

AI-Enhanced Video Analysis for C-UAS Protection of Borders and Critical National Infrastructure

A white paper written by Marco Capriz, Chief Technical Officer Indochina Space



Table of contents.

Abstract	3
The changing C-UAS problem.....	3
Why video analytics matters.....	4
Operational environments.....	5
Why EO/IR is a strong first layer.....	5
AI-enhanced tracking: reducing operator dependency	6
Multi-sensor fusion and the value of a single operational picture.....	7
C-UAS for borders: persistent detection and patrol cueing	7
CNI protection: awareness before escalation.....	8
Why active mitigation should not be the starting point	10
Recommended architecture for Thailand	10
Deployment concepts.....	11
Key performance measures	12
Conclusion.....	13

indochinaspace.com

Abstract

Small, unmanned aircraft systems have changed the security problem for borders, airports, ports, energy facilities, telecoms hubs, military sites, and other critical national infrastructure. We look at this issue in the context of a Thai reality, but the findings can be extrapolated to most countries with similar protection requirements.

A drone does not need to be large, expensive, or sophisticated to create operational disruption. It may be used for reconnaissance, smuggling, harassment, surveillance of security routines, delivery of contraband, or, in more hostile scenarios, as a carrier for a payload. The central problem for a country security and protection services is therefore not only how to defeat a drone, but how to detect it early, classify it correctly, track it continuously, and provide operators with enough evidence to decide what response is lawful, proportionate, and safe.

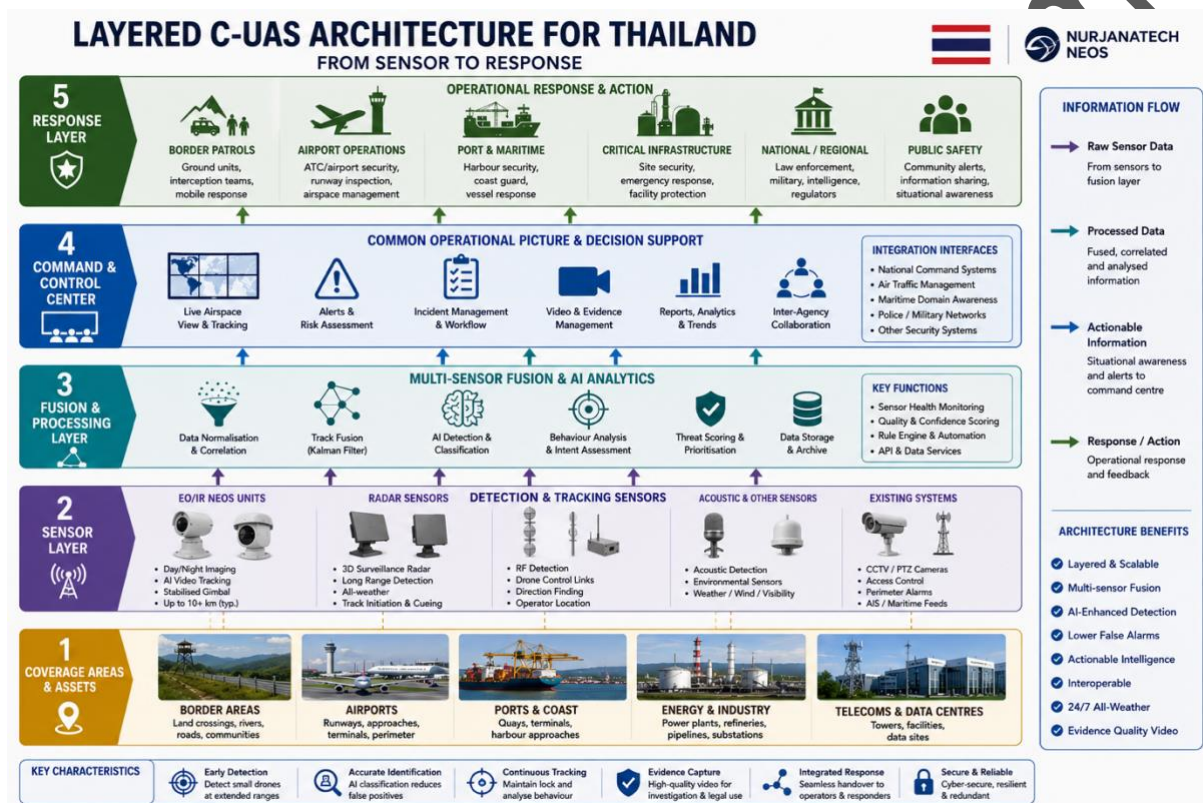


Figure 1: A proposed layered approach to C-UAS responses in Thailand.

AI-enhanced electro-optical and infrared video analysis is particularly well suited to this mission. NurjanaTech's NEOS architecture combines high-resolution EO/IR sensors, automatic video tracking, stabilised imaging, machine-learning-assisted object detection, and multi-sensor fusion. This provides persistent airspace awareness without the operational and regulatory complications that can accompany active mitigation systems, RF jamming, or kinetic interceptors. When integrated with radar, command-and-control systems, patrol units, and existing security infrastructure, NEOS can act as a practical C-UAS detection and decision-support layer for a country's border areas and critical national infrastructure. The result is earlier warning, better classification, improved evidence capture, and a lower-risk route to operational counter-drone capability.

The changing C-UAS problem

Counter-UAS is often presented as a problem of "stopping drones". That framing is incomplete. In most civil, border, and critical infrastructure environments, the first operational requirement is not neutralisation. It is reliable awareness.

A small drone can be difficult to detect because it has a limited radar cross-section, low acoustic signature, variable speed, and the ability to fly at low altitude against cluttered backgrounds. It can also operate at ranges that place the pilot outside the protected perimeter. This matters where border regions, airports, ports, energy sites, industrial estates, and telecoms facilities often include large open approaches, nearby communities, vegetation, mixed terrain, and public access routes.

The drone threat is not confined to military conflict. Recent reporting on global counter-drone demand points to increasing deployment around airports, oil fields, ports, and data centres, with civilian infrastructure protection becoming a major driver of C-UAS investment. Civil environments create a harder systems-engineering problem because detection, tracking, and response must operate without introducing unacceptable secondary hazards.

For most countries, this makes C-UAS a layered security problem. Border agencies need persistent observation over extended areas. Airport operators need early warning without interference with navigation and communications systems. Ports and energy sites need detection over water, perimeter roads, and industrial zones. Telecoms and data centres need protection against reconnaissance, sabotage preparation, and reputational disruption. In all cases, the preferred first layer is a system that can detect, identify, track, record, and communicate the threat clearly.

Why video analytics matters

Traditional CCTV is a passive recording tool. It helps after an event, but it does not reliably produce real-time airspace awareness. Human operators are poor at continuous visual search, especially when the target is small, distant, moving irregularly, or visible only intermittently. The operational burden becomes worse at night, in haze, in rain, or in cluttered backgrounds.

AI-enhanced video analysis changes the role of cameras. Instead of treating video as a display feed for a human to inspect, the system treats video as sensor data. The video stream can be processed continuously to detect candidate objects, track their motion, classify their behaviour, and alert operators when movement matches a defined threat profile. This is the technical distinction that matters: the value is not merely the camera, but the software layer that converts imagery into time-stamped, actionable observations.

NurjanaTech's NEOS system is described as a modular electro-optical tracking system able to detect and track fast-moving objects automatically. It combines high-resolution EO/IR sensors with AI-based trackers, stabilised video, real-time trajectory data, and integration with radar and telemetry systems for fused operational solutions. The system is also described as capable of maintaining tracking beyond 10 km for small UAVs, depending on configuration and environmental conditions.

This matters for C-UAS because a drone sighting is not operationally sufficient. A useful system must answer several questions quickly:

1. Is the object a drone, bird, aircraft, balloon, or visual artefact?
2. Where is it now, and where is it moving?
3. Is it approaching a protected zone?
4. Is it loitering, crossing a boundary, following a road, inspecting a facility, or moving away?
5. Can the event be recorded as evidence?
6. Can the track be handed to security forces, police, airport operations, or a command centre?

This is where AI-enhanced EO/IR analysis is strongest. It provides the classification and confirmation layer that radar alone cannot always supply, while avoiding sole dependence on human visual detection.

Operational environments

As we are based here, we look at Thailand as an example, but many other countries have similar geography and border protection necessities. Thailand's C-UAS requirements are not uniform. Border protection and CNL protection share the same basic threat technology, but their operating conditions differ.

Border areas require wide-area observation, rapid detection of low-altitude movement, and integration with mobile patrols. Drones may be used for route reconnaissance, smuggling, border probing, or observation of security posts. The challenge is persistence: a border segment may include forest, hills, roads, rivers, agricultural land, and villages. A system designed only for a clean perimeter will underperform.

Airports require a different logic. The operational priority is the safety of aircraft, passengers, and airside operations. The uploaded airport analysis correctly identifies that kinetic mitigation near runway environments may create unacceptable foreign object debris risk, while active RF systems may require careful electromagnetic compatibility analysis. It therefore argues for passive EO/IR detection and procedural response, including temporary airspace closure and safe-to-fly verification where necessary. CAAT, FAA, EAS and similar agencies that manage a country's airspace note that UAS detection and mitigation systems at airports require careful review of electromagnetic interference, legal authority, and operational response procedures.

Ports and coastal infrastructure require surveillance over water, quay areas, warehouses, fuel storage, navigation channels, and perimeter roads. Drones may be used to inspect security routines, identify cargo movements, monitor naval or coastguard activity, or approach fuel and logistics facilities.

Energy infrastructure, including power generation, substations, pipelines, gas facilities, and refineries, requires detection of reconnaissance and approach patterns. The same applies to telecoms hubs and data centres, where drones can support physical intrusion planning, payload delivery, or coercive disruption.

The common requirement is clear: Thailand needs systems that can produce reliable airspace awareness over varied terrain and infrastructure types, with evidence-quality video and a command-and-control interface.

Why EO/IR is a strong first layer

Radar is valuable in C-UAS because it can provide range, velocity, and angle measurement. It can perform wide-area detection in conditions where cameras may struggle. However, radar is not always sufficient for classification, evidential recording, and operator confidence. Small drones may be hard to distinguish from birds or clutter. Radar deployment can also raise site-specific questions around spectrum management and electromagnetic compatibility, especially at airports or sites with sensitive communications and navigation equipment.

EO/IR systems provide a complementary capability. Visible sensors can provide high-resolution imagery in daylight. Infrared sensors can support night operations and poor-visibility tracking. A stabilised gimbal can keep the target in the field of view, while the video tracker maintains lock and produces a continuous track. NurjanaTech provides this architecture in terms of image sensors, a positioning system, a control system, and a video tracker. It also notes that visible cameras are useful in good conditions, while IR cameras are more effective at longer range or where visibility is poor.

For C-UAS, this gives EO/IR four specific advantages.

1. First, it is passive. EO/IR sensors do not need to emit RF energy to observe the target, which reduces the risk of interfering with sensitive systems.
2. Second, it supports positive identification. Security operators need to know what they are seeing before escalating. Video evidence is also useful for incident review, prosecution, insurance, and regulatory reporting.

- Third, it supports behavioural analysis. A drone moving along a border road, circling a fuel tank farm, hovering near a runway approach, or repeatedly approaching a telecoms mast is not equivalent to a drone moving away from the protected zone.
- Fourth, it can be integrated with other sensors. EO/IR should not be seen as a replacement for radar or RF detection in all environments. Its strongest role is often as the confirmation, classification, and tracking layer in a multi-sensor architecture.

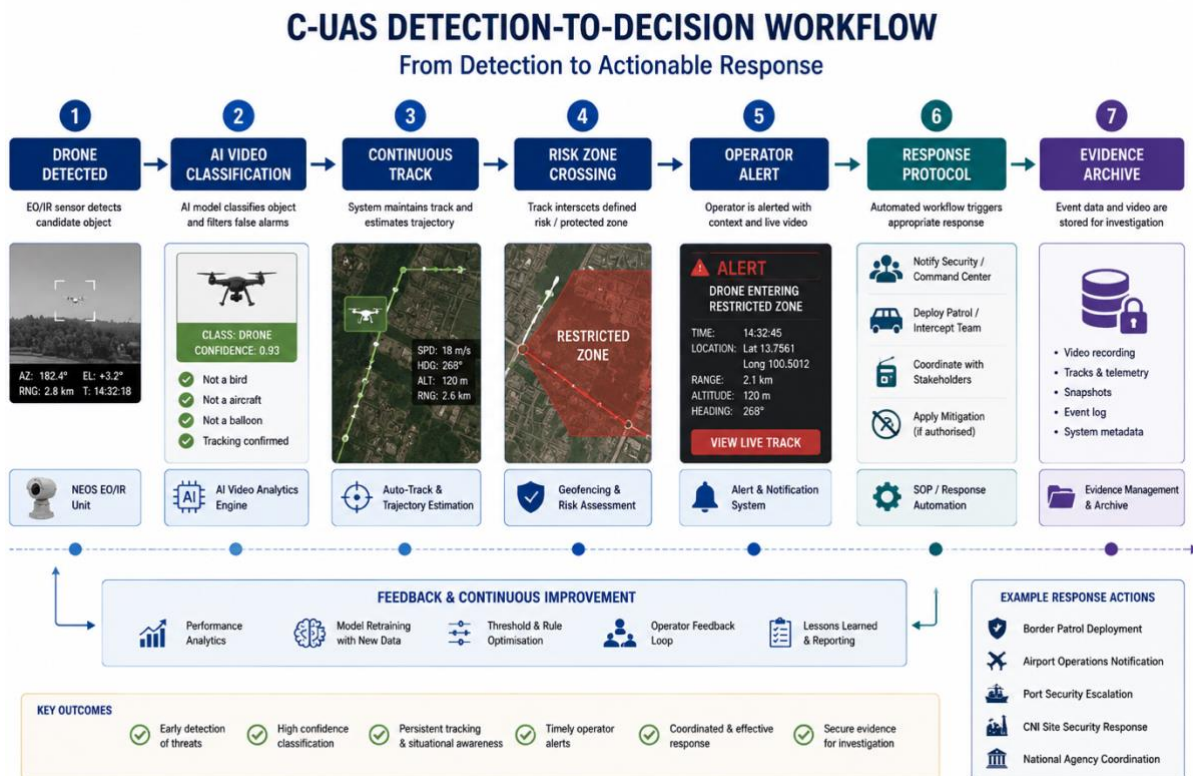


Figure 2: EO/IR detection and processing.

AI-enhanced tracking: reducing operator dependency

The technical problem is not only detecting a small airborne object. It is keeping that object inside the sensor's field of view long enough to understand what it is doing. This is difficult when the target is small, moving quickly, changing apparent size, crossing a cluttered background, or being observed from a moving or vibrating platform.

NurjanaTech's work on electro-optical tracking systems addresses two operator-dependent problems: automatic selection of the best video-tracking algorithm and automatic tuning of the control system that keeps the target centred in the field of view. The system uses deep and machine-learning strategies to select detection/tracking algorithms and control parameters automatically, reducing reliance on an experienced operator during live tracking.

This is operationally relevant for Thailand because C-UAS deployments cannot depend on a small number of expert operators at every border post, airport, port, industrial estate, or energy facility. A scalable system must help ordinary security teams perform at a higher technical level. The AI layer should support the operator by cueing attention, maintaining track, suppressing irrelevant motion, and escalating only when a target's behaviour matches operational rules.

In practical terms, this turns a C-UAS system from a collection of cameras into an operational

Multi-sensor fusion and the value of a single operational picture

No single sensor is ideal in all conditions. EO/IR can classify and record, but its performance depends on line of sight, weather, background, optics, and thermal contrast. Radar can detect movement and provide range but may produce false tracks or require classification support. RF detection may identify control links, but may fail against autonomous drones, pre-programmed routes, or non-standard communications. Acoustic detection may help at short range but is sensitive to environmental noise.

The correct architecture is therefore layered and fused. A radar may provide early cueing. EO/IR may confirm and track. RF sensors may identify the control channel or operator location. Existing CCTV may provide local context. Patrol units may provide ground verification. The command centre must then receive one coherent operational picture rather than several disconnected feeds.

NurjanaTech's data-fusion uses a Kalman-filter-based multi-sensor tracking algorithm that receives target information from radar and electro-optical sensors, weights the reliability of each sensor, and generates a better position estimate than individual sensors alone. In one scenario cited in the document, three radar inputs were fused to produce a lower mean error and higher accuracy than the individual sensors; in another, radar and optical sensors were fused while down-weighting a radar input with a large offset.

This principle is important for C-UAS because false alarms are not a trivial nuisance. Repeated false alerts can desensitise operators. At airports, false alerts can cause operational disruption. At borders, they can waste patrol resources. At energy sites, they can trigger unnecessary lockdowns. Fusion reduces the risk of treating one uncertain signal as operational truth.

C-UAS for borders: persistent detection and patrol cueing

In border security, the most valuable output of a C-UAS system may be not interception, but patrol cueing. A drone detected over a border area may indicate smuggling activity, reconnaissance, or probing. The operational response may involve tracking the aircraft, identifying its origin or landing point, dispatching a patrol, alerting nearby units, or preserving evidence.

AI-enhanced EO/IR systems are well matched to this task because they can create a persistent record of the drone's movement. A border operations centre can use this to answer practical questions: did the drone cross the border, did it hover above a particular site, did it return to a launch point, did it coordinate with ground vehicles, and did it appear repeatedly over several nights?

The deployment model should be modular. Fixed NEOS units could be positioned at high-risk crossing points, border bases, river approaches, or logistics corridors. Mobile units could be mounted on vehicles for temporary reinforcement, special operations, or response to intelligence-led threats. Where radar coverage exists, radar cueing can point the EO/IR system towards a candidate track. Where radar is unavailable or inappropriate, passive EO/IR can still provide a valuable detection and confirmation layer.

BORDER DEPLOYMENT MODEL – AI-ENHANCED C-UAS OPERATIONS

Fixed NEOS Towers, Mobile Units, Patrol Cueing and Drone Launch/Landing Estimation

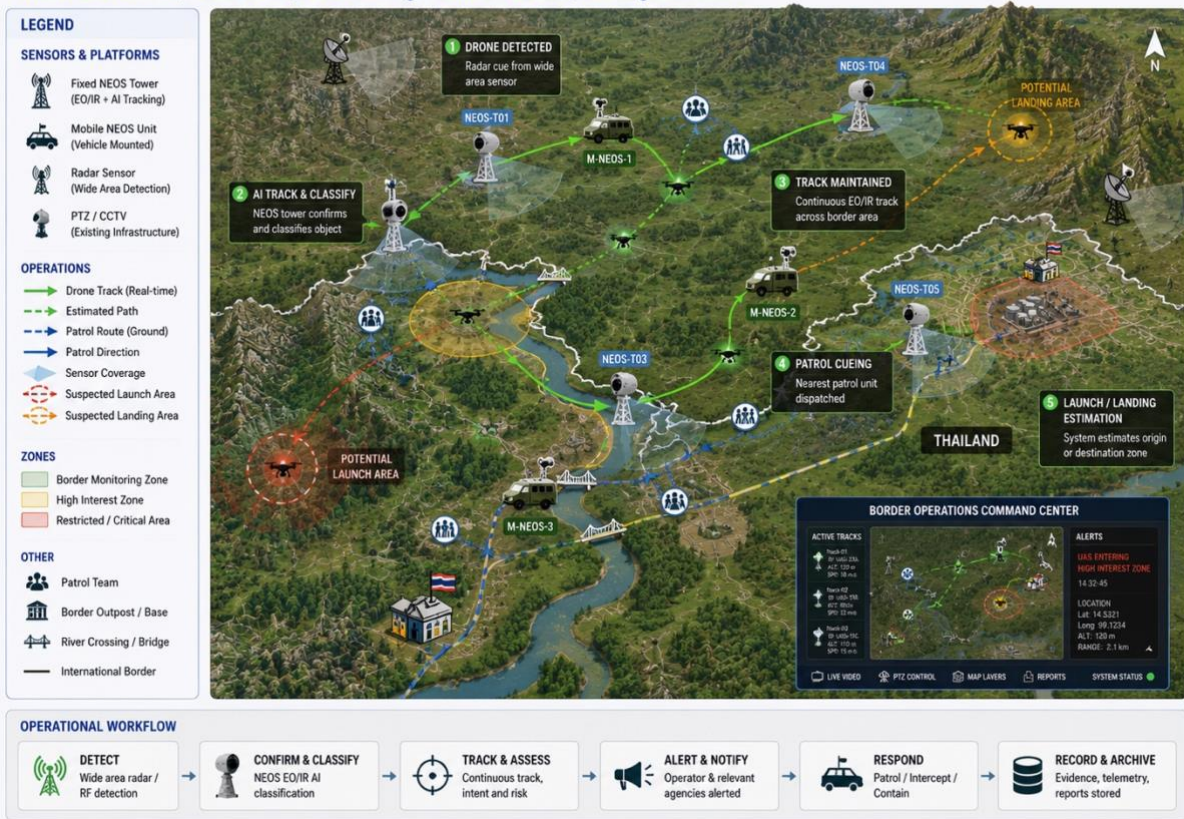


Figure 3: Detection and processing in border areas.

This is also where AI matters. Border monitoring involves long periods of normality interrupted by brief events. Automated detection reduces the probability that a small drone is missed because an operator was looking elsewhere, monitoring another camera, or working at night under fatigue.

CNI protection: awareness before escalation

Critical infrastructure operators generally do not need a military-style air defence system. They need a reliable method to know when an unauthorised drone enters a relevant volume of airspace, what the drone is doing, and whether the situation requires escalation to police, military, regulator, airport authority, or internal security.

This requires the protected site to be modelled in operational zones. A telecoms site may have a monitoring zone, a warning zone, and a critical overflight zone. An energy facility may define stand-off distances around tanks, substations, control rooms, pipelines, and access roads. A port may define zones around fuel storage, naval areas, customs facilities, and cranes. An airport must align zones with runway approaches, obstacle limitation surfaces, air traffic control procedures, and emergency plans.

CNI ZONE MODEL – PROTECTING CRITICAL NATIONAL INFRASTRUCTURE

Layered Protection Through Detection, Tracking and Escalation

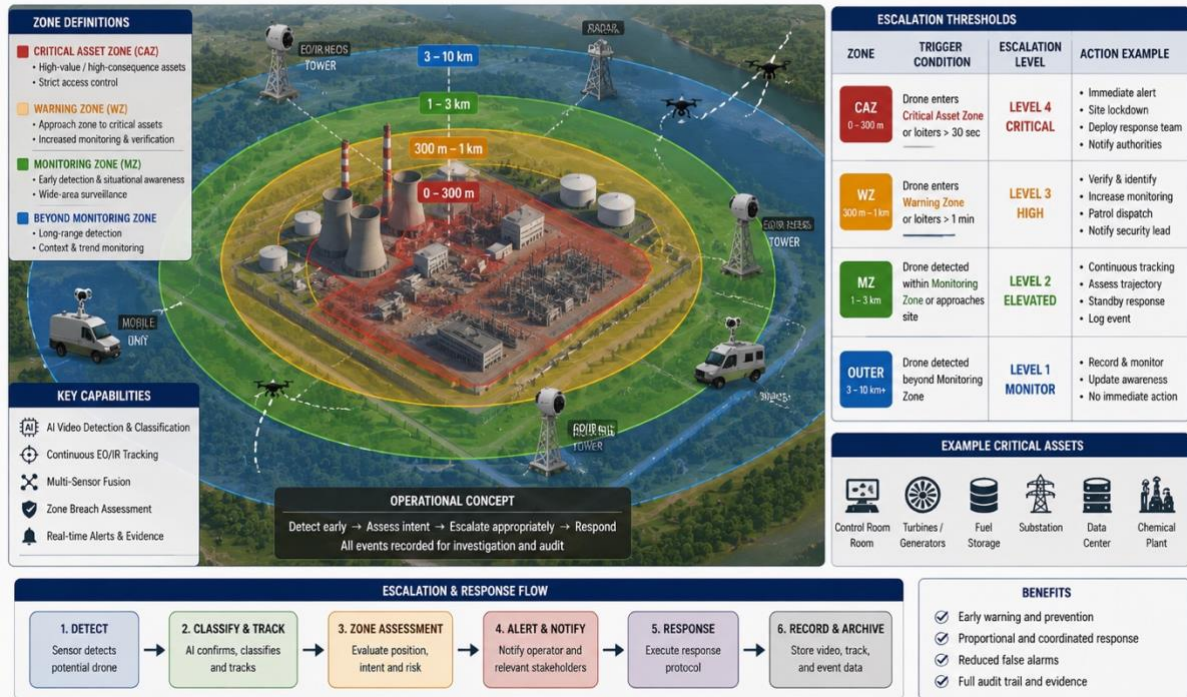


Figure 4: Layered response escalation for CNI protection.

AI-enhanced video analysis can support this by correlating the drone's track with protected zones. The system does not need to "decide" the response. It needs to present the operator with a reliable, time-stamped, visualised track and a recommended escalation level. This distinction matters because C-UAS response in civilian or mixed-use environments must remain under human command.

For airports, this detection-first approach is consistent with the uploaded Thai airport analysis, which recommends passive EO/IR detection and tiered response levels rather than immediate kinetic mitigation in regional airport environments. It also aligns with broader international caution around airport UAS detection and mitigation, where authorities highlight legal, electromagnetic, and aviation-safety considerations before deployment.



Figure 5: Airport intrusion management.

Why active mitigation should not be the starting point

There is a natural temptation to define C-UAS success as the physical defeat of the drone. For some military bases and battlefield environments, that may be appropriate. For civilian infrastructure, border areas near communities, airports, ports, fuel facilities, and dense industrial sites, active mitigation can create new risks.

Kinetic defeat may create falling debris. Net capture may introduce a second airborne system. RF jamming may interfere with legitimate systems and may require legal authority. Cyber takeover depends on drone type, link architecture, and encryption. Directed-energy systems have their own safety and regulatory constraints.

This does not mean mitigation has no role. It means detection, classification, tracking, and procedural response should be the foundation. Active defeat should be added only where the legal authority, safety case, electromagnetic compatibility, rules of engagement, and post-incident procedures are clear.

We argue for a phased model:

1. Phase 1: detection and alerting.
2. Phase 2: classification, tracking, and evidence recording.
3. Phase 3: integration with command-and-control and patrol response.
4. Phase 4: integration with authorised mitigation systems, where appropriate.
5. Phase 5: national or regional airspace-awareness network for border and CNI protection.
6. This pathway avoids purchasing “anti-drone” hardware before the operational picture is understood.

Recommended architecture for Thailand

A practical Thai architecture should be built around a layered sensor and decision-support model.

At the edge, EO/IR NEOS units would provide local detection, identification, tracking, and video evidence. These may be fixed, mobile, or hybrid depending on the site. Border posts and energy sites may use elevated fixed positions. Airports may use perimeter or approach-zone coverage. Ports may need mixed land and maritime views. Temporary event protection may require vehicle-mounted or containerised systems.

At the sensor-fusion layer, radar, RF detection, existing CCTV, access-control alarms, patrol reports, and EO/IR tracks should be combined. Sensor fusion should assign confidence values, remove duplicate tracks, and reduce false alarms.

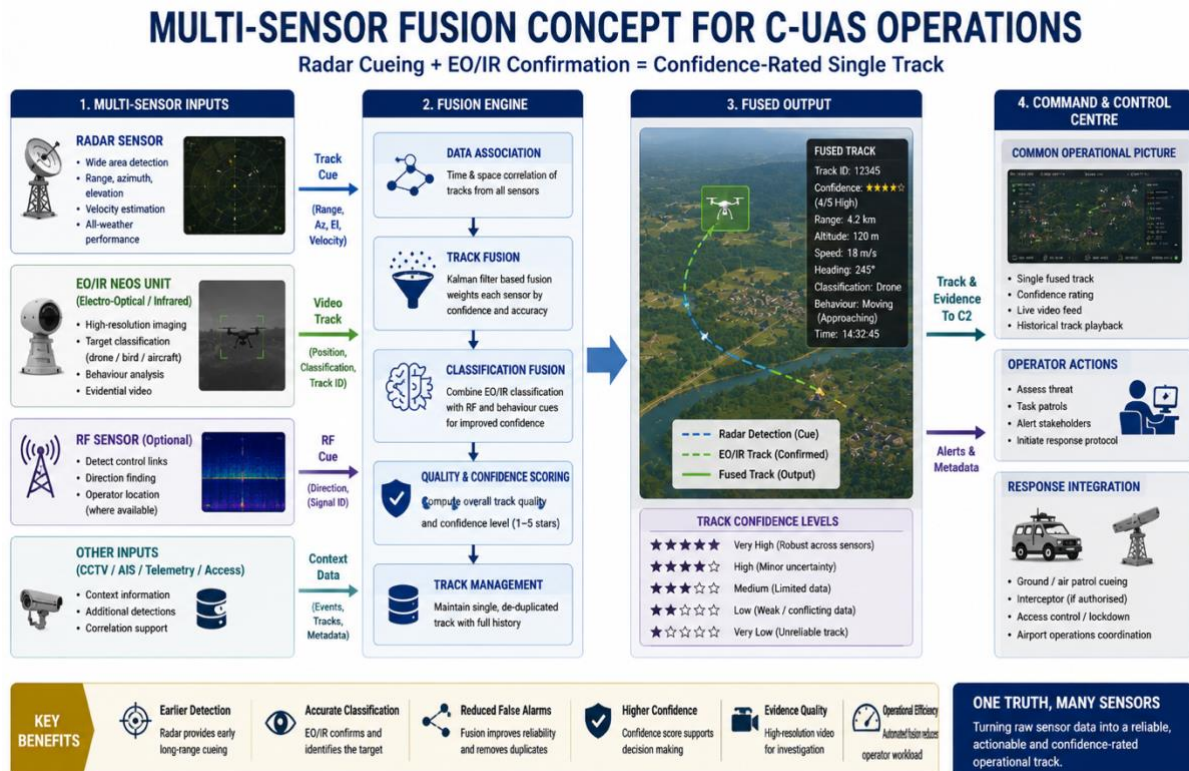


Figure 6: Sensor data fusion processing architecture.

At the command layer, operators should see a common operational picture: track location, heading, confidence, sensor source, video feed, protected-zone crossing, and recommended escalation level. Alerts should be prioritised by risk, not by raw detection count.

At the response layer, the system should trigger predefined procedures. For a border event, this may mean patrol cueing. For an airport, it may mean airside operations notification and defined safe-to-fly procedures. For a port, it may mean harbour security escalation. For an energy site, it may mean restricted-area lockdown and evidence capture.

NurjanaTech's existing materials position NEOS as modular and integrable with radars, command-and-control systems, and existing infrastructure. This is strategically important because Thai customers do not need to replace every existing system. They can add an AI-enhanced video analytics and tracking layer that improves what is already present.

Deployment concepts

For border protection, the recommended configuration is a mixed fixed-mobile network. Fixed NEOS units should cover known crossing points, high-risk river or road approaches, and border bases. Mobile units should reinforce

intelligence-led areas or temporary incidents. Where available, radar cueing should be used for wide-area detection, with NEOS providing classification and evidence.

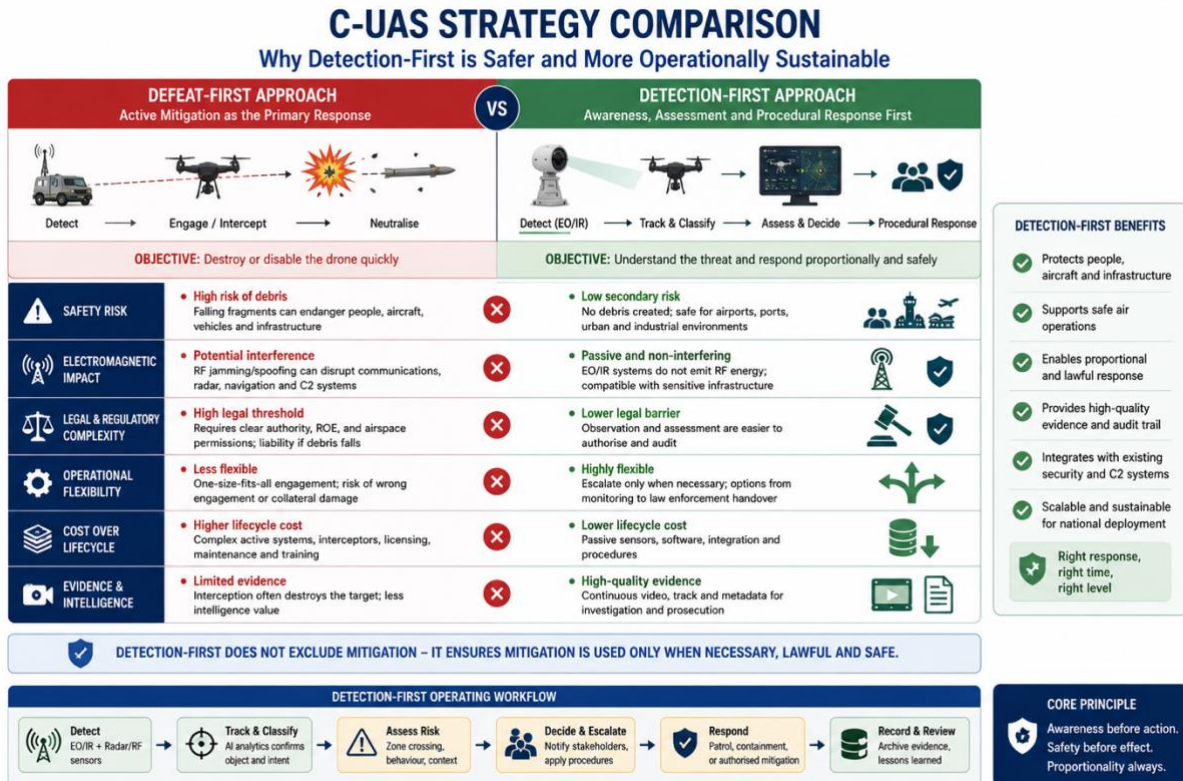


Figure 7: Defeat vs. detection and decision flow comparison.

For airports, the recommended configuration is a passive EO/IR-first architecture, potentially complemented by radar only after electromagnetic compatibility and regulatory analysis. The uploaded airport document estimates that a typical airport surveillance area may extend 9 km beyond the outer perimeter, covering approximately 450 km², and suggests that ~20 NEOS Small systems could provide coverage for the described airport model, subject to final lens, sensor, and connectivity design.

For ports and coastal infrastructure, the recommended configuration is a combined perimeter and waterside model. EO/IR units should monitor port approaches, fuel storage, restricted naval or customs areas, and access corridors. Radar or maritime surveillance feeds may provide cueing where available.

For energy and telecoms infrastructure, the recommended configuration is a zone-based model. NEOS units should be positioned to monitor approach corridors and high-value assets, with alerts linked to site security procedures. The priority is not only detection, but evidence-quality video that supports later investigation.

For national-level deployment, Thailand should consider a federated model. Individual sites retain local control, while national agencies receive selected alerts, metadata, and incident reports. This would allow trend analysis across borders, airports, ports, energy sites, and telecoms facilities without centralising every video feed.

Key performance measures

A Thai C-UAS pilot should be evaluated against operational metrics rather than sales claims. The minimum metrics should include detection probability, false-alarm rate, classification confidence, track continuity, time from detection to operator alert, handover quality to C2, evidential video quality, night performance, weather performance, and patrol response usefulness.

For airports, additional metrics should include compatibility with airside operations, safe-to-fly decision support, runway inspection workflow, and absence of harmful electromagnetic interference. For borders, metrics should include patrol cueing accuracy, launch/landing point estimation, and repeat-event correlation. For energy and telecoms sites, metrics should include zone-crossing accuracy and incident evidence quality.

The data-fusion materials also suggest the value of measuring fused-track accuracy against reference data, because a fused estimate may be more operationally useful than any individual sensor track.

Conclusion

A country's border and critical infrastructure security environment requires a C-UAS approach built on reliable airspace awareness, not on premature reliance on active defeat. Small drones are difficult targets, but the main operational problem is often more basic: seeing them early, knowing what they are, tracking what they do, and giving security operators a clear basis for action. AI-enhanced EO/IR video analysis is well suited to this requirement because it combines passive observation, automatic detection, continuous tracking, classification support, evidential video, and integration with other sensors and command systems.

NurjanaTech's NEOS capability fits this requirement because it is modular, sensor-fusion ready, and designed around automatic electro-optical tracking. For Thai borders, it can support persistent surveillance and patrol cueing. For airports, it can provide passive detection and safe operational decision support. For ports, energy sites, telecoms hubs, and other CNI, it can add a practical layer of aerial threat awareness without forcing customers into high-risk kinetic or RF-based mitigation at the outset. The strongest procurement logic is therefore phased: deploy detection and tracking first, integrate with command-and-control second, add authorised mitigation only where the legal, safety, and operational case is mature. That gives a scalable, technically defensible, and locally supportable path to counter-drone resilience.