

Responding to Hostile Drone Incursions After Detection

Author: Marco Capriz, Chief Technical Officer, Indochina Space

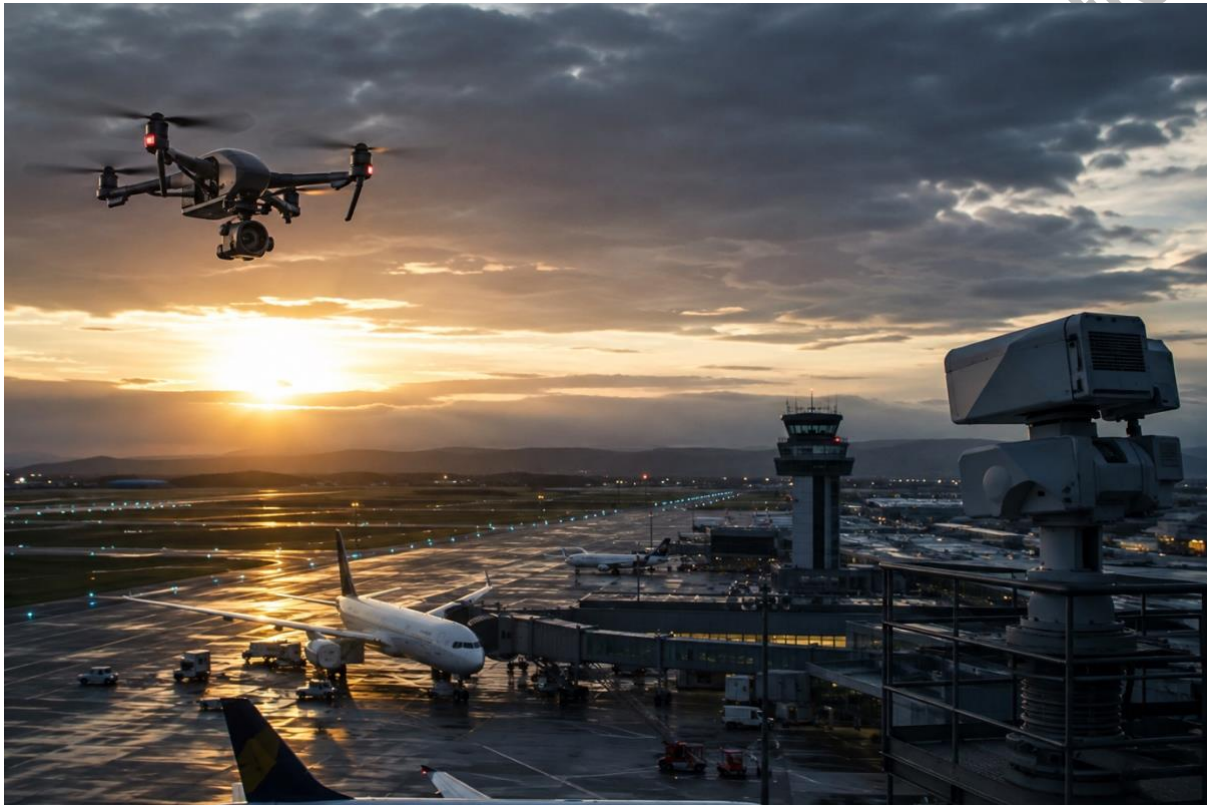


Table of contents

Responding to a Hostile Drone After Detection	1
Table of contents.....	2
Overview.....	3
Operational response issues.....	3
The correct response is a graduated incident protocol.....	4
Detect	4
Confirm and classify	4
Track continuously.....	5
Protect the potential target.....	5
Assess intent.....	5
Available response options.....	6
Operator intervention	6
Protocol or cyber takeover	6
Directed RF disruption.....	7
Capture	7
Kinetic defeat.....	7
Directed energy	8
The most credible solution is to intercept earlier	8
Outer detection zone	8
Classification zone	9
Preferred intervention zone	9
Critical exclusion zone.....	9
A better decision rule.....	9
Airports require a different doctrine from other sites.....	10
Governance is often the real weakness.....	11
Recommended post-detection protocol.....	11
Level 1: Unknown drone, low immediate threat.....	12
Level 2: Drone approaching a protected area	12
Level 3: Probable hostile intent	12
Level 4: Imminent attack	12
What the Leipzig incident suggests.....	12
An Integrated Operational Solution.....	13
Conclusion.....	14

Overview

The [Leipzig/Halle Airport incident](#) of 6 August 2026 exposes the most difficult part of counter-UAS operations. Detecting a drone is now technically achievable. Deciding what to do with it, particularly when it may be carrying explosives and is already above an airport or critical infrastructure site, is considerably harder.

German authorities have confirmed that the drone found near the airport's southern runway carried an explosive device. It was discovered near a Ukrainian cargo aircraft and was subsequently rendered safe. Separately, a DHL cargo aircraft struck an unidentified flying object while executing a go-around approximately six kilometres from the airport. Investigators have not yet established publicly that the object was another drone or that the two events were connected. ([Reuters](#))

Operational response issues

The incident demonstrates a basic operational truth:

A counter-drone system must determine whether intervention will reduce the overall danger or create a worse one.

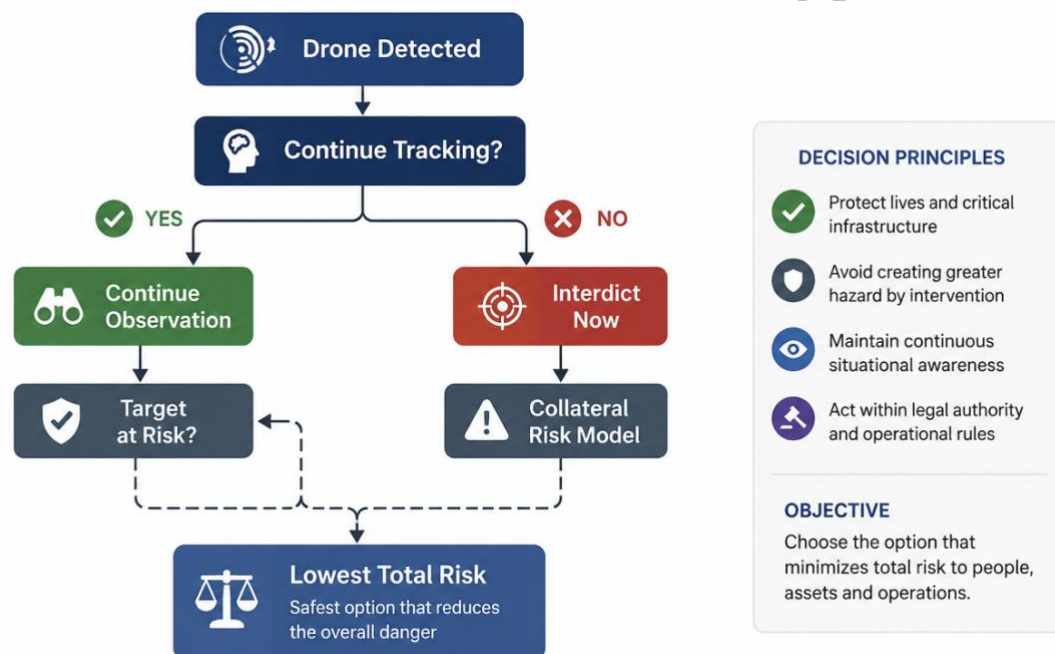


Figure 1: The Counter-UAS decision problem. Counter-UAS is a decision problem, not a shooting problem.

Destroying a drone directly above an aircraft, fuel installation, power transformer, chemical process, public building or crowd may convert an airborne threat into an uncontrolled falling explosive.

There is no universally safe neutralisation method

International guidance is remarkably consistent on this point.

[ICAO warns](#) that counter-UAS measures must not create additional hazards to aircraft, aviation infrastructure, personnel or authorised drone operations. It calls for a comprehensive risk assessment before any mitigation system is deployed.

[EASA](#) similarly treats unauthorised-drone incidents as an aviation safety-management problem rather than a simple security engagement. Its airport guidance focuses on coordinated decision-making between the airport operator, air-navigation service provider, airlines, police and other authorities.

The [US FAA](#) requires certificated airports to maintain an approved UAS response plan covering operational interruption and the safe restoration of normal operations. It does not assume that airport personnel will physically defeat the drone.

[Germany](#), France, Australia, Japan, Singapore and South Korea have taken different legal and technical approaches, but the same pattern appears repeatedly: prevention, early detection, airspace management, police intervention and carefully authorised mitigation are preferred to indiscriminate destruction.

The correct response is a graduated incident protocol

A mature counter-UAS response should follow a structured sequence.

Detect

The site must detect the drone far enough away to create useful decision time.

A single sensor is insufficient. Effective systems normally combine:

- low-altitude radar;
- radio-frequency detection;
- electro-optical cameras;
- thermal cameras;
- acoustic sensors;
- Remote ID or cooperative identification;
- visual reports from trained personnel.

South Korea's new national [performance standard for counter-drone equipment](#) covers radar, RF scanners, electro-optical and infrared cameras, and jammers. This is significant because it recognises counter-UAS as an integrated system whose components must be tested under defined conditions rather than purchased as isolated products.

Confirm and classify

The system must determine whether the object is:

- a drone;
- an authorised aircraft;
- a bird;
- a balloon;
- debris;
- a false electronic detection.

It should then estimate:

- drone type;
- speed and altitude;
- payload;
- probable endurance;
- command-link characteristics;
- autonomy level;
- predicted route;
- possible target.

False alarms at airports can themselves create significant safety and economic consequences. Visual or thermal confirmation should therefore accompany radar or RF detection wherever possible.

Track continuously

Tracking should cover both the aircraft and, where technically possible, the operator.

RF direction finding and AI-assisted optical/thermal tracking may identify:

- the drone's control frequency;
- the controller's approximate location;
- the protocol or manufacturer;
- telemetry or identification data;
- whether the aircraft is being manually controlled.

Locating and arresting the operator is often safer than interfering with the aircraft. [German federal police guidance](#) directs sightings towards police authorities, while French practice assigns counter-drone functions to specialist security units trained in detection, identification, neutralisation and operational coordination.

This approach fails against a fully autonomous aircraft, but it remains the preferred response for many careless, criminal or protest-related incursions.

Protect the potential target

The first active response may involve the airport or installation rather than the drone.

At an airport, this can include:

- stopping departures;
- instructing arriving aircraft to hold or divert;
- ordering a go-around;
- closing one runway while retaining another;
- moving parked aircraft;
- stopping fuelling or cargo handling;
- clearing exposed personnel;
- restricting vehicle movement;
- protecting emergency access routes.

[Singapore](#) used carefully regulated arrivals and departures during its 2019 drone disruption rather than attempting an immediate public neutralisation.

At critical infrastructure, equivalent actions may include:

- placing personnel under cover;
- suspending exposed maintenance;
- isolating hazardous processes;
- moving mobile assets;
- closing air intakes;
- placing fire and explosive-ordnance teams on standby;
- transferring control to backup facilities;
- preparing for loss of a specific asset.

This distinction is important. A successful counter-drone response may be one in which the drone is never physically intercepted, but the intended target becomes unavailable or resilient.

Assess intent

Presence alone does not establish hostility.

The system should evaluate behaviour such as:

- repeated approaches;
- orbiting;
- hovering above a specific asset;
- descent towards an aircraft or installation;
- payload release;
- coordinated movement by several drones;
- absence of a command signal;
- route changes that correspond to aircraft movements;
- deliberate use of terrain or buildings for concealment;
- activity at night or during sensitive operations.

A risk score should combine:

- probability of hostile intent;
- likely payload;
- time to target;
- vulnerability of the target;
- density of people below;
- consequences of interception;
- availability of safe recovery areas.

This creates a rational basis for intervention.

Available response options

No mitigation method works against every drone.

Operator intervention

Police locate the operator, compel landing and seize the equipment. This is usually the safest option where the controller can be found quickly. Its effectiveness depends on detection range, accurate direction finding and a rapid ground response team.

Protocol or cyber takeover

Some commercial drones use known communication protocols that may permit identification, command interruption or controlled landing.

Where legally authorised and technically feasible, this offers a major advantage: the aircraft can potentially be kept under powered control and directed away from the protected site.

Its limitations are substantial:

- it works only against supported systems;
- encryption may prevent access;
- firmware changes can defeat the technique;
- autonomous drones may have no live command link;
- bespoke or military systems may use unfamiliar protocols;
- the drone may be programmed to react aggressively to takeover attempts.

Cyber takeover should therefore be considered one option within a larger architecture, not a universal solution.

Directed RF disruption

A directional jammer may interrupt command or video links.

The difficulty is the failsafe behaviour of the aircraft. Depending on its programming, it may:

- hover;
- land immediately;
- return to its launch point;
- continue along a pre-programmed route;
- climb;
- switch to inertial or visual navigation.

At an airport, return-to-home behaviour could carry the drone directly across an approach path. Broad-spectrum jamming may also affect communications, navigation, surveillance, ground systems or authorised drones.

GNSS jamming and spoofing are particularly hazardous around aviation facilities. [ICAO guidance](#) emphasises that countermeasures must not create unpredictable aircraft behaviour or interfere with aviation systems.

Capture

Capture systems include:

- net launchers;
- interceptor drones;
- tethered systems;
- entanglement devices;
- parachute-equipped nets.

Capture may be appropriate for a small, slow drone over an empty area. It becomes much less attractive when the aircraft may contain explosives, incendiaries or hazardous material.

Physical contact may detonate the payload. A captured drone may also remain dangerous during recovery.

Kinetic defeat

Firearms, missiles and other projectile systems can destroy a drone, but their use at civilian airports and urban infrastructure is usually highly constrained.

Risks include:

- missed shots;
- ricochet;
- falling projectiles;
- battery fires;
- explosive detonation;
- fragmented payload;
- debris ingestion by aircraft engines;
- damage to process equipment;
- injury beyond the perimeter.

Kinetic engagement may be defensible at remote military facilities or over unpopulated ground. It is far less suitable above operational runways, terminal areas, refineries or power stations.

Directed energy

Lasers and high-power microwave systems are increasingly discussed as alternatives.

Lasers can damage propulsion, sensors or structural components, but the drone still falls. They also require line of sight, tracking accuracy, atmospheric clarity and strict controls around aircraft and optical sensors.

High-power microwave systems may disrupt electronics across an area. Their effects on nearby infrastructure, authorised systems and aircraft must be carefully assessed.

Neither method eliminates the ground-consequence problem.

The most credible solution is to intercept earlier

The safest counter-UAS strategy is to create distance between the protected asset and the point of intervention. A practical architecture uses concentric zones.

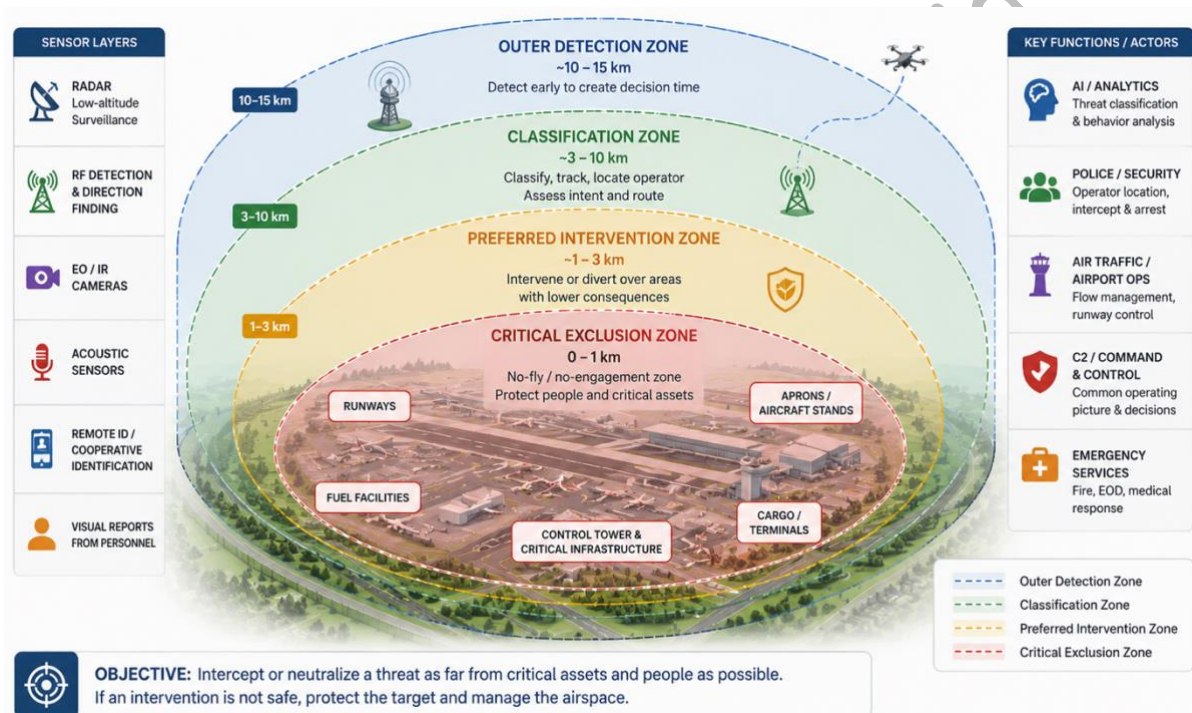


Figure 2: Layered counter-UAS architecture: defend in depth, detect early, assess, and intervene outside the critical area.

Outer detection zone

This may extend several kilometres beyond the perimeter, depending on terrain, airspace, urban development and legal authority.

The objective is to gain time for:

- confirmation;
- operator location;
- police deployment;
- airspace action;
- target protection;
- threat assessment.

Classification zone

The drone's type, route and behaviour are analysed. Authorised operations are separated from unknown ones. The command link and probable controller location are identified.

Preferred intervention zone

This should be located over areas where a forced landing, capture or loss of control would cause relatively limited damage.

Possible areas include:

- empty fields;
- undeveloped airport land;
- reinforced containment areas;
- cleared industrial zones;
- water, where environmentally and operationally acceptable.

The site should pre-map these areas before any incident.

Critical exclusion zone

This is the immediate area around:

- runways;
- aircraft stands;
- fuel installations;
- control towers;
- transformers;
- reactors;
- chemical storage;
- public buildings;
- crowds.

Within this zone, physical engagement may become less desirable because the consequences of successful neutralisation could equal or exceed those of allowing the drone to continue temporarily.

A better decision rule

The correct engagement question is not:

Can we disable the drone?

It is:

Will disabling the drone at this location and at this moment produce a safer outcome than continuing to track and contain the incident?

That decision should be based on a continuously updated collateral-risk model.

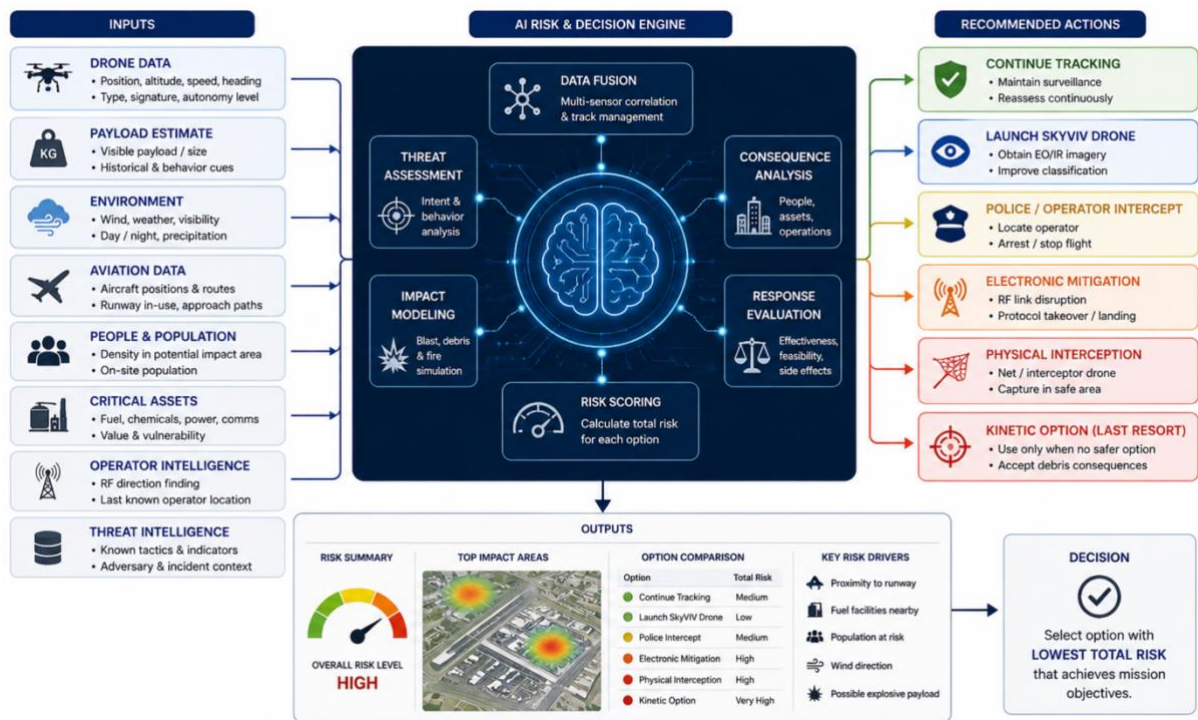


Figure 3: Collateral risk decision engine. AI-powered assessment of intent, consequences, and response options to select the lowest risk.

The model should calculate:

- predicted impact point;
- debris radius;
- probable explosive effect;
- nearby aircraft trajectories;
- population below;
- hazardous materials;
- wind;
- drone velocity;
- remaining endurance;
- probable target;
- consequence of closing the facility;
- consequence of non-intervention.

This is where artificial intelligence and automated decision support may be useful, although the final authority should remain with a trained human commander.

Airports require a different doctrine from other sites

Airports present unusual constraints:

- large, protected areas;
- moving aircraft;
- high closing speeds;
- vulnerable engines;
- dense radio-frequency environments;
- populated approach paths;

- limited tolerance for false alarms;
- severe economic consequences from closure.

The US FAA response-plan model, EASA incident-management approach and ICAO guidance all place substantial emphasis on managing flight operations and coordinating authorities rather than presuming that airport personnel will destroy the drone.

Other critical infrastructure sites may have greater freedom to create controlled engagement zones. Even there, the local environment determines the appropriate response.

- A refinery may be unable to tolerate falling lithium batteries.
- A nuclear site may have extensive standoff areas but highly restricted radio-frequency operations.
- A power substation may accept temporary shutdown of one asset to reduce the attractiveness of a target.
- A port may be able to divert a drone over water, although shipping and environmental risks remain.
- A prison may prioritise capture of contraband drones rather than destruction.

There is therefore no generic counter-UAS deployment.

Governance is often the real weakness

The technology is only one part of the solution.

A complete response requires clear authority for:

- confirming the threat;
- stopping airport or industrial operations;
- closing airspace;
- deploying police;
- activating electronic countermeasures;
- approving physical engagement;
- handling explosives;
- preserving evidence;
- restoring operations.

[Australia's 2026 drone-security consultation](#) explicitly recognises the need for stronger counter-drone capability around airports, critical infrastructure and major events, while balancing safety, enforcement and legitimate drone use.

[France](#) uses specialist national security units with defined detection and neutralisation roles. Germany places significant aviation-security responsibility with the federal police at major airports. South Korea is standardising equipment testing for important national facilities. Singapore combines restricted airspace, enforcement powers and active operational control.

The [European Union's 2026 counter-drone action plan](#) proposes deployment initiatives, AI-supported command-and-control systems, emergency counter-drone teams and annual large-scale exercises. This indicates that Europe increasingly regards the issue as a coordinated operational capability rather than an equipment procurement exercise.

Recommended post-detection protocol

A defensible airport or critical-infrastructure protocol would be:

Detect → confirm → classify → track → locate operator → protect target → assess intent → calculate collateral risk → select authorised response → preserve evidence → restore operations.

The operational actions should be grouped into four levels.

Level 1: Unknown drone, low immediate threat

- Confirm detection.
- Track continuously.
- Check authorised-flight records.
- Locate the controller.
- Alert security and police.
- Prepare operational restrictions.

Level 2: Drone approaching a protected area

- Restrict affected operations.
- Dispatch police towards the controller.
- Clear exposed personnel.
- Activate visual and forensic recording.
- Prepare authorised electronic or capture measures.
- Identify safe diversion or impact areas.

Level 3: Probable hostile intent

- Close relevant runway, airspace or process area.
- Activate the incident command cell.
- Move or isolate vulnerable assets.
- Select a response based on predicted collateral effects.
- Use takeover, directional disruption or capture only where the consequence model supports it.
- Prepare bomb-disposal and fire services.

Level 4: Imminent attack

- Protect life and critical functions.
- Apply the intervention with the lowest expected total harm.
- Accept that no option may be risk-free.
- Maintain evidence collection and secondary-drone surveillance.
- Assume coordinated or follow-on activity until disproved.

What the Leipzig incident suggests

The confirmed presence of an explosive device changes the operational category completely.

This was not an ordinary airport nuisance. It appears to have involved a drone capable of delivering or carrying an explosive payload inside a protected cargo area. German authorities are treating it as a serious security incident, although motive, origin and attribution remain under investigation.

Several preliminary lessons can be drawn without speculating about responsibility:

1. Perimeter fencing alone is no longer sufficient for airport security.
2. Detection must extend outside the airport boundary.
3. Cargo airports and military-logistics hubs may face a higher threat than conventional passenger-airport risk assessments assume.
4. Counter-UAS systems must detect multiple simultaneous objects.
5. Airport operations and counter-drone command systems must share a common operating picture.
6. Explosive-drone incidents require immediate integration with bomb-disposal procedures.
7. The site must continue searching after the first drone is located.

8. Safe neutralisation depends heavily on where the drone is detected.
9. The unidentified object struck by the DHL aircraft shows why airspace protection and drone response cannot be treated as separate systems, although the nature of that object remains unconfirmed.

An Integrated Operational Solution

The operational doctrine described throughout this paper requires more than a collection of sensors. It requires a common operational picture that allows decision-makers to understand the environment, evaluate risk and coordinate an appropriate response before a hostile drone reaches a protected asset.

A combined solution based on **Indochina Space**, **SkyVIV** and **NurjanaTech** provides the foundation for such an operational capability.

The process begins long before an incident occurs. SkyVIV autonomous survey drones periodically overfly the protected area and create a highly accurate three-dimensional digital twin of the airport or critical infrastructure site. Unlike a conventional map, the digital twin contains the exact geometry of buildings, aircraft stands, fuel facilities, roads, towers, power infrastructure, vegetation and surrounding terrain. This model becomes the permanent operational reference within the NurjanaTech Command and Control platform.



Figure 4: Integrated operational solution. From detection to decision: a connected system for complete situational awareness and coordinated response

When the NurjanaTech NEOS detection network identifies an unknown drone, the detection is immediately placed within the digital twin. Operators are therefore not looking at isolated radar tracks or camera images, but at a precise three-dimensional representation of the environment. The system can determine whether the drone is approaching a runway, flying towards a transformer, crossing an aircraft approach path or entering a designated containment area.

The digital twin also allows artificial intelligence to estimate the likely consequences of different response options. Using the three-dimensional model, the Command-and-Control system can predict possible flight paths, identify potential impact areas, calculate debris footprints and determine whether an interception would create greater danger than continued tracking. This directly supports the collateral-risk assessment discussed earlier in this paper.

The response capability extends beyond static detection. Once an incursion has been detected by the fixed NEOS sensor network, SkyVIV drones can be automatically dispatched to intercept the target from a safe distance. These airborne platforms provide high-resolution electro-optical and infrared imagery from viewpoints that fixed sensors cannot achieve. Their sensor feeds are transmitted directly into the NurjanaTech Command and Control system, where they are fused with radar tracks, radio-frequency detections and other available sensor data to produce a continuously updated operational picture.

This sensor fusion substantially improves target classification. Operators can distinguish between birds, authorised drones and genuine threats with greater confidence, determine whether the aircraft is carrying a visible payload, observe abnormal flight behaviour and maintain continuous visual tracking even if the target temporarily disappears behind buildings or terrain. The same capability assists law-enforcement agencies by helping identify launch locations and guiding response teams towards the suspected operator.

The digital twin also supports operational planning before any incident occurs. Airports and critical infrastructure operators can define preferred interception corridors, exclusion zones, emergency landing areas, safe containment locations and critical assets directly within the three-dimensional model. These areas become available to operators immediately during an incident, allowing faster and more consistent decision-making under operational pressure.

Rather than replacing existing security infrastructure, the combined architecture integrates with it. Existing radar systems, optical sensors, thermal cameras, radio-frequency detectors, perimeter security systems and air traffic information continue to perform their individual functions. The SkyVIV digital twin provides the spatial context, while the NurjanaTech Command and Control platform fuses all available information into a single operational picture that supports coordinated decision-making across security, airport operations, emergency services and law-enforcement agencies.

The result is a capability that directly addresses the principal challenges identified throughout this paper:

- Earlier detection and verification through multiple complementary sensor types.
- Accurate three-dimensional situational awareness of the protected environment.
- Continuous AI-assisted tracking within a live digital twin.
- Rapid deployment of airborne optical and infrared sensors to maintain visual contact.
- Improved operator location and forensic evidence collection.
- Dynamic collateral-risk modelling before any intervention is authorised.
- Better coordination between security personnel, airport operations and emergency responders.
- More informed decisions that maximise safety while minimising disruption to airport or critical infrastructure operations.

Instead of concentrating solely on how to neutralise a drone once it reaches a protected asset, this architecture provides the information required to make better operational decisions throughout the entire incident lifecycle, from early detection and classification through to coordinated response, evidence collection and post-incident analysis.

Conclusion

The Leipzig/Halle Airport incident demonstrates that the principal challenge in counter-UAS operations is no longer detecting a drone. The greater challenge is determining how to respond without creating an even greater hazard. Once a hostile drone reaches a runway, aircraft stand, fuel installation or critical infrastructure asset, every available response may carry significant operational, safety and legal consequences.

International doctrine is increasingly converging on a common approach. Successful counter-UAS operations depend on early detection, rapid confirmation, continuous tracking, operator identification where possible, coordinated operational decision-making and carefully controlled intervention. Neutralisation is only one element of the response, and, in many situations, it is not the safest or most effective option.

This paper has shown that the problem cannot be solved by any single sensor or countermeasure. Instead, an effective capability requires an integrated operational ecosystem that combines multiple detection technologies, a common operational picture, artificial intelligence, risk assessment and coordinated command and control.

The combined capabilities of Indochina Space, SkyVIV and NurjanaTech provide a practical implementation of this operational philosophy. By combining persistent three-dimensional digital twins, multi-sensor detection, AI-assisted sensor fusion, dynamic operational planning and integrated command and control, the solution enables operators to understand the operational environment, evaluate the consequences of alternative responses and coordinate the safest available course of action. Rather than replacing existing security investments, it enhances their effectiveness by providing the contextual awareness and decision support that individual systems cannot achieve independently.

The greatest lesson from Leipzig is that response time alone is not enough. Security organisations require decision superiority. They must understand what is happening, where it is happening, what is at risk and which response will minimise the total consequences of the incident. Achieving that level of understanding demands more than detection technology; it requires a continuously updated digital representation of the protected environment integrated with a common operational picture.

As drone technology continues to evolve towards greater autonomy, higher speeds, increased payloads and coordinated swarm operations, counter-UAS systems must evolve beyond isolated detection and mitigation technologies. Future resilience will depend on integrated operational ecosystems capable of fusing information from multiple sources, supporting human decision-makers with intelligent analysis and enabling coordinated action across security, law enforcement and infrastructure operators.

Ultimately, the objective is not simply to stop a drone. It is to protect lives, maintain the continuity of critical operations and ensure that every operational decision reduces overall risk. The organisations that succeed in achieving this will be those that transform counter-UAS from a collection of individual technologies into a unified operational capability.