GOVTECH · DEFENCE INNOVATION · THOUGHT LEADERSHIP

The Sky Is No Longer the Limit — It's the New Attack Surface

Integrated Counter-UAV Defence Systems (ICUDS): An Enterprise Explainer

BY OPTIVALUE TEK

Illustration: OptiValue Tek / Forbes GovTech. Drone silhouettes represent a composite of commercial and tactical UAS types referenced in this article.

In 2023, a commercially available quadcopter carrying a modified payload flew undetected over a critical infrastructure facility for eleven minutes before ground personnel noticed it visually. No alert was raised. No automated response was initiated. The facility had no integrated counter-UAV posture.

This scenario — already well-documented across energy, transport, and government estate sectors — is the operational reality that Integrated Counter-UAV Defence Systems (ICUDS) are engineered to address.

For enterprise decision-makers, ICUDS is no longer a niche military procurement topic. It sits squarely at the intersection of physical security, enterprise risk management, regulatory compliance, and operational continuity. This article explains what ICUDS is, why the integrated model outperforms legacy siloed approaches, what the key architectural layers are, and what any organisation with airspace exposure must assess today.

$4.7B	2,000+	11 min
Global C-UAS market projected value by 2029 (MarketsandMarkets)	Unauthorised drone incursions at major airports globally, 2023	Average detection delay at unprotected critical infrastructure

Why 'Counter-Drone' Alone Is Not Enough

The term 'counter-drone' conjures a simple image: detect a drone, shoot it down. In practice, the threat is far more complex, and the legal, operational, and reputational consequences of a blunt response can be severe. A drone neutralised over a densely populated zone creates a falling-debris risk. Electronic jamming deployed without spectrum coordination can disrupt aviation communications. An organisation that acts without lawful authority to interdict an unmanned aerial system (UAS) may face liability regardless of the original threat posed.

This is precisely why the 'integrated' element of ICUDS is not a marketing flourish — it is the architectural principle that makes counter-UAV capability deployable in real-world environments. Integration means the system's layers communicate in real time, share a common operational picture, apply proportionate responses within a pre-authorised decision matrix, and log every action for audit and legal review.

> *"The question is no longer whether your airspace will be penetrated by an unmanned system. The question is whether your organisation has a coherent, lawful, and proportionate framework to respond when it is."*
>
> **— OptiValue Tek**

The Five Layers of an ICUDS Architecture

A well-designed ICUDS operates across five interdependent functional layers. Each layer has distinct technology requirements, and the value of integration lies in how data and decision authority flows between them.

Layer	Function	Core Technologies	Key Decision Point
Detection	Identify any airborne object within a defined volume of airspace	Radar (primary), RF scanning, acoustic sensors, EO/IR cameras	Coverage geometry and layered sensor fusion to eliminate blind spots
Tracking	Maintain a persistent track of object position, velocity, and trajectory	Multi-sensor track fusion, AI-assisted prediction engines	Handoff latency between sensor types — must be sub-second
Identification	Classify object as cooperative, non-cooperative, or hostile	Remote ID interrogation, RF fingerprinting, AI visual classification	Confidence threshold before escalation — typically 85%+
Neutralisation	Interdict the UAS using the most proportionate available effector	RF jamming, GNSS spoofing, kinetic interceptors, directed energy	Effector selection must be pre-authorised and environment-aware
Command & Control	Unified operating picture, decision support, and audit trail	C2 software, SIEM integration, geofence management	Human-on-the-loop vs. human-in-the-loop — a governance decision

Each layer is a programme of work in its own right. Many organisations mistakenly procure only one or two layers — typically detection and a single effector — and discover that without the command and control layer, they have data without decision-making capability, and without the identification layer, they face an unacceptable risk of interdicting cooperative or authorised aircraft.

The Regulatory Envelope: What Every CISO and Risk Officer Must Know

In most jurisdictions, the authority to interdict an unmanned aircraft — even a clearly hostile one — is reserved to designated agencies. This legal reality does not mean private organisations are powerless; it means that the neutralisation layer of an ICUDS must be designed around the operator's actual legal permissions, with interoperability built in for statutory authorities who hold interdiction powers.

Enterprise ICUDS deployments typically deploy the full detection-to-identification stack under direct organisational ownership, with the neutralisation layer managed either by an authorised service provider or through a pre-agreed activation protocol with a relevant authority. This model — sometimes called 'detect and

hand off' — represents best practice for regulated industries including aviation, energy, and government estates.

> *"Organisations that conflate 'counter-drone capability' with 'interdiction authority' will either under-invest — because they assume they can't act — or over-deploy, creating legal exposure that dwarfs the original threat."*
>
> **— OptiValue Tek Advisory Framework, 2024**

A Deployment Blueprint: What Good Looks Like

Based on OptiValue Tek's advisory work across critical national infrastructure, large venue operations, and government estate security, a mature ICUDS deployment shares a consistent set of design principles:

- **Threat-led sensor architecture.** Sensor selection and placement must be derived from a formal threat assessment — the specific UAS types, operator profiles, and ingress vectors relevant to the protected site — not from vendor product catalogues.
- **Interoperability from day one.** The C2 layer must exchange data with the operator's existing PSMS, SIEM, and statutory authority systems. Proprietary closed systems fail at the integration point.
- **A documented decision matrix.** Every potential UAS classification must map to a pre-authorised response sequence. This matrix is a governance document signed off at executive and legal level.
- **Red team and exercise cadence.** An ICUDS that has not been exercised against realistic threat scenarios — including EW, swarm configurations, and spoofing attacks — is not operationally validated.
- **Legal and audit architecture.** Every detection, classification, and effector activation event must be logged in a tamper-evident, legally admissible format.
- **Spectrum and airspace deconfliction.** RF-based effectors must be coordinated with national spectrum regulators and air navigation service providers.

The Convergence of Physical and Cyber Threat Surfaces

A dimension that many enterprise security teams underestimate is that UAS can be both a physical threat vector and a cyber collection platform simultaneously. A commercial drone equipped with a passive RF interceptor can harvest WiFi probe requests, Bluetooth identifiers, and GSM IMSI data from a facility perimeter. A drone carrying a rogue access point can conduct man-in-the-middle attacks against devices operated by personnel in outdoor areas. These hybrid threat profiles mean that the CISO, not only the physical security director, must have a seat at the ICUDS programme table.

Conversely, the ICUDS itself presents an attack surface. Radar systems, RF sensors, and C2 software are all susceptible to spoofing, denial of service, and cyber intrusion. A mature ICUDS programme includes a cybersecurity architecture review of every component, with particular attention to the interfaces between operational technology (OT) and IT networks.

The Business Case: Framing Investment for Board-Level Approval

For most organisations, ICUDS investment requires board-level approval and must compete with other capital programmes. The business case rests on three credible foundations:

- **Regulatory and insurance pressure.** Critical infrastructure operators now face legal duties to demonstrate a counter-UAS posture; insurers are beginning to differentiate premiums accordingly.
- **Operational resilience.** A single UAS incident at an airport, stadium, data centre, or energy facility can generate costs — in delays, fines, reputational damage, and incident response — that dwarf the cost of a proportionate ICUDS.
- **Enabling value.** A well-designed ICUDS creates airspace situational awareness with positive applications beyond threat response: logistics coordination, maintenance drone management, and estate monitoring.

The capital investment range spans from six-figure deployments for a single high-value site to eight-figure programmes for multi-site critical national infrastructure protection. OptiValue Tek's advisory methodology begins with a calibrated threat and asset assessment before any technology or cost framing — organisations that begin with vendor selection rather than requirement definition consistently over-spend and under-protect.

What Decision-Makers Should Do in the Next 90 Days

The window for proactive ICUDS planning is shortening. Regulatory requirements are hardening, UAS threat sophistication is increasing, and the vendor market still contains significant variation in quality, interoperability, and legal compliance. Three actions are achievable within a single quarter:

1. **Commission a formal UAS threat and vulnerability assessment** for your highest-priority sites. This is the foundation for every subsequent investment decision and is a standalone deliverable with immediate risk management value.
2. **Audit your existing physical security posture** for UAS-relevant gaps — specifically in detection coverage, incident response protocols, and legal authorisation framework for airspace response.
3. **Engage your national aviation authority and relevant law enforcement** to understand the statutory framework within which your organisation can act, and to establish the interoperability relationships that any effective ICUDS will require.

The drone is already in the airspace above every organisation of consequence. The question is not whether it will arrive; it is whether your organisation will know it is there, understand what it is, and be empowered — legally, technically, and operationally — to respond.

ABOUT OPTIVALUE TEK

OptiValue Tek is a specialist advisory and systems integration firm operating at the intersection of defence technology, enterprise risk management, and critical infrastructure protection. Our counter-UAV advisory practice supports government

departments, regulated industries, and large-scale venue operators in designing, procuring, and validating integrated airspace defence capabilities. We are vendor-agnostic, threat-led, and governance-first.

optivalue-tek.com | enquiries@optivalue-tek.com