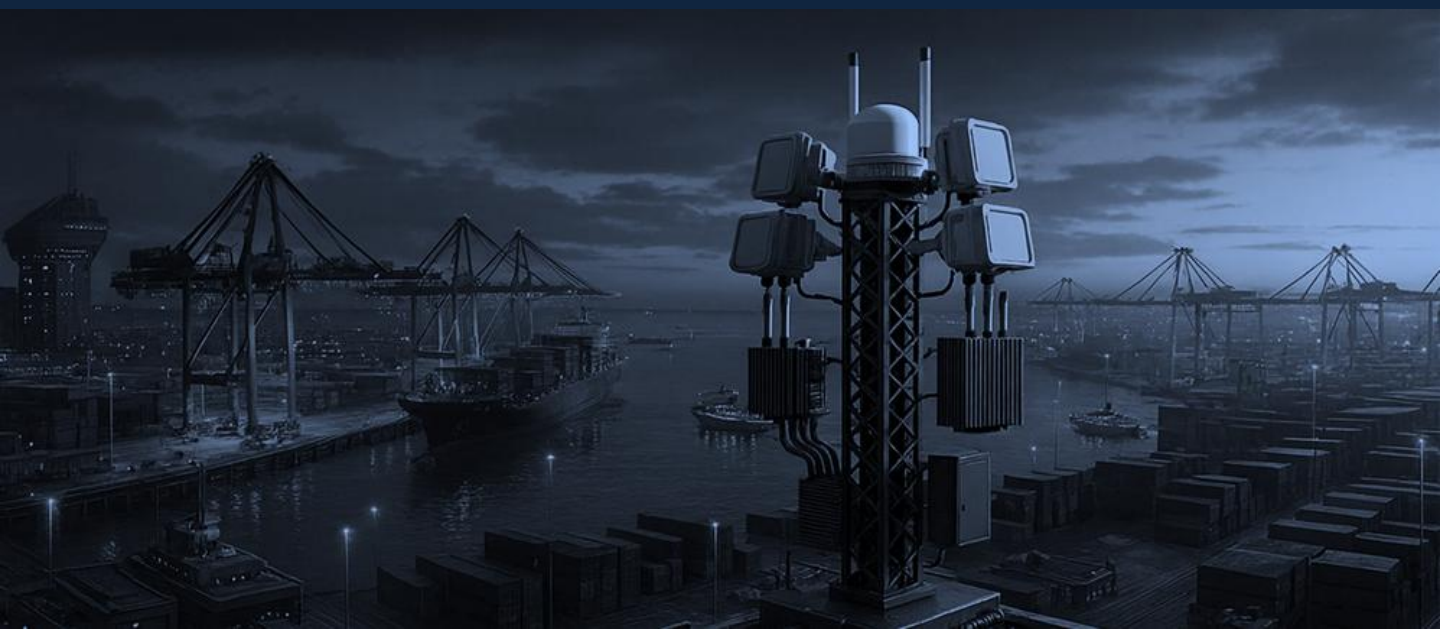
DETECT & DEFEND DRONES

INTERNATIONAL ARMOUR PVT LTD®

DEFENSE SYSTEMS



Autonomous C-UAS System

Direction Finder/Detection 6Km,
3Km Directional Jammer,
2Km Omni Jammer,
2Km of Spoofing,
3.5Km of an Active Radar and Kamikaze drone with Launcher Kit

1. Introduction

Modern warfare is characterized by increasingly complex and asymmetric threats, necessitating advanced, multi-domain defence systems capable of providing situational awareness, threat neutralization, and force protection.

This document introduces a comprehensive integrated electronic warfare (EW) and attack solution that synergistically combines Direction Finding (DF), Radar, EO/IR, Jamming, GNSS Spoofing, and Kamikaze Drone capabilities into a unified platform.

Designed to dominate modern battlefields, this solution offers a seamless blend of detection, disruption, and precision strike capabilities, enabling superior operational performance against a wide spectrum of threats.

1.1. Purpose and Capabilities

This integrated solution is developed to counter emerging threats such as unmanned aerial vehicles (UAVs), guided munitions, enemy radar systems, and hostile communication networks.

It combines detection, localization, and countermeasure technologies with offensive attack capabilities, providing operators with an end-to-end combat solution.

The primary capabilities include:

1. Threat Detection and Tracking: Utilizing radar for real-time surveillance and target acquisition over extended ranges.

2. Signal Interception and Localization: Employing Direction Finding (DF) systems to identify and geolocate radio-frequency emitters, including communication systems and UAV controllers.

3. Electronic Countermeasures (ECM): Implementing jamming techniques to disrupt enemy communications, radar systems, and data links.

4. Navigation Warfare: Deploying GNSS spoofing to mislead or deny adversaries access to satellite navigation systems, effectively neutralizing GPS-dependent threats.

5. Precision Strike Capabilities: Utilizing kamikaze drones equipped with high-explosive payloads for targeted elimination of enemy assets, including radar sites, command centres, and armoured vehicles.

1.2. Integrated Approach

This system’s design leverages synergistic interoperability between its components to provide a multi-layered defence and attack mechanism.

The radar and DF systems deliver accurate detection and localization of threats, enabling the jamming and GNSS spoofing modules to neutralize or mislead enemy systems. Simultaneously, the kamikaze drone provides a kinetic response option, complementing the electronic countermeasures for a comprehensive engagement strategy.

1.3. Operational Significance

The integration of EW systems with kinetic strike capabilities represents a paradigm shift in modern warfare.

This platform enables forces to detect, deny, and destroy threats through both non-lethal and lethal means, providing a strategic advantage in contested environments.

By combining electronic and kinetic warfare, this system creates a force multiplier effect, ensuring mission success against even the most sophisticated adversaries.

2. Why with us?

Most counter-drone systems developed and being marketed across the world majorly cater to stand-alone, piecemeal, or man-operated systems.

In the specific context of the entire spectrum of threats in an area and the possibility of a single point of failure, a far more pervasive solution would be needed. In real terms, a single autonomous system of systems concept that has the ability for multi-spectral illumination and autonomous operations with a central command and control center is the need of the hour.

It is the non-conventional, highly versatile, drone segment, consisting of multi-copters, VTOLs, both FW and Rotary, that pose everyday challenges, which by themselves are morphing daily and pose a threat in the delivery space.

The recent liberalization of Drone Operations in the Indian Airspace will lead to a proliferation of Drone Operations. This could pose further challenges to the safety and security of High-Value Assets, Installations, and Locations. That is why we aim to build the following;

- The world’s only defense system that shields against all categories of drones in all environments
- A unified Command & Control System that can identify friends from foes.
- Wide area Secure Communication Mesh Network based solution
- Fuses multiple sensors that suit a specific environment
- Integrates Multi-Weapons, AI to choose an optimal weapon for a precision hit
- Uses autonomous counter drones to mitigate swarm attacks
- Capability to integrate with other Information Systems.

Manufacturer is developing 12 proprietary modular technologies that can be used separately, or in combination with each other

01

Retractor Mitigation
Takes control of a drone and lands it in a designated area

02

SkyCop Surveillance Drones®
Level 5 autonomous drone that can monitor threats

03

Zombee Mitigation®
Level 5 autonomous drones that can kill threats

04

SkyOS™
Unifies people, process, data and infrastructure related to airspace management

05

SensorFusion AI
A potent mix of sensing technologies

06

SpiderMesh Communication Network®
High-speed wireless mesh network covering upto 4000 sq. km

07

HyperMind Computing™
AI Computer that can plan and execute missions

08

HyperVision Cameras®
Uses machine vision to identify threats

09

Repulsor Mitigation®
Kicks a drone out of a protector area

10

WeaponFusion AI™
Make existing weapons autonomous by integrating them

11

Brig IOT Devices®
Edge AI smart data and control device

12

GlobalGrid Interface®
Unified real time Command and Control interface

3. Proposed Solution – Military Counter Drone Solution

The modern battlefield is undergoing a profound transformation.

With the rapid proliferation of Unmanned Aerial Systems (UAS) - ranging from hobby-grade quad-copters to sophisticated autonomous swarms - the nature of aerial threats has expanded beyond conventional air assets.

Drones are now employed for real-time surveillance, target acquisition, electronic warfare, precision strikes, and kamikaze-style attacks.

Their accessibility, affordability, and ease of deployment make them a serious asymmetric threat, especially in high-altitude border zones.

With the rise of low-cost drone threats, modern militaries are prioritizing counter-drone solutions to protect assets as they target the least protected envelope of the target.

Unlike traditional threats, drones can conduct swarm attacks from unpredictable angles. The traditional weapon systems cannot cope with the maneuverability of the drones.

That is why we propose a combination of RF-based detection systems with soft kill/hard kill countermeasures to address the threats posed by the drones.

In modern airspace management and tactical operations, the ability to quickly and accurately distinguish between friendly, neutral, and hostile aerial entities is critical.

As the complexity of low-altitude traffic increases, particularly with the proliferation of drones and the rise of asymmetric threats, modules like UTM (Unmanned Aircraft System Traffic Management) and IFF (Identification Friend or Foe) must rely not just on real-time sensing but on intelligent context and preloaded knowledge.

This is where the threat library becomes an indispensable asset. A preloaded threat library is a curated database that contains known threat signatures, adversarial behaviors, drone IDs, RF fingerprints, protocol patterns, and flight characteristics of potentially hostile actors or platforms.

When integrated into UTM and IFF modules of the C2 system, it enables automated recognition, classification, and response guidance, enhancing both speed and confidence in operational decisions.

The growing use of mass drone attacks or swarm attacks is a part of threat visualization and in the field will require additional layers of protection than simply more accurate and larger zones of destruction provided by a single layer countermeasure system. It needs beefed-up capability, resulting in blocking or spoofing of swarms by either neutralizing GNSS or communications.

Recommendation Note: Preference for DF + Radar Fusion over Radar + EO/IR

It is recommended that the C-UAS solution prioritize fusion between Direction Finder (DF) and Radar, rather than Radar + EO/IR, as the primary detection and localization layer.

This recommendation is based on operational advantages in both reaction time and detection robustness:

- **Superior Detection Reliability**

• DF systems provide passive, low-latency bearing information based on drone RF emissions (e.g., controller links, telemetry).
• Radar complements this by offering range and altitude data, creating a rapid and accurate 2D or 3D threat localization grid.

- **All-Weather, All-Condition Detection**

• DF and Radar are unaffected by poor visibility (fog, rain, smoke, or night operations), unlike EO/IR, which is heavily dependent on line-of-sight and optical clarity.

- **Faster Target Cueing**

• DF can instantly cue radar for range validation without needing visual confirmation, enabling rapid target engagement before EO/IR can lock on.

- **Reduced False Positives**

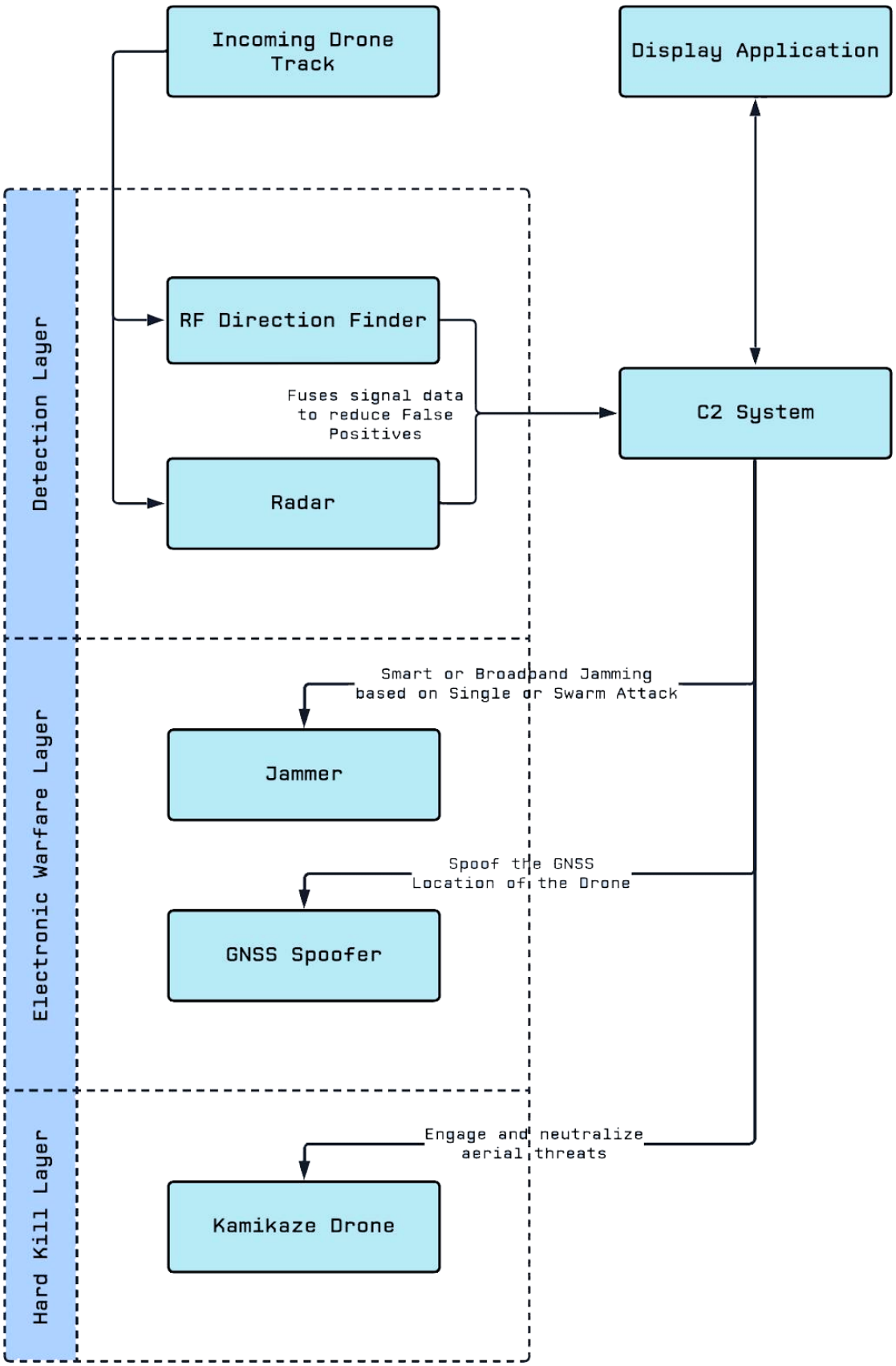
• DF verifies RF activity before radar returns are classified, minimizing radar clutter-induced false alarms.

- **Power and Processing Efficiency**

• DF + Radar requires less processing power and bandwidth than maintaining persistent EO/IR feeds, making it lighter and more scalable on mobile platforms.

Therefore, a DF + Radar pairing offers superior fusion performance in complex electromagnetic and environmental conditions, while EO/IR should be retained as a confirmation and classification layer, not as the primary detection trigger. Please refer to the schematics below for the proposed solution.

A. Solution Schematic – Military Counter Drone Solution



B. Primary Components of the Solution

This proposed Counter-Unmanned Aerial System (C-UAS) solution offers a layered, multi-sensor and multi-effect architecture designed to detect, track, classify, and neutralize a wide range of drone threats - from commercial off-the-shelf UAVs to military-grade platforms.

At the core of the system are advanced RF Direction Finders (DF) and 3D Radar sensors, providing wide-area, all-weather detection and tracking of airborne threats.

For mitigation, the solution integrates both soft-kill and hard-kill options:

- RF Jammers and GNSS Spoofers to disrupt or take control of hostile drones in flight.

- Cued Kamikaze Drones to provide kinetic interception once a threat is confirmed and localized, enabling precise, low-collateral hard-kill engagements against aerial threats.

Component	Function
DF (Direction Finding) System	Detects and locates enemy drone RF signals.
Radar	Detects, tracks, and classifies objects by transmitting radio waves and analyzing their echoes from targets
GNSS Spoofer	Sends false GPS signals to mislead or disable GPS-dependent drones.
RF Jammer	Disrupts drone communications and control links.
Kamikaze Drone	precision-guided systems that intercept and destroy low-altitude aerial threats like drones and helicopters through direct impact.
C2 System	Serves as the central intelligence node that fuses sensor data, executes threat assessment, and orchestrates mitigation actions across jammers, spoofers, and displays.
Display Application	Provides a real-time visual interface for monitoring threats, system status, and operational decisions executed by the C2 system.

C. Detection & Tracking

The first step in countering drone threats is to detect and track them using RF Direction Finder and Radar

C-1. DF (Direction Finding) System

Purpose
- Detects and classifies RF emissions from drones and their controllers.

Operation:
- Uses multiple DF sensors to triangulate drone positions via angle of arrival(AoA) calculations.
- Works on common drone frequencies (2.4 GHz, 5.8 GHz, and military bands).
- Passive operation allows stealth detection without emitting signals.

Deployment
- Fixed installations
- Baseline separation between sensors optimizes triangulation accuracy(typically 100m to 1km apart).

C- 2. Radar

Purpose
- Detects and tracks aerial threats (drones, UAVs, swarms) across a defined airspace volume, regardless of lighting or weather conditions.
- Provide early warning and continuous tracking of airborne targets to enable cueing of other subsystems (e.g., jammers, kinetic effectors).
- Support threat classification based on size, velocity, altitude, and flight behavior.

Operation
- Transmits radio waves that reflect off airborne objects.
- Measures the time delay, Doppler shift, and angle of return to determine: **Range**, **Bearing**, **Altitude** and **Velocity**
- Continuously scans a predefined sector or performs 360° surveillance in rotating mode.
- Applies clutter filtering and micro-Doppler processing to distinguish drones from birds or background noise.
- Outputs track data to a C2 system, which may fuse it with inputs from RF DF.

Deployment
- Fixed installations
- Radar tracking will only be enabled when the platform is stationary
- We are assuming that the platform will be able to provide the YPR data in real time for the Radar system

D. Neutralization Measures

Once the drone is identified as a threat, different countermeasures are used.

D-1. GNSS Spoofer

Purpose
- Disrupts the drone's GPS-based navigation.
- This is primarily used to counter swarm attacks

Operation:
- Sends fake GPS coordinates to confuse or mislead GPS-reliant drones.
- Can redirect a drone to a pre-designated kill zone.
- Works best against autonomous or GPS-dependent drones.

Effect:
- Causes drones to veer off course or land at incorrect locations.
- Can cause force landing or erratic flight behavior in some cases.

D-2. Directional RF Jammer

Purpose
- Disrupts the drone's ability to communicate with its operator and other drones in the swarm.

Operation
- Generates interference over drone command & control (C2) channels.
- Can target specific frequencies to disrupt Wi-Fi, military, and proprietary control links.
- It can be set to intelligent jamming (only activates when a threat is confirmed).

Effect:
- This causes the drone to lose communication with its controller.
- Can trigger return-to-home (RTH) mode or force the drone into a hover/crash state.

D-3. Kamikaze Drone Interceptor

Purpose:
- Provides kinetic interception of drones
- All leakages from the Spoofer layer would be targeted at this layer

Design:
- Small, fast-moving drone with high-explosive (HE) payload or collision-based kill mechanism.
- Integrated with LRF and RF sensors for autonomous target acquisition.

Operation:
- The interceptor drone launches autonomously when a threat crosses the mitigation zone threshold
- Uses AI-powered tracking to home in on the enemy drone.
- Engages in a direct collision or explosive detonation to neutralize the target.

Effect:
- Can engage multiple targets if deployed in swarms.

E. Command & Control (C2) System and Display Application

To orchestrate these components, a centralized C2 system is required.

Threat Detection & Assessment:
- Fuses data from DF and Radar modules.
- Classifies drones by type, threat level, and intent.

Countermeasure Coordination:
- Activates jammer and GNSS spoofer based on real-time threat analysis.
- Initiate the kinetic countermeasures if the electronic warfare fails

User Interface (UI) & Alerts:
- Displays real-time drone positions on a tactical map.
- Provides automated and manual override options.
- It can be remotely controlled via a secure military network.

4. Operational Workflow

Phase	Subsystem	Actions/Function	Data Flow / Decision Logic
Surveillance / Standby	All sensors	The system remains in passive/active scan or idle mode until an anomaly is detected	Periodic health checks, synchronized time clocks (GPS), logging enabled
Initial Detection	RF Direction Finder	Scans 400 MHz – 6 GHz spectrum for drone control links (RC, telemetry, video)	The azimuth angle of the RF source is computed and flagged if in the known threat band
	Radar	Detects moving aerial objects in 3D space	Provides range, azimuth, elevation, speed, and RCS
Threat Classification & Correlation	Fusion Engine	Correlates DF azimuth, radar tracks to identify a potential UAS	If multiple sensors agree, the threat confidence level increases
	C2 System	Displays and prioritizes detected threats with alert levels	Operator alerted if confidence > threshold
Threat Evaluation	C2 with Rules Engine	Evaluates drone type (GPS- based, FPV, swarm) based on signal pattern, flight path, and visual signature	If high-speed and evasive = FPV; if hovering = GPS
Tracking	DF + Radar	Continuously track drone location, heading, and altitude	Target track ID is maintained and updated dynamically
Mitigation Decision	Operator or Auto Mode	Based on ROE (Rules of Engagement) and threat proximity	Escalation strategy initiated
Soft Kill	GNSS Spoofer	Injects false GNSS coordinates to mislead the drone	Effective against semi-autonomous GPS-based drones
	RF Jammer	Blocks control and/or GPS frequencies (e.g., 2.4 GHz, 5.8 GHz)	Causes the drone to loiter, return to home, or crash
Hard Kill (if within range)	Kamikaze Drone (Hard Kill)	Fires upon counter-drone when within kinetic range and the safety envelope is clear	Uses target data from fused sensors
Post-Incident Actions	C2, Logging System	Records all data for debrief and intelligence	Data is pushed to the central server or battle management system
Reset and Resume Monitoring	All subsystems	Resume standard scan cycle	Track any remaining threats or secondary drones

4.1. Summary of Workflow Dependencies

SubSystem	Detection (DF/ Radar)	Sensor Fusion	Threat Evaluation	Soft Kill (Spoofer / Jammer)	Hard Kill (Kinetic)	C2/Operator Interface	Post Incident Actions
RF Direction Finder (DF)	Primary input	Azimuth cue	RC signal type	Required for jammer targeting		Display + status	Log RF source
Radar	Primary input	Range & velocity	Movement pattern	Provides coordinate s	Range data	Tracking overlay	Track archive
Sensor Fusion Engine		Core engine	Decision logic	Provides a unified track	Cue generation	Target UI	Timeline reconstruct
C2 System / Operator UI	Alerts display	Integrates feeds	Operator prompts	Authorizes action	Weapon trigger	Central node	Reporting dashboard
GNSS Spoofer			Evaluate GPS usage	Main mitigation path		Status & control	Spoof log
RF Jammer			Detects RC/GPS band	Main mitigation path		Jam mode select	Jam log
Kamikaze Drone		Aiming input	Lethal force criteria		Core actor	Fire control panel	Engagement report
Data Logger / Recorder	Logs DF / Radar	All fusion events	Evaluation steps	Jam/Spoof attempts	Kinetic logs	C2 Integration	Primary actor

5. Component Ecosystem and Planned Specifications

Planned Specification for Direction Finder

Specification Parameter	Specification Value
Antenna and Detection Parameters	
Drone Detection Range	5km
Azimuth FoV	360°
Elevation FoV	+60° to -60°
Average detection time	<15s
Maximum concurrent detection of drones	60
Maximum concurrent detection on frequency bands	7
Signal Parameters	
Detection Frequencies	433MHz - No direction, only presence 868MHz - No direction, only presence 915MHz - No direction, only presence 2.4GHz 1. GHz 2. GHz 5.8GHz
Direction Finding Accuracy - RMS	7.5° High Bands Only
Detection Output Parameters	
Threat Library	Yes, currently over 450+ models
Identify if the drone is part of the threat library	Yes
What information can the identified target	RF Signature in Threat Library Protocol Make Model Partial or Full Serial Number
What information can be tracked for the target	Standard - Telemetry Protocol is supported (MAVLink and Microhard, etc) Operating freq Azimuth
Provision to add a new drone to the threat library based on RF signature	Yes, 1 Week
Operating Parameters	
Operating Temperature	-30°c to +60°c
Storage Temperature	-40°C to 65°C
Max Humidity	95%
Weight	10-12kg
Power Supply	110-240v
Wattage	Less than 100W

5. Component Ecosystem and Planned Specifications

Planned Specification for RADAR

Specification Parameter	Specification Value
Radar Type	Pulsed Doppler Electronically Scanned Array
Range	2.5 km
Panel Azimuth	90°
Panel Elevation	50°
Angular Resolution	7.5º Elevation and 4.5º azimuth
New Track Acquisition Rate	4s
Max Tracks	1000
Dimensions	Up to 42.5 cm x 33 cm x 18 cm
Operating Temperature	-32 °C to +55 °C
Weather Protection	IP67

5. Component Ecosystem and Planned Specifications

Planned Specification for Radio Frequency Jammer

Specification Parameter	Specification Value
Antenna and Jamming Parameters	
Type of Jamming	Spot, Sweep, Barrage
Jamming Range	3 km
The number of drones that can be jammed concurrently	20
Effective Range for Directional Antenna	3000m with J/S 1:1
Effective Range for Omni Antenna	1500m with J/S 1:1
Average Mitigation Time	15s
Azimuth Coverage	360°
Elevation Coverage	360°
Continuous Jamming Time	3hrs
Cooling Time	30 mins
Signal Parameters	
Jamming Frequency Bands	433-434Mhz 860-925Mhz 1160-1280Mhz 1400-1499Mhz 1560-1620Mhz 2400-2500MHz 5170-5250MHz 5700-5900MHz
Effective Radiated Power (W) at each frequency	100 W Max
Operational Settings	
Provision to switch frequency	Yes
Provision to select multiple bands	Yes
Built-in Test Equipment	Yes
Operating Parameters	
Operating Temperature	-20 to +55 degrees
Storage Temperature	-40 to +60 degrees
Max Humidity	95%
Weight	60Kg
Power Supply	AC230

5. Component Ecosystem and Planned Specifications

Planned Specification for GNSS Spoofer

Specification Parameter	Specification Value
Range and Coverage	
Maximum Jamming Range	2km
Maximum Spoofing Range	2km
Azimuth Coverage	360 degrees
Elevation coverage	360 degrees
Spoofing Mode	Navigation spoofing
Jamming Mode	Sweep
White Listing of Frequency Supported	Yes
Antenna and Signal Transmission	
GPS Bands Spoofing Coverage	L1
Galileo Bands Spoofing Coverage	E1
BeiDou Bands Spoofing Coverage	B1
GLONASS Bands Spoofing Coverage	L1
GPS Bands Jamming Coverage	L2
Galileo Bands Jamming Coverage	E5b
BeiDou Bands Jamming Coverage	B2
GLONASS Bands Jamming Coverage	L2
Transmission Output Variable	30dBm to 51dBm
Performance Metrics and Scalability	
Spoofing Duration:	Continuously on AC Power. 2 hours with battery power
Mitigation Success Rate (Even any other device used in GNSS systems, like smartphones, etc)	> 98%
Number of Drones that can be mitigated concurrently	No upper limit
Environmental and Operational Factors	
Sensor Operating Temperature Range	-40°C to +50°C
Sensor Storage Temperature Range	-50°C to +85°C
Sensor Humidity Range	0% to 95% RH, non-condensing
Sensor EMI/EMC	MIL-STD-461E
Sensor Ingress Protection	IP67
Sensor Built-in Test Equipment	Yes
Sensor Maximum Weight	Main Unit: 7kg Tripod + Antenna: 4kg
Sensor Dimensions	320 x 340 x 96mm (without antennas)
Sensor Idle Power Consumption	30W
Sensor Max Power Consumption	60W
Power Supply Type Supported	Mains or Battery
Power Supply (Mains)	100-240VAC, 100W

5. Component Ecosystem and Planned Specifications

Planned Specification for Counter Drone System

Specification Parameter	Specification Value
Counter Drone Category	Small
Mitigation Drone Category	Small
Counter Drone Operating Frequency	2.4GHz for both uplink and downlink
Counter Drone AUW with battery and standard payloads	1.98 kg Micro 2.8 kg Small
Counter-Drone Physical Dimensions	Less than 330 x 330 x 400 mm (motor to motor)
Counter Drone Chassis	Modular - Carbon Fiber, Nomex with Aircraft Grade Aluminium and Titanium reinforcements
Counter Drone Battery	Inbuilt fixed suitable battery compatible with auto charging capsule
Counter Drone Endurance	Max of 25 mins at optimum speed Endurance at max speed would be 15 mins
Counter Drone Launcher	Provision to engage post-launch in mid-air Provision to launch in follow mode or termination mode Provision to change the mitigation policy from follow to termination in mid-air
Counter Drone Recovery	VTOL – Safe landing zone
Counter Drone Propulsion	Quadcopter Format High-Speed Brushless DCM Electric Propulsion (4xBLDC)
Counter-Drone Launch Modularity	Max drones for launcher - x3 Each drone will have its own channel
Maximum number of drones that can be docked onto 1 unit of launcher	Max drones per system - x99
Counter Drone Rate of Launch	One drone per 2s
Counter Drone Charging Capsule	The canister station will also charge Overcharging cutoff incorporated AC (100 to 240V) or DC of 18V No maintenance for 24 hours of docking (reboot)
Counter Drone Carrying Case	Hard case with trolley arrangement for enabling transportation
Counter Drone Ingress Protection	IP47
Counter Drone Functional Temperature Range	-20 C to 50 C
Counter Drone Functional Humidity Range	RH: 20-80% non-condensing
Counter Drone Operational and Comm	Up to 5km

5. Component Ecosystem and Planned Specifications

Planned Specification for Counter Drone System

Specification Parameter	Specification Value
Counter Drone Max Speed	50 m/s
Counter Drone Maximum Operating Altitude (AGL)	1000m
Counter Drone Maximum Launch Altitude (AMSL)	4000m (Operational ceiling as well, so if launched at 3000m, then max operating altitude would be 1000m AGL)
Counter Drone Wind Resistance	14m/s
Counter Drone Chase mode activation	50m
Counter Drone Mode	Autonomous Waypoint Navigation (pre-defined as well as dynamically adjustable waypoints during flight with support of C2 input)
Counter Drone Autonomy	Fully autonomous from Take-Off to Strike based on the target positions provided by the C2
Counter-Drone Failsafe Features and ECCM Measures	➔ Return to Home on communication failure ➔ Return to Home/Land on low battery
Counter Drone User Controls	One-click launch from the canister / Docking pad
Counter Drone Data Link	Secure communication link between UAV and GCS with a minimum 128-bit encryption
Counter Drone Default Payload	Suitable MV camera with a companion computer
Counter Drone End Game by leveraging the onboard EO sensor	Yes
Counter Drone Anti-Collision Capability	Yes
Counter Drone Day and Night Capability	Yes
Counter Drone Onboard Camera Specs	Camera on top of the body Fixed FoV camera Focal length 21mm Sensor Width 1/1.7 inches Horizontal Width - 1920 Pixels

5. Component Ecosystem and Planned Specifications

Planned Specification for Command & Control Software

The technical specifications mentioned herewith are minima

Software Specifications

- System Features
  - Unified Command and Control System
  - Scalable and Modular Setup
  - Support Multi-Engagements
  - Supports Multi-Node Deployments
  - AI-Based Threat Detection System
  - Supports TCP, UDP, HTTP, REST API, Serial, USB, Protobuf, Modbus, etc.
  - Supports standard and custom data formats for sensor interface
  - Near Real-Time Application
  - Early Detection and Warning System
  - Alert Management System
  - Integrated Record and Replay (video, data, voice)
  - Event / Alert Logs
  - Interfaces for Sensors, VMS, VA, Data Wall, Touch Table, PDA, Mobile, etc.
  - Supports NAS / SAN Storage
  - Situational Awareness Picture to the Operator
  - Supports Linux
- Modules
  - Sensor Interface
  - Sensor Data Processor
  - Sensor Deployment Application
  - Threat Detection and Analysis Application
  - Weapon Assignment Application
  - Decision Support Application
  - Multi-Sensor Object Tracking
  - Database Application
  - Display Interface for Server Class Machines / Touch Table / Tablet
  - / Mobile Devices
  - Alert Management Application
  - Live Events and Videos Record and Replay Application
  - Network Management Application
- Admin Settings
  - Sensor Parameter Configuration
  - Sensor Deployment Plan
  - Sensor Health Status (NMS)
  - Generation of Reports
  - Defining Rule-based actions
  - Configuration of Sensor Priorities
  - Data Filtrations

5. Component Ecosystem and Planned Specifications

Planned Specification for Command & Control Software

Hardware Specifications

- Rack Server for C2
  - OS - Ubuntu 20.04
  - Form Factor - 1U
  - Processor
    - Cores - 16 or more
    - Threads - 32 or more
  - Memory
    - Type - DDR4
    - Total Memory - 64 GB or more
  - Storage - 2TB SSD or more
  - GPU - 8GB GDDR6 or more
  - Ports
    - Universal Audio Jack
    - USB 3.1
    - USB Type C
    - Serial Port
    - HDMI
    - RJ45 Ethernet
      - 1G
      - 10G
  - Display: 22-inch Monitor
- NAS Server:
  - Form Factor - 1U/2U
  - Storage Data - Files / Multimedia
  - Memory - 80 TB or more
  - RAID – Yes

5. Component Ecosystem and Planned Specifications

Planned Specification for Security Operator Application

Direction Window

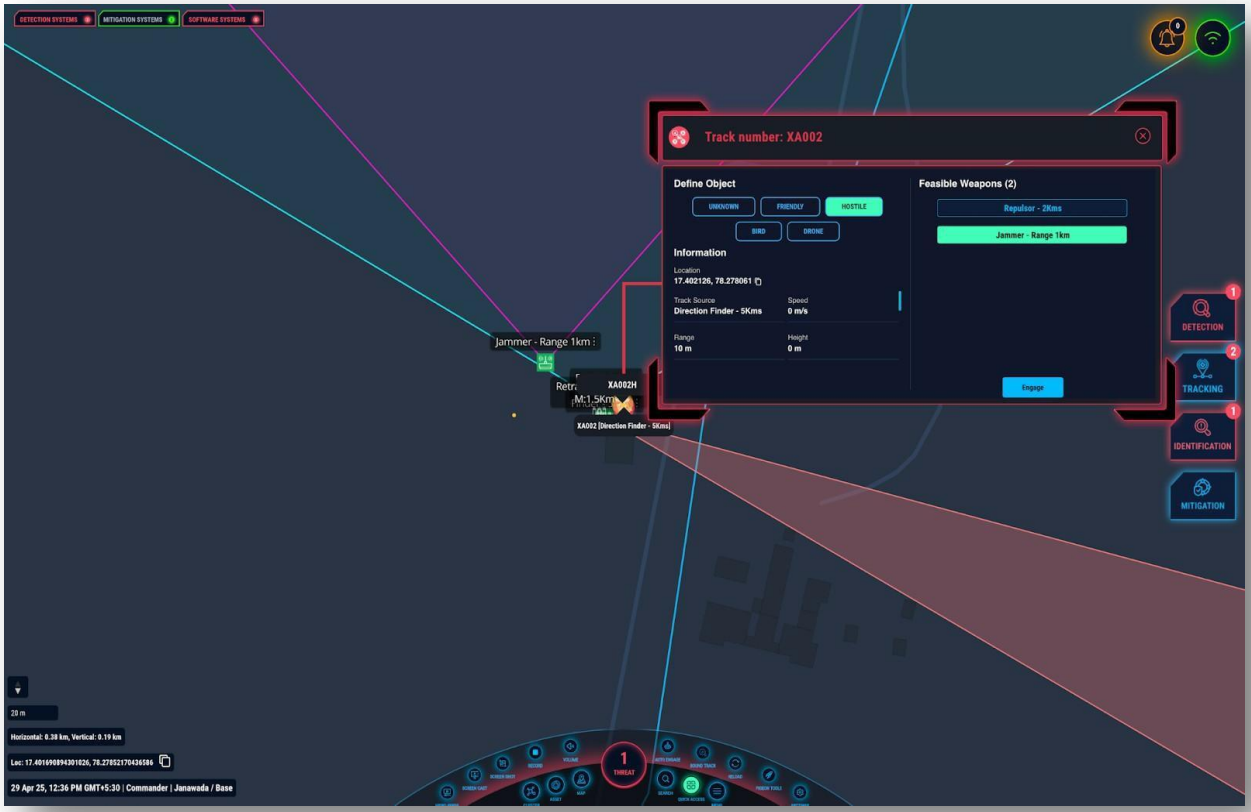
Tracking Window

5. Component Ecosystem and Planned Specifications

Planned Specification for Security Operator Application

Info window of the sensors

Info window of a hostile track with weapon feasibility

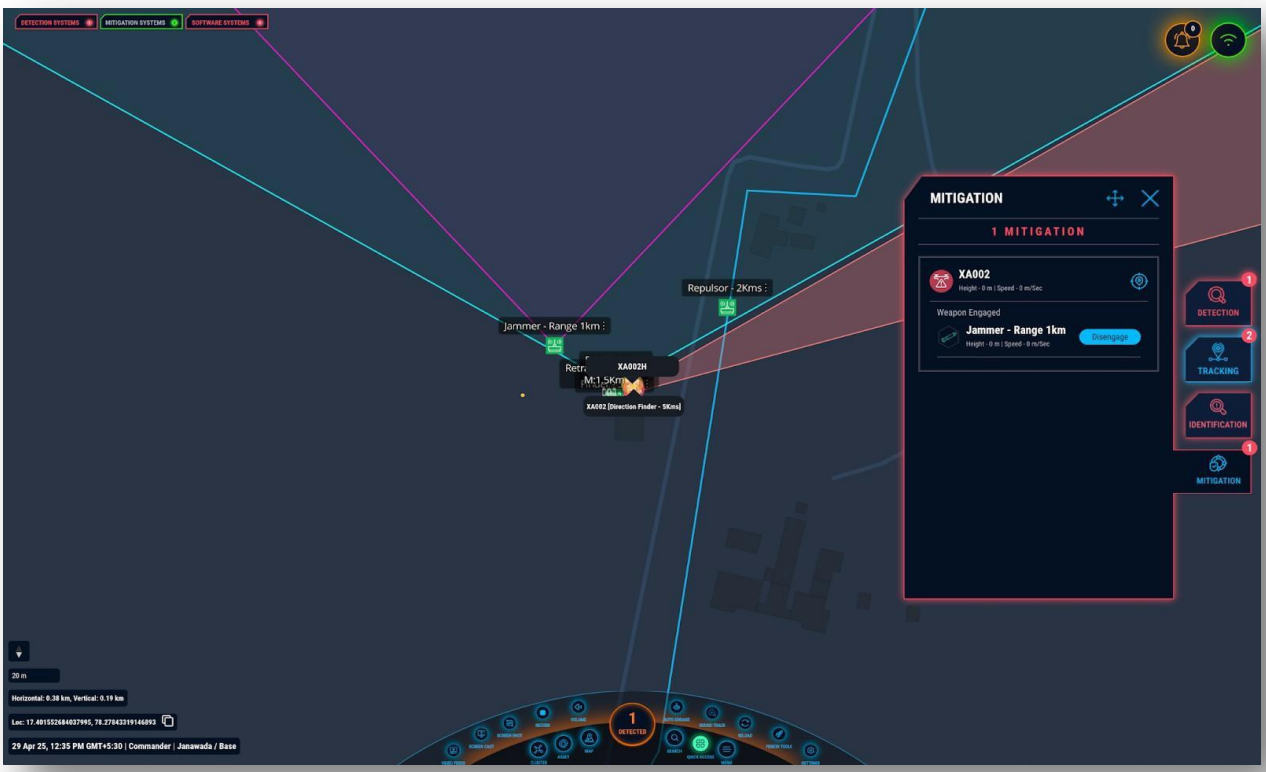


5. Component Ecosystem and Planned Specifications

Planned Specification for Security Operator Application

Identification Window

Mitigation Window



5. Component Ecosystem and Planned Specifications

Software Specifications

- Administrative Operations
  - Setup
    - Create Organization
    - Create Zone
      - Detection Zone
      - Engagement Zone
      - Protected Zone
      - Free Fly Zone
      - No Fly Zone
      - Safe Landing Zone
    - Add, modify, or delete a Building
    - Add, modify, or delete Sensors
    - Add, modify, or delete Machines
- Map Canvas
  - View Map Metadata
  - Tangible object-based intuitive menus for ease of use on the map canvas
    - Map Menu
      - Select Map Type
      - Select Tilt
      - Select Zoom
      - Select Light/Dark Mode
      - Re-center the map
    - Asset Menu (Show or Hide Selection)
      - Zones
      - Buildings
      - Sensors
      - Machines
    - Markings Menu (Show or Hide Selection)
      - Tracks
      - FoVs
      - Azimuth Lines
      - Range Circles
  - Search
    - Assets
    - Address
  - Logs
    - Screenshots
    - Screencast
  - Pigeon Tools
    - Line
    - Polygon
    - Circle
    - Distance Measure
- Sensor Status Snapshot
  - ID
  - Name
  - Type
  - State
    - Operational
    - Communication Link
    - Readiness

5. Component Ecosystem and Planned Specifications

- Alerts Pane
  - List
    - Filters
      - Launch info window for a specific asset with its relevant state data on tap
    - Listed Drone
      - Location
        - Latitude
        - Longitude
        - Azimuth
        - Elevation
        - Velocity
      - Envelope
        - Azimuth
        - Field of View
    - Track
      - Track Number
      - Track Type
      - Track Active Status
        - Primary Reckoning
        - Dead Reckoning
      - Identification Data
        - Make
        - Model
        - Serial Number
        - Operating Frequency
        - Drone Home Location
      - Tracking Data
        - Drone Location
        - Operator Location
        - Altitude
        - Speed
        - Heading
        - Drone Onboard Camera Direction
        - EPOCH Timestamp in Seconds
      - Engage
        - Safe Land
        - Disconnect Controller
      - Disengage
- Threat Table (Available as a shortcut on the map canvas for airspace situational awareness)
  - Detected Pane
    - Operations supported for listed tracks
      - Set Allowed or Blocked
  - Identified Pane
    - Operations supported for listed tracks
      - Engage
  - Engaged Pane
    - Operations supported for listed tracks
    - Disengage

5. Component Ecosystem and Planned Specifications

Hardware Specifications

- Display Hardware - Command Table
  - Screen Size - 55 Inches or more
  - Resolution
    - 4K - 3840x2160 pixels or better
  - Processor
    - Performance - 8 Cores or more
    - Efficient - 12 Cores or more
  - RAM - 32GB DDR5 or better
  - GPU - 8GB GDDR6 or better
  - Storage: 1TB SSD or more
  - Connectivity:
    - WiFi 802.11 a/b/g/n/ac
    - Ethernet
    - Bluetooth 5.0
    - USB 2.0/3.0
    - USB Type C
  - Touch Response - +/- 5s
  - Operating System - Windows 11 Pro
- Display Hardware - Portable
  - Screen Size - Up to 13 Inches
  - Resolution
    - 2K - 2560x1440 or better
  - Processor
    - Performance - 8 Cores or more
    - Efficient - 8 Cores or more
  - RAM - 16GB LPDDR5x or more
  - GPU - 4GB or more
  - Storage - 512GB SSD or more
  - Connectivity:
    - WiFi 802.11 a/b/g/n/ac
    - Ethernet (Via USB Type-C)
    - Bluetooth 5.0
    - USB 2.0/3.0
    - USB Type C
  - Operating System - Windows 11 Pro
  - Battery Life - Up to 19 hours