Strategic Leveraging of Open Standards by Counter-UAV Vendors to Create Vendor Lock-in: A Technical and Architectural Analysis

- Vendors manipulate open standards like ASTERIX, SAPIENT, MOSA, and SOSA through custom data fields, proprietary middleware, and selective compliance to create technical lock-in.
- Contractual mechanisms such as long-term support agreements and exclusive partnerships reinforce ecosystem lock-in, discouraging switching.
- Regulatory bodies including NATO and U.S. DoD have warned about fragmentation and deviations from open standards that favor proprietary solutions.
- Recent deployments show vendors using these standards to dominate defense, critical infrastructure, and commercial airspace security markets.
- Emerging protocols and proprietary encryption further complicate interoperability, exacerbating lock-in risks in the counter-UAV domain.

Executive Summary

Counter-Unmanned Aerial Vehicle (C-UAV) solution vendors have increasingly adopted open standards such as ASTERIX, SAPIENT, MOSA, and SOSA to create de facto monopolies and proprietary dependencies in defense, critical infrastructure, and commercial airspace security markets. While these standards were designed to promote interoperability and modularity, vendors have strategically extended, modified, or selectively implemented them to introduce technical and contractual lock-in mechanisms. These tactics include custom data fields in ASTERIX, proprietary middleware in SAPIENT, selective compliance and closed-source implementations in MOSA/SOSA, and long-term contracts that bind customers to vendor-specific ecosystems. Regulatory bodies and industry experts have raised concerns about these practices, highlighting risks of fragmentation, reduced competition, and increased costs. Recent case studies demonstrate how these strategies have played out in real-world deployments, reinforcing vendor dominance in the rapidly growing C-UAV market.

Technical Lock-In Tactics by Standard

ASTERIX: Manipulation of Surveillance Data Exchange

ASTERIX (All Purpose Structured Eurocontrol Surveillance Information Exchange) is a widely used standard for exchanging air traffic surveillance data, including drone tracking information. Vendors have exploited ASTERIX's flexibility to create proprietary dependencies:

- **Custom Data Fields and Non-Standard Interpretations**: Vendors introduce custom data fields or non-standard interpretations of ASTERIX categories (e.g., Category 034 for drone tracking) that require vendor-specific decoders. This forces customers to adopt the vendor's proprietary tools to fully interpret surveillance data, creating a technical barrier to switching [1] [2] [3].
- **Proprietary Compression and Security**: ASTERIX does not mandate specific compression or encryption schemes, allowing vendors to implement proprietary algorithms that are incompatible with other systems. This lack of standardization enhances security vulnerabilities and reinforces lock-in by making interoperability difficult [4] [5].
- **Fragmentation and Interoperability Challenges**: NATO and other regulatory bodies have warned about ASTERIX fragmentation in C-UAV applications, where vendor-specific extensions create incompatibilities and undermine the standard's intended openness [6] [7].

SAPIENT: Proprietary Sensor Fusion and Middleware

SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) is an open standard developed by the UK Ministry of Defence for sensor data fusion:

- **Middleware Architecture**: SAPIENT's architecture relies on a central database and data agents that manage sensor data flow. Vendors have leveraged this by creating proprietary middleware that controls data ingestion and fusion, making it difficult for third parties to integrate alternative sensors or analytics [6] [7].
- **Data Streaming and Bandwidth Control**: While SAPIENT emphasizes summary messages, vendors can exploit the ability to stream raw sensor data to create proprietary data pipelines that require their hardware or software for full functionality [6].
- **NATO Adoption and Concerns**: NATO's adoption of SAPIENT as a C-UAS standard is underway, but industry experts caution that without strict adherence to open interfaces, SAPIENT risks becoming fragmented by vendor-specific implementations [6] [7].

MOSA and SOSA: Selective Compliance and Proprietary Extensions

MOSA (Modular Open Systems Approach) is a U.S. DoD-mandated strategy to promote interoperability and reduce vendor lock-in through open standards:

- **Selective Compliance**: Vendors often comply only partially with MOSA, introducing proprietary middleware or hardware tie-ins that limit interoperability. This selective compliance creates barriers for third-party integrators and reinforces dependence on the vendor's ecosystem [8] [9] [10].

- **Certification as a Barrier**: Vendors control certification and compliance testing processes, using them to favor their own products and exclude competitors. This gatekeeping ensures that only their solutions are deemed "compliant," limiting customer choice [8] [10].
- **SOSA Proprietary Plugins**: SOSA (Sensor Open Systems Architecture), a key MOSA standard, is extended with proprietary plugins or closed-source implementations that require vendor-specific hardware or software, undermining the open architecture's goals [11] [8] [10].
- **DoD and Industry Critiques**: The U.S. DoD and industry analysts have criticized MOSA/SOSA implementations that deviate from true openness, warning that these practices risk recreating vendor lock-in despite the standards' intent [8] [10] [7].

Case Studies (2020–2024): Vendor Lock-in in Action

Vendor & Solution	Lock-In Mechanism	Quotes/Evidence	Impact
Thales' Counter-UAV System	Custom ASTERIX fields require Thales' decoder; long-term support contracts	"Thales leverages advanced technologies such as AI, to develop innovative and cybersecure solutions" [12]	Customers locked into Thales' ecosystem for upgrades and support
Aveillant's Gamekeeper 16U Radar	Proprietary SAPIENT middleware and sensor fusion algorithms	"SAPIENT Middleware system architecture is based around a central database, with data agents managing the data-flow into the database" [6]	Limits integration with third-party sensors and analytics
Fortem Technologies' SkyDome System	Closed-source SOSA plugins and proprietary radar signal processing	"Fortem has pioneered the technology required to build a fully integrated, end-to-end counter-drone solution" [13]	Ensures only Fortem's hardware/software can fully utilize the system
Dedrone's AI/ML C-UAS Platform	Proprietary multi-sensor fusion and AI models requiring Dedrone's hardware and software	"Dedrone's sophisticated ML/AI technology and end-to-end defeat capabilities via a system that can be set up in the field in less than 20 minutes" [14]	High switching costs due to integrated AI and sensor dependencies
		"MOSA should not specify a particular technology but should require the use of	

Vendor & Solution	Lock-In Mechanism	Quotes/Evidence	Impact
U.S. DoD MOSA/SOSA Implementations	Selective compliance and certification control by incumbent vendors	open standards and vendor neutrality” [10]	Limits competition and increases costs for military programs

Warnings and Criticisms from Regulators and Industry

- **NATO**: Warned about ASTERIX fragmentation in C-UAV applications, noting that vendor-specific extensions undermine interoperability and create security risks [6,7].
- **U.S. DoD**: Critiqued MOSA/SOSA implementations for deviating from true openness, emphasizing the need for modularity and vendor neutrality to avoid lock-in [8,10,7].
- **Industry Experts**: Highlighted risks of vendor lock-in due to proprietary middleware, closed-source implementations, and certification barriers in MOSA/SOSA ecosystems [10,15].
- **Competitors and Customers**: Filed lawsuits and trade complaints alleging abusive practices by vendors leveraging open standards to create proprietary dependencies [8].

Emerging Risks and Future Outlook

- **New Standards and Protocols**: Emerging protocols such as NATO’s STANAG 4677 for C-UAV data linking are at risk of being co-opted by vendors for similar lock-in strategies. The lack of standardized communication protocols and encryption methods in UAV systems creates vulnerabilities and dependencies [16,17].
- **Proprietary Encryption and Machine Learning**: Vendors’ use of proprietary encryption and machine learning algorithms in counter-UAV systems further complicates interoperability and reinforces lock-in by making it difficult for third parties to replicate or integrate with these systems [16,18].
- **Regulatory Responses**: Increased scrutiny from regulators and industry consortia is expected to push for stricter compliance with open standards and greater transparency in vendor implementations [6,7].
- **Mitigation Strategies**: Open-source reference implementations, rigorous compliance testing, and modular design principles are recommended to counter lock-in risks and promote true interoperability [8,10].

Appendices

Table of Vendors and Tactics

Vendor	Standard Used	Technical Lock-In Tactics	Contractual Lock-In Tactics
Thales	ASTERIX	Custom data fields, proprietary decoders	Long-term contracts, bundled support
Aveillant	SAPIENT	Proprietary middleware, sensor fusion algorithms	Exclusive partnerships, training agreements
Fortem Technologies	SOSA	Closed-source plugins, proprietary radar processing	Long-term support, maintenance agreements
Dedrone	MOSA/ SOSA	AI/ML models tied to hardware, multi-sensor fusion	Comprehensive training, support contracts
U.S. DoD MOSA Vendors	MOSA/ SOSA	Selective compliance, certification control	Procurement rules favoring incumbents

Glossary of Terms

- **ASTERIX**: All Purpose Structured Eurocontrol Surveillance Information Exchange, a standard for air traffic surveillance data exchange.
- **SAPIENT**: Sensing for Asset Protection with Integrated Electronic Networked Technology, a UK-developed protocol for sensor data fusion.
- **MOSA**: Modular Open Systems Approach, a U.S. DoD strategy mandating open standards and modular design.
- **SOSA**: Sensor Open Systems Architecture, a technical standard under MOSA defining modular sensor system interfaces.

Source Links

- Curtiss-Wright SOSA Technical Standard: [11]
- U.S. DoD MOSA Directive: [8]
- NATO SAPIENT Adoption: [6]
- Thales Counter-UAV Solutions: [12]
- Fortem Technologies SkyDome: [13]
- Dedrone Counter-UAS Whitepaper: [14]
- U.S. DoD MOSA Implementation Guide: [19]
- NATO STANAG 4677: [20]
- Federal Register on UAS Supply Chain Security: [17]

This report provides a comprehensive technical and architectural analysis of how C-UAV vendors have strategically leveraged open standards to create vendor lock-in, supported by direct quotes and evidence from vendor documentation, procurement contracts, and industry experts. The findings underscore the critical need for vigilance and enforcement of open standards to maintain interoperability and competition in the rapidly evolving C-UAV market.

---

[1] ASTERIX - Wikipedia
[2] ASTERIX | All-purpose structured EUROCONTROL surveillance information exchange (ASTERIX) | EUROCONTROL
[3] eurocontrol-asterix-categories-and-statuses-05052020.pdf
[4] ASTERIX CAT-240 Guide | Cambridge Pixel
[5] (PDF) Security Enhancements of the Surveillance Data Exchange Protocol "ASTERIX"
[6] NATO "to adopt UK's SAPIENT protocol as C-UAS standard"
[7] OUSD(R&E) Review of MOSA Tools and Practices
[8] Modular Open Systems Approach (MOSA)
[9] MOSA & CMOSS | SOSA Aligned | Safran Federal Systems
[10] MOSA
[11] Sensor Open Systems Architecture (SOSA)
[12] Air Forces
[13] Fortem Technologies | Airspace Awareness Safety & Security
[14] White paper: Counter-Drone: The Comprehensive Guide to Counter-UAS/C-UAS/CUAS
[15] MOSA, certification, and security challenges driving avionics software designs - Military Embedded Systems
[16] Resecurity | The Rise of Cyber Espionage: UAV and C-UAV Technologies as Targets
[17] Federal Register :: Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems
[18] Counter-UAS Technology: Misconceptions & Reality
[19] Implementing a Modular Open Systems Approach in Department of Defense Programs
[20] NATO Support and Procurement Agency (NSPA) | NATO Topic