TED UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

CMPE 491- Senior Project I

ATLAS (Autonomous Threat Localization and Avoidance System)

Project Specifications Report

14.11.2025

Team Members:

Ege Hiçdönmez - 37135702660

Selen Erdem - 24334689144

Zeynep Selçuk - 11203309784

Can Gündoğdu - 46954601016

1. Introduction

In this project, an autonomous surveillance system ATLAS (Autonomous Threat Localization and Avoidance System) is developed to enhance border operations. Continuous monitoring of the border regions that are hard to reach by human force is intended to be reached by UAVs. The system is planned to reduce the need for human patrols in risky environments and weather conditions.

Through coordinated swarm behavior, coverage of large areas along the border would be provided and potential threats would be detected, classified and reported to the command center simultaneously. Communication among the drones and with the command unit is planned to increase the rate of adaptive responses.

This system is intended to offer a new approach to blind spot and border monitoring methods.

1.1 Description

ATLAS is designed as a multi-UAV surveillance and threat detection system. Each drone will scan the area from different angles to create a complete image and share the data with the command center continuously. When a threat is detected, system will alert the command center.

The swarm behavior of the drones would allow the system to monitor larger areas, adapt to the changing conditions and continue with the mission in various scenarios.

Scope of the project includes:

- Autonomous swarm patrol missions in blind spots and border area
- Threat detection using real time data
- Localization and reporting of suspicious activities
- Continuous communication between drones to provide swarm coordination
- Avoidance algorithm to prevent UAVs from collisions
- Adaptability to weather conditions and environmental changes
- Real time command center communication

1.2 Constraints

1.2.1 Communication Range Constraints

All UAV-to-UAV and UAV-to-command-center communication is limited by the maximum signal transmission range. Loss of signal in mountainous or forested terrain may affect swarm coordination.

1.2.2 Computational Resource Limitations

On-board processors have limited computing power. Real-time threat detection and image processing must be optimized to run under strict memory and CPU constraints.

1.2.3 Weather Condition Limitations

UAV operation is restricted by heavy rain, strong wind, fog, and extreme temperatures. The system must remain functional within a limited set of environmental conditions defined by the drone hardware specifications.

1.2.4 Regulatory and Airspace Constraints

The UAVs must comply with national aviation regulations. Flight altitude, no-fly zones, and required permissions limit where and how the system can operate.

1.2.5 Payload Constraints

Each drone has limited payload capacity, which restricts the weight of sensors, communication modules, and computing units it can carry.

1.2.6 Sensor Accuracy Constraints

The accuracy of onboard sensors (thermal cameras, LiDAR, night-vision modules) is limited by hardware specifications. Low-light conditions, fog, or long distances reduce detection precision.

1.2.7 Processing Delay Constraints

Real-time threat classification must be performed within milliseconds, but hardware and algorithm limitations may introduce delays that affect response time.

1.2.8 Bandwidth Constraints

High-resolution video streaming from multiple UAVs simultaneously can exceed available bandwidth, causing data loss or reduced frame rates.

1.2.9 Energy Consumption Constraints

Activating high-power sensors or maintaining constant communication increases power usage, reducing overall mission time.

1.2.10 Terrain Restrictions

Rugged terrain, tall vegetation, and narrow valleys can disrupt GPS signals and reduce the drones’ ability to maintain autonomous formation.

1.2.12 Safety Constraints

The system must avoid flying over populated civilian areas to reduce the risk of accidents or unauthorized monitoring.

1.3 Professional and Ethical Issues

All team members must follow the professional engineering standards and safety protocols in all aspects of the project design and implementation. According to the ACM Code of Ethics and Professional Conduct and the IEEE Code of Ethics, aside from the general ethical rules, the project has to follow the other professional obligations too.

1.3.1 Professional Responsibilities

- Team members must ensure that, within the simulation, all algorithms and communication models are tested transparently and validated objectively.
- Honesty and clarity must be maintained for the results and limitations.
- Ensuring the system sticks to best practices in security-critical software and safety.
- The project must be done with proper documentation, acknowledgment and collaboration.

1.3.2 Ethical Responsibilities

- **Privacy and data protection:** The system must not gather, store, or process personal data without any legal basis. The system must protect and respect data according to necessity.

- **Human oversight:** The system must not follow full autonomy in decision-making. Human operators have the authority over all system decisions and actions to prevent unintended autonomy-based harm.
- **Fairness and non-discrimination:** The system‘s design and algorithms must not be biased against any group or region. All authorization and decision-making processes should be followed objectively.
- **Safety and transparency:** Any type of real-world implementation must conform to international aviation safety and data governance standards. Explainability and traceability will be considered during the project.

1.3.3 Academic and Research Ethics

All team members must commit to academic honesty with proper citations and references for the intellectual and open-source properties, in accordance with their licenses. All references will be acknowledged.

2. Requirements

This section defines the functional and non-functional requirements of ATLAS system. Requirements are derived from the project objectives, technical context and operational constraints which are mentioned in project proposal. These requirements specify exactly what the system must accomplish and performance characteristics it must maintain to ensure reliable and efficient operation.

2.1 Functional Requirements

FR-1. Autonomous Patrol Operation

The system shall simulate multiple UAV deputy capable of autonomously patrol assigned virtual regions. Each agent shall follow predefined or dynamically assigned waypoints within the simulation environment.

FR-2. Simulated Real-Time Threat Detection

Each virtual UAV shall process simulated camera inputs to detect threats represented among the simulation environments. Detection shall occur in real time.

FR-3. Virtual Threat Localization

The system shall determine object's location with the simulation coordinate system once it detects a simulated threat.. The output shall record the threat's coordinates in simulation world units (x, y, z e.g.).

FR-4. Swarm Coordination Through Software Messaging

UAV agents shall exchange status information through an internal communication layer (for example: message bus, mutual network). Shared data shall support mutual awareness of agents, consistent patrol coverage, and collision-free movement within the simulation.

FR-5. Communication with Ground Control Interface

The system shall transmit all relevant state information, UAV positions, detections, drone statuses, to a command center interface. This interface may be a dashboard, GUI, or terminal-based monitoring system.

FR-6. Collision Avoidance in Simulation

Each UAV agent shall implement collision-avoidance behavior using simulated camera data. UAV agent must change its path to prevent collisions with other UAVs or other defined, detected environmental obstacles.

FR-7. Dynamic Mission Reconfiguration

The simulation control interface shall allow operators to modify mission parameters in runtime without in need of a simulation restart. Dynamic mission changes include patrol areas, flight paths, altitude levels, or detection manners.

FR-8. Virtual Emergency Procedures

The system shall simulate emergency conditions such as connection loss, or camera failure. Each UAV agent must behave according to user predefined emergency behaviors these behaviors shall include pause, return to a base coordinate, simulated landing, or stop.

FR-9. Data Logging and Simulation Recordkeeping

The simulation shall record event logs, UAV pathways, detection timestamps, communication messages, and emergency sparks.

2.2 Non-Functional Requirements

NFR-1. Responsive Simulation Update Cycle

The system shall process UAV situation updates, threat-detection logic, and communication events within each simulation routine without causing delays that prevent UAVs from completing their movement or detection tasks on time.

NFR-2. Timely Detection Processing

Threat-detection algorithms shall complete execution within the same simulation routine in which they are triggered, ensuring that detection results are available before the upcoming movement update.

NFR-3. Prompt Message Delivery

Swarm coordination shall prevent from delaying behind UAV movement updates, messages issued between UAVs, or between UAVs and the command center must be sent through the simulation routine in which they are sent.

NFR-4. Guaranteed Separation Enforcement

The collision-avoidance logic shall prevent UAVs from intrigue each other or intersecting paths within any simulation routine. UAV positions must always remain distinct.

NFR-5. Modular Component Structure

Movement control, detection, communication and visualization components must be implemented as separate modules to ensure that modules shall be changed or replaced without affecting each other.

3. References

[1] Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics

[2] IEEE Computer Society. (2014). *Software Engineering Code of Ethics and Professional Practice*. https://www.computer.org/education/code-of-ethics

[3] Institute of Electrical and Electronics Engineers. (2018). *IEEE Code of Ethics*. https://www.ieee.org/about/corporate/governance/ieee-code-of-ethics.html

[4] Tavani, H. (2021). *Computer and Information Ethics*. In **Stanford Encyclopedia of Philosophy**.

https://plato.stanford.edu/entries/ethics-computer/