# Conceptual Design and Planning Final

Meredith Nye, Abe Perkins, Sterling Sloan, Aaron Stewart, JieJun Stowell, Austin Williams
*Electrical and Computer Engineering Department*
*Tennessee Technological University*
Cookeville, TN
mrnye42@tntech.edu, asperkins42@tntech.edu, sbsloan42@tntech.edu,
ajstewart42@tntech.edu, jjstowell42@tntech.edu, agwilliams43@tntech.edu

## I. Introduction

Unmanned aircraft systems, colloquially referred to as drones, have been integrated into society over the course of the past decade. Paired with their integration were a slew of safety concerns, which, until recently, have had very few practical solutions. In September 2023, the Federal Aviation Administration (FAA) issued a new requirement stating that registered drones above a certain weight must emit an identification signal, dubbed "Remote ID". This signal constantly transmits information about the drone such as the serial number of the drone, the current geographical latitude and longitude of both the drone and the controller, the current altitude of both the drone and the controller, the current velocity of the drone, an emergency status, and a time stamp [1].

### A. The Formulated Problem

Given the preceding information, the team has been tasked with creating an electronic sensing system to detect drones that both enter the Tennessee Technological University (TTU) airspace and emit the Remote ID signal. Once detected, the information about the drone will be relayed to the TTU police department so they can assess the threat to campus security and take whatever action they deem necessary. The system will be constrained with regards to ethical engineering decisions, existing standards for operation, potential broader impacts, and specifications relayed to us by the team's customer and advisor. These constraints are as follows:

1) The system shall detect and track remote ID emitting drones for the contiguous Tennessee Technological University campus.
   - The contiguous university covers a total area of approximately 267 acres or 11,630,000 square feet.
2) The system shall record and store all data recovered from the Remote ID signal.
3) The system shall notify campus police in real-time upon detection of a drone in flight.
   - "Real-time" is constrained by the networking and hardware capabilities.
4) The data shall be displayed in real-time upon detection of a drone in flight.
5) The system shall allow campus police to authorize drones for permitted flights in a specified time frame.
   - This constraint was requested by the TTU police as there are certain drones that are permitted to fly on campus. The police do not want to receive an alert for a permissible drone.
6) The system shall increase the alert's urgency if a drone is detected in a private geographical region.
   - The private geographical regions will be defined by the TTU police.

## II. Ethical, Professional, and Standard Consideration

### A. Ethical

Along with the constraints placed on the system by stakeholders in this project, the team must take into account the ethical concerns of creating the drone tracking system.

One such concern that the team must address is the willingness of the campus community to be tracked to such a degree. TTU Policy 190 (Unmanned Aircraft Systems) dictates that to operate a drone on TTU property, a user must comply with any local, state, and federal policies and standards [2]. In line with this, according to Part 107 of Title 14 of the Code of Federal Regulations, one specific rule is as follows: "Do not fly a drone over people unless they are directly participating in the operation" [3]. Neither local nor Tennessee state laws offer any extra stipulations to this rule, so it is plausible to say that flying a drone on a college campus inherently breaks this rule. While legally these drones are in fact breaking a law, is it truly necessary to enforce it at all times? How would enforcement of this rule reflect back on the university? In the current digital landscape, people have a hard time believing that they are not under constant observation.

This brings us to an ethical dilemma where the team likely will leave the ultimate decision up to TTU police. In reality, they are likely not going to go out and examine each drone that shows up on the receiver. Doing so would impose a negative perception of campus culture, which is something the university would strive to avoid. The purpose of the team's system is to legitimize the idea that, if a drone is found to be in severe violation of the law, the campus police have the capabilities to take care of the problem.

### B. Standards

The drone tracking system will emit and receive signals in ranges between 2 and 5 GHz. This will require us to adhere

to FCC Policy 47 CFR § 15, limiting the power and exposure levels to safe levels [4]. For receiving data from drones, the team will be utilizing the elements required to be transmitted by Remote ID drones as stated in FAA Policy 14 CFR § 89.305 and 14 CFR § 89.315 [5].

With regards to data transmission and storage, the team will build the team's network architecture to uphold the transmission standards of IEEE 802.11 and the protection standards of TTU Policies 403 and 856. The IEEE standard is the basis for all Wi-Fi communications worldwide, and specifies which bands of frequency are able to be used for which purpose. TTU policies 403 and 856 defines standards for surveillance camera usage on campus and data protections standards respectively [6–8].

### C. Broader Impacts

A drone tracking system for campus police will have both positive and negative impacts for the people involved. It is important for us to consider what effects the team's system will have on the people using it and the people that will be subject to its use.

Tech police will be positively impacted by the use of this system because they will be able to help keep the TTU campus safer. Being able to identify the control station's location will allow them to stop the pilot from endangering bystanders and help suppress unsafe drone practices. Bystanders can rest easy knowing that campus police will have a quicker more efficient means of stopping the drone before it can recklessly harm them or others. Students and staff will also have a stronger level of protection if people are attempting to spy on them. The drone's user will be much easier to locate if they were using their drone to record into a student's dorm room window for example. This will improve privacy of Tech.

However, there are negative impacts that need to be considered as well. Tech could be viewed as overstepping their boundaries as an authority figure. To outsiders looking in or the drone pilots, a figure of power doing more to regulate and gather information about people may be too much. The main concern of negative impacts is the perception of the system. There may be a perception issue that TTU may be too controlling on the front of their campus. The university would also accumulate data on people that aren't students, and this could be seen as an invasion of privacy for many. This also creates a constraint on the project because if the radius is beyond campus then it will pick up signals of people who aren't on campus. This would hurt TTU's perception because people will question why a university is collecting data upon them when they're not on school property and have no connection to the university. The system being used on a public state university could be cause for concern across the state as the question would arise when state wide drone tracking may be employed.

## III. Block Diagram

The full block diagram is shown in Fig.1 near the end of the document. The detailed explanations of the subsystems are as follows.

### A. Power

The power system will be split into two parts. One will power the receiver system, while the other will power the camera system. Since the two systems will likely be installed at different locations and have different power requirements, they will need to be powered separately.

1) Receiver Power: The power for the receiver system will most likely have access to an outlet, so the AC voltage will need to be transformed and converted to the required voltage for the receiver system.
   a) Transformer:
      - Input- 120 V 60 Hz
      - Output- Transformed power at 60 Hz
   b) DC Conversion:
      - Input- Transformed power at 60 Hz
      - Output- Desired power for the Receiver

      Voltage regulator or buck converter circuits may also be required to meet the receiver's power requirements.

2) Camera Power: The power for the camera system may not be able to rely on power to be transformed from a wall outlet, so the team will need to use a power source, battery, and voltage regulation to obtain the required power for the camera and motors.
   a) Power Source: A power source will be needed to reduce the requirement for maintenance on the system. Since the camera system will likely need to be located outdoors, the usage of solar energy is a convenient solution.
      - Input- Solar energy
      - Output- DC Power to charge battery
   b) Battery:
      - Input-DC Power from solar panel
      - Output- DC Power
   c) Voltage Regulator: The team would also need a voltage regulator circuit such as a buck converter to meet the camera and motor power requirements.
      - Input- DC Power
      - Output- Required DC power for the camera

The power systems will comply with NEC 310.15 and IEC 60364-1 standards detailed in the project proposal.

### B. Receiver

The Receiver system will be responsible for receiving and unpacking Remote ID (RID) data to be sent by the network to the database.

1) Antenna and SDR
   - Input- RID signals at 2.5 GHz and 5 GHz range
   - Output- RID digital signal
2) Microprocessor

- Input- RID digital signal
- Output- Packaged RID Data

3) Storage Drive
   - Input- Packaged RID Data
   - Output- Packaged RID Data

The receiver will only be picking up RID signals from the frequency bands of 2.5 GHZ and 5 GHz. The receiver will also need to be limited to its range so that it does not encroach upon people or areas that are off campus.

### C. Database

The Database system will receive the packaged data from the receiver, camera, and user input. Then, the system will unpack the data, store the information in the database, and feed the necessary information to the camera and website.

1) Data Processing
   - Input- Packaged data from camera and Receiver.
   - Output- ID, Location/Altitude, Velocity, Control station location/Elevation, Time Mark, Emergency status, Images.
2) Drone Authorization
   - Input- User Input.
   - Output- Drone Location/Altitude, Control station Location/elevation.
3) Database Access
   - Input- User Input.
   - Output- ID, Location/Altitude, Velocity, Control station location/Elevation, Time Mark, Emergency status, Images.

The constraints for this subsystem is the amount of data it can hold, depending on how frequently drone is detected, old data might not be accessible after certain time period.

### D. Camera

This subsystem will be responsible for tracking and capturing both the drone mid-flight and, in optimal cases, the drone pilot when they are within camera range. This is important for documentation purposes, and will greatly assist campus police in the event of a repeat offender. The hardware will pertain to the motor-camera assembly, while software will pertain to the micro-controller and code to drive the system.

1) Hardware
   - Input- Power, Motor and Camera control signals
   - Output- Camera Shutter and Motor Control Signal(s)
2) Software
   - Input- Position, altitude, and velocity of drone and pilot.
   - Output- Clean image/video of drone and/or pilot.

Constraints applicable to this sub-system are in relation to TTU Policy 403, along with ethical considerations of monitoring a non-campus affiliated person(s). Policy 403 defines intent of camera usage and limits to storage of camera data while on-campus. Ethical considerations involve limiting or eliminating the recording of off-campus individuals not directly involved in the capture of unauthorized drone transit on-campus.

### E. Website

The website subsystem will take in data from the database along with input from the user connected to determine what output will be returned to the user. It will allow the user to view the flight path of the drone across campus and, if captured, images of the drone in flight and/or the drone user.

- Input- Raw data from database and user-selected inputs
- Output- Organized data presented in a concise, usable manner.

This system is constrained by the requirement that the team's system as a whole should work in "real-time." While this length of time has no true definition, the team's project limits this value to less than one second.

## IV. Timeline

The timeline is shown as a Gantt chart in Fig.2 below. It follows the outline of the block diagram, showing the previously not included camera subsystem and timeline of system's design to highlight how the subsystems interact with each other as well as adjusted dates to reflect the block diagram.

## V. Conclusion

The conceptual design of the team's Drone Tracking System contains five central systems, with six total subsystems. The subsystems include the power system, the sensing and decoding system, the network, the camera-tracking system containing both hardware and software designs, and the website. This document will serve as an outline for the team's design moving forward, but does not list specifics required for a working system.

## References


[1] "Remote identification of drones," Federal Aviation Administration, Available: https://www.faa.gov/uas/getting_started/remote_id [Accessed Feb. 15, 2024].

[2] "190 unmanned aircraft," Tennessee Technological University, Available: https://tntech.navexone.com/content/dotNet/documents/ [Accessed Mar. 7, 2024].

[3] "Part 107- unmanned aircraft systems," Title 14- Aeronautics and Space, Code of Federal Regulations, Availiable: https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107 [Accessed Feb. 15, 2024].

[4] "Part 15- radio frequency devices," Title 47- Telecommunication, Code of Federal Regulations, Available: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15 [Accessed Feb. 19, 2024].

[5] "Part 89- minimum message elements broadcast by standard remote identification unmanned aircraft," Title 14- Aeronautics and Space, Code of Federal Regulations, Available: https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-89/subpart-D/section-89.305 [Accessed Feb. 15, 2024].

[6] "Ieee 802.11-2020: Collision avoidance in wireless networks," American National Standards Institute, Available: https://blog.ansi.org/ieee-802-11-collision-avoidance-wireless-networks/ [Accessed Feb. 19, 2024].

[7] "403 safety and security camera acceptable use," Tennessee Technological University, Available: https://tntech.navexone.com/content/dotNet/documents/ [Accessed Feb. 19, 2024].

[8] "856 data security and handling policy," Tennessee Technological University, Available: https://tntech.navexone.com/content/dotNet/documents/ [Accessed Feb. 19, 2024].

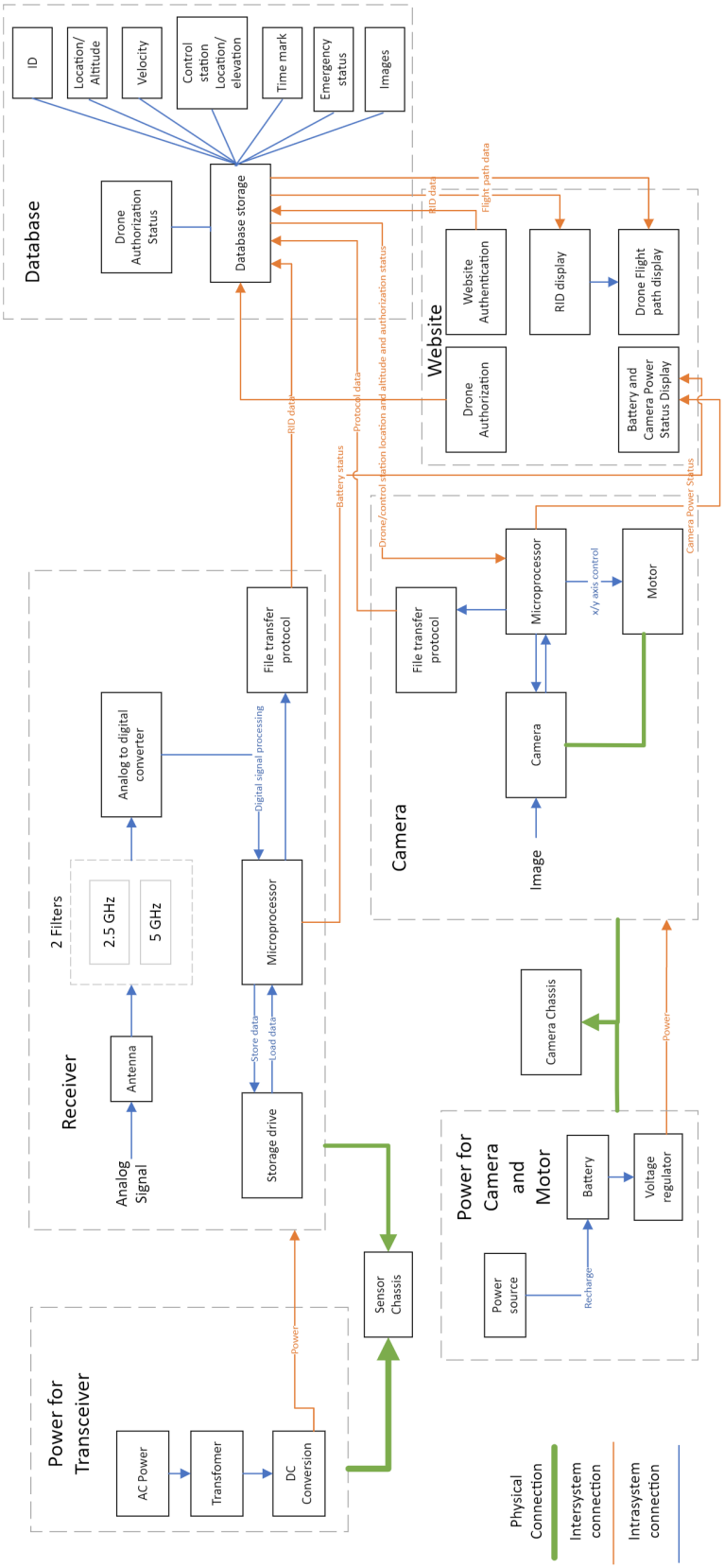


Fig. 1. Block Diagram

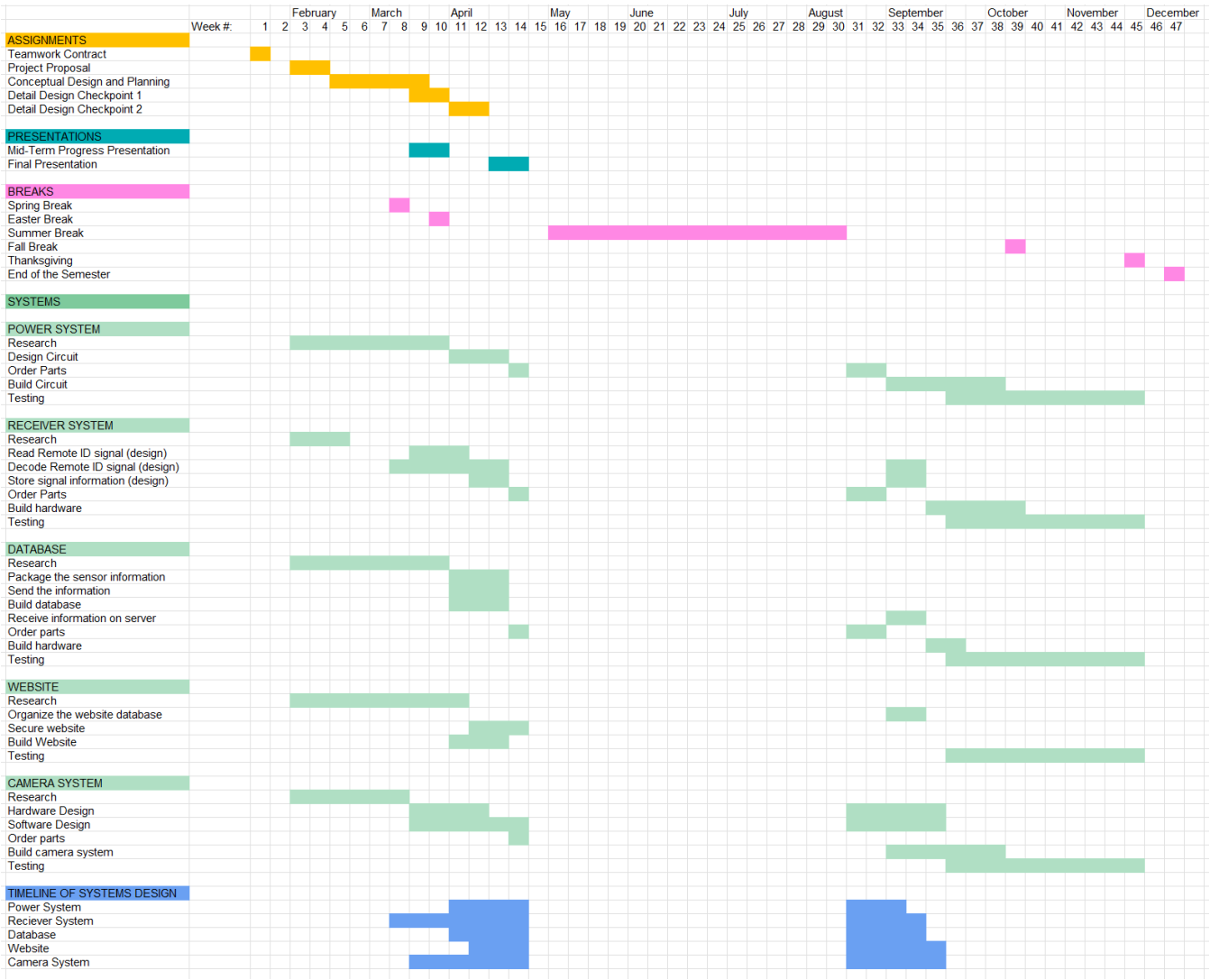


Fig. 2. Gantt Chart