10/29/2017

Team 13: Drone Disabling Device

Gregory Boldt, Latarance Butts, Brandon Eiler, Jordan Lane-Palmer, Deshon Purvis, Natalie Villar, Justin Wawrzyniak

FAMU-FSU College of Engineering 2525 Pottsdamer St. Tallahassee, FL. 32310

Abstract

Disclaimer

Acknowledgement

Table of Contents

List of Tables

List of Figures

Notation

Chapter One: EML 4551C

1.1 Project Scope

The objective is to develop a device to secure a specified air space from unmanned flight vehicles. The key goals include the following:

- Neutralize unmanned flight vehicles within a specified air space
- Ensure the device is portable
- Maintain environmental safety
- Function properly over necessary time period
- Comply with safety and legal regulations

The primary market includes military and civilian safety (i.e. sporting events, political events, concerts, etc.). The presence of drones with potential explosives and cameras could pose security risks on the battlefield and in heavily populated public areas. The secondary market involves defense agencies and private security companies who could utilize this product to improve their security strategy. The assumptions made are that the device is to neutralize unmanned flight vehicles, specifically drones. The stakeholders involved include Tameika Hollis and Stan Zoubek from Northrop Grumman, Shayne McConomy, Camilo Ordonez, and Chiang Shih from the FAMU-FSU College of Engineering.

1.2 Customer Needs

Our initial sponsor for the project was Vice President of Mission Systems, Tameika Hollis. For more specific details and assistance we were directed to Stan Zoubek. Stan is our new point of contact and works as the Chief Engineer of Advanced Technology at Northrop

Grumman. For identifying our customer needs the following questions were posed to Stan and his response is given in Table 1. From his responses we were able to identify the customer needs for the project.

Table 1 Interpreted Customer Needs from Questionnaire with Sponsor

Question?	Customer Statement	Interpreted Need
What is the size and type of drone to be neutralized?	Recreational drones that could be carrying IED's or have cameras.	Disable non-military, typical household drones.
How long does this device need to be operable for?	Device should be operable for time necessary until user powers off.	Maximum time possible.
What is the outcome of the neutralized drone?	Looking to just neutralize the drone given the time constraints, but if possible recover the drone if it is not completely destroyed.	The threshold or minimum requirement would be to disable the drone. Recovering the drone would exceed expectations.
Is the device expected to be autonomous?	No, due to time constraints it will most likely not be possible but ideally that's what we would want.	The threshold or minimum requirement is that the device provides user operation.
Is there a specific range that the device must function within?	100 yds in radius, 100 ft altitude; may realize this is not possible and constraints may need to be adjusted.	Operate device at maximum range possible.
Does the device need to be portable?	Yes, be able to assemble device within 4 hours.	Portable device with a quick set-up time.
What is the purpose of Northrop Grumman sponsoring this project?	Aid-to-hire and give students an understanding of the learning process. Northrop Grumman is not looking for a proof of concept to scale.	Our team should focus on the development process over delivering the final product.

1.3 Functional Decomposition

Now that customer needs are established, the direction for the project is identified. Our objective to secure the air space from drones is divided into four functions: Assemble device, Locate drone, Neutralize drone, and Disassemble device. These major functions are further refined into more specific sub-functions shown below.

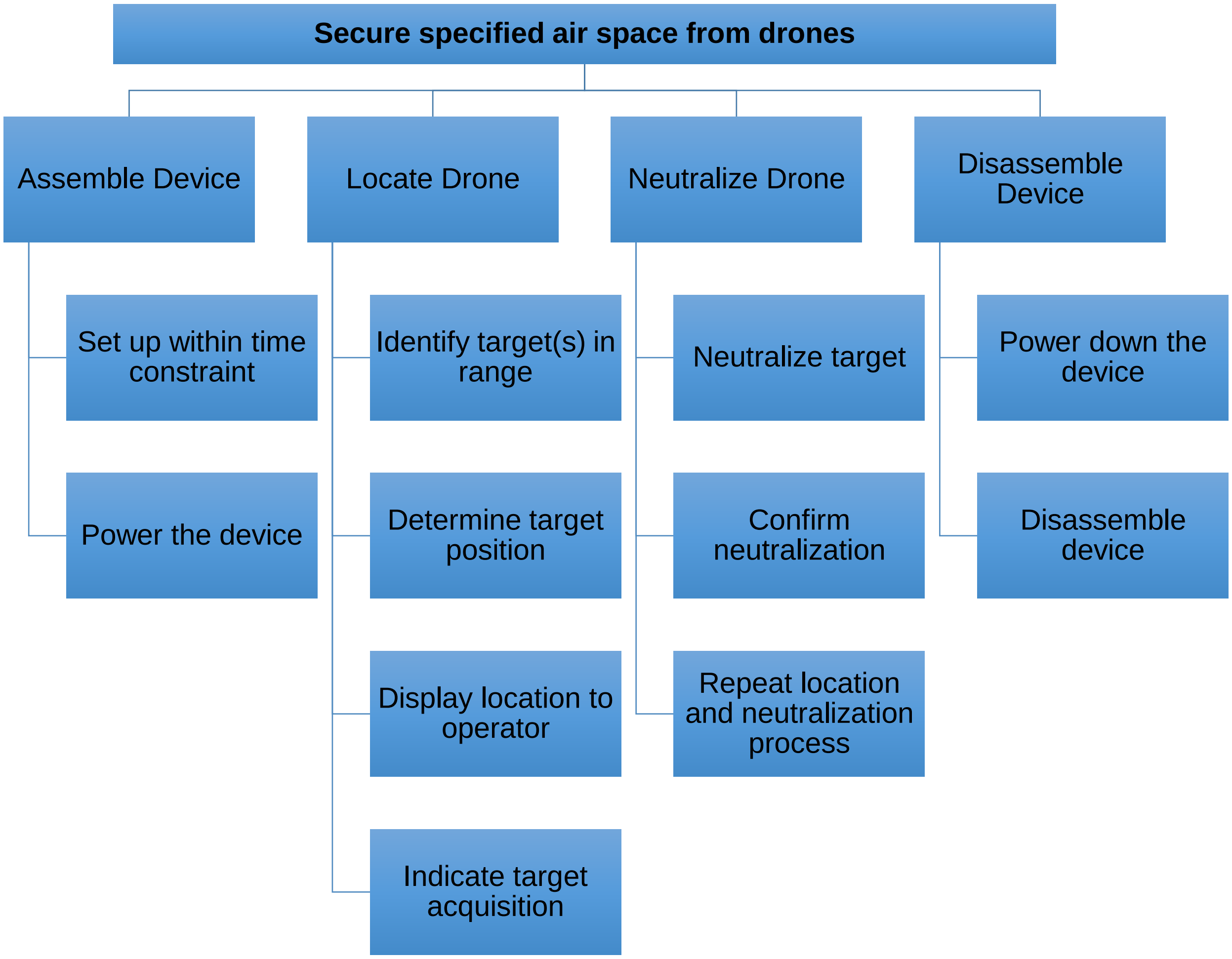


Figure 1 illustrates a functional decomposition for the drone disabling device.

1.4 Target Summary

Metrics are broken up into two separate categories: metrics that are measured with a yes/no answer and metrics that are measured with a target value. The first set of metrics focuses mainly on the function of the drone and the customer requirements. The second set of metrics focuses on certain subsystems and measures if the device will meet the requirements.

The first set of metrics shown in Table 2 defines how the device should function. If the device completes the specified function, then the metric is scored with a yes; if not, it receives a no. The device first needs to power up. After that, it needs to identify that there is a drone in range and lock on to the drone. The device then neutralizes the drone and powers off when the user decides. The device will take down multiple drones within the full time of use, so the device will repeat the functions throughout use. The device is portable to allow for movement from one site to the next if the user wishes to have a different area protected. With the idea of potential recovery, the device must complete minimal damage to the drone. This device must be safe for the surrounding environment including the people that are in range of the device.

The second set of metrics defines the target values to determine if the device works properly meeting the customer needs. These metrics are shown in Table 3. These targets are gathered in two ways: customer definition of targets and the team definition of targets after verifying them with the customer. The customer defines an assembly and disassembly time of 4 hours for each. The device is to work plugged into a standard US wall outlet, so the device will have a current of 15-20 Amperes and a voltage of 120 Volts. The customer defines the neutralization area to have a 30-foot range from the device in the shape of a dome. The device will not neutralize drones below it. For example, if the device is placed on a building the neutralization area does not include the area downwards. The device finds the drone within the 30-foot range and locks onto it in 30 seconds. After the drone is locked on, the drone is neutralized within 5 seconds. The device should have at least a 90% chance of hitting the device so there is little risk to the surroundings. The device should also be able to neutralize 90% of drones on the market. The total cost of production should be less than $5000 USD.

1.5 Concept Generation

The drone disabling device needs to neutralize a target drone within a range of 30 feet from the device. To accomplish this, the device is broken down into different components. First, the device must detect if a drone is within the range. Second, the device must be properly aimed at the target drone. Lastly, the device must neutralize the target drone. As a result, the device has three systems; Detection, Control, and Neutralization. There are six concepts for the detection system, three concepts for the control system, and another six concepts for the neutralization system. Of the six concepts generated for the neutralization system, four of them are electrical approaches and the remaining two are mechanical attacks.

Table 2 shows the various concepts for each of the necessary device systems.

System	**Concept**
Detection System	1. Audio Detection 2. Video Detection 3. Thermal Detection 4. Radio Frequency (RF) Detection 5. Radar Detection 6. Operator Detection
Control System	1. Manual Control 2. Remote Control 3. Automated Control

Neutralization System	1. Radio Frequency (RF) Interference 2. Sound (Pressure) Wave Attack 3. Electromagnetic Pulse (EMP) Attack 4. Hacking Attack 5. Weighted Net Attack 6. Projectile Attack with Epoxy-Based Ammunition

Drone Detection System

Detecting target drones within the secure airspace is vital. Current products on the market are autonomous and utilize an array of detection methods. These products are scaled up for military and/or commercial applications. The detection range for these products surpasses the required range for the project and far exceeds the budget. Project cost constraints require the development of lower-scale detection system or integration a cheaper detection product. Six different solutions to accomplish the drone detection are roughly detailed in table 3 below. The importance of each category is ranked with 1 being the most important category. Categories with a (+) after them indicated that a higher value is desirable and vice versa for categories with a (-) after them. The effectiveness is considered the probability of successfully detecting various drones. The complexity refers to the difficulty in developing the detection system.

Table 3 displays a summary of various detection methods with respect to specified categories.

Rank	Categories	Audio	Video	Thermal	Radio Frequency	Radar	Operator
1	**Effectiveness (+)**	Low	Medium	Medium	Medium	Low	Medium
2	**Range (+)**	Low	Medium	Medium	High	Medium	Low-Medium
3	**Cost (-)**	Low	Low-Medium	Medium	High	High	None
4	**Complexity (-)**	High	Low	Low	Medium	High	None
5	**Size (-)**	Small	Medium	Medium	Medium-Large	Medium-Large	None

A summary of each of the detection methods (audio, video, thermal, radio frequency, radar, and operator) is below.

1. Audio Detection

To experiment with development of an audio detection device would be time consuming. The use of neural networks to distinguish between drones sounds and other environment sounds [1]. The negative characteristics of audio detection is complexity and short range. Additionally, audio detection in busy urban areas is not effective [2], thus, limiting the potential markets for the drone disabling device. A positive characteristic of this method is that the microphones required are low cost [3]. These microphones would need to be set up in an array to maximize effectiveness.

2. Video Detection

Current products on the market utilize autonomous video detection of drones [4]. For these systems, high accuracy is necessary to eliminate false alarms when a bird or other flying objects are identified as drones. The development of a video detection system would allow middle of the pack effectiveness and range at the tradeoff of higher costs and larger size. Autonomy is not a customer requirement for the project, so development of a user-operated version would eliminate any complex software. The with sufficient resolution, the device operator can identify a target drone. Detecting the approximate direction of a drone by other detection methods and then using video camera(s) to display the target to the user may also be a viable option.

3. Thermal Detection

Drone cameras are typically lightweight and a small payload for a drone. Therefore, drones with cameras do not need to be large or powerful to pose a security threat. This makes thermal detection more difficult for smaller drones because they do not produce a lot of heat. Thermal detection can, however, detect drones carrying IEDs that would typically need gas-powered engines to carry the larger payload [2]. Thermal detection has similar qualities to video detection but at a slightly greater cost. Even if a thermal detection system is not needed, thermal vision could be a useful feature to the operator in the neutralizing phase. An example of thermal vision detecting a drone is illustrated in figure 2.

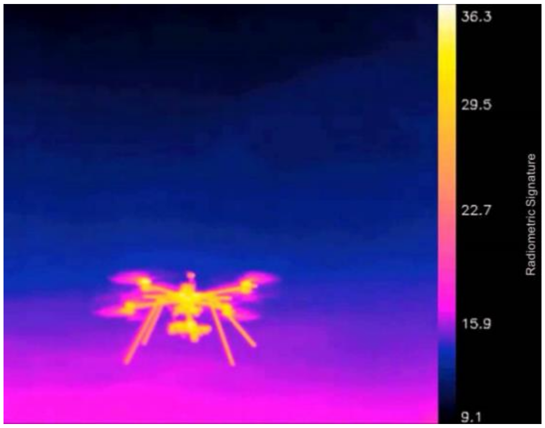


Figure 2 shows a larger drone detected on thermal imaging [5].

4. Radio Frequency (RF) Detection

Radio frequency (RF) detection is considered the most effective detection method [2]. A household drone will typically communicate with the user at a frequency of either 2.4GHz or 5.8GHz [6]. Advanced detection devices currently on the market utilize this information to detect drones at long distances and can also provide GPS coordinates of the drone, altitude of the drone, GPS coordinates of the pilot, unique identifier of the drone [7]. These are all very attractive features and if the budget permits, it may be beneficial to purchase a lower range system. If no such model exists, development of a system should be considered. Figure X illustrates the methods for detecting the drone and the drone controller using radio frequency. Figure 3a shows that to identify the location of the drone, a transmitter (Tx) and a receiver (Rx) are needed. Figure 3b shows that if the drone transmits radio frequency back to the drone controller via video feed, then it is possible to detect the location of the drone and drone controller with just a receiver (Rx).

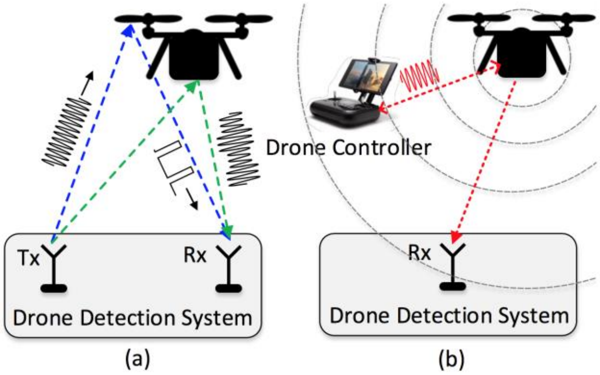


Figure 3 displays both potential radio frequency detection approaches [8].

5. Radar Detection

Traditional radar systems can be modified to detect small drones, but it will also detect birds [2]. Most commercially available drone radar detection systems are very expensive. It may be possible to alter an existing radar product to detect much smaller devices such as drones. If budget permits, combining radar detection with other detection methods may help increase accuracy.

6. Operator Detection

Utilizing the eyesight and hearing of the operator to detect drones is also an option. This method leaves the effectiveness up to the operator. For an operator with poor eye sight or bad hearing, this method could be risky. Additionally, unideal weather conditions may reduce effectiveness. Requiring the operator to be continuously searching for drones with may then require a second operator to perform the neutralizing solution. This method does eliminate the cost of a detection system and complexity of developing a system.

Controls System

The control system is necessary to aim the device at the target drone. Manual control, remote control, and automated control are the three concepts for the control system and are detailed below.

1. Manual Control

Possible manual control systems include a handheld device or a device with manual rotation by the operator. A handheld device (figure 4a) would operate similar to a gun and the user would aim. An example of a manual rotating control system is shown in figure 4b.


(a) (b)

Figure 4 depicts two possible manual control methods [9] [10].

2. Remote Control

The user controls the movement of the device remotely. The user will be equipped with a video feed showing where the camera is pointing. The user can also control the attack with the controller. A functional schematic of remote control is shown in figure 5.

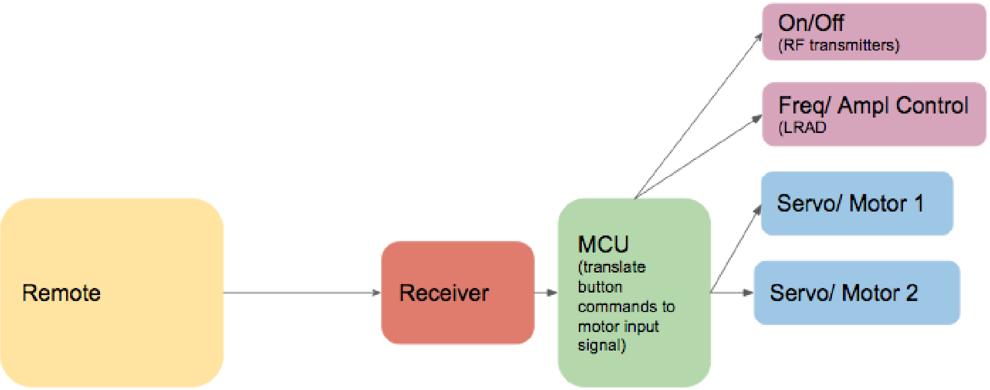


Figure 5 shows a functional breakdown of a remote-control method.

3. Automated Control

The user detects and tracks the location of the drone. The user can choose to control the attack, or have it automated as well. A functional schematic of automated control is shown below in figure 6.

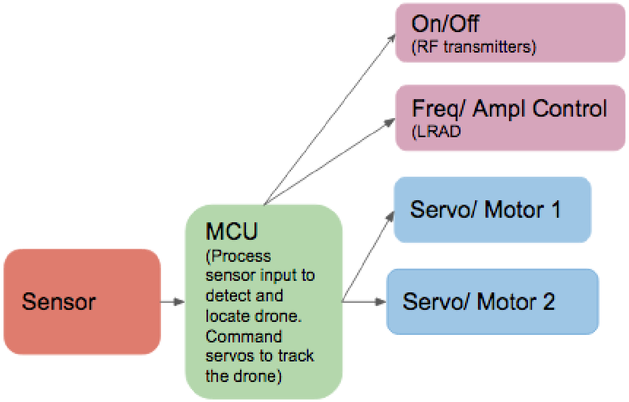


Figure 6 shows a functional breakdown of an automated control method.

Neutralization System

The neutralizing system is the most important system of the project. Once the target drone has been identified using the detection system, the drone must be disabled. Six different approaches are detailed below. Four of the neutralizing methods are electrical based and the remaining two are mechanical based.

1. *Radio Frequency (RF) Interference*

Most commercial drones communicate on frequencies in the 2.4Ghz band. By

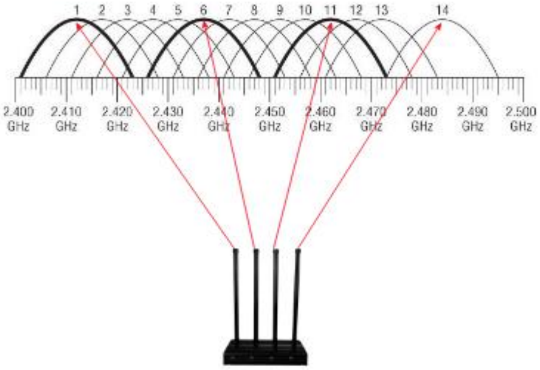


Figure 7 illustrates how four antennas can effectively jam the 2.4GHz band.

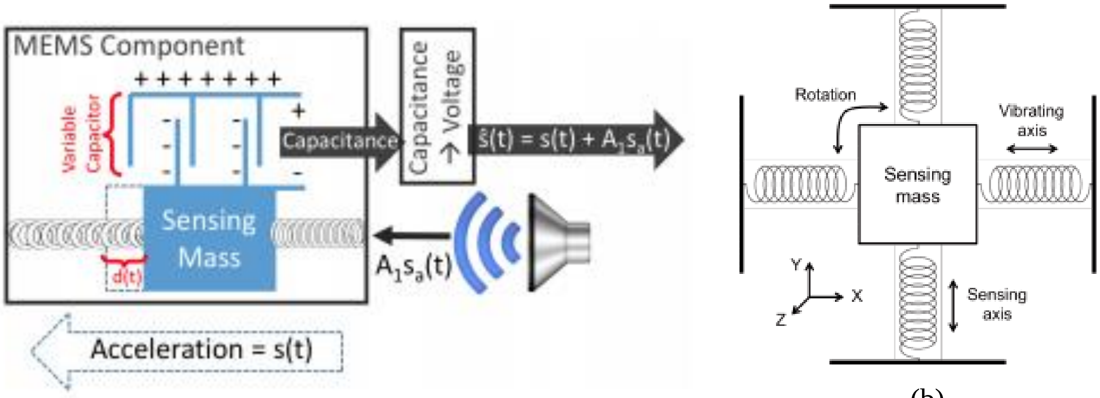
emitting a set of signals at frequencies that overlap communication channels shown in figure 7, communication will be prevented by interfering with the waves being sent to the drone from the remote. The result of this attack can vary on the drone. Some drones will hover in place when they can no longer receive commands from the controller, others may return to base, or fall from the sky. Table 4 gives a consolidated look at some of the potential positives and negatives of this neutralizing approach.

Table 4 shows the pros and cons of the radio frequency (RF) interference method.

Pros	Cons
• High probability of success • Effective mid-flight • Quickly effective • Super low cost	• Doesn't counter against pre-programmed flight since some drones will hover until communication is restored. • Small possibility of interference

2. *Sound (Pressure) Wave Attack*

Drones are equipped with an inertial measurement unit (IMU) determines the drone orientation in space by capturing measurements in each of the 6 degrees of freedom. These microsensors work by capturing the small force that's applied on them when the drone accelerates in any direction. This force is translated to a proportional



(a) (b)

Figure 8 shows an example of (a) an accelerometer [11] and (b) a gyroscope [12] used on a commercial drone.

voltage which the flight controller then interprets. Interference with the drone's accelerometer (figure 8a) and gyroscope (figure 8b) are the target of this approach. By providing these sensors with false orientation measurements that the flight controller interprets (spoofing), one can essentially influence the functionality of the drone. By emitting sound waves, which act as pressure waves, the sensitive microsensors pick up on the small force. This force may not be large enough to provide a drastic change in the sensor measurements, but providing this force at the resonant frequency of the sensor, these forces are amplified substantially. A long range acoustic device would be used to transmit the sound waves since they are designed to for the specific purpose of long range transmission. Table 5 gives a consolidated look at some of the potential positives and negatives of this neutralizing approach.

Table 5 shows the pros and cons of the sound (pressure) wave attack.

Pros	**Cons**
• Decent probability of success • Effective mid-flight • Effective even for pre-programmed flight • Simplicity	• May take a while to find resonant frequency • May not be able to find resonant frequency • Pricy

3. *Electromagnetic Pulse (EMP) Attack*

In this approach, a device is fired which produces a directed EMP that causes a current-surge in a flight critical electronic circuit component. Possible flight critical components that could be affected could include, but are not limited to, MCU,

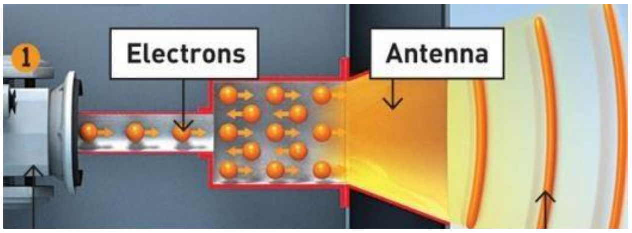


Figure 9 illustrates how an EMP works [13].

accelerometer, gyroscope, and RF module. As demonstrated by the figure 9, an EMP works by generating a high power burst of electrons that is irradiated as microwaves and focused by an antenna. A successful EMP attack is an effective solution for disabling a drone that has a preprogrammed flight path. Limitations of EMP include: adhering to FCC regulations, high power requirements, inability to generate a strong enough pulse to cause a surge at the required distance, and the expense of the design may exceed budget.

4. *Hacking Attack*

A hacking attack has the potential for recovery of the drone intact or assuming control of the drone. Projected budget of this attack system is on the lower end of the concepts, however, many drones may need to be purchased and tested to determine if the attacks can work for a range of drones. Exploitable vulnerabilities may be limited to drones that use certain microcontrollers or protocols and any vulnerability is subject to patching in the future by the manufacturer. Other drawbacks include: not being able to perform the hack in an acceptable time period, certain attacks being specific to the type of drone, and in the event of a successful attack the drone operator may be able to regain control. In the event of choosing this approach, the model of drone may have to be preselected and the attacking method built specifically for that model of drone. Three specific hacking attacks include interception, distributed denial of service, and buffer overloading. A final design may include one or multiple of these specific attacks.

Communication Interception

A spoofing attack consists of intercepting the original communication route or flight plan and replacing it with the attacker's communication route or flight plan. A simple communication interception method may be to instruct the drone to shut down and a more complex method may be to gain full access to the MCU and take over flight of the drone. A schematic of interception is shown in figure 10.

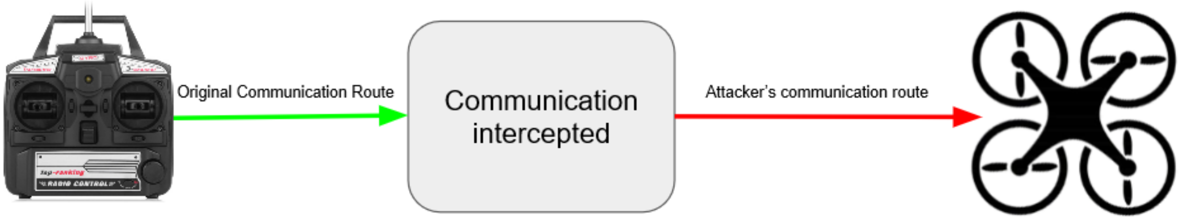


Figure 10 depicts a simple schematic for interception method [14].

Distributed Denial of Service (DDoS)

In a DDoS attack, the attacker sends from a laptop or other wireless device a substantially large number of transmission requests that overloads the drone’s MCU and causing it to malfunction or shut down completely. As long as the communication protocol of the drone is known, this method should be effective since there are currently few effective methods for protecting against a DDoS attack. A schematic of a DDoS attack is shown in figure 11.

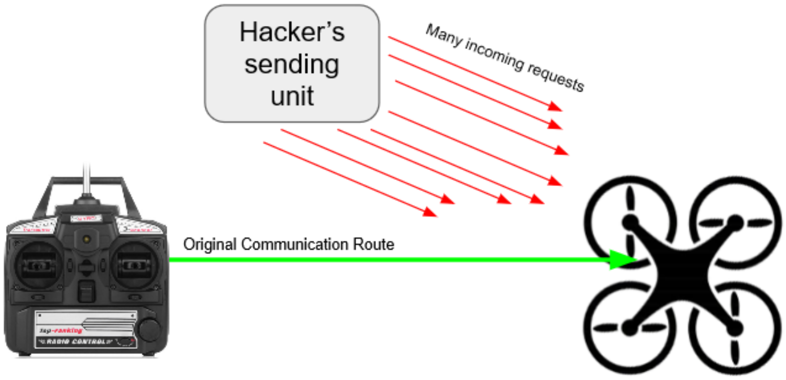


Figure 11 depicts a simple schematic for DDoS attack method [14].

Buffer Overloading

A buffer overloading attack consists of sending a substantially large data packet to the drone that overloads the memory capacity of the drone’s buffer and causes the MCU to crash or have to dump the flight data. The buffer capacity of each drone may differ and the result to the MCU of different drones may differ. A schematic of buffer

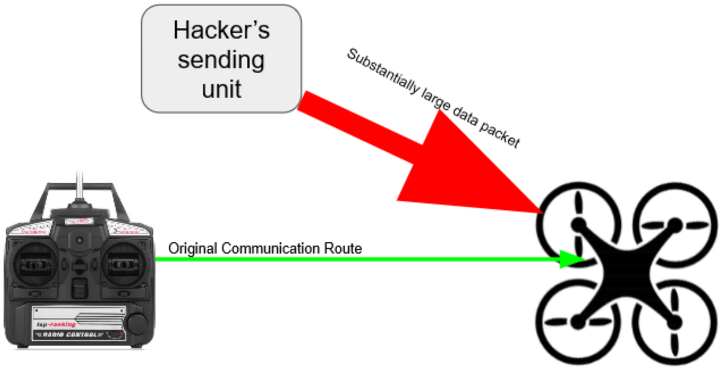


Figure 12 depicts a simple schematic for buffer overloading method [14].

overloading is shown in figure 12.

5. Weighted Net Attack

This concept involves the deployment of a weighted net from a rotating device with two degrees of freedom. The detection system chosen communicates to the cannon that a drone is within range. Then, the device orients itself at the proper angle in order to begin the neutralization process. When a drone is present, the device stops motion again reorienting itself to locate the drone with the CO2 cannon. It then verifies that the drone is still within the given range of the sensor, and shoots out a projectile that houses a weighted net. Weights are attached to the outer parts of the net evenly spaced. The specific weight has not been calculated but if chosen, will be determined. The CO2 tank requires replenishment depending on the time of operation along with the number of times it shoots out the projectile. The projectile that the net is housed in has a timer that goes off at a particular time and begins deployment of the net. This deployment allows for the net to open up and neutralize the drone. This timing is based off of the proximity to the drone. Once the projectile is shot out of the CO2 cannon, there is a string that stays lodged inside the cannon to allow for reuse of the net. The user untangles and retrieves the drone captured to allow for reuse of the net. In the case that the reuse of the one net is not possible, the implementation of housing multiple nets within the cannon will be

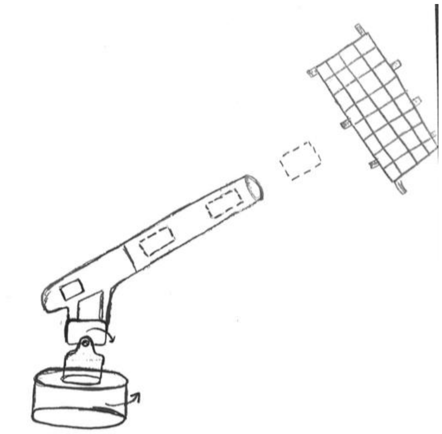


Figure 13 illustrates a rough sketch of the weighted net attack.

completed. The housed nets are envisioned as ammunition that provide for faster neutralization of multiple drones within the 30-foot dome. Figure 13 shows the device explained above. This method of neutralization allows for a large surface area to be covered when the net is shot out of the cannon. On the other hand, if the drone is moving at a high speed within the range, it will be more difficult to neutralize the drone. The method of attack works best on a stationary target.

6. Projectile Attack with Epoxy-Based Ammunition

The methodology behind this operation is that it is supposed to be a device which works in tandem with a single carbon dioxide canister to shoot projectiles at the drone. The projectile would be of a similar nature to the capsules utilized by paintball gun. Paint ball guns primarily work by propelling a soft-shelled capsule at a set velocity allowing for the paint to cover the target [15]. This device would have similar elements to that of a recreational paintball gun scaled for a larger application. The ammunition for this device would contain a fluid like epoxy insulation foam in which the capsule will expand upon contact with the drone. The drone will be hindered by the additional mass added by

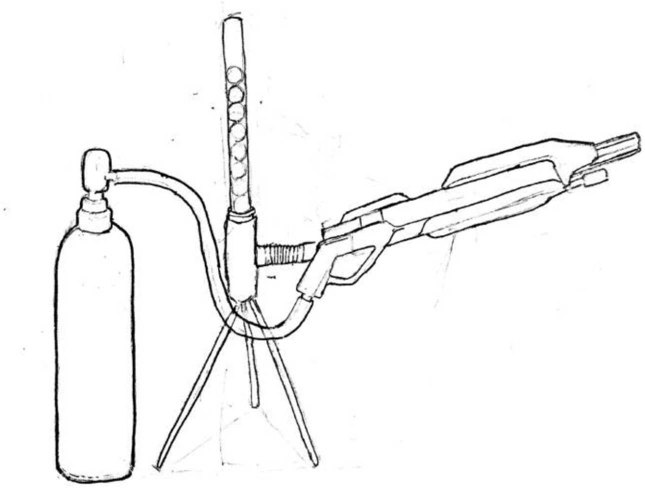


Figure 14 illustrates a rough sketch of the projectile attack with epoxy-based ammunition.

epoxy foam. This material would be like that of self-healing polymerization in which combines a free radical peroxide initiator, polymethyl methacrylate and epoxy vinyl to create a new expanding polymer [16]. This might potential method worth exploring, but the rate of response from the reaction would be a large deciding factor in whether or not this is a feasible solution. The device concept (figure 14) would fire the capsules in rapid succession, to increase the chances of contact with the target. The usage of a system that locks onto the drones would be a necessary addition to the projectile based device, to improve functionality. The size of the ammunition is still under consideration since a larger sized ammunition would require a higher velocity to break upon contact. A projectile based device faces several major obstacles. The first is that the impact on the environment must be strongly evaluated, since the drone disabling device has the potential to be used in a variety of environments, many of which would involve large groups of people. The second obstacle with this design is that pressurizing the capsules, and finding the most cost-efficient method of obtaining the capsules. Utilizing this method would require a more specialized user, preferably one that is used to shooting moving targets. Drones are a more difficult target to hit when compared to traditional target since they would be able to change direction almost instantaneously. Finding the correct material that is best suited for the interior is still being determined. Table 6 gives a consolidated look at some of the potential positives and negatives of this neutralizing approach.

Table 6 shows the pros and cons of the projectile attack with epoxy-based ammunition.

Pros	**Cons**
• Simplicity of operation • Complete neutralization of drone	• Finding the correct ammunition • Tracking the drone might add a level of complexity to the development of the device

1.6 Concept Selection

To select from the concepts for the detection, control, and neutralization systems, a house of quality (HOQ) method was used. A HOQ is a selection matrix where concepts are compared with regards to various categories. For each system, applicable categories are ranked based on customer importance. A higher rank indicates a more important category. Additionally, categories are characterized as positive or negative. Higher values are desirable for positive categories (i.e. range) and undesirable for negative categories (i.e. cost). The HOQs used for each system are populated with qualitative values. Numerical values corresponding to the qualitative values are given in table 7 and are based on the category.

Table 7 displays the quantitative values associated with the HOQ qualitative values.

	Quantitative Value	
Qualitative Value	**(+) Category**	**(-) Category**
None	0	10
Low/Small	3	9
Low-Medium	4.5	7.5
Medium	6	6
Medium-Large	7.5	4.5
High/Large	9	3

It is important to note that limited information is available regarding many of the concepts generated. Also, current products on the market are much more advanced then required for the project. As a result, qualitative values reflect a "gut feeling" based off all information gathered. In order to increase the chances of a successful product, multiple concepts could be pursued for a single system.

Drone Detection System

The six concepts for the detection system include audio, video, thermal, radar, user, and radio frequency. The concepts are evaluated on five categories. The most important categories, as deemed by the customer, are effectiveness and range. The goal is to maximize these two categories. For the project, effectiveness is considered how well the detection system identifies drones in the airspace. The cost of the detection system and the complexity to develop the system are important as well. Due to budget constraints, the cost of the system is significant and needs to be minimized as much as possible. Due to time constraints, the system must not be too complex that it cannot be finished in time. The least important category is the size of the system. The device just needs to be portable enough to assemble in 4 hours and has no size constraints. A smaller device is more desirable to the customer; therefore, the category is in the decision matrix.

Radar and radio frequency (RF) detection methods are most effective because they can detect drones well regardless of weather. User and video detections are highly effective only during ideal weather conditions. Thermal detection can identify drones in non-ideal conditions better than video detection. The audio detection method is the least effective because detection is near impossible in noisy environments. The exact range for each concept is uncertain so values are estimated relative to each other. Receiving RF waves is possible at very long distances and is considered the longest-range concept. Current radar systems are capable of very long-range detection as well. A scaled down version to detect smaller flying objects such as drones is predicted to have slightly less range. The range of video and thermal detection systems depend on the resolution of the camera used. To achieve the same range as a radar or RF detection method, a very expensive camera is required. The eyesight of the user determines the range of detection, so the concept is given a relatively low range. The audio detection method has low range. Using an array of microphones may increase the range and effectiveness but drives up cost, complexity, and size. Having a user detection method eliminates the cost, complexity, and size of the system. The high effectiveness and range of the radar and RF detection approaches come at an increased development cost and size. Thermal detection costs slightly more than video detection, as one would expect. Audio detection is the most complex because it requires machine learning to properly distinguish drone sounds from other environmental sounds. A large database of sounds is necessary for effective detection. Similar to audio detection, extensive data collecting would be required to properly identify a drone using radar detection. The complexity of RF detection comes from needing to distinguish drone RF waves from other RF waves in the airspace. Video and thermal detection methods require machine learning to determine if an object is a drone, however, data is readily available for identifying moving objects on a video feed. The development of software to distinguish between birds and drones is still necessary though which increases the complexity. For audio detection, the size of a microphone is small, whereas, video and thermal cameras are larger. Table 8 shows the HOQ for the detection system.

Table 8 displays the HOQ for the detection system of the device.

		Detection Systems					
Rank	**Categories**	**Audio**	**Video**	**Thermal**	**Radar**	**Radio Frequency**	**User**
5	**Effectiveness (+)**	Low	Medium	Medium-High	High	High	Medium
5	**Range (+)**	Low	Medium	Medium	Medium-High	High	Low-Medium
3	**Cost (-)**	Low	Low-Medium	Medium	High	High	None
3	**Complexity (-)**	High	Medium	Medium	Medium-High	Medium	None
1	**Size (-)**	Small	Medium	Medium	Medium-Large	Medium-Large	None
		75	106.5	109.5	109.5	121.5	122.5

From the house of quality, the radio frequency detection approach and the user detection approach are the top choices followed closely by the radar, thermal, and video detection methods. The audio detection method has the lowest score of all the detection concepts. All though user detection method has the highest score, it is not necessarily the best choice when considering the device targets. The lower end range may not give the user enough time to aim and neutralize the drone before entering the airspace. Additionally, a distracted user may fail to identify a drone completely. Moving forward, a user detection method is considered a last resort if the detection system fails. RF detection appears the top choice for achieving the device targets. This method is selected to move forward with. Because a video feed may be needed for the control and neutralization systems, the video detection method is selected as a back up if RF detection is not feasible. Small-scale testing will be performed on these methods to validate their effectiveness.

Control System

The method used to evaluate and select a control system from three proposed ones (Hand held, remote, auto) is a decision matrix. The categories used to evaluate systems were; Response time, Accuracy, Cost, Complexity, and ease of use. The ranking in response time is based on the predicted time the system will take to detect and tract an unfriendly drone. The accuracy is based off the predicted ability of the system to accurately strike the target using a mechanical approach, as electrical approaches are omni directional. The complexity of the system is ranked on how the device will be integrated into the device. Ease of use is determined on the ability of a layperson to utilize the system without any formal training. Lastly the cost of the system was based on the availability, time to develop, and cost of an existing system. Using the decision matrix, the Automated system was calculated to be the most desirable system. Due to the immense amount of time to develop the automated system, and the scope of this project, the runner up of a hand-held system was selected. Table 9 below shows the HOQ created for the control system.

Table 9 displays the HOQ for the control system of the device.

		Control Systems		
Rank	**Categories**	**Hand Held**	**Remote**	**Auto**
5	**Response Time (+)**	Medium	Low	High
4	**Accuracy (+)**	Low	Medium	High
1	**Cost (-)**	Low	Medium	High
2	**Complexity (-)**	Low	Medium	High
3	**Ease of use (+)**	High	Medium	Low
		96	75	17

Neutralization System

The categories to rank the neutralization systems were chosen based upon customer needs and subsequently generated targets. Effectiveness is the most important category based upon the purpose of the device, which is to neutralize a drone within a specified airspace. If this objective is not met, then the device is deemed a total failure. The rating in the category is based on the likelihood of that solution meeting the target of 90% combined probability. The combined probability includes the likelihood of hitting the target and the likelihood of the solution disabling the drone. The next category is the likelihood that the solution is effective within the 30-foot radius of the dome. Ease of operation is an indicator of how easy it would be for a trained operator to operate the device effectively and quickly to meet the targets of effectiveness and neutralization time. Public safety and environmental safety are indicators to harm that may come to people or the environment within the dome of airspace. This device has the possibility to function in populated areas and safety as well as minimizing interference to other electronics is a goal. Total cost is an indicator of whether the total cost of the project remains within the $5,000 budget. Complexity is a measure of the amount of moving parts and/or conditions that have to be met for the solution to be successful. Portability is a measure of if the solution is able to be setup within the 4-hour requirement. Based on the house of equality the top three solutions in order are RF, Sound, and Hacking. The subjective reasoning behind these decisions is that RF alone may only cause the drone to hover and not bring it out of the airspace and may need other solutions to finish the job, however, RF is considered the most likely to affect the drone in some manner. The Net and Epoxy solutions' probability of being able to strike the drone decrease as the velocity of the drone increases whereas the velocity of the drone less affects the electrical solutions. An EMP attack, which causes a current surge, has possibly the highest chance of permanently disabling the drone of all the solutions, however, it is the least feasible of solutions to build based on the high complexity and cost of building an EMP generator. It is possible that it is impossible to get the amount of power required to disable a drone at the target distance of 30 feet. The table below displays the HOQ with the corresponding ratings for the neutralization systems of the device.

Table 10 displays the HOQ for the neutralization systems of the device.

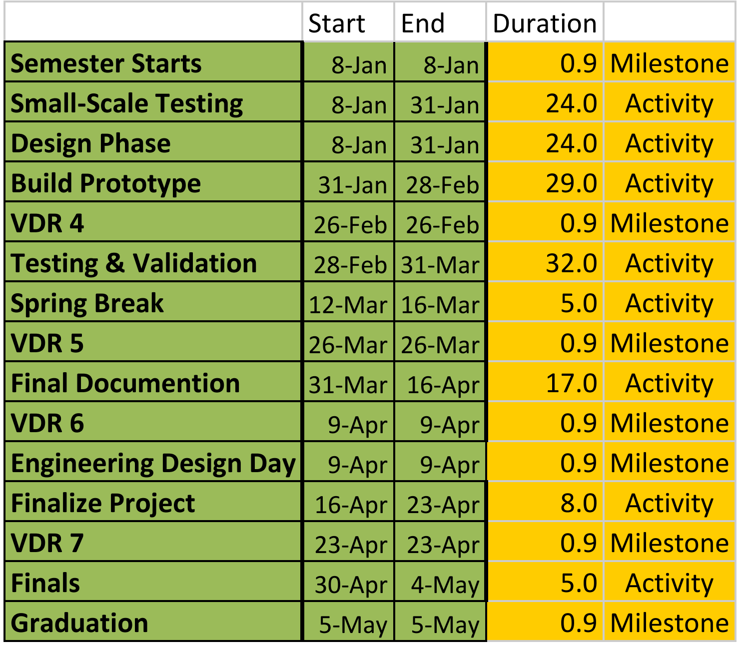
		Neutralization Systems					
Rank	**Categories**	**Net**	**Epoxy**	**RF**	**Sound**	**EMP**	**Hacking**
8	**Effectiveness (+)**	Medium	Medium	High/Large	Medium-Large	Low-Medium	Medium
7	**Range (+)**	Low/Small	Medium	High/Large	High/Large	Low/Small	High/Large
6	**Ease of Operation (+)**	Medium	Low/Small	Medium	Medium-Large	High/Large	Medium
5	**Public Safety (+)**	Low/Small	Low/Small	Medium	Medium-Large	Medium-Large	Medium
4	**Environmental Safety (+)**	High/Large	Medium	High/Large	Medium-Large	Medium-Large	High/Large
3	**Total Cost (-)**	Medium	Medium	Low-Medium	High/Large	High/Large	Medium
2	**Complexity (-)**	Medium	High/Large	Medium	Medium-Large	High/Large	High/Large
1	**Portability (+)**	High/Large	High/Large	High/Large	High/Large	High/Large	High/Large
		195	180	279	262.5	202.5	246

1.8 Spring Project Plan

In the upcoming month, the test bench will be created to verify our possible solutions. This test bench will involve a smaller scale testing of the neutralization methods to deem them as viable solutions or not. The small-scale testing will involve verifying if jamming the 2.4GHz radio frequency band to disrupt the controller to drone communication works with a household drone. Based on the possible outcomes, a second method will be applied. The possible outcomes of the first neutralization method are that the drone will just fall from the sky, the drone will hover until it regains communication with the controller, the drone will leave the specified air space and return to its origin, or the method will not work. The second method uses sound waves to confuse the gyroscope causing false orientation readings being sent to the flight controller causing it to terminate flight and fall from the sky. Testing at this stage is important because if either of the methods of neutralization do not work then we need to go back to our generated concepts. If the sound waves do not confuse the gyroscope and the drone remains hovering in the airspace, a mechanical approach can be used such as the weighted net or the epoxy attack. These approaches work better when the target is stationary therefore a combination of jamming the frequency and a mechanical attack could be another complete attack.

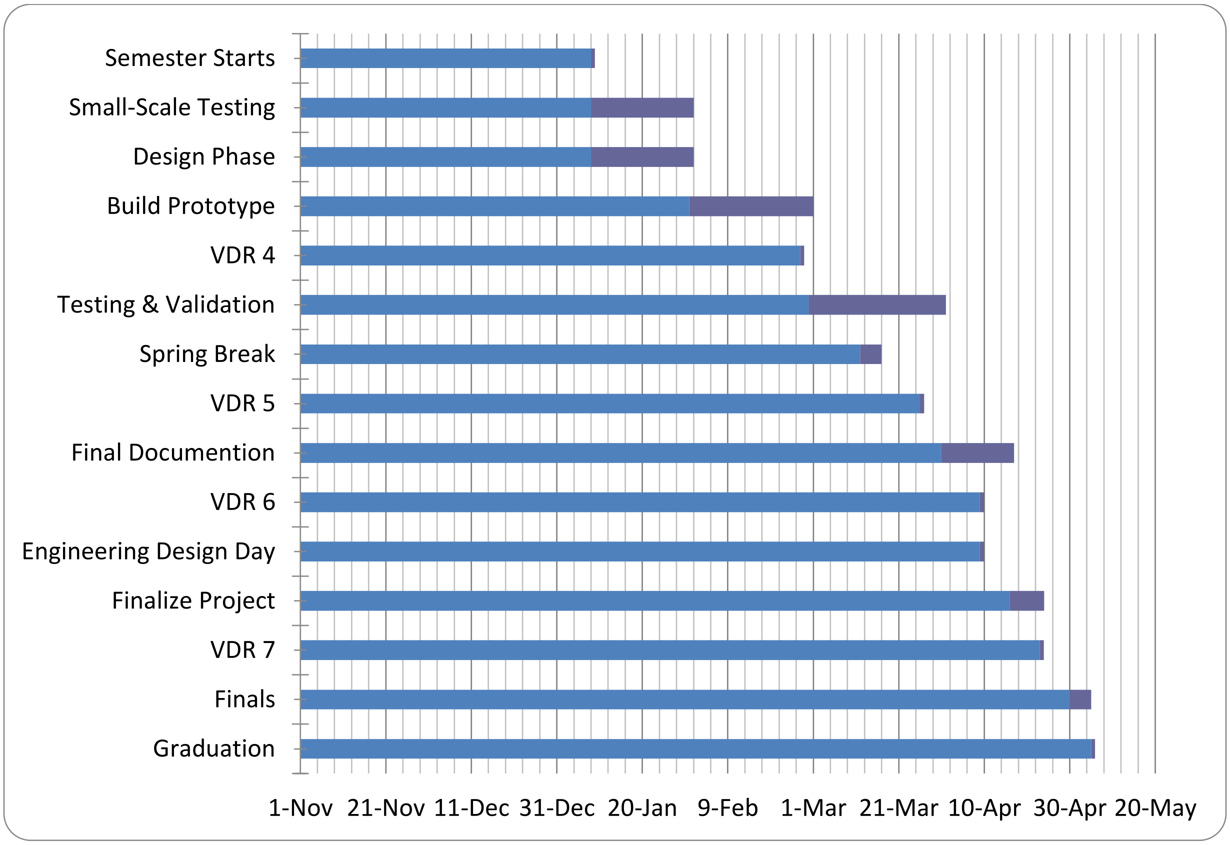
The milestones for spring semester include: semester start, VDR 4, VDR 5, VDR 6, Engineering Design Day, VDR 7, and graduation. The activities that are necessary to see those milestones met are addressed below in table 13. The timeline for the project is further represented in figure 21 as a Gantt chart.

Table 13 displays the start date, end date, and duration of milestones and activities



	Start	End	Duration	
Semester Starts	8-Jan	8-Jan	0.9	Milestone
Small-Scale Testing	8-Jan	31-Jan	24.0	Activity
Design Phase	8-Jan	31-Jan	24.0	Activity
Build Prototype	31-Jan	28-Feb	29.0	Activity
VDR 4	26-Feb	26-Feb	0.9	Milestone
Testing & Validation	28-Feb	31-Mar	32.0	Activity
Spring Break	12-Mar	16-Mar	5.0	Activity
VDR 5	26-Mar	26-Mar	0.9	Milestone
Final Documention	31-Mar	16-Apr	17.0	Activity
VDR 6	9-Apr	9-Apr	0.9	Milestone
Engineering Design Day	9-Apr	9-Apr	0.9	Milestone
Finalize Project	16-Apr	23-Apr	8.0	Activity
VDR 7	23-Apr	23-Apr	0.9	Milestone
Finals	30-Apr	4-May	5.0	Activity
Graduation	5-May	5-May	0.9	Milestone

Figure 21 displays the project timeline represented as a Gantt chart



In January, we will purchase the necessary materials to perform the small-scale testing. By the end of January, we intend to have completed all necessary small-scale testing and ironed out all design related issues. Through the month of February, we will be in the construction phase of the product. In the meantime, there will be various Design Reviews that we will have to prepare to present our current progress on the final product. Also, the website for our project will be designed and updated as important milestones are hit. The website will also include all of our deliverables from the fall semester which involved the planning phase and all the research that was done. Given that the device is fully built by the end of February, we intend to begin testing of the product through the months of March and April. At the end of April our team will have designed a fully functioning device with the necessary evidence that proves our device accurately and effectively disables drones within the specified air space of a 30-foot radius done. At the beginning of May, we will present our final product and report on all the steps that were taken to get to the final fully functioning deliverable. Once this is completed, we will graduate May 5th, 2018.

Chapter Two: EML 4552C

2.1 Spring Plan

Project Plan.

Build Plan.

Appendices

Appendix A: Code of Conduct

Mission Statement

Team 13 (Drone Disabling Device project team) is committed to ensuring a positive work environment that supports professionalism, integrity, respect, and trust. Every member of this team will contribute a full effort to the creation and maintenance of such an environment in order to bring out the best in all of us as well as this project.

Roles

All team members are responsible for any role(s) they are assigned. Specific roles are assigned based on each team member’s skills and are included in the following:

Project Manager

Project manager is responsible for communication with our sponsor in a professional and timely manner. Will assign tasks for team members and will look over final results prior to submission. Project manager will organize and schedule team meetings and any other necessary events. Responsible for enforcing all code of conduct rules and promoting team enthusiasm.

Lead Mechanical Engineer

Oversees the design, build, and testing of mechanical aspects of the project. Cooperatively works with other lead engineers on tasks overlapping multiple disciplines. Verifies integrity of mechanical systems of the project. Responsible for ensuring all mechanical documents are accurate and transferred to scribe upon completion.

Lead Computer Engineer

Oversees the design, build, and testing of programming aspects of the project. Cooperatively works with other lead engineers on tasks overlapping multiple disciplines. Responsible for ensuring computer aspects of the design integrate with the rest of the design. Responsible for ensuring all computer documents and source code are accurate and transferred to scribe upon completion. Also acts as assistant webmaster.

Lead Electrical Engineer

Cooperatively works with other lead engineers on tasks overlapping multiple disciplines. Responsible for design, production, integration, and documentation of all electrical aspects including, but not limited to circuitry, hardware, and fields.

Financial Advisor

Handles the overall project budget and documents all financial related expenses. Prior to the purchase of parts, the financial advisor must find multiple competitive quotes and receive approval from advisor.

Webmaster

Creates a team website that is easily accessible and user friendly. Responsible for keeping website up-to-date with the latest reports and presentations.

Scribe

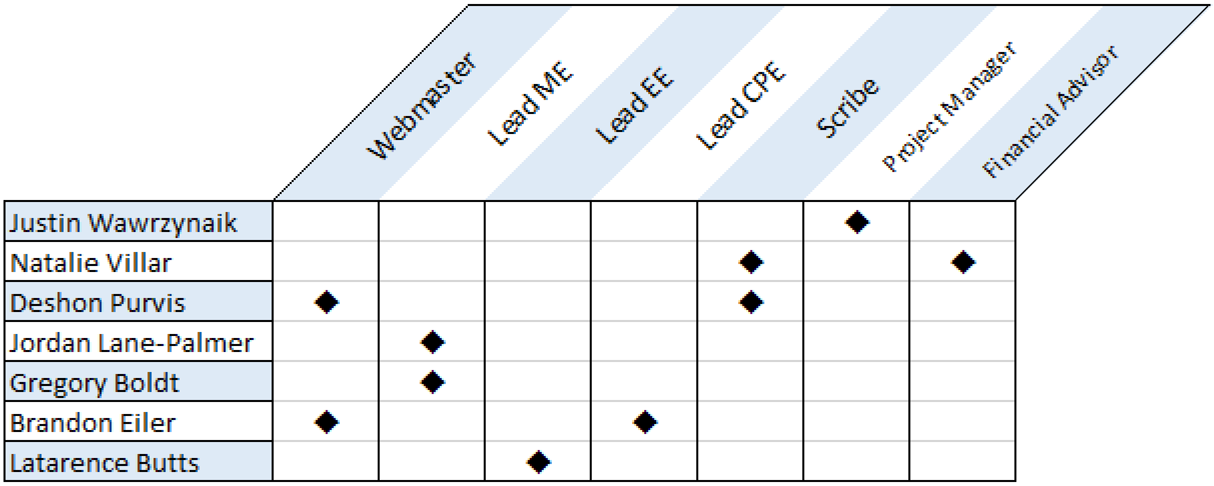
The main responsibility of the scribe is to keep documentation of all team activities. This includes maintaining the evidence book and acquiring all documents from other leads. Any emails or phone calls deemed important must be recorded by the scribe.

All Team Members:

- Abide by code of conduct
- Active participation in the project
- Delivers on commitments

- Be open minded to ideas and comments from all other members
- Be respectful to all team members, advisors, and sponsors
- Ask for assistance from other team members when needed
- Promote a positive team image

Organization Chart



	Webmaster	Lead ME	Lead EE	Lead CPE	Scribe	Project Manager	Financial Advisor
Justin Wawrzynaik						◆	
Natalie Villar					◆		◆
Deshon Purvis	◆				◆		
Jordan Lane-Palmer		◆					
Gregory Boldt		◆					
Brandon Eiler	◆			◆			
Latarence Butts			◆				

Figure 15 is an organization chart indicating what roles each member will be responsible for.

Weekly Meeting Times

Each team member's availability is given and consolidated to the calendar shown in figure 2 (last page). Weekly team meetings have been tentatively scheduled for the weekends. Weekday meeting can be coordinated if necessary but must be respectful of team member's stated availability.

Communication

The main outlets for communication will be over the phone and text messaging on the team GroupMe chat. Secondary forms of communication will include emails for documentation purposes and comments left on documents in the team Google Drive.

GroupMe chat notifications should not be silenced for any reason. Group members will be courteous and not "blow up" the GroupMe chat with excessive messages. Team member will send only project related messages via the GroupMe chat.

Emails must be checked at least once daily by all group members but 2-3 times is preferred. All information from the sponsor or critical group decisions will be sent via email. Time-sensitive information may also be added into the GroupMe chat or communicated over the phone.

Meeting cancellations must be sent to all group members via the GroupMe chat. It is preferred that a 1-2 day heads up on cancellations will be given. It is unlikely that a group member can attend all team meeting and must inform the group in advance if they cannot attend a team meeting. The absent group member(s) must provide a valid explanation for missing the meeting except if for personal reasons. Repeated absences will be brought to Dr. McConomy's attention for further action.

Team Dynamics

Team members are encouraged to be a part of all aspects of the project and not confined entirely to their roles. Team member are encouraged to voice all suggestions, concerns, constructive criticism, and/or ideas they may have. Sexual harassment or disrespect of any kind will not be tolerated and will be addressed immediately. All members should embrace roles, responsibilities, and tasks that challenge them but should feel comfortable asking for help if needed. At the end of the day, we shall work as a team to ensure deadlines are met.

Ethics

All team members should be familiar with ethics taught in Engineering Design Methods (EML4550) and NSPE Engineering Code of ethics. The group should ask the sponsor about any confidential information that needs to be protected when speaking with industry competitors.

Dress Code

There is no dress code set forth for team meetings. A business casual dress code will be adopted for sponsor meetings and may be subject to lessen if deemed suitable by the group. A strict business formal dress code will be enforced for group presentations.

Weekly and Biweekly Tasks

Weekly and Biweekly tasks will be delegated at team meetings and work on through the team Google Drive. Therefore, attendance to these meetings is required. Absences to team meeting without meaningful excuse are not allowed and will be reflected on team member reviews.

Decision Making

A voting system will be implemented for all decisions made relating to the project. The majority of the team must agree and that decision must be documented. Any members who are believed to have a conflict of interest in the decision making process are excluded from voting. Potential ethical and moral conflicts should be considered during all decision-making processes. Proper research must be done prior to decision making to help ensure a proper decision is made.

Conflict Resolution

If a conflicting event occurs between team members, the following rules shall apply:

1. All parties will be given a chance to present their argument free of interruption.

2. Team members must actively listen to the arguments presented and attempt to understand the pros/cons.
3. The event shall be resolved with a vote, favoring the majority.
4. Project Manager will have final say for a split decision.
5. If conflict continues, instructor intervention is required.

Statement of Understanding

By signing this document, the members of Team 13 agree to all the above and will abide by the code of conduct set forth by the group.

Name	***Signature***	***Date***
Natalie C. Villar	Natalie C Villar	09/22/17
Justin M. Wawrzyniak		9/22/17
Gregory Boldt		9/22/17
Jordan M Lane-Palmer		9/22/17
Deshon A Purvis	Deshon	9/22/17
Latarence Butts	Latarence Butts	9/22/17
BRANDON EILER		9/22/17

Team Member Availability

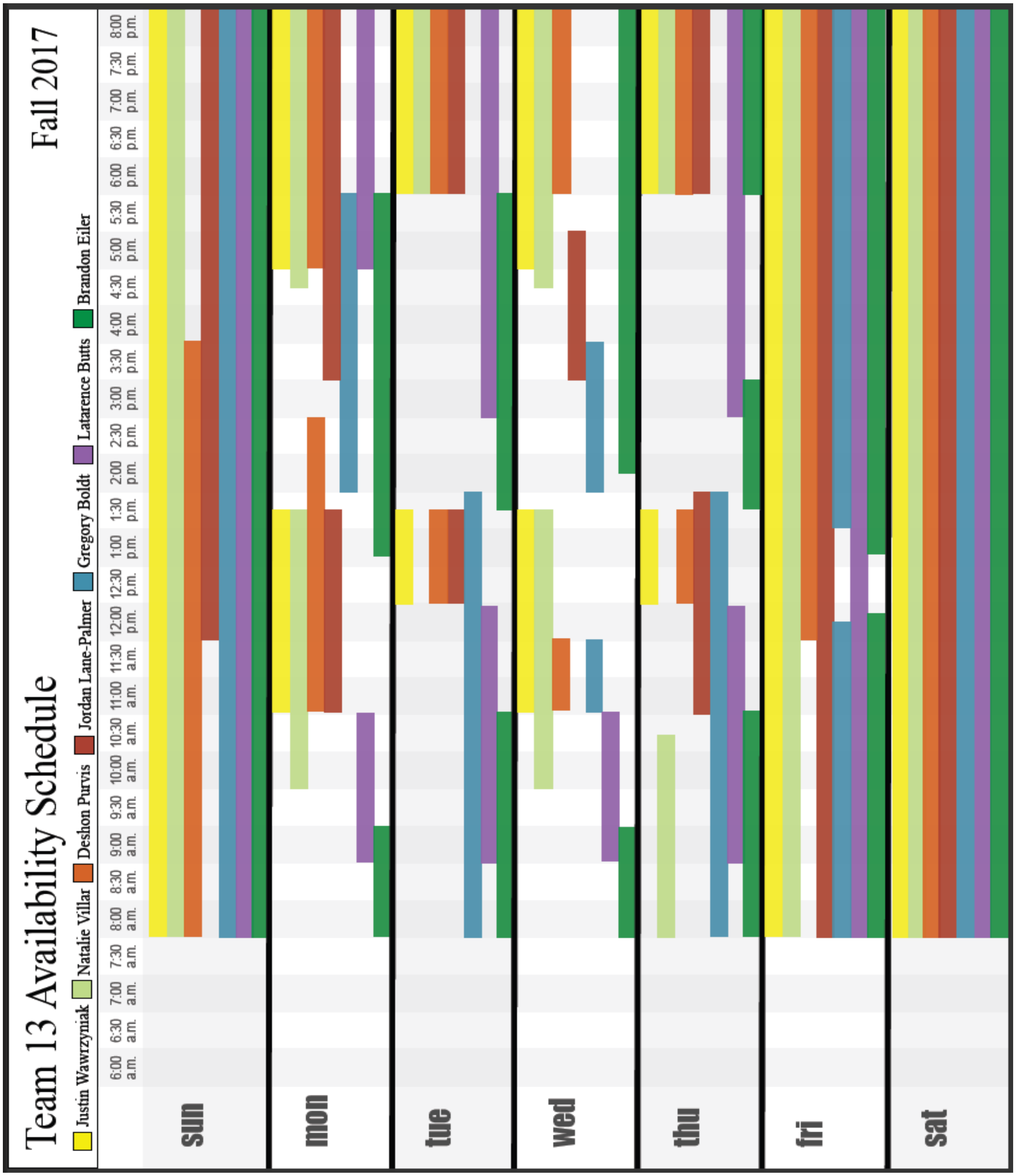
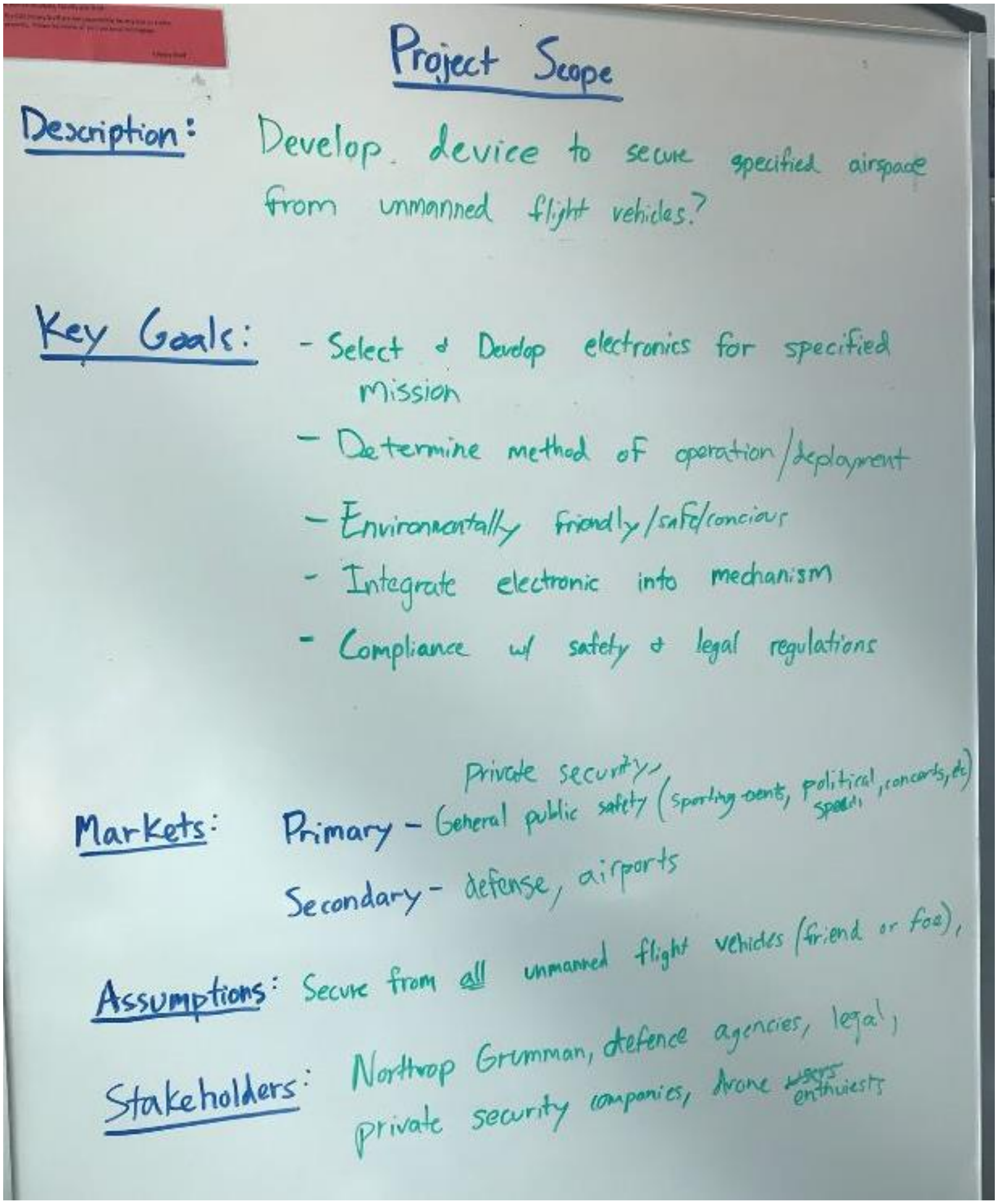


Figure 16 shows a calendar representation of all team members weekly availability.

Appendix B: Project Scope



Project Scope

Description: Develop device to secure specified airspace from unmanned flight vehicles?

Key Goals:
- Select & Develop electronics for specified mission
- Determine method of operation/deployment
- Environmentally friendly/safe/concious
- Integrate electronic into mechanism
- Compliance w/ safety & legal regulations

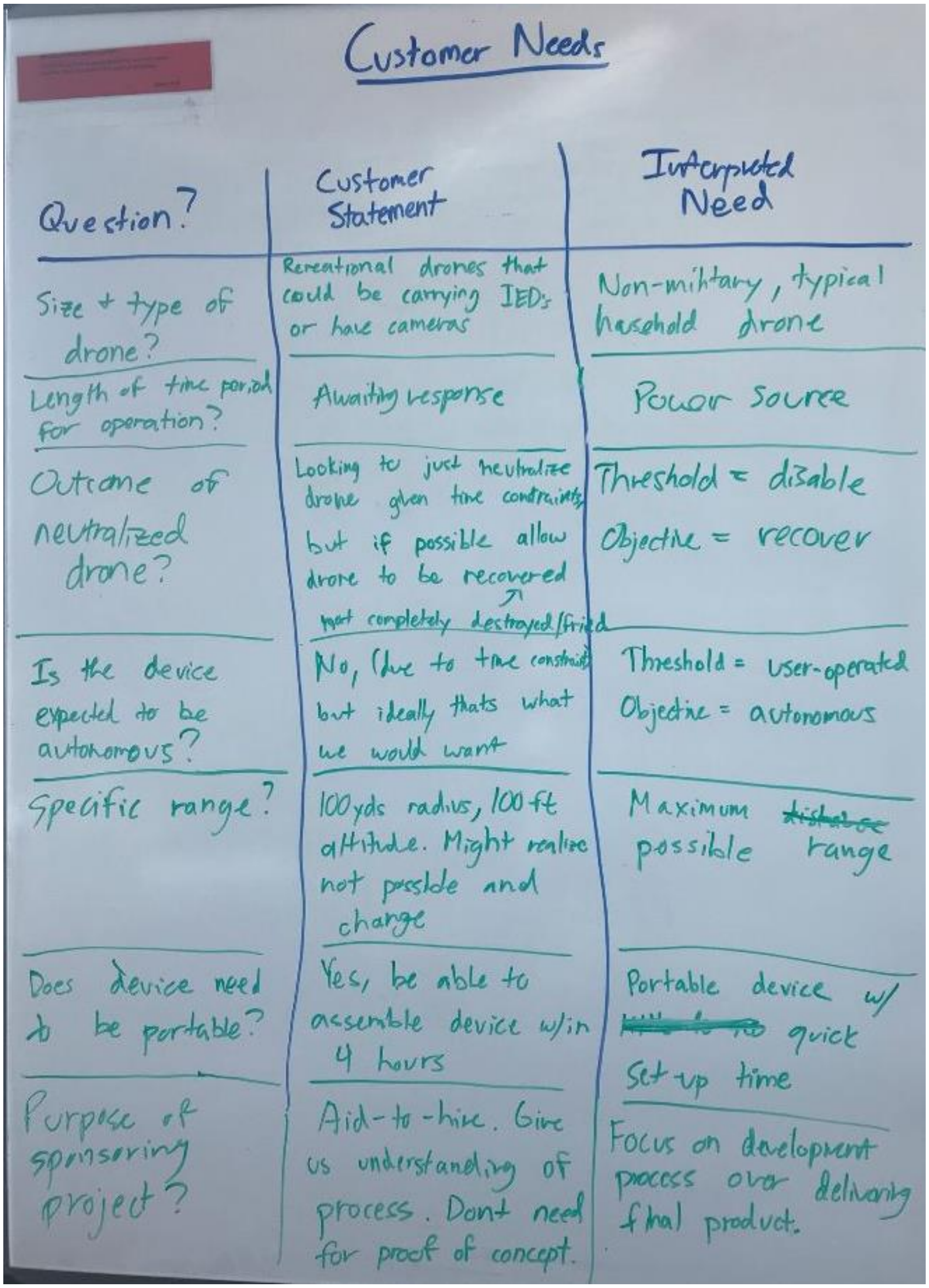
Markets:
Primary - General public safety (sporting events, political speech, concerts, etc) Private security,
Secondary - defense, airports

Assumptions: Secure from all unmanned flight vehicles (friend or foe),

Stakeholders: Northrop Grumman, defence agencies, legal, private security companies, drone ~~users~~ enthusiests

Figure 17 displays our team brainstorming for the project scope.

Appendix C: Customer Needs

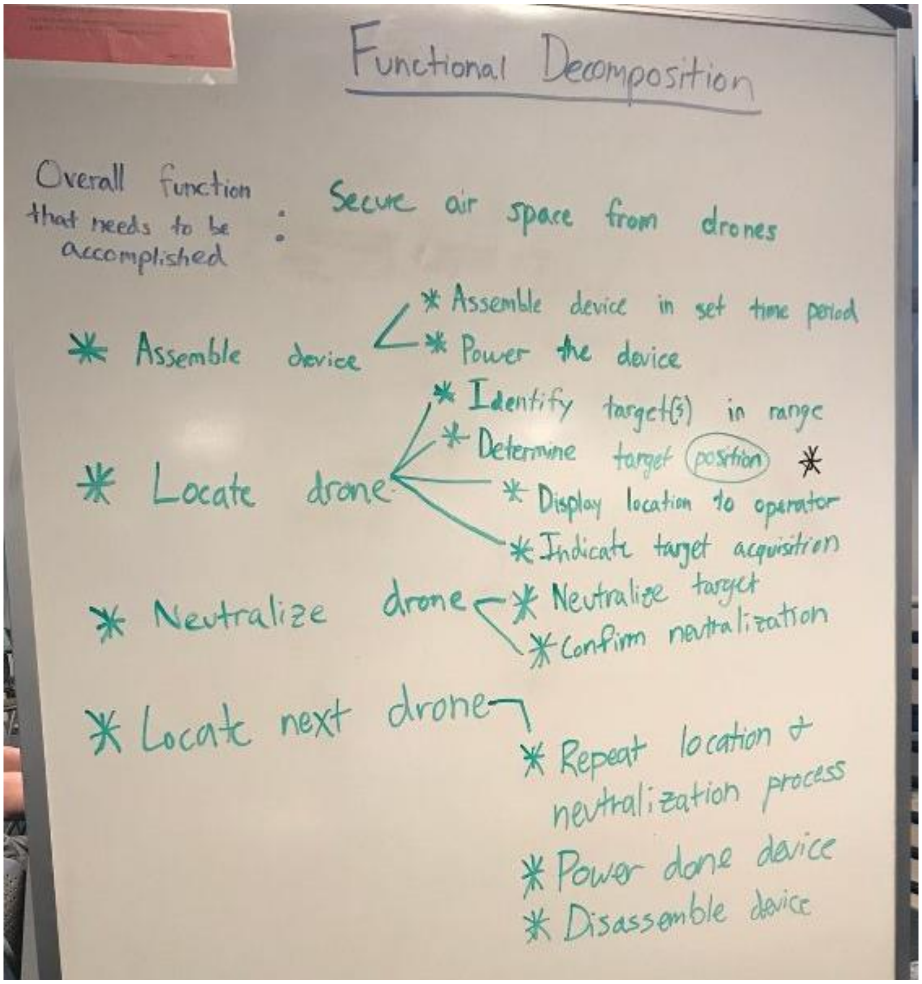


Customer Needs

Question?	Customer Statement	Interpreted Need
Size + type of drone?	Rereational drones that could be carrying IED's or have cameras	Non-military, typical household drone
Length of time period for operation?	Awaiting response	Power Source
Outcome of neutralized drone?	Looking to just neutralize drone given time constraints but if possible allow drone to be recovered not completely destroyed/fried	Threshold = disable Objective = recover
Is the device expected to be autonomous?	No, (due to time constraint) but ideally thats what we would want	Threshold = user-operated Objective = autonomous
Specific range?	100yds radius, 100ft altitude. Might realize not possible and change	Maximum ~~distance~~ possible range
Does device need to be portable?	Yes, be able to assemble device w/in 4 hours	Portable device w/ [illegible] quick Set-up time
Purpose of sponsoring project?	Aid-to-hire. Give us understanding of process. Dont need for proof of concept.	Focus on development process over delivering final product.

Figure 18 displays the team brainstorming done for identifying customer needs.

Appendix D: Functional Decomposition



Functional Decomposition

Overall function that needs to be accomplished : Secure air space from drones

* Assemble device
  * Assemble device in set time period
  * Power the device
* Locate drone
  * Identify target(s) in range
  * Determine target position *
  * Display location to operator
  * Indicate target acquisition
* Neutralize drone
  * Neutralize target
  * Confirm neutralization
* Locate next drone
  * Repeat location & neutralization process
  * Power done device
  * Disassemble device

Figure 19 displays the team brainstorming for the functional decomposition.

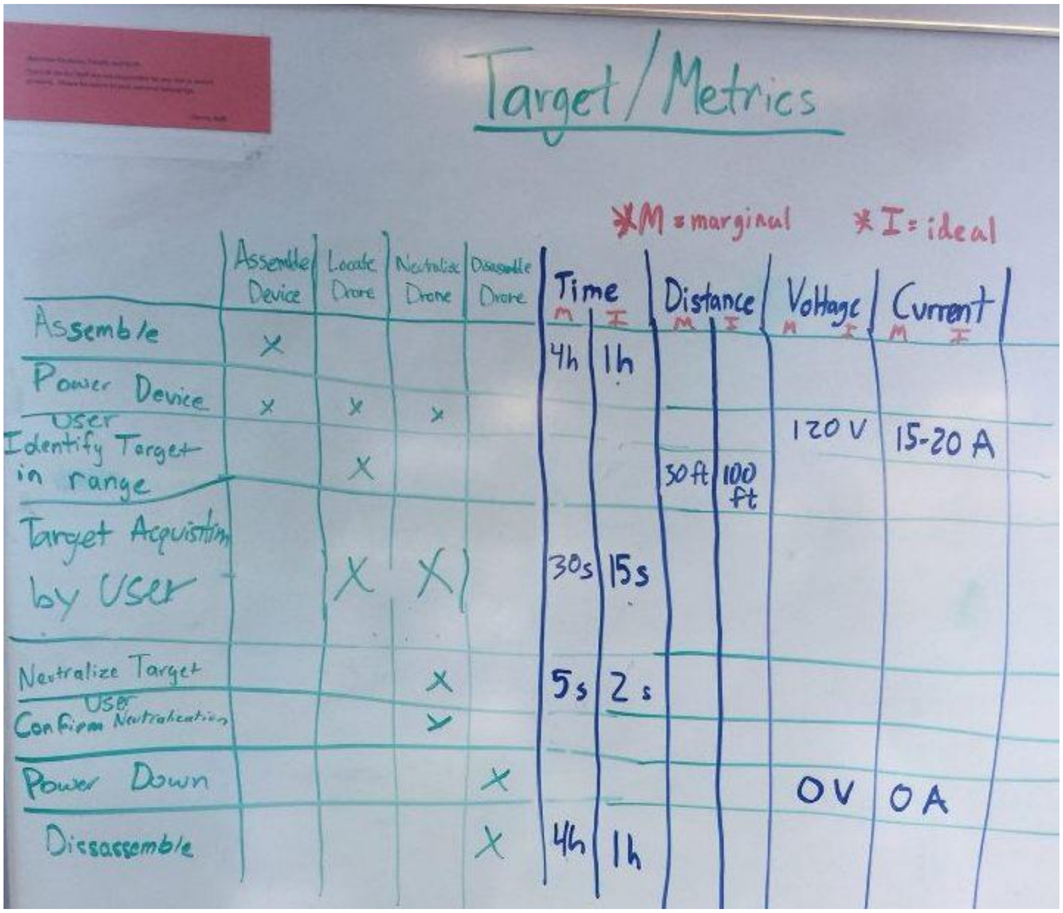
Appendix E: Target Catalog

Table 11 Qualitative Metrics

METRIC	**YES**	**NO**
Power up device	YES	
Identify drone	YES	
Lock on to drone	YES	
Neutralize drone	YES	
Repeatable	YES	
Power down device	YES	
Portable	YES	
Minimal damage to drone	YES	
Safe for surrounding environment	YES	

Table 12 Quantitative Sub-System Metrics

SUB-SYSTEM METRICS	**TARGET**	**UNITS**
Time to assemble device	4	hr
Device current	15-20	A
Device voltage	120	V
Range of device (dome)	30	ft
Time to find/lock on to target drone	30	s
Time to neutralize drone	5	s
Probability of hit	90	%
Probability of takedown	90	%
Time to disassemble device	4	hr
Project cost	5000	USD



Target/Metrics

*M = marginal *I = ideal

	Assemble Device	Locate Drone	Neutralize Drone	Dissasemble Drone	Time M	Time I	Distance M	Distance I	Voltage M	Voltage I	Current M	Current I
Assemble	X				4h	1h						
Power Device	x	x	x						120 V		15-20 A	
User Identify Target in range		X					30 ft	100 ft				
Target Acquisition by User		X	X		30s	15s						
Neutralize Target			x		5s	2s						
User Confirm Neutralization			x									
Power Down				x					0 V		0 A	
Dissassemble				X	4h	1h						

Figure 20 displays team brainstorming of targets.

References

1. Sungho, J., Jong-Woo, S., Young-Jun, L., Woong-Hee, K., YoungHyoun, K., & Hae-Yong, Y. (2017, January 20). Empirical Study of Drone Sound Detection in Real-Life Environment with Deep Neural Networks. Retrieved November 3, 2017.
2. Naboulsi, Z. (2015, May 28). Drone detection: What works and what doesn't. Retrieved November 03, 2017.
3. Surveillance-Video. (2017). Dotworkz KT-MIC Outdoor Microphone Kit. Retrieved November 03, 2017.
4. Sensia Solutions. (2015, July 24). UAV, RPAS, INFRARED DETECTION. [Infrared system to uav detect]. Retrieved November 3, 2017.
5. Surveillance-Video. (2017). Veilux VB-70IRC80L650D Bullet Camera. Retrieved November 03, 2017.
6. Jammer. (2017). Drone Killer 6 - Powerful UAV (GPS WIFI 5GHz) Jammer. Retrieved November 03, 2017.
7. Chalambalis, D. (n.d.). Detect Drones. Retrieved November 03, 2017.
8. MNS Laboratory. (2016, June 29). DronePD - Drone Police Department - project [System Overview]. Retrieved November 3, 2017.
9. Chua, Mike. “Bring Down Rogue Drones In A Controlled Manner.” MikeShouts, MikeShouts, 26 May 2016.
10. Sharma, Kritika. “Exclusive: Delhi Police to Use High-Tech Sound Device to Disperse Unruly Protesters.” India Today, India Today, 1 May 2013.

11. Trippel, Timothy. “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks.” University of Michigan, 1 Apr. 2017.
12. Son, Yunmok, and Hocheol Shin. “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors.” Usenix Advanced Computing Systems, 12 Aug. 2015.
13. Voute, Christopher, et al. “Making Electromagnetic Weapons: Directed Microwave Energy.”WonderHowTo, WonderHowTo, 9 Feb. 2012.
14. Sneiderman, P. (2016, June 08). Here's how easy it is to hack a drone and crash it. Retrieved November 02, 2017.
15. Harris, T.(2001, May).How Paintball Works. Retrieved November 03, 2017.
16. Dailey, M., Silva, A., McIntire,P., Wilson,G., Moore,J., & White,S. (2014, September) A self-healing biomaterial based on free-radical polymerization. Retrieved November 03, 2017.