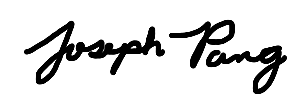
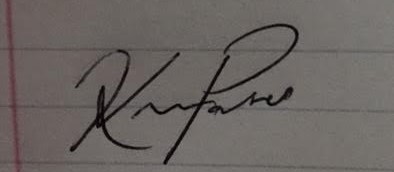
Adaptive Spectrum Sensor

Final Report

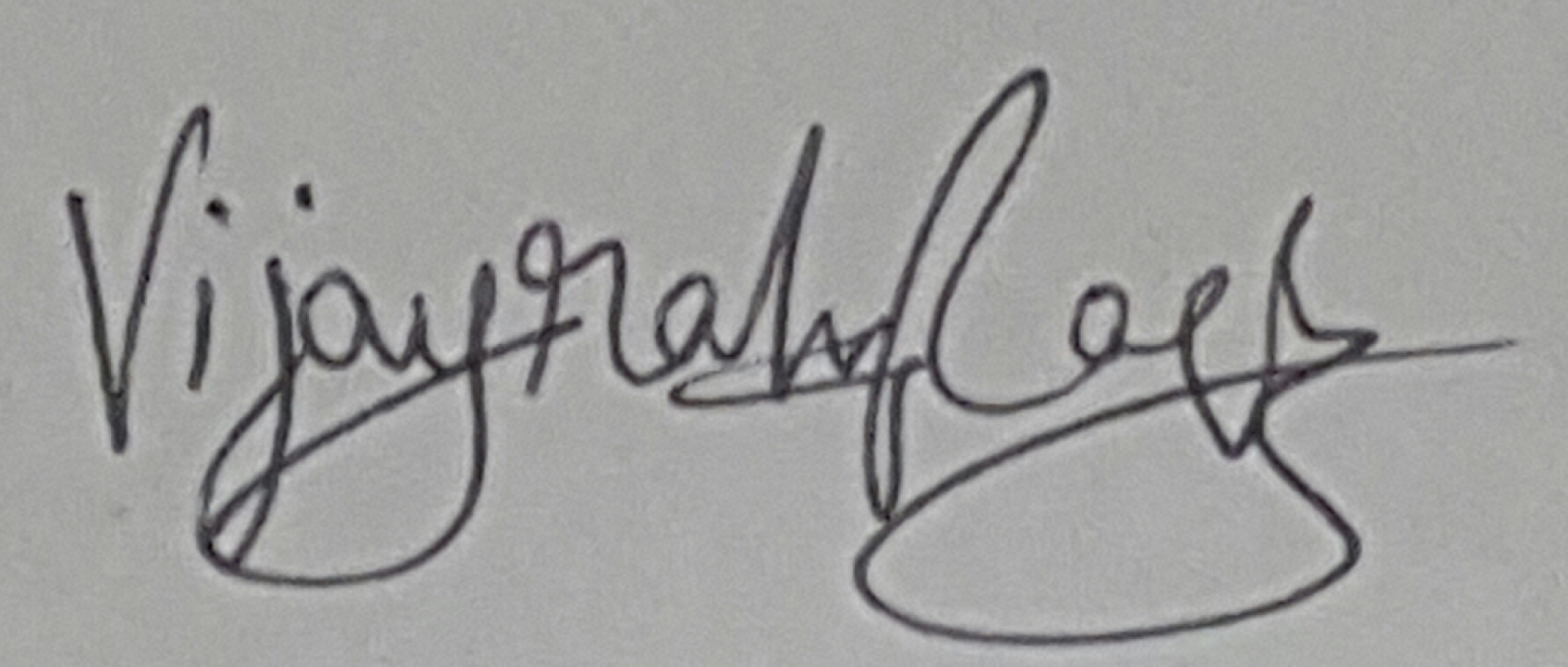
Group 5

5/2/2017

“I pledge my honor that I have abided by the Stevens Honor System.”

Andrew Guthrie Joseph Pang Kunal Patel

C:\Users\Class2017\Desktop\signature.PNG

Vijayrahul Rajathiruvenkatapathy Thomas Wright



Project Advisor: Prof. Bruce McNair

***Identification of Sponsors***

MITRE Corporation has offered to sponsor this project by providing equipment and technical expertise. Namely, they have provided this project with two USRP N210 Software Defined Radios. These were integral to the project and the project would not be possible without this equipment. The group would like to thank Ryan Nilsen, Adam Parks, and Marcin Wojcik for technical advice, and Bill Urrego for his implementation of the white paper, “Convolutional Radio Modulation Recognition Networks.”

# Executive Summary

This project leverages software defined radio (SDR) principles to isolate signals and classify modulation of those signals across a wide spectrum. We are using two Ettus Research Universal Software Radio Peripherals (USRPs) to sense and isolate signals, along with a computer to perform signal processing once the radios acquire RF power samples. Signals are processed through a machine learning model trained to recognize many types of modulation. Testing shows a signal processing time of around .02 seconds, and a machine learning time of several seconds, with the ability to identify 11 different types of modulation. The team presented a pitch in front of mock investors, and will be ready for Design Day on May 3.

# Table of Contents

[Executive Summary 3](#_Toc481507097)

[Table of Contents 4](#_Toc481507098)

[Section – I: Project Definition and Plan 6](#_Toc481507099)

[1. Mission Statement 6](#_Toc481507100)

[2. Background 6](#_Toc481507101)

[3. Stakeholder List 6](#_Toc481507102)

[4. Analysis of Stakeholder Needs 9](#_Toc481507103)

[5. Project Scope and Resources 10](#_Toc481507104)

[6. Project Plan 10](#_Toc481507105)

[Section – II: Design, Evaluation & Optimization 11](#_Toc481507106)

[1. Requirements 11](#_Toc481507107)

[2. Constraints and Assumptions 11](#_Toc481507108)

[3. Applicable Codes/Standards/Regulations 13](#_Toc481507109)

[a. Professional and Ethical Issues 13](#_Toc481507110)

[4. Concept Development and Selection 13](#_Toc481507111)

[5. Design: Architecture, Materials, Layout, Manufacturing considerations 16](#_Toc481507112)

[6. Design Evaluation Methods 17](#_Toc481507113)

[a. Methods: Analytical, Simulated, Physical Tests 17](#_Toc481507114)

[b. Physical Prototyping: Plan and Budget 18](#_Toc481507115)

[c. Prototype Build and Test Report 18](#_Toc481507116)

[7. Design Evaluation Report: Performance, Reducibility and Cost 19](#_Toc481507117)

[8. Design Revisions and Optimizations 20](#_Toc481507118)

[9. Final Design Specification with BOM 20](#_Toc481507119)

[Section – III: Entrepreneurship & Business Development 20](#_Toc481507120)

[1. Business Objectives and Risks 20](#_Toc481507121)

[2. Competitive Intelligence: Market Analysis 20](#_Toc481507122)

[3. Lean Canvas Business Model 21](#_Toc481507123)

[4. Financial Analysis 21](#_Toc481507124)

[5. Intellectual Property 23](#_Toc481507125)

[Section – IV: Results 24](#_Toc481507126)

[1. Conclusions 24](#_Toc481507127)

[2. Recommendations 24](#_Toc481507128)

[Appendices 25](#_Toc481507129)

# Section – I: Project Definition and Plan

## Mission Statement

The Adaptive Spectrum Sensor project will offer the Army the capability to identify RF signals in a given area of the RF spectrum like never before. An increased level of situational awareness, which provided by the project, will lead to a significant tactical advantage for its operators. Unlike current systems that are bulky and expensive, our product will use Software Defined Radio and commercial-off-the-shelf technologies to deliver a low cost and reliable solution. This approach will maximize the amount of capabilities that the Army has available to them for the least amount of resources spent. The sponsor of the project, MITRE Corporation, is lending equipment and technical expertise as necessary. The team will use these resources to develop the project over the course of the Senior Design process.

## Background

This project takes advantage of a very up and coming topic in the field of wireless communications, the software defined radio. The key objective of this project is to identify and determine modulation schemes of signals encountered in an open environment. This will be accomplished by scanning a spectrum larger than the bandwidth of the radio, meaning the radio will also have to change center frequencies many times per second in order to record a clear picture of the spectrum. It will also need to be able to determine the modulation type of signals that are found, all in as short of a period of time as possible.

Current spectrum analyzers are heavy and expensive, whereas SDRs provide the opportunity for hardware convergence. Significant amounts of signal processing are handed over to a general-purpose processor. Our development will be using regular, commercially available laptops which are good representations of the type of device the software will be capable of running on. With this type of design, a software radio is produced which can receive and transmit a wide variety radio protocols with a very low hardware investment. Additionally, spectrum sensing is very processing intensive and generally the hardware to implement this capability is very expensive. Creating a lightweight solution could be a very beneficial utility for the Army.

The Department of Defense (DoD) currently has a different physical system for each mission function. This means that a single vehicle mounted system solely for extracting frequency and modulation data could cost tens of thousands of dollars to the Army, and has its own set of antennae, FPGAs, processors, etc. Leveraging Software Defined Radio capabilities, all of these individual systems could be joined into a small number of systems. The goal of this project is to create a lightweight solution using COTS (Commercial off-the-shelf) products, making the end result much cheaper than the traditional model being deployed. Making a software spectrum analyzer will mean that even if the hardware it is running on fails a copy could easily be installed on a different laptop or similar. By carrying around significantly less hardware the DoD also benefits from moving less payload and saving gas and potentially lives.

## Stakeholder List

Table 1 lists both active and passive stakeholders, and their views and actions as they relate to this project.

Table 1 Stakeholders

| **Stakeholder** | **Role** | **Location** | **Goal** | **Method** | **Current Solution** |
| --- | --- | --- | --- | --- | --- |
| **Active Stakeholders** | | | | | |
| MITRE (Customer/ Sponsor) | Providing capabilities to their sponsor/ customer. | Wherever the US has a military presence in the world and could benefit from a better understanding of the RF spectrum in that area. | It is their mission as a not-for-profit corporation. | Internal R&D as well as sponsoring outside teams while providing engineering expertise to complete the task. | Currently they are not filling this need.  An alternative would be to use heavier, costlier, and more time consuming methods. |
| Army Corporate (Acquisition) | Acquire capabilities and/or a tactical advantage for the Army | All over the world | To defend our country and/or gain an advantage over the enemies. | Hiring an outside company to fill this need. | Do not have this particular capability. An alternative would be to use heavier, more costly, and more time consuming methods. |
| Soldier | Operating and maintaining the equipment in order to complete the mission in which they were given. | Wherever they are deployed, large variety of environments | To serve their country/follow orders. | By having a knowledge of the products operation and implementing the product in the field. | Do not have this capability. An alternative would be to use heavier, more costly, and more time consuming methods. |
| Developers | Interfacing with hardware, developing software and algorithms to create this product. | New Jersey | To complete graduation requirements, gain knowledge of spectrum sensing on the hardware and software levels, to create a product that will support our military. | By applying their knowledge and education, researching topics of interest, generating detailed planning, and spending many man hours of work. | N/A |
| **Passive Stakeholders** | | | | | |
| RF Producers | Producing RF signals | Wherever they are | To communicate using wireless technology | Utilizing wireless technology | N/A |
| Ettus Research (Hardware Producer) | Leading supplier of software defined radio platforms | Headquarters in Texas | Designs a wide range of Universal Software Radio Peripheral (USRP) products and other radio related platforms | To support development environments and products are designed for Radio Frequency related tasks and applications like spectrum monitoring, satellite navigation and so on. | N/A |
| FCC or other RF governing bodies | Regulates interstate communications (radio, TV, satellite) | FCC-located in US, and other governing body locations | For controlling state and international communication functions and for public safety, and homeland security | Encouraging leadership in the communication infrastructure, promoting broadband facilities innovation, supporting nation’s economy | N/A |

## Analysis of Stakeholder Needs

For analysis of stakeholder needs, the group took a Voice of Customer Poll, and derived stakeholder needs from customer communications.

Table 2 Voice of Customer Table

|  |  |  |
| --- | --- | --- |
| **Verbatim (VOC)** | **Restated as Customer Need** | **Derived Requirement** |
| Want this to be light, cost effective, and less time consuming | Develop an affordable and handy spectrum analyzer using USRP | Affordable, Timeliness, Price |
| Want to come up with a process to automatically scan a large bandwidth and lock onto possible signals. | Ability to scan a large bandwidth and identify the necessary signals of interest. | Accuracy, High Performance Level |
| Develop some type of classification scheme to break down the signal into its constituents to provide meaningful metric. | Develop an algorithm that provides accurate signal detection into meaningful, human readable information. A neural network could be one of the suitable candidate for the algorithm. | Precision,  Ease of Use (interpreting output) |
| Ability to differentiate signals from noise and lock onto their bandwidth. | Identify signals in noisy environments. Accurately detect signals. Determine the bandwidth of signals of interest. | Accuracy |

From Table 2, one can see that the goal of this project is not only create a capability for the customer, but complete the task quickly and at a low cost. The main stakeholder in this project is the military, so their concerns are first and foremost. This product is made with the ultimate goal of being implemented on hardware the military is going to use in the field. Our sponsor, MITRE, is federally funded contractor of the military. They are providing assistance with the project, and have the same goals the military does. The basic overview of these goals is to be able to read a wide frequency band, determine where signals are located on the band, be able to successfully identify modulation type of found signals, and output the information in an easy to understand format. Ideally it will be able to find signals in a few seconds and identify modulation types in real time.

However, by nature of the product, there are other stakeholders involved. Perhaps the second most important stakeholder is the FCC and other radio frequency governing bodies. The spectrum sensing project that we are going to be creating is made with the goal of determining what channels are open for communications, as well as analyzing the spectrum that is scanned and being able to understand what communication is taking place. The group needs to be careful while testing in order to not operate in any bands that are off limits for non-licensed users. This includes not broadcast or interrupting broadcasts that are regulated by the FCC. An example of a potential violation is scanning cellphone communications on a cellular band while testing out our software. This violates the FCC’s regulations. If we violate regulations, the FCC could get involved and taking legal action. Similarly, if we were broadcasting over restricted frequencies and interfered with communications, such as over the FM or AM bands, the FCC would also be the ones that would have to contact us and resolve the issue.

The third most important stakeholder is the soldier. The final product needs to be able to be easily utilized and provide data that is easily read by an average user. One potential need of this stakeholder, that may not have been thought of initially, is the ability to change the color scheme of the team’s software to operate in different lighting conditions. Another potential requirement could be to add a text-to-speech readout of important data. When thinking about the user as a stakeholder, important ergonomic requirements appear that were not initially thought of.

## Project Scope and Resources

From a big picture perspective, the design needs three basic functionalities. First is the ability to identify and isolate radio frequency signals. The second is the ability to determine the modulation type of analog and digital signals from a broad-spectrum scan. The third is to display the analysis in an easy to read and interpret user interface. Once those three basic objectives are met, the next step is simply being able to do all of those things better. This includes being able to analyze a variety of both analog and digital signals, and being able to break down the broad spectrum band faster and with a greater success rate. The ultimate end goal would be able to gather data on every signal that can be scanned in a very brief period of time with a very low error margin.

To complete this task, we are using several different resources; some of which were self-obtained and some of which were provided by MITRE. As a group, we acquired GNU radio (widely used in research and real-world systems), an environment for implementing software defined radio projects, established standardized environments to program in, and implemented tools for version control. From MITRE we received radios which will be used as the RF front end for this project. Their task will be to receive the RF spectrum data to be analyzed. The other resources we have available to us are contacts in MITRE who are designated to provide assistance to us, our project advisor, and the money allocated to our group for the sake of completing the project.

## Project Plan

The current plan is to go through the steps laid out in the project scope first. The first thing that needs to be done is identifying and isolating we need to gain the ability to analyze both an AM and FM signal. The next step we have is to determine how to analyze a basic digital signal. These two steps are going to be done together as a group using the GNU radio environment and the tools that are provided. The next big step is to start working through a broader range of the RF spectrum, and gaining the ability to extract and analyze a larger variety of signal types. From there, the last stage in development of the main project is taking what was done using the higher-level GNU-radio blocks and modifying or entirely redesigning them using C++ or hardware implementation to increase performance. Another task, which is going to occur in parallel to the others, is to develop a user interface.

# Section – II: Design, Evaluation & Optimization

## Requirements

The key objective of this sensing and detection project is to identify signals and determine modulation schemes of signals encountered in an open environment. Several other requirements can be extrapolated from the Stakeholder Needs section. Weight, cost, and speed are major stakeholder concerns. Additionally, the sponsor requires that the project team develops a process to automatically scan a large bandwidth and identify possible signals. Our understanding of this statement is that the spectrum analyzer must have the ability to scan a large bandwidth and identify signals of interest. For this process, an efficient algorithm will be created that provides accurate signal detection into meaningful, human readable information.

They would like the analyzer to differentiate signals from noise and determine their bandwidth. Restating as the customer need, the analyzer must identify signals in noisy environments. Accurately detect signals and determine the bandwidth of signals of interest. Along with the targeted customers of our product, our team itself has certain requirements that we must oblige carefully like meeting with the FCC regulations, safety hazardous and vice versa. From the above outlined analysis, the team developed the following requirements.

1. The system shall utilize one or more USRPs, and one or more commercial off the shelf computers.
2. The system shall identify signals and determine modulation schemes of those signals with a THRESHOLD confidence of 70%, and an OBJECTIVE confidence of 85%.
   1. The system shall identify signals and determine modulation schemes of those signals within a THRESHOLD time of 3 seconds, and an OBJECTIVE time of 2 seconds from the time the signal enters the system.
      1. The system shall be able to identify the following analog modulation schemes: NBFM/AM-SSB, AM-DSB, WBFM.
      2. The system shall be able to identify the following digital modulation schemes: BPSK, QPSK, 8PSK, 16QAM, 64QAM, BFSK, CPFSK.
3. The system shall scan a spectrum larger than the instantaneous bandwidth of the radio.
4. The system shall have a GUI to display signal information and take in user controls.
   1. The system shall display signal information to the user.
      1. The system shall display textually signals it identifies.
   2. The system shall take controls from the user.
      1. The system shall operate on the spectrum specified by the user.
      2. The system shall accept scanning FFT bin size from the user.
5. The system shall conform to specified size and weight restrictions.
   1. The system shall weigh no more than 20 pounds.
   2. The system shall occupy less than 2.5 cubic feet.
6. The system hardware shall cost less than $10,000.
7. The system shall not break applicable laws and codes.

## Constraints and Assumptions

There are several categories of constraints and assumptions that are considered in creating this project. Listed below are economic, environmental, health and safety, manufacturing, and sustainability considerations.

* Economic: cost estimation, survey of funding sources

The products we will be utilizing are Commercial-Off-The-Shelf, readily available to anyone who desires them. Components can be chosen based on low price and upgraded as more funding sources become available. Fortunately, the project idea comes from a sponsor, who has a customer interested in the technology. By providing the team with existing resources, the economic impact for the company is minimal, but they have the potential to receive a very easily produced, functional product.

* Environmental: impact estimation, survey of legislations and regulations, design considerations/solutions

One consideration that must be made with the product is to ensure that it is RoHS Compliant. RoHS (Restriction of Use of Hazardous Substances) regulations ensure that hazardous substances are not used in new electronic and electronic equipment. The product must not include levels of lead, cadmium, polybrominated biphenyl (PBB), mercury, hexavalent chromium, and polybrominated diphenyl ether (PBDE) flame retardants that are higher than RoHS standards. Employees may require RoHS training before manufacturing the product. Other than keeping in line with RoHS compliance, there should not be many other environmental considerations that would cause design constraints.

* Health and safety: impact estimation, survey of legislations and regulations, design considerations/solutions

The device itself is unlikely to pose serious direct health risks in normal usage scenarios. Like most electronics, the device runs the risk of hazardous materials within the electronic components, the possibility of electrical shock and heating associated with most electronics, and concerns with RF safety (power output and frequency). Some other safety concerns arise with the use of RF bands. Bandwidth allocation is regulated by the Federal Communications Commission (FCC) in the United States. The responsibilities of the FCC have increased to accommodate the regulatory issues presented by these emerging radio and other new technologies. The responsibility for the radio spectrum is divided between the [FCC](http://www.fcc.gov/) and the National Telecommunications and Information Administration ([NTIA](http://www.ntia.doc.gov/)). Currently, only frequency bands between 9 kHz and 275 GHz have been allocated with several constraints. For our project, it is important to be wary that we are not interfering on any bands that are used for emergency communications or used for primary communications/services. Additionally, they cannot also claim the protection from harmful interference from stations of a primary service. Also, major RF transmitting facilities such as radio and television broadcast stations, experimental radio stations undergo routine evaluation for RF compliance whenever a proposal is submitted to the FCC for modification or development of a transmitting facility or renewal of a license. If our prototype commercially becomes available, it must abide by these rules in order to be successfully delivered to the military for deployment.

* Manufacturability: resource and facility requirements, possible source of such resource and facility

Due to the fact that this project has primary goals of using readily available hardware and open source software, there are no manufacturability concerns worth noting. Concerns in availability of the USRP radios are minimal. Additional vendors may be sought out if for some reason the USRP systems are unavailable.

* Sustainability: assessments of above points over time, solutions for above points over time.

All concerns presented above will be the same in the near future. If the availability of USRP radios is reduced, other vendors may be sought out. FCC Rules and regulations will change over time, but the system can adapt to meet these needs. Additionally, if a cognitive radio based approach was used in the allocated bandwidth in the US or Internationally, the system would be even more functional since that is its main use case.

## Applicable Codes/Standards/Regulations

One responsibility with this project is the use of the RF spectrum. In order to comply with FCC Code Title 47 CFR Part 15, the device must be a passive scanner and cannot transmit at all. Bandwidth allocation is a great concern when dealing with wireless communications. While bandwidth allocation is regulated by the FCC in the United States it is important to be wary of which bands are being used for the project. Some allocations being used are critical and lives can actually depend on the use of these bands. It needs to be ensured that the product does not interfere with any bands used by law enforcement, emergency services, news, etc. Only licensed users should be able to access the bands in use and are not to be interfered with.

## Professional and Ethical Issues

There are also many security concerns that should be taken when using cognitive radio and Dynamic Spectrum Allocation (DSA). There are two types of users defined through DSA. Licensed users are allowed access to the spectrum at all times while unlicensed users can use the spectrum if it is not being used by licensed users. This can be an area of vulnerability for cognitive radio and spectrum use. A major feature of cognitive radios is that they are given the ability to learn. This also opens up security concerns because detrimental behavior can essentially be taught to the radio if a malicious user gains access.

The two major classifications of attack that must be noted are On-Path and Off-Path attacks. On-Path attacks include observing and transmitting data to the system in real time or spoofing, injecting, removing or altering data. Denial-of-Service (DoS) attacks are an example of an on-path attack. Off-Path attacks are less direct and include injecting data into a stream that could later be accessed by the system, spoofing other devices on the network, and transmitting traffic that cannot be seen. Some attack mitigations that can be used include improving sensor inputs so that the system can differentiate between natural and man-made RF events, carefully analyzing radio policy to protect against malicious sensor inputs, and making sure authentication procedures are in place so that signals from unlicensed users are verified. Finally, since we are not transmitting over the air, we do not have to worry about interfering with critical systems such as the police, fire department, emergency centers and such.

## Concept Development and Selection

Identifying the acquired signals will rely on more in-depth knowledge of the signals contained in each part of the spectrum. A beneficial way to begin looking at a system is as a black box, where all that matters is the inputs and outputs.

System

RF signals

User controls

Signal information

Figure 1 Black Box System Representation

This Figure 1 shows the top-level view of the project, with the SDR system treated as a black box. The input to the system are the various RF signals in the area around the device. The system will focus on RF signals in a band specified by the user, and will output data about these signals using a graphical user interface. Data will include relevant information about all signals found in a selected range, such as their center frequencies, modulation types, and the types of signals that may be found, such as LTE, 4G, 3G and other types. Unused or free bands in the spectrum being analyzed will also be highlighted in the output.

To develop concepts, the team researched the various architectures that hobbyists and companies implement when using USRPs. The team came up with two implementation possibilities.

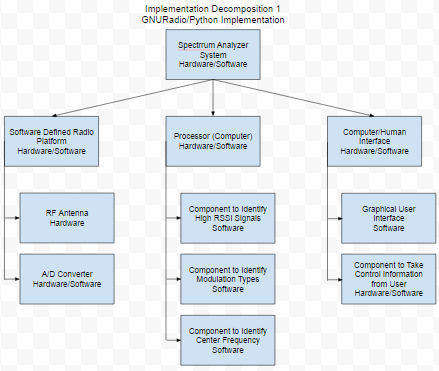


Figure 2 Implementation 1: GNURadio and Python

In implementation 1, all the signal processing and identification is done by a computer using Python code from GNURadio. In this implementation, the SDR front end serves only as the antenna and sampler. A computer will implement all of the software for this program, including the software components to identify high RSSI signals, modulation types, and center frequencies of relevant signals. Finally, an interface will allow the user to send commands to the program, and display the relevant information back to the user.

GNURadio is an open sourced software development toolkit that utilizes drag and drop blocks to create programs, and is widely used for Software Defined Radio applications. As GNURadio already has extensive libraries for signal processing applications, this implementation will give the most resources and developmental flexibility to the team from the outset. Many resources and tutorials exist for GNURadio as well as developmental tools and sources of expertise. Additionally, most of the current team already has experience with programming languages like Python.

The final performance of implementation 1 will ultimately be limited by the clock speed of the microprocessor system, and the speed at which it can read data from the A/D converter. All processing will have to be done by this processor, including the identification of the signals, their modulation, and their center frequency. The same system will also be handling controls and the graphical user interface to the operator.

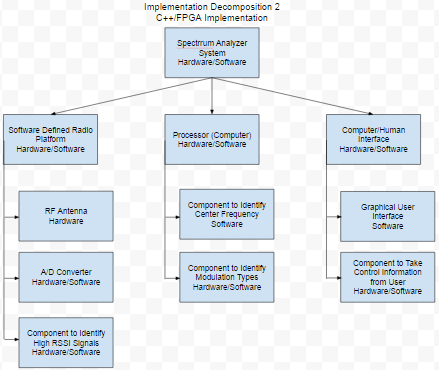


Figure 3 Implementation 2: C++ and VHDL

In implementation 2, some of the signal processing is offloaded onto an FPGA, programmed in VHDL or Verilog. The Software Defined Radio utilized again for its antenna and sampling capabilities, but the FPGA is used for its ability to perform signal processing calculations to reduce the load on the computer being used as the processor. Further efficiency improvements are made by implementing the rest of the of software for this system in C++, which is generally faster and requires less computational overhead than Python. In this implementation the interface is similar to the last, where there is a graphical user interface to display signal information and taking command information from the user.

The FPGA is not gated by the clock speed of a microprocessor, and can do a large number of concurrent operations much faster than a microprocessor. They are very good for signal processing applications. However, a large amount of specific expertise is required to properly create efficient code for an FPGA, and there are far fewer resources and libraries available for this specific application. Development time will be much longer than with Python and the effectiveness will be highly dependent on programmer skill, a team member specializing in this area would be highly recommended.

Implementation 1 is likely a better solution due to development time. Once the concept is proven sound and the device works, it might be possible to re-implement it with C++ and FPGAs (or ultimately custom integrated circuits) for better performance in future iterations.

## Design: Architecture, Materials, Layout, Manufacturing considerations

This project will be implemented using one or more Universal Software Radio Peripherals (USRP). Two platforms were available to our group: USRP X300 and USRP N210 (both designed by Ettus Research). Each has its own advantages and disadvantages. For our project, we will be handling the USRP N210.

Some specification about the USRP N210 model is that it provides high-bandwidth, high-dynamic range processing capability. The modular design allows the USRP N210 to operate from DC to 6 GHz, while a multiple-in, multiple-out (MIMO) expansion port allows multiple USRP N210 series devices to be synchronized. It can also stream up to 50 Mega-samples/second (MS/s) to and from host applications. Users can implement custom functions in the larger FPGA fabric which can process up to 100 MS/s in both transmit and receive directions.

For the programming aspect of this project, N210 are compatible with the USRP Hardware Driver (UHD) like all other USRP models. They are compatible with other third-party software frameworks, including GNU Radio companion software, LabVIEW, and Matlab. The UHD architecture, provides this powerful compatibility along with the ability to use APIs of C++ and Python, which will be mostly used for developing and analyzing our system of interest. This represents a combination of implementations 1 and 2, explained in the previous sections.

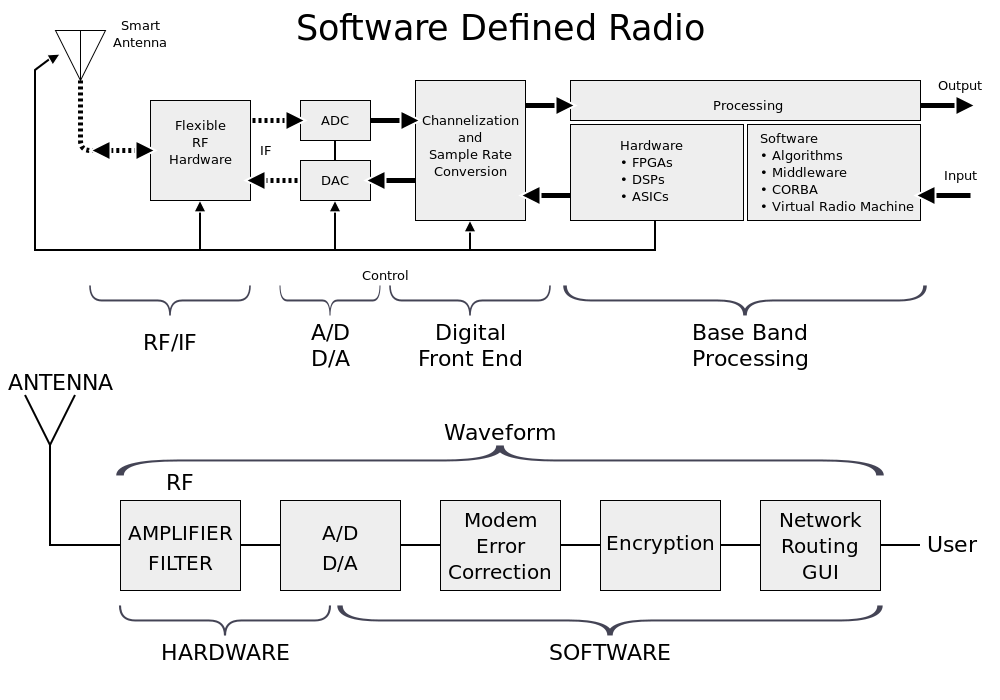


Figure 4 Software Defined Radio Architecture

A common model or system setup for SDRs is the SDR itself contains an antenna and the ability to sample signals at a given sample rate, and then a processor attached to the radio performs processing in terms of modulation and demodulation, FFTs, filtering, and other functions normally done on an FPGA in a traditional radio. SDRs still have FPGAs in a more flexible configuration that can still be controlled with software. SDRs are becoming especially useful learning and analyzing tools, especially for hobbyists and at universities for teaching at undergraduate and graduate levels.

## Design Evaluation Methods

## Methods: Analytical, Simulated, Physical Tests

Due to the nature of the project’s sponsorship, the group is equipped well enough to perform physical tests on the system that will equate to realistic use cases. Firstly, the group has been provided with two SDRs. This allows one system to be set-up as a transmitter, and the other as a receiver. Having a transmitter available means that the group now has the ability to feed signals of known characteristics into the receiver to test its performance. Additionally, the group is equipped to test over-the-air performance. This will be the intended use case, and with the use of GNURadio, realistic signal-to-noise ratios (SNR) can be achieved by adding noise to the system to best simulate a real scenario.

Once the transmitter is verified as being functional, the receiver can then be worked on. All further testing will take place in the form of signals being fed from the known working transmitter into the receiver, via a wired or over-the-air connection. The first evaluation for the receiver will be whether or not it can identify signals of X type (this will be dependent on the signal being worked on at the time; the group is starting from the most basic analog signals and moving towards more complex ones) that are fed in at a very strong SNR (roughly >40dB) over a wired connection. This will be the ‘best case’ scenario. If this case does not function as planned, it can be determined that a re-work is necessary. Once success is achieved in the ‘best case’, the SNR will be dropped by adding noise at the transmitter via GNURadio. The minimum SNR at which the receiver can identify a signal will be known as the sensitivity of the system. Repetitive tests will be done at various sensitivity levels to identify the success rate in identifying signals. This will produce a metric such as “the receiver can identify signals at a 10dB SNR with 70% success”. By the end of the project the group will be able to present a table of signal types and success rates at various sensitivity levels. Once an acceptable baseline is achieved, more complex scenarios can be tackled.

Prior test plans were isolated to single signals. Any over-the-air receiving will consist of multiple signal types and must be handled accordingly. The bandwidth of the receiver’s frequency range of interest will certainly impact scanning speed; developing an algorithm for scanning a given bandwidth centered on a given frequency is part of the development of this project. Benchmarking of the group’s algorithms will be performed by scanning a variety of bandwidths and recording the time it takes to complete the scan. These tests will have to be performed on an identical spectrum. Initially the scans can be performed when there are no signals present to isolate the scanning speed from other variables; this will be most useful internally, when developing the algorithms and testing the impact of code changes. When the spectrum scanning and signal identification portions of the project are merged, the group will have to perform additional testing to ensure that the results of the isolated tests are consistent with the merged product. A good test case for this stage of the project would be to randomly generate signals that the scanner can identify over a given bandwidth and to see how successful the receiver is in accuracy of identifying signals and in scan speed.

Once the group has done its best in signal identification and spectrum scanning algorithms, they will have tabulated data to present to stakeholders. This data will give stakeholders the ability to make conclusions such as “in under 2 minutes the receiver can complete a 500MHz scan and find all of X-type signals within an SNR of YdB”. Having these metrics will allow the stakeholders to identify if the project is usable for their needs and if the project has been a success or failure.

## Physical Prototyping: Plan and Budget

Due to the benefit of having a sponsorship with a large company, the group is able to immediately start working on a physical prototype. All development will be carried out on the platform that will be used for final production. So far, the only cost incurred has been a switch for the purpose of networking the radios to the development machine. Further development is to be done in software (requiring no extra funding).

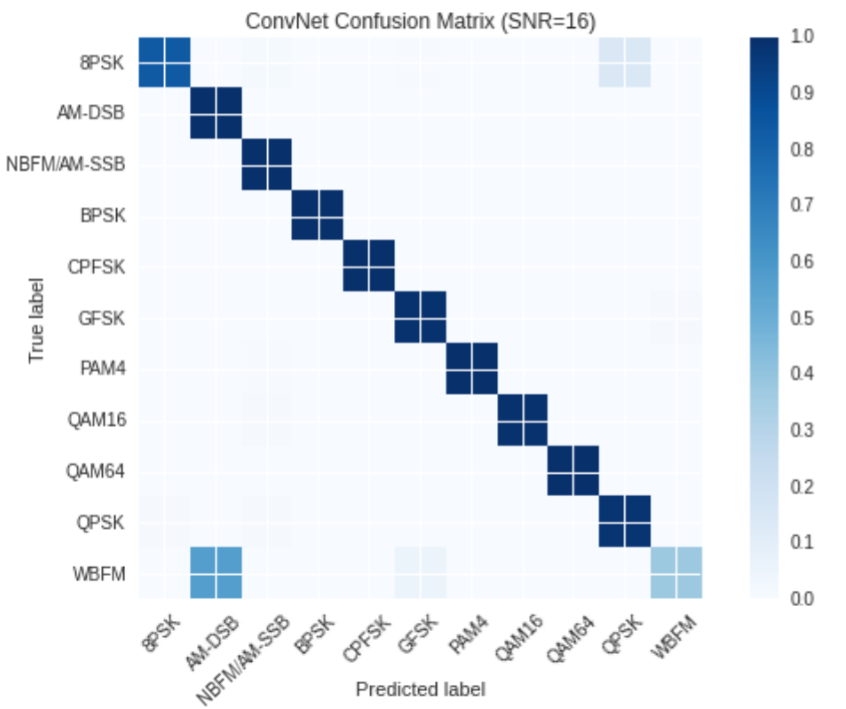
The final prototype will consist of two SDR platforms. One will be used as a transmitter strictly for demonstration and testing. The transmitter is not part of the final product, but is necessary for the group to arrive at the final product. The second SDR will be the receiver, the focus of the project. The only other hardware required is a laptop for interfacing with the radio and processing data. The sponsor has provided the means of connecting the laptop and radios to each other. The software making all of this possible is the focus of the group and will control the aforementioned hardware.

## Prototype Build and Test Report

The group has identified two main metrics to quantify the performance of this report: scan time and identification accuracy. Scan time, shown in Figure 5, shows there is a linear relation between the width of the given spectrum, and the time taken to scan that spectrum. These can be lowered with more testing.

Figure 5 Scan bandwidth versus time

The second metric is modulation classification accuracy, taken from the white paper upon which our machine learning code is based. On the vertical axis is the actual modulation type of a given signal, on the horizontal axis is the predicted label by the machine learning code, and the color of a given data point gives the percentage of times a modulation type was predicted given a certain type of signal. An ideal test would be shown as a dark blue diagonal line from upper left to lower right. Real testing shows that WBFM signals are often misinterpreted as AM-DSB, which we confirmed with our own testing.



## Design Evaluation Report: Performance, Reducibility and Cost

Performance will be the limiting factor of this design; the team is limited to the computing power of the computer, which is significant in processing heavy tasks such as Fast Fourier Transforms (FFT), which will be used significantly in this project. This can be significantly improved by implementing an FFT on the FPGA in the radio. This will offload an immense amount of calculation from the computer, but will take much more effort in implementation from the team, as currently none of the team have the expertise to implement an FFT on an FPGA.

There is very little to be reduced in this system. Two commercial off the shelf products are being used to complete this project with very little room for customization. On such reduction that could be implemented is the offloading of FFT processing to the FPGA of the radio.

For the capability the team is attempting to introduce, the cost is very good. The team is using approximately $6000 worth of commercial off the shelf hardware to implement a functionality that, when offered with less capability, is tens of thousands of dollars in the commercial world. Coupled that these costs were either already in the possession of team members or provided by the sponsor, there is very little project cost incurred to the team’s budget.

## Design Revisions and Optimizations

One design decision made is on which implementation to proceed. We have shied away from using GNURadio Companion, a graphical tool that allows a user to build signal processing flowgraphs by dragging and dropping functional blocks. GNURadio Companion has limitations such as not being able to implement if statements or for loops, which can be written using GNURadio’s Python APIs. GNURadio’s Companion outputs Python code, on which we based our signal processing, but altered extensively to better fit our needs.

## Final Design Specification with BOM

The final design specification consists of two USRP N210s connected to a COTS computer. The BOM is as follows.

|  |  |  |  |
| --- | --- | --- | --- |
| Item No. | Name | Description | Quantity |
| 1 | Software Defined Radio | USRP N210 | 2 |
| 2 | Laptop | Macbook Pro | 1 |
| 3 | Ethernet cables | CAT-5 | 3 |
| 4 | Ethernet switch | TRENDnet 5-pot Unmanaged Gigabit Switch | 1 |
| 5 | 2450 MHz Antenna | Vert2450 Antenna Ettus Research | 2 |
| 6 | 900 MHz Antenna | Vert900 Antenna Ettus Research | 2 |

# Section – III: Entrepreneurship & Business Development

## Business Objectives and Risks

Due to the nature of the project and the nature of MITRE as a company, there are minimal business objectives associated with the project. MITRE acts as a non-profit military contractor, so it does not make a profit and does not make products with the intent of being marketed to a broader consumer base. Our main business objective is to create a product that the army would be interested in acquiring or investigating more.

## Competitive Intelligence: Market Analysis

Currently there is little in the way of competition for our product. Other software that exists to perform similar tasks has limited functionality and is not capable of providing the full scope of information that our product will be able to provide. Additionally, the software is always bundled with expensive hardware designed for use in the field. Our software will be easily available independently as well as providing greater functionality than the competitors. It will allow for separate hardware purchases that may be cheaper or custom made. Due to the unique nature of our sponsor and product, other issues such as the target audience of our product and the cost at which it will be sold are not factors. This also allows the software to be tailored very specifically to the needs of our only current customer, the army, which provides a secondary competitive advantage when compared to companies making similar products.

## Lean Canvas Business Model

  A lean business model canvas was developed that displays market information for the system. Due to the nature of MITRE, our business model is very well defined and circumvents most of the problems projects encounter. Our project is the rough equivalent to the government contacting freelance workers to do unpaid work. Our problem, solution, metrics, and our unique value proposition was all passed down to us directly. We knew they had the problem of dealing with bulky signal processing equipment, and we were suggested to use a software defined radio. We were provided a receiver to build off of as well as recommendations of software to use to start. Because we have one customer with very clearly defined somewhat niche needs who has a monopoly on the work produced, anything to do with marketing or market research or cost is totally null.

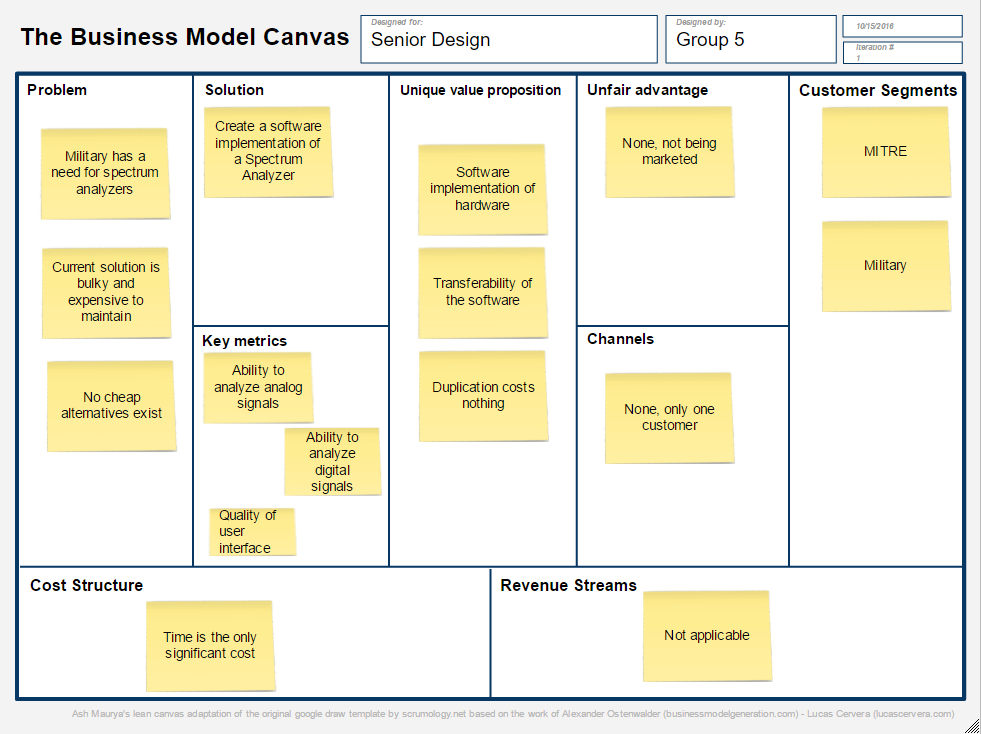


Figure 6 Business Model Canvas

## Financial Analysis

**Cost and Pricing Revision**

**Cost of Materials**:

Quantity 10: 4000

Quantity 100: 3700

Quantity 1000: 3400

Materials include a laptop, 2xSoftware Defined Radio, Ethernet cables, RF cables, antennas. All parts would qualify for a discount if purchased in bulk.

**Cost of Testing and Manufacturing**:

Assuming costs are per unit

Quantity 1: 2000

Quantity 2: 2000

Quantity 3: 2000

Manufacturing is not a factor as the products are off the shelf. Labor costs are fixed, so cost per unit would be identical.

**Selling Price**:

Adding slight markup to the sum of the previous two costs…

Quantity 1: 15000

Quantity 2: 14500

Quantity 3: 14100

**Profit per Unit**:

Quantity 1: 9000

Quantity 2: 8800

Quantity 3: 8700

Number of units estimated to be sold in year one: 35

Total Project Duration: .5 years

Number of Workers Needed: 5

Payment Breakdown for Workers: $70,000/year

Cost of Machinery/Materials: 5000 (computers for development)

Other: 10000 (In case…)

Total Cost: $190,000

**Revenue Projection, Breakeven Point, Gross Margin, and Overall Evaluation**

Revenue projected at EOY 1: $315,000

Profit at EOY 1: $125,000

Breakeven Point: $190,000

Gross Margin: 39.68%

What does this mean for an investor?

Based on the financial projections, we will make a profit of 40% on each dollar spent.

Price:

Competitor 1: $50,000

Competitor 2: $150,000

Customer/Investor Cost Savings:

35,000 per unit

## Intellectual Property

Intellectual property has not yet been identified between the sponsor and the project team. At this point, the team has a spoken agreement to not reveal proprietary information to outside people, and we will resolve whether the project team or the sponsor owns the intellectual property. As of now, our only goal is to deliver our project to the Army successfully.

# Section – IV: Results

## Conclusions

This spectrum sensing project’s goal to demonstrate spectrum sensing using widely available hardware and open source software. The team has begun to isolate signals and classify modulation of those signals across a wide spectrum using efficient. The team has all been familiarized with GNU radio as well as the basic requirements for what the project entails. The website has been established successfully and network connection is established to the receivers, allowing the team to work on the project from home. Version control, a method for sharing thoughts and work, as well as a weekly schedule have been established.

* At high SNR (over 20 dB), our analog modulation results are comparable to the white paper’s results.
* More testing would be needed to assess the accuracy of the system when presented with digital modulation signals.
* Wideband – FM signals are misidentified as AM-DSB, as also found by the white paper.
* The machine learning model could be improved with more real signal learning, and deploying the production version of TensorFlow – TensorFlow Serving. TensorFlow builds and trains

neural networks to detect and decipher patterns and correlations, analogous to the learning and reasoning which humans use.

## Recommendations

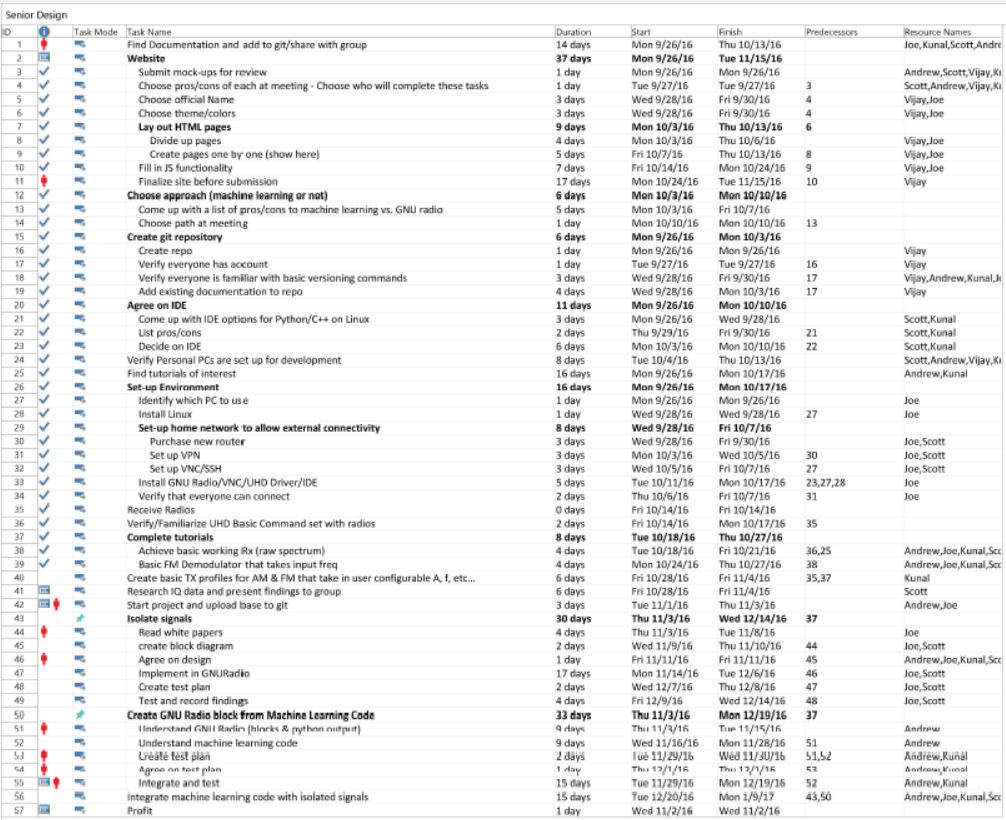
For the current step of making a basic working model, there is only a small recommendation for the scope of this project. Currently, our model is implemented in python for efficiency, so it may not be as fast as C/C++ based software. In the future, if the software defined platform is flexible with variety of programming languages, then the maximum benefit of the platform could be achieved than what is currently being possessed including the low cost and low power consumption. In order to develop a successfully working simple model, both sub-teams are communicating well and have established a methodology to do their respective tasks. Once this is completed, the next step will be to optimize and add new features into our model. This is a very broad goal for which we have not established specifics. In the broadest sense, we are looking to get as many signals identified and demodulated as fast as possible and achieve expected accuracy at the same time. One of our ideas is implementing parts of our software using specialized hardware chips for mathematically heavy work. Another idea is modifying the machine learning algorithm to run with high accuracy as well as at a greater rate. These are both topics which are currently secondary and will be researched further in the near future. Moreover, in order to show the input and output of our model visually, we are using are Python’s standard GUI package Tkinter. Using this robust package, we will be able to show and explain the structure of our design to any person with non-technical background and also to help anyone understand our project easily.

# Appendices

1. **Team organization chart**



1. **Project Gantt Chart**



1. **Prototyping and Testing Budget**

Projected as of 2 May, 2017:

Gigabit Ethernet Switch: $20

Walkie Talkies for demonstration: $30

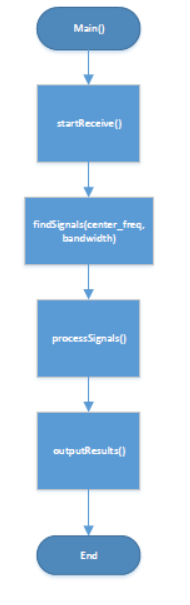
Actual as of 2 May, 2017:

Gigabit Ethernet Switch: $18

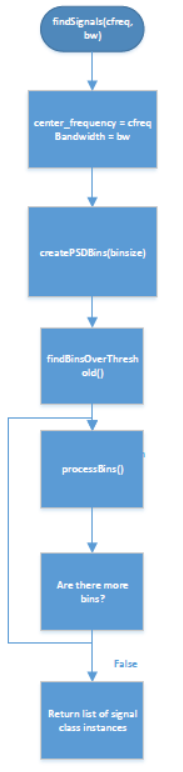
Walkie Talkies for demonstration: $36

1. **Design Documents: Drawings, Layouts, Analysis reports**

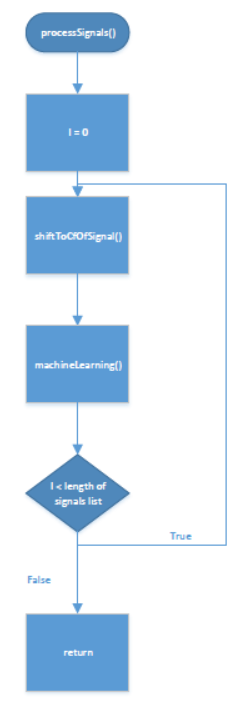
Main Signal flow:



Finding Signals:



Processing Signals:



1. **References cited**

“A short history of software-defined radio (SDR) technology” Nutaq, <http://www.nutaq.com/blog/short-history-software-defined-radio-sdr-technology>

Before the Federal Communications Commission Washington, D.C. 20554, In the Matter of Inquiry Regarding Software Defined Radios, FCC Cong., 7 (2000) (testimony of Featherstun, Frolio, Harralson, Schwarz, on belhalf of BellSouth).

Birmingham, W., & Acker, L. (2007). Software-defined radio for undergraduate projects (1st ed., Vol. 39, ACM SIGCSE Bulletin, pp. 293-297, Tech. No. 1-59593-361-1). New York, NY: SIGCSE.

Blum, Josh. "Introductory Tour of the GNU Radio Project." Josh Knows. N.p., n.d. Web. 08 Mar. 2016.

Clancy, T. Charles, and Nathan Goergen. "Security in Cognitive Radio Networks: Threats and Mitigation." 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008) (2008): n. pag. Web.

"Overview - GNU Radio - Gnuradio.org." GNU Radio. GNU Radio, n.d. Web. 08 Mar. 2016.

RF Allocation chart in the US: https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

RoHS Guide. (n.d.). Retrieved March 14, 2016, from http://www.rohsguide.com/

USRP N210 Information, from https://www.ettus.com/product/details/UN210-KIThttp://gnuradio.org/redmine/projects/gnuradio/wiki

http://www.xilinx.com/appnotes/dspintro.pdf