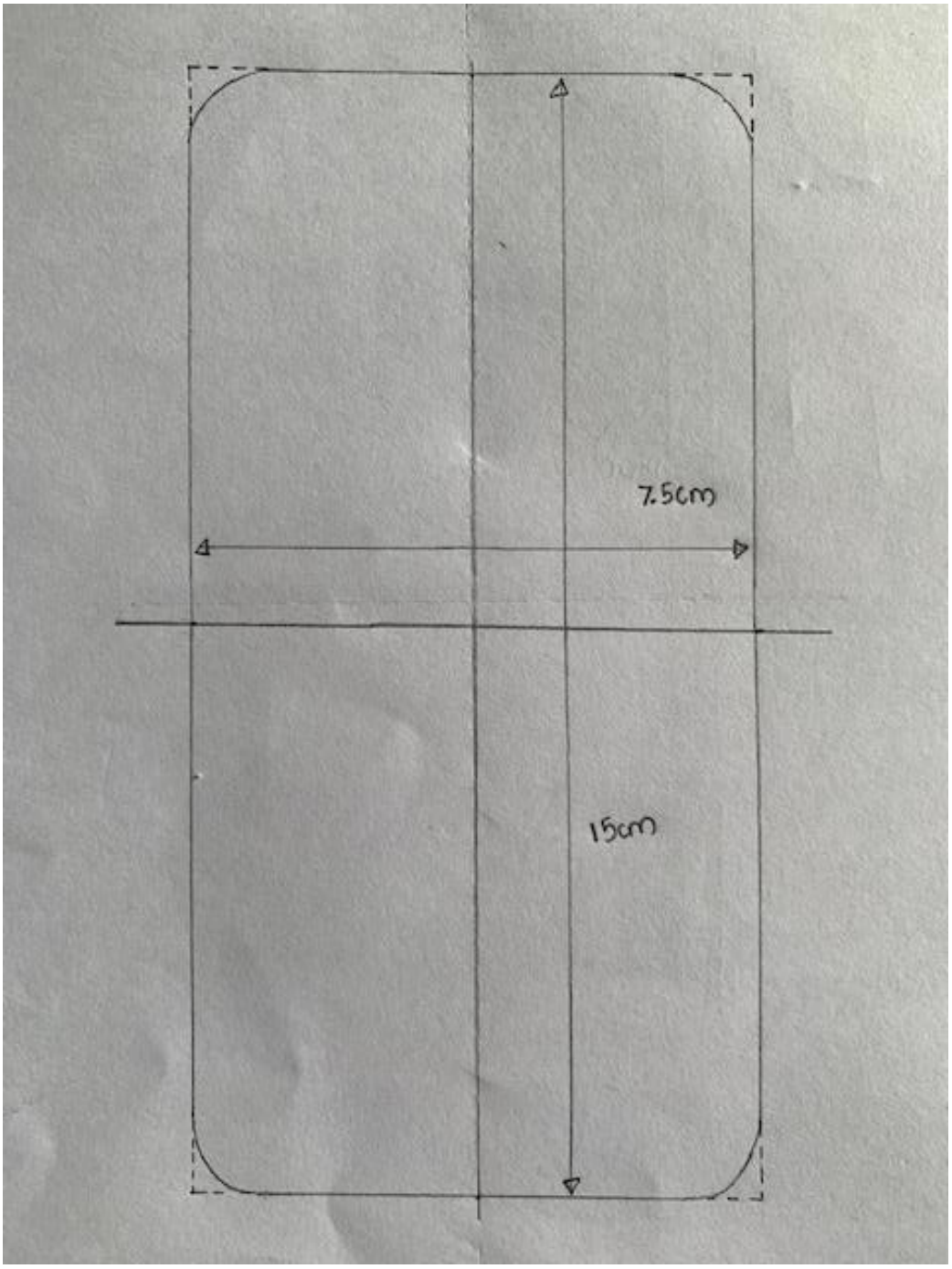
At the end of the conceptual design stage, a one hand sketch design was selected.



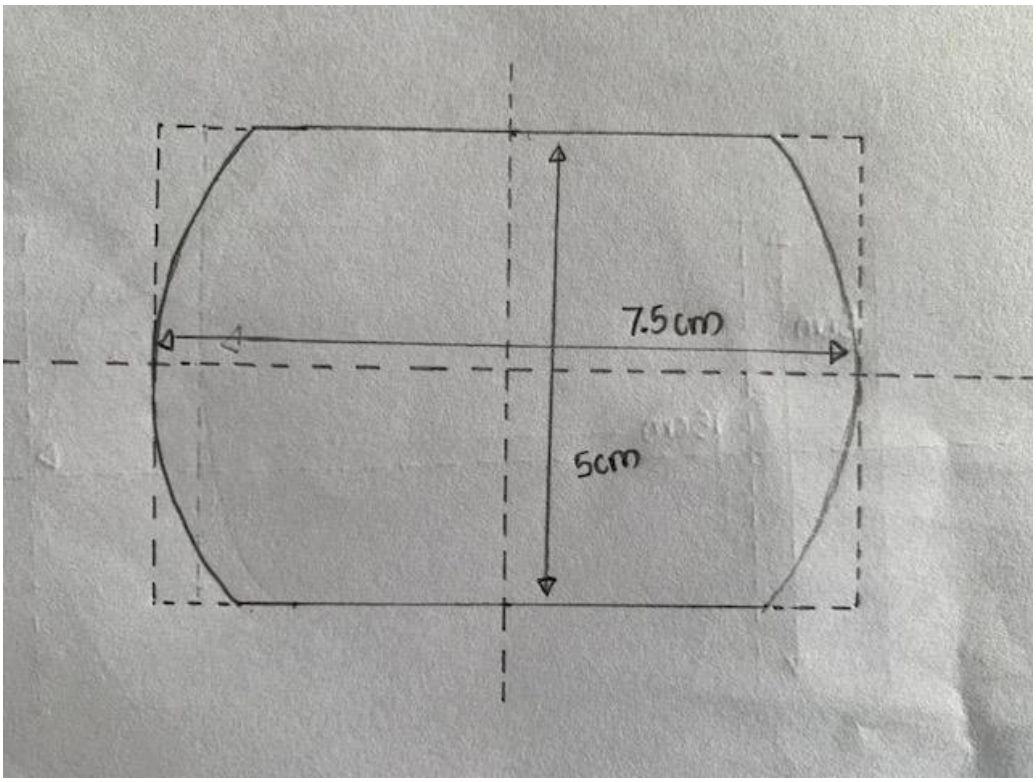
After making some minor changes to the above design, final enclosure design sketches were made using free hand sketching technique and then imported to the SOLIDWORKS Designing tool.

FREE HAND-DRAWN SKETCHES

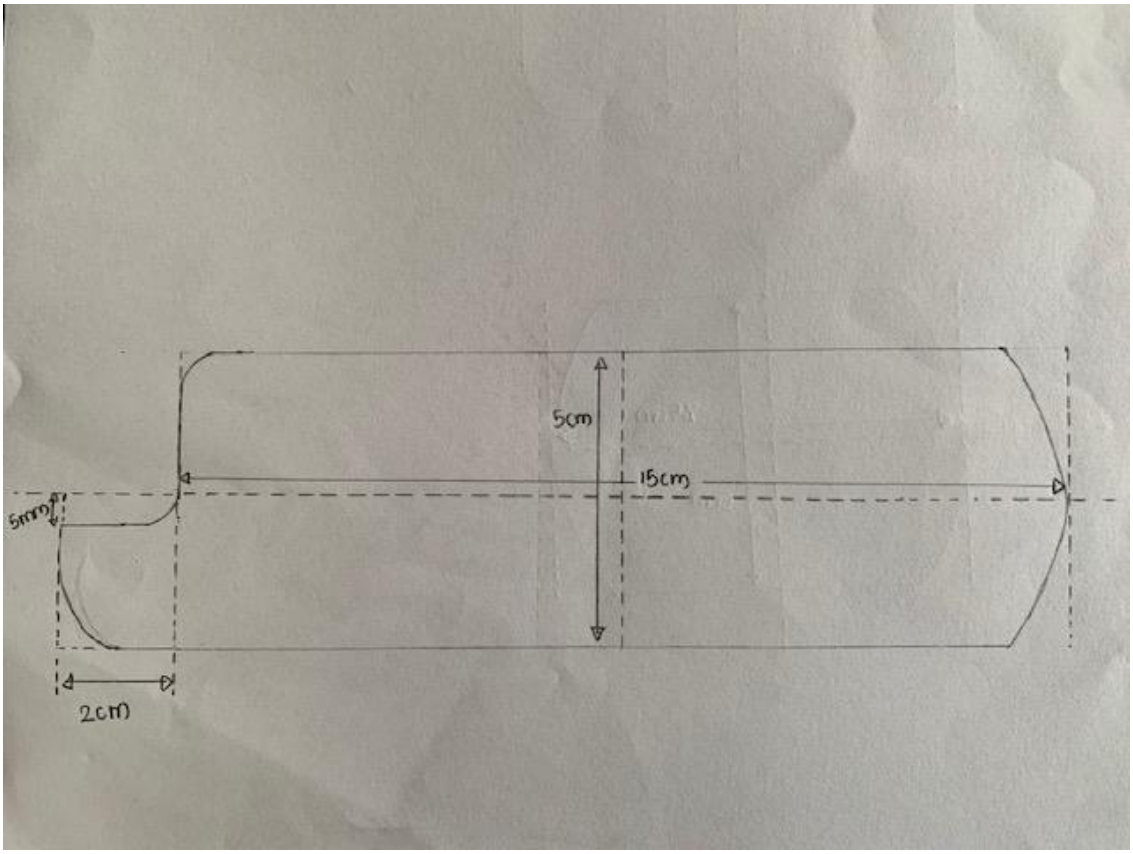
First, several free hand drawn sketches were made with perfect dimensions to visualize the final enclosure and then they were imported to SOLIDWORKS Designing canvas.



Top View



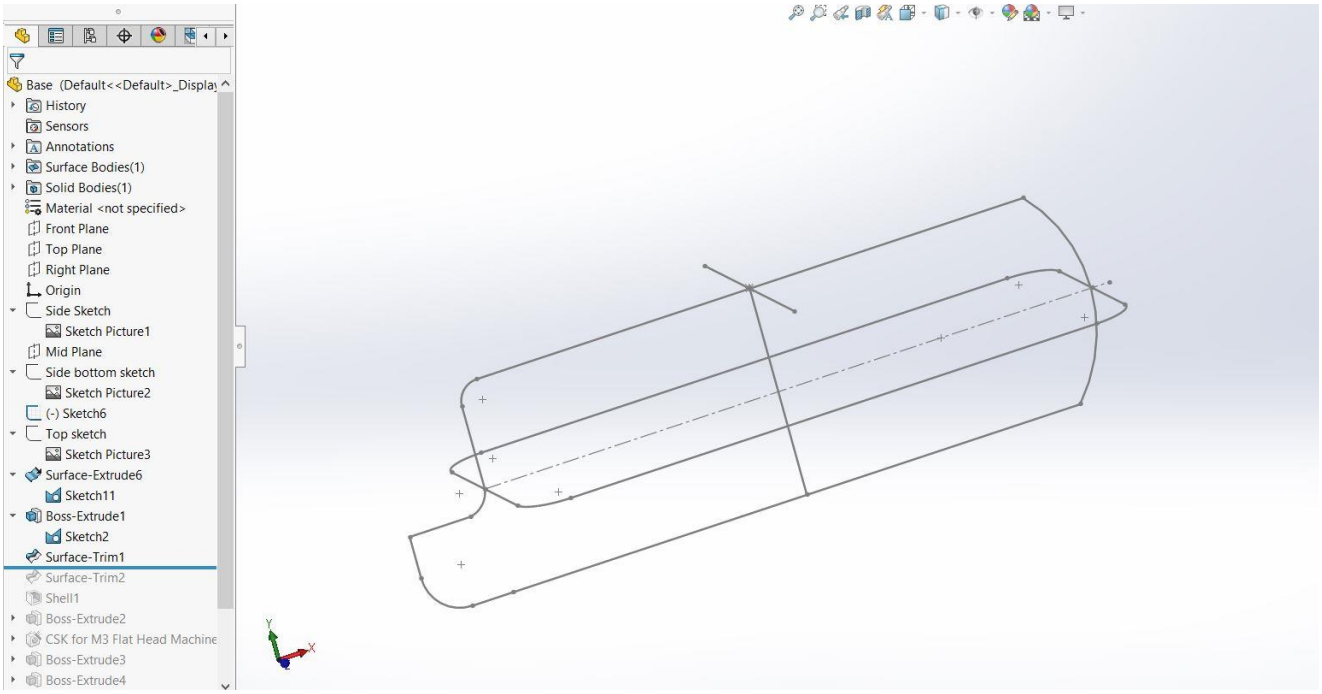
Side View 1

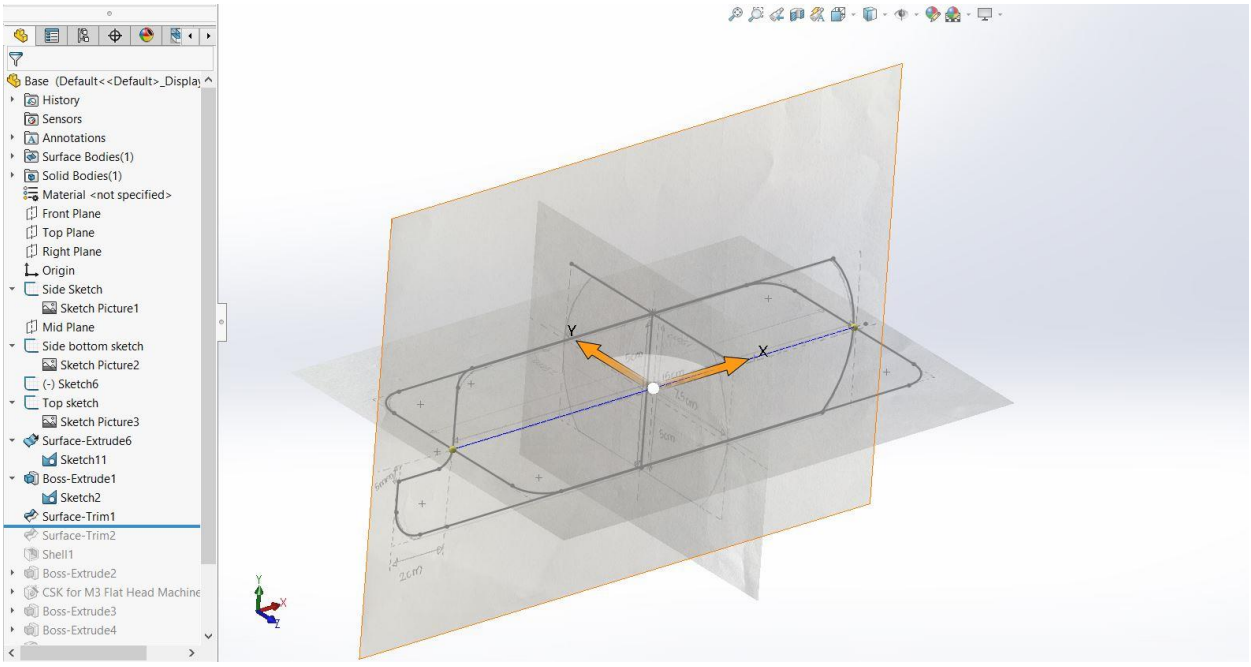


Side View 2

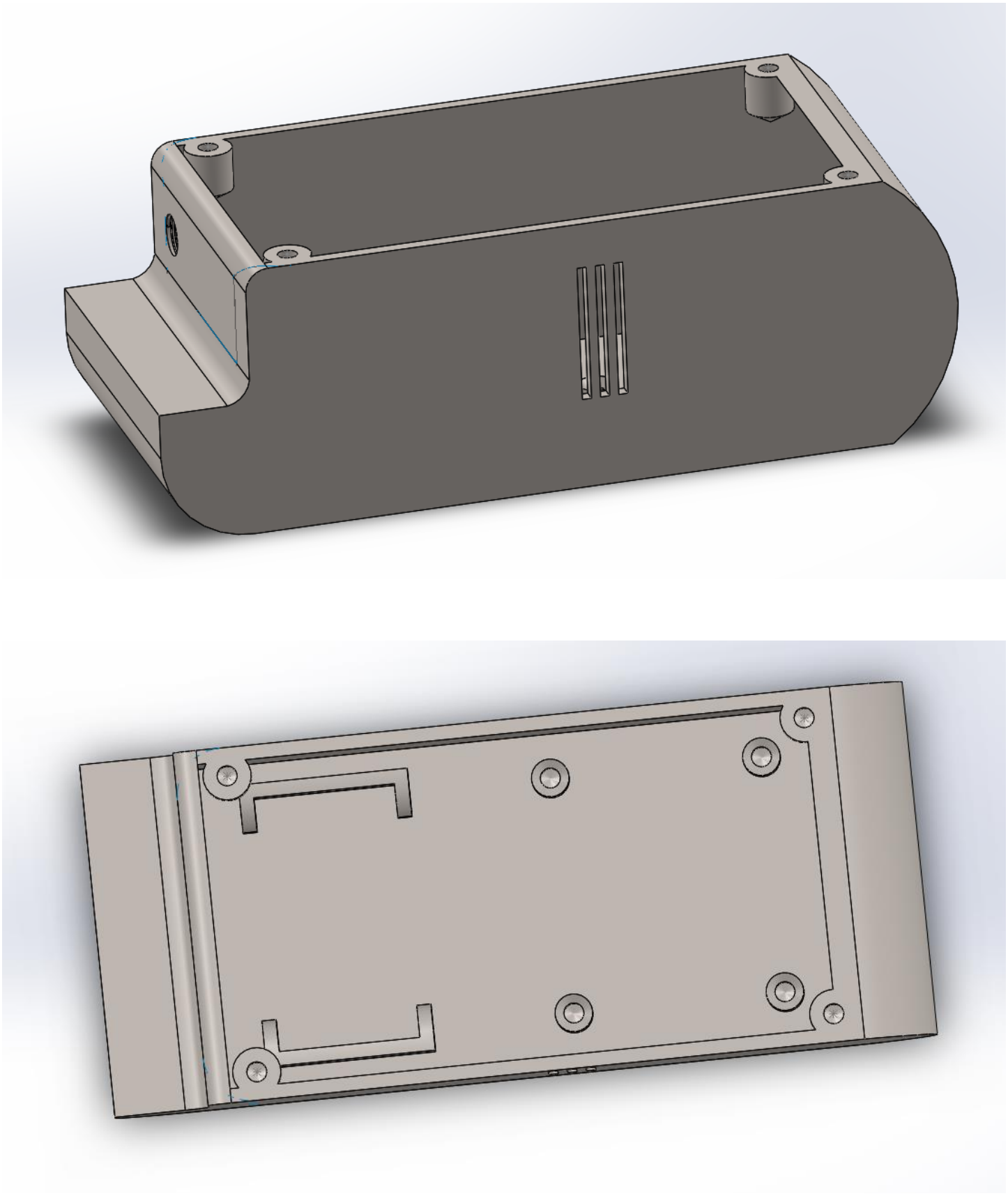
SOLIDWORKS DESIGN

Rather than designing sketches using in-build shapes and tools in the software, free-hand sketches were imported to the designing pane and then enclosure was designed using those sketches.

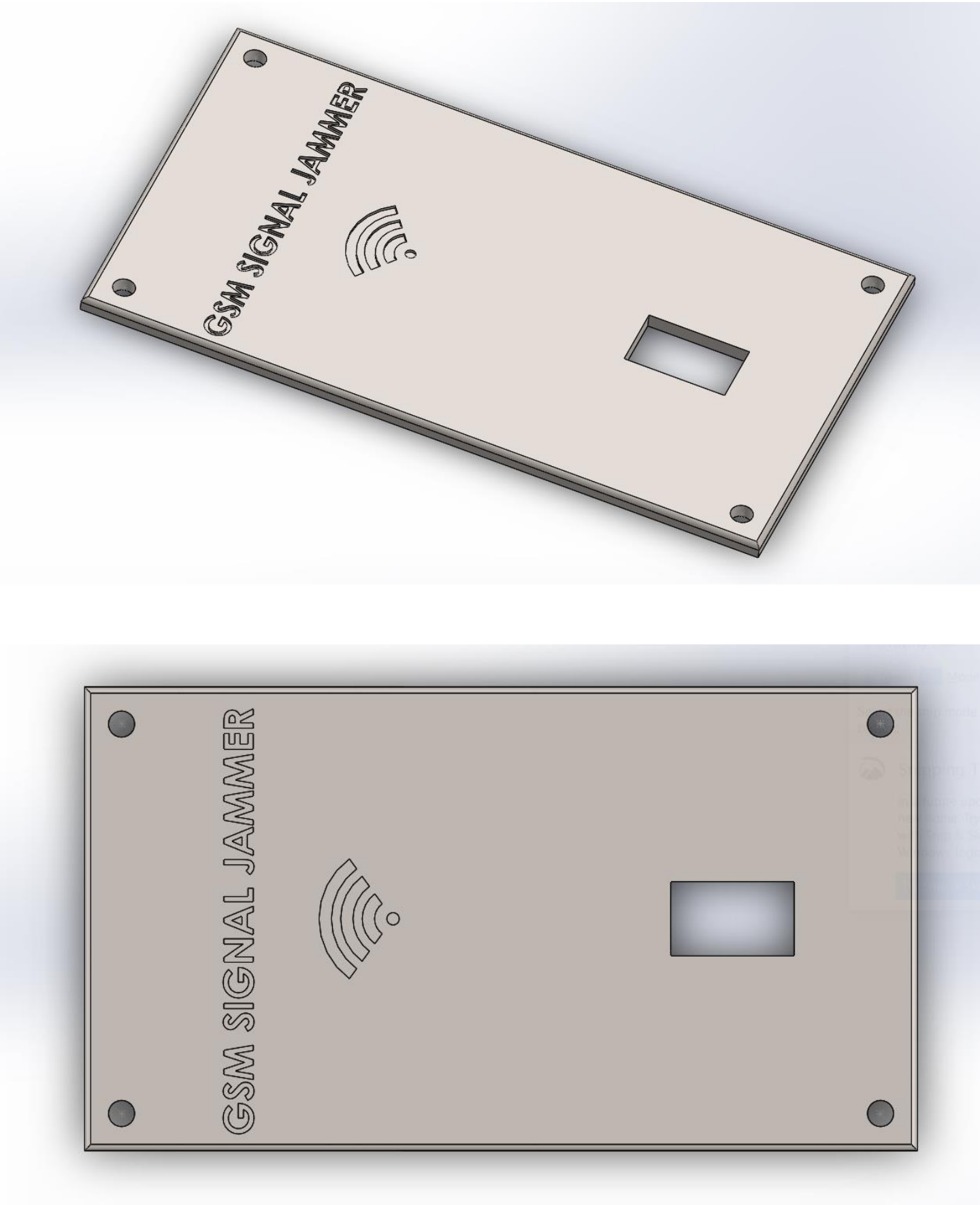




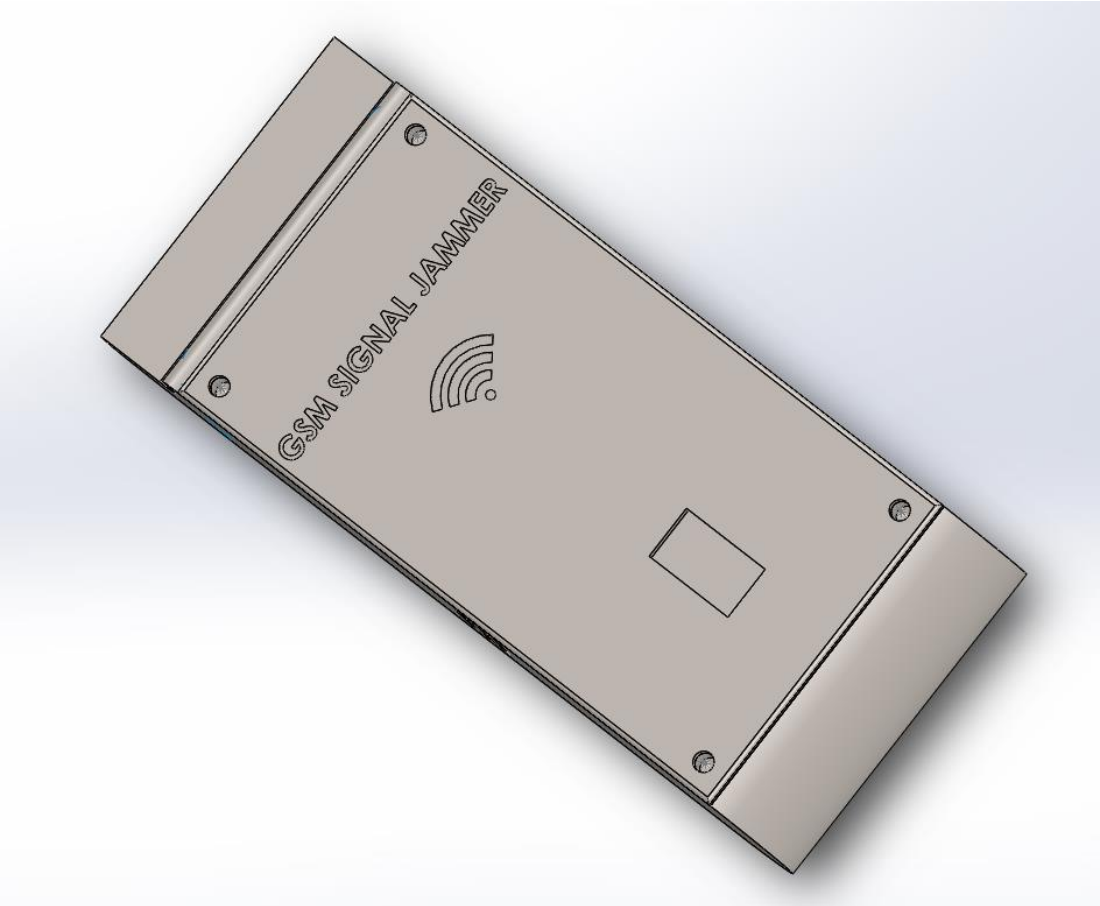
Imported Sketches in SolidWorks



Base of the Enclosure



Top Cover of the Enclosure



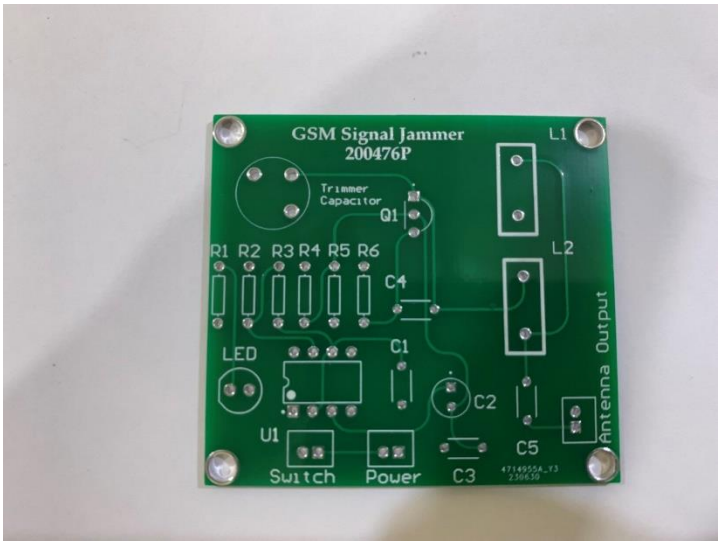
Final Assembly of the Enclosure

When designing the enclosure, four hollowed fixed vertical cylinders were made to mount the PCB firmly and some holder designs were made to place the 9V battery in the enclosure. Separate holes were made to place on the body and top cover to place GSM antenna and the power switch.

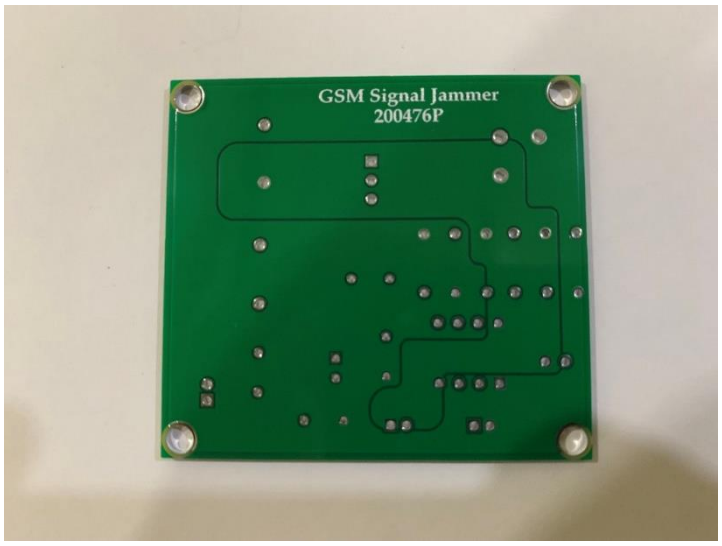
For demonstration purposes, the enclosure was made using a 3-D printing method. But, for mass production, injection molding is preferable.

FINAL PRODUCT

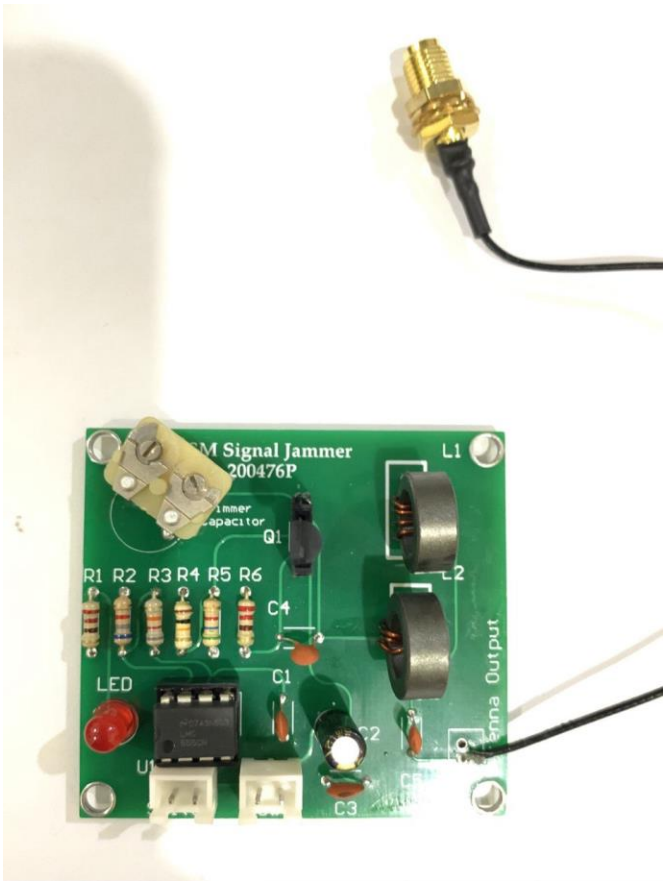
After two main stages of design process, final product is made based on the user requirements and suggested modifications to the initial product.



Final PCB – Top Layer

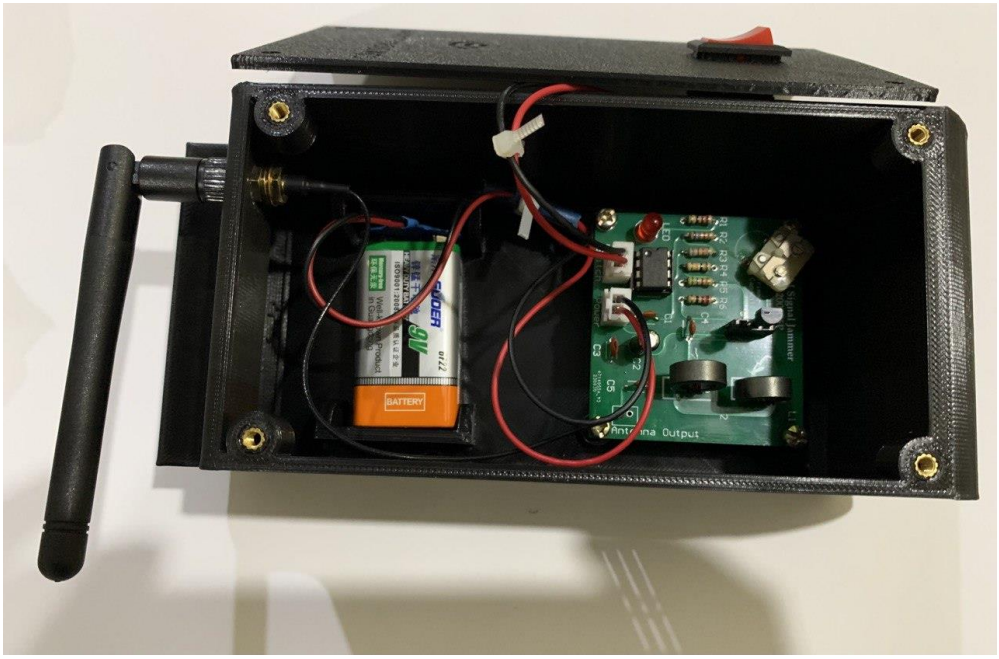


Final PCB – Bottom Layer

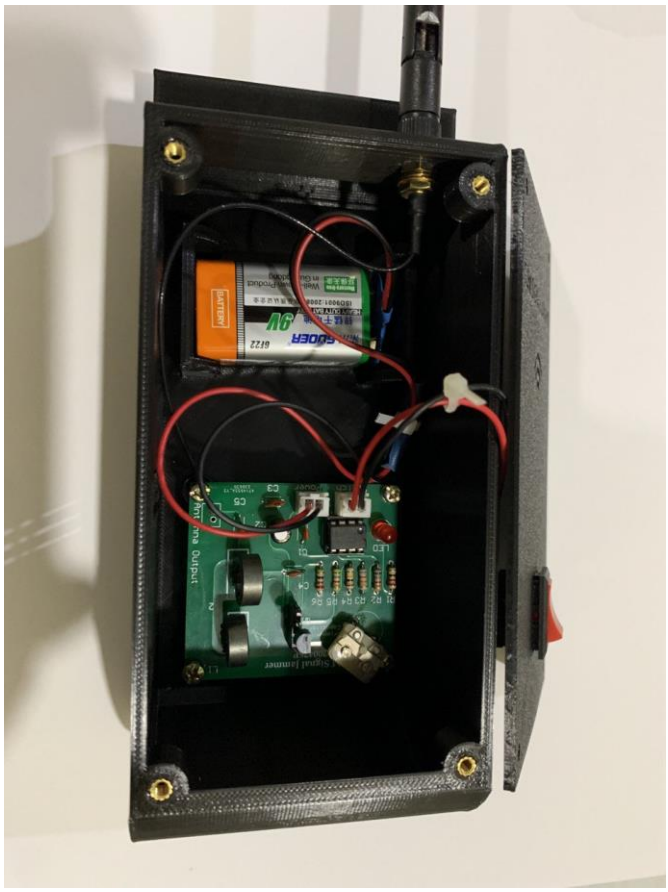


Soldered PCB – Top Side

Soldered PCB – Bottom Side



Inside of the Enclosure



Inside of the Enclosure

Outside of the Enclosure

CONCLUSION

The rapid growth of technology has led to the widespread use of mobile phone communication, with numerous advantages such as supporting games, online videos, e-commerce, and social media platforms. However, the extensive use of mobile phones in inappropriate places like churches, mosques, meeting rooms, courtrooms, and exam halls has become disruptive. To address this issue, my project aimed to design and construct a GSM jammer system that blocks GSM signal usage in designated areas.

The system effectively generates interference between mobile phones and the base transceiver station, causing the mobile phone to display “No Network”. Objectives are successfully achieved by integrating various sub-systems, including the power supply unit, intermediate frequency section, and radio frequency section. The jammer system produces a stable noise signal at 7 MHz and an output frequency close to 900 MHz, effectively disrupting GSM900 network signals used by mobile phones.

DATASHEETS

- LMC555CN CMOS Timer IC
- BC547B Transistor
- 30pF Trimmer Capacitor
- SMA Coaxial Cable Connector

REFERENCES

[1] N. G. Chrig Gupta, "Analysis of Jammer Circuit," November 2014. [Online]. Available: http://ijergs.org/files/documents/ANALYSIS-99.pdf.

[2] O. J. O. &. A. O. Habib, "Cellphone Network Jammer Circuit Using NE555 Timer," July 2022. [Online]. Available: https://fpiwitedjournal.federalpolyilaro.edu.ng/administrator/docs/8775809.pdf.

[3] E. A. a. S. S. Diana Starovoytova Madara, "Design and Testing of a Mobile-Phone-Jammer," *Innovative Systems Design and Engineering,* vol. 7, no. 7, 2016.