Identification Friend-or-Foe (IFF) Infantry System

ECE4012 Senior Design Project

SixPlus Team
Project Advisor, Dr. Tentzeris

Vijay Krishnan vvkrishnan@gatech.edu, Team Leader
Vishal Devidas, vdevidas3@gatech.edu, Software Lead
Donghoon Han, dhan46@gatech.edu, Design & Testing Lead
Rishabh Patel, rpatel436@gatech.edu, Web Master
Kevin Waddles, kwaddles3@gatech.edu, Hardware Lead

Submitted

2019 Dec 2

Executive Summary

In the chaos of a battle, identification of forces can be a challenge, especially when warring sides share similar camouflage patterns and are usually hidden behind obstacles. The challenge of distinguishing a soldier as a “friend” or a “foe” can lead to an inadvertent attack by a military force on their own forces while attempting to pursue an enemy.

Current military organizations employ Identification Friend-or-Foe (IFF) systems to distinguish allied forces from enemies. IFF systems “enable military and civilian air traffic control interrogation systems to identify aircrafts, vehicles or forces as friendlies, and determine their bearing and range” [1] by autonomously receiving and transmitting RF signals. IFF systems are also widely used in the military to identify unmanned aerial vehicles (UAVs).

While current IFF systems are primarily used in large scale regulation (military vehicles and fighter aircrafts), it has yet to be developed for use by ground forces. Given that there have been several incidents of fratricide throughout the course of modern warfare (most notably, in the “1991 Gulf War where 24% of the 148 U.S. battle deaths were due to friendly fire” [2]), the production of an IFF system for ground troops is a necessity.

The team will design and prototype a lightweight, portable IFF system (named SP-READ) which can be fashioned and utilized by infantry soldiers. The IFF system also has the potential to be used in training exercises in which new recruits can improve their skills in hostile detection within a contained environment.

The expected outcome of the design is to produce a fully functional prototype within a $700 budget provided by the ATHENA Lab and the ECE 4012 Department.

Table of Contents

SixPlus Radio Encrypted Awareness Device (SP-READ)

1. Introduction

The Six Plus team will design an infantry IFF system which enables ground troops in the military to identify soldiers as a friend or a foe. The team is requesting $700 towards the development of the SP-READ prototype.

1.1 Objective

The team will design and prototype a system that enables ground troops to accurately identify friendly targets. SP-READ functions as a two-factor identification system mounted on a soldier's forearm and firearm respectively, which will communicate with the SP-READ of a given target to confirm identity. All soldiers will be equipped with a Bluetooth module that will function as an active encrypted beacon. When a soldier is prepared to identify a target, he/she will switch their beacon to a listener mode and decrypt the target soldier's active beacon. Once the signal is decrypted successfully, SP-READ will wait for a 'line-of-sight' confirmation by another signal that is transmitted by the systems' transceiver unit. The transmitted signal will be reflected via a Van Atta reflector array which will be present on the target. This reflected signal from the target's Van Atta array reaches the aggressor soldier's Van Atta tag where the SP-READ on the aggressor soldier's arm can now accurately identify an unknown target as a friend or a foe. In the event a Van Atta deciphers that a target is not in the 'line of sight', but the Bluetooth unit identifies that the target is in the senders' vicinity, the sending soldier will be notified accordingly.

1.2 Motivation

Incidents of friendly fire have plagued warring sides through the course of modern warfare. During the Gaza War of 2003, “three soldiers were killed and 24 others were injured” [3]. Moreover, during the Syrian Civil War in 2017, the United States military incorrectly identified a group of soldiers as adversaries, leading to an accidental attack resulting in 18 deaths [4]. Additionally, a recent analysis of empirical data from the Vietnam War and Operation Desert Storm report fratricide rates of 2% [2].

As a response to friendly fire incidents, IFF Systems were developed for military vehicles and fighter aircrafts for identifying aerial vehicles as a friend or a foe. Although the current IFF Systems prevent accidental firing among military vehicles, IFF systems protecting ground troops from friendly fire are underdeveloped. The SixPlus team will develop and prototype a system designed to protect ground troops from friendly fire incidents. Although IFF Infantry System solutions are under development by governments throughout the world, such solutions are not priced commercially. The SixPlus team will ensure sophisticated prototype functionality by making the device secure from adversary spoofing attacks, a common issue with beacon incorporated design. This prototype offers a commercially available IFF Infantry System which is expected to cost $700 for development.

1.3 Background

Extensive research has been devoted to the development of IFF Systems for preventing friendly fire incidents. Although the research primarily focuses on developing IFF Systems for military vehicles and fighter aircrafts while IFF Systems for protecting ground troops are still underdeveloped. Researchers at Cornell University have developed an IFF System for Infantry; however, that system utilizes laser for signal propagation which requires ideal weather conditions for expected functionality, and the system is limited to close proximity operation [5]. The SixPlus team will develop a prototype which would provide similar functionality to the Cornell University's research; however, the team's prototype will utilize RF in conjunction with Bluetooth for a multi-factor authorization, as opposed to simply using laser.

2. Project Description and Goals

The primary objective of the SixPlus Team is to develop a working system that successfully differentiates individuals as a friend or foe. The operating principle behind this system involves two main components: a broadcaster and a transponder. These devices will communicate wirelessly through radio frequencies (24 GHz). The broadcaster will consist of an antenna, amplifier, and signal processing hardware. The transponder is composed of an FMCW radar, a pre-identification processing unit that encrypts/decrypts the data, and a passive Van Atta reflector array that reflects a signal upon reception. These devices will be advertised to defense companies, military organizations and potential civilian hunters. System features are as follows:

General

- Bluetooth range of 500 meters, Van Atta range of 10-20 meters

- Target cost is less than $700
- Low power consumption (mWs of power)

Broadcaster

- Aimed signal transmitted has 10 degrees of coverage

Decoder (Transceiver Unit/Van Atta Array/Bluetooth Module)

- Smart reflector badge that reflects transmitted signal with +/- 2 degrees of error
- Lightweight and durable badge affixed to combatant's gear
- Successful encryption/decryption processing of signals

3. Technical Specifications & Verification

Table 1. Van Atta Specifications

Operational Frequency	24GHz
Power Consumption	120mW
Functional Range	50m to 100m
Reflection Precision	+/- 2 degrees
Battery Life	2 hours

Table 2. Transceiver Unit (FMCW)	
Frequency Range	24.025 GHz – 24.225 GHz
Chirps	Chirp Time: 3000 us, Samples per Chirp: 32, Chirps per Frame: 42, Shape: upchirp
Bandwidth	200 MHz
Antennas	RX: 2, TX: 1
Device Settings	RX BGT LNA Gain: Enabled

Table 3. Beacon/Signal Authentication Specifications	
Levels of Encryption	2 levels (8-bit preliminary encryption with 4-bit variable encryption with Key Management)
Type of Encryption	American Encryption Standard (suggested)
Signal Type	Bluetooth Beacon with configured 8-bits stream
Encryption Resolution	8 bits for authentication
Bit Error Rate	3.125% (1 bit per 32 bits)
Table 4. Multi-Feedback Infinite Gain Bandpass Filter Specifications	

Mid-Band Gain (AV)	16.000
Critical Frequency	106.355 kHz
Quality Factor	9.351

Table 5. Total System Specifications (SP-READ)	
Total Power Consumption	
Operational Range	20m – 30m
Operational Frequency	24 GHz
Weight	
Supply Voltage	9V Battery, 5V Power Bank

4. Design Approach and Details

4.1 Design Approach

There are two main aspects to the success of the IFF (Identification Friend or Foe) system: A Van Atta reflector tag which provides line-of-sight confirmation, and an encrypted Bluetooth beacon module which confirms target identity and proximity. Fig. 1a displays the block diagram of the system and Fig. 1b displays a sketch of the implementation.

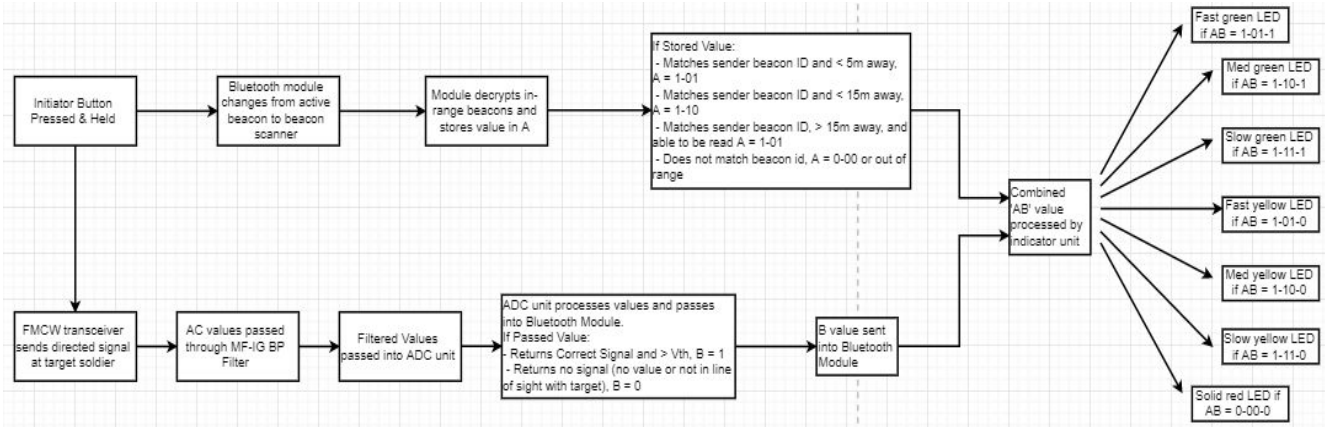


Figure 1a. Block Diagram of System

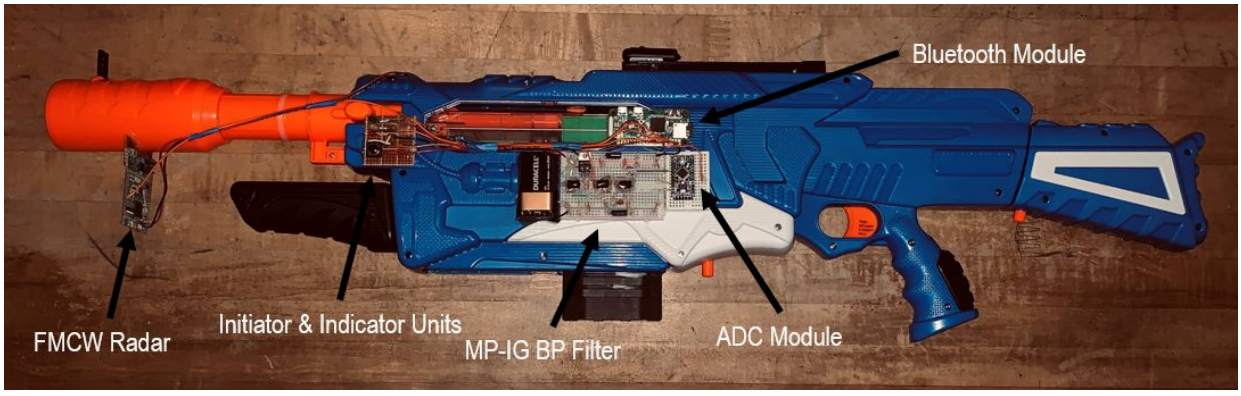


Figure 1b. Full System Schematic

4.1.1 Van Atta Reflector

Functionality

The Van Atta Reflector array is one of the most important elements in the system design. When it receives an incoming signal, the device reflects this wave by adding a phase respective to the point of incidence such that all incoming waves will be transmitted as outgoing in a uniform direction. This ensures that signals transmitted to the Van Atta reflector will be received with great accuracy. The functionality of this phenomenon can be seen in Fig. 2.

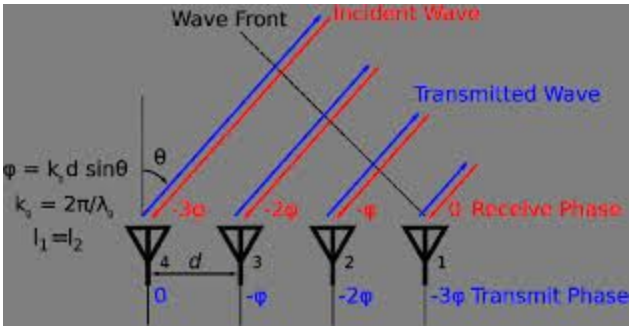


Fig. 2. Van Atta Reflector function

Power

The Van Atta Reflector tags operate at 24 GHz with 70 mW power consumption. Power to the Van Atta reflector array can be distributed through batteries, or solar panels. While solar panels will provide a sleeker, light-weight design, they are not as damage resistant as batteries and have variable performance (due to sunlight availability). For these reasons, batteries, which are more damage resistant, easily replaced and cheaper, are used in the implementation design. Two AAA batteries will be used.

Implementation

The Van Atta reflector tag will be placed on the back of a soldier's uniform (a plastic casing may be needed around the tag to keep the reflector safe from damage). A transceiver unit along with its

corresponding filter and Arduino will be placed under the barrel of the sending soldiers' firearm. The initiation trigger, Bluetooth module, and corresponding indicator piece will be fastened to the buttstock of the soldier's weapon. The transceiver unit must operate at the same frequency of the Van Atta reflector (24 GHz) for success. This interaction between the transceiver and Van Atta reflector is displayed in Fig. 3. The indicator piece is comprised of LED lights that indicate the response (a green light indicating a friendly soldier in range and line of sight, a yellow light indicating a friendly soldier in range but not in line of sight, and a red light indicating no soldier in the vicinity). Figure 3 demonstrates the communication between the FMCW and the Van Atta tag.

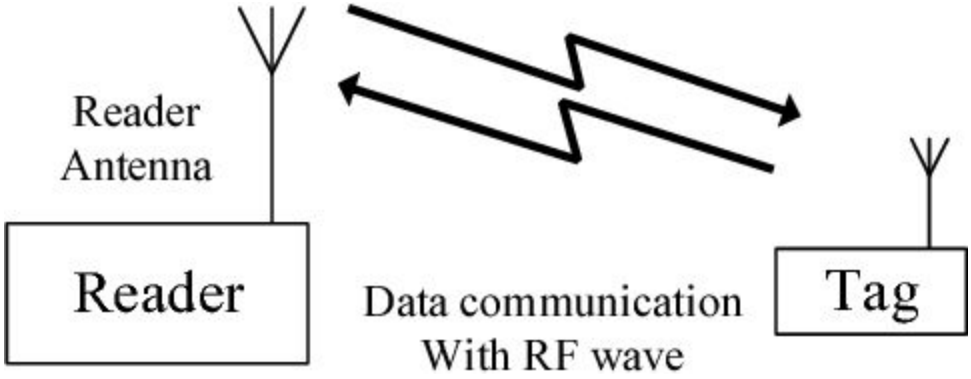


Fig. 3. FMCW reader receiving reflected Van Atta signal

4.1.2 Bluetooth Module and Signal Encryption/Decryption

One important factor to note about the Van Atta Reflector is that there is no means to discriminate signal traffic. This means that even an enemy signal could be reflected by the Van Atta reflector array since it passively reflects signals, thus exposing a soldier's location. This was the inspiration behind the multi-factor authentication with an encrypted Bluetooth module. The Bluetooth module will actively transmit a beacon with an encrypted signal value. When the module is set to listen, it will be listening for incoming beacons upon which it must successfully decrypt the signal in order to confirm that the interrogator Bluetooth module is employing the same cryptographic algorithm as the target. Among the

several commercially used encryption techniques, AES (Advanced Encryption Standard) is a method that is trusted by the US government and other organizations that requires high priority data protection due to its high Avalanche Effect (a property that that reflects the performance of a cryptographic algorithm). Thus, a transmitted signal will be encrypted using the AES encryption method (scrambling and inversion of signals) and can only be decrypted by devices containing the appropriate decryption key. By utilizing this two-fold security measure, we can ensure the security of the signal and the integrity of a soldier's position. The basic functionality of encryption/decryption is displayed in Fig. 4.

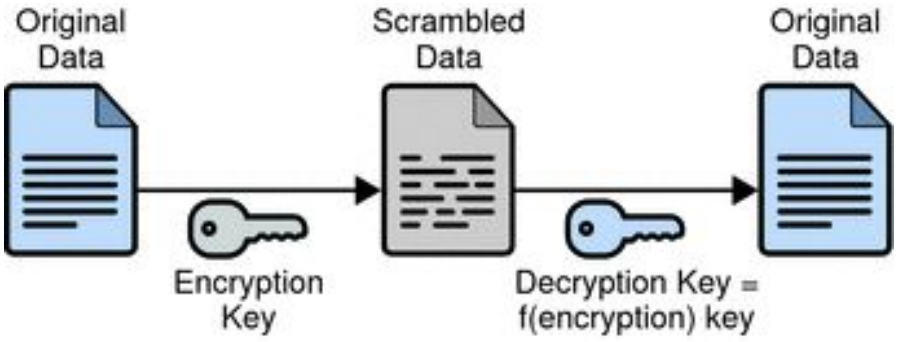


Fig. 4. Encryption/Decryption Mechanism

4.2 Codes and Standards

4.2.1 Transmitter Codes and Standards

The 24 GHz FMCW radar utilized in the design operates in the 24 to 25.5 GHz frequency band and is primarily used for telecommunications, industrial, scientific and medical (ISM) applications. The United States FCC parts 15, 18 and 90 cover standards for the use of communication devices, ISM applications and radio location systems of commercial devices [6].

4.2.2 Encryption Codes and Standards

NIST (National Institute of Standards and Technology) standards for data encryption specifies in SP 800-175B Section 3 that cryptography is broken down into Cryptographic Hash Functions, Symmetric Key Algorithms and Asymmetric Key Algorithms. AES (the algorithm to be used in the IFF system), is a Symmetric Key Algorithm and is among the classes of algorithms that are approved for use, according to subsection FIPS 202. [7]

4.3 Constraints, Alternatives, and Tradeoffs

4.3.1 Constraints

Inter-system compatibility

To ensure that all components of the system (Van Atta, Raspberry Pi (Bluetooth), Arduino, Transceiver, etc.) operate synchronously, they must all operate at a compatible frequency. Since the Van Atta is the limiting factor for functional frequency, all devices must operate at 24 GHz, modulated at 100 KHz.

4.3.2 Tradeoffs

Some important design decisions to consider for the final prototype of the IFF system are deciding between batteries and solar panels for the Van Atta reflector, modifying the Van Atta tag to optimize angle of transmission vs. precision of reply, and the overall complexity of the encoding algorithm.

Batteries vs Solar Panels

The decision to utilize batteries over solar panels to power the Van Atta tag was discussed in section 4.1.1. The two AAA batteries being used will have a battery life of two hours with the Van Atta's power consumption. If this proves to be too short of a lifetime, solar power may need to be used for the final design.

Angle of Transmission vs Signal Precision

To improve the odds that a response signal is returned to the reader, the angle at which a signal is transmitted can be increased to reach a larger ground radius. However, in order to receive a signal with the highest precision (less than two degrees of signal deflection from the Van Atta), a signal must be transmitted in as narrow of an angle as possible.

Encryption Complexity

To ensure maximum integrity, a complex encryption algorithm will keep the Van Atta safe from reflecting an enemy signal; however, as the complexity of the algorithm becomes greater, it will take a significantly longer period of time for a transmitted signal to be decrypted and reflected back to the sender. As a part of the prototyping testing process, a balance will need to be achieved between signal security and speed of signal affirmation (friendly vs. non-friendly).

5 Schedule, Tasks, and Milestones

The PERT chart shown in Appendix A outlines all tasks that must be completed prior to the senior design expo for Fall 2019. Each task listed on the chart is labeled with an optimistic, likely, and pessimistic time, based on the skill sets of each team member and the difficulty of each task.

The critical path, which is listed underneath the PERT chart, identifies the minimum time required to produce a final prototype. Many of the tasks within the critical path, such as prototyping and testing, are subject to large time variation; it is difficult to predict the full scope of technical errors that might arise during the process. As such, the pessimistic time for most tasks within the critical path are longer than the optimistic time by roughly a week.

The Gantt chart in appendix B displays important tasks, milestones and the critical path of the overall project timeline. Each member of the group had a significant contribution towards the completion of each of the element on the Gantt chart. Vijay, being the team leader, was in charge of budgeting after there was a consensus on supplies from the software (Vijay, Vishal, Rishabh) and hardware (Kevin, Donghoon) teams. Product design was split into two parts based on the two teams previously described, as well as the QFD chart where critical trade-offs were examined. Upon completion of the prototype, the team worked together for testing as well as presentation preparation. Prototyping and testing, as expected, took the longest time to complete as there was a time when the team had to go back to restructure our product design, however with sound collaboration, it was possible.

6 Final Project Demonstration

The project demonstration will take place in the Georgia Tech McCamish Pavilion. The system will have the ability to be removed and attached to any individual, where the identification of a friend and a foe will take place. The demonstration steps will be as follows:

1. Two individuals, person A and person B, will be required for a successful demonstration.
2. A Bluetooth module and Van Atta reflector will be attached to the chest of person A, and the initiator unit, indication unit, Arduino, transceiver unit and accompanying filter will be attached onto the firearm of person A. Person B will have the exact same setup outfit.
3. Person A and B will both be broadcasting an encrypted Bluetooth beacon until Person A (interrogator) will attempt to confirm the identity of person B.
    a. Person A will point the firearm at Person B and push the initiator button which will convert his status from active beacon transmitter to listener and transmit a signal from his transceiver unit to Person B's Van Atta tag.
    b. Once Person A successfully decrypts the beacon from Person B, as well as confirms the line-of-sight status from the reflected signal, Person A can view the identification status of Person B on the indication unit on Person A's firearm.
        i. If Person A precisely aimed at the tag of Person B, a green LED will light up indicating Person B is in proximity and line-of-sight
        ii. If Person A did not aim his firearm directly at Person B, a yellow LED will light up indicating Person B is in proximity, however not in line-of-sight.

iii. If Person B is out of range from Person A, a red LED will light up indicating that no targets are in proximity of Person A.

Following these steps will provide the audience a validation of the project specifications. An abbreviated version of these steps will be performed throughout the design process for prototype testing. Code will be synced with the systems so that, upon reset, the system can function properly. The system requires low power which can be sourced from a power bank.

7 Marketing and Cost Analysis

7.1 Marketing Analysis

IFF systems are currently in use in various military organizations; however, due to their sheer size and rapid power consumption, it has yet to be miniaturized for ground troops. One such product that has been specifically developed to identify ground troops is called Bluedome. The Bluedome IFF system is still under development by Israel Aerospace Industries (IAI), with performance specifications as shown in Table 6 [8].

Table 6. IAI IFF System Specifications

Battery Life	> 4 days
Weight	< 140 g
Battery Type	Universal Standard
Interrogation	Line of Sight and Non-Line of Sight (Los, NLos)

Similarly, there are other defense research labs and government funded projects that attempt to provide ground troops with IFF systems. Currently, the Russian government is funding six enterprises that are engaged in the project but hopes to open private businesses that will work on the equipment in three shifts, thus reducing production costs [9]. However, all these projects focus on different implementations of beacon-only systems which can be susceptible to interception and integrity loss. SP-READ utilizes multi-factor authorization in a passive system; the device only responds true positive when both halves of the system are confirmed. This gives SP-READ a significant advantage over the competition.

7.2 Cost Analysis

The total equipment cost for a single prototype unit of SP-READ is approximately $93.20. The table below shows a breakdown of how the costs are distributed. The most expensive component is the FMCW radar costing $89.90.

Product	Quantity	Unit Price	Total Price
Van Atta Reflection Array	1	$20	$0 (received for free)
FMCW Radar (FMK24A)	1	$89.9	$89.9
Transmitter (nRF24L01)	1	$1.20	$1.20
ATMega328P (microcontroller)	2	$2	$4
PCB connectors	5	$1.50	$7.50
Logical gates	5	$0.69	$3.45
TOTAL COST	1	$113.20	$93.20

The development costs listed in the table below were determined by assuming a labor cost of $35 per hour. The development and testing of a custom PCB board will require the majority of labor hours (280 hours per unit).

Project Component	Labor Hours	Labor Cost
Processing Unit Development		
Design	16	$560
Fabricate	18	$630
Assembly	120	$4200
Cryptographic Algorithm Development	110	$3850
Code Debugging	16	$560
Total System Assembly		
Assembly	112	$3920
Testing	160	$5600
Organization		
Group Meetings	250	$8750
Demo Preparation	100	$3500
TOTAL LABOR	920	$31570
TOTAL COST		$31570

Assuming a fringe benefit percentage of 10%, and an overhead percentage of materials and labor costs of 105%, the table below displays the expected total costs.

Labor	$31570
Fringe Benefits % of Labor (10%)	$3157
Subtotal	$34727
Overhead, % of Materials and Labor (105%)	$36463.35
TOTAL	$71190.35

An expected production run for the product will consist of 25000 units produced. The sales expense constitutes approximately 2.5% of the selling price for a given unit. Over a 5-year period, the projected price per unit (while including 10% fringe benefits, and 105% overhead), is $380.83, providing a $50 profit per unit. With the given selling price, the expected revenue is $9,520,750, and expected profit is $1,250,000.

8 Conclusion

The implementation of the system was a success. The SP-READ system operated as intended and can accurately state the status of a designated target instantly. Limitations of the SixPlus team's prototype of SP-READ include range and the ability to confirm a true negative. Many of the functional limitations of the product can be attributed to budget and technology restrictions, however the SixPlus team is confident that these challenges can be overcome with more sophisticated machinery and an increased budget. The ability to confirm a true negative is something that the SixPlus team will need to conduct more research on as this is something that would require extensive knowledge of the enemy. Overall, the SixPlus team has successfully met the intended goals for SP-READ and are highly pleased with the performance of the prototype.

9 Leadership Roles

The project is headed by Vijay Krishnan, Director of Communications, who will act as a liaison between the SixPlus team and Dr. Emmanouil Tentzeris. Vijay also oversaw the project to ensure that task deadlines were met according to the proposed timeline. The team has been working in two sub-teams: hardware and software. Kevin Waddles is the hardware lead and has been responsible for coordinating with the Athena lab and ECE 4012 department to procure essential components and devices needed. Donghoon Han is the design/testing lead and has been responsible for designing and testing the prototypes to verify performance. The combined efforts of Kevin and Donghoon have been pivotal in the successful performance and optimization of the hardware elements of SP-READ.

Rishabh Patel and Vishal Devidas form the software team of SixPlus. Vishal Devidas has acted as our software lead and has been responsible for planning and implementing a working encryption algorithm. Rishabh Patel has managed and updated the team's website with relevant information as the team's webmaster, while assisting Vishal with software tasks. Vijay has actively worked with Vishal in developing the software components of the SP-READ system and has served as the communication link between the hardware and software teams.

In the last few weeks leading up to the Fall 2019 Design Expo, Vijay Krishnan will transition into the role of expo coordinator, and will oversee the preparation and presentation of the final project. Rishabh Patel will take on an additional role as documenter, and will record all meeting notes in an organized, coherent matter for future reference.

10 References

11 [1] “Raytheon: Identification Friend or Foe (IFF),” Raytheon: Customer Success Is Our Mission, 05-Mar-2019. [Online]. Available: https://www.raytheon.com/capabilities/products/iff. [Accessed: 06-Mar-2019]

12 [2] Mark Thompson, “The Curse of ‘Friendly Fire’”, Time Magazine, Jun. 11, 2014. [Online]. Available: http://time.com/2854306/the-curse-of-friendly-fire/. [Accessed Mar. 4, 2019]

13 [3] H. Greenberg, “Gaza: 3 soldiers killed, 24 injured in friendly fire incident,” *Ynetnews*, 14-Jun-2011. [Online]. Available: https://www.ynetnews.com/articles/0,7340,L-3651165,00.html [Accessed: 19-Apr-2019].

14 [4] F. News, “'Misdirected' airstrike killed 18 allied Syrian forces, US military confirms,” *Fox News*, 13-Apr-2017. [Online]. Available: https://www.foxnews.com/world/misdirected-airstrike-killed-18-allied-syrian-forces-us-military-confirms. [Accessed: 19-Apr-2019].

15 [5] W. H. Lui and A. Shreedhar, “IFF System for Infantry,” *IFF System for Infantry - Cornell ECE 4760*. [Online]. Available: http://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/f2012/wl378_as889/index.html. [Accessed: 19-Apr-2019].

16 [6] “Rules & Regulations for Title 47,” *Rules & Regulations for Title 47*, 21-Dec-2017. [Online]. Available: https://www.fcc.gov/wireless/bureau-divisions/technologies-systems-and-innovation-division/rules-regulations-title-47. [Accessed: 20-Apr-2019].

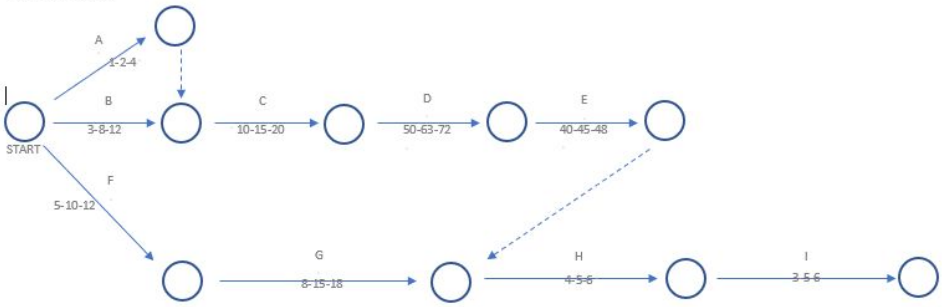
17 [7] E. Barker, “Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,” *NIST Special Publication*, Mar-2016. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/sp/800-175b/archive/2016-03-11/documents/sp800-175b-draft.pdf.

18 [8] “BlueDome,” *iai.co.il*. [Online]. Available: http://www.iai.co.il/2013/36802-46519-en/BlueDome.aspx. [Accessed: 19-Apr-2019].

19 [9] R. Tomkins, “Russian companies to produce individual soldier IFF sensor systems,” *UPI*, 07-Jul-2014. [Online]. Available: https://www.upi.com/Defense-News/2014/07/07/Russian-companies-to-produce-individual-soldier-IFF-sensor-systems/9391404760708/. [Accessed: 20-Apr-2019].

Appendix A

PERT Chart



Task	Label	Optimistic (T0)	Most Likely (Tm)	Pessimistic (Tp)	Expected Duration (Te)
Budgeting	A	1	2	4	2.167
Project Design	C	10	15	20	15
QFD Chart	B	3	8	12	7.833
Project Summary	F	5	10	12	9.5
Project Proposal	G	8	15	18	14.333
Prototyping	D	50	63	72	62.333
Testing	E	40	45	48	44.667
Project Presentation	H	4	5	6	5
Design Expo Preparation	I	3	5	6	4.833

Critical Path: B-C-D-E-H-I, **Expected Duration:** 7.833 + 15 + 62.333 + 44.667 + 5 + 4.833 = 139.666 days

Appendix B

Gantt Chart

Task Name	Start Date	End Date	Duration (Days)
Budgeting	22-Aug	12-Sep	20
Project Design	3-Sep	22-Oct	50
QFD	30-Aug	8-Sep	9
Final Project Summary	30-Nov	6-Dec	7
Project Proposal	28-Nov	11-Dec	14
Prototyping	25-Oct	26-Nov	32
Testing	25-Oct	29-Nov	36
Project Presentation	30-Nov	2-Dec	3
Design Expo Preparation	29-Nov	1-Dec	3