

MTRX1701

**Introduction to Mechatronic
Engineering**

Assignment 4

**Major Assignment/Case Study
Report**

**Drone Detection and Neutralisation System
(DDANS)**

Group: Vishant Prasad (470416309), Yu Hz (460207869), Humaira Nisha
(460477819)

Submission Date: 6:05 pm, 9 June 2017

Executive Summary

The following report incorporates the design process, description and construction of the Drone Detection And Neutralisation System (DDANS). The goal of the project is to serve as protection at a venue or public event, keeping the airspace and overall sanctioned area of the event clear of all possible small scale aerial vehicles and therefore, airborne terror attacks. The system relies on hardware technologies to sense and neutralise the threat. The overall project is a mechatronic based system.

Executive Summary	1
Summary Description	2
Mission Overview	2
Requirements Analysis	3
Functional Specifications	4
Environment Specifications	5
Functional Block-Diagram	6
Component Description	7
Other Mechatronic Components	7
Description of Actuators	8
Description of Sensors	9
Control Systems Description	10
Computing and Processing Elements	10
Hardware	10
Software	11
Process Description	12
Diagrams	12
Summary	12
Testing	13
Recommendations	13
Appendix	14
Reference List	16

Introduction

The aim of the project referred to as Drone Detection And Neutralization System is to allow for the security of public events within an open environment of any kind. The DDANS possesses the capability to provide ariel protection from drone inspired terror attacks and other airborne small vehicle attacks. The system operates day or night through almost all weather conditions at any location necessary. DDANS will detect such vehicles and will neutralise the threat.

Summary Description

DDANS is ideally designed for operation in stadium events, restricted areas, headquarters and military bases and defensive areas, carnivals, concerts festivals and other public events. DDANS is a joint computer-radar mechatronic system that will detect any small airborne vehicles such as drones. The detonation function will be immediately disabled upon the hijacking the drone as the attacker will have no control over the drone and their signal will be jammed with no outputs from them being able to be received by the drone. Means of hacking the drone will be reduced upon hijacking the drone using an encrypted signal and source firewalls. Backup countermeasures must be considered in the case of the system failing or not operating as per planned. Furthermore, the system must have appropriate and strong security to eliminate the possibility of hacking the system.

Mission Overview

Prior to operation of the system, a perimeter must be set up surrounding the area being monitored. The perimeter must be large enough to cover the designated area of the public event but also must not be larger than the range of the systems signals. The system is able to detect the drone within the area of service or the public area and will attempt to hijack the drone allowing for the user to overtake the controls of the drone from the attacker. Hacking the drone will be accomplished by decryption of the source signal. From this stage the drone will be identified through the vast database in the case the drone is a news drone or unit. In the case the drone is not a threat, the controls will be returned to the previous source otherwise, the drone will be landed at a designated position away from the event or protection zone where it then will be powered down. From here, ground units such as a bomb squad, hazmat unit, fire department, police or SWAT can advance on the drone and investigate its contents with care. The system can track the location of the attacker or the drone control and further assist in the investigation of the attacker. Security of the civilians is the highest priority therefore, any drone within the zone will be hijacked prior to identification to eliminate any chance of an attack or explosion from the drone. Any explosives, chemical weapons, radiological or biological weapons possessed by the drone therefore, will have no chance or time to explode within the area and affect the dense population.

Requirements Analysis

The requirements of this system includes the operation of the system must be constant through a long period of time or the time of the entire event being protected as well as possibly until all civilians have left the area and is clear of the dense population.

Furthermore, the requirements include the system to be operational through differing times of the day and through the night with no issues. The system must also be operational through a variety of weather conditions as long as the civilians are still present in the area and can only be powered down when either the customer is satisfied with the services to be switched off and/or until the population has dispersed. DDANS must primarily avoid the detonation of an enemy explosive situated on a drone or other airborne small vehicle. The system may also accomplish this objective with explosives placed on a motor vehicle, boat or person. The system must limit the collateral damage when the threat is destroyed and there must be no chance of any civilians being injured and killed. The size of the explosive of the simulated dirty bomb is estimated to be about 1 kilogram with the drone similar to a DGI Phantom weighing about 3 kilograms and is approximately 29 centimetres wide, 14.4 centimetres long and 19.2 centimetres in height. The area being protected in this report will cover a situated population at the Sydney Harbour on New Year's Eve event. The 'dirty-bomb' is planned to carry the bomb to Mrs Macquarie's Chair to go off at midnight in close proximity to both large numbers of civilians and the Garden Island Naval base (where the ship is docked). The area is estimated to be 30 acres (12 hectares) of land connecting Garden Island to the mainland.

Furthermore, the cost the system has no limits. The system project matrix ideally has no limitations except the features must be optimized to allow for maximum security and safety.

	Constraint	Optimize	Accept
Feature		X	
Cost			X
Time	*	*	*

Figure 1: Project Matrix Diagram (Plan)

Distances (m):	Force (kPa):	Injuries:	Structural Damage:
1	1000	Severe contusion and injury, ruptured internal organs, bone fractures, internal bleeding, concussion and prolonged loss of consciousness. Fatalities possible.	Irreversible distortion and destruction to metal structures, shape and appearance.
2.7	100	Severe contusion of the entire of the entire body, injuries, loss of consciousness, bone fracture, nose and ear bleeding. Possible internal injury and bleeding.	Major damage that may lead to partial collapse of walls, pillars and ceilings. Total destruction of lightweight components.
11	10	Fatalities are ruled out at this distance. Minor injuries may occur.	Minor damage may be caused to machinery that will not disable it. Lightweight component parts may be damaged severely deformed.

Functional Specifications

DDANS firstly, utilizes sensors to detect any drones within the designated area. This is accomplished by employing a radar system. The system utilizes a solid state radar system that is lightweight and mobile allowing for quick deployment anywhere at anytime. The system itself is cost effective and small weighing less than 20 kilograms. Examples of such radar that are calibrated for drone and unmanned aircraft vehicle detection include the Sharpeye Solid State X-Band Doppler Radar, Sharpeye SXV and Cx Eye. The 'dirty-bomb' of 1 kilogram weight has a relatively small explosion radius considering the entire area being monitored is approximately 30 acres therefore, the system range must be able to cover such an area.

Most of the above drone detection systems have a 1 kilometre range therefore, capable of covering the area as evidenced by calculations in figure 2. The drones range must also be within the signal coverage after it is hijacked and must stay within the signals range until it is at the clear zone location where it can be attended to by ground units. This maybe accomplished by using other radio signals, adjusting or employing an appropriate radar with the appropriate range/coverage or boosting the signal source or signal along its transmission. Utilizing filters is an appropriate method to negate signal interruption and noise from the surrounding with many other signals (especially with the large amount of people in the area and such individuals technological devices). Negating the noise from other alternative sources is important to allow for the system to accurately and efficiently identify the threat. The drone is to be detected at a safe distance away from the crowd in the case of any such errors or detonation and to reduce any chance of casualties of injuries. Furthermore, the drone must be able to identify and differentiate between threats and

surveillance or tv station and recording drones. Similar differentiation must also be made for other mediums of vehicles.

Any threat must be neutralised with minimal collateral damage therefore, the system must be able to move the threat away from any populated areas, to a secluded and quick to travel to zone that is restricted for security and safety. The line of sight is also a major consideration as a blind spot can put the population at risk as it is a path or area that is not being monitored by the radar system.

Environment Specifications

The area is situated within the Sydney Harbour which is an urban setting. The area is a port for ships and contains a large park area with trees and surrounding warehouses and relatively small sized buildings away from the city centre. The area would therefore, have a large population in a small area on the Island. There is a connection to the mainland. There is a relatively clear airspace with no major structures towering over the area.

The nearest clearing for the bomb to be escorted to would most likely be either the ocean however, if the bomb is chemical, biological or radiological then sealife, fauna and flora would be at risk with the water being contaminated. The water would also at the time most likely be populated with multiple boats and spectators on ships. Therefore, a safer option would be to escort the bomb to a setup clear zone such as an open field with easy access for vehicles and staff for disarming, dismantling and investigating. The zone would have to be kept clear through the night or the event of people. This zone would be the soccer field at Double Bay Wharf on the corner of William Street, Ocean Avenue and Bay Street. This is an easy zone for police, bomb squad and other necessary ground units to travel to with three roads around the field. A motor vehicle would take 15 minutes to get to the location travelling over a journey of 6.4 kilometres. This is approximately a sufficient time for the drone to be landed from Garden Bay Island to the Double Bay Wharf allowing for the drone to be quickly attended to. The quickest and shortest path to Double Bay Wharf from Garden Island is 1.9 kilometres which is the path that will be autonomously followed by the drone. This path information can be uploaded to the system using software such as Google Maps, MATLAB and a GPS.

Other sensors such as ultrasonic sensors can allow for the detection of obstacles when the drone is travelling autonomously. A user can take over this auto-pilot mode of the drone and manually control the path of the drone and its motion and can use the cameras and GPS locator to determine its position at all times. The drones path would have to avoid most of the more densely populated areas which at the time would be close to the water frond therefore, a path has been traced out displayed in figure 3. The surrounding environment at the time will contain many other signals which will require filtering to allow for the system to perform accurately. The system components must be functional through all and any weather condition that the event continues through or the population attends. For example, light to heavy rain, heat, storms and windy conditions however, there would most likely be no snowy and the event may not continue at the location if there is hail or heavy storm conditions.

Functional Block-Diagram

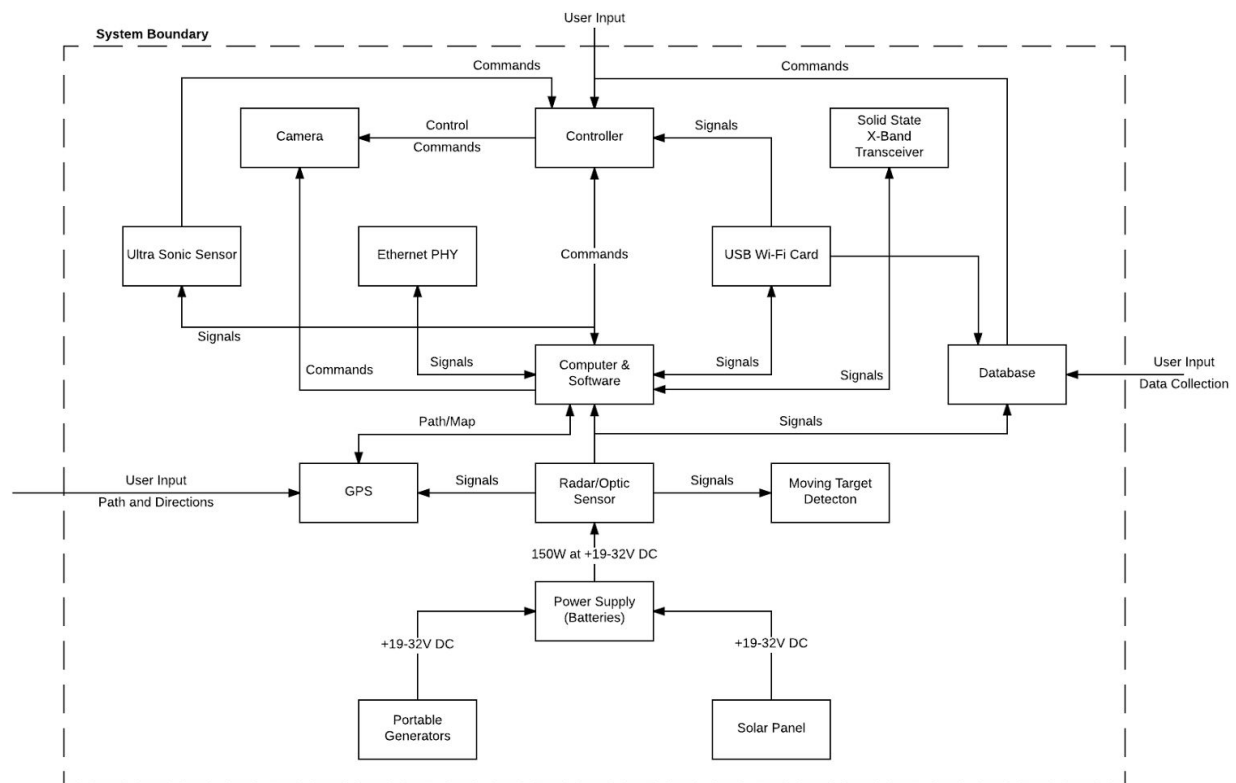


Figure 4: Functional Block - Diagram

The radar system being employed is a SharpEye SxV with CX Eye Software and a GPS and mapping system. Such mapping software can include Matlab and Notepad+ with positions and coordinates tracing out a path on Google Maps or Google Earth uploaded onto the system to allow for the drone to travel the designated planned path to the restricted safe zone where the bomb can be attended to by a bomb squad, police, etc.

The main processing unit within the computer responsible for the hijacking of the drone will be a Raspberry Pi that will disable the drone using Wi-Fi connection as many drone do utilize Wi-Fi connections with USB or a Wi-Fi card and an antenna.

Multiple radar nodes would have to be implemented as each node covers a range of 1 kilometre. Most drones have a 3-5 kilometre, use only 2.4GHz Wi-Fi and GPS L1 with others operate at 5.8GHz, 433MHz and 928MHz can control 500-1000 metres at maximum range.

The signal jammer within the system will require a filtering which can be accomplished with MATLAB via sensor sampling and signal smoothing by applying a moving average filter eliminating some degree of unwanted interference and noise.

Component Description

<u>Actuators</u>	<u>Description</u>	<u>Sensors</u>	<u>Description</u>
Controller	The controller is used to carry out operations of the drone. Joystick and on screen control.	Moving Target Detection (MTD)	Detects any moving objects within the airspace as a change in the foreground with reference to a background.
Radar Antenna	Antenna used to boost the range of the radar, 522mm Rotating Array 360 degree coverage.	GPS	Hema Navigator HN7 detects the drones position as it enters the restricted airspace.
Electrical Motors	Motors that control components of the drone and radar to allow for antenna rotation.	Optic Sensor	Electro optical sensors paired with the radar. Detects the change in light and converts such magnitude in change into an electronic signal.
Rotors	Component of the drone, rotor blades, radar and signal sensors.	Electro Optical Camera Sensors	Deployed on a Single Mast Solution (SMS) for mobile and semi-permanent presence.
Servo Valve	Offers closed loop control of acceleration, velocity, position and force monitoring concerning the drone.	Ultrasonic Sensor	Set on the drone, it uses sound waves to measure the distance from an enemy objects.
Camera	Recording and capturing of the drone and it's perspective.	Radio Dish	A kind of powerful specialized Antenna that is used to receive radio waves from astronomical radio sources.
Single-Gimbal Control Moment Gyroscope (CMG)	Controlling the attitude of aircraft. Maintain a reference direction in the GPS and radar system.	X-Band Transceiver	Transmit and receive radio waves in 8-12Hz.
Signal Jammer	Jams up to 3 kilometres. 2.4GHz Anti-Drone 4 bands GPS L1 82W Signal Jammer.	Radar SharpEye SxV	Detects drones and UAVs with a 360 degree line of sight. Portable, compact and durable. Solid State radar employed as the transceiver.

Other Mechatronic Components

The radar sensor being utilized is the SharpEye SxV with corresponding CX Eye Software. The batteries employed into the system is military specification batteries for mobile and man portable applications such as the radar system and computer.

The power supply of +19-32VDC will be generated from either a portable fuel generator or electrical generator at night or a solar panel during the day.

The user can utilize the interface between the controller and a tablet displaying mapping and telemetry data. Premium mapping software can also be employed to map out any obstacles, tall objects, trees, etc and keep the system up-to-date rather than relying on Google's delayed satellite images. Such software includes terrain tools, mapt.io or GIS Interactive Mapping software. This can be coupled with an ultrasonic sensor for maximum accuracy. Specifications of the radar system includes its ability to provide all weather, day and night detection, deployment of a single unit or multi-node system to cover a larger area, environmentally sealed to work in extreme cold, heat as well as making the unit water proof. Other hardware components include mobile phones and smartphones or tablets, laptops or computers and monitors. Wi-Fi & Ethernet (Internet Connection) is a more software requirement that is necessary for the operation of hijacking the unidentified drone.

Description of Actuators

Controller: 4 channel joystick 2.4 Ghz and computer software will be used to control the drone, the joystick will be supplied by 3V batteries, and the computer will connect to the power supply system. IG will be used as an app to monitor the state of drone and be displayed on the computer screen.

Electrical motor: DC motor is set as a radar spinner, the spinner will be connected to motor controller that the spinning speed is able to modified by it with the control signals received from the computer. The initial velocity will be set to 12 RPM, and this will adapt to the reality when it is operating.

Servo Valve: It offers closed loop control of acceleration, velocity, position and force monitoring concerning the drone. It will be controlled directly by receiving computer signals, and port the hydraulic fluid to adjust the state of drone. The power is provided by battery on the drone.

Camera: The camera module we selected is GoPro HERO4 Black, It has good performance and high resolution in case of moving objects capturing with slow motion. It is controlled by computer and it sends messages back via Wifi connection. It uses its own battery of 5 - 12V.

Single-Gimbal Control Moment Gyroscope(CMG): This is utilized within the GPS system and component of the radar to reference the direction of the object being detected. This is also the attitude controller inside the drone, It adjust the attitude of drone using the sensed angular momentum, then it causes the drone rotate it utilizes power from the supply of the system or component power supply [1].

Signal Jammer: 2.4GHz Anti-Drone 4 bands GPS L1 82W Signal Jammer is used [2], the maximum jam distance is 3000m, it is activated when the unknown drone is detected. Interference signal will be emitted towards the enemy targets due to the instruction signals sent by the processor. Individual battery of 29V is used as its power supply.

Description of Sensors

GPS: The Hema Navigator HN7 will be used as GPS to display the detected unknown drone on the map with a cable connected to computer. It also receives the signal from the radar sensor.

Meanwhile, the power will be supplied by a cable connected to computer via the main power source/supply. It receives the wave signals from several satellites and processes the signal in its processor, then processes them into location coordinates, display to its screen, and send the coordinates to the computer. This can also be displayed to any user's devices such as a tablet or smartphone.

X-Band Transceiver: X-band wave is the waves whose frequency is at range 8-12Ghz. Means that rain, sea, snow, sand, dust and other forms of clutter does not affect the system. It will transmit the radio wave then receive the back waves, then uses them to measure the distance, angle, coordinates between the transceiver and objects [3].

Moving Target Detection (MTD): Similar to a radar, it indicates what is the moving object in a specified area, it uses Doppler effect to measure the received waves bounced back from objects, thus apply the calculation based on the relationship between observer and signal source, obtain the speed, distance information of a target [4].

Optic sensor: Optic sensor is used in pair with radar, because the radar signal is incredibly huge, the normal electrical measurement is not enough to measure those data. In this case, the light is used to transfer information for analysis, then the light information will be processed using diffraction grating spectrum of light.

Electro Optical Camera Sensors: It converts light into electronic signals [5]. This sensor measures the quantity of light, then translate the signal to a readable form of data for an instrument.

Ultrasonic Sensor: This sensor emitting the sound waves, at the same time, it receive the back sound waves. It measuring the distance between the drone and the objects through processing the time differences by ToF method [6].

Radio Dish: The radio dish is used to receive the the waves especially from radio sources in the sky, it is paired with radar and enhance the efficiency of receive signal. Sensing is accomplished through the EM spectrum transmitted, reflects from a 'scatterer' and gets read by a receiver. Pulse width is employed for required range resolution and appropriate bandwidth.

SharpEye SxV: Is a solid state radar that is employed as a transceiver which requires no maintenance or servicing. This radar system is specifically designed for the detection of small airborne/aircraft threats such as UAVs and drones. Contains a 360 line of sight resulting in no blind spots where the radar cannot detect an object. The radar system can operate through the night utilizing radio signals and waves to detect threats alongside electro optical cameras. The system can detect small, slow moving targets in all weather conditions [7].

The system is capable of detecting offshore IEDs using the camera and character recognition system and cross checking registered ships with a database system. Offshore threats can be detected in a similar manner as airborne targets utilizing the SharpEye SxV radar system.

Control Systems Description

A computer is being used to control the drone and the process of hacking the drone using Wi-Fi. This is the major component of control of the drone as it is the interface of connection of the radar system. This computer will be used for viewing the details and for displaying the gathered data that is being analysed constantly in order to detect any potential risk and identify the control source of the drone in the restricted area for example whether the drone indicates any potential risk or it is being used for other uses such as TV station for broadcasting purpose or surveillance. This computer configuration operates with a single mainframe computer and database system. The computer system contains a slight unnoticeable delay or lag as the signals travel to the components and receive corresponding signals. With the computer system having an optimal processor, graphics card and RAM alongside fast Wi-Fi connection, DDANS will have the capability of fast responses and display of information to the user.

The Minimum Specifications Required for the Computer Control System:

- Intel Core i5 Processor
- 2GB RAM
- NVIDIA GeForce GT240 Graphics
- Windows 7 or Windows 10 32 or 64 BIT

Computing and Processing Elements

The computerised control unit of the system requires the similar power source. However, the specifications are confined to specific combinations of several softwares and hardwares. Although, several alternatives can be found for specified components being used in this process, the more preferred ones for this process are noted below:

Hardware

Computer Hard Drives - In order to operate the different softwares required for this entire procedure. Store information concerning the systems operation and software and hardware memory as well as databases containing information on non-threatening targets.

Smart Devices (Smart Phone, GPS) - To track down and map the drone position, location, speed and other details regarding its motion and nature. The GPS has a 5 to 25 second delay that does negatively affect the accuracy of the system however, the threat will be hacked and signals jammed from the attacker disallowing for detonation of the bomb.

Wireless/Wired Internet Connection - Wi-Fi connection is preferred more in order to prevent any interface with the crowded mobile network in the heavily crowded area

Controller (Joystick) - Used to control the direction while flying the drone to a safer area out of the restricted zone for further inspection.

Power Supply - Required to operate the entire system. However solar batteries can also be used as an alternative source to provide the system with electrical energy.

Sensors - Required to measure entities like distance, angle, coordinates between the Transceiver and objects and even for tracking down the drone to find the exact location by using sensors like the GPS, X-Band Transceiver, ultrasonic sensor, etc.

Video Dish (Radio Dish) - It is paired with radar and enhance the efficiency of receive signal.

Software

MATLAB - Used to analyse the raw data obtained from the sensors and to process the data for graphing, plotting and for carrying out other necessary calculations in order to find the object's distance, location and mapping. Also utilized for photo recognition, filtering of signals, license plate recognition and detection of threats within the hardware of the system and the surrounding scripts that they run. Coding style is evident on the following website: <https://au.mathworks.com/help/vision/examples/digit-classification-using-hog-features.html>

Database Management System Software - Used to cross-check a drones details with none non-threatening/registered legally clearanced drones or UAVs in the Harbour area and on the night of New Year's Eve. Required to keep the system updated and to back up and to store the required information in order to access them later on if required.

Non-Threats: Commercial Flight

Any flights for commercial gain require certification of both the pilot (or UAV Controller) flying the actual drone, and the business which is conducting the operation. The pilot must have a UAV Controller's Certificate (formerly called Remote Pilot Certificate) and the business must have a UAV Operator's Certificate (or UOC).

From 25th September 2016 the term UAV will generally be replaced with RPA in official documents and the UAV Controller's Certificate will be replaced by the Remote Pilot Licence [8].

Anti-Virus - In order to keep the system keep running smoothly and to prevent it from crashing. This also helps to keep up the speed of the system.

Raspberry Pi SSH - Used to hack in through a system, where in this case it can be used to hack the UAV if it's using a Wi-Fi connection. It can also be used to carry out such software scripts and modify and delete system files and intercept video and sensor feeds.

Internet Connection - In order to keep up the system updated with the tracking information and then mapping the drone. Some other control processes also work better with the internet connection.

CX Eye Software - This software system is utilized for the Can be used for capturing pictures and also to act as surveillance camera.

GPS Software - In order to find the location of area of the drone or even the location of the control system from where the potentially risky UAV is being operated.

Mapping Software - Used to track down the exact location of the control system of the drone and also used for the drone itself. These sets of information are then viewed in the map for further action to be carried out.

Notepad+ - Can be used to store different information while analysis is going on or any decision has been taken.

Internet Browser (Internet Explorer, Mozilla Firefox) - Is used for internet surfing for useful information and also for mapping.

Video Recording & Playback Software - Used to record video, capture and view such footage. Also used to be read by software.

Process Description

Protection is a priority within this system and it is important to consider the threat of the systems controls being breached by unauthorised users, especially when using Wi-Fi as a means of communication with control machines. Therefore, countermeasures such as wireless security protocols, encryption, firewalls, anti-virus, authority levels and clearances and open ports are necessary for protection against any attempted breaches to the system. This can be employed into the system using third-party software or creating a custom built software and scripts to protect the system however, this will take more time and resources than outsourcing to another company such as Norton, McAfee or AVG Anti-Virus.

A priority of DDANS is to disable the enemy's capability of communicating with the drone therefore, signal source jamming is also a necessity in the security of the system. This would be accomplished using a Wi-Fi network-based attack against the drone. The SharpeEye SxV receives power from a generator and power supply and is connected to the mainframe computer to allow for the transmission of received and recorded data. Furthermore, the GPS is coupled with the radar system that also is connected to the mainframe computer. The connection for the radar and GPS can be wireless, however, is preferred to be a wired system to allow for quicker response times and reduce delay and lag in the transfer of data. The SharpEye SxV operates with its own custom software that allows for interfacing with the radar sensors and is capable of communicating with the computer systems able to receive information and send specific signal commands to concentrate on the desired target and aim its cameras in the corresponding direction. The database system can also be utilized to recover from system failures, loss of system data and corruption. Similarly, a false alert system is already in place on the radar for emergency deactivation in necessary circumstances, which is controllable by the user. The ultrasonic sensor interacts with the interface of the radar system and allows for the detection of any low altitude flying objects.

Diagrams

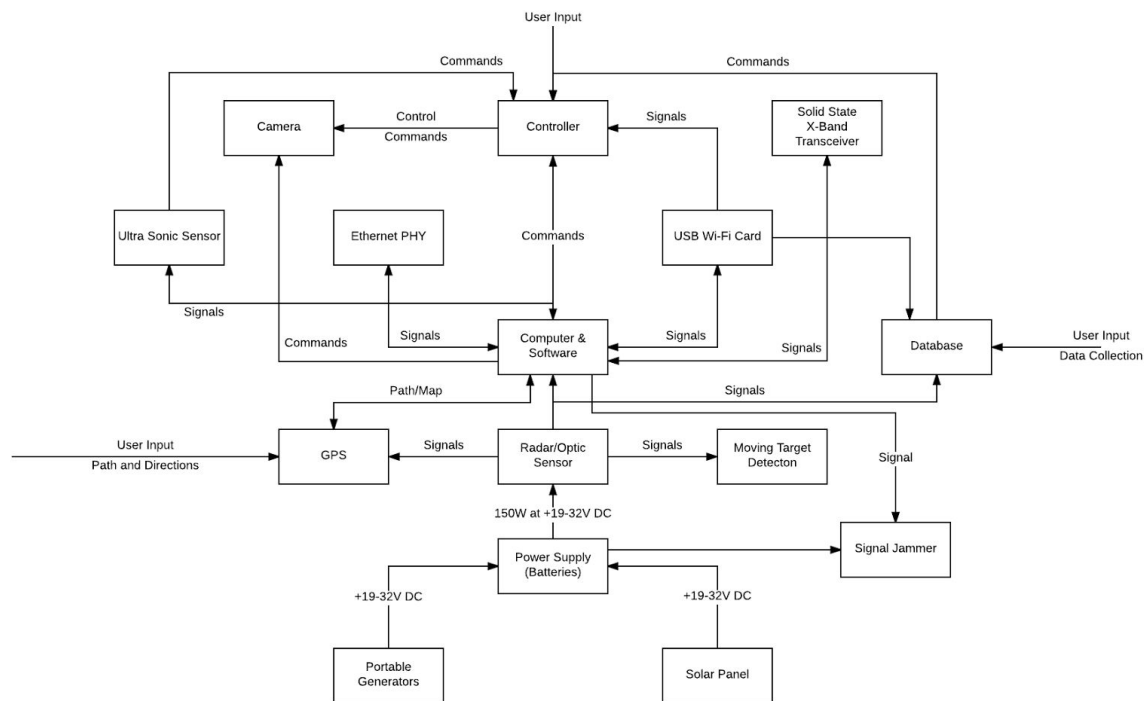


Figure 9: Block Diagram

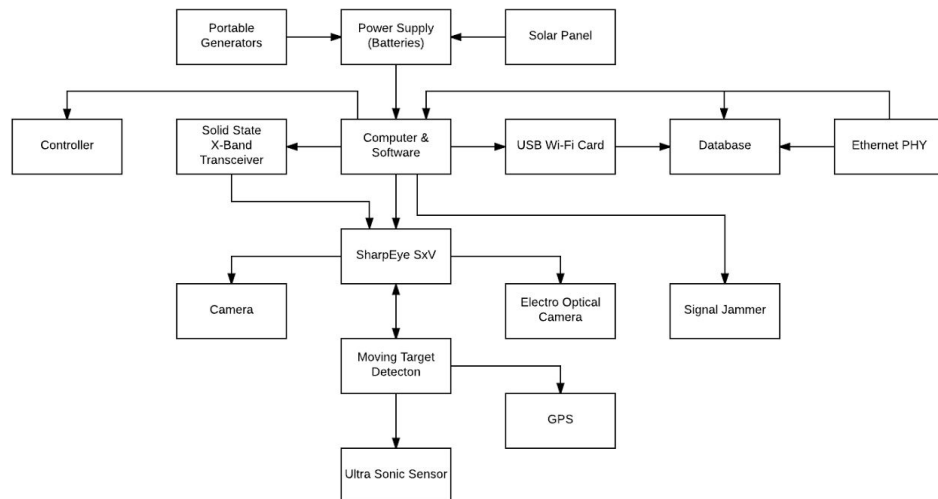


Figure 10: Hierarchical Block Diagram

Summary

DDANS therefore, possesses the capability to defend a designated perimeter from an airborne UAV or drone attack and from on-road, vehicular IED attack. For the detection of IEDs off shore or on a person (suicide bomb or vest) DDANS will require a larger system space with an increased number of sensors, computer hardware and software, actuators and processing capabilities. DDANS satisfies the stated requirements being that it is operational at night, in a densely populated area with high levels of noise, during all weather conditions, minimises collateral damage caused when intercepting and neutralising the attacking UAV and prioritizes the safety of civilians. Furthermore, the system operates over the range of Garden Island Bay keeping spectators of the public event safe and the sensors cover the optimal range of the event.

Testing

After the production of the system, physical testing of components as well as the mission itself must take place before deployment on the market. Inspection of the systems and its many steps and components must be employed to reduce the likelihood of errors. Testing also involves considering all requirements to be checked are satisfied.

It was found that the system neglects the efficiency of determining in a quick manner the difference between a drone that is a threat and one that is not. This is due to the fact every drone within the detection zone of the radar system will have to be taken to the safe zone and cross-checked with the database. However, since the detection zone is small, relative to the Sydney Harbour area, and since most of the drone recording and surveillance will be operational closer to the Harbour Bridge and Opera House, little to no drones will be detected within that small zone of Island Bay.

Most of the Harbour area is a no fly zone for civilian drones and recreational drones therefore, planned drone flights can be cleared prior to system operation. Furthermore, since it is New Year's Eve within this scenario only regulated and monitored drones will be operational which is a command that is able to be communicated to the system to ignore this target using RFIDs (Radio-Frequency Identification). All officially monitored and non-threatening drones on the night will have this form of identification to allow for close monitoring using electromagnetic fields to automatically identify and track these tags attached to the drones. The system can read these tags and using simple coding, such tagged targets can be ignored by the system and not cause an alert or hijacking. Another issue that was found when testing the system against the requirements were the fact that the hijacking can only occur using Wi-Fi and control from the source signal can only be accomplished on Wi-Fi operated drones only. Therefore, the signal jammer has been introduced in the system (as mentioned in parts above) to disallow any radio signals communicating with the drone in the case of a threat that is detected through the radar system. This allows for no chance of detonation of the bomb close to the attackers target (Mrs Macquarie's Chair) or the population densely packed at Garden Island Bay.

Conclusion

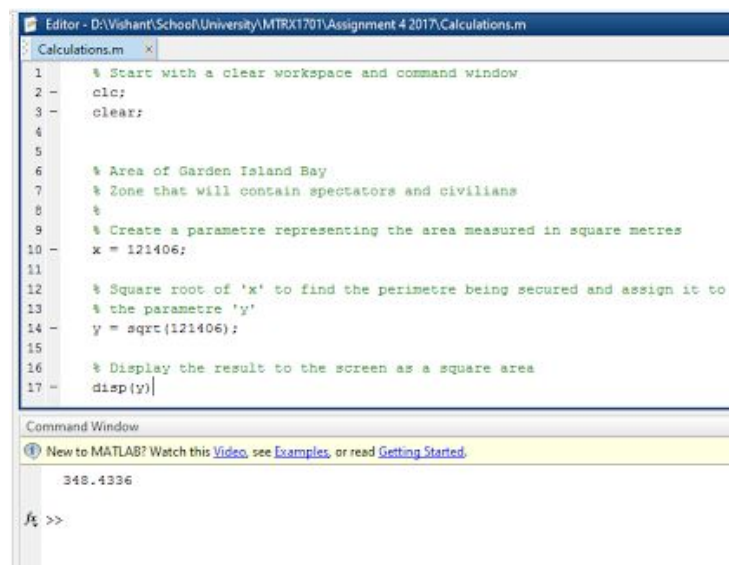
In conclusion, DDANS is a reliable method to eliminating an attack from a UAV or drone carrying a 'dirty-bomb', prioritising the safety of civilians and minimising and eliminating the collateral damage caused by neutralizing the drone. DDANS can be employed in the detection of vehicular on road IEDs and motor vehicle threats therefore, further displaying its effectiveness against terror attacks.

Recommendations

Recommendations for future advances on this project includes employing a system that can cross-check a drones identification efficiently and quickly against known database stored information of other drones and quickly label it as not a threat.

Furthermore, research can be done to identify the 'dirty-bomb' using devices that can detect radiation, biological contents and scan the contents of the bomb material. For example, a device that can detect what is the materials that is being carried with the drone. Employing more detection components and increasing the coverage range can be accomplished by employing signal boosters, transformers or antennas. Alongside introducing such components, further processing power and computer and hardware will be required. This can be accomplished by increasing the processing power and capabilities of the mainframe computer and/or adding other computer nodes in a star style computer system configuration.

Appendix



```
Editor - D:\Vishant\School\University\MTRX1701\Assignment 4 2017\Calculations.m
Calculations.m
1 % Start with a clear workspace and command window
2 clc;
3 clear;
4
5
6 % Area of Garden Island Bay
7 % Zone that will contain spectators and civilians
8 %
9 % Create a parametre representing the area measured in square metres
10 x = 121406;
11
12 % Square root of 'x' to find the perimetre being secured and assign it to
13 % the parametre 'y'
14 y = sqrt(121406);
15
16 % Display the result to the screen as a square area
17 disp(y)

Command Window
New to MATLAB? Watch this Video, see Examples, or read Getting Started.
348.4336

fx >>
```

Figure 2: Target Area and Calculations

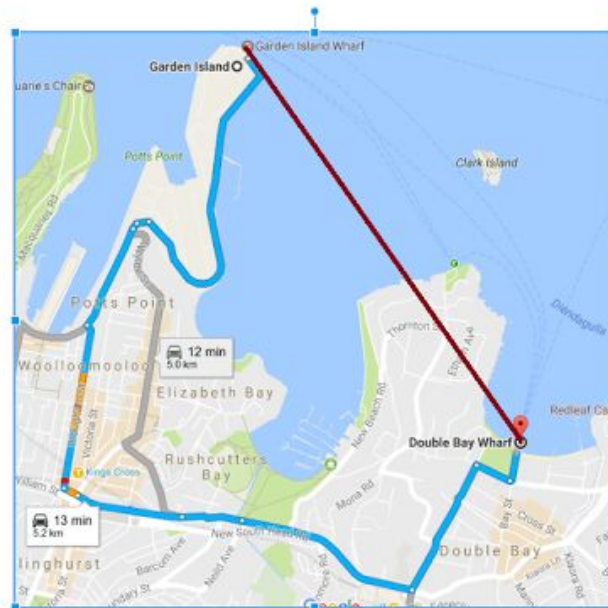


Figure 3: Path Taken by Motor Vehicles in Blue, Path Taken by the Drone Red.

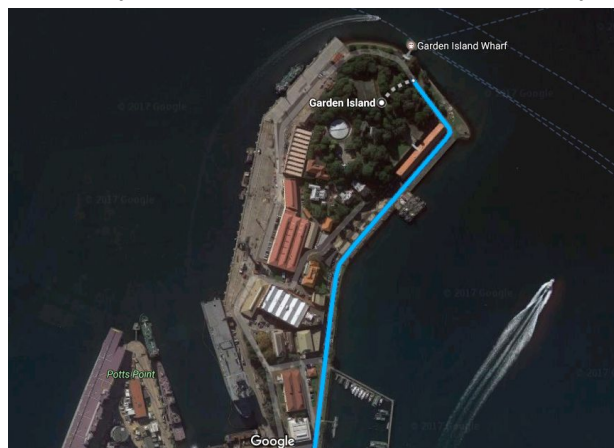


Figure 5: Garden Island

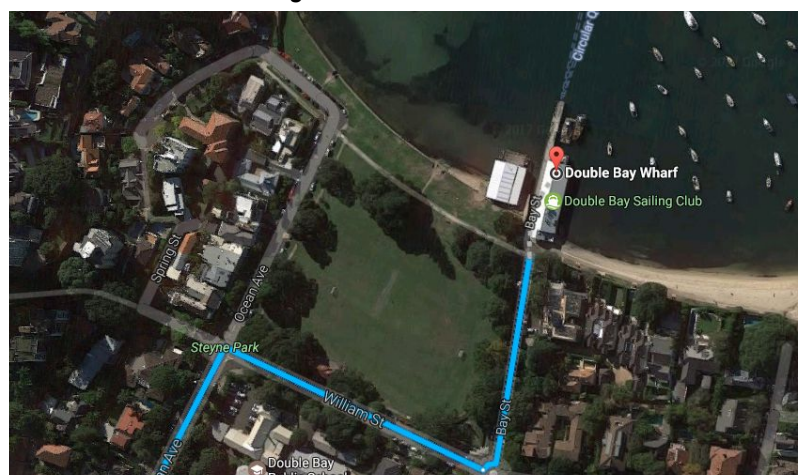


Figure 6: Secure Location: Double Bay Wharf

```
% Load training and test data using [imageDatastore].
syntheticDir = fullfile(toolboxdir('vision'),'visiondata','digits','synthetic');
handwrittenDir = fullfile(toolboxdir('vision'),'visiondata','digits','handwritten');

% [imageDatastore] recursively scans the directory tree containing the
% images. Folder names are automatically used as labels for each image.
trainingSet = imageDatastore(syntheticDir, 'IncludeSubfolders', true, 'LabelSource', 'foldernames');
testSet = imageDatastore(handwrittenDir, 'IncludeSubfolders', true, 'LabelSource', 'foldernames');
```

Figure 7: Scripts for MatLab Photo Recognition

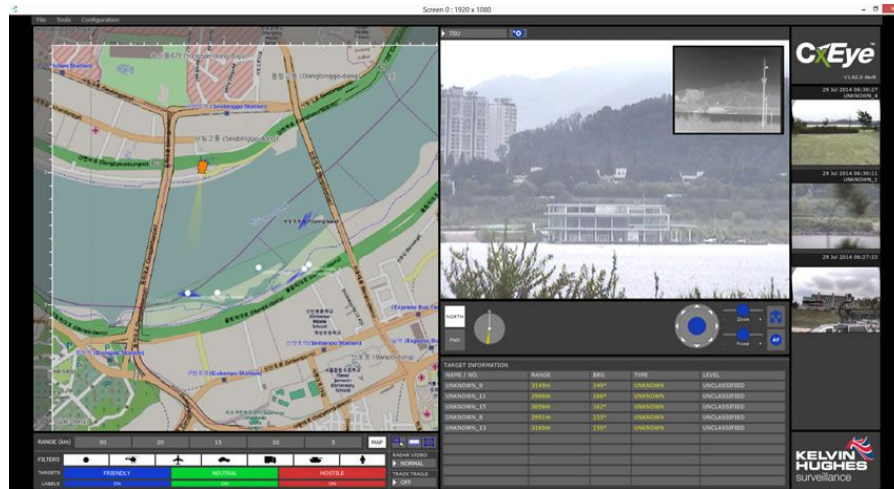


Figure 8: CX Eye Software and Mapping

Reference List

- [1] T. Meng and S. Matsunaga, "Failure-tolerant control for small agile satellites using single-gimbal control moment gyros and magnetic torquers", *Acta Mechanica Sinica*, vol. 28, no. 2, pp. 551-558, 2012.
- [2] 2017. [Online]. Available: <http://jammers4u.com/drones-jammer>.
- [3] "Radar Basics", *Radartutorial.eu*, 2017. [Online]. Available: <http://www.radartutorial.eu/07.waves/Waves%20and%20Frequency%20Ranges.en.html>.
- [4] A. Budillon and G. Schirinzi, "Performance Evaluation of a GLRT Moving Target Detector for TerraSAR-X Along-Track Interferometric Data", *IEEE Transactions on Geoscience and Remote Sensing*, vol. 53, no. 6, pp. 3350-3360, 2015.
- [5] "Electro-optical sensor payloads for small UAVs", *Militaryaerospace.com*, 2017. [Online]. Available: <http://www.militaryaerospace.com/articles/print/volume-24/issue-10/technology-focus/electro-optical-sensor-payloads-for-small-uavs.html>.
- [6] "Ultrasonic Sensors | Technical Guide | Australia | Omron IA", *Omron.com.au*, 2017. [Online]. Available: http://www.omron.com.au/service_support/technical_guide/ultrasonic_sensor/index.asp.
- [7] M. 2017, D. 2017, P. 2017, M. 2017, D. 2017 and P. 2017, "New contract wins for SharpEye™ SxV security radar", *Kelvin Hughes.com*, 2017. [Online]. Available: <https://www.kelvinhughes.com/news/203-new-contract-win-for-sharpeye-sxv-security-radar>.
- [8] "Civil Aviation Legislation Amendment (Part 101) Regulation 2016", *Legislation.gov.au*, 2017. [Online]. Available: <https://www.legislation.gov.au/Details/F2016L00400>.

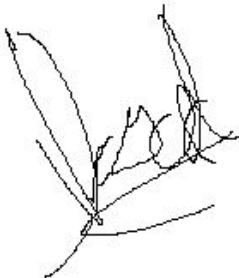
MTRX1701 Major Assignment

Detailed Statement of Contributions

Add lines as needed to present your entire table of contents.

Section	Section Title	Group Member Contribution		
		<i>Vishant Prasad</i>	<i>Yu Hz</i>	<i>Humaira Nisha</i>
1	Summary Description	50%	0%	50%
1.1	Mission Overview	50%	0%	50%
1.2	Requirements Analysis	50%	0%	50%
1.3	Functional Specifications	50%	0%	50%
1.3	Environment Specifications	60%	0%	40%
1.4	Functional Block-Diagram	100%	0%	0%
2	Component Description	20%	40%	40%
2.1	Other Mechatronic Components	0%	50%	50%
2.2	Description of Actuators	30%	70%	0%
2.3	Description of Sensor	30%	70%	0%
2.4	Control Systems Description	0%	0%	100%
2.5	Computing and Processing Elements	0%	0%	100%
2.5.1	Hardware	0%	0%	100%
2.5.2	Software	0%	0%	100%
3	Process Description	100%	0%	0%
3.1	Diagrams	100%	0%	0%
4	Summary	100%	0%	0%
4.1	Testing	100%	0%	0%
5	Recommendations	100%	0%	0%
6	Appendix	100%	0%	0%
7	References	0%	100%	0%
8	Presentation	90%	5%	5%
Overall Contributions		50%	25%	25%

Change the names in the declarations below to the true names of your group members.

<p>I, <i>Vishant Prasad</i>, declare that this table accurately reflects my contribution to this assignment.</p> <p>Sign:</p>  <p>Date: 6/9/2017</p>	<p>I, <i>Yu Hz</i>, declare that this table accurately reflects my contribution to this assignment.</p> <p>Sign:</p> <p>HONGZHAN YU</p> <p>Date: 6/9/2017</p>	<p>I, <i>Humaira Nisha</i>, declare that this table accurately reflects my contribution to this assignment.</p> <p>Sign:</p> <p>HUMAIRA RASHID</p> <p>Date: 6/9/2017</p>
---	---	--