Identification Friend-or-Foe (IFF) Infantry System

ECE4011 Senior Design Project

SixPlus

Dr. Tentzeris

Team Members:

Vishal Devidas
Donghoon (Leo) Han
Vijay Krishnan
Rishabh C. Patel
Kevin Waddles

Submitted: 4/19/2019

Table of Contents

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 $1500 budget provided by the ATHENA Lab.

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 a $1500 budget from the ATHENA Lab to develop the prototype.

1.1 Objective

The team will design and prototype a system that enables ground troops to accurately identify friendly targets. A pre-identification system mounted on the target's forearm will receive an encrypted signal from the transmitter on the aggressor soldier's weapon. Once the encrypted signal is decrypted successfully, it is transmitted via a Van Atta reflector array on the target's arm to the Van Atta reflector array on the aggressor soldier's arm. The reflected signal from the target's Van Atta array reaches the aggressor soldier's Van Atta array where the pre-identification system on the aggressor soldier's arm identifies the reflected signal as either a friend or a foe. If the target soldier is an enemy, the frequency-modulated continuous waveform (FMCW) radar mounted on the aggressor soldiers identifies the reflected as an enemy.

1.2 Motivation

Incidents of friendly fire have plagued the 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 IFF Infantry System 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 and they utilize a beacon which is designed to withstand adversary spoof attacks. The IFF Infantry System team will design and develop a prototype where its functionality would be independent from a beacon implementation, making it truly invincible to adversary spoof attacks. The prototype offers a commercially available IFF Infantry System which is expected to cost upwards of $1500.

1.3 Background

Extensive research has been devoted to the development of IFF System for preventing friendly fire incidents. Although the research focuses on developing IFF Systems for military vehicles and fighter aircraft, IFF Systems are still underdeveloped for protecting ground troops from friendly fire. The 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 IFF Infantry System team will develop a prototype which would provide similar functionality to the Cornell University's research; however, the team's prototype will utilize RF for signal propagation while avoiding the use of a beacon.

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

- Range of at least 50 m - 1 km
- Target cost is less than $500 (transmitter and receiving unit)
- Low power consumption (mWs of power)

Broadcaster

- Aimed signal transmitted has 10 degrees of coverage

Transponder (Van Atta Array/Pre-Identification Processing Unit/FMCW Radar)

- Smart reflector badge that reflects back 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

Table 1. Van Atta Specifications

Operating Frequency	24 GHz
Power Consumption	70 mW
Functional Range	50m to 1000m
Reflection Precision	± 2°
Battery Life	2 hours

Table 2. Signal Authentication Specifications	
Levels of Encryption	2 levels (16 bits preliminary encryption and 8 bit variable encryption with key management)
Type of Encryption	American Encryption Standard (AES)
Signal Type	Bit stream (16 bits for Identification)
Encryption Resolution	16 bits for Authentication
Bit Error Rate	3.125% (1 bit per 32 bits)

Table 3. Systems Specifications	
Total Power consumption	~500mW
Operational Range	500m to 1000m
Transmission Frequency	24 GHz
Weight	~70g
Temperature Allowance	0~+70°C
Supply Voltage	5V

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 and the encryption/decryption of signals passed to and from the device. Fig. 1a displays the block diagram of the system and Fig. 1b displays a sketch of the implementation.

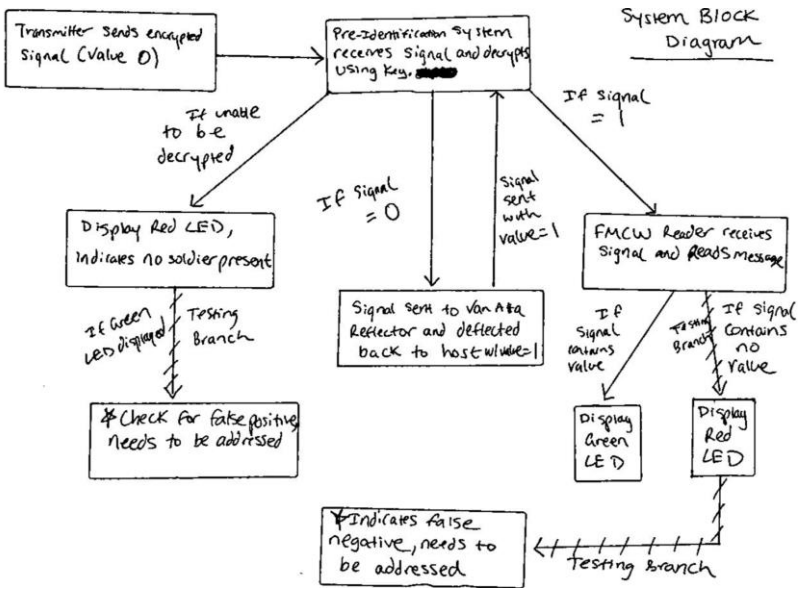


Fig. 1a. Block Diagram of IFF System. The testing branches (marked with dashes) displayed are solely for the purpose of prototype debugging and addressing errors.

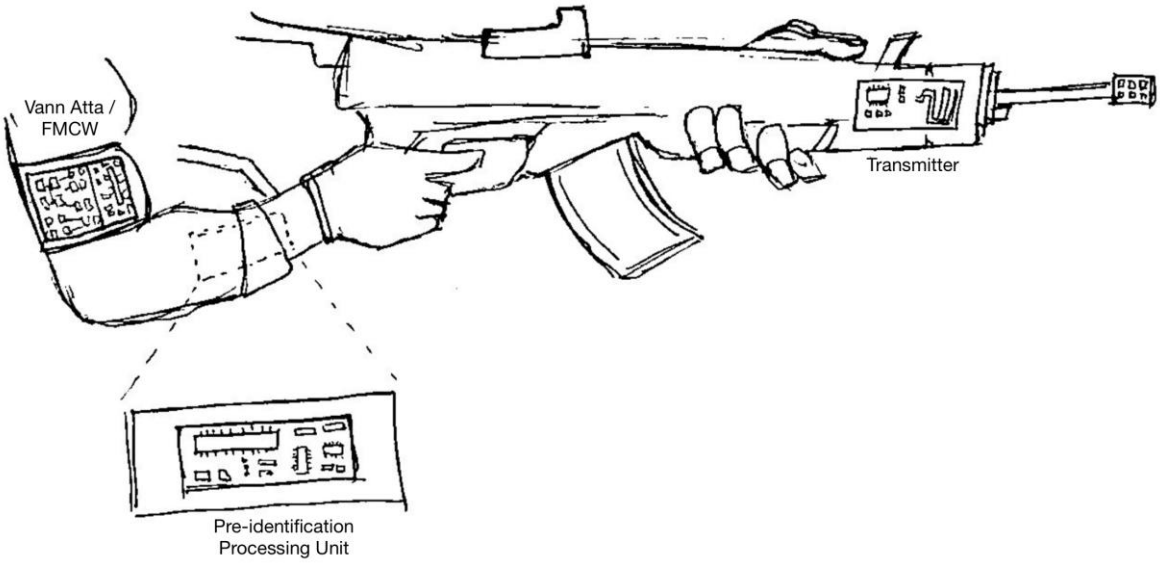


Fig. 1b. System implementation sketch

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.

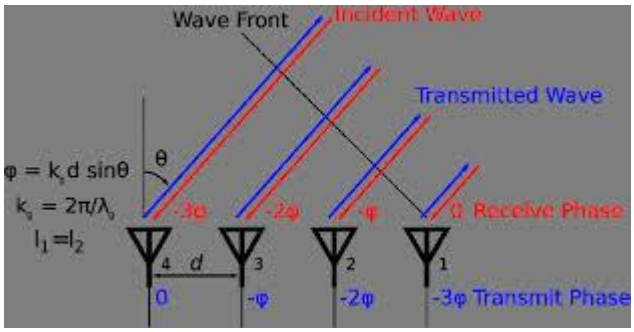


Fig. 2. Van Atta Reflector function

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 a soldier's uniform on the outer arm region (a plastic casing will be around the tag to keep the reflector safe from damage). A FMCW reader will also be attached near the Van Atta tag and placed on the inner forearm region of the soldier to read an incoming reflected signal. The FMCW radar must operate at the same frequency of the Van Atta reflector (24 GHz) for success. The interaction of the radar with the directed incoming Van Atta signal is displayed in Fig. 3. An LED light will be installed on the radar as an indicator of the response (a green light indicating a friendly soldier, a red light indicating the transmitted signal was not received). Lastly, the initiation signal will be transmitted by a frequency compatible (24 GHz) transmitter which will be mounted on the firearm of the soldier (this can be seen on the system diagram from Fig. 1).

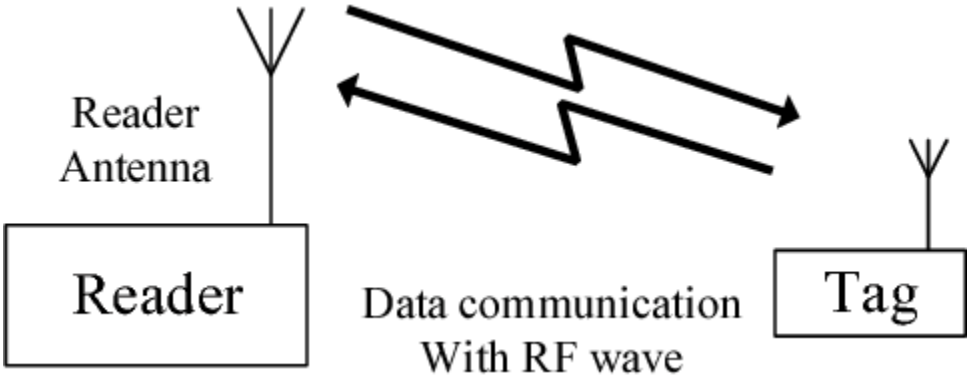


Fig. 3. FMCW reader receiving reflected Van Atta signal

4.1.2 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 would be reflected by the Van Atta reflector array, thus exposing a soldier's location. To overcome this challenge, the tag will be paired with a pre-identification (PI) system to only allow friendly signals to be reflected. The system is simply an encryption/decryption filter that will only allow transmitted signals with the same encryption pattern to be successfully decrypted. 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.

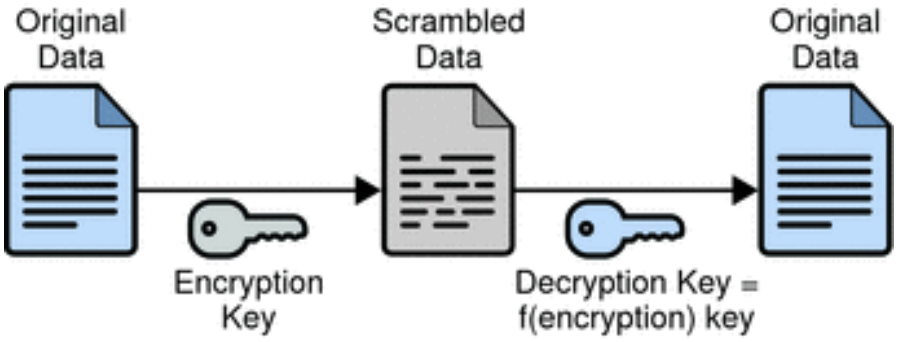


Fig. 4. Encryption/Decryption Mechanism

In addition, the encrypted signal will be transmitted with a binary bit stream, which will indicate to the PI system whether a signal is incoming or outgoing; this is important as an outgoing signal will need to be sent to the receivers' PI system and then directed to its Van Atta reflector, but an incoming signal will need to be sent to a receivers' PI system followed by its FMCW radar to indicate the status of a response.

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 reflector, FMCW reader, and Transmitter) 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.

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.

6. 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 pre-identification radar/reflector array system will be attached to the arm of person A. Another pre-identification radar/reflector array system will be attached to the arm of Person B.
3. Person A will be handed a broadcasting device, two cases will be shown.
    a. Person A will point the transmission signal with an angle of 10 degrees towards Person B.
        i. In this case, an indicator will be displayed to Person A suggesting this person is a friendly.
    b. Person A will point the device to a person not wearing the system.
        i. In this case, an indicator will be displayed to Person B suggesting this person is not a friendly.

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 battery.

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 4 [8].

Table 4. IAI IFF System Specifications

Battery Life	> 4 days
Weight	< 140g
Battery Type	Universal Standard
Interrogation	Line of sight (LoS) and Non-Line of Sight (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 a beacon system. SP-READ is a passive system; the device only responds when a valid encrypted signal is received, unlike a beacon, which is constantly pinging a signal back to a centralized base. 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. Table 5 shows a breakdown of the how the costs are distributed. The most expensive component is the FMCW radar costing $89.90.

Table 5. Equipment Costs

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 Table 6 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).

Table 6. Development Costs

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%, Table 7 displays the expected total costs.

Table 7. 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.

Table 8. Selling Price and Profit per Unit (Based on 25000 units produced)

Parts Cost	$140
Total Labor	$15
Fringe Benefits, % of Labor (10%)	$1.5
Overhead, % of Materials and Labor (105%)	$164.33
Sales Expense	$10
Profit	$50
SELLING PRICE	$380.83

8. Current Status

Currently, the team has completed all preliminary tasks required for the design of the system. This includes budgeting of system components and creation of a QFD to identify essential features and tradeoffs between various desired attributes. The team is currently in the early stages of design and prototyping; initial designs using Van Atta reflector arrays, interrogator units, and FMCW modules have been sketched out and discussed.

In terms of documentation, the team has finished composing the project summary and project proposal required for the intermediate senior design course. Both

documents outline the many deadlines and considerations that must be accounted for throughout the entire project.

9. Leadership Roles

The project is headed by Vijay Krishnan, Director of Communications, who will act as a liaison between SixPlus and Dr. Tentzeris. Vijay will also oversee the project so that task deadlines are met according to the proposed timeline. The team has been into two subteams: hardware and software. Kevin Waddles is the hardware lead and is responsible for coordinating with the Athena lab to procure essential components and devices needed. Donghoon Han is the design/testing lead and is responsible for designing and testing any prototypes to verify performance.

Rishabh Patel and Vishal Devidas form the software team of SixPlus. Vishal Devidas acts as our software lead and is responsible for planning and implementing an encryption system. Rishabh Patel will manage and update the team's website with relevant information as the team's webmaster, while assisting Vishal with software tasks.

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 finalized project. Rishabh Patel will take on an additional role as documentor, and will record all meeting notes in an organized, coherent matter for future reference.

10. References

[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]

[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]

[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].

[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].

[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].

[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].

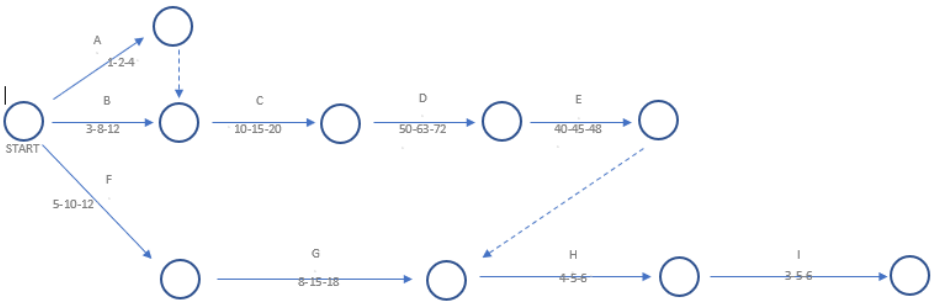
[7] E. Barker, “Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,” *NIST Special Publication*, Mar-2016. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/sp/800-175b/archive/2016-03-11/documents/sp800-175b-draft.pdf.

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

[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