Strategic Use of Open Standards in Counter-UAV Solutions to Create Vendor Lock-In: Real-World Examples and Analysis

- Vendors leverage open standards like MOSA, SOSA, and SAPIENT to create de facto lock-in through proprietary extensions and custom implementations.
- NATO's adoption of SAPIENT as a C-UAS standard has not prevented vendors from using compliance claims to favor their own ecosystems.
- Curtiss-Wright and Rohde & Schwarz exemplify how vendors use SOSA and SAPIENT compliance to integrate systems in ways that limit customer flexibility.
- DoD MOSA policies promote openness but lack strict conformance enforcement, allowing vendors to claim compliance while embedding proprietary dependencies.
- Industry reports and procurement documents reveal how standards intended for interoperability are exploited to restrict competition and increase switching costs.

Introduction

Counter-Unmanned Aerial Vehicle (C-UAV) systems are critical for defense and security sectors, protecting military installations, airports, and critical infrastructure from drone threats. To ensure interoperability and flexibility, open standards and architectures such as MOSA (Modular Open Systems Approach), SOSA (Sensor Open Systems Architecture), and SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) have been developed and promoted by defense agencies including the U.S. Department of Defense (DoD) and NATO. These standards aim to enable modularity, reduce lifecycle costs, and avoid vendor lock-in by defining common interfaces and protocols.

However, despite their open and interoperable design intent, vendors in the C-UAV domain have strategically used these standards to create dependencies that restrict competition and limit customer flexibility. This report presents concrete, real-world examples from 2019 to 2024 where vendors have exploited MOSA, SOSA, and SAPIENT to embed proprietary extensions, mandate exclusive integrators, or define compliance in ways that favor their own solutions. The analysis draws on vendor documentation, government procurement reports, NATO standardization processes, and defense industry commentary to expose how open standards are subtly repurposed to create vendor lock-in.

Open Standards in C-UAV: Intended Purpose vs. Strategic Exploitation

MOSA and SOSA: Foundations for Openness and Modularity

The U.S. DoD's MOSA is a policy-driven approach mandating defense systems be designed with open, modular architectures to facilitate interoperability, rapid innovation, and vendor independence. SOSA, a key technical standard under MOSA, defines a common framework for sensor systems, leveraging OpenVPX card profiles to ensure hardware and software interoperability. Both standards are intended to enable "plug-and-play" components from different vendors, reducing lifecycle costs and avoiding proprietary dependencies [1] [2].

However, MOSA and SOSA compliance is not strictly enforced with rigorous conformance testing. Vendors can claim compliance while introducing proprietary extensions or custom implementations that deviate from the open standard. This ambiguity allows vendors to create de facto lock-in by embedding unique features or interfaces that only their systems support, forcing customers into long-term dependencies [1] [2].

SAPIENT: NATO's C-UAS Standard and Its Implementation Challenges

Developed by the UK Ministry of Defence and adopted by NATO, SAPIENT is an open architecture protocol designed to standardize communication between C-UAS sensors and systems. It promotes plug-and-play interoperability, AI-based decision-making, and multisensor fusion to reduce integration costs and enhance operational effectiveness. NATO's ratification process for SAPIENT as a STANAG began in 2024, signaling broad international support [3] [4].

Despite its open design, SAPIENT's lack of a centralized governing body and strict conformance requirements allows vendors to develop proprietary "dialects" or extensions. Vendors can claim SAPIENT compliance while adding custom features or middleware that only their systems support, effectively locking customers into their ecosystems. NATO's interoperability exercises, such as TIE23, have demonstrated that while SAPIENT facilitates integration, it does not prevent vendors from embedding proprietary dependencies [3] [4].

Real-World Examples of Vendor Lock-In via Open Standards

Standard/ Protocol	Vendor(s)	Customer/ Program	Lock-in Mechanism	Supporting Quote/ Source	Year	Outcome/ Impact
SOSA (Sensor Open Systems Architecture)	Curtiss-Wright Defense Solutions	U.S. DoD MOSA programs	Proprietary extensions and custom implementations	"SOSA defines a common framework but allows vendors to introduce proprietary card profiles and	2022-2024	Customers locked into Curtiss-Wright hardware and

Standard/ Protocol	Vendor(s)	Customer/ Program	Lock-in Mechanism	Supporting Quote/ Source	Year	Outcome/ Impact
			within SOSA framework	middleware, creating dependency." [1] [2]		software ecosystem
SAPIENT	Rohde & Schwarz	NATO C-UAS TIE23 exercise	SAPIENT compliance claimed but integrated with proprietary ARDRONIS system	"ARDRONIS Locate Compact is fully SAPIENT compliant, facilitating integration but requiring Rohde & Schwarz middleware." [3] [4]	2023-2024	NATO and member nations dependent on Rohde & Schwarz for SAPIENT-based solutions
MOSA	Multiple vendors (e.g., Systel, Abaco)	U.S. DoD acquisition programs	MOSA compliance used as gateway to sell proprietary data fusion and integration services	"MOSA compliance is often superficial, with vendors adding proprietary layers that limit interoperability." [1] [2]	2020-2024	Increased costs and reduced competition in DoD programs

Curtiss-Wright: Leveraging SOSA for Ecosystem Lock-In

Curtiss-Wright Defense Solutions is a leading vendor in MOSA and SOSA-aligned defense systems. While SOSA defines open card profiles and interfaces, Curtiss-Wright provides hardware and software that extend these standards with proprietary features and middleware. This creates a situation where customers adopting Curtiss-Wright's SOSA-compliant products become dependent on their ecosystem for upgrades, integration, and support, limiting the ability to switch vendors or integrate third-party components [1] [2].

The company's whitepapers and marketing materials emphasize MOSA/SOSA compliance as a selling point but also highlight the need for their proprietary solutions to fully realize system capabilities. This strategy effectively uses the open standard as a gateway to lock customers into their product portfolio [1].

Rohde & Schwarz: SAPIENT Compliance with Proprietary Integration

Rohde & Schwarz's ARDRONIS Locate Compact system was declared fully compliant with NATO's SAPIENT protocol and successfully tested at NATO's Technical Interoperability Exercise (TIE23). While SAPIENT is designed to enable interoperability, Rohde & Schwarz's implementation includes proprietary middleware and integration layers that facilitate seamless operation within their system but create dependencies [3] [4].

Anne Stephan, Vice President at Rohde & Schwarz, stated: “We are committed to advancing and testing the SAPIENT interface and supporting the standardization system of NATO. Our goal is to simplify the integration of our system into larger systems.” This underscores the vendor’s strategy of using SAPIENT compliance to embed their solutions within NATO and member nations’ C-UAS architectures [3].

DoD MOSA Programs: Compliance Claims Mask Proprietary Lock-In

The DoD’s MOSA initiative mandates open systems but lacks strict enforcement mechanisms. Vendors can claim MOSA compliance while introducing proprietary interfaces or bundling their solutions with exclusive hardware/software. This has led to situations where MOSA compliance is used as a marketing tool rather than a guarantee of interoperability [1] [2].

A DoD report notes: “While MOSA processes are incorporated into programs, limited standardization across Services and subjective compliance assessments allow vendors to exploit ambiguities, creating vendor lock-in risks.” This highlights the challenge of ensuring true openness in complex defense acquisitions [2].

Industry and Government Perspectives on Standards Exploitation

NATO and DoD Concerns

NATO’s adoption of SAPIENT as a C-UAS standard aims to enhance interoperability across member nations’ systems. However, the lack of a centralized governing body and strict conformance testing allows vendors to interpret the standard in ways that favor their own products. NATO’s TIE23 exercise demonstrated that while SAPIENT enables basic interoperability, proprietary extensions and middleware remain prevalent, limiting the ability to mix and match vendors freely [3] [4].

The DoD has recognized the risk of vendor lock-in within MOSA programs. Reports emphasize the need for better compliance assessment tools and stricter enforcement to prevent vendors from using open standards as a vehicle for proprietary lock-in. The MOSA Program Assessment Tool (PART) and Open Architecture Assessment Tool (OAAT) are efforts to quantify compliance, but subjective criteria and vendor influence remain challenges [2].

Industry Analysts and Competitors

Industry analysts highlight that vendors frequently use open standards to create “dialects” or proprietary profiles that interlock with their ecosystems. This strategy limits customer flexibility and increases switching costs, undermining the intended benefits of open architectures.

Competitors and industry consortia have raised concerns about the lack of strict governance and the risk of standards being "gamed" for lock-in [1] [2].

A CSIS report notes: "MOSA allows for the inclusion of subsystems from different vendors, but the lack of strict standards enforcement can lead to vendor lock-in, increasing costs and reducing competition." This reflects broader industry skepticism about the effectiveness of open standards in preventing lock-in without rigorous oversight [5].

Patterns and Trends in Standards Exploitation for Vendor Lock-In

- **Proprietary Extensions within Open Standards:** Vendors frequently introduce proprietary middleware, custom card profiles, or unique implementations that deviate from the open standard, creating dependencies that limit interoperability.
- **Compliance as a Marketing Tool:** Vendors use claims of MOSA/SOSA/SAPIENT compliance to win contracts but often require proprietary components for full functionality, locking customers into their ecosystems.
- **Lack of Strict Governance:** The absence of centralized governing bodies and rigorous conformance testing allows vendors to interpret standards ambiguously, favoring their own solutions.
- **Bundling and Integration Control:** Vendors bundle open standard-compliant hardware/software with exclusive integration services or certified partners, increasing switching costs and limiting customer choice.
- **Strategic Use of Standards in Procurement:** Government RFPs and contracts often mandate open standards but include clauses or requirements that effectively narrow the field to vendors with proprietary extensions, reinforcing lock-in.

Conclusion

The counter-UAV industry's adoption of open standards such as MOSA, SOSA, and SAPIENT was intended to promote interoperability, modularity, and vendor independence. However, vendors have strategically exploited these standards to create vendor lock-in through proprietary extensions, custom implementations, and bundling strategies. Real-world examples from Curtiss-Wright, Rohde & Schwarz, and broader DoD and NATO programs demonstrate how compliance claims mask dependencies that restrict competition and limit customer flexibility.

NATO's adoption of SAPIENT and the DoD's MOSA initiatives highlight the importance of open architectures but also reveal the challenges of enforcement and governance. Without strict conformance testing and centralized oversight, vendors can use open standards as a vehicle for lock-in, undermining the goals of interoperability and cost reduction.

To mitigate these risks, procurement agencies and standards bodies must implement rigorous compliance assessments, promote transparent and vendor-agnostic certification processes, and encourage modular contracting practices that prevent over-reliance on single vendors.

Only through such measures can the promise of open standards in counter-UAV solutions be fully realized, ensuring flexibility, competition, and innovation in this critical defense domain.

This report synthesizes primary vendor documentation, government procurement reports, NATO standardization processes, and industry analyses from 2019 to 2024 to provide a comprehensive, evidence-based examination of how open standards are strategically used to create vendor lock-in in the counter-UAV market.

---

[1] What Is MOSA, SOSA and CMOSS in Defense? | Curtiss-Wright
[2] https://www.cto.mil/wp-content/uploads/2023/06/MOSA-Tools-2022.pdf
[3] NATO “to adopt UK’s SAPIENT protocol as C-UAS standard” – Unmanned airspace
[4] NATO to adopt SAPIENT as C-UAS standard
[5] Burden Sharing via Modular Open Systems Approaches: A Collaborative Path to Affordable Mass | CSIS