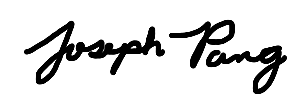
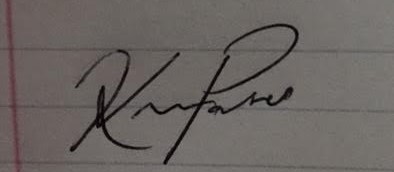
SPECTRUM SENSING and SIGNAL IDNETIFICATION using USRP

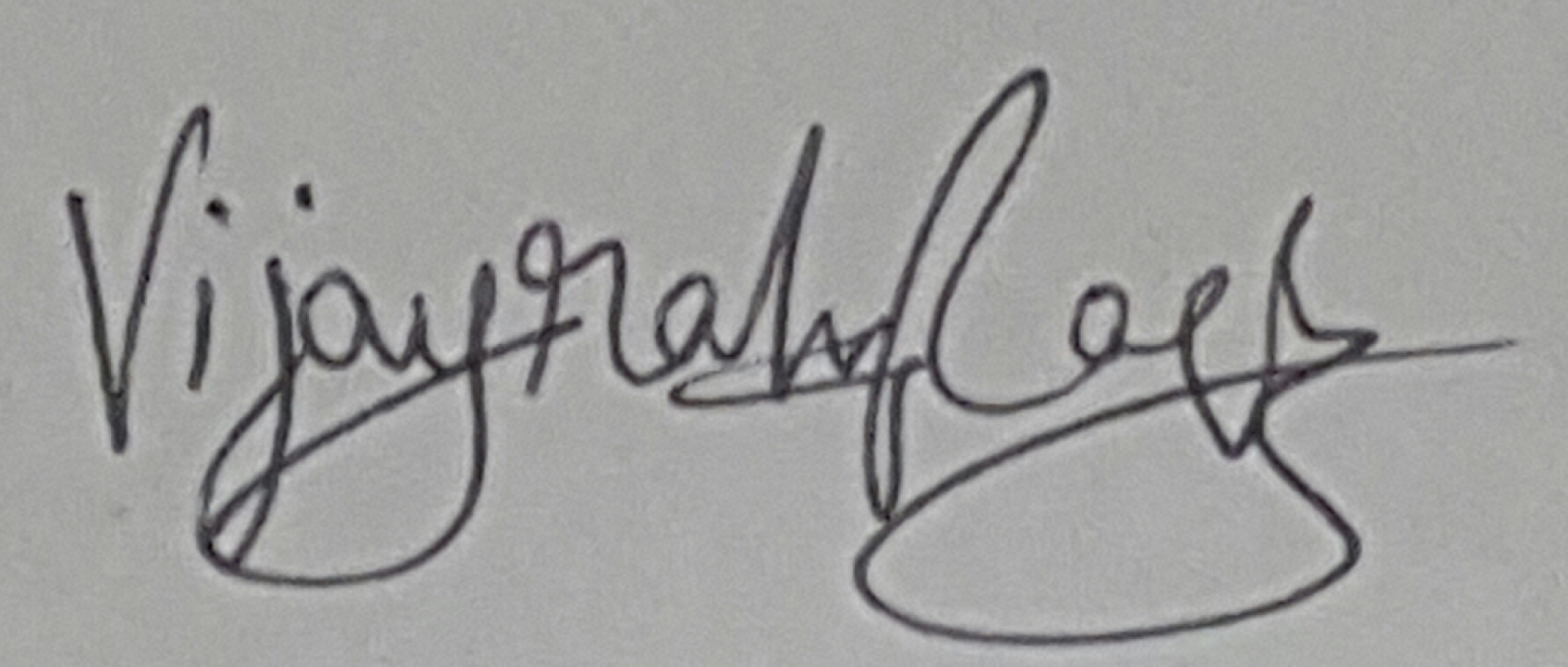
Spring Interim Report

Group 5

“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. More information will be included in this section as the team discusses intellectual property and information appropriate to publish with the sponsor.

# Executive Summary (start in Fall, Flesh out in Spring)

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 signals and then isolate them, 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. Early testing shows a signal processing time of around .1 seconds. Through several optimizations, the team hopes to get this time down to less than .01 seconds. The team is preparing for a pitch in front of mock investors, and will be ready for Design Day on April 5. The executive summary will include more information as it comes about and is relevant in future iterations of this report.

# Table of Contents

[Executive Summary (start in Fall, Flesh out in Spring) 4](#_Toc468786908)

[Table of Contents 5](#_Toc468786909)

[Section – I: Project Definition and Plan (initial in Fall, refined in Spring) 7](#_Toc468786910)

[1. Mission Statement 7](#_Toc468786911)

[2. Background 7](#_Toc468786912)

[3. Stakeholder List 8](#_Toc468786913)

[4. Analysis of Stakeholder Needs 11](#_Toc468786914)

[5. Project Scope and Resources 12](#_Toc468786915)

[6. Project Plan 12](#_Toc468786916)

[Section – II: Design, Evaluation & Optimization (initial in Fall, refined in Spring) 13](#_Toc468786917)

[1. Requirements 13](#_Toc468786918)

[2. Constraints and Assumptions 14](#_Toc468786919)

[3. Applicable Codes/Standards/Regulations 15](#_Toc468786920)

[a. Professional and Ethical Issues 15](#_Toc468786921)

[4. Concept Development and Selection 16](#_Toc468786922)

[5. Preliminary (Fall) and Detailed Design (Spring): Architecture, Materials, Layout, Manufacturing considerations 18](#_Toc468786923)

[6. Design Evaluation Methods 19](#_Toc468786924)

[a. Methods: Analytical, Simulated, Physical Tests (Fall) 19](#_Toc468786925)

[b. Physical Prototyping: Plan and Budget (Fall) 20](#_Toc468786926)

[c. Prototype Build and Test Report (Fall/Spring) 21](#_Toc468786927)

[7. Design Evaluation Report: Performance, Reducibility and Cost 21](#_Toc468786928)

[8. Design Revisions and Optimizations (Fall/Spring) 22](#_Toc468786929)

[9. Final Design Specification with BOM (spring) 23](#_Toc468786930)

[Section – III: Entrepreneurship & Business Development (primarily TG course requirements) 23](#_Toc468786931)

[1. Business Objectives and Risks (Fall) 23](#_Toc468786932)

[2. Competitive Intelligence: Market Analysis (Fall) 24](#_Toc468786933)

[3. Lean Canvas Business Model (Fall) 24](#_Toc468786934)

[4. Financial Analysis (Spring) 25](#_Toc468786935)

[5. Intellectual Property (Spring) 25](#_Toc468786936)

[Section – IV: Results 26](#_Toc468786937)

[1. Conclusions 26](#_Toc468786938)

[2. Recommendations 26](#_Toc468786939)

[Appendices 27](#_Toc468786940)

# Section – I: Project Definition and Plan (initial in Fall, refined in Spring)

## Mission Statement

The Spectrum Sensing using USRP 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 will be 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 project will be sponsored by MITRE, 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 process 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 in theory 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 off of 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, 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 (initial in Fall, refined in Spring)

## 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: Amplitude Modulation, Frequency Modulation, and Phase Modulation.
      2. The system shall be able to identify the following digital modulation schemes: Binary Phase-Shift Keying, Binary Frequency Shift Keying, and Amplitude-Shift Keying.
3. The system shall scan a spectrum larger than the instantaneous bandwidth of the radio at least twice every second.
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 graphically the RF spectrum it is analyzing.
      2. The system shall display textually signals it identifies.
      3. The system shall indicate RF bands it identifies as unused.
   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.

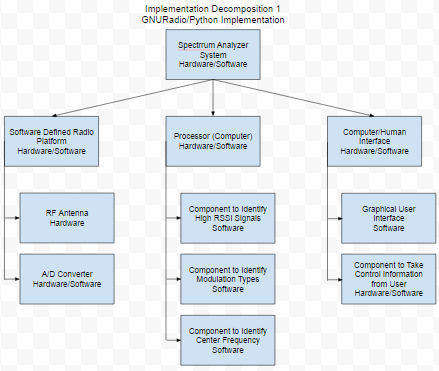


Figure 2 Implementation 1: GNURadio and Python

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 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.

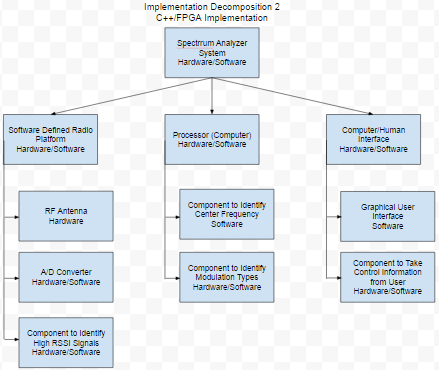


Figure 3 Implementation 2: C++ and VHDL

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.

## Preliminary (Fall) and Detailed Design (Spring): 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.

The USRP N210 provide high-bandwidth, dynamic range processing capability. The daughterboard in the radio 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-per-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 the transmit and receive directions.

USRPs interface with software through the USRP Hardware Driver (UHD), which provides a multitude of C++ and Python APIs. These APIs are compatible with other third-party software frameworks, including GNU Radio, LabVIEW, and Matlab. The team is using the UHD APIs extensively to interact with the signal processing blocks provided by GNU Radio. This represents implementation 1, explained in the previous sections.



Figure 4 Physical Architecture

The final configuration for the project became one USRP to receive broadband RF power to find signals, one USRP to capture samples of specific signals, and a computer to perform all of the processing. These major components are networked together through a Gigabit Ethernet switch, giving rise to the physical architecture shown in Figure 4. Software architecture is much more complex, thus architecture models are provided in Appendices Section D.

## Design Evaluation Methods

## Methods: Analytical, Simulated, Physical Tests (Fall)

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 (Fall)

Due to the benefit of having a sponsorship of 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 open-sourced 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. The prototype will be used to perform demonstrations that reinforce tabulated performance data using generated and over-the-air signals.

## Prototype Build and Test Report (Fall/Spring)

Early prototype testing showed about .55 seconds from signal input to information output. One level lower, this means it took one-tenth of a second for the signal power to be received by one radio, identified in GNU Radio, pushed to a queue, then pulled from the queue, the other radio tuned to the frequency of the signal, then a sample of the signal captured and sent to the machine learning algorithm. The completion of an end-to-end test was good, but the latency left much to be desired.

The team then formed latency goals. Starting at .55 seconds for a full system run through, it was determined that goals would be .1 seconds as a safe goal, .01 seconds as a realistic goal, and .001 seconds as a reach goal. Several ways to improve the latency of the system were identified, and the team current has the model running at right around .1 seconds, reaching our safe goal. The team has further identified that about 80% of the current run time is in one step that can be greatly reduced. Options in GNURadio will allow this time to be greatly reduced (GNURadio has a bandwidth-latency tradeoff that will be adjusted more to the latency side).

As data is received through further testing, this section will include further numerical data showing the progress in reducing latency of the system. The team has achieved the “safe goal” and expects to achieve the “reasonable goal” in the next couple of weeks. Research has shown that the “reach goal” may be unattainable because of radio hardware limitations (i.e. one refocus of a frequency takes about .002 seconds, which is above that goal).

## Design Evaluation Report: Performance, Reducibility and Cost

Preliminary testing has given the group a performance baseline that can be assessed for progress and improvement. The first integrated, full-system run scanned a given area of the RF spectrum consisting of a single, known signal, and identified the modulation type of the signal using machine learning. The successful run is the product of hard work on many fronts by the entire team, and leaves clear areas for improvement.

The integrated test used a fixed 1MHz bandwidth. This was to keep some calculations (such as FFT bin size, and thus identified signal bandwidth) fixed and simplified. The final requirement is to have a bandwidth that is much larger than 1MHz if the user desires. This may have to be done by breaking up the desired bandwidth into smaller, more manageable sections of the spectrum. The constraint for the largest bandwidth that can be scanned without performing broken-up scans is the front-end noise performance. Scanning a large bandwidth has implications on the noise floor of the receiver that would negatively impact system performance.

Next, the signal detection algorithm can be improved. Instead of relying on a user configured squelch value, statistical analysis can be performed on the power spectral density (PSD) to compare the signal levels to the mean based on a threshold number of standard deviations.

Performance, rather than cost or any other constraint, is the limiting factor in this project. The most significant limitation is computing power, which is a valuable resource in processing heavy tasks such as Fast Fourier Transforms (FFT), which are used significantly in this project. This leads to increased runtime. The main focus of the optimization and refinement stages (along with improving accuracy, mentioned above regarding signal detection algorithms) is reducing system runtime.

Runtime can be significantly improved by implementing an FFT on the FPGA in the SDR. 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. A more costly laptop would likely make the software run faster but not on a magnitude that would mask a poorly written piece of software, so it would be best to write good software and not rely on marginal hardware gains in this area. Lastly, optimizing any software developed by the group is the area in which the group will spend the largest amount of time. Reducing the portions of code spending the most amount of time, the group can drastically reduce runtime.

There is very little to be reduced in this system in terms of hardware and cost. Two commercial off the shelf products are being used to complete this project with very little room for customization. For the capability the team is attempting to introduce, the cost is very good. The team is using approximately $3000 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 (Fall/Spring)

The first set of design decisions consisted of choosing between a standard development environment (IDEs, Operating System, version control). This laid the foundation for smooth development and progress through the entire project.

Next, it was decided to first work on the transmitter and then the receiver. It was decided that the transmitter should have several profiles of known signals (FM, AM, etc.) made with configurable parameters so the group could use the transmitter to feed signals into the receiver at later stages in the project.

Dividing up subtasks that project must complete was done next. The machine learning, signal identification, and signal data gathering portions of the code were delegated to separate members of the group. This was done with the main intention of working in parallel, and putting group members where their skills suit them best.

The team decided that the GNURadio Companion, a graphical tool that allows a user to build signal processing flowgraphs by dragging and dropping functional blocks, was too limiting and decided to move to strictly python based code. The group spent time learning how GNURadio Companion works, and that knowledge will definitely not be wasted using the python API for GNURadio, using python based code will allow much more flexibility as to what the program can accomplish.

The machine learning section of the group decided to focus efforts firstly on getting an interface that can work with the rest of the program, and then on having an effective means of training the software with known signals separately from the main operation of the code. This means that the software can be run quickly, recalling previous training data rather than having to train the program at runtime.

Initial signal identification efforts were made using a static squelch value that the user would have to set manually. Setting the squelch value just above the noise floor would effectively only show valid signals. This method is not preferred however, as the system should not rely on manual user input of the squelch value. The group decided that statistical analysis on the Power Spectral Density bins would work best in determining existent signals. The group will compare the mean noise level to each bin, triggering a signal if the bin is a certain threshold amount of standard deviations away from the mean.

## Final Design Specification with BOM (spring)

|  |  |  |  |
| --- | --- | --- | --- |
| **Description** | **Quantity** | **Cost to Group ($)** | **Estimated Actual Cost ($)** |
| Laptop | 1 | 0 | 700-2500 |
| ETTUS N210 SDR | 2 | 0 | 1200-2500 |
| SMA Antenna - 850MHz | 4 | 0 | 5-30 |
| Ethernet Cable | 3 | 0 | 15-45 |
| Network Switch | 1 | 10 | 10 |

# Section – III: Entrepreneurship & Business Development (primarily TG course requirements)

## Business Objectives and Risks (Fall)

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 doesn’t make a profit nor make products with the intent of being marketed to a broad consumer base. On the other hand, our major business objective for this project is to create a product that the army would be interested in acquiring, testing and investigating further. Our focus is mainly on commercial-off-the-shelf hardware and open source platforms which keeps our costs to a minimum, and allows us to offer our product to customers at a price unmatchable by our competitors. Success criteria focuses on the product’s ability to accurately identify anomalous signals. Innovation develops from using our low cost hardware to perform a very complex task reliably, and using key machine learning algorithms to have the product to continuously train itself and become smarter, produce efficient results over time.

## Competitive Intelligence: Market Analysis (Fall)

Currently there is little in the way of competition for our product. Target competitors are other defense contractors in the defense industry and the wireless communications industry. Due to the nature of this industry it is difficult to know what the competitors offer, however the group has operated under MITRE’s guidance especially during the project development phase to ensure that the project has an edge against any competition.

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. 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.

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 (Fall)

  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.

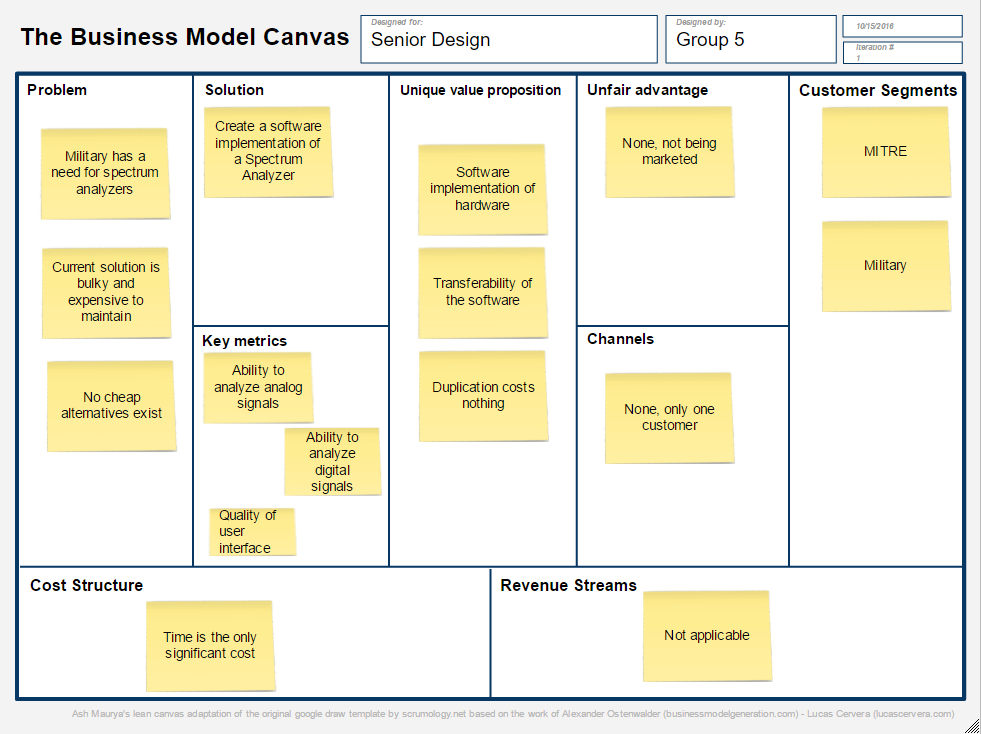


Figure 5 Business Model Canvas

## Financial Analysis (Spring)

Making a financial analysis, our team decided to sell a laptop along with USRP and its necessary software packages starting at $8,500. Additionally, there is opportunity for licensing the software to users who already have the software. This amount was decided based on the cost of materials (laptop and front-end) and the time spent designing and implementing the system. This cost is significantly cheaper than what the army currently has available to them, and still leaves room for profit if one was to sell this product for that purpose. Additionally, licensing the software would bring a very steady income on a monthly or yearly basis that could be used for further development costs.

## Intellectual Property (Spring)

Intellectual property for any tools and assistance given by MITRE is their belonging, whereas any development by the team belongs to the team. At this point, the final project has not been formally presented to MITRE, so more IP discussions can occur once MITRE assesses the quality of the teams work. The team has decided to initially have a successfully working prototype for Senior Design day and observe feedback of the visitors from viewing and analyzing the prototype. If the group receives positive feedback from these events, the group will proceed further by discussing about patents and other necessary disclosures with our sponsor MITRE.

# 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 all been established.

Currently the team has sub-divided into working on two major tasks. One of the major tasks is identifying signals from a broad spectrum radio scan. The other major task is using key machine learning tools to identify modulation once the signal has been identified so it can then be demodulated. Especially machine learning software library Tensor flow helps the team by providing necessary functions to achieve and analyze the modulation of signals. The team is motivated towards optimizing our basic working model, a point we are very close to reaching. Our project meanwhile has many significant benefits in terms of design. The GNU Radio program which is an Open source platform has the availability of all components and it is key to making this project stand out. Implementing the model is low cost compared to other options on the market.

## Recommendations

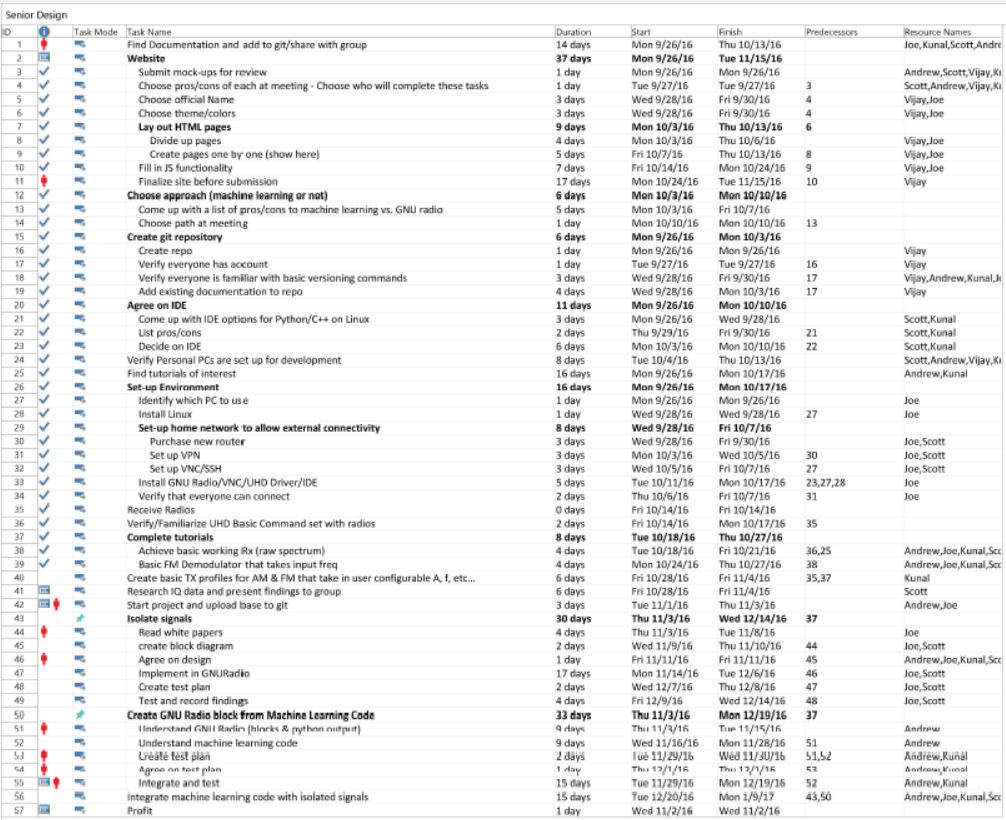
For the current step of making a basic working model, there is only a small recommendation for the scope of this project. Currently, our model is implemented in python for efficiency, so it may not be as fast as C/C++ based software. In the future, if the software defined platform is flexible with variety 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 design, both sub-teams are communicating well and have established a methodology to do their respective tasks. Once this step is finished, the next step will be optimization. This is a very broad goal which we have not established specifics for as of yet. In the broadest sense we are looking to get as many signals identified and demodulated as fast as possible. 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 more 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.

# Appendices

1. **Team organization chart**



1. **Project Gantt Chart**



1. **Prototyping and Testing Budget (projected – Fall, Actual –Spring)**

Projected as of 5 December, 2016:

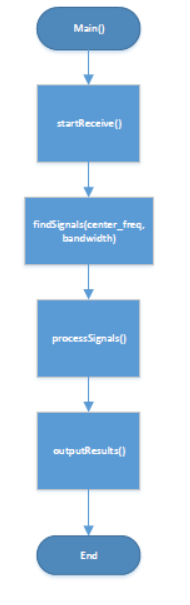
Gigabit Ethernet Switch: $20

Actual as of 5 December, 2016:

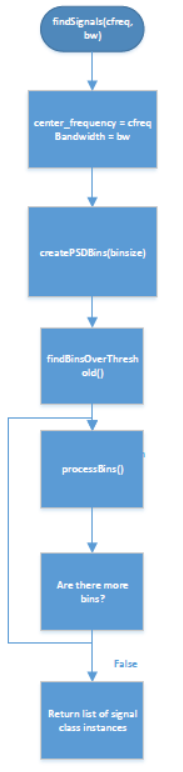
Gigabit Ethernet Switch: $18

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

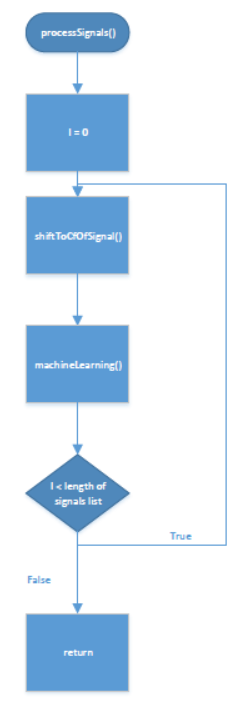
Main Signal flow:



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