Proceedings of the Annual General Donald R. Keith Memorial Conference
West Point, New York, USA
April 23, 2026
A Regional Conference of the Society for Industrial and Systems Engineering

Drone-Augmented Ground Sensors: A Model-Based Systems Engineering Approach to Area Denial

Benedetto Fusco, Ashley Hubert, Dan Velarde, Kathryn Wegler, Justus Whitaker, and Vikram Mittal

Department of Systems Engineering, United States Military Academy, West Point, New York 10996

Corresponding author's Email: Vikram.mittal@westpoint.edu

Author Note: The views expressed herein are those of the authors and do not reflect the position of the United States Military Academy, the Department of the Army, or the Department of War.

Abstract: Conventional minefields, while historically effective, present significant operational, humanitarian, and legal challenges due to their cost, rigidity, and indiscriminate nature. Modern military operations require area-denial solutions that are precise, adaptive, and ethically compliant, minimizing risk to civilians while maintaining tactical effectiveness. This research presents a Model-Based Systems Engineering (MBSE) approach to designing a non-lethal, sensor-augmented area denial system capable of detecting, classifying, and reporting adversary movements without the use of explosives. The design process includes a comprehensive stakeholder analysis, which defines system requirements and guides architectural decisions. A formal Analysis of Alternatives also evaluates multiple concepts against criteria such as effectiveness, scalability, cost, reusability, and disposability. The resulting design integrates a network of low-power, distributed ground sensors with autonomous drone overwatch to enable persistent monitoring, positive identification, and human-in-the-loop. The developed prototype includes a sensor node, an integrated drone, and a drone hub.

Keywords: military system design, MBSE, advanced sensing, autonomous drones

1. Introduction

Modern battlefields demand precision, adaptability, and ethical accountability. Traditional area-denial systems, which are centered on landmines, can be effective; however, they are costly, rigid in deployment, and inherently indiscriminate. To remain both effective and responsible in future conflicts, militaries must transition from static explosive obstacles to adaptive, intelligent systems capable of denying terrain without causing unintended harm. Recent advances in low-power electronics, multi-modal sensing, and autonomous systems enable a reimagining of area denial through a systems-based approach that provides persistent monitoring without explosive hazards by integrating distributed ground sensors with aerial overwatch platforms. These systems can detect and classify intrusions in real time, coordinate with precision fires when necessary, and safely deactivate after mission completion, maintaining tactical effectiveness while supporting compliance with international humanitarian law.

This project seeks to design a safe, sensor-based area denial system that uses distributed multi-modal sensors to track adversary movement and integrates drone overwatch for verification and targeting support. It leverages a model-based systems engineering (MBSE) approach to ensure traceability from stakeholder needs through conceptual design and prototyping. A comprehensive stakeholder analysis, incorporating operational, technical, and humanitarian perspectives, guides the development of system requirements and the logical architecture. An Analysis of Alternatives (AoA) evaluates multiple configurations against these criteria, resulting in the selection of a hybrid ground sensor and drone overwatch concept. This paper presents the system development methodology, stakeholder analysis, conceptual design, and prototype development.

2. Background

2.1 Area Denial in Modern Land Warfare

Shaping terrain through area denial is a fundamental aspect of modern land warfare. By controlling how and where an adversary can maneuver, commanders protect key assets, channel enemy forces into engagement zones, and create conditions for decisive fires. At its core, area denial seeks to “divert, disrupt, delay, or damage” the enemy to create advantages in maneuver and time (Joint Chiefs of Staff, 2016).

Minefields remain the most widely recognized and historically prevalent form of area denial. However, a minefield is not effective on its own. As shown in Figure 1, obstacle belts are integrated with overwatch positions that provide observation and fire control over the denied area (U.S. Department of the Army, 2004). From these positions, soldiers monitor the obstacle, detect breaching attempts, and coordinate indirect fires. When an enemy force begins clearing operations, artillery, mortars, or air-delivered fires can target the slowed and exposed element. This integration transforms the obstacle from a passive barrier into an active defensive system that concentrates combat power at the point of enemy vulnerability.

Breaching such obstacles is deliberate and hazardous. Attacking forces must locate the minefield, mark its boundaries, and commit engineers to clear lanes under fire. The defender's objective is to disrupt this breach, destroy key assets, and break the attacker's momentum while forces are confined to narrow, predictable paths.

Recent conflicts illustrate the broad impact of mine-based area denial. The Korean Demilitarized Zone remains heavily shaped by minefields that have helped deter large-scale incursions for decades (Feng, 2024). In the ongoing Russia–Ukraine conflict, extensive mine emplacement has slowed maneuver, complicated counter-offensives, and restricted civilian access to infrastructure and farmland (Human Rights Watch, 2023). Across these cases, landmines continue to shape operational tempo and restrict movement, demonstrating their persistent role in land warfare. While the U.S. military's recent focus has been on counterterrorism, the rise of near-peer competitors is driving a renewed need to conduct large-scale, force-on-force operations, where effective area denial remains critical.

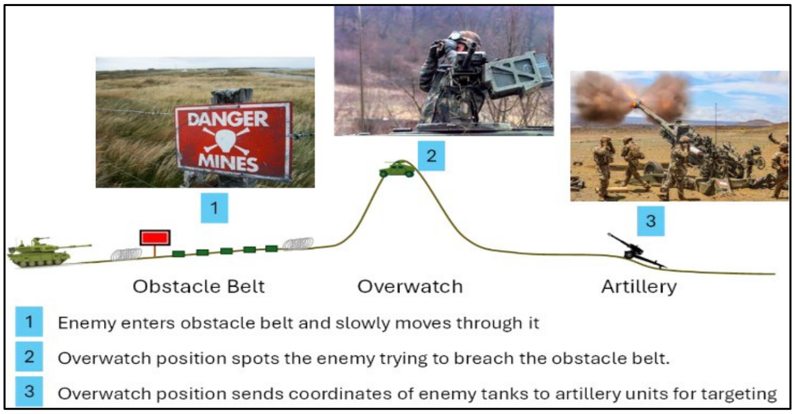

Figure 1: Schematic of the current area denial process.

2.2. Issues With Current Systems

Despite their effectiveness, mine-based systems pose significant operational and humanitarian challenges. Mines can be emplaced manually or deployed rapidly using scatterable delivery systems (SCATMINES), but they do not produce decisive effects on their own. Instead, indirect fires generate most casualties, while the minefield fixes and exposes the enemy. This reliance on overwatch creates vulnerability, as fire control positions are susceptible to artillery and, increasingly, drone strikes. While artillery has long been a threat, the rapid evolution of drones has made these positions even more exposed. Modern battlefields demand faster tempos and greater adaptability than static minefields can provide.

Additionally, repurposing or removing minefields presents long-term risks. Scatterable mines often include self-destruct mechanisms that limit their active duration to several hours or days, but dud munitions remain a concern and the shortened duration reduces operational flexibility. Conventional mines without self-destruct features pose even greater disposal challenges. The humanitarian consequences are substantial. In 2023, at least 5,757 casualties from landmines and explosive remnants of war were recorded across 55 countries, with civilians accounting for 84 percent of known casualties and children representing 37 percent of civilian casualties (Monitoring and Research Committee, 2024). These figures underscore the persistent risks of traditional area denial systems and highlight the need for more adaptive and discriminate alternatives.

The Remotely Monitored Battlefield Sensor System-II (REMBASS-II) is a piece of existing technology which addresses a few of these concerns. It is a sensor-based system, using three sensor transducers and a sophisticated signal processing to achieve a high probability of detection with very low false alarm rates (L3Harris). This eliminates much of the need for overwatch positions. It also offers an idea to minimize the humanitarian consequences of minefields by providing an avenue to area denial without using explosives. However, the REMASS-II remains limited in adaptability and integration, lacking the ability to dynamically coordinate sensing, identification, and response across a distributed system. As such, it does not fully address the need for responsive, scalable, and tightly integrated area denial capabilities on modern battlefields.

3. Methodology

This project applies an MBSE approach to guide the development of a safe, sensor-based alternative that improves tactical effectiveness while eliminating humanitarian risk. The proposed solution is referred to as the Future Area Denial System. MBSE is the formal application of modeling to support system requirements, design analysis, verification, and validation beginning in the conceptual phase and continuing throughout the system life cycle. In MBSE, the primary systems engineering artifact is an integrated, coherent system model rather than a disconnected set of documents and diagrams (Delligatti, 2014). This approach provides the structure needed to capture stakeholder requirements, define architectures, and evaluate design trade-offs throughout development.

Figure 2 presents the methodology used in this study. The foundation of the analysis is a system model that includes requirements analysis, logical architecture, and physical architecture. These models were developed in Magic Systems of Systems Architect using Systems Modeling Language (SysML). The study began with a comprehensive stakeholder analysis to identify the operational, tactical, and humanitarian needs that shaped system requirements. Three primary groups contributed: combat engineers as operational users, forward area operators as mission commanders, and humanitarian organizations as compliance stakeholders. Their priorities were gathered through interviews and reviews of representative operational scenarios and used to derive operational requirements and guide requirement development and ensure alignment with mission objectives and ethical standards. Stakeholders' needs informed the model through operational requirements describing what the system must accomplish in context. The requirements analysis produced performance metrics and identified high-level functions necessary to meet stakeholder needs. These functions are represented in the system's logical architecture.

The functional framework was then used to generate alternative solutions for a future area denial system. Metrics derived from the requirements analysis were applied to evaluate each alternative using a quantitative value model approach (Sage and Rouse, 2009). The Analysis of Alternatives (AoA) scored each option on a scale from 0 to 100. It evaluated alternatives as the sum of how the specific system was projected to do in terms of each requirement. The highest-scoring solution was selected. These results informed further development of the logical architecture, which defines the behaviors and interactions required to perform each system function. This logical architecture was refined into a physical architecture that specifies the hardware and software components needed to realize those functions. The physical architecture generated technical requirements that were traced back to the original requirements to ensure end-to-end traceability.

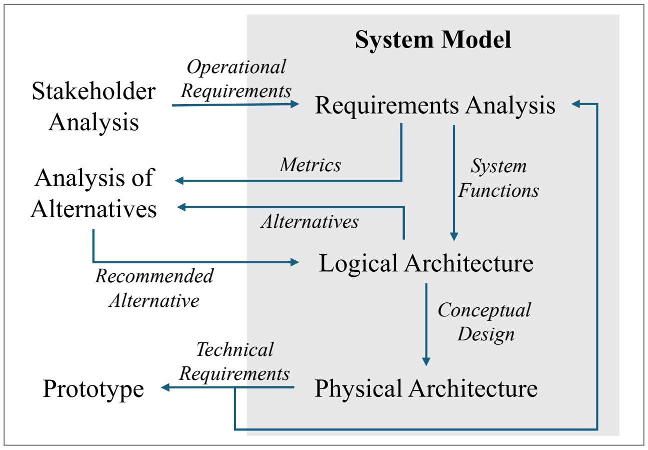

Figure 2: MBSE-based methodology used for designing a future area denial system.

4. Logical Architecture

Four alternatives were evaluated for this system, using SCATMINES as a baseline and three sensor-based concepts derived from stakeholder requirements. While SCATMINES provide area coverage and engagement, they lack discrimination, safe escalation, and long-term safety. The three alternatives address these gaps through different approaches: aerial sensing with drone-based engagement, ground sensors that cue indirect fire, and a hybrid system combining ground detection with aerial verification. All four were assessed against 13 parameters, including accuracy, range, and disposability. The Analysis of Alternatives selected the hybrid system as the preferred solution. Full details of the analysis are provided in (Fusco et al., 2026).

The selected system operates as a continuous, multi-phase autonomous process designed to detect, analyze, and relay environmental data to support rapid situational awareness. As shown in Figure 3, the operational cycle begins with the detection phase. Distributed ground sensor pucks monitor designated areas using onboard motion sensors and ranging systems. When a sensor detects an anomaly, it transitions from standby to alert, records its GPS coordinates, and transmits detection data to the command node via radio (interface R1).

In the tasking phase, the command node receives the alert, processes the coordinates, and assigns the event to an available drone through interface R2. The node enters an alert state and activates the selected drone by transmitting the target GPS coordinates (interface T2).

The observation phase begins as the drone autonomously navigates to the reported location using GPS waypoint guidance. In flight, it activates its onboard camera and applies AI-based visual detection to identify, classify, and track targets in real time. The drone streams live video and associated metadata, including GPS location, object classification, and movement data, to Forward Area operators through its video transmitter (interface T1). The command node remains in a monitoring state, relaying the feed to enable human-in-the-loop verification.

During the data relay phase, operators assess live conditions, confirm detections, and provide targeting guidance or redirect the drone for additional coverage. The system maintains this posture until the operator confirms mission completion or determines that the alert was a false alarm.

In the recovery phase, the drone autonomously returns to its hub for data offload, battery recharge, and network reintegration. The system then resets to standby for the next detection event, while sensor pucks continue continuous monitoring. This closed-loop architecture enables persistent area monitoring while preserving human control in the targeting decision process, supporting both operational effectiveness and ethical compliance requirements.

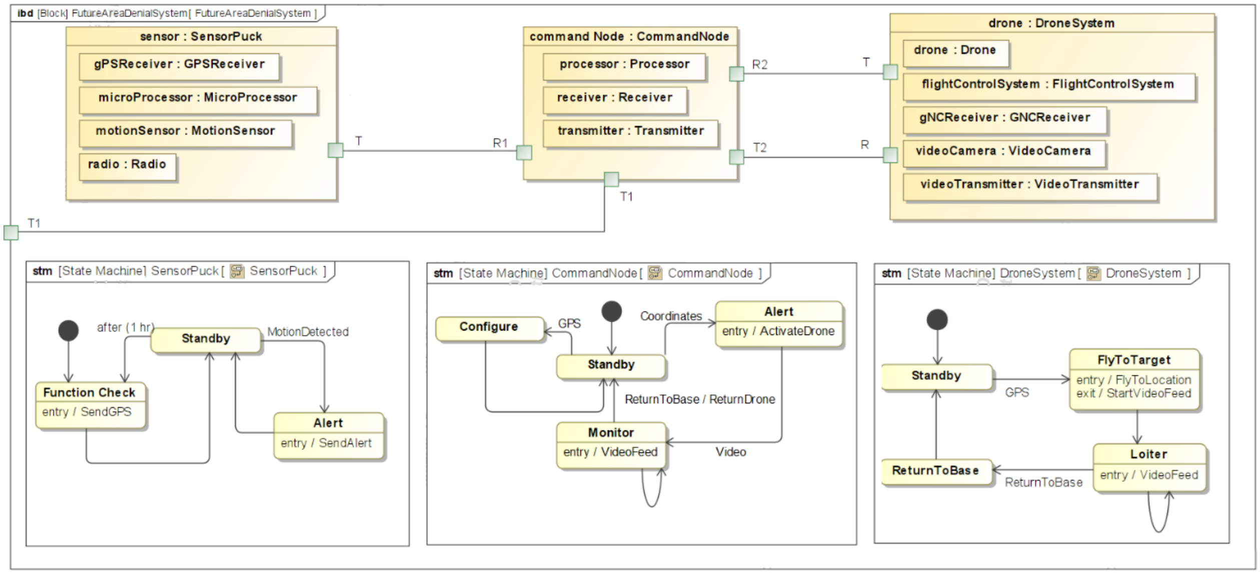

Figure 3: Logical Conceptual Design.

5. Physical Architecture

The physical architecture defines the hardware and software components required to implement the logical operational flow. As shown in Figure 4, the system comprises three primary subsystems: sensor puck, command node, and drone. This modular architecture enables independent subsystem development and testing while supporting scalability through the addition of sensor pucks or drone units without redesigning core components.

The Sensor Puck Subsystem is a self-contained detection unit built around an ESP32 microcontroller that manages local processing and state control. The puck integrates a 24 GHz mmWave radar for movement and presence detection, an inertial measurement unit for orientation data, and a GPS module for precise geolocation. Upon radar detection, the system fuses radar, Internal Measurement Unit (IMU), and GPS data to compute the target's geographic coordinates rather than simply flagging a presence event. A multi-sample confirmation threshold filters false positives before a detection is declared. The puck then packages the event as a JavaScript Objective Notation (JSON) message and transmits it via ESP-NOW, a peer-to-peer radio protocol requiring no Wi-Fi infrastructure, making the system viable in remote or contested environments. Multiple pucks operate as a mesh network and report to a gateway node that bridges the sensor layer to the command node over serial communication. The puck operates on battery power with low-power standby modes to maximize deployment duration.

The Command Node Subsystem consists of a central processor, implemented on a Raspberry Pi, which manages detection prioritization, waypoint generation, drone tasking, and event logging. It ingests alerts from the sensor puck network via the gateway node and translates GPS coordinates into drone waypoints. The command node also includes the system radio transceiver, implemented using a FireBeetle ESP32, which manages communications with the sensor network. Although these components are logically part of the command node subsystem, the Raspberry Pi controller and ESP32 transceiver are physically mounted within the drone enclosure to reduce latency, wiring complexity, and communication dependencies. Integrated with the command node is the drone enclosure, which provides charging, launch, landing, and environmental protection. The hub aligns the drone with a fixed charging interface to ensure consistent electrical contact and supports automated takeoff and landing sequences. It also houses backup command functionality integrated with the sensor network, ensuring continued system operation in the event of primary operator disconnection.

The Drone Subsystem integrates a flight control system for autonomous navigation, a Guidance, Navigation, and Control receiver for waypoint following, and a camera with onboard AI processing for target classification. After receiving data from the command node, the drone autonomously navigates to the designated location, conducts visual reconnaissance, and streams real-time imagery to an operator to review. A human operator retains authority over response actions.

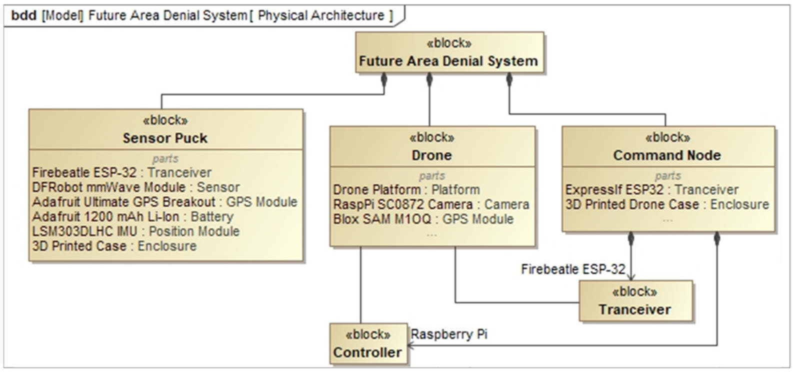

Figure 4: Block Definition Diagram of the physical architecture of the system

6. Prototype

Figure 5 shows the sensor puck, drone, and drone hub enclosure developed as a system prototype. The sensor puck is built around a custom printed circuit board (PCB) that integrates components into a compact, field-deployable form factor. The PCB minimizes footprint and power consumption while maintaining signal integrity across sensing, processing, and communications. Data from the radar, IMU, and GPS modules are routed to the onboard microcontroller, which performs data fusion, filtering, and event formatting before transmitting alerts through the integrated radio. The electronics are housed in a 3D-printed enclosure that protects components from environmental exposure while preserving sensor field of view and radio performance. The enclosure also supports battery integration and provides structural stability for ground deployment, enabling rapid fabrication, iterative refinement, and scalable production.

The drone prototype builds on a generic platform developed by the Electrical Engineering program at the United States Military Academy, which already includes the flight controller, GPS receiver, and onboard camera. This project integrated the command node hardware into the airframe by mounting a FireBeetle ESP32 transceiver to the on-board Raspberry Pi in the drone enclosure. When a sensor puck declares a detection, the alert is transmitted through the mesh network to the gateway and then received by the onboard ESP32 transceiver. The transceiver forwards the message to the Raspberry Pi, which prioritizes the event, converts the reported coordinates into waypoints, and sends commands to the flight control system. The drone then autonomously navigates to the location while streaming video to the control station for operator assessment.

Prior to launch, the drone remains docked within a 3D-printed protective enclosure that provides environmental protection, structural support, and a fixed charging interface. Upon receiving a validated tasking signal through the onboard transceiver, servo actuators open the enclosure to enable automated takeoff. After mission completion and landing, the enclosure closes to shield the drone and reestablish charging contact. This integrated prototype demonstrates the full physical implementation of the architecture, from distributed ground sensing through airborne response and protected recovery.

Testing of the full system was limited due to difficulty integrating the drone and the sensor puck. However, in isolation, both components work. The sensor puck can detect movement up to 25 meters and the drone is capable of acting as surveillance. Additionally, within the scope of the prototyping phase, certain features from the full project scope were not implemented due to time and cost constraints. The drone vision model was excluded due to insufficient onboard processing power and limited mounting space. Sensor puck battery life is reduced, as smaller cells are used to meet testing requirements. Autonomous recharging at the drone hub is also unsupported, as the current airframe is incompatible with the wireless charging interface specified in the full design.

Figure 5: Images of the Prototype: Sensor Puck PCB (left), Drone (center), and Drone Hub Enclosure (Right)

7. Conclusion

This research demonstrates the application of MBSE for the design of a safe, sensor-based alternative to traditional minefields. Through stakeholder analysis, requirements analysis, an AoA, and system architecting, the project identifies a feasible and ethically compliant solution that integrates ground sensors with autonomous aerial overwatch. This hybrid configuration provides scalable, precise, and reversible area denial capabilities while eliminating many humanitarian and legal risks associated with explosive ordnance systems.

The selected concept incorporates ground-based sensors with drones for aerial surveillance, providing an optimal balance of effectiveness, cost, and sustainability. It enables persistent monitoring, rapid detection, and human-in-the-loop verification while reducing the risk of collateral damage. The system's modular architecture allows for future improvements in sensing, communications, and autonomy as technology advances.

Future work will focus on expanding prototype testing to validate system performance in realistic field conditions, regarding both deployment and coordination of the system. There will also be a focus on exploring enhanced power management and communication resilience to improve overall system performance capabilities. This project provides a scalable framework for future non-lethal area denial systems that align with modern operational needs and ethical imperatives of modern warfare.

References

Delligatti, L. (2014). *SysML distilled: A brief guide to the systems modeling language*. Addison-Wesley.

Feng, J. (2024). Map shows where North Korea has placed land mines in demilitarized zone. *Newsweek*. https://www.newsweek.com/north-south-korea-map-dmz-land-mines-1895427

Fusco, B., Hubert, A., Velarde, D., Wegler, K., Whitaker, J., & Mittal, V. (2026, April). *Drone-augmented ground sensors: A model-based systems engineering approach to area denial*. In *Proceedings of the IEEE Systems Conference (SysCon)*, Halifax, Canada.

Human Rights Watch. (2023). Landmine use in Ukraine. https://www.hrw.org/news/2023/06/13/landmine-use-ukraine

Joint Chiefs of Staff. (2016). *Joint publication 3-15: Barriers, obstacles, and mine warfare for joint operations*. Washington, DC: Joint Chiefs of Staff.

L3Harris, *"REMBASS-II AN/GSR-8(V),"* available:107924.pdf

Monitoring and Research Committee. (2024). *Landmine monitor 2024*. Geneva, Switzerland: International Campaign to Ban Landmines.

Sage, A. P., & Rouse, W. B. (2009). *Handbook of systems engineering and management* (2nd ed.). Wiley.

U.S. Department of the Army. (1998). *Field manual 20-32: Mine/countermine operations*. Washington, DC: Department of the Army.