

Development of an RFI Signal Strength Detector

by

Nontshumayelo Mguni



*Thesis presented in fulfilment of the requirements for the
degree of*

Master of Engineering (Electronic)

in the Faculty of Engineering at Stellenbosch University

Supervisor: Dr J. Gilmore (SU), Dr A. Barnard (SU) and Dr G. Wiid (CPUT)

April 2022

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: April 2022

Copyright © 2022 Stellenbosch University
All rights reserved

Abstract

The integrity of the SKA telescopes' measurements is dependent on sufficient detection and elimination of Radio Frequency Interference (RFI). This is for both within the SKA premises and surrounding farms. A system to detect and log the various RFI sources is imperative to achieving radio quiet zones.

In this thesis, a hand-held/portable RFI signal strength detector is developed to aid the existing system of eliminating the RFI sources. The focus of this thesis is the design of a receiver that detects the major culprits namely Wi-Fi, Bluetooth and cellular networks. The detected levels are displayed visually on the device while logging the data simultaneously. Furthermore, this thesis includes the design of a signal processing system that processes the measurements that are logged along with their timestamp and positioning data to generate graphical feedback to the end-user.

To test the device in a controlled environment, measurements were acquired in a reverberation chamber. The performance of the receiver was tested separately and showed a sensitivity of approximately -50 dBm which is well above the -75 dBm the system was designed for. This performance was carried through into the measurements taken with the full system implemented. The signal processing operated as desired, and graphs can be used to inspect the maximum power, time occupancy over a set time frame.

Opsomming

Die integriteit van die SKA-teleskope se metings is afhanklik van voldoende opsporing en uitskakeling van Radiofrekwensie-interferensie (RFI). Dit geld vir beide binne die SKA-perseel en omliggende plase. 'n Stelsel om die verskillende RFI-bronne op te spoor en aan te teken is noodsaaklik om radiostil sones te bereik.

In hierdie tesis word 'n draagbare RFI-seinsterkteverklikker ontwikkel om die bestaande stelsel te help om die RFI-bronne uit te skakel. Die fokus van hierdie tesis is op die ontwerp van 'n ontvanger wat die hoof oorsake van RFI, naamlik Wi-Fi, Bluetooth en sellulêre netwerke, opspoor. Die bespeurde vlakke word visueel op die toestel vertoon terwyl die data gelyktydig aangeteken word. Verder sluit hierdie tesis die ontwerp van 'n seinverwerkingstelsel in wat die metings wat saam met hul tydstempel en posisioneringsdata aangeteken word verwerk om grafiese terugvoer aan die eindgebruiker te genereer.

Om die toestel in 'n beheerde omgewing te toets, is metings in 'n nagalmkamer verkry. Die werkverrigting van die ontvanger is afsonderlik getoets en het 'n sensitiwiteit van ongeveer -50 dBm getoon wat ver bo die -75 dBm is waarvoor ontwerp is. Hierdie prestasie is deurgevoer in die metings wat geneem is met die volledige stelsel geïmplementeer. Die seinverwerking werk soos verlang, en grafieke kan gebruik word om die maksimum krag, tydbesetting oor 'n vasgestelde tydraamwerk te inspekteer.

Acknowledgments

Although only my name appears on the front page of my thesis, I could not and did not complete it on my own. This Master's degree is the result of the efforts of many people, and I'd like to take this opportunity to express my gratitude toward the following persons:

- My supervisors for their support throughout this process. You've been supportive in ways I didn't expect from a supervisor during the challenges I've faced since moving home for lockdown. I appreciate all of your counsel and words of wisdom and recognizing when I needed a break. Also, thank you for all of your additional assistance towards the end of the thesis.
- The South African Radio Observatory (SARAO) for funding this research.
- Everyone who was involved in the physical configuration of this project. Starting with Mr Wessel Croukamp, Mr Gift, and Mr Wynand from Stellenbosch University's (SU) for helping me etch breakout board and drilling all of my enclosure's cut-outs. Also Mr Arendse (SU) for his willingness to solder my tiniest components for me. In addition, Circor - a component placement company, that offered to place the components of my final PCB using their heat flow machine for me.
- All those who helped me gather measurements. I appreciate your patience with me. A special thank you to Mrs Anneke Bester (SU) for always being kind and willing to help, and to Dr Kurt Coetzer (SU) for his readiness to assist me in finding emissions. Also, Jason, Siya, Tankiso, and Kabo from SARAO's RFI team, who have been really helpful with the chamber tests and are always a pleasure to work with. Thank you for making me feel welcome to measure.
- To my friends, for always sending me encouraging messages and reassuring me that God wants me to succeed. This year has shown me how fortunate I am to have such close friends. Special thanks to Philip Goosen, William van Wyk, Dylan Fry and Alford Sibanda for always being available for technical advice. I'm looking forward to making up for the times I could not participate this year.
- To my family, I'd like to express my gratitude to my parents for working tirelessly to guarantee that I have a good education and want for nothing. I'm here because of your sacrifices. Thank you, Solomuzi and Nothando, for all the laughs during the years, for consoling me at difficult times, and for supporting me through it all. I thank my family for praying for me every day this year.
- Above all, I'd like to express my gratitude to God for His constant presence in my life, especially in the last two years. I am thankful for all of the insights I've learned from His Word that have kept me from losing hope. I am grateful to God for the community of people that he has placed around me.

Contents

Declaration	i
Abstract	ii
Opsomming	iii
Acknowledgments	iv
List of Tables	viii
List of Figures	ix
1 Introduction	1
1.1 Background	1
1.1.1 Square-Kilometre Array	1
1.1.2 Radio frequency interference on SKA1-MID site	2
1.1.3 Existing RFI detection and mitigation techniques in SKA1-MID	3
1.2 Motivation	5
1.3 Objectives	6
1.4 Thesis Layout	6
2 Literature Study	7
2.1 Characterizing RFI of Interest	7
2.1.1 Cellular networks	7
2.1.2 Wi-Fi	9
2.1.3 Bluetooth	10
2.2 Electromagnetic Compatibility	13
2.2.1 Source and victim	13
2.2.2 Current flow	14
2.2.3 Unintentional antennas	14
2.2.4 Coupling mechanisms	14
2.2.5 EMC shielding	15
2.3 Description of RF receiver fundamentals	16
2.3.1 Scattering parameters	16
2.3.2 Mixing signals	18
2.3.3 Noise performance	19
2.4 Analogue to Digital Conversion	20
2.4.1 Quantisation	20
2.4.2 Sampling	22
2.5 Processing Options	23

2.6	Conclusion	24
3	RF Receiver Front-end	25
3.1	Receiver Architectures	25
3.2	Design of the Receiver Signal Chain	27
3.2.1	Chosen signal chain receiver	29
3.3	Antenna	30
3.3.1	Antenna directivity, radiation efficiency and gain	30
3.3.2	Antenna selection	31
3.3.3	Measurements	32
3.4	Low-noise Amplifier	34
3.4.1	Linearity of LNA	34
3.4.2	Selecting an LNA	34
3.4.3	Measurements	35
3.5	Power Splitter	36
3.5.1	Characteristics of power splitters	36
3.5.2	Selection of a power splitter	37
3.6	Filters	38
3.6.1	Characteristics	39
3.6.2	Selection of filters	39
3.6.3	Measurements	40
3.7	Power Detector	41
3.7.1	Characteristics of power detectors	41
3.7.2	Selection of a power detector	43
3.7.3	Measurements	43
3.8	Performance of the RF Front-end Receiver	44
3.8.1	Simulation	44
3.8.2	Measurement	46
3.9	Conclusion	49
4	Signal Processing	50
4.1	System Overview	50
4.2	Micro-controller	51
4.2.1	STM32 development board	51
4.2.2	Transferring data on the micro-controller	54
4.2.3	Timers and timer interrupts	54
4.2.4	ADC on STM32F334R8	55
4.2.5	Time controlled LEDs	56
4.2.6	Position tracking data	57
4.2.7	Real-time clock	58
4.2.8	Memory and storage	59
4.3	Post-processing and GUI	63
4.3.1	Serial communication protocol	64
4.3.2	Data Processing	65
4.4	Conclusion	65
5	System integration	66
5.1	Sub-circuits	66
5.1.1	Power distribution	66

5.1.2	SD card connector slot	68
5.1.3	USB interface	69
5.1.4	GNSS receiver	70
5.2	Printed circuit board design/layout	71
5.3	Enclosure	73
5.4	Conclusion	75
6	Performance of RFIPD_v00	76
6.1	EMC Compliance Testing	76
6.1.1	Reverberation chamber	76
6.2	Measurements	77
6.3	Functionality Tests	80
6.3.1	Frequency sweep test	80
6.3.2	Power level sweep test	82
7	Conclusions and Recommendations	84
7.1	Conclusions	84
7.2	Recommendations	85
	Bibliography	86
A	STM32 Board Ranges	89
B	RFIPD Configuration Phases	91
B.1	Circuit Schematic Design	92
B.2	PCB Layout design	93
B.3	Enclosure Design Dimensions	95

List of Tables

1.1	Current frequency range on SKA1-MID site, characterised according to precursor telescope's parameters.	2
2.1	South Africa's cellular network spectrum allocations for service providers [9][11]	8
2.2	Brief summary on the development of Wi-Fi standards [16]	10
3.1	Centre frequencies and bandwidth of RFI signals of interest	27
3.2	Specifications of ANT-LTE-SMA-MON antenna [40]	32
3.3	Specification of the SMA3103 LNA at test frequency, 1 GHz [42]	35
3.4	Specifications of the SEPS-4-272+ power splitter [45]	38
3.5	Specifications of RF front-end bandpass filters for each channel	39
3.6	Specifications of LT5538 log power detector at 880 MHz	43
3.7	The RF receiver's passband peak, stopband peak and stopband attenuation . .	45
4.1	Key specifications of STM32F334R8 micro-controller	52
4.2	The settings for the timers implemented on the micro-controller	55
4.3	Nyquist frequency for each channel to be sampled	55
4.4	Example of NMEA message structure for when the message is \$GNRMC . . .	58
4.5	Comparison of the accuracy of implementing the RTC with the 32.768 kHz source and 40 kHz source	59
4.6	Primary flash memory organization	60
4.7	FAT file system comparisons	62
4.8	Comparison of the data rates achieved with different writing buffer lengths . .	62
4.9	Description of serial communication protocol for messages sent from the RFI Detection App to the RFIPD	64
5.1	GNSS LNA and antenna	71

List of Figures

1.1	Precursor receivers, HERA (a) and Meerkat (b), located on the Meysdam and Losberg farms in South Africa’s Karoo region that are planned to be integrated into SKA1-MID [2].	1
1.2	Setup for characterising environmental RFI at SKA1-MID [5]	3
1.3	Spiral design layout of SKA1-MID antenna locations on NRF-owned land and expanding onto servitude farms [1]	4
2.1	GSM/GPRS/EDGE data transmission frame [13]	9
2.2	Model of (a) UMTS data [14] and (b) LTE Type 1 [15] transmission frame for 3G and 4G technology	9
2.3	2.4 -2.408 GHz of ISM band shared by Bluetooth, BLE, Wi-Fi communications [19]	11
2.4	Classic Bluetooth data packets [21]	12
2.5	Bluetooth Low-Energy data packets [22]	12
2.6	Diagram illustrating the three elements involved in generating interference in a system: Noise Source, Path, Victim [23]	13
2.7	Illustration of (a) electric fields coupling onto adjacent conductor through capacitive coupling and (b) magnetic fields coupling onto adjacent conductor through inductive coupling [23]	15
2.8	Diagram of an n-port <i>black box</i> network [26]	16
2.9	Illustration of the result produced through mixing two signals to achieve (a) up-conversion and (b) down-conversion [28]	18
2.10	Illustration of SNR in a signal with noise [31]	19
2.11	Difference between 1-bit, 2-bit, 4-bit and 16-bit resolutions [33]	21
2.12	Sampling and quantisation of a continuous-time, continuous-range signal [34]	22
2.13	Effects of sampling at different frequencies [34]	23
3.1	Tuned radio frequency receiver [26]	25
3.2	Super-heterodyne receiver [26]	26
3.3	Direct-conversion / Zero IF receiver [26]	26
3.4	Signal chain design 1 considered for the RFIPD_v00 receiver	27
3.5	Signal chain design 2 considered for the RFIPD_v00 receiver	28
3.6	Final receiver front-end design for RFIPD_v00	29
3.7	Model of the radiation pattern of an (a) isotropic, (b) omnidirectional and (c) directional antenna, illustrating the directivity of each type of antenna [39]	30
3.8	Illustration the the movement of the chosen antenna’s tilting mechanism [40]	32
3.9	Reflection coefficient measurements from the manufacturer conducted with ground plane (black) and measurement conducted without a ground plane (red)	33
3.10	Plot showing the 1 dB compression point of amplifier [26]	35

3.11	S-parameter gain that was (a) provided by the manufacturer and (b) measured on a custom SMA3103 breakout board	36
3.12	Main topologies for power splitter design: Resistive, Wilkinson and Hybrid Divider [43]	37
3.13	S-parameters of SEPS-4-272+ power splitter	38
3.14	Diagrams of the frequency response for polynomial filters - (a) Butterworth, (b) Chebyshev 1, (c) Chebyshev 2, and (d) Elliptic filters [44]	39
3.15	Filter responses provided by the manufacturer (black) and measured on custom breakout boards (red) for each RF channel filter - (a) filter TA0627A with f_{center} of 895.5 MHz (b) TA0391A with f_{center} of 1745 MHz (c) TA0401C with f_{center} of 1950 MHz (d) TL0009A with f_{center} of 2450 MHz	40
3.16	Diagram showing the effect of varying RC time constants on the shape of the envelope in a envelop detector [46]	41
3.17	Results of power detector performance test	44
3.18	AWR model of receiver	45
3.19	Transmission coefficients from the simulation of the RF front-end done in AWR	46
3.20	RF Frontend output across channels when input frequency is 895,5MHz	47
3.21	RF Frontend output across channels when input frequency is 1747,5MHz . . .	47
3.22	RF Frontend output across channels when input frequency is 1950MHz	48
3.23	RF Frontend output across channels when input frequency is 2450MHz	48
4.1	An overview of the signal processing system	50
4.2	Nucleo-F334R8 Development board layout, where (a) Top layout (b) Bottom layout[50]	52
4.3	Micro-controller flowchart diagram	53
4.4	Screenshot of memory regions used in the micron-controller.	60
4.5	File Allocation Table(FAT) file system layout structure	61
4.6	Screenshot of the two tabs in RFI Detection App, whereby (a) the first tab is related to serial communication functions and (b) the second tab is related to data processing functions.	63
5.1	Schematic diagram of SD card peripheral	69
5.2	Schematic diagram of USB peripheral	70
5.3	Schematic diagram of GNSS tracking sub-circuit	71
5.4	Top and bottom layer design of RFI detector PCB	72
5.5	A photo of the enclosure with the RF antenna and GNSS antenna connected .	74
6.1	Diagram of (a) a model of the layout of the SARA0 reverb chamber [55] and (b) the actual measurement setup	77
6.2	Radiated power as measured in the RC with the DUT off (blue trace) and with the DUT on (black trace) when the RFIPD enclosure is open	77
6.3	Radiated power as measured in the RC with the DUT off (blue trace) and with the DUT on (black trace) when the RFIPD enclosure is closed	78
6.4	A picture of the shielded loop probe	78
6.5	A picture of the RFIPD setup when enclosure is open with shielding over the GNSS receiver and the GNSS antenna removed from it's hole	79
6.6	Radiated power as measured in the RC with the DUT off (blue trace) and with the DUT on (black trace) when the RFIPD enclosure is open with shielding over the GNSS receiver and the GNSS antenna removed from it's hole	79

6.7	Screenshot of the output from the PC software when a frequency sweep at a power level of -10dBm is set to step from a frequency of 600 MHz to 2600 MHz, in steps of 10 MHz, holding at each step for 1s is applied at the RFIPD input, where (a)Channel 1 (b) Channel 2 (c) Channel 3 (d) Channel 4.	81
6.8	Screenshot of time occupancy report from the PC software display	82
6.9	Screenshot of the RF Front-end output across channels when input frequency is 895,5MHz and the power level is set to step from a frequency of -100 dB to 0 dB, in steps of 10 dB, holding at each step for 4s.	82
A.1	STM32 MCU's categorised according to ARM processor and suggested application [49]	89
A.2	STM32F334 block diagram illustrating the features of microcontroller [56] . .	90
B.1	Full schematic diagram	92
B.2	Bottom PCB layer	93
B.3	Top and bottom PCB layer	94
B.4	Dimensions of the enclosure Lid	95
B.5	Dimensions of the enclosure Bottom	96

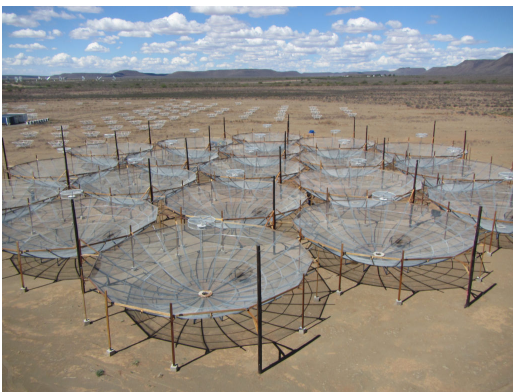
Chapter 1

Introduction

1.1 Background

1.1.1 Square-Kilometre Array

The Square-Kilometre Array (SKA) is a large-scale collaborative project which combines the efforts of international engineers, scientists and policy makers to create the world's largest radio telescope. Remote locations in Australia and South Africa were selected to co-host the SKA after satisfying scientist's criteria such as population density, atmospheric properties, and proximity to support bases. The Australian site, also known as SKA-LOW, will host thousands of low-frequency antennas and the South African site, known as SKA-MID, will host hundreds of receiver dishes that cover the mid-frequency and high-frequency of the SKA [1].



(a)



(b)

Figure 1.1: Precursor receivers, HERA (a) and Meerkat (b), located on the Meysdam and Losberg farms in South Africa's Karoo region that are planned to be integrated into SKA1-MID [2].

The SKA-MID is currently in phase 1 (SKA1-MID) of its development in South Africa's Karoo, which currently hosts the Meerkat and HERA (Hydrogen Epoch of Reionization Array) precursor projects, seen in Figure 1.1. The Meerkat is currently the most sensitive telescope in the southern hemisphere. However, once it is fully integrated into the completed SKA1-MID then the SKA will have that title. Until then, the bandwidth

observed of SKA1-MID is characterised by the precursor telescopes listed in Table 1.1 [3].

Astronomy receiver	Frequency bandwidth
HERA	50MHz – 250MHz
MeerKAT UHF	580MHz – 1015MHz
MeerKAT L-Band	900MHz – 1670MHz
MeerKAT S-Band	1750MHz – 3500MHz

Table 1.1: Current frequency range on SKA1-MID site, characterised according to precursor telescope’s parameters.

The phased approach of having precursors has provided invaluable insight and knowledge for scientists to use in the next decade of the SKA project. Additionally, the scalability gained from using antenna arrays makes the potential of expansion of the SKA nearly limitless. This is a state of the art venture into unknown avenues of astronomy.

1.1.2 Radio frequency interference on SKA1-MID site

Electromagnetic interference (EMI) is a form of electromagnetic disturbance which poses a threat to the effective operation of electronic systems. Radio-frequency interference (RFI), on the other hand, is EMI which lies within the radio frequency spectrum range (3kHz to 300GHz) [4]. In radio astronomy, RFI refers to man-made signals which exceed the power levels of the natural signal observed, creating a misidentification of astronomical signals. The high sensitivity of SKA1-MID receivers makes it highly susceptible to various RFI.

The radio spectrum is highly populated nowadays, creating many possible sources of RFI. The disturbances can originate, as mentioned in [1], from either

- External sources which are emissions that radiate radio waves in close proximity to the SKA1-MID receivers. These may or may not be controlled by SKA.
- Internal sources refer to devices with an electromagnetic by-product generated by the components in the system.
- Overhead sources refer to transmitters passing above the site for example aircraft and satellites.

The radio frequency bandwidth in which SKA1-MID operates was observed for an hour using a wide-band omnidirectional antenna and the MESA Product Solutions RTA-3 real-time analyser, see the measuring vehicle setup in Figure 1.2. FM radio, SABC TV, UHF Satcom, GSM, aeronautical navigation, satellites and ISM (Wi-Fi) signals were all identified to be the main sources of RFI [5]. Furthermore, it is important to note that the impact of the different sources is not the same. The impact of RFI is accessed by the signal strength and frequency. Weak, out-of-band RFI may have minimal impact on observations. Strong and persistent signals, however, may corrupt observation data and if the signal is strong enough it may permanently damage the telescope.



Figure 1.2: Setup for characterising environmental RFI at SKA1-MID [5]

1.1.3 Existing RFI detection and mitigation techniques in SKA1-MID

For hyper-sensitive receivers of cosmic emissions, the presence of RFI adds to the power measured. Therefore the measurements are in fact combinations of desired cosmic emission and RFI. Depending on time occupancy and strength of the RFI signal the level of difficulty to detect these will vary, for example, it may be easier to spot a strong, spiking pulse RFI signal than a continuous weak RFI signal. The SKA1 team is constantly on the lookout for ways to improve the detection, monitoring and elimination of all known and potential RFI signals. There have been many developments to suppress RFI emissions or possibly fully remove the RFI source.

Limiting the possible RFI is one of the biggest motivations for selecting the remote Karoo in South Africa. The expansion of the SKA1-MID requires more space beyond the original Karoo Observatory. The majority of dishes are positioned at the core of the site, then the rest of the dishes are spread across multiple land properties in 3 spiral lines, as shown in Figure 1.3. The National Research Foundation (NRF) owns the land of the SKA1-MID core, and with the help of SANParks, it has been declared a national park as means of protecting the land. The land along the spiral arms of SKA1-MID is protected using servitude agreements with the property owners. Having secured land is a fundamental step to regulating RFI by having it as law. Furthermore, the SKA1-MID is protected by the Astronomy Geographic Advantage Act, 2007 (Act No. 21 of 2007) (Government Gazette Notice 33462, 20 August 2010) [6].

Initiatives to protect SKA1-MID signal integrity from RFI began on the design level by adding features that limit the impact of RFI. One such feature is the antenna design which suppresses signals that are outside of the line of sight or from irrelevant directions. Another feature is, when non-astronomical signals are detected, they can be eliminated using sophisticated computing approaches. However, RFI signals are not always detectable. Additionally, using more sophisticated techniques, the SKA telescopes will reduce the effect of RFI by not distorting the astronomical component of a signal which was mixed with interference. The above-mentioned approaches to eliminating RFI make use of al-

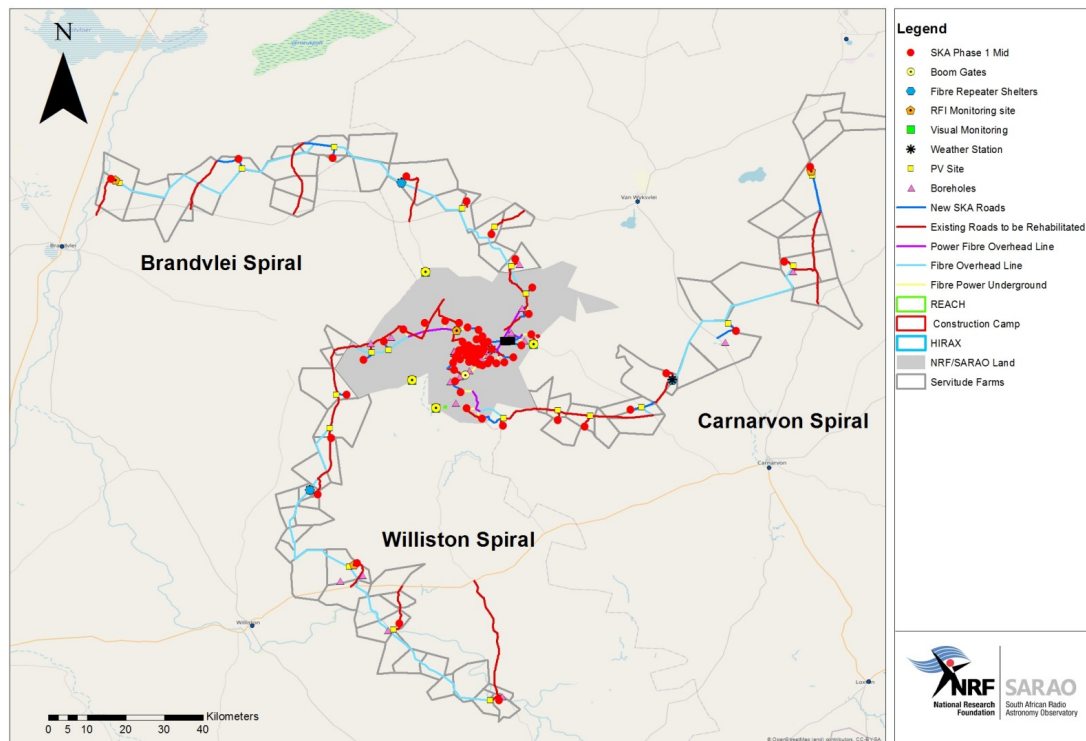


Figure 1.3: Spiral design layout of SKA1-MID antenna locations on NRF-owned land and expanding onto servitude farms [1]

gorithms in the back-end processing of the telescopes system. Theoretical algorithms are based on either one or a combination of signals in the time domain, frequency domain, spectrogram domain, statistical domain and polarimetry domain [7]. They operate by identifying the presence of RFI on the incoming signal, then correcting the data in the desired domains [8].

To detect, identify and locate the sources of RFI can be a daunting task for the SKA1-MID RFI team. As illustrated in Figure 1.2, it is common practice to drive for hours with a mounted antenna connected to a hand-held real-time analyser (RTA) in search of the RFI source. It is much like looking for a needle in a haystack.

In 2016 [8], a plan was set out to create an RFI detection and monitoring system which incorporates 1) a fixed station that monitors continuously in the centre of the site and 2) a portable system that could be set up anywhere. The ideal plan was to have this system cover a range of 20MHz to 15GHz , the same bandwidth as the SKA and use fibre optic cables to minimize EMI. The SKA Reconfigurable Application Board (SKARAB) would be used as the key digital signal processing unit for the incoming data [8].

The fixed monitoring subsystem will be mounted in pre-selected positions and monitor RFI emissions using omnidirectional antennas. Also, it will connect to the control building using fibre optics to ease the control of executing different programmes. The mobile monitoring device needs to be just as sensitive as the fixed monitor. The concept for mobile monitoring is to have a rechargeable battery-powered device that can be left unattended overnight in a remote area of the site to do measurements. The presence of humans may cause transients, affecting the measurements negatively.

Finally, the third form of RFI monitoring that is planned is the deployable monitoring devices. These are to be positioned on the edges of the site to keep track of any spectral changes. The demand for high sensitivity is not a key factor, but rather the ability to measure high powered signals without saturation. The positions of these devices are temporary and may be moved routinely after a set time frame [8].

1.2 Motivation

Regardless of the multiple regulations, RFI from the environment is always present and changing. This is both at the SKA1-MID core and the servitude farms. There are some restrictions and limitations in the current methods of detecting, identifying, and mitigating RFI sources effectively, listed below:

- Using RTAs to find RFI sources around the SKA site is very time-consuming because there is no guideline to narrow the search area. Furthermore, RTA's are generally expensive and it requires highly skilled personnel to operate the RTA, therefore only a few people can perform this task.
- Additional design features using advanced computer algorithms in the telescopes are better suited for removing internal and overhead RFI sources e.g. EMI, "sky noise" and satellites orbiting. However, it is not as well-suited for locating external sources and then removing them. It is preferable for the telescopes to capture celestial signals free of external RFI signals, such as Wi-Fi, than to process signals that are approximated after computationally filtering out the external source, hence physically removing the external source is desired.
- There are many rules and regulations for entering the SKA1-MID site. However, people can become complacent and forgetful of rules, and there is no way to check that there are no hidden sources of RFI radiating from personnel's belongings or vehicles as they enter. Furthermore, it is important to check the emissions of vehicles entering, because some vehicles' Bluetooth modules continue to be active while the car is off.
- There is no way for servitude farm owners to detect emissions from their property by themselves.

The integrity of the SKA1-MID telescope measurements is dependent on the absence of RFI. The presence of RFI can corrupt time-critical data, furthermore the presence of strong RFI may damage the physical receiver instrumentation. It is important to improve the existing techniques.

In summary, an instrument is required to assist current mitigation systems to be more effective. A small, low-cost, easy-to-use RFI signal strength detection system for the identification of major/common external sources, specifically Wi-Fi, Bluetooth and cellular networks are needed to improve the regulation of RFI sources of SKA1-MID. This is so that individuals can operate the device after a basic demonstration or tutorial. This would allow security guards to enforce rules and regulations more effectively at gates by performing quick RFI detection tests. Additionally, servitude farm owners may also

detect and control emissions on their property by themselves. Finally, such a device could be deployed on a mobile platform such as a drone and returned with feedback regarding the positioning of RFI signals, therefore immensely limiting the region for the RFI team to "hunt" and remove the source.

1.3 Objectives

After a rundown on the background, motivation and aim of this thesis, we can go on to define the study's goals. The steps taken to reach the purpose are outlined in the thesis objectives. Three objectives were determined based on the preceding discussion.

The first objective is to investigate and characterize the relevant RFI signals which include cellular networks, Bluetooth, and Wi-Fi. Understanding these signals is necessary for developing specifications and design requirements for the remaining goals.

Secondly, a mobile RFI power detector must be designed and implemented to detect and visually indicate the presence of the relevant RFI signals. If possible, indicate the signal strength and the frequency band in which power was detected. Furthermore, log measured data along with corresponding GPS position and timestamp. This device must be suitable for each of the three scenarios listed below:

- At the entrances of the SKA1 site, security personnel use it to verify for compliance with emissions regulations.
- Servitude farm owners use it to keep track of the emissions produced on their farms.
- Automatically collect data when deployed on a UAV or bakkie.

Due to the fact that this is an initial prototype, the RFI power detector will be referred to as RFI power detector version 0, or abbreviated as RFIPD and RFIPD_v00.

The final objective is to design and develop a PC software program that presents processed data and generates graphs relating to the power of the measured signals. This is important for further analysis and evaluation of observed measurements over a time frame.

1.4 Thesis Layout

Chapter 1 provided a brief introduction to the RFI environment in SKA1-MID and laid out the motivation behind and objectives of the project. **Chapter 2** provides more in-depth background knowledge on the RFI signals of concern in the project, as well other topics pertinent to the completion of the project. The RF receiver front-end design and tested is described in **Chapter 3**, while **Chapter 4** describes all the signal processing done to data being measured. This includes logging the data along with GPS positioning and transferring to the PC software program that does further processing and data visualisation. The integration of all the systems sub-circuits and physical layout of the RFIPD is discussed in **Chapter 5**, with the results and conclusion given in **Chapters 6** and **Chapters 7** respectively.

Chapter 2

Literature Study

The aim of this section is to provide background information on the thesis themes. To begin, the characteristics of cellular networks, Wi-Fi, and Bluetooth operation and data transfer are investigated. This is followed by discussions on electromagnetic compatibility and then fundamental principles surrounding receivers.

2.1 Characterizing RFI of Interest

Characterizing input signals is necessary to provide parameters for designing any receiver system. The RFI power detector aims to detect and locate removable external sources of RFI that have been previously found in SKA1-MID. These were identified in Section 1.2 to be cellular networks, Bluetooth and Wi-Fi. This section investigates the nature of these signals as they propagate in space.

2.1.1 Cellular networks

Cellular network technologies have evolved tremendously over the years. The demand for faster network communications and data transmission speeds of cellular networks is constantly increasing. The various technological developments of mobile phone networks are categorized into generations, starting with the second generation (2G), and followed by the third generation (3G), fourth generation (4G) and the much anticipated fifth generation (5G) technologies.

2.1.1.1 Background

The term “2G” refers to the first cellular network to be established at the beginning of the 1990s, called Global System for Mobile Communications (GSM) technology. Voice transmission was the primary objective of mobile phones in those days. The demand for data transmission capabilities grew as the use of the internet increased. This demand was met by enhancements for GSM called General Packet Radio Service (GPRS) and later with Enhanced Data Rates for GSM Evolution (EDGE) which was slightly faster. There are four frequency bands allocated for GSM, GPRS and EDGE devices, 850 MHz, 900 MHz, 1800 MHz and 1900 MHz. The available frequencies differ by country. In South Africa, only the 900 MHz and 1800 MHz bands are available for the public market [9].

When 3G cellular networks emerged, there were many competing 3G technologies, the two main being UMTS and CDMA2000, each with their extensions [10]. These technolo-

gies are not compatible and since there is no global agreement on a common 3G technology, some mobile devices may not have access to 3G in specific countries. Nonetheless, 3G introduced faster data transmission speeds than the 2G technologies. South African cellular networks use UMTS in the 900 and 2100 frequency bands.

Service Provider	700/800	900	1800	2100	2300	2600
Vodacom		22 MHz	24 MHz	35 MHz		
MTN		22 MHz	24 MHz	40 MHz		
Cell C		22 MHz	24 MHz	30 MHz		
Telkom			24 MHz	30 MHz	60 MHz	
Rain			34 MHz			20 MHz
Liquid	10 MHz		24 MHz			
TOTAL	10 MHz	66 MHz	154 MHz	136 MHz	60 MHz	20 MHz

Table 2.1: South Africa’s cellular network spectrum allocations for service providers [9][11]

The 4G technology, also known as Long Term Evolution (LTE) had higher data transmission speeds, shorter latency¹ and better energy efficiency than the previous generations [10]. Unlike with 3G technology, LTE barely has any competition making it the forerunner of 4G technologies. In South Africa, 4G operates in the 2100 MHz, 2300 MHz and 2600 MHz spectrums. The fixed spectrum assignment to several South African service providers over the 2G-4G spectrum is shown in Table 2.1.

In South Africa, as well as many other regions of the world, the latest 5G technology is still a relatively new network. The transition to 5G necessitates a lot of infrastructure upgrades to help amplify the high-frequency signal over long distances and barriers. The prediction of growth in the number of 5G users and the cellular network market share in 2025 can be found in [12], however, it is excluded from this project due to insufficient usage of 5G at the time of writing. To further narrow the target frequencies, this project will concentrate on the 900 MHz, 1800 MHz, and 2100 MHz frequency bands, which are used by at least two service providers and are the most occupied.

2.1.1.2 Data transmission

The evolution of cellular networks has an emphasis on the improvement of data speeds. However, this would not be possible if the data transmission methods did not change from circuit switching data to packet-oriented data transmission techniques. Circuit switching data transfer in the telephone context is when caller A calls caller Z, but the only way for the communication to be established is if a switch is turned to connect the users [10]. This switch then serves as a dedicated data transmission path between the callers until the call is terminated. Alternatively, packet-oriented data transmission divides the data into smaller data packets and transfers each packet using the most optimal route determined by a transfer algorithm.

¹The amount of time it takes for a data packet to travel from point A, to point B. The user experience is improved as the network latency is reduced.

Data is transferred in frames, which are made up of sequences of smaller frames and sub-frames. In 2G technologies, Time Division Multiple Access (TDMA) is used to allow multiple user data to be transmitted in the same frequency band, but with the data divided into periodic timeslots. A single TDMA frame has 8 timeslots separated by 577 s, as shown in Figure 2.1 [13]. The data sent within the timeslots are known as transmission bursts. Each timeslot data structure has a guard period (GP), which is a period of time when no data is sent as a means of safeguarding between adjacent bits of different timeslots. Furthermore, the frame contents will vary depending on the type of data sent.

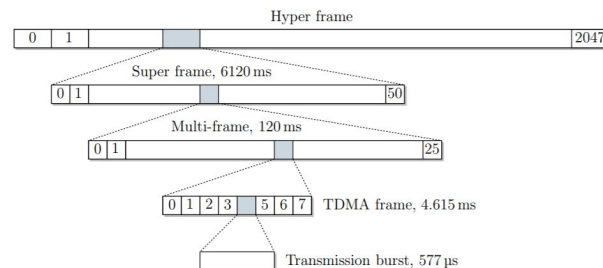


Figure 2.1: GSM/GPRS/EDGE data transmission frame [13]

The transmission frames for UMTS and LTE networks are shown in Figure 2.2a and 2.2b, respectively. The UMTS frame is broken into 666.7 s time slots [14], similar to 2G, with a GP at the conclusion of each.

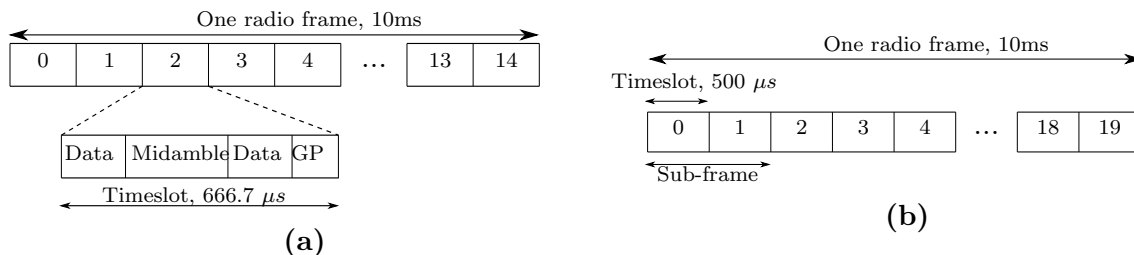


Figure 2.2: Model of (a) UMTS data [14] and (b) LTE Type 1 [15] transmission frame for 3G and 4G technology

In LTE technology, there are two types of transmissions: Type 1 and Type 2. Type 1 transmits the uplink and downlink data packets on different frequency bands, but Type 2 transmits both uplink and downlink data on the same frequency. Nonetheless, both versions use 10ms data frames that are further broken into 0.5 ms timeslots [15]. Each transmission burst is also safeguarded by GPs.

2.1.2 Wi-Fi

Wi-Fi, formally known as IEEE802.11, is a wireless networking system that supports the transmission of data over the internet as well as communication between linked devices. There are various variations of Wi-Fi standards and with each new development comes improved transmission speeds and the enablement of more devices to be connected simultaneously.

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year released	1999	1999	2003	2009	2014	2019
Frequency	5GHz	2.4GHz	2.4GHz	2.4GHz & 5GHz	2.4GHz & 5GHz	2.4GHz & 5GHz
Data Rate (max)	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	1.-12Gbps

Table 2.2: Brief summary on the development of Wi-Fi standards [16]

2.1.2.1 Background

The first Wi-Fi standard was IEEE802.11a, which was followed by IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ac and IEEE802.11ax respectively [16], see Table 2.2. These standards operate in either the 2.4 GHz bandwidth, 5 GHz bandwidth or both. The frequency band is divided into channels of communication, the 2.4 GHz band has 14 channels of which 3 overlap. Furthermore, the 5 GHz band has 40 channels only with 1 overlapping. The most common modulation scheme is the OFDM scheme which spreads data from a single transmission across various channels and transfers it in parallel instead of sequentially [17]. The modulation process of Wi-Fi signals is very intricate. As newer standards are developed it is important to ensure compatibility with older standards. This is achieved by having combinations and dynamic modulation schemes.

2.1.2.2 Data transmission

The transmission of Wi-Fi data occurs in streams of data packets. The OSI model can be used to represent the transmission of Wi-Fi data between devices. The OSI model is a seven-layer framework that depicts how data is encapsulated and transported from one device to another in a network [16]. WiFi only operates with the last two layers, namely the data link and physical (PHY) layer. The data-link layer is kept the same to support backward compatibility with previous Wi-Fi standards. The PHY layer is the bigger focus because it describes the format of data as it moves through space. The physical layer is made up of data packets whose length and exact format varies depending on the standard. When packets are either too large according to the fragmentation threshold or there is too much potential data loss for a single frame, they can be fragmented into smaller ones [17].

2.1.3 Bluetooth

Bluetooth is a wireless technology designed to transfer data between personal devices within a relatively small vicinity, creating what is formally referred to as a Wireless Personal Area Network (WPAN).

2.1.3.1 Background

The first version, Bluetooth v1, was released in 1999 and it had a data rate of 700 kbps, named the Basic Rate (BR). This version was standardized according to the IEEE802.15 standard, but all versions from v2 were managed and approved by the developing company, Bluetooth Special Interest (SIG) instead. Bluetooth v2 and v3 were released with faster data rates of 3 Mbps and 24 Mbps deemed as the Enhanced data rate (EDR)

and High Speed (HS) respectively [18]. The advancements made with these first three versions were mainly focused on increasing throughput and are altogether classified as Classic Bluetooth or Bluetooth BR/EDR.

The release of Bluetooth v4 in 2009 introduced a Low-Energy feature that was designed to use significantly less power than the previous versions. This addition to Bluetooth technology was too extensive to be regarded as Classic Bluetooth, but rather Bluetooth Low Energy (BLE). The introduction of BLE does not eliminate the need for the Classic Bluetooth, because the two technologies have different modulation schemes meaning that BLE devices are not compatible with Classic Bluetooth devices. Classic Bluetooth is found in devices such as wireless headsets, speakers, printers and keyboards. BLE devices have smaller batteries, for example, fitness tracker watches, beacon services and blood pressure monitors. The low power consumption of BLE is possible because it sets devices to sleep when they are not transferring data so that the battery can last for a long time. In some cases, such as on smartphones, there is a dual option accepting both types of Bluetooth connections.

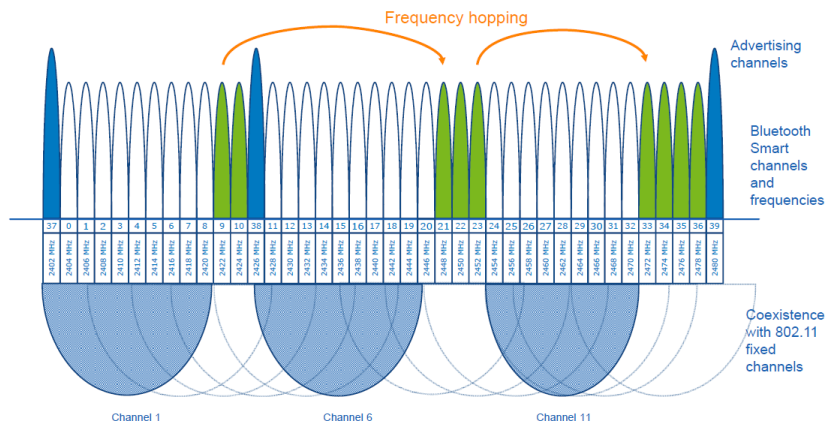


Figure 2.3: 2.4 -2.480 GHz of ISM band shared by Bluetooth, BLE, Wi-Fi communications [19]

Bluetooth operates in the industrial, scientific and medical (ISM) band from 2.4 -2.480 GHz. This bandwidth experiences a lot of interference because it is a global license-free bandwidth. There are many other types of signals transmitted in the ISM band, such as Wi-Fi. Bluetooth SIG implemented a Frequency Hopping Spread Spectrum (FHSS) technique which fragments the bandwidth spectrum into smaller frequency channels [20]. This enables data to be transmitted at varying frequencies within 2.4-2.480 GHz by hopping to uninterrupted “free” channels.

2.1.3.2 Data transmission

Bluetooth data is divided into small packets and then transferred to the WPAN. The type of Bluetooth technology determines the number of frequency channels, transmission protocol, and data packet format. The frequency spectrum of Classic Bluetooth technology is divided into 79 channels, which are 1 MHz apart. The data packets follow a random frequency hopping pattern to a different frequency channel according to the GFSK modulation scheme. Classic Bluetooth operates at $625 \mu s$ in the time domain, as illustrated

in Figure 2.4

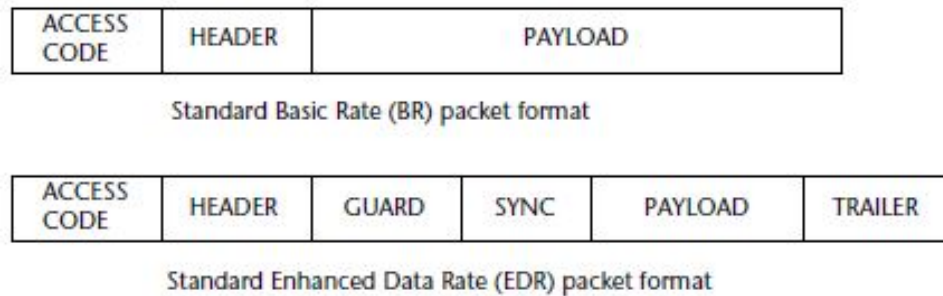


Figure 2.4: Classic Bluetooth data packets [21]

The BLE frequency spectrum is divided into 40 channels, each with a bandwidth of 2 MHz. Three of the channels are dedicated advertising channels for when devices are looking for new BLE connections. These channels are very important for identifying and establishing new connections. For this reason, they are spaced apart to avoid the 3 Wi-Fi channels. The remaining 37 channels are for transferring the actual data. Unlike Classic Bluetooth, the data packet form for all BLE devices is the same; the packets only varied in transmittable bit lengths.

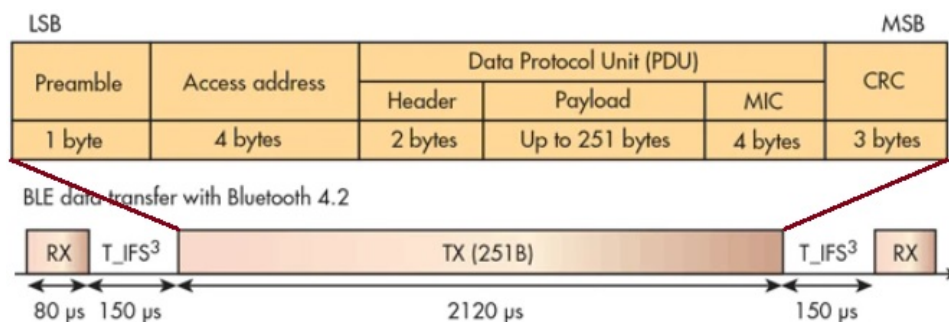


Figure 2.5: Bluetooth Low-Energy data packets [22]

The general format of BLE packets is shown in Figure 2.5. Data packets are delivered and received several times during a connection, with a 150 μ s delay between each successive packet. This creates a burst-like pattern in the time domain with some bursts longer than others depending on the data they carry. The minimum transferred bits in a packet for the data rate of the specific Bluetooth technology can be used to compute the shortest possible information burst.

$$t_{\text{Burs}} = (8 * \sum \text{Bytes}) / \text{DataRate} \quad (2.1)$$

Bluetooth v4.0 is capable of transmitting a single bit every 1us, therefore the bitrate is 1 Mbps.

2.2 Electromagnetic Compatibility

Electromagnetic compatibility (EMC) concepts are applied in multiple aspects of the development of the RFI power detector and its circuit board. EMC refers to an electronic system that can sustain its intended functionality in the midst of changing electromagnetic energy. This includes internal fields produced by the components of the system as well as the external fields. Essentially, EMC is the absence of EMI. In the case of an EMC issue, which will be referred to as interference for the remainder of this section, there are three elements involved that need to be identified namely the noise source, coupling path and the victim as displayed in Figure 2.6.

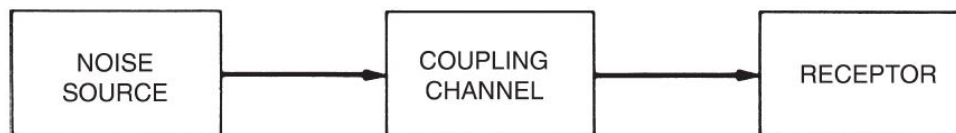


Figure 2.6: Diagram illustrating the three elements involved in generating interference in a system: Noise Source, Path, Victim [23]

Applying good EMC principles during the planning stages of a project can result in huge cost savings and even save lives. This makes the understanding of EMC concepts essential in the testing of electronics, by aiding in finding the root cause of any unanticipated emissions. EMC is the protection of the signals of a system, therefore maintains signal integrity of a system. Dr Hubing discusses in [23] a few EMC principles to take into consideration when designing a circuit board or fault finding on an existing board. The principles include identifying prospective sources and victims, determining current flow, identifying potential unintentional antennas, and analyzing potential coupling mechanisms, which are all discussed in more detail below. In addition, EMC shielding is discussed as a means of preventing interference from occurring between the source and the victim.

2.2.1 Source and victim

EMC problems are resolved by either eliminating or reducing the effect of the source or coupling mechanism on the victim. It is generally easier to identify the source and the victim than the coupling path. It would be ideal if the noise source can be located and removed, or more distance be put between the victim and source. However, this is not always possible or practical in a system.

Different types of signals found in electronics can cause varying degrees of interference in a system. High-speed components on digital circuits, such as clock signals are some of the most common sources that emit high frequencies. In addition, these narrowband frequencies have harmonics that must also be considered. Non-periodic digital signals, on the other hand, are less troublesome because the interference generated is more broadband meaning that they do not radiate as well as the narrowband frequencies. Lastly, analogue signals can be either narrowband or broadband and special care should be taken to understand what different analogue signals are expected to look like in both time and frequency domains. Analogue signals can be very sensitive to low levels of interference and the only way to ensure signal integrity is to eliminate the noise source [23].

2.2.2 Current flow

In circuit design, engineers often neglect the path on which the current is most likely to flow. In order to identify the most critical current paths, the first thing to remember is the foundational fact that current flows in a loop. In other words, all current leaving a component needs a path to return. Circuit board designers should avoid having more than one potential return path because that leads to uncertainty.

Furthermore, if the current has more than one possible return path it will always flow in the path of least impedance. The path of least impedance is dictated by the resistance for very low frequency (kHz and lower) applications. Furthermore, as the frequency changes and increases, the path of least resistance for the same system may vary.

2.2.3 Unintentional antennas

When electronics that are not intended to transmit or receive electromagnetic fields begin to do so, this is referred to as an unintentional antenna. To avoid or identify this, the proper design precautions should be taken into account.

Unintentional antennas occur on a board when there are two parts of a conductor that have a voltage difference between them. Almost any conductor of any length can radiate, though not always effectively. Furthermore, conductors that are at least a quarter wavelength of the signal or a multiple thereof will radiate or receive electromagnetic energy more effectively. Because the higher the frequency, the shorter the wavelengths, and the more likely it is that even a transmission line might be a possible radiator, it is best practice to utilize matched transmission lines or design them to be shorter than $\lambda/4$.

2.2.4 Coupling mechanisms

Coupling is shown in Figure 2.6 as the path by which energy is transferred from the noise source to the victim, and thereby causing interference. The four coupling mechanisms that can occur in an electronic system are conductive, capacitive, inductive and radiated coupling [24]. These coupling mechanisms can occur individually or simultaneously, making it more complicated to identify.

Conductive coupling occurs when energy is transferred between a source and victim circuit that share a common current path, such as a transmission line, stripline or cable. To resolve this issue, the noise must be filtered out of the conductor or the common current paths of the source and victim circuits should be separated. A common example of this is power lines coming from DC-DC converters can sometimes be carrying switching noise from the converter [25].

A varying current in a conductor generates an electric field, making it a potential source of interference. **Capacitive coupling** refers to when such a conductor's electric field couples onto a parallel victim conductor within the near-field region. The potential difference between the source and victim conductor creates the effect of a capacitor. Therefore, the induced current, I_{victim} can be calculated using the sources' voltage, v_{source} , as follows:

$$I_{\text{victim}} = C \frac{dv_{\text{source}}}{dt} \quad (2.2)$$

The magnitude of the equivalent capacitance, C in equation 2.2, changes with the distance between the source and victim or with the presence of electric screening material. Capacitive coupling is also referred to as electric coupling, because it is based on the induction through electric fields, as shown in Figure 2.7a [24].

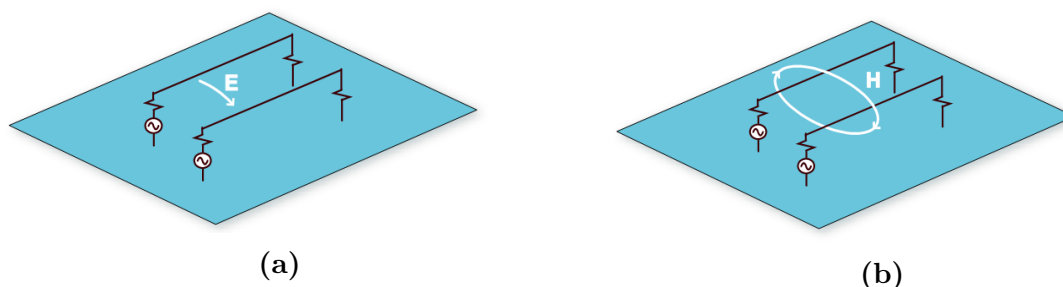


Figure 2.7: Illustration of (a) electric fields coupling onto adjacent conductor through capacitive coupling and (b) magnetic fields coupling onto adjacent conductor through inductive coupling [23]

Inductive coupling, on the other hand, is based on magnetic induction in the near-field. When alternating current flows through a conductor, it creates a time-varying magnetic field. Mutual inductance, M in equation 2.3, occurs when a magnetic field cuts an adjacent conductor and inducing a voltage in it, as shown in Figure 2.7b. In the context of inductive coupling, it is the source's magnetic field inducing the voltage in the victim. The induced voltage, V_{victim} can be calculated from the source's current, i_{source} , as:

$$V_{\text{victim}} = -M \frac{di_{\text{source}}}{dt} \quad (2.3)$$

According to Faraday's Law, the induced voltage in the victim loop is proportional to the rate of change of the magnetic flux. This field loses its intensity as you move further away from the conductor. Therefore, increasing the space between the source and the victim can eliminate this coupling problem, because the magnetic fields spread out and are much weaker at a further distance [24].

The last coupling mechanism is **radiative coupling**. This refers to far-field coupling of an electromagnetic field over a medium such as air between a source and a victim acting as antennas. The degree of the coupling depends on how effective the source and victim are at radiating and receiving at the coupling frequency.

2.2.5 EMC shielding

One of the most widely used techniques in the design of electronic devices to prevent coupling between a source and victim is shielding. Shielding is a method of creating a barrier between electronics and the surrounding environment to prevent electromagnetic signals from travelling between the spaces. This is necessary to protect sensitive devices and signals from interference. There is more consideration in designing an enclosure beyond the common mistake of simply placing electronics in a box enclosure and assuming it is shielded.

Electromagnetic waves are made of an electric wave perpendicular to a magnetic component that propagates through space at the same frequency. The purpose of a shield is to divert the propagation of at least one of these components for an electromagnetic wave coming from inside or outside the shield enclosure. An electromagnetic wave cannot exist without one of the two wave components. The propagation of the electric components is blocked by a conductive material, and the magnetic components are blocked by material with high magnetic permeability. The shielding barrier attenuates by either reflecting or absorbing the electric or magnetic waves [25] [24].

2.3 Description of RF receiver fundamentals

This section introduces the key ideas that must be understood before designing the RF receiver in this thesis. A RF receiver is required to capture the signals of interests in the RFIPD. The goal of the RF receiver design is to collect the incoming signal with as much power as feasible while producing as little noise as possible. The scattering parameters are introduced first, then signal mixing, noise performance theory, and finally analogue to digital conversion. These fundamental concepts are applied to the design and evaluation stages of an RF receiver.

2.3.1 Scattering parameters

Scattering parameters (s-parameters) are a well-known circuit analysis technique in high-frequency circuits. This method can be used to describe an electrical network and its response to input signals. It can describe the behavior of RF receivers varying number of ports by examining the signals at each input or output network port. It treats any network as a *black box* which can represent any device, or system, which is illustrated as a n-port network in Figure 2.8.

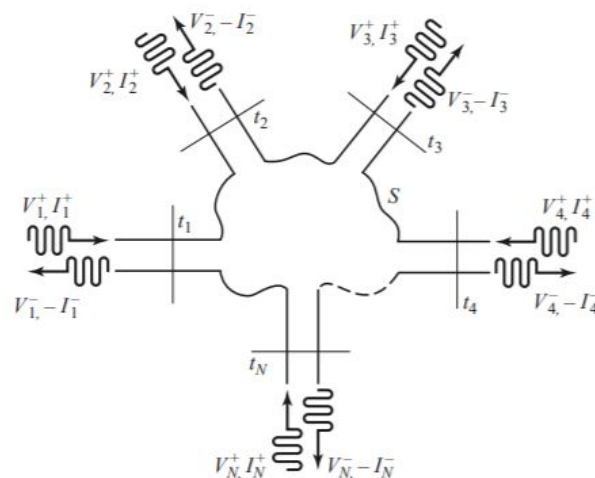


Figure 2.8: Diagram of an n-port *black box* network [26]

The terminal ports(t_1, t_2, \dots, t_n) are defined by the corresponding incident voltage (V_n^+) and current (I_n^+) waves as well as the reflected voltage(V_n^-) and current (I_n^-) waves.

The relationship between V_n^+ and V_n^- at any terminal is used to define the $[S]$ matrix as follows [26]:

$$\begin{bmatrix} V_1^- \\ V_2^- \\ \vdots \\ V_n^- \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} & \cdots & S_{1n} \\ S_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ S_{n1} & \cdots & \cdots & S_{nn} \end{bmatrix} \begin{bmatrix} V_1^+ \\ V_2^+ \\ \vdots \\ V_n^+ \end{bmatrix} \quad (2.4)$$

or simplified to

$$[V^-] = [S] [V^+] \quad (2.5)$$

Each S-parameter in the $[S]$ matrix is defined as

$$S_{xy} = \left. \frac{V_x^-}{V_y^+} \right|_{V_{y^+ \text{ for } \dots}} \quad (2.6)$$

Equation 2.6 indicates that there is an incident wave, V_y^+ , entering port y and the reflected wave V_x^- is being measured at port x . All other ports are terminated with matching loads. S_{xy} is known as the transmission coefficient because it indicates how well the incident wave is transmitted to port x . Furthermore, the S-parameters can also show how much of the incident wave is reflected at the same port. This is known as the reflection coefficient, denoted as S_{xx} [26]. The $[S]$ matrix can be converted into other matrix parameters such as the impedance and admittance matrices as needed.

Two-port networks are the most common devices which one may come across. These include attenuators, amplifiers, filters. In the case of a two-port network the S-parameters are S_{11}, S_{12}, S_{21} and S_{22} . As explained above, S_{11} and S_{22} are known as the reflection coefficients, denoted Γ [27]. Theoretically, $\Gamma = -\infty$ would be ideal, however, this is not practical. There is bound to be some degree of mismatching, this is known as the return loss (RL),

$$RL = -20 \log |\Gamma| \quad (2.7)$$

The return loss is used in a similar manner with Γ to describe the total losses affecting the reflection coefficient. As the degree of reflection decreases, the S_{11} will be observed to be more negative. Furthermore, the Γ is also used to determine a term known as the voltage standing wave ratio (VSWR), according to equation 2.8 [26]. VSWR is an indication of how well the port is matched to the transmission line and load. Standing waves in transmission lines can occur when there is a lot of reflection. This can produce resonance on a transmission line, causing the line to radiate. The VSWR is commonly used to define how much of the voltage on a transmission line is a standing wave. The smaller the VSWR, the better the matching of the port.

$$VSWR = \frac{1 + |\Gamma|}{1 - |\Gamma|} \quad (2.8)$$

Lastly, S_{12} and S_{21} are the transmission coefficients. Depending on whether the device under test (DUT) is an active or passive network, the transmission coefficient could be used to obtain either gain (G) or insertion loss (IL) [27]. Active devices have an external source that contributes some energy to the incoming signal, therefore the output power may surpass the incident power. In this case, the transmission coefficients are used to obtain the gain in dB. Alternatively, passive devices do not have a source, meaning that these devices have a gain of either less than or equal to unity. This is referred to as IL

because energy is lost between the incident and output ports. Insertion loss is written as a positive value, that indicates how much power was lost, therefore IL should ideally be $0dB$ in a system [26].

2.3.2 Mixing signals

Signals are mixed in an RF receiver to translate an incoming signal to a different frequency using a mixer. Many receiver designs use a mixer, and choosing the parameters of a mixer in a receiver design is critical to achieving the intended result. As a result, the concept of mixing signals is investigated to comprehend how various parameters affect the mixed signal. A mixer is a three-port network with two inputs and a single output. A mixer can be used to either mix-up (up-conversion) or mix-down (down-conversion) an incident signal, as shown in Figure 2.9. In both cases, the incoming signal is mixed with a regulated local oscillator signal (f_{LO}) which ultimately determines whether the incident signal is mixed up or down.

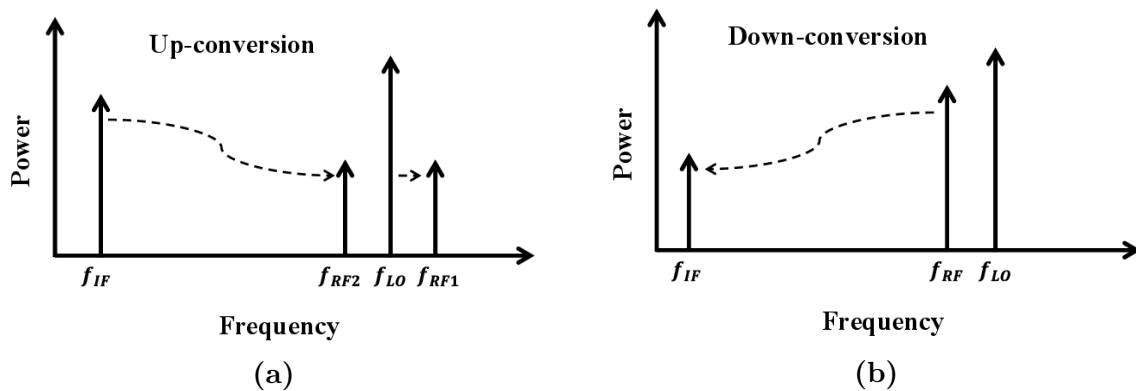


Figure 2.9: Illustration of the result produced through mixing two signals to achieve (a) up-conversion and (b) down-conversion [28]

Up-conversion occurs when a signal with an intermediate frequency (f_{IF}) lower than (f_{LO}) are mixed, to produce a RF signal (f_{RF}) at a higher frequency, represented as:

$$f_{RF} = f_{LO} \pm f_{IF} \quad (2.9)$$

On the other down-conversion occurs when an RF signal (f_{RF}) is mixed is mixed with a higher (f_{LO}) resulting in a signal with an intermediate frequency (f_{IF}). Down-conversion is written as [29],

$$f_{IF} = f_{LO} \pm f_{RF} \quad (2.10)$$

Signal mixing is fundamentally a time domain multiplication and a frequency domain convolution. From frequency multiplication fundamentals, there are two results produced as shown in Fig. 2.9. Additionally, there is another frequency that can result in the same f_{IF} [29]. This is known as the image frequency and must be filtered out.

2.3.3 Noise performance

When designing a RF receiver, noise is an element that is always found in the received signal. The amount of noise passed through the receiver should be kept to a minimum to achieve high sensitivity. Overlooking noise performance and sensitivity can degrade the system significantly. Evaluating sensitivity and noise performance is extremely important in designing a receiver. Fortunately, there are numerous properties that can be used to characterize various types of noise on the system. These include SNR, Noise figure, noise floor, and a variety of others.

In the receiver system, the noise power spectral density is a combination of noise received from the environment via the antenna and noise generated within the receiver. The environmental noise is typically the stronger interference and depends on temperature, frequency, the environment and the antenna properties. Furthermore, techniques such as shielding discussed in Section 2.2.5 are effective in attenuating this noise. The noise generated within the receiver, on the other hand, depends on the physical temperature of the receiver, the bandwidth and thermal noise generated in the parts of the receiver. This relationship between these factors is shown in the noise power, eq 2.11.

$$P_{Noise} = kTB \quad (2.11)$$

where

- k - Boltzman constant
- T - Temperature (Kelvin)
- B - Bandwidth

The amount of noise power ultimately added to the desired received signal is this noise power spectral density (noise floor) multiplied by the receiver bandwidth. The greater the bandwidth, the more noise can be picked up from the wider ranges.

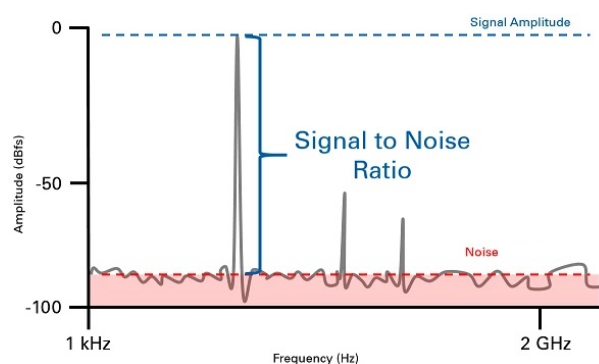


Figure 2.10: Illustration of SNR in a signal with noise [31]

The noise floor describes the strength of the noise floor and is therefore used to determine the Signal-to-noise ratio (SNR or S/N ratio). The SNR is a measure of how strong the desired signal is to the noise floor [30], shown in Figure 2.10. It is often used as an indicator of the sensitivity of a receiver. The smaller the SNR of a signal, the more difficult it is to distinguish the signal from the noise floor. The signal needs to surpass a

set threshold to be detected.

Furthermore, noise factor, denoted F in eq. 2.12 is the ratio of the input SNR to its output SNR indicating the level of noise introduced by a single component or chain of components. A lower noise factor value indicates that the input has a lower S/N ratio and an improved larger output S/N ratio. Noise factor has a wider range of applications, making it more relevant than S/N ratio measurements. Noise figure (NF) is the logarithmic scale conversion of the noise factor, mathematically expressed as

$$NF = 10\log_{10}F \quad (2.12)$$

including the noise factor, it becomes

$$NF = 10\log_{10}\left(\frac{S_{input}/N_{input}}{S_{output}/N_{output}}\right) \quad (2.13)$$

Noise generated within the receiver is typically dominated by the LNA, if it has high gain and low NF.

2.4 Analogue to Digital Conversion

Analogue signals, such as audio and temperature have a continuous range of values. Analogue signals cannot be directly conveyed through computers without some processing, because computers only operate with digital signals. Digital signals have a discrete range of values. The conversion of an analogue signal into a digital signal is a crucial step in any digital signal processing system. This creates a digital signal replica/model of the original analogue signal to allow digital computation. For this thesis, analogue to digital conversion acts as the bridge between the RF receiver signals and the signal processing signals. The precision of this conversion is determined mainly by the resolution and sampling rate of the converter with respect to the bandwidth of the measured signal. These are the two factors to consider when selecting an ADC. These factors are discussed in detail below.

2.4.1 Quantisation

Quantisation is the process of converting a continuous-amplitude analogue signal into a discrete-amplitude signal. This produces a finite number of values across the amplitude range, known as quantisation levels, see the horizontal progressions in Figure 2.11. The fundamental idea of this process is that continuous analogue values between 0 and V_{ref} are approximated to the next or previous closest quantisation level [32]. Therefore, the more quantisation levels, the smaller the step size from one quantisation level to the next quantisation level. Resolution bits is a way of defining the step size of ADCs. Figure 2.11 shows how different resolution bits affect the number of quantisation levels and step size and essentially how accurately the original signal is replicated.

The relationship between resolution, step size and quantisation level is expressed in equation 2.14 [32] as,

$$s = \frac{A}{N} \quad (2.14)$$

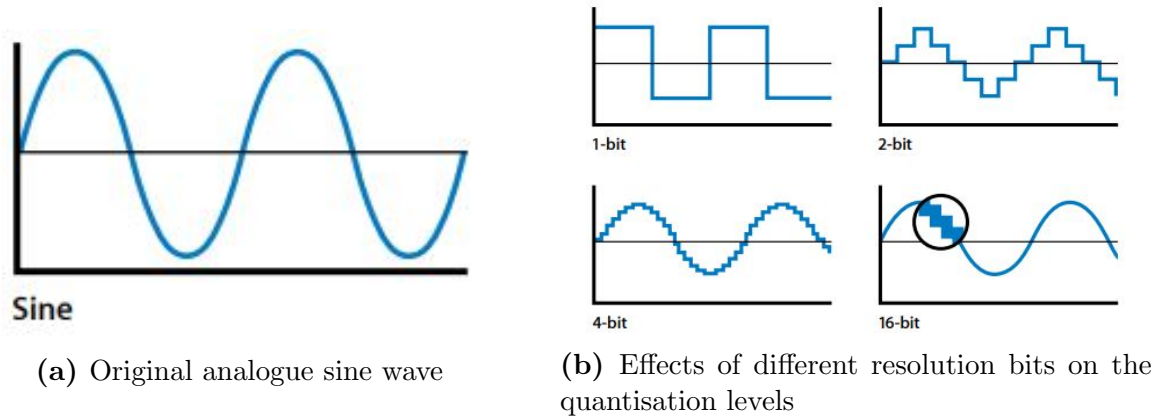


Figure 2.11: Difference between 1-bit, 2-bit, 4-bit and 16-bit resolutions [33]

$$s = \frac{A}{2^r} \quad (2.15)$$

where

- s = step size
- r = resolution bits
- N = number of quantisation levels
- A = Amplitude of V_{ref}

Equation 2.14 shows that the higher the resolution bits, the smaller the step sizes of each quantisation level. Generally, ADC's capable of higher resolution bits tend to be more expensive. One can spend less by using the minimum resolution required for the application. The minimum resolution describes the maximum quantisation error acceptable without compromising the integrity of the signal too much. The quantisation error is a measure of the amount of information lost, mathematically expressed as [34],

$$e(n) = x_Q(n) - x(n) \quad (2.16)$$

where

- $e(n)$ = quantisation error
- $x_Q(n)$ = quantized signal
- $x(n)$ = incoming signal

According to equation 2.16 having a very high-resolution ADC may seem ideal, but it is partnered with a higher financial cost, a need for higher computational speed and a need for bigger storage for more samples. The trade-off between all these aforementioned factors is also affected by the desired sampling rate.

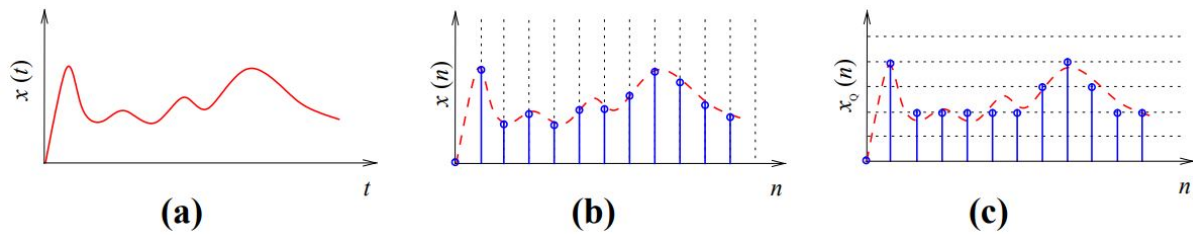


Figure 2.12: Sampling and quantisation of a continuous-time, continuous-range signal [34]

2.4.2 Sampling

Sampling refers to the periodic recording of instantaneous values of the incoming analogue signal to create a discrete-time range for the digital signal. Figure 2.12 shows how the combination of quantization and sampling, complete the digitization process of a signal.

Furthermore, figure 2.12 shows that the sampled signal is equivalent to the product of the incoming continuous signal, $x(t)$, and a train of impulses. If a dirac impulse train with a sampling period T is defined as,

$$w(t) = \sum_{n=-\infty}^{\infty} \delta(t - nT_s) \quad (2.17)$$

, then the sampled signal can be expressed as

$$\begin{aligned} x_\delta(t) &= x(t) \cdot w(t) \\ &= x(t) \cdot \sum_{n=-\infty}^{\infty} \delta(t - nT_s). \end{aligned} \quad (2.18)$$

To map $x(t)$ to the sequence of discrete samples, $x(n)$, let $t = nT$, such that

$$x_\delta(n) = \sum_{n=-\infty}^{\infty} x(nT) \cdot \delta(t - nT_s). \quad (2.19)$$

From the fundamentals of Fourier transform [35], the frequency domain equivalent is obtained from convoluting the incoming signal $X(\omega)$ with a impulse train at sampling rate of ω_s , as given by equation (2.20).

$$\begin{aligned} X_\delta(\omega) &= X(\omega) \otimes W(\omega - n\omega_s) \\ &= \frac{1}{T} \sum_{n=-\infty}^{\infty} X(\omega - n\omega_s) \end{aligned} \quad (2.20)$$

In both domains it is evident that an appropriate sampling rate is required in order to re-create the signal without losing the integrity of the incoming signal. Figure 2.13 shows the effects of using impulse trains at different sampling rates, measured in samples per second (SPS) or Hz.

The selected sampling rate will result in one of the following conditions:

Under sampling: When $\omega_s > 2\omega$, the signal overlaps leading to aliasing, where the signal cannot be reproduced due to the information being corrupted- Figure 2.13a

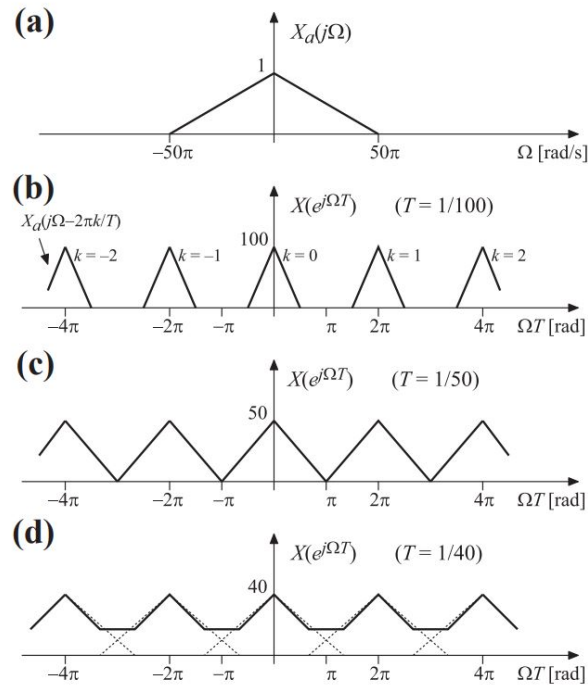


Figure 2.13: Effects of sampling at different frequencies [34]

Perfect sampling: When $\omega_s = 2\omega$, the signal can be reproduced fully- Figure 2.13b

Over sampling: When $\omega_s < 2\omega$, the incoming signal can be reproduced fully with all the information- Figure 2.13c

In order to capture all the information of a signal without aliasing, the sampling frequency has to be at least double the frequency of the highest frequency component contained within the signal. This condition is known as the Nyquist criterion.

2.5 Processing Options

Technology would not have reached all the advances if it were not for the ever-growing microelectronic and microprocessing systems. Complicated signal processing manipulation of a signal can now be achieved on very powerful microprocessor. The following is a brief description of the various processing technologies that could be used for the signal processing system in this project:

General purpose microcontroller/microprocessor

Microcontrollers are generally easy to implement code on, but are not specialized for complicated mathematical computations. Also, the programs are run sequentially and one is limited to the pre-designed hardware layout. This decreases power efficiency.

DSP

DSP's are specifically designed for executing math computations, but not so much for computational processing.

Field programmable gate array(FPGA)

FPGAs can implement fully parallel algorithms due their extreme design flexibility. They need firmware and software coding which make them rather complex to work with. These boards can be designed to have the shortest distances between components on the board

as well as having dedicated hardware. This is power efficient in the sense that no unnecessary.

Application-specific integrated circuit (ASIC)

ASICs are processing boards designed for a specific application which makes it more power efficient because of the minimum number of components. This is not ideal for prototyping versions because the hardware design is fixed. A mistake made using an ASIC can be a very costly mistake.

GPU

GPU's have very high computing capabilities commonly used for applications such as real-time computer graphics.

The device to be selected has to have a low power consumption rating, because power is limited in the case that the platform with which the receiver is used is a UAV. The more the power used, the shorter the flight time. Given the relatively low processing requirements, budget and components availability a microprocessor approach is chosen.

2.6 Conclusion

This chapter provided background knowledge on characterisation of the RFI signals of concern. The findings here are used in Chapter 3 to define requirements for the RF front-end. Thereafter electromagnetic compatibility, EMC shielding as well as RF receiver fundamentals were discussed. In Chapter 3 these RF fundamentals will be further elaborated upon to describe the full RF front-end design of the system. This chapter concludes with a study of how signals are converted from an analogue state to a digital, as well as a comparison between different signal processing technologies.

Chapter 3

RF Receiver Front-end

The radio receiver is the entry point of a signal into the RFIPD. This makes the design of this part one of the most important because any issues developed in this phase will be passed onto the succeeding parts of the RFIPD system. This chapter explores the benefits and drawbacks of different receivers, followed by a detailed description of the selected receiver design methodology, and concludes with an analysis of the built receiver performance.

3.1 Receiver Architectures

Before building an RF receiver, there are three basic architectures to consider: tuned radio frequency (TRF), super-heterodyne architecture, and direct conversion architecture. The fundamentals of these architectures serve as the foundation for many sub-architectures. These are fine-tuned to meet the needs of the application. Combining more than one of these architectures and using a switch to toggle between two or more receiver architectures has become more common on receiver designs to offer versatility in the application.

Tuned radio frequency

Tuned radio frequency radio receivers were one of the earliest receiver configurations to be developed. Figure 3.1 shows that it was primarily composed of a sequence of tunable filters and amplification, followed by demodulation.

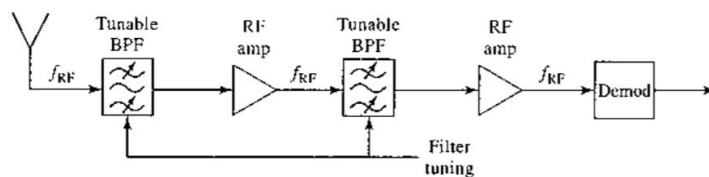


Figure 3.1: Tuned radio frequency receiver [26]

Variable capacitors and inductors were often used for filtering, however, these filters have a wide passband and hence cannot achieve good selectivity. Alternatively, tunable passband amplifiers were used. Because all of the amplification takes place on the RF signal, the amount of amplification that can be done without generating oscillation is limited [36]. As a result, this is not an ideal receiver configuration for high RF signals.

Super-heterodyne

The super-heterodyne receiver is the most frequently implemented configuration across all RF receiver systems. In a typical signal chain, as shown in Figure 3.2, the incoming RF signal is first filtered by a pre-selection filter, after which it passes through a low-noise amplifier that enhances the chosen band while suppressing noise.

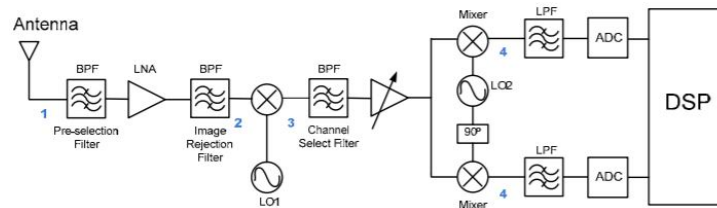


Figure 3.2: Super-heterodyne receiver [26]

The term “heterodyne” refers to the mixing of signals, which is achieved by the mixer and the local oscillator [26]. In the frequency domain, mixing the RF signal with the local oscillator signal produces a sum and difference of the signals in the output, as illustrated in Figure 2.9. Because the sum provides a higher frequency output than the original RF signal, the ADC sampling rate requirements (Section 2.4.2) are higher. For this reason, the lower frequency component of the output (i.e. the intermediate frequency (IF)) is low-pass filtered and amplified separately at a lower sampling rate. Some receivers are complete after this stage, known as a single conversion receiver. A dual-conversion system, on the other hand, is an extended receiver chain that includes a second phase of down-conversion to a lower IF that is closer to the baseband. An I/Q modulation method that separates the IF signal into its “in-phase” and “quadrature” components is sometimes used in the second mixing phase. These two sub-signals provide better amplitude/phase information to be sampled.

Direct-conversion

Direct-conversion configured receivers are very similar to the super-heterodyne receivers. Both architectures start by filtering and amplifying the incoming signal. The key difference between these two architectures is the amount of down-conversion done during the mixing phase. Unlike super-heterodyne mixers, the direct-conversion uses the LO to mix the incoming RF signal to baseband [36] as shown in Figure 3.3.

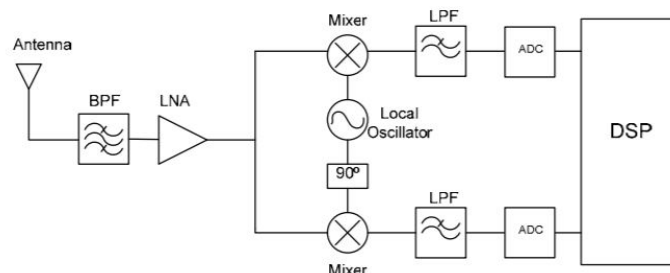


Figure 3.3: Direct-conversion / Zero IF receiver [26]

For this reason, this is also known as the Zero-IF receiver architecture. Unfortunately, the proximity to DC signals makes this architecture more susceptible to DC noise. Therefore, the accuracy of the LO is important to achieve a signal shifted to as close to

zero as possible. This is usually used in systems where the transmitting devices LO is known, for example, radar systems. The baseband signal is then filtered, followed by an ADC for sampling. This architecture uses fewer components than the super-heterodyne architecture.

3.2 Design of the Receiver Signal Chain

The core architectures, discussed above, are used to design the receiver front-end. The signal chain for the RFIPD_v00 is designed using the super-heterodyne and Zero-IF basic architectures as a foundation. The RFIPD_v00's RF front-end is designed to measure the frequency bandwidths mentioned in Table 3.1, based on the RFI sources' categorization in Section 2.1. Furthermore, after consultation with RFI staff from SARA0, the receiver was requested to detect atleast -75 dBm. For more sensitive measurements, the RTA is to be used.

Signal name	RFI Signal	f_{centre}	Frequency bandwidth
RF1	2G (uplink)	895.5 MHz	39 MHz
RF2	3G (uplink)	1747.5 MHz	75 MHz
RF3	4G (uplink)	1950 MHz	60 MHz
RF4	BLE and Wi-Fi	2450 MHz	100 MHz

Table 3.1: Centre frequencies and bandwidth of RFI signals of interest

Multiple design iterations were explored, as well as the advantages and disadvantages of each system of designs. Figures 3.4 and 3.5 show two of the designs that were under consideration, with the variables affecting each element's placement briefly described.

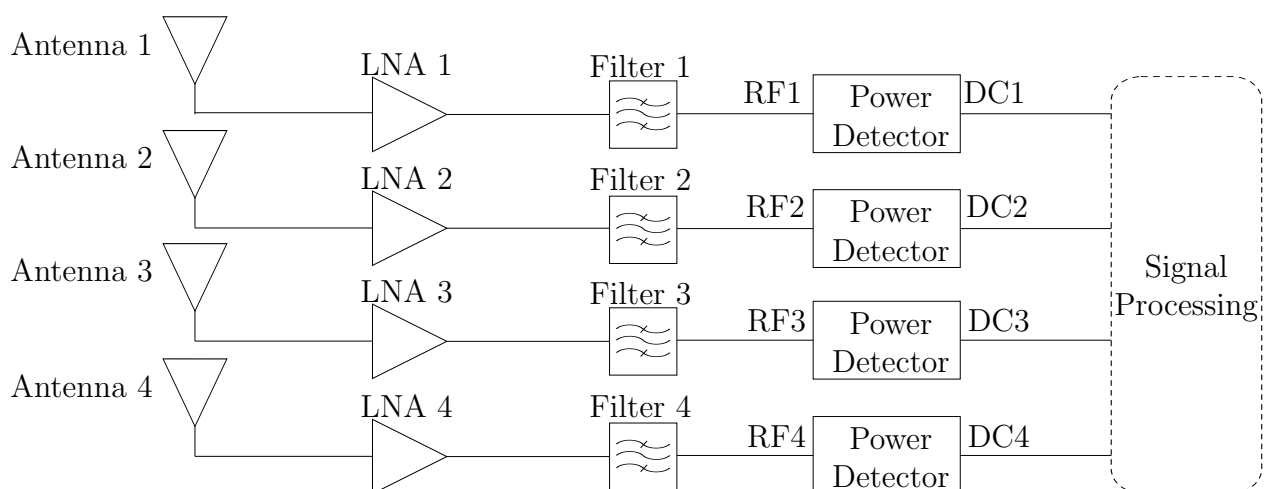


Figure 3.4: Signal chain design 1 considered for the RFIPD_v00 receiver

The RFI signals in Table 3.1 are popular frequency bands that have a wide range of antennas to choose from off the shelf. Therefore, four separate antennas can be used to capture each frequency band. This creates four transmission channels in the signal chain, as seen in Figure 3.5, with each channel employing components tuned to the specific bandwidth. Alternatively, a single wideband antenna with a bandwidth of 600MHz to 2600MHz can be utilized to catch all of the RFI frequencies. This means the signal chain has only one channel, but it can be split into four channels later in the signal chain to allow the signal processor to discern between the different frequencies, as shown in Figure 3.4. The reason for this is that a front-end with only one channel that is not separated into channels with narrower bandwidths necessitates significantly more processing to determine the detected signal's frequency band. Each design under consideration employs a narrowband filter that separates the signals RF1, RF2, RF3, and RF4 into independent channels. As a result, by the time the signal reaches the processor, the frequency band of the incoming signal is known.

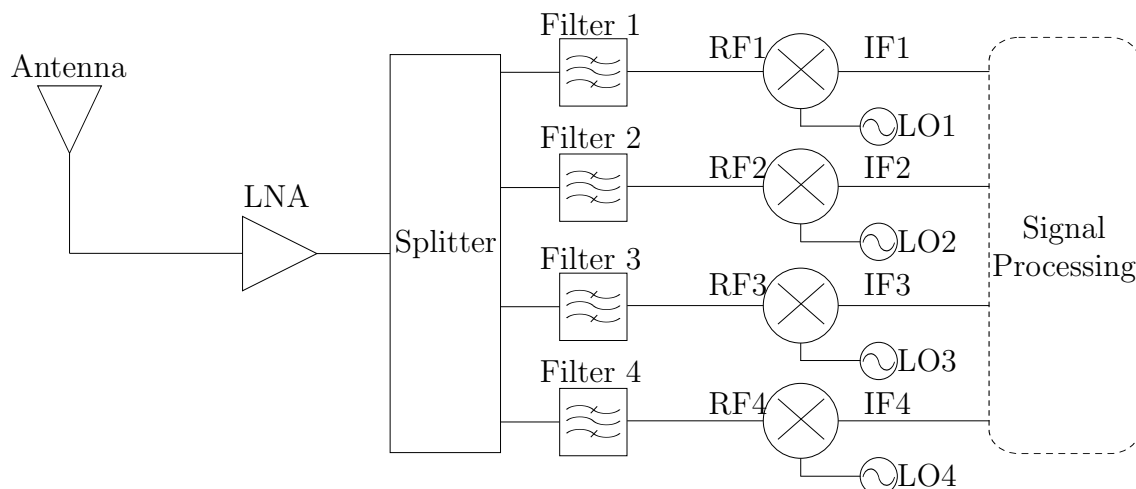


Figure 3.5: Signal chain design 2 considered for the RFIPD_v00 receiver

Furthermore, all possible designs contain an amplification stage to give the incoming signal gain. Each channel in Figure 3.5 uses a narrowband LNA for each incoming signal, however, only one wideband LNA is used in Figure 3.4. Narrowband LNAs are more likely to provide better performance because narrowband LNAs generally have better return losses and gains than wideband LNAs. The use of multiple narrowband LNAs, on the other hand, is likely to cost more than a single wideband LNA. Additionally, using several amplification stages, such as those shown in Figure 3.2, were investigated. The number of amplification stages required is mostly determined by the degree of amplification achieved in each phase compared to the total amplification required. Furthermore, the probability of oscillation increases with each amplification stage employed. As a result, a trade-off must be made between the amount of amplification or amplifiers, the risk of oscillation, and the cost.

A mixer is used in Figure 3.4's design to down-convert the high RF signals, to either a lower IF or zero-IF. The degree of down-conversion is set by each channels' local oscillator according to one of the following ways:

1. Downconversion of each RFI signal by the same value ($LO1 = LO2 = LO3 = LO4$), essentially shifting all frequency bands by the same value. This would mean the same LO source can be used for each channel, however, IF3 and IF4 may still be relatively high and with a carrier above $1GHz$. Furthermore, each channel will still be at different centre frequencies.
2. Downconversion of each RFI signal to the same IF ($IF1 = IF2 = IF3 = IF4$). This method can shift the RF signals to any low IF or down to Zero-IF. At this point, each RFI channel will have each their signal's spectrum down at the same IF and therefore a relatively low sampling frequency is required.

The conversion of the RF signals into power, can either be done as part of the front-end or the processing. Figure 3.4 does the conversion through calculations in the signal processing phase. Alternatively, Figure 3.5's design uses hardware to measure the power. This technique decreases the required sampling frequency immensely because it generates a DC power signal.

After considering all the above-mentioned factors, a final signal chain design was selected. It is discussed in the following section.

3.2.1 Chosen signal chain receiver

Beyond the two alternatives presented in Figure 3.5 and 3.4, many signal chain combinations were considered. Figure 3.6 shows the final signal chain after comparisons. This section explains the factors that went into making this decision as well as the reasoning behind it.

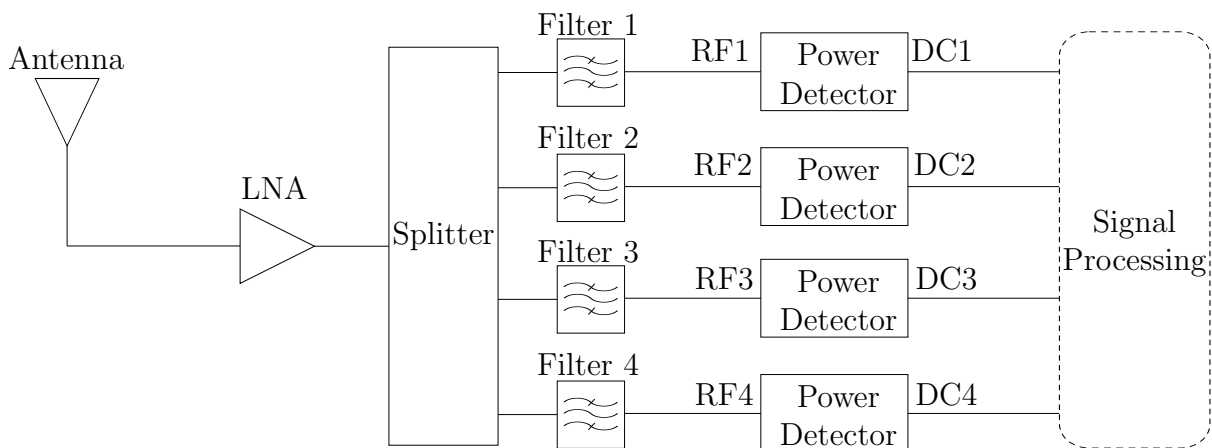


Figure 3.6: Final receiver front-end design for RFIPD.v00

The final receiver only employs one wideband antenna, to achieve the practicality and simplicity required of use as a handheld device. The wideband RF signal is designed to be amplified by a wideband LNA which should have good gain despite the wide frequency band. While the sensitivity of the system is likely to suffer when using a wideband LNA compared to four narrowband LNA's, it was judged that the benefit in terms of cost justifies the trade-off. Overall, employing a single wideband antenna and LNA is substantially less expensive than utilizing many narrowband antennas and LNAs. In the continued

effort to create a tiny receiver system with few components, an LNA with a good gain is also necessary because it is the only amplification stage. The wideband signal is divided into four channels, each of which is filtered into the desired frequency ranges. This allows the processor to easily discern between various frequency bands of the power signals measured. Finally, the signal passes via a power detector, which 1) reduces the number of samples required. 2) Reduce the amount of computing power required to complete a power conversion calculation. The mixer is excluded from the final receiver mainly because the local oscillator is difficult to design without generating leaking harmonics and also, the power detector proved to be more efficient for this application. The power detector's operation and features, as well as those of the other components, are explained in further depth in the sections that follow.

The characteristics, parameters and unit testing of each element in the final receiver is discussed from Section 3.3 to 3.7. To make the RFIPD_v00 easily replicable, only off-the-shelf components are used. Another reason is that designing separate components while developing a comprehensive system would create more work and be a longer development process. Additionally, despite the fact that there is no fixed budget, the components are selected to be as low-cost as feasible without compromising performance in the pursuit of a low-cost device overall.

3.3 Antenna

The role of the antenna in the front-end is to capture electromagnetic waves and convert them into an electric signal, which is then transmitted to the rest of the receiver [37]. The performance of the antenna, being the first component of a receiver system, is important to the receiver's entire functionality. The subsections that follow discuss antenna properties that are used in antenna selection as well as the measurements of the chosen antenna.

3.3.1 Antenna directivity, radiation efficiency and gain

A good understanding of radiation properties such as directivity, efficiency, and gain is required when selecting a good antenna [37] [38].

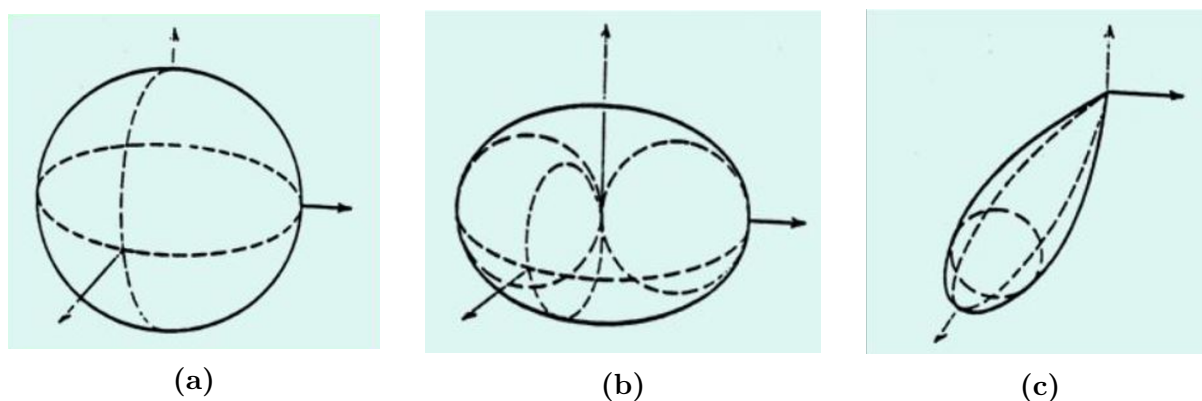


Figure 3.7: Model of the radiation pattern of an (a) isotropic, (b) omnidirectional and (c) directional antenna, illustrating the directivity of each type of antenna [39]

The directivity property of an antenna represents the measure of the concentration of an antenna's radiation pattern in a particular direction. This is illustrated in the form of polar radiation patterns in Figure 3.7. The isotropic antenna is theoretically lossless and it radiates equally in all directions, resulting in a spherical radiation pattern. This results in the directivity of 1 (0 dB) [38]. However, in practice, such a radiation pattern and directivity is not possible. Antennas with an equal radiation pattern in one plane (xy, xz or yz) are classified as omnidirectional. Alternatively, antennas can have higher directivity by being focused in a specific direction, classifying them as directional antennas. Antennas are commonly measured relative to the ideal isotropic antenna, with the unit *dB* [38]. Mathematically, directivity is expressed as

$$D = \frac{U_{max}}{U_{avg}} \quad (3.1)$$

where

D is directivity

U_{max} is maximum radiation strength

U_{avg} is average radiation strength across all directions

Portions of the power delivered to an antenna are not present in the output power or radiated power. This is due to re-occurring losses such as resistive losses in the imperfect metals used. The efficiency for a receiving antenna can be phrased as the relationship of the potential power captured from all angles to the power output. In transmitting antennas, the efficiency (η) is defined as the input power (P_{in}) to the radiated power (P_{rad}) as shown in eq. 3.2. For the same bandwidth, the same antenna receives as efficiently as it will transmit, hence the same equation describes efficiency for both modes of operation.

$$\eta_{rad} = \frac{P_{rad}}{P_{in}} \quad (3.2)$$

Finally, as shown in eq. 3.3, the gain of an antenna is a property affected/influenced by both the directivity and efficiency.

$$G = \eta_{rad} D \quad (3.3)$$

Considering eq. 3.1 and 3.2 this expands to

$$G = \frac{P_{rad} U_{max}}{P_{in} U_{avg}}. \quad (3.4)$$

In the case of a lossless antenna, eq. 3.3 shows that the gain will equal the directivity; otherwise, the gain will always be smaller than the directivity [38]. This is because directivity does not compensate for losses between P_{rad} and P_{in} , it only takes the given radiation pattern into account.

3.3.2 Antenna selection

There was a wide range of types of antenna designs to be considered, for example, wire antennas, aperture antennas and printed antennas, but these did not meet all the requirements [38]. The project required a robust, small antenna that could be mounted externally on a shielding case. To receive all of the RFI signal bands in Table 3.1 from all directions of

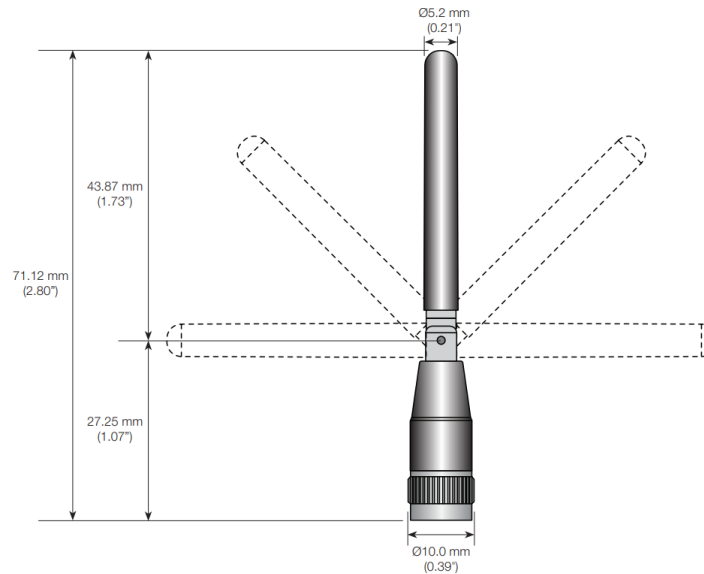


Figure 3.8: Illustration the the movement of the chosen antenna's tilting mechanism [40]

a plane, a wideband, omnidirectional antenna was required. These requirements were satisfied by a passive whip antenna from Linx Technologies, named ANT-LTE-SMA-MON. For design simplicity, a passive antenna was used, knowing that a dedicated low noise amplifier would follow in the signal chain to compensate for the passive antenna's lack of amplification. Table 3.2 [40] displays the antenna's specifications at the recommended frequencies of operation. Furthermore, this is an omnidirectional antenna with a tilting wand that allows the directivity plane to be changed, illustrated in Figure 3.8.

	698-960 MHz	1710-2170 MHz	2300-2400 MHz	2500-2700 MHz
Peak Gain	5.8 dBi	3.7 dBi	2.0 dBi	1.4 dBi
Average gain	-0.5 dBi	-1.75 dBi	2.9 dBi	-3.05 dBi
Efficiency	82 %	70 %	52 %	60 %

Table 3.2: Specifications of ANT-LTE-SMA-MON antenna [40]

The peak and average gain, relative to the isotropic antenna is shown to vary over different frequency bands in Table 3.2. This means that two signals of equal power but different frequencies will not be converted into the same electric signal magnitude. This is because the majority of antennas are designed to be resonating devices that work efficiently across a narrow frequency range, therefore, variations in the efficiency are expected from a wideband antenna such as this. This is a compromise taken so that a wide frequency range can be received. The antenna was chosen by inspecting the efficiency to ensure that the bands of interest had a high or at least moderate efficiency. Given the antenna's low cost and wide frequency bandwidth, it would be difficult to obtain an antenna with more constant performance.

3.3.3 Measurements

An antenna's performance can be verified using a variety of tests in the far-field and near field. These can reveal the radiation pattern, directivity, efficiency and gain of the antenna which can be seen in [40] for this antenna. Measuring the S-parameters of an antenna is a simple test for observing gain, compared to anechoic chamber tests or over-the-air tests.

Because an antenna is a one-port network, it only has one S-parameter, S_{11} also known as the reflection coefficient (Γ).

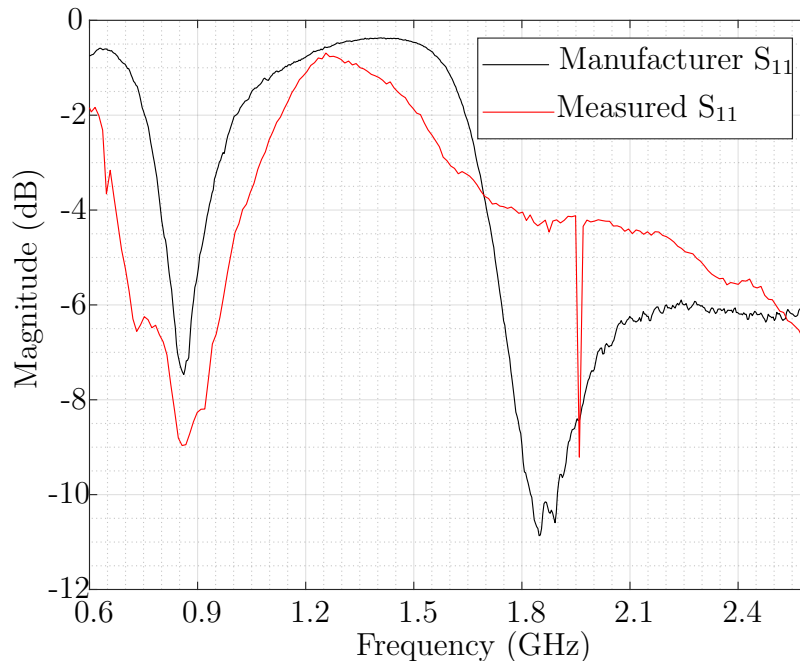


Figure 3.9: Reflection coefficient measurements from the manufacturer conducted with ground plane (black) and measurement conducted without a ground plane (red)

The reflection coefficient for 600 MHz - 2.6 GHz of the ANT-LTE-MON-SMA antenna is shown in Figure 3.9, under two testing environments, described below:

1. This is a measurement with the antenna positioned straight (i.e not tilted), and in the centre of a ground plane of unspecified length. This measurement was provided by Linx Technology and the measuring instruments were unspecified.
2. This is a measurement with the antenna connected directly to the Agilent PNA-X network analyser, which was calibrated prior to the testing. There is no ground plane in this test.

From Figure 3.9 it is observed that the overall trend of the two graphs, barely follows one another. This drift between the plots is attributed to a change in measuring environments, showing the effects of having good grounding for an antenna. A $1/4 \lambda$ monopole antenna is more effective on a ground plane because it appears to behave like a $1/2 \lambda$ dipole, as explained in [37].

A general rule of thumb is that a Γ of less than -10 dBm within the desired frequency range is acceptable for an antenna. However, achieving such performance across all the frequencies of a wideband antenna is very complex and costly. Therefore the -10 dBm was relaxed and a Γ of less than -5 dBm to -4 dBm is tolerated due to cost constraints. The manufacturer's result satisfies this requirement within the RFI signal bandwidths. According to the standard, the measurement without ground in 3.9, shows that the antenna will only receive the 895.5 MHz, 1950 MHz and 2450 MHz frequency channels reasonably well. Unfortunately, a lot of energy will be lost in the 1747,5 MHz frequency channel

when there is no ground plane. Hence the circuit layout of the receiver will be designed to have a full ground plane on the bottom. The desired effect of this is to have a Γ closer to that provided by the manufacturer, where the Γ is shown to be below -5 dBm across all four RF receiver channels.

3.4 Low-noise Amplifier

An LNA is a sensitive amplifier designed to amplify the signal while suppressing the noise floor. It is placed immediately after the antenna in the receiver to attenuate any noise gathered as early as possible. Another benefit of this positioning is that it can amplify small signals that would otherwise be lost in the noise floor. This section discusses the elements to consider when selecting an LNA, as well as the measurements of the chosen LNA.

3.4.1 Linearity of LNA

Amplifiers are linear devices meaning that the input and output power of signals are directly proportional. A device is linear, when the output response $y(t)$ for input signals, $x(t)$ can be expressed, according to [41] as

$$y_1(t) = fx_1(t) \quad (3.5)$$

$$y_2(t) = fx_a(t), \quad (3.6)$$

such that

$$ay_1(t) + by_2(t) = fax_1(t) + bx_2(t). \quad (3.7)$$

The difference between the input and output port signal's power is a constant gain function. However, as the output power increases, the gain begins to deviate from the constant value. As the gain deviates, the 1 dB compression point is when the output power is has deviated 1 dB away from the theoretical linear output power. The 1 dB compression point is used to describe the linearity of the LNA. Power levels that exceed this point cause the amplifier to saturate, introducing possible distortion, harmonics and noise to the signal [26]. Therefore, LNA's should be operated slightly below their 1 dB compression point to be safe.

3.4.2 Selecting an LNA

A good amplifier must have good isolation to prevent reflected signals entering the output port from travelling through to the input port. The level of isolation is represented by the S_{12} parameter, as discussed in Section 2.3.1. Therefore, the greater the magnitude of isolation, given in dB, the less energy can travel in the reverse direction. Too much reflected energy can be damaging to the device and/or system.

Furthermore, noise parameters that are discussed in Section 2.3.3 and the linearity of LNA's that are discussed above were taken into consideration when selecting an LNA. The LNA was required to have a gain of at least 20 dB across the bandwidth interest. An ON Semiconductor MMIC amplifier named SMA3103 was selected. Table 3.3 is a summary of the key parameters [42] for the selected LNA.

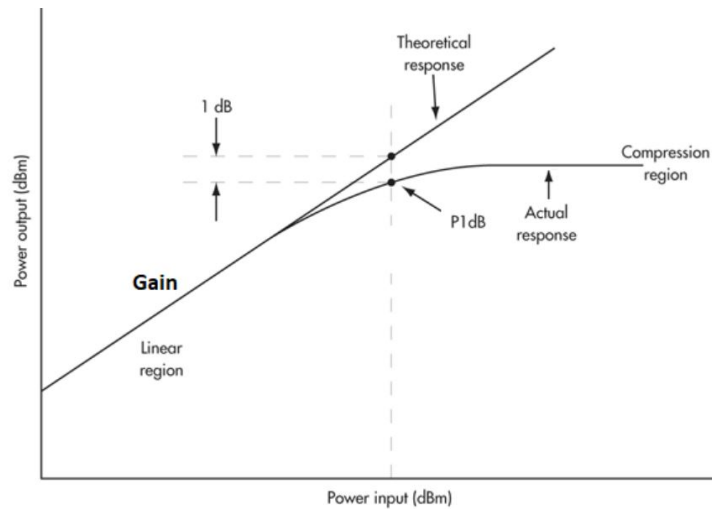


Figure 3.10: Plot showing the 1 dB compression point of amplifier [26]

	Minimum	Typical	Maximum
Frequency	0.1 GHz	-	3.3 GHz
Power gain	24 dB	26.5 dB	29 dB
Isolation	31 dB	33 dB	-
Input RL	12 dB	20 dB	-
Output RL	12 dB	20 dB	-
NF	-	4.7 dB	5.3 dB
P_{1dB}	6 dBm	8.2 dBm	-

Table 3.3: Specification of the SMA3103 LNA at test frequency, 1 GHz [42]

The SMA3103 provides a high gain at low current demand. It draws a typical current of 19 mA ($I_{max} = 25$ mA). Table 3.3 shows that the LNA has good isolation and almost no energy can pass in the reverse direction. Over 20 dB is attenuated in the reverse direction, according to the S_{12} specification. The SMA3103, has a low NF , but is acceptable when considering the high gain, isolation and return loss. Lastly, the P_{1dB} of 8.2 dBm has a moderate dynamic range, and this creates the upper limit for the power that can be transferred into the following component for the LNA to remain in its linear region.

3.4.3 Measurements

A breakout board was designed to test the SMA3103 with its biasing network [42]. The gain is measured by connecting the breakout board to a VNA to obtain S_{12} , this is shown in Figure 3.11. Furthermore, the gain as measured by the manufacturer is also shown in Figure 3.11.

The SMA3103 is said to have a nearly constant gain of approximately 28.5 dBm according to Figure 3.11, however, these results could not be replicated on the breakout board. A lower gain is measured on the breakout board which is mostly between 25-26 dBm below 1.5 GHz, however, the gain begins to drop until 20.8 dB, at 2.6 GHz. This

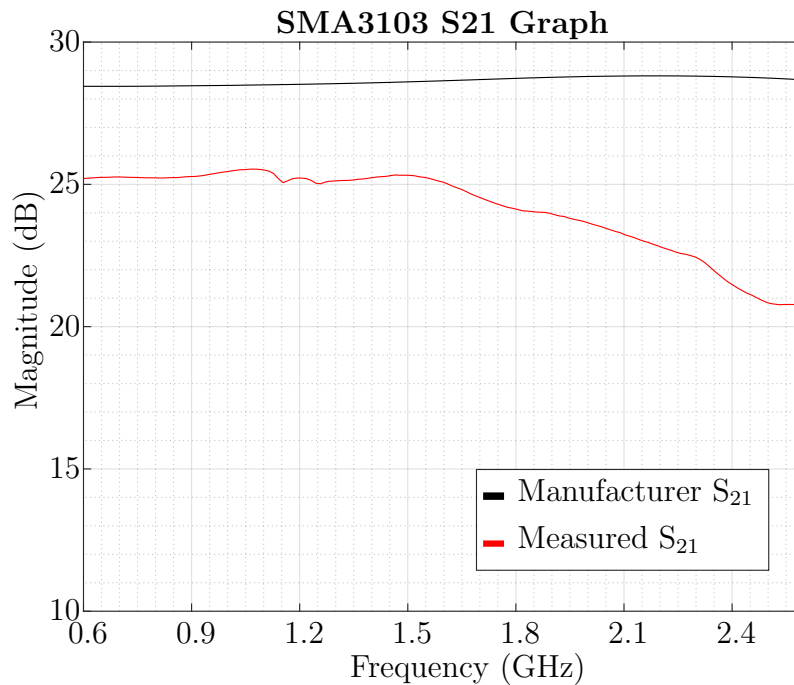


Figure 3.11: S-parameter gain that was (a) provided by the manufacturer and (b) measured on a custom SMA3103 breakout board

difference in gain measurements is attributed to using different passive components in the biasing network. The same valued components are used in the biasing network, but the components are from different manufacturers. Fortunately, the gain measured on the breakout board is adequate for the front-end design.

3.5 Power Splitter

The power splitter is placed third in the signal chain to provide four equal channels that will be filtered into narrowband (more on this in Section 3.6). Considering that power would be divided by the power splitter, the power detector was placed after the signal had gone through an amplification phase. This section describes how a power splitter works as well as the factors that influence the quality of its splitting capabilities. Furthermore, the power splitter that was selected is discussed.

3.5.1 Characteristics of power splitters

A power splitter can function as either a splitter or a combiner depending on the orientation of the device. The power splitter/combiner is a reciprocal, passive device meaning that it uses isotropic materials which make the input and output ports interchangeable. Power splitters have a minimum of 3 ports of which the respective transmission coefficients are the same, such that $S_{13} = S_{31}$. When there are multiple inputs supplied to the device, it acts as a combiner and outputs the sum of the inputs. The combining takes into account the differences in phases, magnitudes, etc. It is important to know the specifications of the incoming signals to estimate the expected output and how they will be summed. Alternatively, when there is a single input signal applied to the output of the combiner, then the device operates as a power splitter. For an n-port power splitter,

it splits the signal into $(n-1)$ port signals with zero phase difference between any two outputs. There needs to be good isolation between the output ports to prevent the energy of adjacent ports from leaking into one another.

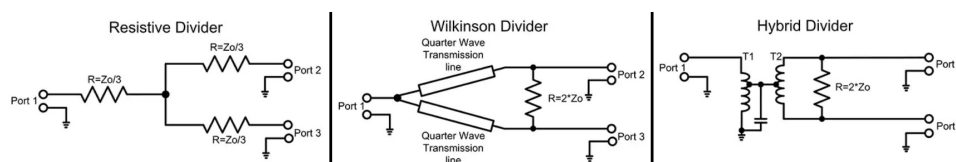


Figure 3.12: Main topologies for power splitter design: Resistive, Wilkinson and Hybrid Divider [43]

A seemingly direct solution for splitting signals could be a simple T-shaped transmission line. However, this does not provide isolation between the ports. In this case, when one output is shorted, the other outputs are shorted as well. The three main topologies used in power splitter design are the Resistive, Wilkinson and Hybrid splitter networks [43], shown in Fig. 3.12.

The resistive network often uses resistors in a symmetrical star topology. As a result, because all of the ports appear the same, there is no dedicated output port [44]. The resistors provide isolation between outputs, making it better than the simple T-shaped transmission line configuration. The simplicity, small size and low cost of this network design are appealing factors; however, this is at the expense of having power resistive losses.

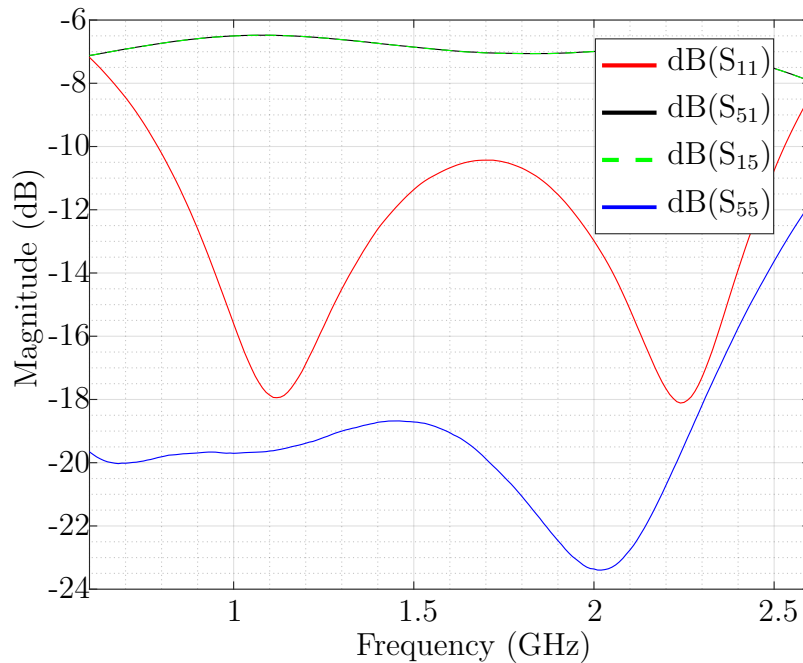
Secondly is the Wilkinson network which is a reactive system. It uses uncoupled $\lambda/4$ transmission line(TL) transformers, making it ideal to implement directly on standard PCB transmission lines. The frequency bandwidth is a factor in the TL length. The crossing resistor does not experience any potential difference because of the equivalent output ports, therefore it does not dissipate power. Rather, it acts as a means of isolation and matching network.

3.5.2 Selection of a power splitter

The receiver design requires a 4-way power splitter that will have a minimum level of attenuation on the signal. The Mini-circuit's SEPS-4-272+ power splitter was selected to split the single channel from the LNA into four in-phase channels.

The theoretical insertion loss for a 4-way power splitter should be 6 dB, but Table 3.4 shows the slight deviation in practice. The maximum deviation of the insertion loss from the ideal is 2.6 dB which is acceptable performance for a power splitter. Furthermore, the high isolation is good for preventing cross-talk of signals on the output side. Finally, the VSWR at both the input and output is relatively low which is a good indication of well-matched ports of 50Ω . This device could not be tested on its own using a spare unit because international stock shortages caused by the COVID-19 pandemic limited the number of units available for order.

	Minimum	Typical	Maximum
Frequency	690 MHz	-	2700 MHz
Insertion loss	7.5 dB	8.6 dB	-
Isolation	15 dB	20 dB	-
$VSWR_{input}$	-	1.5 : 1	-
$VSWR_{output}$	-	1.2 : 1	-

Table 3.4: Specifications of the SEPS-4-272+ power splitter [45]**Figure 3.13:** S-parameters of SEPS-4-272+ power splitter

The performance of the power splitter is illustrated with the S-parameters of the 5th port in Figure 3.13 provided by the manufacturer [45]. The transmission coefficients are identical and vary between -6 dB and -8 dB over the RFI signal bands. The reflections coefficient at the input port, S_{11} , has large deviations in values, nonetheless, remain less than -10 dBm for all the RFI signal bands on interest. The reflection coefficient at the output port, S_{55} , is very low below -18 dB, but it rises significantly above -18 dB after 2.4 GHz. This increase in the reflection coefficient is still less than -10 dB, making it acceptable and not posing a significant risk of creating reflections.

3.6 Filters

The purpose of the filters in the receiver is to convert each wideband signal coming out of the power splitter into a narrowband signal that corresponds to the bandwidths of the RFI signals of interest. Filters are employed to restrict the frequency range of each channel that exits the power splitter. This step is critical because it allows the signals in the channels adjacent to one another in the receiver to be distinguished from one another

according to their frequency. This section discusses the characteristics of different filters and the measurements of the chosen filters.

3.6.1 Characteristics

Filtering can occur in either the digital domain or in the analogue domain depending on the nature of the incoming signal. Digital filters are implemented in the case of a sampled, digitized input signal. Therefore, since RF signals are being filtered, the receiver radio uses analogue filtering.

Mathematically, the filtered function is the Fourier multiplication of the Filter transfer function($H(j\omega)$). The filtering function is designed to maximize the passband whilst attenuating frequencies outside of the passband. The selected passband of the frequency response determines whether the filter is a low-pass, high-pass, bandpass, notch or comb filter.

$$V_{out}(j\omega) = H(j\omega).V_{in}(j\omega) \quad (3.8)$$

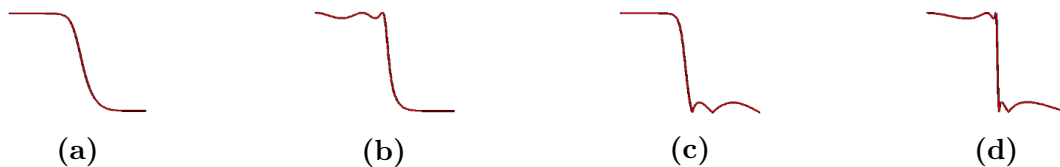


Figure 3.14: Diagrams of the frequency response for polynomial filters - (a) Butterworth, (b) Chebyshev 1, (c) Chebyshev 2, and (d) Elliptic filters [44]

Different polynomial transfer functions, including Bessel, Butterworth, Gaussian, Chebyshev, and Elliptic, can be used to create the transition between the passband and stopband. The response of some transfer functions is depicted in Figure 3.14, which shows the impact of each on the flatness in the passband, stopband, and transition in between.

3.6.2 Selection of filters

Four bandpass filters are required to restrict the frequency bandwidth of each channel in the receiver to meet the RFI signal bandwidths. Aside from having passbands that match the RFI signals bandwidths, the filters had to be surface mount for a compact design, have an insertion loss of less than 3 dB, and have a rejection band greater than 30 dB. Tai-saw Technology offers a wide selection of small surface mount filters. Their filters were the best low-cost COTS options found at that time, that came closest to meeting the requirements. The table contains the specifications for each filter that was chosen.

Filter	TA0627A	TA0391A	TA0401C	TL0009A
Passband (MHz)	876 - 915 MHz	1710 - 1785 MHz	1920 - 1980 MHz	2400 - 2500 MHz
Insertion loss	2.2 dB	2.6 dB	2.4 dB	1.5 dB
Stopband attenuation	13 - 25 dB	14 - 25 dB	25 - 44 dB	25 - 30 dB

Table 3.5: Specifications of RF front-end bandpass filters for each channel

The insertion loss (IL) in filters is related to passband signal attenuation; therefore, a lower IL is preferable. Table 3.5 shows that all of the filters met the 3 dB requirement for IL . Although an IL of zero is ideal, any insertion loss less than 3 dB is acceptable. The stopband attenuation refers to the amount of signal suppression outside of the passband. With a larger stopband rejection, the passband becomes more distinct. Table 3.5 shows that the minimum out-of-band rejection requirement was not met by the filters selected. This may be detrimental to the receiver system, however, they were chosen since they were the closest options to the requirements found.

3.6.3 Measurements

To verify performance, each filter was placed on a breakout board of its own and the S_{21} was measured, as shown in Fig. 3.15. This is plotted against the manufacturer's results for S_{21} .

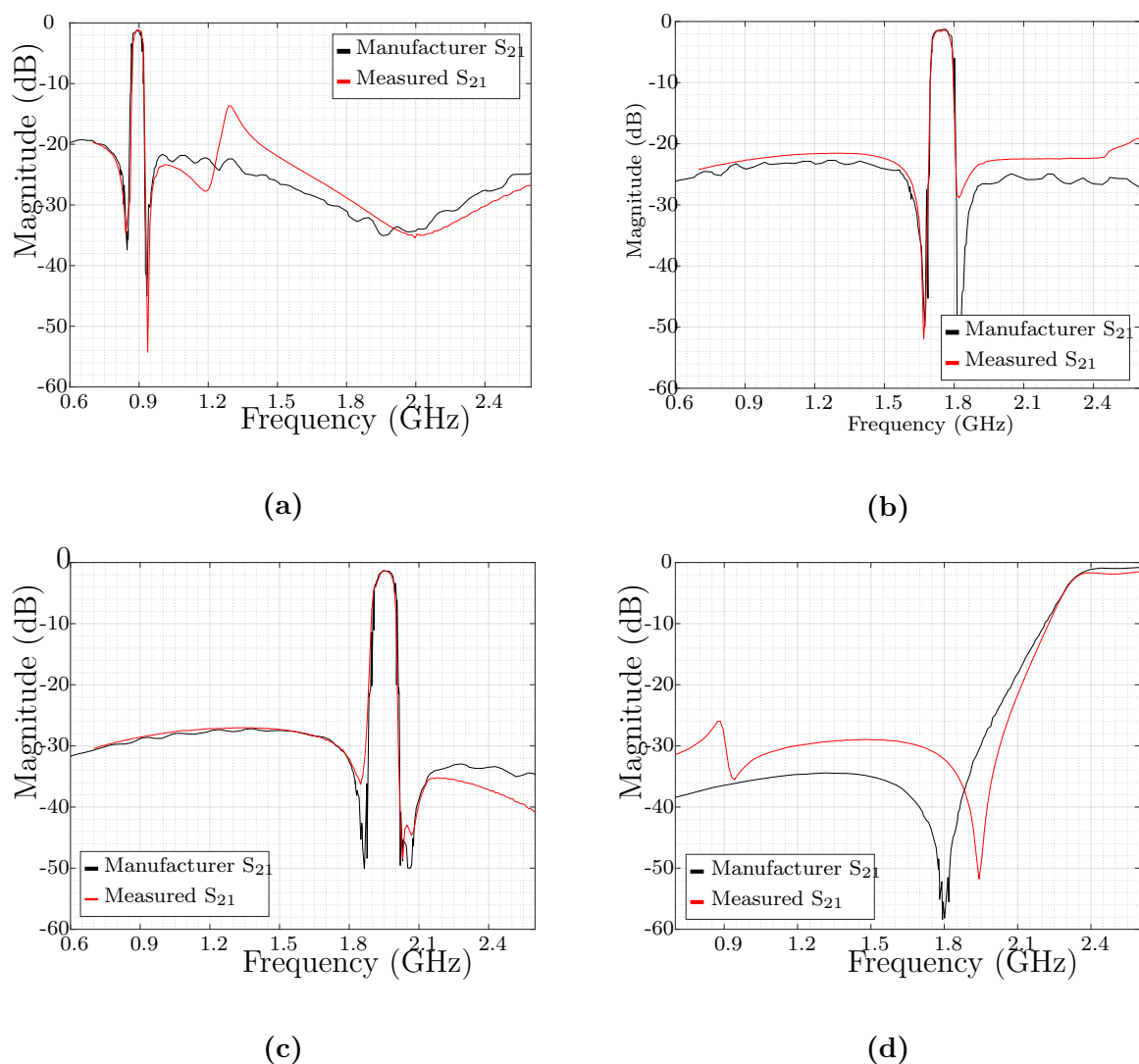


Figure 3.15: Filter responses provided by the manufacturer (black) and measured on custom breakout boards (red) for each RF channel filter - (a) filter TA0627A with f_{center} of 895.5 MHz (b) TA0391A with f_{center} of 1745 MHz (c) TA0401C with f_{center} of 1950 MHz (d) TL0009A with f_{center} of 2450 MHz

The passband for Figures 3.15a to 3.15c is narrow, with sharp cut-offs, and both the manufacturers' and breakout board measurements are in agreement. The transition from passband to stopband in Figure 3.15d, on the other hand, occurs over a wide range of frequencies that are not well matched between the manufacturer and breakout board readings. However, the passband (above -3dB) remains well matched over a 100MHz bandwidth and is suitable for the project's needs.

3.7 Power Detector

The power detector is the last analogue component in the RF receiver architecture before the signals are processed. The purpose of the power detector is to do the conversion of the incoming RF signals into their equivalent power signals, as demonstrated in Figure 3.6. The properties of different power detectors are discussed in this section as well as the performance of the chosen power detector is analysed.

3.7.1 Characteristics of power detectors

RF power detectors are devices that convert an input RF signal power (peak, RMS, etc) into a DC signal. The relationship between the input signal power and output voltage level depends on the type of RF detector. Common RF detectors include envelope detectors, log amplifier detectors and RMS detectors.

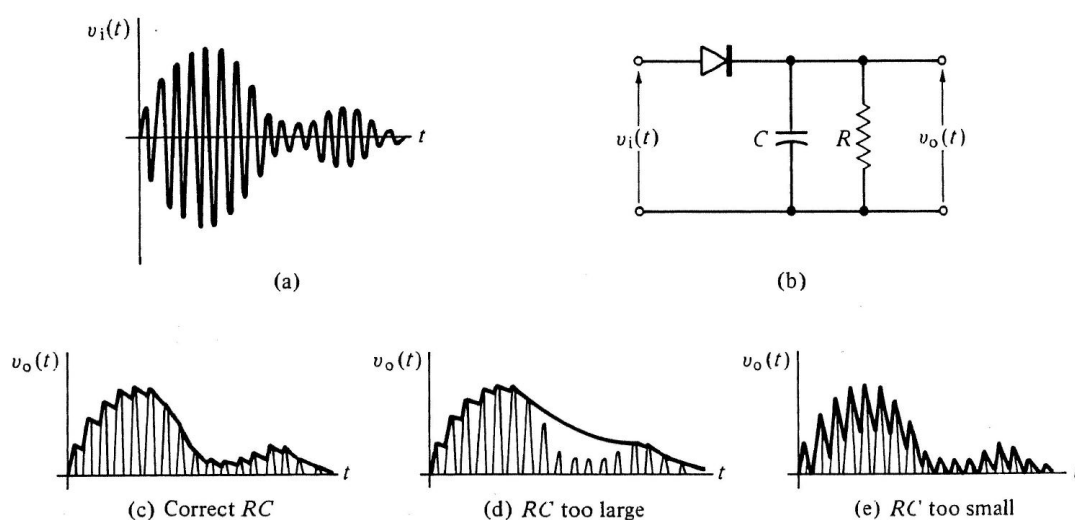


Figure 3.16: Diagram showing the effect of varying RC time constants on the shape of the envelope in an envelope detector [46]

Envelope detector

The envelope detector is essentially a diode peak detector circuit. Its functionality is based on a non-linear $V-I$ diode relationship. When the diode is forward biased with a signal above the threshold knee voltage, the output is the positive "envelope" of the input. Additionally, a parallel capacitor is used to create a holding effect on the most positive input value. The capacitor discharges over time when the input has a negative gradient [47]. The rate of discharge determines how well the output follows the ideal envelope, see Fig. 3.16. This is determined by the RC time constant [47]. The relationship between

the input and output signal is dependent on the range of input power. For signals with lower power, the output is equivalent to the square of the input voltage signal. This is known as the square law [26],

$$V_o = mV_i^2 \quad (3.9)$$

and since $P = V^2/R$, therefore,

$$V_o \propto P_{in}. \quad (3.10)$$

Input signals with mid-range power have a proportional relationship with the output signal. The two signals are related by a constant, m as follows,

$$V_o = mV_i \quad (3.11)$$

therefore,

$$V_o^2 \propto P_{in}. \quad (3.12)$$

Finally, beyond a certain threshold input power level, the output signal is constant at saturation [26]. The expected range of input power is very important to ensure that the envelope detector operates in the desired region so that the relation of V_o to P_{in} will be correct.

Log detector

The log amplifier is possibly the most commonly used detectors. This detector is comprised of a series of cascaded amplifiers and diode detectors. This combination of components create an output dc voltage that is proportional to the log of the input power [48]. Therefore the conventional response has V_o directly proportional to the decibel input power range P_{in} (dB). Using inverse log manipulation, we see that,

$$P_{in} \propto 10^{mV_o+n}, \quad (3.13)$$

where m and n are constants.

The log detector is a good choice for many cases, specifically where a fast response time or a wide dynamic range is needed [48]. The fast response time makes it optimal for systems expecting pulsed signals and the wide dynamic range improves the sensitivity for low signal levels [47]. However, these detectors are not well-suited for signals with regular fluctuation in peak to average (PAR) power ratio, for example, amplitude modulated (AM) signals.

RMS detector

Unlike the envelope and log detectors, the RMS detectors measure relative to the input RMS value instead of the actual power levels. The root-mean-square (RMS) value of the incoming signals refers to the dc signal required to deliver the power as the RF signal [47]. The calculation performed by the RMS detector is mathematically represented as,

$$V_{in(RMS)} = \sqrt{\frac{1}{N} \sum_i^N v_{in}^2}. \quad (3.14)$$

This conversion process is, therefore, less responsive than other detecting techniques. Nonetheless, the RMS detector is the best solution for signals with high crest factors or alternating crest factors. Systems that work with complex waveforms should use RMS detectors because the signals' crest fluctuations do not affect the performance of the RMS

detector [47].

Power detectors in receiver systems are primarily used to perform power measurements or as part of power control sub-systems. The different power detectors discussed above show how different information regarding the incoming signal's power can be obtained. The measurement is then related to the input using the various relationships of the detectors. Furthermore, the power detector can form a feedback loop that controls the systems power gain or a variable gain amplifier (VGA) [47]. This is done to prevent damage to the succeeding sensitive components from excessive incident power. Other applications include input protection, RF pulse detection and radar.

3.7.2 Selection of a power detector

For this project, the power detector is the last analogue component of the receiver chain. The power detector, like the LNA, power splitter, and filters, was required to be a surface mount component in order to achieve a compact design. Furthermore, because the power detector's output is sent into a signal processing system, the power detector's output voltage cannot exceed the processor's maximum input voltage. As a result, the output voltage of the power detector had to be less than 3.3V, which is the system voltage of the processing unit implemented in Chapter 4. These requirements significantly reduced the number of possibilities for off-the-shelf RF power detectors that work across all the RFI signal bandwidths concerned. Because of its wide dynamic range and sensitivity of up to -70 dBm, the Linear Technologies LT5583 log-amplifier power detector was chosen from the few remaining possibilities.

	$f_{RF} = 880MHz$	$f_{RF} = 2140MHz$	$f_{RF} = 2700MHz$
Input dynamic range	-75 to 10 dBm	-72 to 10 dBm	-72 to 10 dBm
Output slope	19.0 mV/dB	17.7 mV/dB	17.6 mV/dB
Rise time	100 ns		
Fall time	180 ns		

Table 3.6: Specifications of LT5583 log power detector at 880 MHz

Table 3.6 shows some of the power detector's most important features, such as its quick rise and fall times. This demonstrates the LT5583's short response time, which is critical for this project because the transmission bursts outlined in Section 2.1 are also quite fast. With these fast rise and fall times, the power detector will be able to react quickly to the expected data packets and detect fully data packets of at least 280 ns.

3.7.3 Measurements

A breakout board was designed and etched to test the LT5583 in isolation from the rest of the receiver circuit. The LT5583 provided an option to include an additional low-pass filtering stage. Adding a second step of filtering could improve stopband rejection, but this would necessitate more design work to fine-tune each filter to the receiver channel. Furthermore, adding this stage of filtering to the system would add IL to the system,

attenuating the signal in the passband, which was not wanted. A Rohde and Schwarz SML03 signal generator was used to supply a signal to the LT5538 and the output voltage was measured.

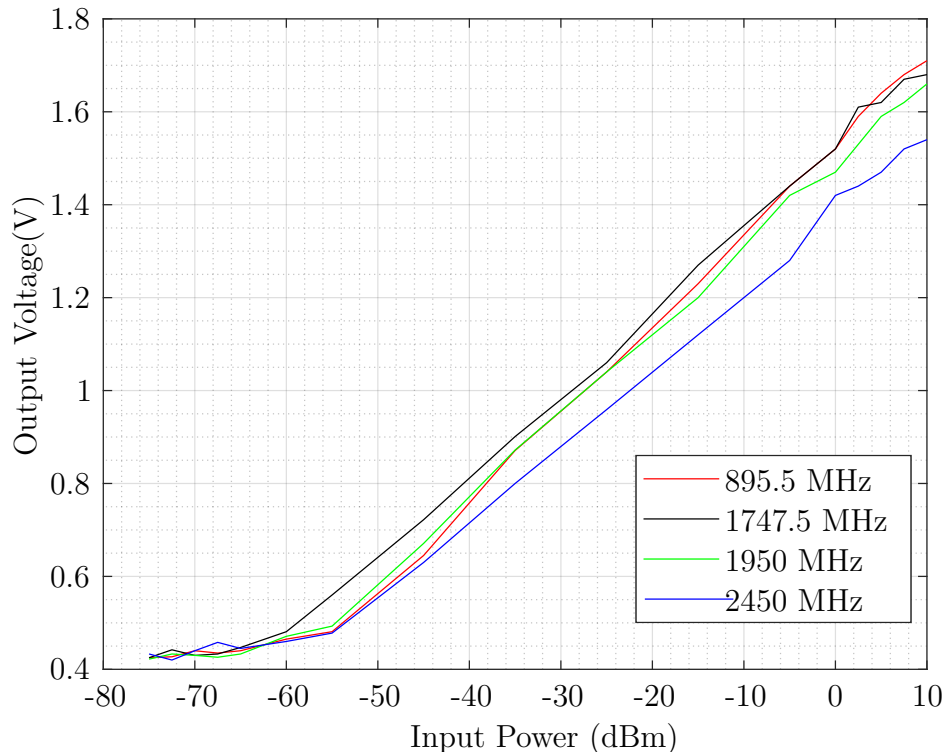


Figure 3.17: Results of power detector performance test

Fig. 3.17 shows the voltage response of the LT5538 over the operation input power range for each channel in the receiver. A linear trend relative the logarithmic power scale (i.e dBm scale) is observed as expected for a log amplifier detector, in accordance with eq. 3.13. This trend changes between -60 to -65 dBm as the power detector maintains an output slightly above 400 mV regardless of the change in input power. This means that the sensitivity is about 10 dB poorer than stated in Table 3.6.

3.8 Performance of the RF Front-end Receiver

After all of the components have been chosen and the respective unit and component testing have been conducted, they are combined in simulation to see how the receiver will perform. After that, the performance of the RF receiver circuit board can be evaluated. The RF-receiver must be tested in order to determine how well RFI signals can be captured and hence detected. This testing is crucial in determining the sensitivity of the RFIPD. The outcomes of the chosen final receiver design are covered in this section.

3.8.1 Simulation

A model of the receiver design is created in AWR (see Figure 3.18) to inspect the RF signals. For the receiver design layout refer back to Figure 3.6. The power detector is

not included in this model because it is solely to inspect RF signals. The S-parameters measured on the breakout boards for each component are imported into the model. The full receiver is a 5-port network, and the forward transmission coefficient for each channel is graphed in Figure 3.19.

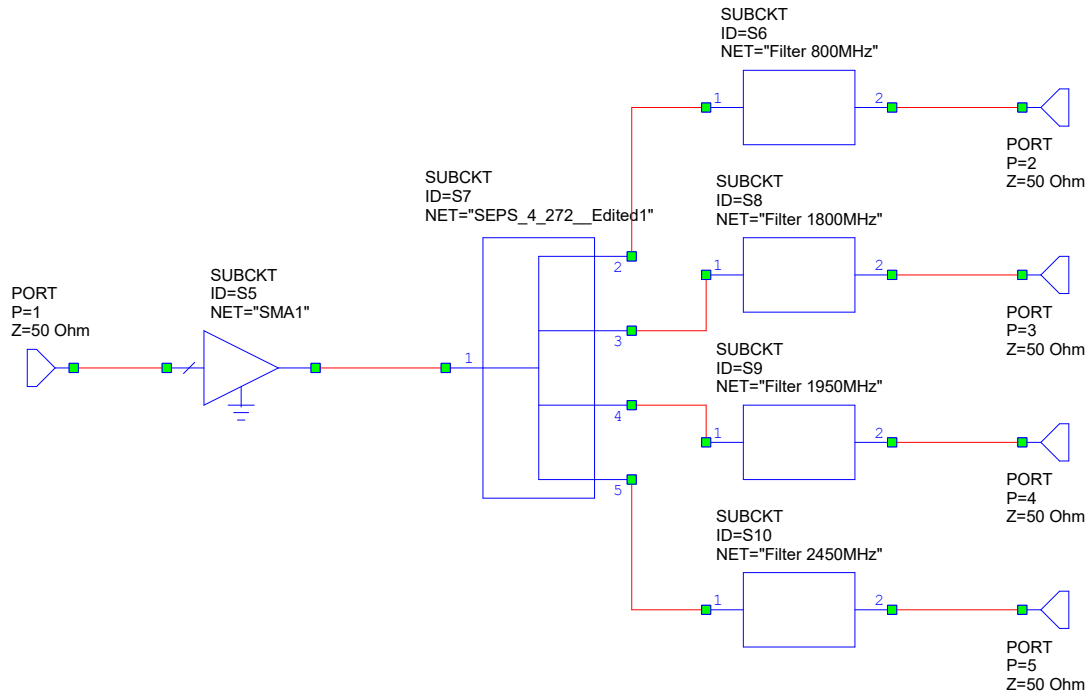


Figure 3.18: AWR model of receiver

The accumulation of the gains and losses are observed through the simulation. In each channel, the passband formed by the filters is evident. Table 3.7 uses the signal peak of the signal in the passband and that in the stopband to obtain the a stopband attenuation.

Channel f_{center}	Passband _{Peak}	Stopband _{Peak}	Attenuation _{Stopband}
895.5 MHz	26.89 dB	1.03 dB	25.86 dB
1747.5 MHz	0.63 dB	-11.14 dB	11.77 dB
1950 MHz	2.7 dB	-26.3 dB	29.08 dB
2450 MHz	8.44 dB	-14.56 dB	23 dB

Table 3.7: The RF receiver's passband peak, stopband peak and stopband attenuation

All of the passbands should ideally be well above 0 dB, as with dB(S21) in Figure 3.19, while the stopbands should be significantly lower, like dB(S41). This would ensure large stopband rejection so that the signals in the passband are more distinguishable from the signals that are out-of-band. From Table 3.7 it is seen that the stopband attenuation from the receiver channels ranges from 11.77 to 29.08 dB. The filters used had small stopband attenuation, and this has negatively impacted the receiver's performance as expected.

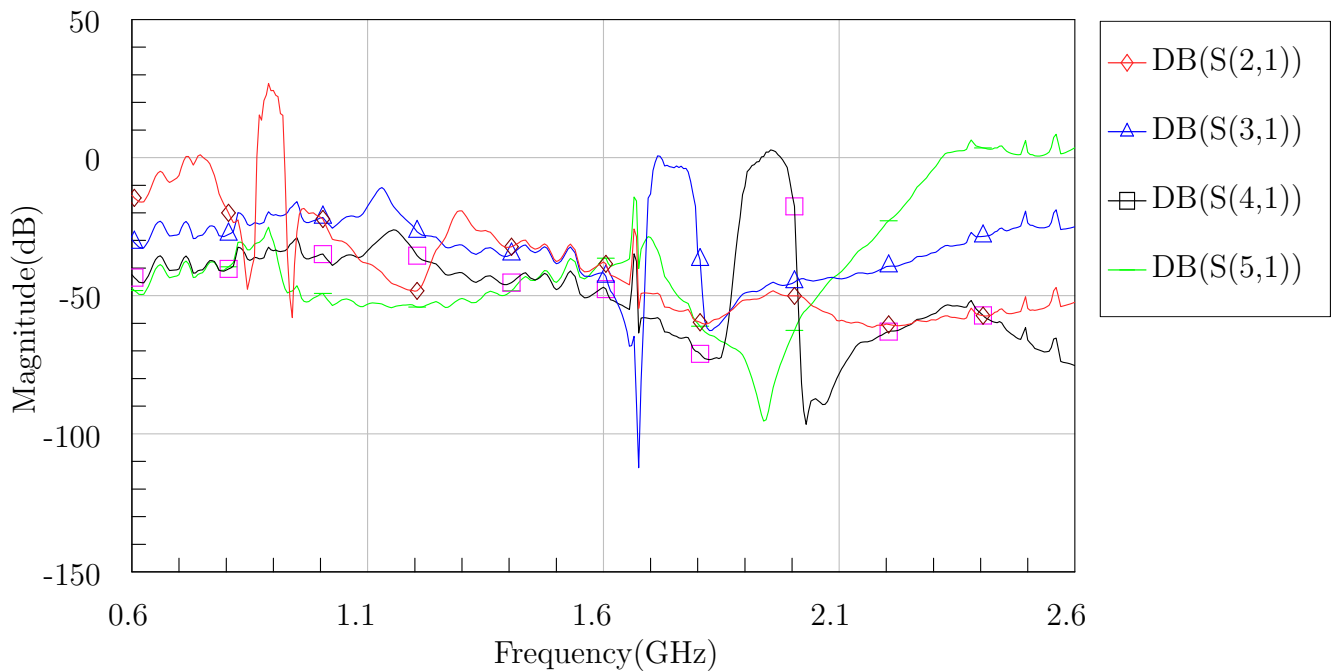


Figure 3.19: Transmission coefficients from the simulation of the RF front-end done in AWR

Furthermore, it was noted in Section 3.4 that the LNA's gain dropped substantially after 1.5 GHz. The impact this has on the receiver is that stopband signals below 1.5 GHz will receive a lot of gain, this effect can be seen in all of the channels in Figure 3.19. This raises the noise floor, making it more difficult to distinguish the signal from the noise.

3.8.2 Measurement

The performance of the RF front-end was evaluated on the PCB that was manufactured which is discussed in detail in Section 5.2. The Rohde and Schwarz SML03 signal generator was used to provide variable power level inputs at the centre frequencies of each channel: 895.5 MHz, 1747.5 MHz, 1950 MHz, and 2450 MHz. These are the centre frequencies of the RFI signals that are supposed to be detected. Each RF channel was measured for all iterations of centre frequencies and the results are displayed in Figure 3.20 to 3.23.

Each figure below should ideally depict the channel tuned to the incoming signal in the matching frequency as the only signal, with variations due to changing power levels. However, all of the channels change as the power levels for all of the frequencies change. This indicates that either the filters are not filtering as well as expected or that there is channel coupling. This results in a decrease in the system's theoretical sensitivity of -75dBm. Channels 1 and 4 show superior performance when compared to the other channels, which have difficulty distinguishing between detected frequencies. These results are in agreement with the simulation, because in both cases it is concluded that the signals are not attenuated well for out-of band signals.

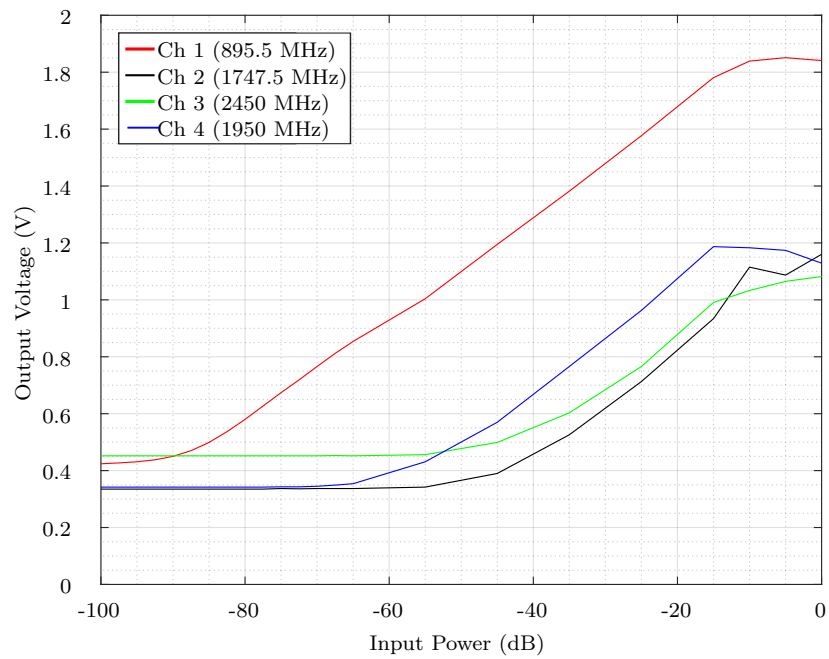


Figure 3.20: RF Frontend output across channels when input frequency is 895,5MHz

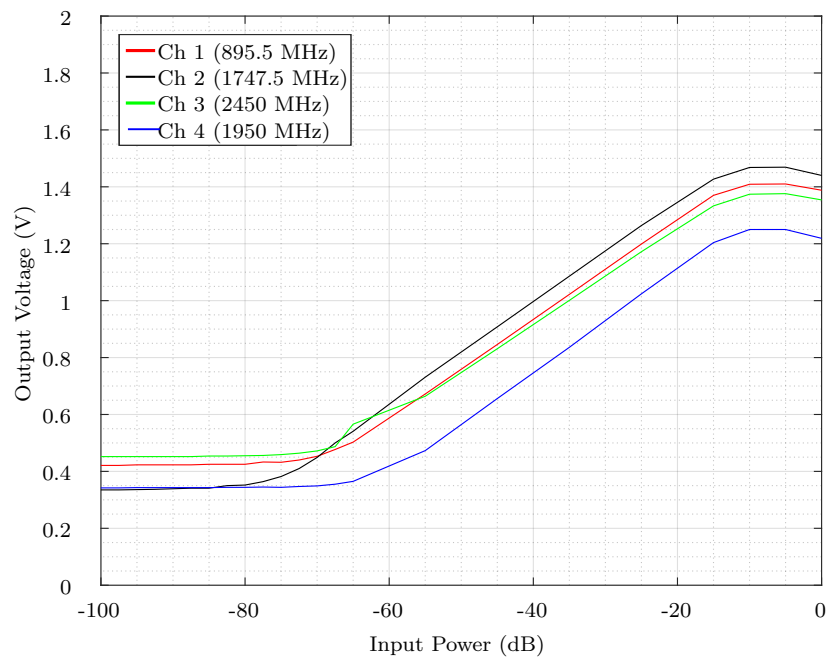


Figure 3.21: RF Frontend output across channels when input frequency is 1747,5MHz

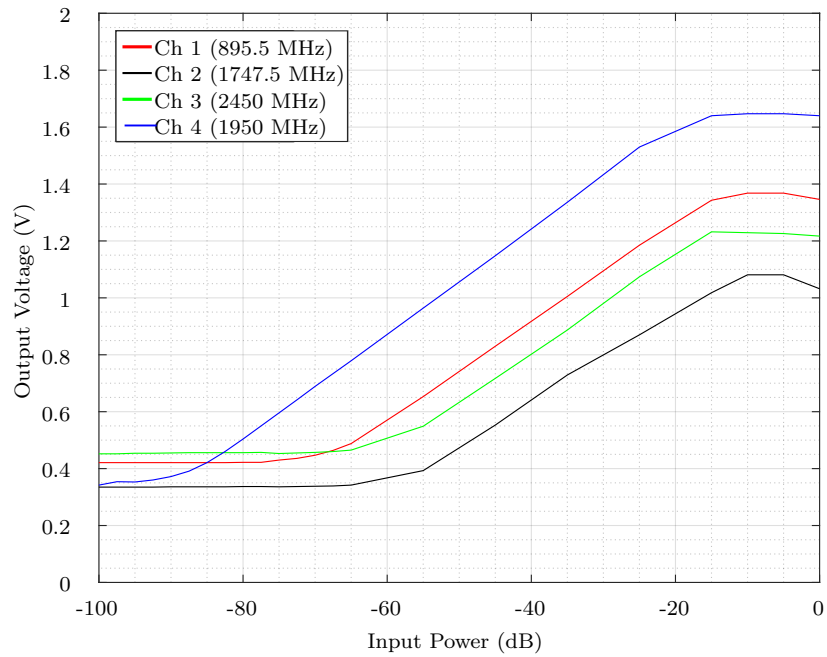


Figure 3.22: RF Frontend output across channels when input frequency is 1950MHz

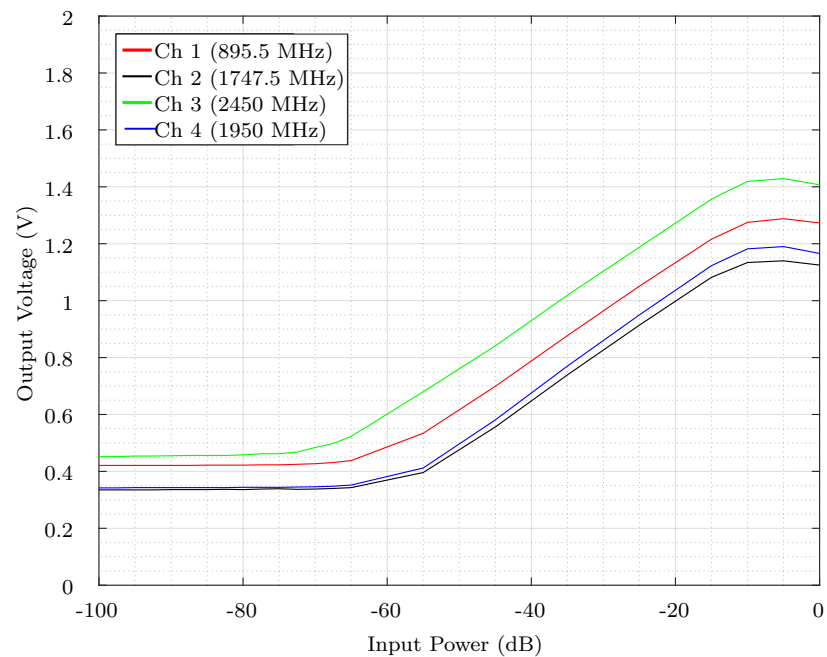


Figure 3.23: RF Frontend output across channels when input frequency is 2450MHz

3.9 Conclusion

The goal of this chapter was to design the RFIPD's receiver front-end and test its performance. After weighing the pros and cons of several architectural and receiver design alternatives, a design was chosen that required fewer components and significantly less computational power in signal processing than the other options. This receiver was made up of a wideband antenna, a wideband LNA, a 4-way power splitter, four narrowband filters, and a power detector that would send the signals to the signal processing system, which will be explained in the next chapter. The considerations taken when selecting each of the components were discussed and the performance was tested where possible. Finally, the receiver was simulated and built for testing. Its performance was discovered to be less sensitive than the desired -75 dBm. This was mostly due to the filter's poor stopband rejection as well as the fluctuating gain noticed in the LNA s-parameters. Consequently, the low sensitivity developed here is carried over to other portions of the project, affecting the overall performance of the RFIPD.

Chapter 4

Signal Processing

The design and implementation of the signal processing system are discussed in this chapter. The purpose of this system is to process the signals acquired by the RFIPD_v00 and to provide a platform on which to present them in a manner that can be easily interpreted by the end-user. By implementing such a system, the signals captured by both the RF front-end and position tracking system can be logged, processed, the information extracted can be analysed and decisions can be made regarding the RFI environment. This chapter begins with a general overview of the processing system design, followed by detailed descriptions of its various components.

4.1 System Overview

A signal processing system is designed to process the signals transferred through the receiver front-end and position tracking system. Figure 4.1 shows an overview of how the elements of the signal processing system interact. The system is divided into two phases - data acquisition and data processing.

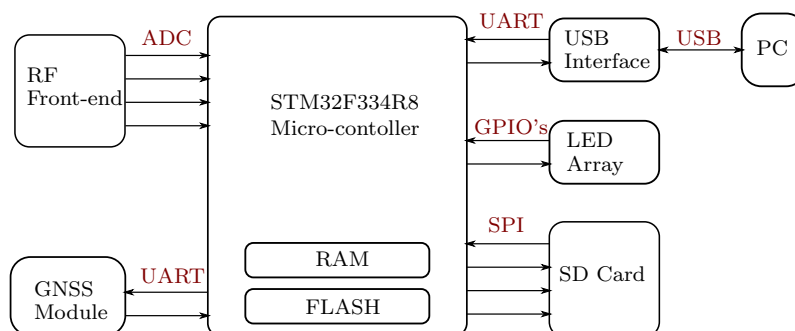


Figure 4.1: An overview of the signal processing system

Data acquisition is implemented on the micro-controller to collect and sort the input data coming from the receiver front-end and the position tracking system. The design of the receiver was discussed in Chapter 3, and the position tracking system is to be discussed in Section 4.2.6. The input data can be logged onto secondary memory, so that it can undergo data processing at a later stage. Additionally, the receiver data is used to indicate the signal strength using an array of LED's. Given the system design, the micro-controller is required to have at least

1. An analogue-to-digital converter capable of digitizing all four front-end channels at a suitable frequency, as described in Section 2.4.
2. Two UART's to support communication between the position tracking system and the USB interface.
3. Data transmission support for secondary memory/SD card
4. Eight general-purpose input and output (GPIO) pins to be used to control the array of LEDs.

The implementation and performance of each of these sub-elements is discussed from Section 2.4 to 4.2.8.2.

Data processing is the process of extracting information from the data and presenting it to the end-user in a meaningful format. For this project, data is sent from the SD card to a computer via a USB interface connection, where it is processed using a PC software program. The acquired data is subjected to power calculations, with the results shown as a report or charts. The end-user can then analyse the data and make decisions based on their findings. The design and functionality of the PC program is described in Section 4.3 and examples of results generated by the software are shown in Figure 6.7.

4.2 Micro-controller

Micro-controllers are generally easy to program, however, they are not specialized for complicated mathematical computations. In comparison to alternative processing technologies (see Section 2.5), this makes it an excellent choice for data acquisition. The RFIPD_v00 uses the STM32F334R8 micro-controller in particular. This section explains why this micro-controller was used, highlights some significant features, and gives an overview of the software.

4.2.1 STM32 development board

The STM32 series of 32-bit micro-controllers provide a wide selection range of versatile and highly configurable micro-controller units (MCU). Appendix A shows how the series is categorised according to its core processor and the suggested best-suited applications for each MCU. Each MCU is embedded with an Arm[®] Cortex[®]-M core, flash memory, static random-access memory (RAM), a debugger and multiple peripherals [49].

The Nucleo-F334R8 development board was selected because it met the minimum requirements of features needed for data acquisition, listed in Section 4.1. Additionally, figure 4.2 shows that the Nucleo board supports both Arduino connectors and STmorpho connectors, providing easy access to GPIO's. Furthermore, the decision on this board selection was also highly motivated by the fact that these boards were readily available to use from the Stellenbosch Electronics Engineering Department. This Nucleo-64 pin board houses an STM32F334R8 micro-controller in an LQFP64 package, with a CPU capable of 72MHz. The default CPU clock speed when the software was first launched was 64 MHz; this was not changed because the speed difference would be insignificant for the performance of this project. Table 4.1 shows some of the key features of the STM32F334R8

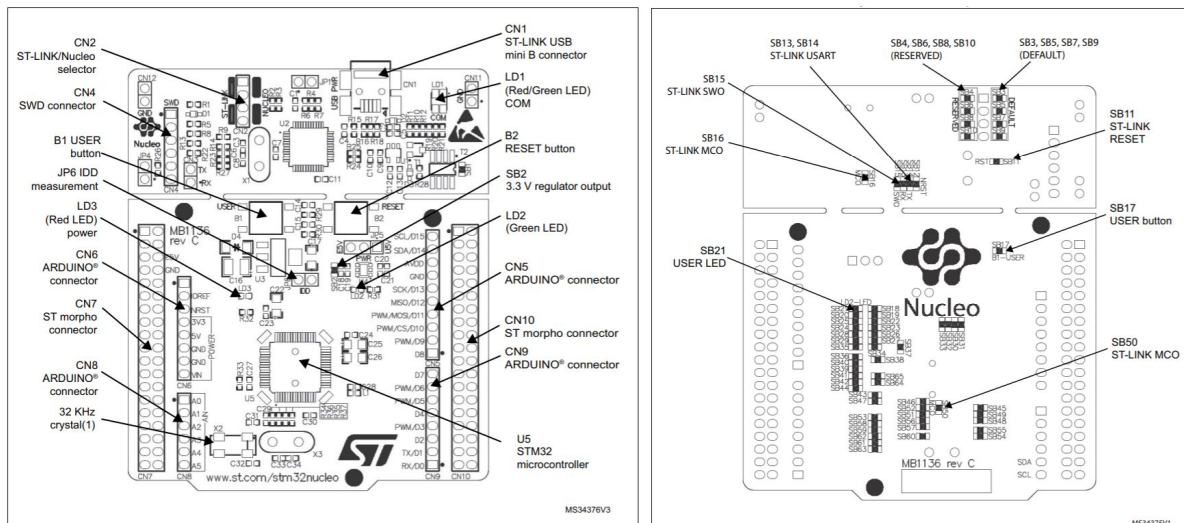


Figure 4.2: Nucleo-F334R8 Development board layout, where (a) Top layout (b) Bottom layout [50]

micro-controller and a more detailed block diagram can be found in Figure A.2.

Specifications	Value
Power Supply	2 – 3.6 V
12-bit ADC	2 (21 channels)
SPI	1
UART; USART	1; 2
Flash memory	64 kB
SRAM	16 kB

Table 4.1: Key specifications of STM32F334R8 micro-controller

The Nucleo-64 boards are divided into two sections namely the ST-Link/V2-1 and the target STM32 MCU section as shown in figure 4.2. The ST-Link/V2-1 is the embedded debugger and programmer tool for the target STM32 micro-controller. This ST-Link/V2-1 section can be cut off from the board to remain only with the smaller STM32 MCU section. The micro-controller can still be programmed using jumper cables from the serial wire debugging (SWD) connectors on the ST-Link/V2-1 [50]. The micro-controller was programmed and debugged using STM32CubeIDE and its built-in visual-based configuration tool, CubeMX.

The flow diagram for the micro-controller program is illustrated in Figure 4.3. This high-level outline of the program illustrates the sequence of the micro-controller. The program begins by configuring the peripheral and running a startup sequence that takes less than 1 minute to complete. Thereafter it runs whichever mode it was last operating in. Note that the micro-controller program works in tandem with the PC data processing software (discussed in Section 4.3.1), the modes used are set using the PC software.

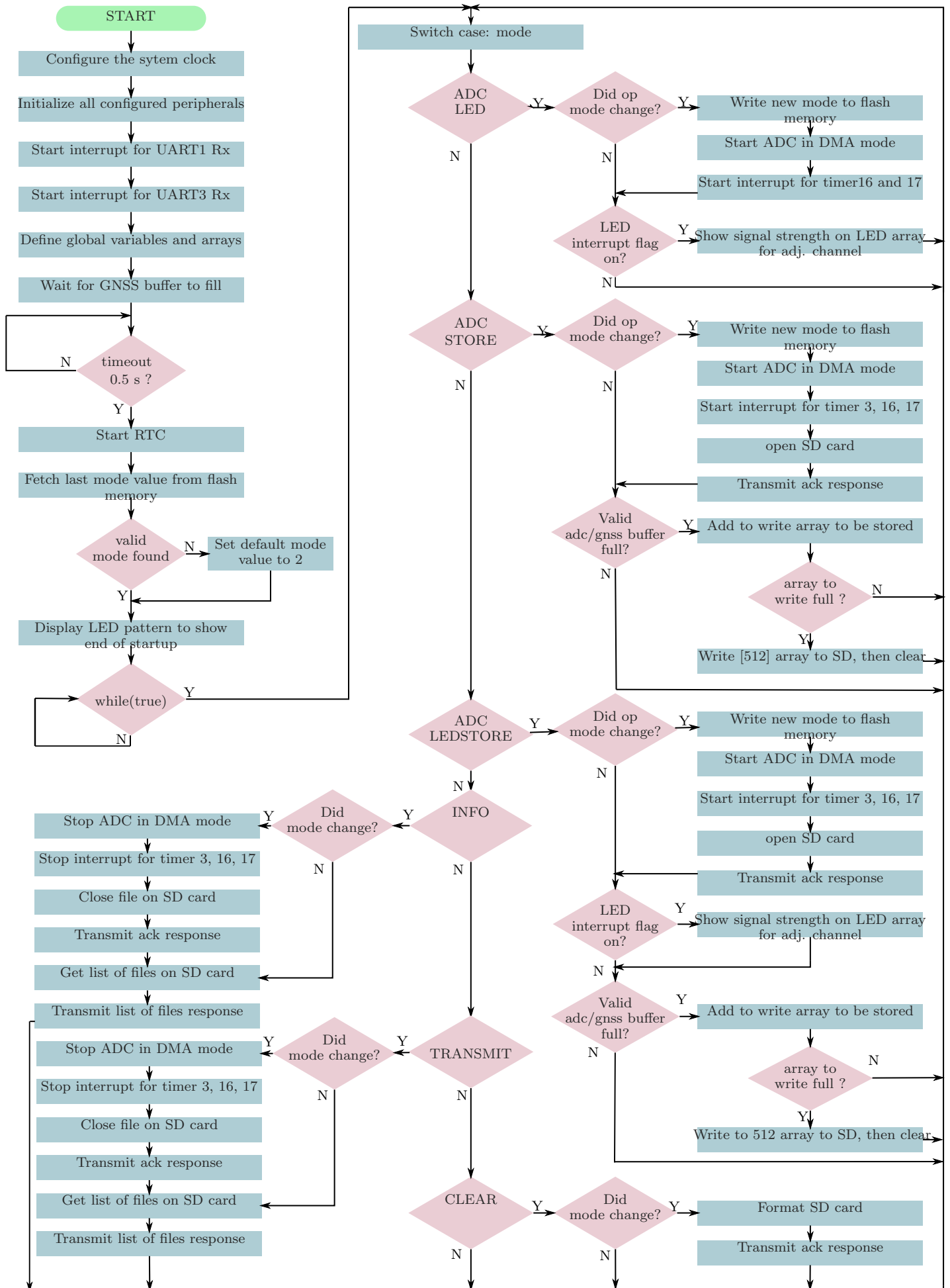


Figure 4.3: Micro-controller flowchart diagram

4.2.2 Transferring data on the micro-controller

When selecting the communication protocols (e.g UART, I²C and SPI), how they are implemented is important. Factors such as throughput and transfer rates are dependent on the implementation of communication interfaces. The exchange of information between the STM32 and a connected device can occur in the following 3 modes: polling, interrupt and DMA mode [51]. Selecting the correct transfer mode for an application is important for streamlining the data transfer process over the interface. The 3 modes operate as follows:

Polling mode is also known as “blocking” mode because this mode “blocks” the main function until the transfer command is satisfied with the data requirements such as the size or length of data. This transfer mode should be implemented in cases where a high transfer rate is not a priority in the main function.

Interrupt mode is also known as “non-blocking mode” because it allows the main function to continue running, while the data transmission is happening. This mode triggers an interrupt after the completion to inform the rest of the program of the completed transmission. This is well suited for applications with randomly timed data transmissions or transmission speeds relatively slower than the other operations on the MCU [51].

DMA stands for “direct memory access”, meaning that the peripheral data can bypass the CPU, and write or read directly onto the internal memory. This mode allows communication interfaces to be used at their fastest transfer rates, providing the best data transmission throughput [51]. This is the best mode for high-speed communication, while the CPU continues with other tasks.

4.2.3 Timers and timer interrupts

A timer, also referred to as a counter, is a piece of hardware in many micro-controllers that counts up and down. They count up to a certain counter period that is restricted by the counter resolution; for example, a timer with a counter resolution of n -bits can only count up to $2^n - 1$ ¹. Timers are widely used to write non-blocking code, track execution time, and control the toggling of a pin. Furthermore, timers can be used in conjunction with interrupts to write functions outside of the main function.

The Nucleo-F334R8 has seven 16-bit and one 32-bit timers available, of which three 16-bit timers are implemented in this application. Each 16-bit timer can count from 0 up to 65535 (max), before rolling over to 0. This counter period can be changed to achieve a desired timer counting rate. Additionally, a pre-scaler value can also be set to further adjust the duration of the counting rate. The pre-scaler is a value that divides the system clock frequency (*sysclk*), to make the timer tick at a slower rate. The counting rate (in seconds) refers to the time taken from 0 to roll-over; and it is calculated using equation 4.1.

$$CountingRate = CounterPeriod * \frac{Prescaler}{Sysclk} \quad (4.1)$$

¹Value is can be written in a notation with a deducted 1 because we start counting from zero

For this program, TIM3, TIM16, and TIM17 are used. Each of the three timers has a different function. The ADC's sampling rate is triggered by TIM3, TIM16 is used to average samples at the frequency rate, and the LED display is toggled according to TIM17 triggers. The values chosen as the pre-scaler, the counting period for each timer is shown in Table 4.2. Knowing that the sysclk for this project is 64 MHz, the counting frequency is also calculated in the table.

Timer	Pre-scaler	Counter period	Counting rate	Counting freq.
TIM3	64-1	20-1	18.7 μ s	53.465 kHz
TIM7	6400-1	2000-1	200 ms	5 Hz
TIM16	6400-1	100-1	9.898 ms	101.025 Hz
TIM17	6400-1	50000-1	4.999 s	0.2 Hz

Table 4.2: The settings for the timers implemented on the micro-controller

The values provided in Table 4.2 are motivated for in the section in which the TIM is applied (See Section 4.2.4 and Section 4.2.8.2).

4.2.4 ADC on STM32F334R8

The Nucleo-F334 board comes with two 5 MSPS embedded 12-bit ADCs with a total of 21 channels across both ADC1 and ADC2. The ADCs can be used in either independent mode, or in dual mode whereby they are synchronised to work together. Furthermore, the ADCs can be set up to implement various conversion modes, for example, single-shot mode, continuous mode, circular mode and scan mode [49].

For this project, the four receiver output channels need to be sampled. To select the minimum sampling frequency, the Nyquist theorem is generally exercised. Furthermore, the signals expected from each channel differ according to the various protocols of the technology discussed in Chapter 2. To obtain the Nyquist sampling frequency, each channel's highest frequency component is inspected. The highest frequency component is deducted from the shortest data transmission burst and displayed in Table 4.3.

Channel	Protocol	shortest t_{burst}	fastest frequency	$f_{nyquist}$
1	GSM	577 μ s	1.733 kHz	3.466 kHz
2	2G	577 μ s	1.733 kHz	3.466 kHz
3	3G	1 ms	1 kHz	2 kHz
4	BLE	40 μ s	25 kHz	50 kHz
	Wifi	25 μ s	40 kHz	80 kHz

Table 4.3: Nyquist frequency for each channel to be sampled

A sampling frequency of 50 kHz is selected because

1. It is well above the Nyquist frequency of the first three channels, meaning that they will be oversampled.
2. It perfectly matches the Nyquist frequency of the BLE component.
3. Given the asynchronous nature of Wi-Fi, even though it is 50 kHz below the $f_{nyquist}$, it will still be detected within the window over which it is averaged for data reduction.

The sampling rate is controlled by a timer, the TIM3 interrupt, which was described above. This is in the effort of achieving as accurate samples as possible. Note that, because using rounded numbers to configure the timers, the sampling rate ended up being 53.465 kHz. This is slightly higher than initially planned and it also satisfies the sampling rate requirements. The TIM3 interrupt is triggered at a rate of 53.465 kHz and scans all four ADC channels simultaneously. As a result, each channel is sampled at a rate of 53.465 kHz. These samples are temporarily kept in a circular buffer.

The ADC is set to have an 8-bit resolution, which results in 256 quantisation steps for the 3.3 V range. This translates to a sampling accuracy of 12.8 mV/step, which is sufficient for this project. Also, having a lower resolution results in faster ADC sample conversion times. Furthermore, an 8-bit resolution is preferred since it allows for more measurements to be stored in less time and requires less SD card storage than greater resolutions.

Data reduction is a necessary step to avoid having to keep an unreasonable amount of data. The sampling frequency is set to a value that assures changes in power in each signal channel are consistently detected; yet, for an end-user, each sampled value is not necessary. Instead, an averaging window of about 10 ms is chosen to collect data over the defined threshold. The averaging window is regulated by TIM16, see Table 4.2 for the exact times. Instead of 53.456 kHz, data is transferred to the storage buffer at a rate of 101 Hz. It should be noted that each channel has a distinct threshold that is determined by the noise floor measured in Section 3.8. As a result, only values that are strictly above the threshold are averaged, and even if only one value over the threshold is identified in the average window, it is preserved.

4.2.5 Time controlled LEDs

LEDs are utilized to show the signal strength of each channel, using the averaged ADC samples. For power levels 1 through 4, which are each a quarter of the 3.3 V range limit, it uses four LEDs to show signal intensity. Another set of four LEDs is used to indicate the RF channel that is currently displayed. The signal strength from all four channels cannot be examined at the same time; this would necessitate more GPIOs and, presumably, would be untidy due to the abundance of cabling. TIM17 controls the frequency channels, which alternate. As a result, the signal strength of an alternate channel is presented every 5 seconds.

4.2.6 Position tracking data

Position tracking has become a complementary feature on most modern mobile technologies to provide navigation, time, speed or position. In the case of this project, it is required for tracking the position and time of the data measured by the RFIPD. This allows one to determine the positions of measurements and greatly narrows down the search area of an RFI source. Therefore, the RFI team will have a smaller region to search for and remove the RFI source using their bakkie and RTA system.

A satellite navigation (satnav) system refers to a constellation of satellites that work together to provide the geospatial position of a receiver. Satnav has evolved from primarily being military instrumentation to becoming a commercial and consumer accessible technology that allows anyone with a receiver to receive this satellite data. Some of the most commonly known and used satnav systems include the United States Global Positioning System (GPS), Russia's Global Navigation Satellite System (GLONASS), China's BeiDou Navigation Satellite System (BDS) and the European Union's Galileo. Nowadays, however, receivers are not necessarily restricted to receiving data from only one satnav system. Global Navigation Satellite System (GNSS) encompasses all the satnav systems, and therefore allows receivers to receive from a combination of constellations of satellite systems. Using multiple satnav systems simultaneously provides improved accuracy and availability at all times.

All GNSS signals are transmitted in the L-band (1–2GHz), which is divided into 5 narrower bands. Each satellite transmits multiple signals in different frequency bands [52]. Satellites are continuously transmitting signals which hold navigation messages relating to their position in orbit and time. The signals are demodulated by the receiver and through trilateration, receivers compute their position. The receiver can then pass this information to other connected devices. There are multiple standards to transmit data computed by the receiver to relay various types of GNSS information. The National Marine Electronics Association (NMEA) standard has become the most popular because it uses ASCII messages which are human-readable, and the data format provides a convenient way to read GNSS data.

All NMEA messages begin with a \$ and a message ID. The message ID is made up of a talker identifier and a sentence format key. The “talker identifier” indicates the satnav system used, meanwhile the sentence format key defines the content of the data fields in the message. The message ID is followed by comma-separated data fields and then an asterisk indicates the end of the data fields. The asterisk is followed by a checksum value which is a hexadecimal result of the XOR of all the preceding characters (except for the \$ and *). The message is terminated with a carriage return and line feed character.

All the position, date and time data required in this project are available in the data fields of NMEA messages with “\$GNRMC” message ID, whereby the GN indicates that the project receives GNSS signals. This is therefore the only NMEA string of interest for the timestamping of measurements in this project.

The following is an example of such a “\$GNRMC” NMEA message:

```
$GNRMC,083559.00,A,4717.11437,N,00833.91522,E,0.004,77.52,091202,,A,V*57\n\r
```

Name	Format	Example data
Message ID	string	\$GNRMC
time	hhmmss.ss	083559.00
status	character	A
latitude	ddmm.mmmmm	4717.11437
NS	character	N
longitude	ddmm.mmmmm	00833.915
EW	character	E
spd	numeric	0.004
cog	numeric	77.52
date	ddmmyyy	091202
mv	numeric	-
mvEW	character	-
posMode	character	A
navStatus	character	V
cs	hexadecimal	*57
<CR><LF>	character	-

Table 4.4: Example of NMEA message structure for when the message is \$GNRMC

The GNSS module produces NMEA strings of output every second (1 Hz). For this project, NMEA messages are read over UART at the default baud rate of 9600bit/s. After each character is read, the UART interrupt handle is called to see if the \$ starting character has been received again and the GNSS buffer begins to fill. As the buffer fills, a checksum is performed to ensure that the message ID is valid. Before the data fields may be used, both of these must be valid. As previously stated, just the string with the message ID "\$GNRMC" is saved. The time and date fields are used to establish the Nucleo board's Real-Time Clock (RTC). Furthermore, the other fields will be used in post-processing, therefore they must be saved.

4.2.7 Real-time clock

A real-time clock (RTC) is a device used in micron-controllers to keep track of track of time and date. In this application, the RTC is set using the time and date data from the GNSS receiver. When GNSS data is unavailable, such as inside a building or in overcast weather, the RTC is set to the default time and date of January 1, 2000, at midnight. The RTC's date is used to create the filename for the data file, ensuring that measurements from each day are saved in a separate file. The format of the data file is explained in detail in subsection 4.2.8.2. Furthermore, the RTC's time is used to log timestamps in the data file stored on the SD card, it is therefore critical that the time is kept precise. The ticking rate is determined by what source it is connected to. The Nucleo-F334R8 board has two options of using either a 32.768 kHz crystal or a 40 kHz RCL network as the source for the RTC. A comparison was conducted of how accurately the RTC kept to a smartphones clock, when using the two different sources, with the results provided in Table 4.5.

Table 4.5 compares the time recorded on a phone to the time recorded on the Nucleo-F334R8's RTC using two different sources. The RTC time using the 40 kHz source deviated over two minutes from the correct time after five minutes. The 32.768 kHz

Device	Duration
Phone clock	5:00 minutes
RTC with 32.768 kHz	5:01 minutes
RTC with 40 kHz	7:02 minutes

Table 4.5: Comparison of the accuracy of implementing the RTC with the 32.768 kHz source and 40 kHz source

crystal source, on the other hand, has only diverged by about one second from the correct time. This one-second difference is insignificant and is most likely attributable to a poor reaction time when the clock is stopped. Therefore the RTC was implemented, with the 32.768 kHz source.

4.2.8 Memory and storage

Understanding the memory addressing is important when handling data processing systems. Selecting the appropriate memory for data takes into consideration the storage capacity, and required speed of the memory technology.

Memory is classified as either volatile or non-volatile. Volatile memory describes memory that needs the power to retain data stored, for example, random access memory (RAM), static-RAM (SRAM). Alternatively, the non-volatile memory will retain data stored even when the power is off, for example, read-only memory (ROM), electronically erasable programmable read-only memory (EEPROM), flash etc. Both volatile and non-volatile memory is incorporated in this project. The storage in this project is discussed as primary and secondary memory in the following subsections.

4.2.8.1 Primary memory in micro-controller

Primary memory in a system refers to the memory embedded in the Nucleo-F334R8 micro-controller, as illustrated in Figure 4.1. As a result, the processing unit has direct access to primary memory. The Cortex-M4 core processors implement a Harvard memory architecture, meaning that they have separate memory and pathways for storing data and program instructions. The cortex has a total of 4GB of address space which is divided linearly toward program memory, data memory, registers and I/O port, of which there are up to 12 Kbytes of SRAM and up to 64 Kbytes of flash memory available. Figure 4.4 shows how much of each memory was used for this project. It has limited some features of the program, such as the naming of the data file which will be discussed in the section to follow.

Data generated during runtime, for example, variables require fast retrieval times from memory, therefore they are stored in the SRAM. Static random-access memory is a fast type of RAM, which can be addressed as fast as the maximum clock frequency. Additionally, SRAM can be directly accessed by the CPU and the DMA bus with minimal waiting periods.

The program memory must be non-volatile to retain the program regardless of the state of the power supply. The flash memory stores the actual program by setting the

Region	Start address	End address	Size	Free	Used	Usage (%)
CCMRAM	0x10000000	0x10001000	4 KB	4 KB	0 B	0.00%
RAM	0x20000000	0x20003000	12 KB	184 B	11,82 KB	98.50%
FLASH	0x08000000	0x08010000	64 KB	6,33 KB	57,67 KB	90.11%

Figure 4.4: Screenshot of memory regions used in the micron-controller.

Flash memory addresses	Size (bytes)	Name
0x0800 0000 - 0x0800 07FF	2K	Page 0
0x0800 0800 - 0x0800 0FFF	2K	Page 1
0x0800 1000 - 0x0800 17FF	2K	Page 2
⋮	⋮	⋮
0x0800 F000 - 0x0800 F7FF	2K	Page 30
0x0800 F800 - 0x0800 FFFF	2K	Page 31

Table 4.6: Primary flash memory organization

micro-controller boot address equal to that of the flash memory. Flash memory is a special type of EEPROM with fewer limitations on how to read/write to either a single block of memory or a set of blocks of memory. Table 4.6 shows the addressing of the flash memory in the processor and how 64 KB is divided into 32 blocks of 2 KB “pages”. The program is stored from Page 0, taking up a variable number of blocks depending on the program size. This leaves a few blocks towards the bottom still available. The purple block in table 4.6 indicates the block used to store the last operating mode of the RFI detector to be retrieved during the next time the micro-controller is switched on. The different modes are discussed in detail in Section 4.3.1.

4.2.8.2 Secondary memory - SD card

Secondary memory refers to storage that is not connected directly to the processor. Secondary memory is added because the storage capacity of the primary memory is not sufficient for the storage requirements. The following items must be stored as part of the project’s storage requirements:

1. ADC data of the four channels that have been averaged across a 10 ms window is required for the project. Since there are only four 8-bit values, this array is updated at a rate of 400 Bytes/s.
2. GNSS data that is saved in an 8-bit array with a length of 75 bytes. The minimum time it can take for a new array to be filled is 1 s (the same as how often GNSS modules transfers a set of NMEA strings). This means that the GNSS array is filled with new data at 75 Bytes/s.

An SD card is connected as a form of secondary flash memory dedicated to storing the ADC and GNSS data.

Types of SD cards

There is a wide variety of SD cards, each with varying specifications relating to the storage capacity and read/write speed ratings. There are four data storage capacity families, namely, SD (64 MB to 32 GB), SDHC (4 GB to 64 GB), SDXC (8 GB to 1 TB) and SDUC (2TB to 128TB). The storage capacity can be matched with different speed ratings depending on the card's bus interface. The speed rating is an indication of the maximum transfer rate of the bus interface which ranges from 12.5MB/s default speed to an impressive 624MB/s available on the UHS-3 bus interface. However, these speeds are not guaranteed transfer speeds, therefore it is important to consider the class speed as which is the minimum sustainable read/write speed on the card.

SD card file systems

Data is stored and organised on an SD card according to the selected file system, for example, NTFS, ext3, FAT file systems. The file system on a particular device is set when formatting the storage device. It divides the storage space into smaller virtual compartments called clusters. These clusters can either be occupied with data, empty or corrupt. The purpose of a file system is to control/manage the way files are named, the directories, the access to files and the available space of a storage device. The options of file systems available are dependent on the type of operating system (OS) and the storage device is formatted.

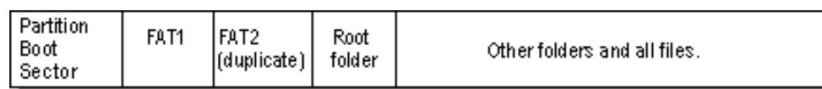


Figure 4.5: File Allocation Table(FAT) file system layout structure

The most popular file system for small flash devices such as memory cards, and USB sticks is the FAT file system (FatFs). FatFs divides clusters into sectors of typically 512 or 1024 bytes, depending on the volume size. The first sectors are reserved for information regarding the file system and stored data. Figure 4.5 shows a generalized layout of FatFs, where the boot loader code occupies one or more sectors in the first addressing location. The key/identifying feature on FatFs is the use of File Allocation Table (FAT) to keep records of which files are stored in which cluster. A second copy (FAT2) of the table is kept for cross-checking and backup in case FAT1 is damaged/corrupt. The root folder contains the directors and file names. FAT1, FAT2 and the root folder each must have fixed locations that the boot sectors can access with ease. Most of the storage is used for keeping the files and data, known as the data region. A storage device can have multiple volumes (i.e. partitions) and each partition has dedicated FAT and root folders at the starting address.

The FAT file system has various versions of the file systems named FAT12, FAT16 and FAT32 and exFAT file systems, which have been released throughout the years of increasing demand for bigger storage characteristics. Table 4.7 shows the developments made for each version regarding maximum file size, volume size and cluster size. The

	Maximum file size	Maximum volume size
FAT12	16 MB (for 4 KB cluster) 16 MB for 4 KB cluster	16 MB for 4 KB cluster 16 MB for 4 KB cluster
FAT16	2 GB	16 GB for 32 MB cluster
FAT32	4 GB	32 GB (Windows OS)
exFAT	4 EB	NONE

Table 4.7: FAT file system comparisons

exFAT may appear to be the most popular option because of the virtually unlimited storage, however, this project cannot accommodate it because the STM32 FatFs library only supports FAT12, FAT16 and FAT32. Therefore, the FAT32 file system is used which is advantageous because it is the most widely used FatFs because of its compatibility with a wide range of operating systems.

SD card on STM32-F344R8 micro-controller

A communication protocol is required for data to be transmitted between the SD card and the microcontroller. Since the Nucleo-F334R8 board only supports SD card communication over SPI, it is the protocol used as illustrated in Figure 4.1. In addition, the microcontroller can only support FATFS devices. However, the FATFS library provided by CubeMX requires additional programming. As a result, a generic FATFs library by Elm Chan [53] is downloaded and integrated into the project. This library is used to store and read data files on the SD card, list the stored files, and format the storage.

The Elm library has multiple functions for example `f_open`, `f_write`, `f_read`, `f_sync`, `f_close` and `f_mkfs` to name a few. The SD card's most time-sensitive requirement is its write speeds, which must be fast enough to ensure that all data is saved. Data should be written in 512-byte blocks or multiples thereof, according to the earlier discussion. To verify this impact and determine the writing rates to an SD card accomplished in over SPI, the execution time of writing arrays of various sizes is observed. See the outcome Table 4.8.

	Execution time	Data rate
70 Bytes	11.6 ms	6.034 kB/s
511 Bytes	11.6 ms	44.05 kB/s
512 Bytes	5.6 ms	91.428 kB/s
513 Bytes	18 ms	28.5 kB/s
1024 Bytes	5.5 ms	186 kB/s
2000 Bytes	19 ms	105.263 kB/s
4096 Bytes	9.6 ms	426.66 kB/s

Table 4.8: Comparison of the data rates achieved with different writing buffer lengths

Table 4.8 demonstrates that all the red rows (not multiples of 512) have slower data rates than the white rows (multiples of 512). As both the ADC and GNSS arrays are less

than a multiple of 512, they are merged to a larger storage array of 512 Bytes. Therefore storage array is appended every 10 ms with 4 Bytes and every 1 s with 75 Bytes. When the storage buffer can no longer be appended to, all currently stored data is written to the data file on the SD card, so that the latest data may begin filling it up again. Since the rate of 475 Bytes added to the storage buffer every second is significantly below the data rates achieved by a 512 Byte array, all of the data is stored.

4.3 Post-processing and GUI

A graphical user interface (GUI) is an effective way to allow/provide a means for users, regardless of technical ability, to communicate with the RFIPD, by using simple trivial visual queues.

The Tkinter python GUI library includes a variety of widgets to create a powerful object-oriented interface using simple buttons and other widgets, instead of changing lines of code. Figure 4.6 shows the two tabs of the RFIPD GUI.

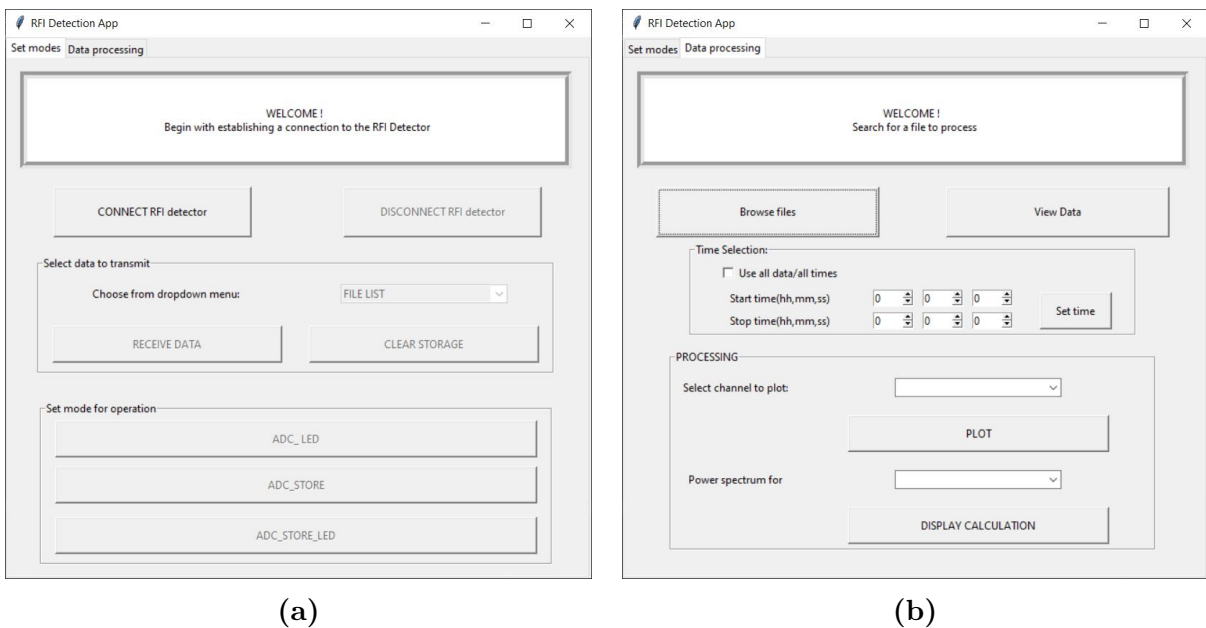


Figure 4.6: Screenshot of the two tabs in RFI Detection App, whereby (a) the first tab is related to serial communication functions and (b) the second tab is related to data processing functions.

The first tab's functionalities include establishing a connection or ending a connection with the RFIPD, download data from a selected file, and also setting the operation mode of the RFIPD. The second tab is aimed at processing the data which has been retrieved and stored on the hosting computer. These functions are discussed in more depth in the subsections which follow.

4.3.1 Serial communication protocol

The first tab includes functionalities used to connect to the RFIPD and transfer data while the RFIPD is connected. A connection to the RFIPD is established by scanning the available COM ports to find the matching port name. The baud rate for this connection is set relatively high at 38400 bits/s to promote fast communication. For communication between devices, it is good practise to create a communication protocol describing how to set up/end a connection, start/end a message, as well as how to deal with corrupt messages. A basic communication protocol of how data is formatted over the connection is described in Table 4.9. The RFIPD will only process received data that adheres to the formatting described in the table, otherwise received data is disregarded by the micro-controller.

Mode	Name	Description
\$1<enter>	ADC LED	Set the ADC to operate with only the ADC and LED array display activated
\$2<enter>	ADC Store	Set the ADC to operate with only the ADC and SD card data logging activated
\$3<enter>	ADC Store LED	Set the ADC to operate with the ADC, LED array display, and the SD card data logging activated
\$I<enter>	Information	Alert the RFID that a connection has been established and send information relating to the files available in the SD card storage
\$T<int><enter>	Transfer	Transfer the file in the position in index of <int> of the list of files previously sent
\$C<enter>	Clear	Delete the file in the position in index of <int> of the list of files previously sent

Table 4.9: Description of serial communication protocol for messages sent from the RFI Detection App to the RFIPD

All messages sent are 3 bytes long and begin with a dollar symbol. The second byte describes to function being requested and the last byte depends on the second byte. Messages are transferred over a serial connection using the commands of the communication protocol. Commands are formatted into binary to eliminate delays converting while it is transferred. The micro-controller can now be set to operate in different modes, depending on the application or the operation. The only requirement for data being sent to the PC is to end with a <enter> character so that the Python serial line reader can read the serial line like a string of characters.

4.3.2 Data Processing

The data downloaded using the first tab is read from a binary file, hence the first processing of data is a conversion back into ASCII human legible values which are saved onto the local PC as comma-delimited CSV data files. The functions available for the post-processing of the data are seen in Figure 4.6b. These functions do not require a connection to the RFIPD, because data is loaded from the CSV files saved onto the local computer. The CSV data is filtered to have a multidimensional array for the selected data format. The data in a selected CSV file is read and parsed into useful formats which are meaningful to a user to view namely ISO time, date and voltage values. This includes:

- The raw ADC values are a representation of the voltage at the ADC pins relative to the maximum readable voltage of the ADC. The raw values are converted to the equivalent voltage value using Equation 4.2 and stored in a 2D array

$$V = \frac{ADC_Value}{2^{Resolution_bits}} * V_{max} \quad (4.2)$$

- The NMEA string provides the date and time in a ddmmyy and hhmmss.xx format. Using python's datetime class, this can be changed into the common ISO 8601 format time format, including more information such as the UTC zone information. Furthermore, more timestamps are created for the many ADC values between each NMEA string
- The latitude and longitude data is presented to the user with the along with the corresponding timestamps and samples in the form of a CSV.

These values are used to perform the following functions:

Line graph plot This provides a visual representation of the power detected over a selected time frame for each frequency channel individually or simultaneously. Patterns of recurring signals can be identified through the observation of the time graph.

Calculate Average and Max power Feedback on the power levels read in are displayed relating to the power vs voltage graph in the datasheet of the power detector

Time occupancy Feedback on the time occupancy of signals above a given threshold is given. Gives an idea of how often RFI is detected for a given time frame.

The operation of these functions is presented in Chapter 6 where the RFIPD's functionality is tested.

4.4 Conclusion

As the RF front-end captured signals in Chapter 3, the RF signals must be signal processed to extract useful information from the signals. This Chapter covered all of the stages of signal processing, including data acquisition and data processing. Signal processing is a critical stage in this project to ensure that the third research goal is met. This establishes a system for data interpretation by providing the data to the user visually.

Chapter 5

System integration

The process of configuring all of the different elements required by the RFIPD to generate one coherent system is referred to as system integration. So far, the RF receiver and the signal processing system have been discussed as core elements of the RFIPD development. However, for a completely functional RFIPD, these two pieces must be powered, have a way to link and communicate, and much more. This chapter describes the RFIPD's sub-circuits, followed by their integration onto a single circuit board, and concludes with the design of the enclosure that houses all of these pieces.

5.1 Sub-circuits

The term "sub-circuits" refers to the circuitry required to support the cohesive operation of the RFIPD's RF receiver and signal processing system. These sub-circuits are used to:

1. Distribute the power in the RFIPD
2. Support a USB connection and communication between the RF receiver and PC software
3. Support data storage on an SD card
4. Provide location and timestamp data that will be stored

They are an important part of the configuration of the functionality of the RFIPD. This section discusses the attributes and design concerns of the sub-circuits, as well as how they integrate into the RFIPD.

5.1.1 Power distribution

The power supply unit is an essential part of any electronic system. It is important to ensure that enough reliable power (i.e. voltage and current) can be consistently delivered to maintain a fully operational system. Electronics usually require a constant voltage value; meanwhile, the current demand is dynamic and prone to fluctuations. A voltage regulator is a component used to ensure a stable voltage signal is supplied regardless of changes in the power supply or change in the load's current demand. The two main types of voltage regulators are linear and switching voltage regulators.

Linear voltage regulators are based on using a differential amplifier to manage the difference error between the input power supply and the reference voltage. This error voltage drives a transistor pass element, and therefore adjusting the effective resistance of the transistor. This creates a voltage drop proportional to the resistance and the wasted energy is dissipated as heat in the pass transistor. This is an inefficient way to transform the power because more power is wasted as the voltage drop increases or when more current is drawn. Linear regulators can consequently only perform step-down DC-DC conversion. Therefore, there is a minimum dropout voltage of usually 2V, needed to achieve the conversion. However newer linear voltage regulators have been designed to minimize this value to have a low dropout voltage (LDO).

Switching voltage regulators consist of four main components, namely capacitor, inductor, diode and transistor. The capacitor and inductor are used to store energy when connected to power, then discharge the energy through the load when power is disconnected. The diode controls the direction of the flow of the current. The transistor is used as a switch by operating it only in its off or saturation region. In off-mode, there is no power used and there is a negligible voltage drop across the transistor when it is in saturation mode. This is the more effective use of the transistor because minimal power is wasted and dissipated in the transistor. Therefore, switching voltage regulators are more power-efficient than linear voltage regulators.

Furthermore, the rate of the switching is controlled by a feedback loop oscillation device, commonly known as a pulse width modulator (PWM). The PWM adjusts the duty cycle of the transistor's switching rate (the ON time) depending on the voltage. This makes sure that the switch is on for a minimum duration whatever the case is and less power is wasted. This is how the output voltage is maintained stable, however, the high-frequency switching is a source of potential EMI and noise. This can create a ripple in the output signal.

Additionally, the switching regulators have more flexible possibilities of output voltages, given the same voltage input. Connecting the different components, 3 topologies can be achieved - buck, boost or buck-boost regulator. For controlling the frequency and duty cycle, the buck converter outputs a voltage less than the input voltage, the boost converter has an output voltage higher than the input voltage and the buck-boost can have a higher or lower output voltage than the input voltage.

5.1.1.1 Selecting a voltage regulator

The power for this project is regulated by NCV4274c LDO linear voltage regulators from ON Semiconductor manufacturers. The NCV4274c protects against short circuits, reverse battery/polarity and thermal overload conditions. This regulator delivers 5V with a low dropout voltage of 0.5 V and an output current capability of 400 mA. To ensure that the overall current demands of the system are met, two NCV4274c regulators are used to independently power the major sub-systems, i.e. RF receiver and NUCLEO-F334R8 board.

The first of the NCV4274c regulators is dedicated to delivering power to the receiver. The RF receiver mainly consists of passive components with only the LNA and power

detector requiring power to operate. The receiver LNA and power detector draw a maximum of 25 mA and 36 mA, respectively. Independently, it may not appear to be much, but altogether it accumulates across to the multiple RF channels and the full RF receiver is expected to draw a maximum of 169mA.

The other NCV4274c voltage regulator is used to supply power to the micro-controller on the NUCLEO board. The micro-controller operates on 3.3 V logic voltage, however, the NUCLEO board has a few 5 V tolerant I/O pins. One of the 5V tolerant pins is the external voltage supply pin through which the micro-controller is powered. The board draws approximately 100 mA in RUN mode, however, it can draw up to 300 mA when the USB is connected for either communication, programming the micro-controller or debugging. This excess current serves the purpose of USB enumeration, to detect, identify and upload the drivers necessary. Furthermore, the micro-controller has a regulated 3.3V output with a maximum current of 500 mA, which is used to the power GNSS receiver circuit, and SD card connector circuit.

5.1.1.2 Selecting the power supply

The power supply, preceding the voltage regulators must be portable and deliver the required power to the regulators without exceeding the maximum power ratings of the regulators. Batteries are a common choice for low voltage electronic projects such as this one due to their portability and general availability. In addition, they are generally a low ripple voltage source, which makes them suitable for analogue RF applications as well. The battery's characteristics such as material type, voltage, capacity, energy- and power density, as well as charge/discharge cycles have to be considered for each application as they have a significant influence. There is an endless list of types of batteries and characteristics such as the lifetime, energy capacity, power capacity and size that need to be taken into consideration for each application. The suggested battery for the RFIPD is a 6V rechargeable lead-acid battery with a 4.5 Ah nominal capacity. This battery is suited for this application given its ability to operate in extreme temperatures found in the Karoo, and they're readily available locally. Furthermore, they have higher power density (the amount of power (time rate of energy transfer) per unit volume) but a low energy density (the amount of energy stored per unit volume). This is an acceptable trade-off given that it is rechargeable.

5.1.2 SD card connector slot

SD cards are available in 3 different sizes, namely Standard SD (32.0×24.0×2.1 mm), Mini SD (21.5×20.0×1.4 mm) and MicroSD (15.0×11.0×1.0 mm). The MicroSD card slot has the smallest form factor therefore it is used in the project to minimize board space usage. A micro SD card with normal, high-speed or UHS-1 bus interface uses a single row of 8 I/O pins. Additionally, a new pin layout was designed for SD cards with UHS-2 and UHS-3 bus interfaces, whereby an additional row of I/O pins are located below the standard first row. Therefore, to maximize the speeds achievable with the UHS-2 and UHS-3 bus interface, the memory card connector should be aligned with the new 2-row pin layout. Furthermore, an 8-pin connector can pin used, however, the data transfer speed will be limited to normal, high speed or UHS-1 bus ratings. In this project this is sufficient speed, therefore an 8-pin connector is used.

Figure 5.1 shows the I/O pins available for the standard SD card as well as the mapping for communication over SPI. There are six communication channels (clock, command and four data lines), however, in SPI mode only 4 of the 6 communication pins/channels are required. The STM32f334r8 board supports FATFs for SD card only over SPI.

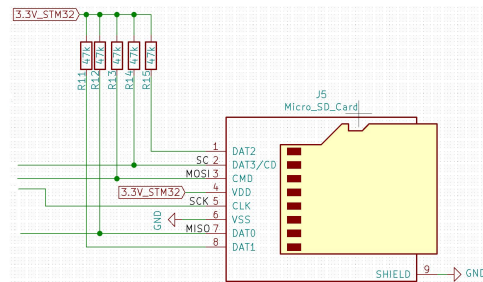


Figure 5.1: Schematic diagram of SD card peripheral

The microSD card operates on a 2.7-3.3V supply and is powered by the micro-controller. Each pin is connected directly to a corresponding pin on the micro-controller. In SPI mode, DAT1 and DAT2 don't have connections, meaning that they are floating pins. Leaving these as floating pins means that a floating, random signal is at those pins which can affect the normal functioning of the SD card. This is avoided by using pull-up resistors of $47\ \Omega$ to have a constant value for the pin. Pull-ups are not necessary on SPI traces, but because of the long lengths, pull-ups are used to clean up the signal transitions. The pull-up resistors create definitive values for the pins when there is no data transmission. This is with the exception of the CLK pin because the high speed and short rise/fall time on this pin is very sensitive and a pull-up resistor may cause distortion.

5.1.3 USB interface

This project requires data to be transferred from the SD card to be transferred to a computer for post-processing. The SD card data is transmitted using the micro-controller's UART and computers receive over USB communication. The two communication standards are summarized below:

Universal Asynchronous Receive Transmit (UART) sends data using a TX/RX line of device1 connected to the RX/TX line of device 2. It does not use a clock to keep the devices synchronised, alternatively, a transfer speed is known as baud rate to be the same on both devices to ensure that data arrays are sent and received at the same rate.

Universal Serial Bus (USB) sends and receives data using a twisted-pair, labelled D+/- . Devices connected via USB have to undergo USB enumeration before data packets can be exchanged. USB enumeration refers to the process of a computer detecting the USB connection and loading the necessary drivers. Each information packet begins with an identifier that is used in the enumeration process to identify the device and upload the necessary drivers.

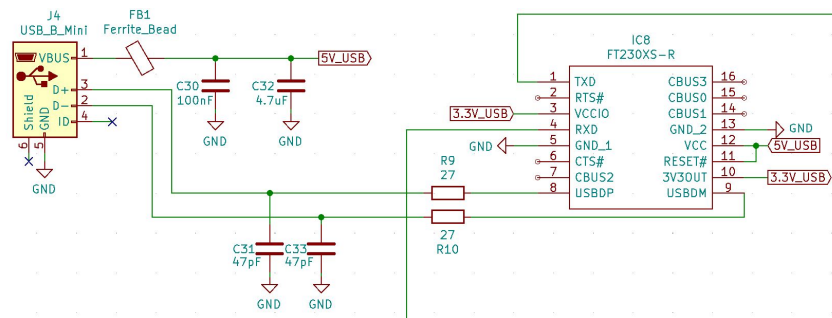


Figure 5.2: Schematic diagram of USB peripheral

These are incompatible technologies, therefore the USB to UART interface is required. A USB to serial UART interface is used to bridge the difference in communication standards. It camouflages itself as a serial port on the computer. The FT230XS chip from the FTDI chip is used to translate USB to serial UART and vice versa. There are many commercial manufacturer competitors, however, FTDI devices are preferred because their devices enumerate automatically. Additionally, FTDI drivers are available for free will usually automatically download once the connected device is identified.

The FT230XS sub-circuit is only powered when it is the detector is connected to the PC for data transfer. The computer USB port supply 5V with a current limit of 500mA. A ferrite bead is added to the power line to block and potential EMI from leaking towards the computer. In addition, care is taken to use a cable with ferrite beads on it to protect the RFIPD from EMI coupled into the cable.

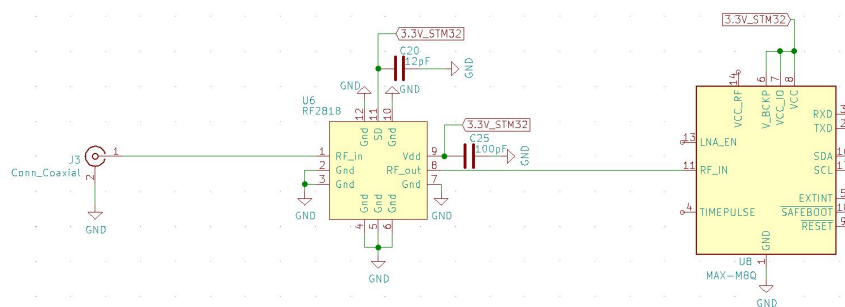
5.1.4 GNSS receiver

A receiving antenna and a receiver module are the basic components of any GNSS receiver system. Numerous criteria are considered when designing a GNSS receiver system for varying applications. Such criteria include size, power, accuracy, multi or single-band systems, etc.

Many receiver modules are designed with an integrated antenna, which allows for a more compact design and a shorter transmission line which implies fewer losses. For this project, however, an integrated antenna is not feasible because the receiver is enclosed meaning that no GNSS signals would reach the module's integrated antenna. For this reason, an omnidirectional monopole GNSS antenna from Taoglas (part no. TaoTS.07.0113) is used to receive position signals. It is a passive antenna, with a similar design to the RF receiver front-end antenna. Since it is a passive antenna, the RF2818 LNA from RFMD is added to the signal chain to provide gain. Additionally, the approach of using a passive antenna with an LNA is typically more cost-effective and simpler to design than an active antenna. The specifications of both the antenna and LNA are in Table 5.1.

The selected LNA is titled a "GPS LNA", however, the bandwidth covers the full GNSS L1 band therefore, GNSS data is received as well. It comes with SAW filters at the input and output filters which suppress noise and therefore improve sensitivity. The high gain, and low noise figure and integrated filters result in high performance in a very compact LNA.

Parameter	Specification
Antenna	
Frequency Band	1561 – 1660 GHz
LNA	
Bandwidth	1500 – 1600 MHz
Noise figure	1.55 dB
Gain	15-17dBm

Table 5.1: GNSS LNA and antenna**Figure 5.3:** Schematic diagram of GNSS tracking sub-circuit

Once the signal is captured by the antenna-LNA combination, it is transmitted to the receiver module that handles the task of processing the satellite signals into information relating to its position and time. Considering the need for a GNSS receiver module that uses an externally connected antenna and knowing u-blox to be a reputable and reliable developer of receiver modules, the MAX-M8Q was selected for this project. This module has a position accuracy error of 2.5 m, which is enough to narrow down the location of an RFI source for the RFI team. Additionally, it can achieve a refresh rate of 18 Hz, however, it is used with a 1Hz refresh rate because 1-second updates are sufficient for this project.

5.2 Printed circuit board design/layout

A printed circuit board (PCB) is designed to host the RF front-end circuit as well as all of the sub-circuits discussed in Section 5.1. This PCB is active with a variety of signals, including RF signals, digital signals, and DC signals. The complete circuit schematic can be seen in Appendix B. The PCB was designed in Ki-cad, manufactured by WH Circuits and assembled by Circor and Mr Arendse at Stellenbosch University.

The PCB was designed on two copper layers, with an FR4 substrate between. This is a commonly used substrate, because of its durability, as well as its resistance to moisture and fire. The border outline of the board is not a common design, because the PCB was designed to fit into the enclosure discussed in Section 5.3. The board has three mounting holes which align with those of the enclosure to ensure the PCB is fitted securely.

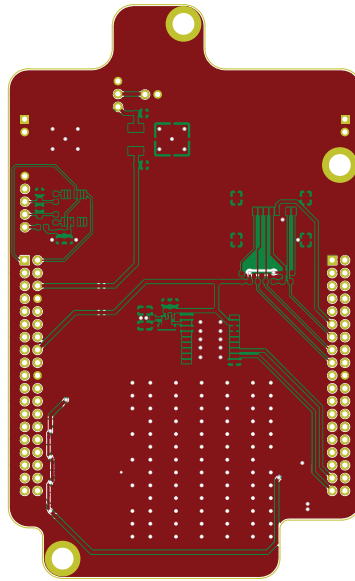


Figure 5.4: Top and bottom layer design of RFI detector PCB

A multi-layer board is necessary for routing crossing copper tracks, the top and bottom layers of the PCB are shown in Figure B.5. Furthermore, it leaves excess copper planes which are used as ground and provide easy short ground connection paths for sub-circuits. In the effort of having a ground connection near an IC connector, it should be checked not to create a loop. Current flowing in a loop is susceptible to behaving like an inductor, creating an EM field which is EMI in this case. If it is not feasible to have a grounded region adjacent to an IC, then the use of vias becomes the next best option. Vias to a ground plane on the opposite layer are a useful tool to still ensure a short return current path to ground. Having a continuous ground plane adjacent to or below signal tracks is a good technique for restricting coupling. Furthermore, the mounting holes of the enclosure are used as a ground connection and when the board is mounted in with conductive screws, this creates a ground connection to the enclosure. This implies a larger ground surface area for return currents and restricts stray EMI.

The RFIPD's PCB is designed to minimize interference between different types. The RF receiver is on the bottom layer on the lower half of the board and the sub-circuits are placed on the top layer on the upper half of the board. This is to create a physical separation between the receiver and the sub-circuits to minimize interference between each other's signals. Furthermore, this separation of these sections on the board is so that there can be a ground layer on either side of circuitry as suggested above. The PCB is also constructed with pins that match the Nucleo-F334R8 board's morpho pins. Before inserting into the RFIPD PCB, the ST-Link is broken off to create space for cabling. The positioning of this is such that there is a ground plane of the PCB directly under the micro-controller. No circuitry was placed here as a precaution of having coupling with the stacked setup.

RF Signals

RF signals are very sensitive to losses in traces between components, therefore the RF front-end's traces are the first to be traced to ensure optimal routing of transmission lines. All the transmission lines are designed to be shorter than a quarter wavelength

of the highest frequency component expected in that trace. This ensures that there is minimal radiation from that transmission line. Thus the impedance of the line will have little effect on the behaviour of the load, but the load is rather affected by the impedance of the source. Impedance matching is important for preserving signal integrity in transmission lines, and since only commercial components were used, each selected component was selected under the condition of having 50 Ω impedance.

Digital Signals

There are multiple digital signals transmitted between the microcontroller and sub-circuits. The potential of emissions/radiation from digital signals depends greatly on the data rate. In the case of synchronous circuits with digital clock signals switching periodically at a fraction or multiple of the system clock frequency, they produce EMI that is narrowband with harmonics. To avoid such EMI from creeping into other signals, they should be traced physically at a distance from the other signals and have a continuous ground along the trace. Their signal integrity is preserved by making them as short as possible and avoiding sharp turns in the traces. Additionally, vias are avoided on such signals because the sudden change in direction of the path for a very high-frequency signal can cause interruptions in the data carried by the signal. However, generic digital signals that are not periodic, produce broadband noise with lower power levels, because of switching at a slower random rate. These are not as sensitive to routing as periodic digital signals.

Power Signals

Finally, power signals are traced last because they are less tricky to route. Power signals are needed to reach almost every active component on the board. To ensure that the power levels are maintained by the time the current reaches all components, it is important to reduce the amount of resistance in the power tracks. This is done by making the traces thicker than the default trace, because this creates a greater surface area for the current to move much easier and reach its destination with less resistive losses. Furthermore, the power traces are traced away from both RF signals, and digital clock signals to prevent the EMI from coupling onto the clean DC supply and making it noisy.

5.3 Enclosure

There are a variety of sizes and materials of enclosures to choose from, to best suit different applications. The RFI detector is housed in an aluminium enclosure (127 x 81 x 57mm) from Fi-box, as shown in Figure 5.5. This enclosure's role in this project is to house electronics, provide communication peripheral connectors, and act as EMI shielding. It aids in protecting the circuitry from atmospheric conditions and circuit failures caused by environmental variables.

The enclosure's electronics require a mechanism to accept input and transmit output to the PC software. Even while an enclosure should not contain any discontinuities, some, such as holes for I/O peripherals, are unavoidable. Apertures are necessary such that the user only gets access to the peripherals and power connectors because the RFIPD is powered externally.

The placement of the peripherals is slightly reliant on the PCB layout because it is preferable to place connectors close to their position on the PCB. However, this may

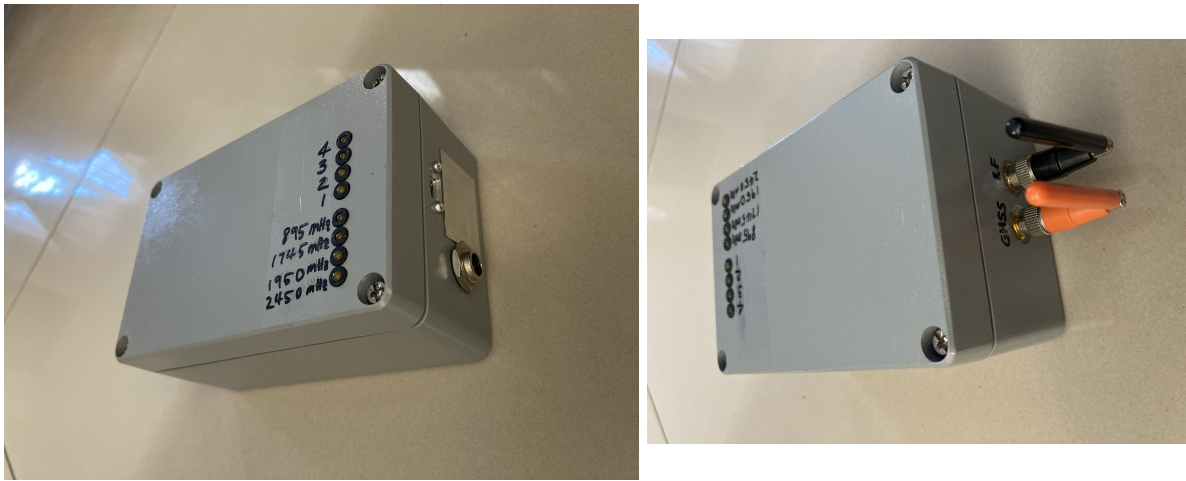


Figure 5.5: A photo of the enclosure with the RF antenna and GNSS antenna connected

not be possible to maintain a coherent design. Additionally, the aperture is designed to allow enough room for a hand or tool to bolt in the connectors. The physical positioning for the connectors and peripherals necessary to access from outside the box was designed using Auto-desk Inventor. The full dimensions of the enclosure design with the apertures may be found in App B.

Furthermore, since the enclosure is connected to ground, the effective aperture size for peripherals can be reduced by making a continuous ground connection to the connectors body. Panel mount connectors with a conductive body are typically employed so that they connect to ground as they touch the enclosure surface.

For each peripheral connector, the following design considerations are made:

- **Antenna:** Two receiver antennas are positioned next to each other using panel-mount SMA connectors. Each antenna is connected to the PCB through an SMA-to-u.FL coaxial cable connection.
- **Power:** To connect to power, a circular 2 mm power jack connector is panel mounted. To filter the incoming power, and improve the shielding because of the big aperture needed, a filter capacitor is used.
- **Switch:** The initial design includes a switch, however the switch's body is made of plastic, which prevents it from providing a continuous ground with the enclosure. Furthermore, it took up a lot of room on the interior of the enclosure and increased the cabling. Therefore, this aperture was sealed with aluminium tape.
- **USB:** A mini USB connector is securely panel-mounted with screws to the side. This connector has been set securely to withstand wear and tear from frequent cable insertion and removal.
- **LED Array:** Each LED is housed in a plastic holder; metallic holders would be preferable, but they are larger, and the present design layout did not allow enough space for them.

Care was taken when assembling to connect wires correctly. Once the PCB is mounted and all the connectors are connected, the lid is closed and only persons familiar with the interior layout and design should open. It may be opened to update the program loaded

on the micro-controller, or for maintenance.

Notably, the enclosure was found to have an environmental gasket instead when it arrived. A replacement EMI gasket was provided by staff at SARAQ to replace the environmental gasket before closing the lid. In the effort of ensuring, proper connections, the insulation coating was sanded as much as possible to make good contact electric with the metal of the lid and bottom once closed.

5.4 Conclusion

The integration of the subsystems was discussed in this chapter, describing how the mobile RFIPD was finally assembled and fitted in a shielded enclosure for evaluation. Final testing results are discussed in the following chapter.

Chapter 6

Performance of RFIPD_v00

When the RFIPD is completely constructed and mounted in the shielded enclosure, it is tested to evaluate how well it performs. Two types of testing are carried out with the goal of (1) examining any emissions generated by the RFIPD and (2) verifying the RFIPD's functionality. This chapter describes the setup of both tests, and their outcomes.

6.1 EMC Compliance Testing

EMC compliance testing for any product is important to ensure that the device will operate well in its electromagnetic environment without creating any disruptions/interference to the operation of already existing instruments in the environment. Based on the nature of the DUT, the measurements may include tests such as emissions test, immunity test, total radiated power tests, antenna radiation efficiency, shielding effectiveness, electromagnetic field tests and many more. Various measurement facilities can be used to achieve these tests, for example, anechoic chamber (AC), open area site tests (OATS), reverberation chambers (RC) and many more. Each type of facility has its advantages and disadvantages which make them optimal for some types of measurements, but not others.

6.1.1 Reverberation chamber

This project was required to emit as close to no emissions as possible and therefore the total radiated power, as well as the shielding effectiveness, are tested to ensure compliance. These tests are conducted in an RC, as explained in [54]. An RC is an indoor measurement facility made of highly conductive material which causes many reflections at the conductive boundary reflector. The functionality of an RC is based on statistical theory, which is outside of the scope of this project.

The RC at the SARAO Cape Town offices is used to conduct these tests, with the assistance of the RFI team there. It has dimensions of 5m x 3.8m x 2.78m, and it has a large zig-zag stirrer¹ which is controlled on MATLAB from outside the chamber. The layout of the SARAO RC is illustrated in Figure 6.1, showing the positions of the antenna, the stirrer and the DUT which is the RFIPD.

¹A spinning device that is used to aid improve the accuracy of measurements.

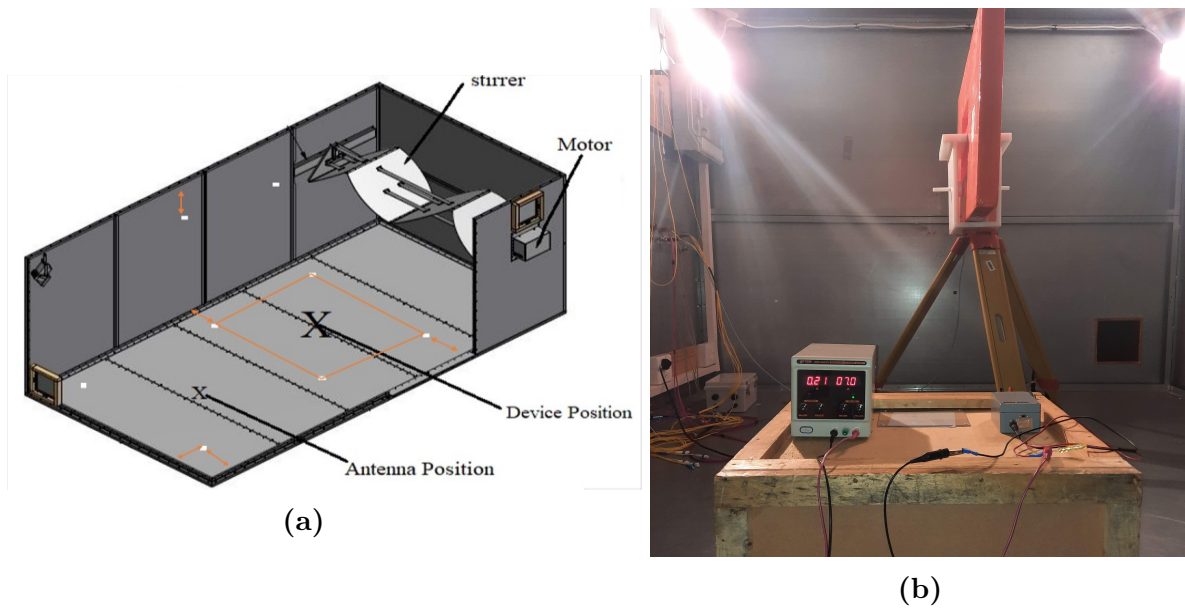


Figure 6.1: Diagram of (a) a model of the layout of the SARAO reverb chamber [55] and (b) the actual measurement setup

6.2 Measurements

The setup of the measurements are shown in Figure 6.1b. The radiation tests are conducted following the substitution method described in [54], which involves the following two steps:

1. Measuring the total power in the absence of the RFIPD, and use this as a baseline.
2. Introducing the RFIPD into the the environment and measure the received power. The total radiated power of the RFIPD can be achieved from the difference in the two readings of the received power.

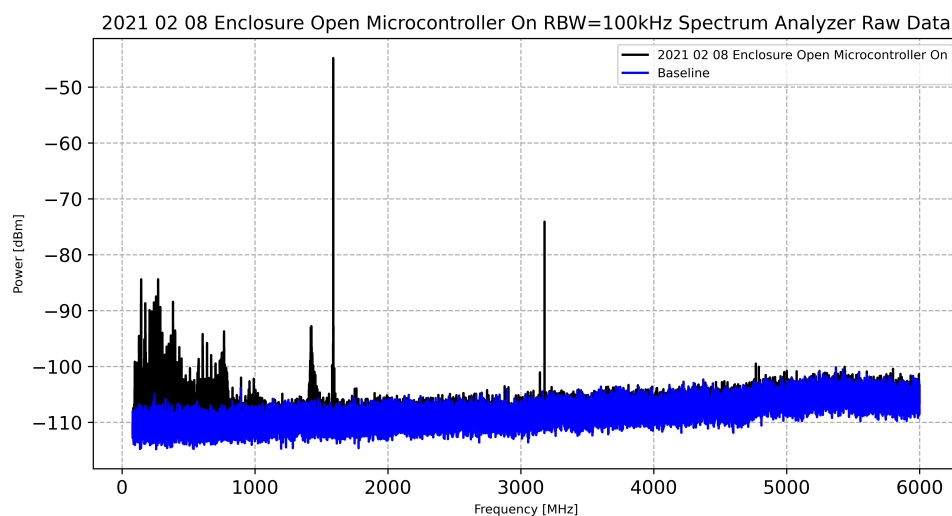


Figure 6.2: Radiated power as measured in the RC with the DUT off (blue trace) and with the DUT on (black trace) when the RFIPD enclosure is open

Using these measurement steps, the shielding effectiveness is determined by comparing the emissions test conducted while the lid of the enclosure is off, and when the lid is sealed. From Figure 6.2 it can be seen that the levels of noise from the RFIPD when the enclosure is open is mostly at low levels, except at approximately 1.58 and 3.16 GHz. This is the energy being emitted through the open enclosure. It is suspected that these emissions originate from the GNSS receiver module, as 1.58 GHz is well within the range of GNSS signal bandwidth. Furthermore, the 3.16 GHz is a harmonic of the 1.58 GHz emission.

Figure 6.2 also shows low frequency noise (below 1 kHz). This noise is classified as system noise and is generated by the micro-controller. The power levels do not exceed -80 dBm, which is an acceptable noise level for the system, because it is more than 10 dBm below the sensitivity that the RFIPD is designed to detect. Additionally, it is outside of the frequency bandwidth that is processed by the RFIPD.

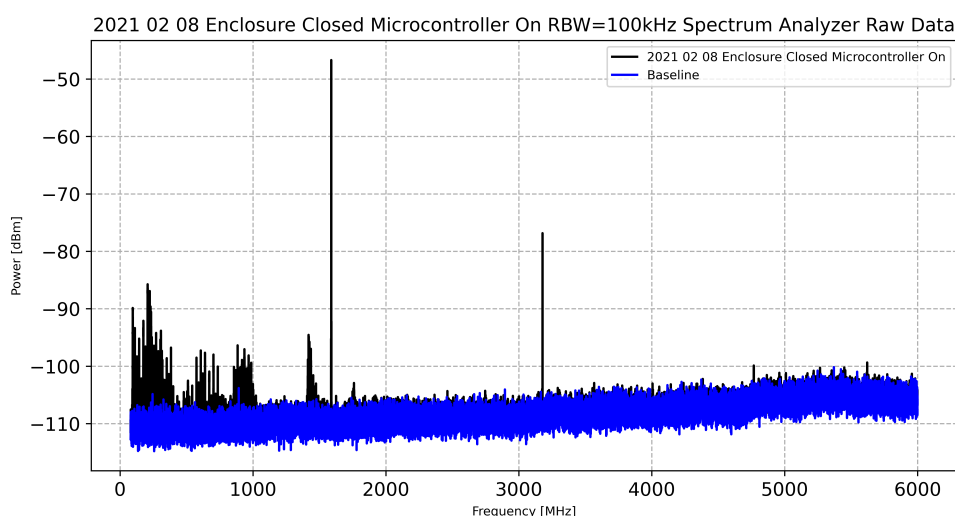


Figure 6.3: Radiated power as measured in the RC with the DUT off (blue trace) and with the DUT on (black trace) when the RFIPD enclosure is closed

When the emissions are tested with the lid of the RFIPD sealed, there appears to be just a -1 dB change in the 1.58 GHz peak. This means that the shielding is ineffective. The energy escaping from the enclosure is caused by the enclosure gasket and/or peripheral connectors not making full conductive contact with the enclosure due to the non-conductive paint coat on the enclosure. The efforts to sand the coat off were ineffective. This effectively means larger apertures via which the energy inside can radiate out.



Figure 6.4: A picture of the shielded loop probe

A shielded loop probe, as shown in Figure 6.4, was used to verify the notion that the 1.58 GHz signal originates from the GNSS receiver. This probe was designed and constructed by Dr. Kurt Coetzer from Stellenbosch University. The probe was moved across the several sub-circuits while watching the power spectrum on an oscilloscope. When hovering over the GNSS receiver, the reading would jump, implying that the noise originated over the GNSS module. This noise was coupling onto the power and causing a ripple in the 3.3 V power trace.

Further experiments with the probe were carried out with only the GNSS receiver sub-circuit powered by a DC bench supply. The noise was still present. This test ruled out the possibility that the noise was caused by other circuit paths, such as the micro-controller or the power supply, interfering with the GNSS receiver.



Figure 6.5: A picture of the RFIPD setup when enclosure is open with shielding over the GNSS receiver and the GNSS antenna removed from it's hole

Copper tape was applied over the GNSS receiver in an effort to shield it, as seen in Figure 6.5. Interestingly, this did not produce the desired result. However, when the GNSS receiver was shielded and the GNSS antenna was removed from its hole, no noise was measured, as shown in Figure 6.6. The enclosure was indicated to be working as an antenna once the antenna established a connection with it (when it was securely fixed in its hole).

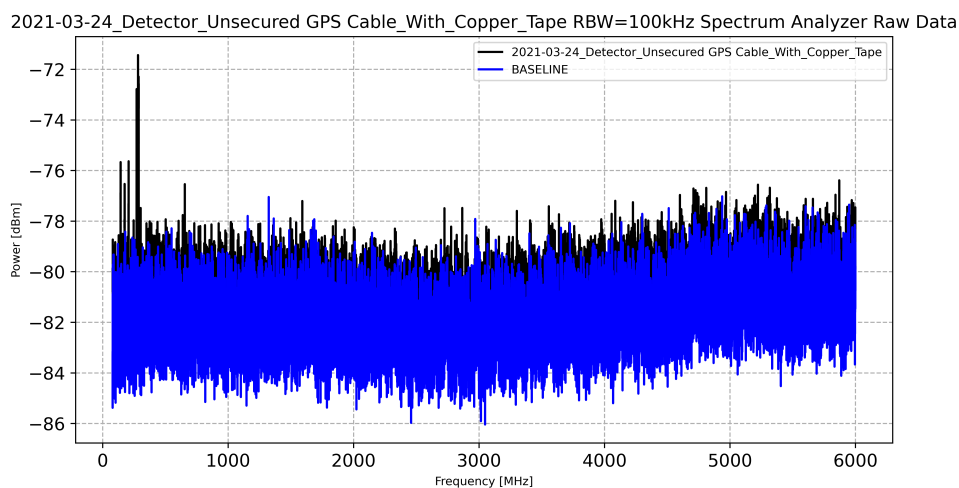


Figure 6.6: Radiated power as measured in the RC with the DUT off (blue trace) and with the DUT on (black trace) when the RFIPD enclosure is open with shielding over the GNSS receiver and the GNSS antenna removed from it's hole

Finally, after sending the board to RF Design for further examination, it was determined that the GNSS LNA was oscillating. To combat this, the layout design should have included vias underneath the IC leading to the ground layer, as well as via stitching around the footprint and GNSS receiver traces.

6.3 Functionality Tests

Functionality testing refers to a wide range of types of testing used to determine whether a system or application functions as intended. The RFIPD must go through functionality testing in order to confirm the overall operation of the system.

Up to now, unit and component testing for the RF front-end have been completed and detailed in Chapter 3. Since then, multiple different sub-systems were integrated to build the RFIPD, therefore the functionality tests also act as an integration test to ensure that all of the connected sub-systems can work cohesively together. Functionality testing is carried out to ensure that the RFIPD and PC software perform in compliance with the specifications stated in this thesis. The specification to be validated are:

- the operation of the RF front-end after integration with all other systems
- the data visualisation of time stamping during measurements
- that essential power feedback reported

The principle idea behind a functionality test is to use an appropriate input and then compare the result to the requirements or specifications. For the RFIPD, the tests comprise a frequency sweep test and a power level sweep test that are discussed in detail below.

6.3.1 Frequency sweep test

This test is conducted to see the frequency response of the channels, it shows how much each channel measures across all the frequencies. The test is done using the Rohde and Schwarz SML03 signal generator, in a step-wise setting, at a power level of -10dBm. The frequency is set to step from a frequency of 600MHz to 2600MHz, in steps of 10MHz, holding at each step for 1s. The tests are carried out in the RC to establish a controlled environment for the experiments. The signal generator cycles back to 600MHz after finishing one sweep, and is run until 1000 MHz into the second sweep, resulting in a second peak in Figure 6.7a.

The presence of coupling between channels is prominent because outside of the frequency bands set, other frequencies are picked up. This could lead to false indications of RFI within a specific bandwidth. Therefore a threshold is set to prevent any false detection. The filter shapes can clearly be seen at the correct frequencies. The rejection at the other frequencies is not as expected. The filter at 2450 MHz is not doing as well as it should, which indicates that a narrower band-pass filter would be a more appropriate choice for this application.

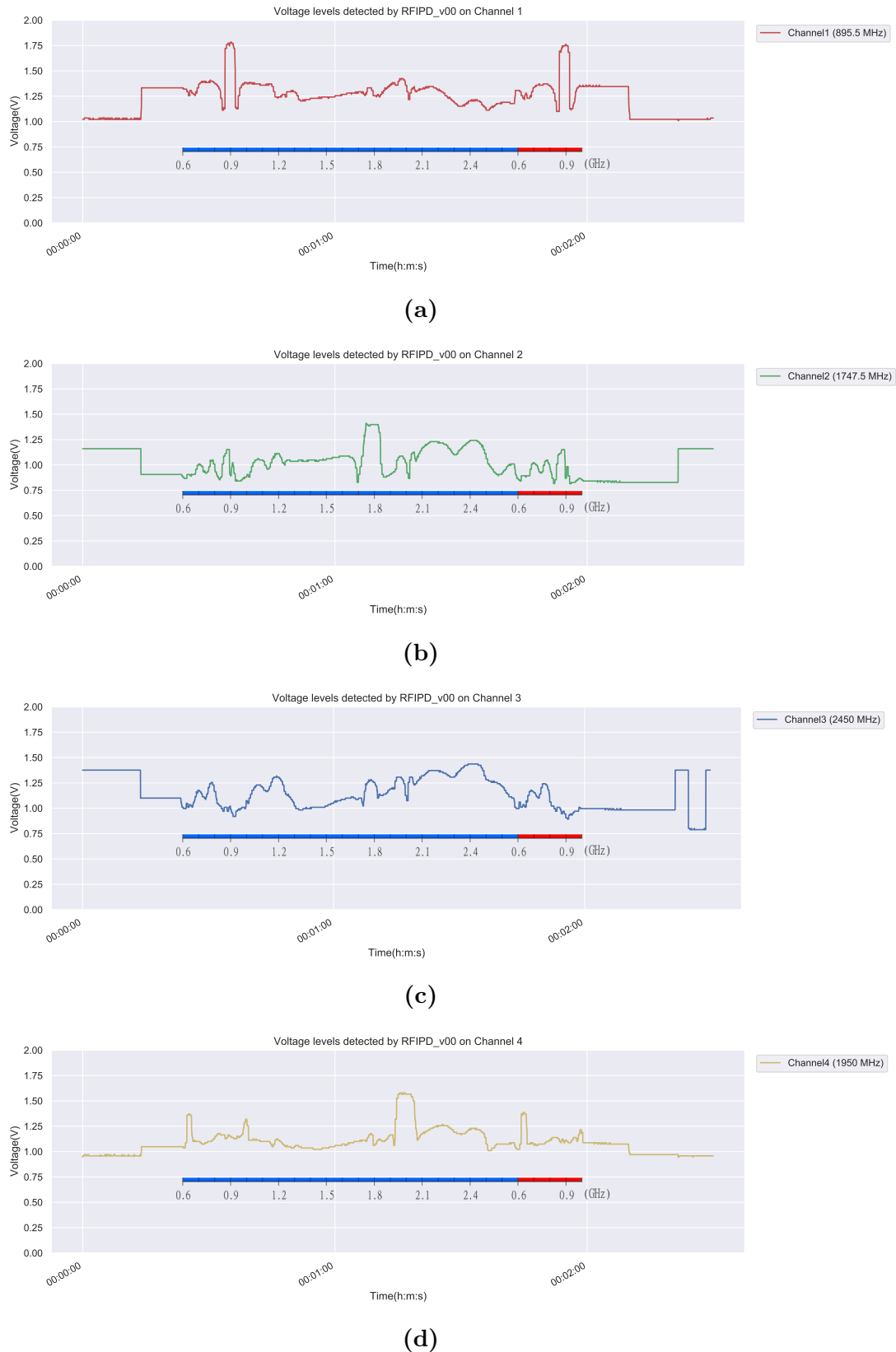


Figure 6.7: Screenshot of the output from the PC software when a frequency sweep at a power level of -10dBm is set to step from a frequency of 600 MHz to 2600 MHz, in steps of 10 MHz, holding at each step for 1s is applied at the RFIPD input, where (a) Channel 1 (b) Channel 2 (c) Channel 3 (d) Channel 4.

Furthermore, the PC software processes the data to report on the peak power, average power and time occupancy for the time frame inspected. Figure 6.8 shows a screenshot of the time occupancy measured for the RF channels during the frequency sweep. The voltage axes can be mapped to dBm using Figure 3.20 to 3.23.

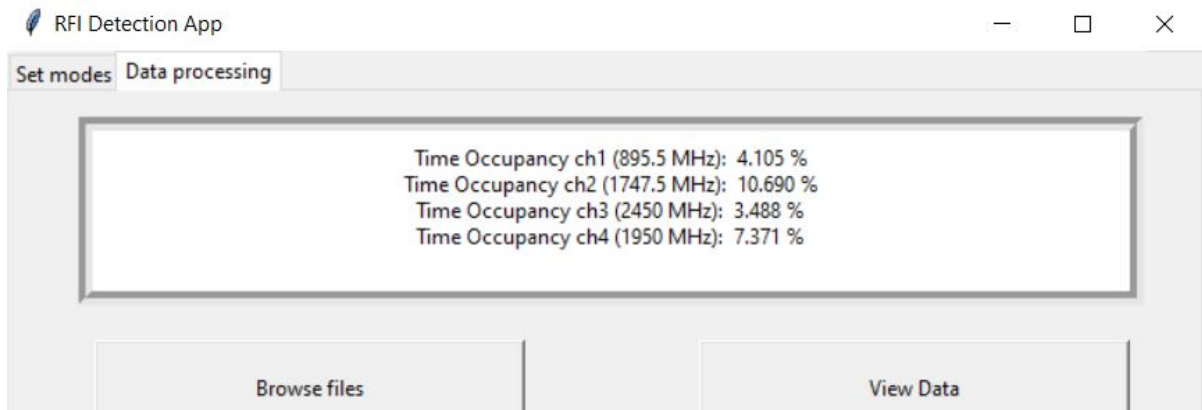


Figure 6.8: Screenshot of time occupancy report from the PC software display

Both Figure 6.7 and 6.8 are validation of the functionality of the system. This serves as verification of the data visualisation of signals using the timestamps, the reporting on the power observed, and the overall operation of the RFIPD along with the signal processing system designed.

6.3.2 Power level sweep test

This test is conducted to see the power level response of the channels, it shows how sensitively each channel can detect. The test is done using the Rohde and Schwarz SML03 signal generator, in a step-wise setting, at the four center frequencies found in the receiver, that is 895.5 MHz, 1745 MHz, 1950 MHz and 2450 MHz. The power level is set to step from a frequency of -100 dB to 0 dB, in steps of 10 dB, holding at each step for 4s. The tests are carried out in the RC to establish a controlled environment for the experiments.

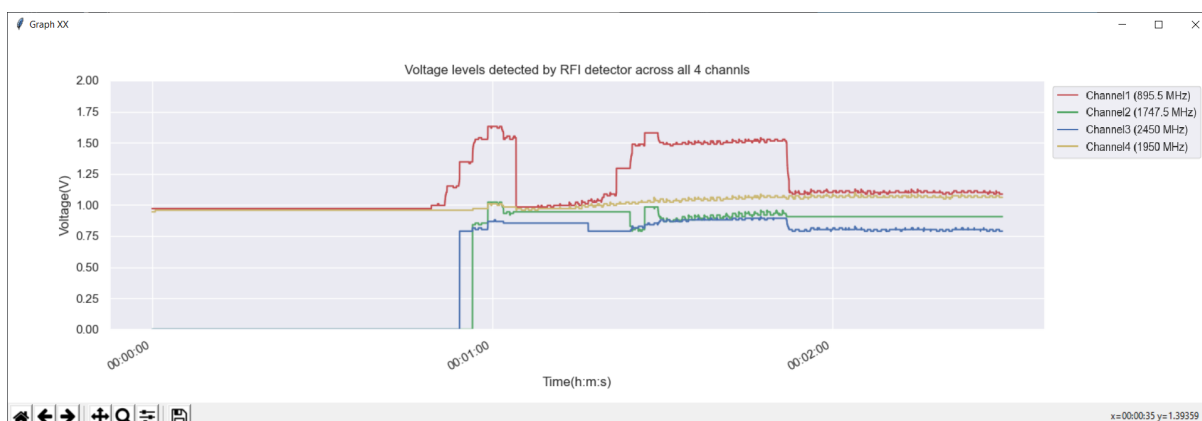


Figure 6.9: Screenshot of the RF Front-end output across channels when input frequency is 895,5MHz and the power level is set to step from a frequency of -100 dB to 0 dB, in steps of 10 dB, holding at each step for 4s.

Figure 6.9 shows 5 steps in the signal in which each step represents 10 dBm. This means that Channel 1 is detecting at least -50 dBm from the peak of 0 dBm. The other channels fluctuate depending on how strongly they are coupled to Channel 1 or how much of the 895.5 MHz passes through their filter. The performance achieved on the power sweep tests at the other frequencies were poorer than for Figure 6.9 in terms of sensitivity, because they distinguished even less than 5 steps. There the most sensitive that the RFIPD could detect is in Channel 1, at -50 dBm.

Chapter 7

Conclusions and Recommendations

7.1 Conclusions

The main objective of this project was to develop a portable RFI detection system capable of detecting major sources of RFI, namely Bluetooth, Cellular and Wi-Fi signals. The device should display signal levels of each of these frequency bands while keeping a log of the time and position of the detections that can be downloaded and processed at a later stage using custom-made software also developed as part of the project.

To begin, the RFI signals of interest were studied to determine their characteristics. This involved analyzing how they each transfer data packets in both the temporal and frequency domains. The properties of RFI signals were used to define the RF receiver's requirements.

The most important aspect of the RFI detector was the design of the RF receiver as it is responsible for the critical task of capturing the signals. Several iterations of RF receiver designs were compared, and a final receiver was chosen based on cost-effectiveness, and the extent of the post-processing required. Once the components were procured, where possible, they were tested against the manufacturer specifications performance. Some deviation from the reported performance was discovered, possibly due to non-idealities and variances in testing environments. Alternatives could not be ordered due to Covid-19 limits on manufacturer deliveries and the project's timeline. The frequency response was simulated using the present values. Furthermore, after acquiring the receiver circuit board, its performance was tested. Power was detected in different frequency bands, but the out-of-band region was high in each channel's reading. This meant that the filters were allowing signals in their stop-band to pass through, making it difficult to distinguish between the different channels detected. The RF PCB was created to integrate the RF receiver as well as multiple sub-circuits in order to realize the entire system. These included sub-circuits for power regulation, SD card storage, GNSS receiver, USB interfacing.

A signal processing system was developed in a 2-phase sequence, (1) data acquisition followed by (2) data processing. The data acquisition was implemented on the Nucleo-F334R8 micro-controller board because it has all of the required peripherals and communication protocols required. The micro-controller board is plugged into the PCB and all of this is housed in an enclosure. The enclosure makes the instrument compact, and more durable to its environment and is also meant to suppress external EMI from entering.

Furthermore, the enclosure includes a USB interface peripheral that allows the RFIPD mode to be changed when connected to PC software. This PC software is designed to generate power calculations and graphs.

Finally, with all the elements completed, the performance of the full system was tested. Firstly, environment emissions testing inside a RC found that the GNSS receiver circuit was causing noise at 1.58 GHz. This emission could not be contained using the enclosure due to the size of the apertures in the enclosure being too big, making the enclosure ineffective. Secondly, functional testing of the RFIPD was tested and the output from PC software were displayed to validate the features designed for.

7.2 Recommendations

The following recommendations were developed using the results of the testing conducted in the thesis:

- The receiver sensitivity must be enhanced in order to obtain a far more sensitive system. This can be accomplished by adding a second low-noise amplification stage and utilizing filters with improved out-of-band rejection.
- To minimize the interference generated by the system, the layout of the GNSS receiver should be re-evaluated. The use of vias and via fence around high frequency traces should be noted.
- To make the device less susceptible to EMI, the peripheral connectors chosen should make a full conductive connection with the enclosure, reducing the effective aperture size. Furthermore, the connection between the enclosure's lid and its bottom must be continuous.
- For a smaller hand-held device, the micro-controller IC can be designed to be on the PCB, rather than plugging the full Nucleo board in. This allows I/O pins to be traced in the most efficient manner possible, resulting in shorter cables connecting to peripheral connectors.

Bibliography

- [1] SKA Organization, “SKA Phase 1 Construction Proposal”, SKA Organization, Tech. Rep., 2021, p. 278.
- [2] SARAO, *SARAO-South African Radio Astronomy Observatory*, Available at <https://www.sarao.ac.za/>.
- [3] SKA Organization, “MeerKAT Fact Sheet”, SKA Organization, Tech. Rep., 2016, p. 4.
- [4] “IEEE Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz”, *IEEE Std C95.1-2019 (Revision of IEEE Std C95.1-2005/ Incorporates IEEE Std C95.1-2019/Cor 1-2019)*, pp. 1–312, 2019.
- [5] A. J. Otto, R. P. Millenaar, and P. S. van der Merwe, “Characterising RFI for SKA phase 1”, in *2016 Radio Frequency Interference (RFI)*, IEEE, 2016, pp. 81–84.
- [6] Government of South Africa, “Astronomy Geographic Advantage Act”, vol. 516, no. 666, pp. 1–3, 2008.
- [7] J. Querol, A. Perez, and A. Camps, “A review of RFI mitigation techniques in microwave radiometry”, *Remote Sensing*, vol. 11, no. 24, 2019.
- [8] R. P. Millenaar and A. J. Otto, “Innovations in instrumentation for RFI monitoring”, in *2016 Radio Frequency Interference (RFI)*, IEEE, 2016, pp. 65–68.
- [9] B. E. Howell and P. H. Potgieter, “Spectrum shortage and merger by any other name in South Africa”, eng, ser. 23rd Biennial Conference of the International Telecommunications Society (ITS): ”Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world”, Online Conference / Gothenburg, Sweden, 21st-23rd June, 2021, Calgary: International Telecommunications Society (ITS), 2021.
- [10] Phoenix Contact, *Mobile Communications Data transmission in industry*. 2012, vol. 49, pp. 11–30.
- [11] SMTA, *Global Mobile Frequencies Database*.
- [12] S O’Dea, • *Mobile technology share by generation 2016-2025 — Statista*, 2020.
- [13] M. Sauter, *From GSM to LTE-Advanced Pro and 5G*. Wiley, 2021.
- [14] M. Hedef, S. Bendoukha, and S. Weiss, “A Fast and Robust Blind Detection Scheme for Downlink UMTS TDD Component”, no. May 2014, pp. 4–7, 2006.
- [15] H. Mousavi, I. S. Amiri, M. A. Mostafavi, and C. Y. Choon, “LTE physical layer: Performance analysis and evaluation”, *Applied Computing and Informatics*, vol. 15, no. 1, pp. 34–44, 2019.

- [16] Tektronix Inc., “Wi-Fi : Overview of the 802.11 Physical Layer and Transmitter Measurements”, *Tektronix*, p. 44, 2013.
- [17] S. Ganguly and S. Bhatnagar, *IEEE 802.11 Wireless Networks*. 2008, pp. 135–148.
- [18] N. Gupta, “Inside Bluetooth Low Energy”, p. 458, 2016.
- [19] *Bluetooth® Low Energy Channels - Developer Help*.
- [20] *Understanding Bluetooth Range — Bluetooth® Technology Website*.
- [21] Ashley Raymer, *Bluetooth Key Terms — Momentaj Inc*, 2018.
- [22] Sachin Gupta, *BLE v4.2: Creating Faster, More Secure, Power-Efficient Designs—Part 1 — Electronic Design*, 2016.
- [23] T. Hubing and N. Hubing, *LearnEMC - PCB Layout*.
- [24] T. Williams, *EMC for product designers*, 5th. Elsevier Ltd., 2016, p. 564.
- [25] H. W. Ott, *Electromagnetic Compatibility Engineering*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011.
- [26] D. M. Pozar, *Microwave engineering*, 4th. John Wiley & Sons, Inc., 2011.
- [27] Keysight, “S-parameter measurement:Basics for High Speed Digital Engineers”, *Keysight*, 2013.
- [28] H. Termos, “Study of up & down conversion technique by all-optical sampling based on soa-mzi”, 2017.
- [29] C. Rauscher, V. Janssen, and R. Minihold, *Fundamentals of Spectrum Analysis*. Rohde & Schwarz, 2001, p. 216.
- [30] Tektronix, “Noise Figure”, Tektronix, Tech. Rep., 2014, p. 63.
- [31] National Instruments corp., *Understanding Frequency Performance Specifications - NI*, 2021.
- [32] S. Gupta and A. Phatak, “ADC Guide, Part 1-The Ideal ADC”, Tech. Rep., 2012.
- [33] A. Inc, “Soundtrack Pro 3 User Manual”, Tech. Rep., 2009.
- [34] R. Chellappa and S. Theodoridis, *Academic Press Library in Signal Processing: Volume 1 - Signal Processing Theory and Machine Learning*. 2014, vol. 1.
- [35] B. P. Lathi and R. A. Green, *Linear systems and signals*. Oxford University Press New York, 2005, vol. 2.
- [36] P. Cruz, H. Gomes, and N. Carvalho, “Receiver Front-End Architectures – Analysis and Evaluation”, in *Advanced Microwave and Millimeter Wave Technologies Semiconductor Devices Circuits and Systems*, InTech, 2010, p. 28.
- [37] “A PRACTICAL GUIDE TO RF FOR EMBEDDED DESIGNERS proliferating , driven by a vast and”, Digi International Inc, Tech. Rep., 2017, p. 17.
- [38] A. Anderson, “Selecting Antennas for Low-Power Wireless Applications”, *Analog Applications*, pp. 20–23, 2008.
- [39] M. Johnson, H. Patel, P. Tikoo, J. D. Britto, and J. Borade, “Survey on antennas and their types”, *International Journal For Science Technology And Engineering*, vol. 3, pp. 22–30, 2017.
- [40] *Ant-lte-mon-sma data sheet*, Linx Technologies, 159 Ort Lane, Merlin, 2019, p. 18.

- [41] B. Razavi, *RF Microelectronics , Second Edition*. Prentice hall New York, 2013, vol. 53, pp. 1689–1699. arXiv: [arXiv:1011.1669v3](https://arxiv.org/abs/1011.1669v3).
- [42] SCILLC, “SMA3103 Datasheet”, ON Semiconductor, Tech. Rep. 7169, 2013, p. 8.
- [43] A. Pini, *Routing RF Signals Using Power Dividers/Combiners — DigiKey*, 2019.
- [44] A. Gallo, “Basics of RF electronics”, Tech. Rep., 2011.
- [45] Mini-Circuits, “Power Splitter / Combiner SEPS-4-272+ Datasheet”, Brooklyn, Tech. Rep., p. 1.
- [46] Geza KOLUMBAN, “ EIE331: Communication Fundamentals”, The Hong Kong Polytechnic University, Tech. Rep.
- [47] B. Schweber, *Solving the RF Power-Detection Challenge — DigiKey*, 2016.
- [48] L. E. Frenzel, *Design RF detectors for wireless devices FAQs*, 2007.
- [49] STMicroelectronics, *STM32 Arm Cortex MCUs - 32-bit Microcontrollers - STMicroelectronics*, 2021.
- [50] STMicroelectronics, *UM1724 User manual*, 2020.
- [51] C. Noviello, *Mastering STM32*. Leanpub, 2016.
- [52] Orolia, *The GNSS Spectrum - Orolia*, 2021.
- [53] Elm Chan, *FatFs - Generic FAT Filesystem Module*, 2021.
- [54] Q. Xu and Y. Huang, “Anechoic and reverberation chambers: Theory, design, and measurements”, 2019.
- [55] T. Nhlapo, R. Geschke, and P. Wiid, “Emi risk assessment methodology for farming communities close to a radio quiet zone”, in *2018 IEEE 4th Global Electromagnetic Compatibility Conference (GEMCCON)*, 2018, pp. 1–5.
- [56] STMicroelectronics, “STM32F3 series Mainstream 32-bit MCUs Releasing your creativity Content”, Tech. Rep., 2017.

Appendix A

STM32 Board Ranges

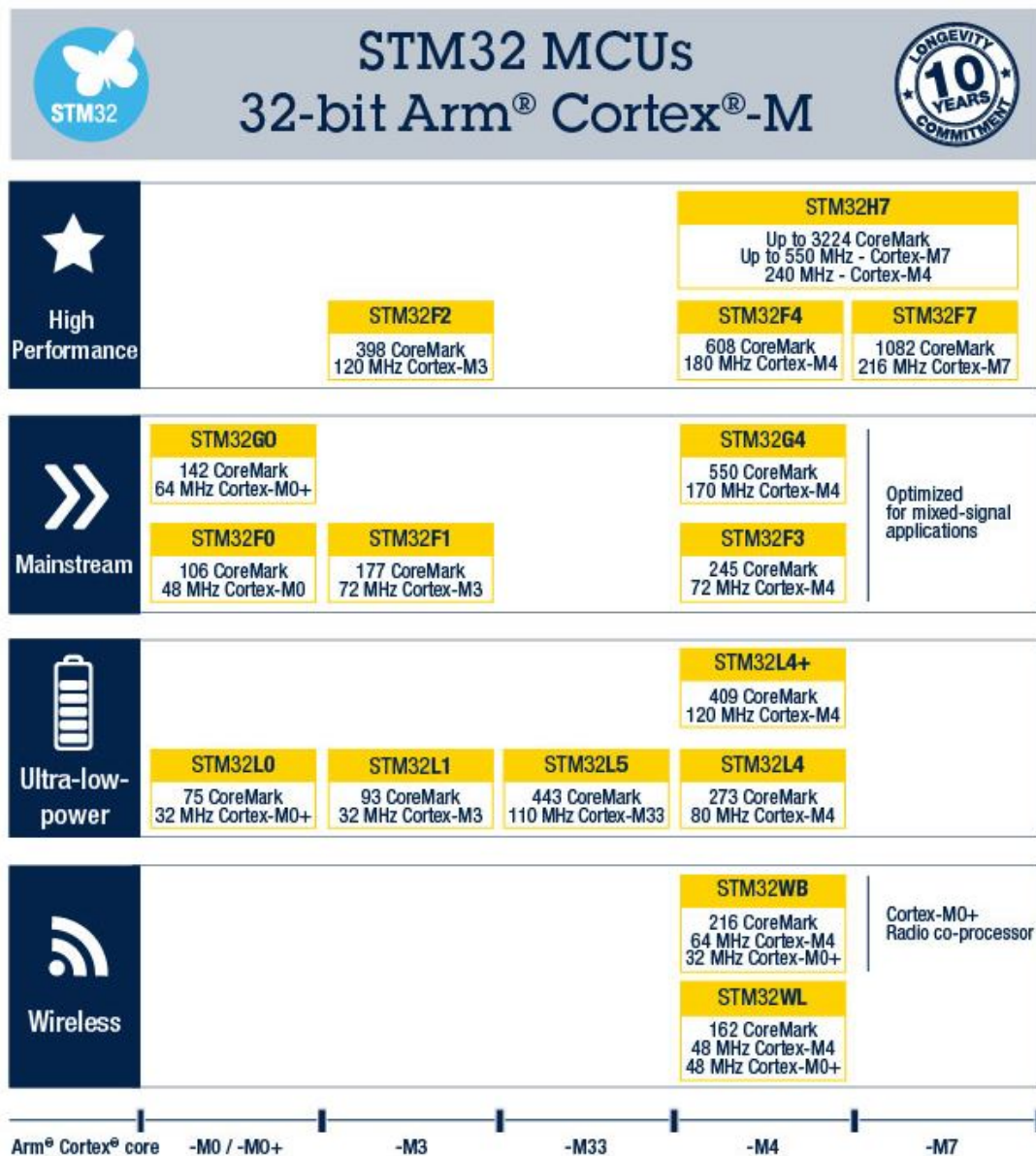
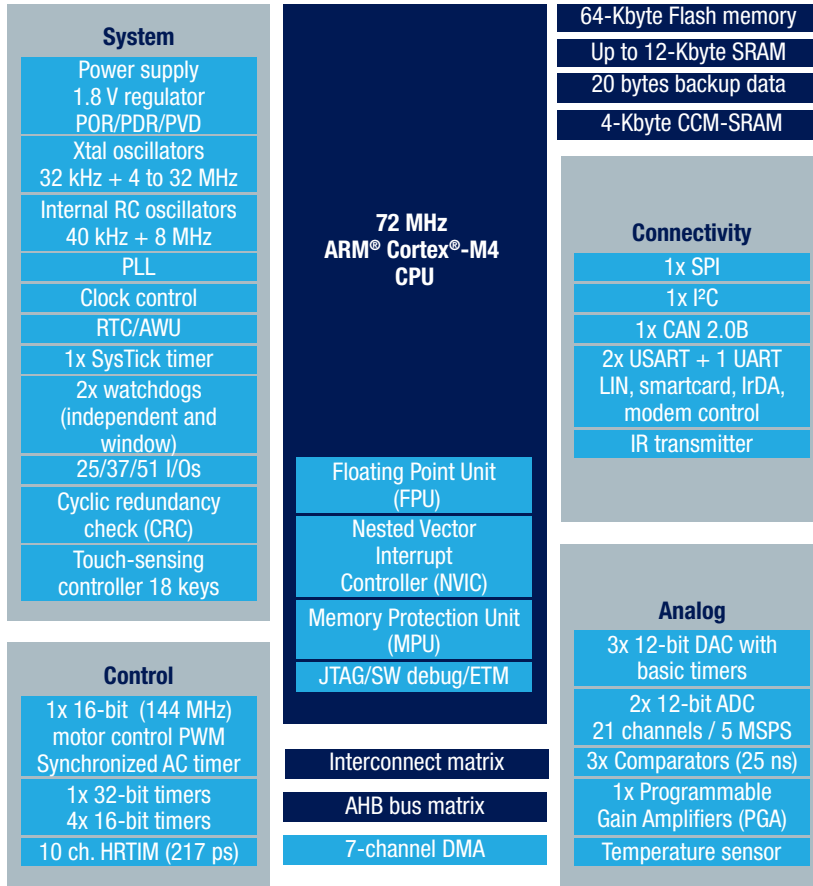


Figure A.1: STM32 MCU’s categorised according to ARM processor and suggested application [49]

STM32F334 BLOCK DIAGRAM



APPLICATION TARGET

STM32F334 devices greatly simplify digital control of complex power-supply topologies used in:

- Data servers
- Telecom infrastructure
- Wireless charging points
- Lighting
- Welding
- Industrial power supplies
- Digital switch mode power supplies (D-SMPS)

COMPLEX WAVEFORM BUILDING AND MULTI-EVENT HANDLING (FROM HRTIM) - EXAMPLE

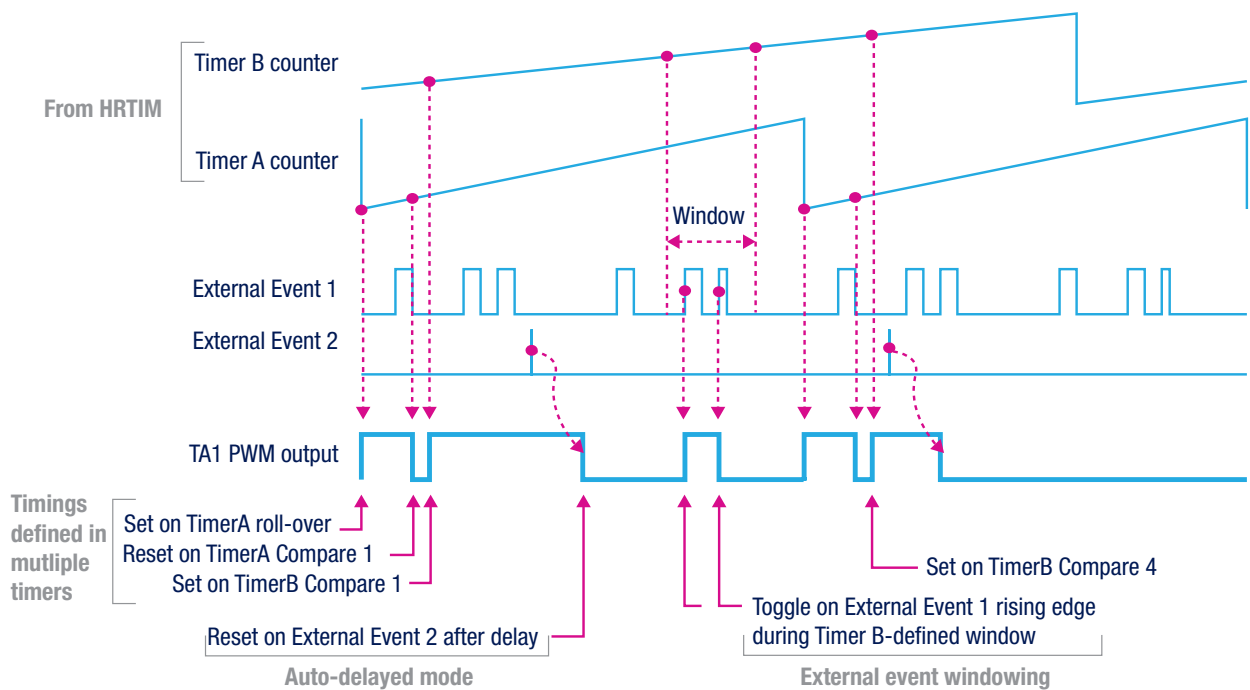


Figure A.2: STM32F334 block diagram illustrating the features of microcontroller [56]

Appendix B

RFIPD Configuration Phases

Below is a list of figures designed at various phases of the RFIPD construction:

- Schematic design of the RFIPD circuit
- The top and bottom side of the PCB layout
- The dimensions of the enclosure, along with its apertures

These figures are displayed in the sections to follow.

B.2 PCB Layout design

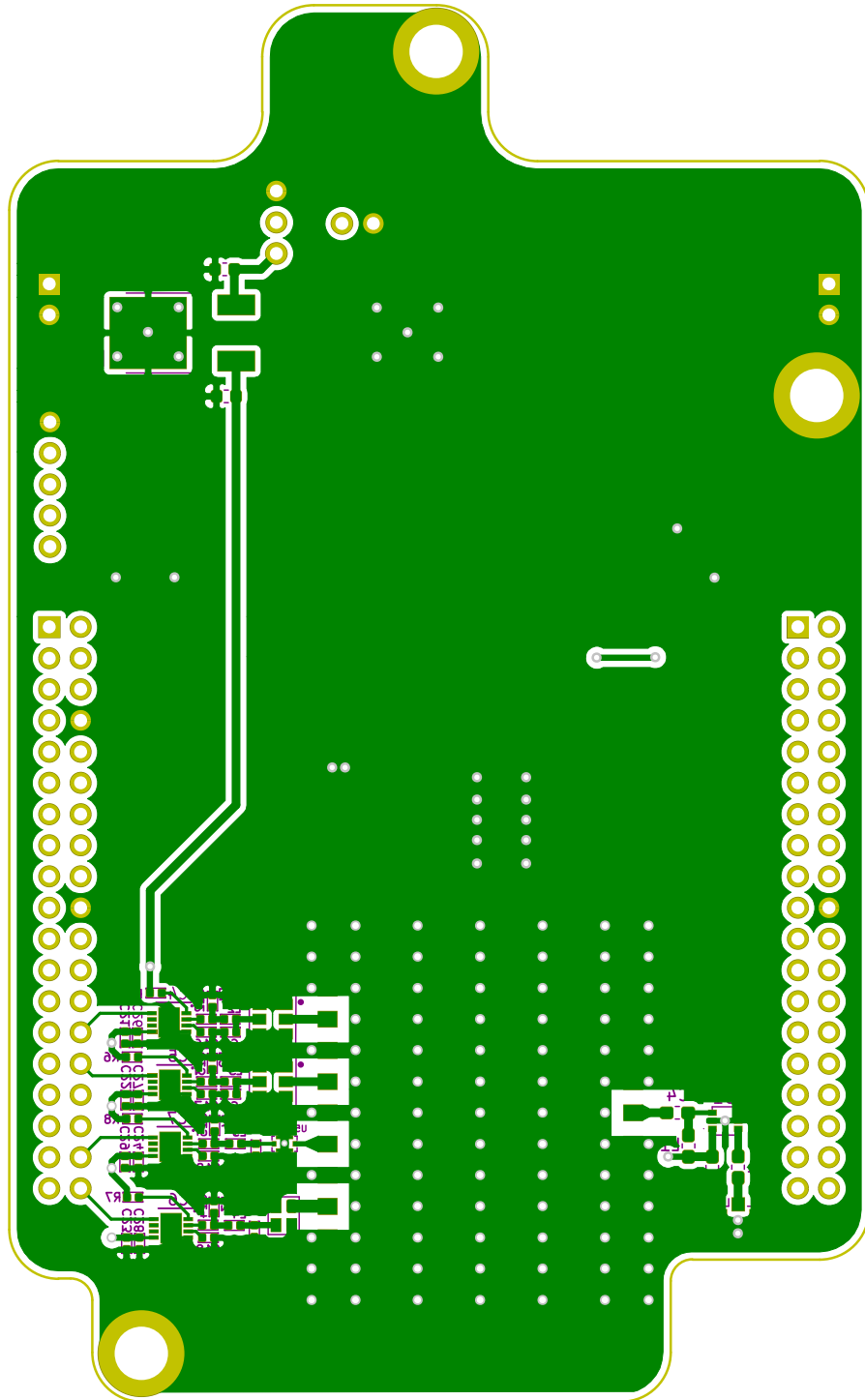


Figure B.2: Bottom PCB layer

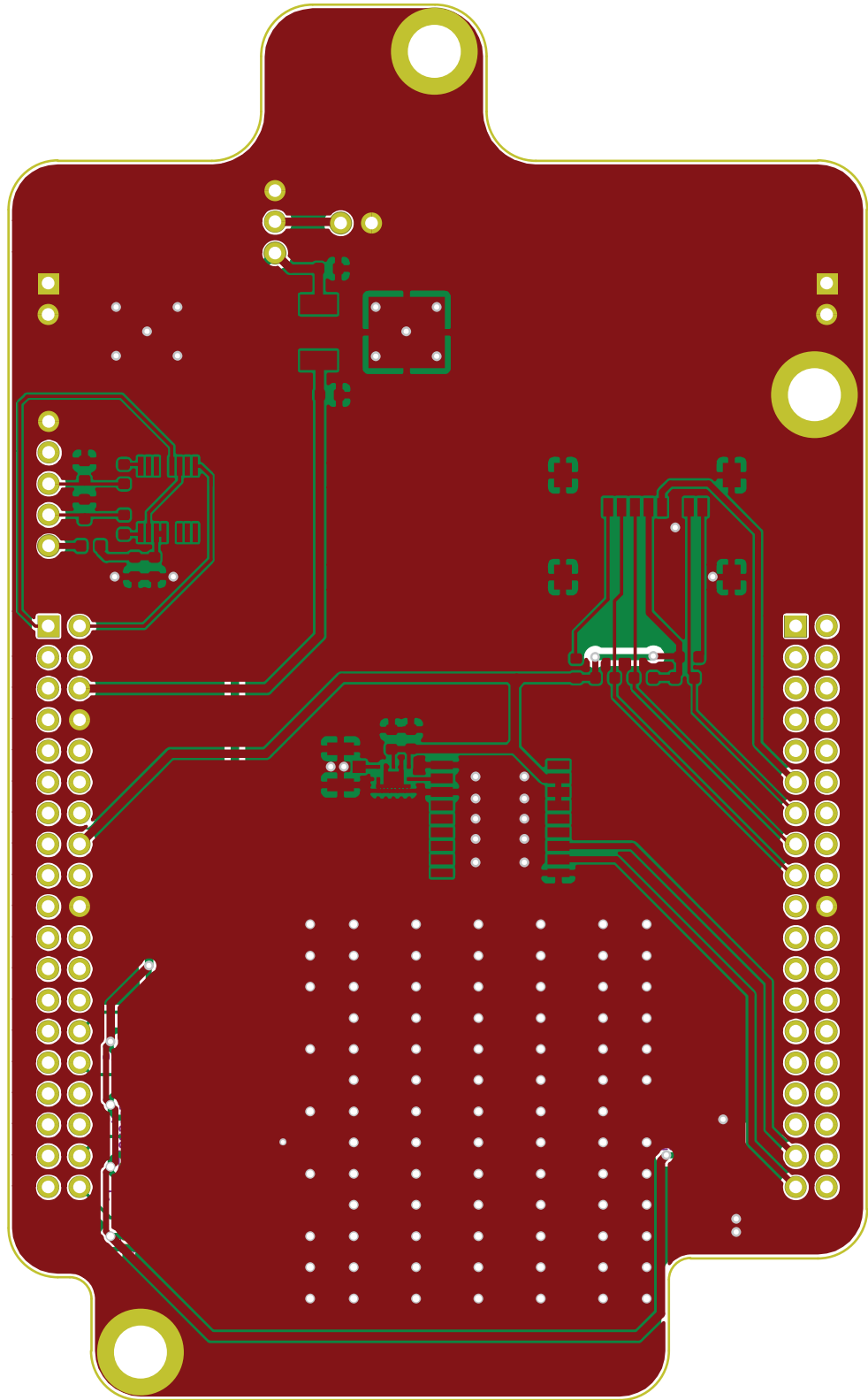


Figure B.3: Top and bottom PCB layer

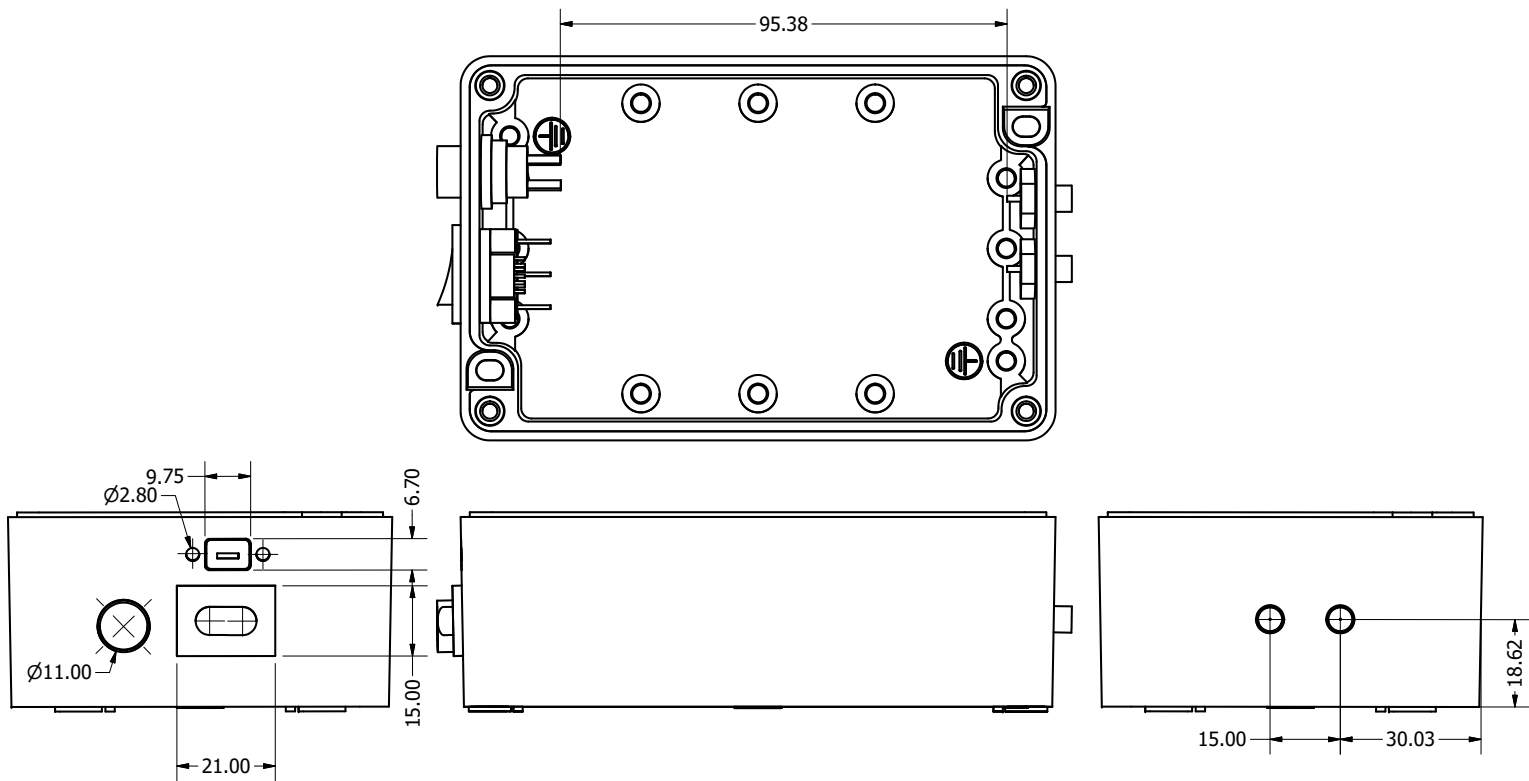


Figure B.5: Dimensions of the enclosure Bottom