Date: 2025-09-28

White paper: 9 principles for Effective CUAS procurement

Yes, drones are a threat, but panic procurement can be just as dangerous.

Across Denmark, and increasingly across Scandinavia, organizations are under pressure to strengthen their airspace awareness. The urgency is real. But acting too fast carries its own risks: buying systems that look good on paper but fail in practice can create noise, missed detections, operator overload, legal exposure, and wasted budgets.

From lessons learned in other countries and deployments, here are some principles worth weighing:

#1. Detection starts with radar and/or acoustic — RF alone is not enough

At today's risk level, with adversarial threats in play, detection must be based on technologies that see all drones, not just those transmitting signals. Radar and acoustic sensors provide that foundation: radar delivers precise localization in time and space, while acoustic fills gaps for small, low, or slow drones in cluttered environments.

Passive RF still has value; it can enrich the picture with classification data and help identify pilot locations, but by itself, it will miss autonomous or deliberately covert drones. That makes it a complement, not a substitute.

The right foundation depends on the site: large and complex facilities such as airports typically build around radar, while smaller sites such as utilities, datacenters, or prisons may rely more on acoustic, with RF layered in for added awareness.

- **Fusion matters more than any single sensor**.
  EO/IR imagery, analytics, and automated tracking only add value if radar cueing delivers enough pixels on target. Without that, analytics sees blur, and operators drown in nuisance alarms.

- **Automate, but keep human oversight**
  Automated classification and camera handoff are essential to track fast, maneuvering drones. But automation must be paired with human-in-the-loop controls, interlocks, and clear rules of engagement.

#2. Mitigation must be legal, safe, and realistic

Civilian users cannot rely on jamming. Options like high-intensity searchlights can improve night-time visual acquisition and act as a deterrent, but they:

- Don't affect thermal or autonomous systems
- Perform less well in poor weather
- Carry aviation and eye-safety risks

Any deployment must be paired with legal review, safety interlocks, ATC coordination, and insurance.

#3. Look for proven systems and integrators

In urgent procurement, prioritize solutions with operational track records, tested integrations, training, and support. Real-world validation reduces risk far more than flashy concepts.

#4. Demand a compliance & safety package

Ask suppliers to deliver rules of engagement templates, operator training, interagency coordination plans, and test results from controlled conditions.

#5. Think in layers, not silver bullets

A resilient CUAS system combines radar detection → EO/IR classification → automated tracking → safe mitigation options → law enforcement escalation. This layered approach minimizes false confidence.

#6. Start small, then scale

Consider beginning with a low-complexity detection system as a "*sandbox*." It gives individuals and teams a chance to learn workflows and responsibilities, *what to do, how, and who decides*, before scaling to advanced CUAS. Skipping this step often leads to expensive systems that cannot yet be operated effectively.

#7. Choose open, vendor-agnostic platforms

The drone threat is a moving target. What's considered best-in-class today may no longer be sufficient 12–24 months from procurement. A CUAS platform must be open by design, able to integrate sensors and effectors from different vendors in a true system-of-systems approach.

- This ensures you can evolve and adapt as threats change.
- It allows different levels of protection across multiple sites, from basic monitoring at less critical facilities to full multi-layered defense at priority assets.
- One-size-fits-all is not scalable, and proprietary lock-in risks leaving organizations with expensive but inflexible systems.

#8. Start with site surveys, don't buy blind

Every site is different. Terrain, clutter, critical zones, and even local weather all shape how CUAS technology will perform. What looks great on a datasheet or in a demo can behave very differently once deployed at an airport perimeter, an energy facility, or a city-center rooftop.

That's why professional site surveys are essential before procurement. A proper survey:

- Maps blind spots and clutter sources
- Tests how sensors behave in the real RF and visual environment
- Clarifies what level of protection is realistic at each site

Skipping this step increases the risk of investing in a system that fails to meet operational needs, the classic mistake of *buying blind*. By contrast, a modest upfront survey investment reduces risk, sets expectations, and ensures the system is tailored to the environment where it must actually work.

#9. Plan for interoperability and data sharing

Detection alone is not enough; the value lies in ensuring that the right people can act on the information in real time.

A CUAS platform should support secure, vendor-agnostic data sharing across multiple stakeholders: police, airport authorities, security companies, and perimeter guards on the ground.

In the defense world, standards like ATAK enable a common operating picture across units. Civilian end users should demand the same principle: open platforms that distribute sensor detections, classifications, and alerts seamlessly to all relevant teams.

Without interoperability, you risk siloed systems where one group sees the threat while others remain blind, slowing response and eroding trust in the system.

Bottom line: Decision-makers need confidence, not panic. A phased, layered, and legally compliant approach, starting simple and building capability, is the surest way to deliver real situational awareness and durable security.