

Unlocking Interoperability: The Promise of the SOSA Standard



Several US Army organizations have been embracing the C5ISR/EW Modular Open Suite of Standards (CMOSS) under the SOSA flag. Earlier this year, Program Executive Office Command, Control, Communications, and Network (PEO C3N) established a new program office, Product Manager CMOSS Mounted Form Factor (PdM CMFF), as part of its Mission Command portfolio. In addition, Project Manager Positioning, Navigation, and Timing (PM PNT) is soliciting proposals for its CMFF APNT Block II Card effort. Also, Project Manager Tactical Radios has requested White Papers for a number of CMOSS-compliant technologies, including an SDR card to support SINGARS, WREN TSM, ATC (VHF/UHF LOS AM/FM) waveform applications and digital radioheads. | US ARMY PHOTO

By Barry Manz

FOR DECADES, THE defense electronics industry has relied on closed, proprietary ecosystems. Most of these EW, SIGINT, radar and communications systems were custom-built, platform-specific and often developed by a single contractor; they were designed for peak performance on a particular model of aircraft, ship, satellite or vehicle. They were extremely costly to upgrade and difficult to integrate with other systems built by other companies, even within the same platform or chassis, without a complete redesign. Although this approach has worked reasonably well for many years, it has proven inflexible in an era of accelerating technological change. Development of the Sensor Open Systems Architecture (SOSA) standard, which is still in progress, has the potential to do away with this archaic technology paradigm.

The Department of Defense (DOD) has long pushed for open architecture approaches. It began exploring open standards in the 1990s, mainly in response to escalating system costs, lengthy development timelines, and the increasing obsolescence of stove-piped systems populated with proprietary technologies. Early efforts focused on enabling modularity and interoperability to improve system sustainability and reduce vendor lock-in.

One of the first major initiatives was the Open Systems Architecture (OSA) approach, promoted by the Navy in the late 1990s and early 2000s. It emphasized using commercial off-the-shelf (COTS) components and defined interfaces to support modular design. This was followed by broader DOD adoption under the Modular Open Systems Approach (MOSA), which became formalized in acquisition guidance and policy documents.

In the 2010s, MOSA gained traction with efforts such as the Army's CMOSS (C5ISR/EW Modular Open Suite of Standards), the Navy's Integrated Topside (InTop) initiative, and the Air Force's OSA Implementation Guide. In 2019, MOSA was formally mandated by the US Congress and the DOD, requiring all new defense programs to be designed using a modular open systems

approach “to the maximum extent practicable.” This cemented open standards as a foundational requirement for modern US defense acquisition. These initiatives aim to foster rapid development, enable faster technology refresh, and ensure critical systems can be adapted across platforms and vendors.

The Defense Standardization Program and Open Systems Joint Task Force (OSJTF) further institutionalized the approach across the services, promoting standards like VME and OpenVPX and later software-focused frameworks like the Future Airborne Capability Environment (FACE). These efforts culminated in the SOSA Consortium, managed by The Open Group. The consortium aimed to unify sensor processing architectures under one umbrella using aligned hardware and software profiles.

So What Is An “Open” System?

In defense industry parlance, an open system represents a technology architecture prioritizing interoperability and flexibility. It emphasizes creating systems with standardized interfaces that can communicate across different platforms and manufacturers. The core principle is to design technology that allows easy communication, as well as replacement and upgrading of components without requiring a complete system redesign.

An open architecture uses well-defined, non-proprietary interfaces and modular components, allowing different systems – hardware and software alike – to communicate, interoperate, and evolve more freely. This approach helps to reduce vendor “lock in” by creating modular frameworks through which a system can use any company’s product as long as it meets a given set of open standards. If another vendor develops a better compliant solution later on, such as an ADC module for example, this new capability can be more easily integrated into the system via open standards. This approach is particularly valuable in military technology contexts, where

complex equipment, such as radars, radios and EW systems, must remain adaptable over decades of potential use.

The strategic advantages of an open systems approach include lower long-term maintenance costs, faster technology insertion, enhanced scalability and, ultimately, improved operational capabilities across different military branches or even across a coalition of forces. It transforms defense acquisition from a rigid, monolithic process into a flexible, iterative model more aligned with commercial technology cycles.

“Striking the right balance in the open standards space is challenging,” says Justin Moll, Vice President, Sales and Marketing at Pixus Technologies. “On one hand, you want maximum compatibility and interoperability; on the other, you need enough flexibility to support creative new designs. The SOSA team is very aware of that tension. They understand the importance of innovation and are working to ensure the standard supports both consistency and forward-looking design freedom.”

SOSA

Today, eight major DOD initiatives – electronic warfare to RF systems, mission computing, and command and control – are built on open standards. Many of these efforts interconnect with broader frameworks such as CMOSS, VICTORY, FACE, and HOST, creating a DOD-wide shift toward modular, interoperable system design. SOSA is one of the most ambitious and influential of these initiatives. Developed with significant input from the Army, Navy, Air Force, and industry, SOSA provides a common framework for creating interoperable, reusable, and upgradeable sensor processing systems. It incorporates standards like OpenVPX for hardware and FACE for software while introducing detailed profiles and definitions specific to sensor and EW systems.

Acquisition policies and funding mandates will ultimately favor MOSA compliance. As Rodger Hosking, co-founder of Pentek (now part of Mercury Systems), notes, "The government will favor bids that have SOSA-based content. They're doing that because it reduces the total cost of ownership, as you're using more standardization for the components on the boards and chassis."

"In the past," explains Steven Edwards, Director of Secure Embedded Solutions at Curtiss-Wright, "there were specific pins that everybody had to use, but there also were leftover pins that a company could use for its purposes. One of the goals of SOSA was to eliminate that possibility, and they did that by defining profiles. So, if you define a board that matches the profile, it's possible to assemble a system with boards from multiple vendors that work together."

Hosking agrees, emphasizing how SOSA simplifies future upgrades. "Even if you stay with the same vendor," he says, "if it follows the SOSA standards, the next generation of technology insertion will be much easier. That means you won't have to start from scratch every time you want to add something new, which is how it has been since I've been in this business."

Conformance involves ensuring that a design aligns with the SOSA technical profiles, and certification is the formal verification that the design meets those requirements through rigorous third-party testing. However, the question remains how much this process will cost manufacturers. "Every product will undergo conformance testing," says Edwards. "That could be millions of dollars. We're all waiting to see exactly how the verification process will work when independent verification labs are set up. Then we'll see what the pricing looks like."

Hardware rather than software development has been fastest under SOSA, thanks partly to the foundation provided by the

VITA standards. “The hardware momentum is proceeding nicely,” says Edwards, “It’s had a solid starting point with VITA, and even though SOSA is driving back into VITA now, from a hardware perspective I think all of the required elements are fairly well defined.”

“It’s important to remember that SOSA is still finalizing its technical standard,” Edwards explains. “Although the standard itself has been published, the associated performance specifications are only now beginning to be released, which means no vendor can currently claim full compliance with the SOSA technical standard because the verification criteria are still being defined.”

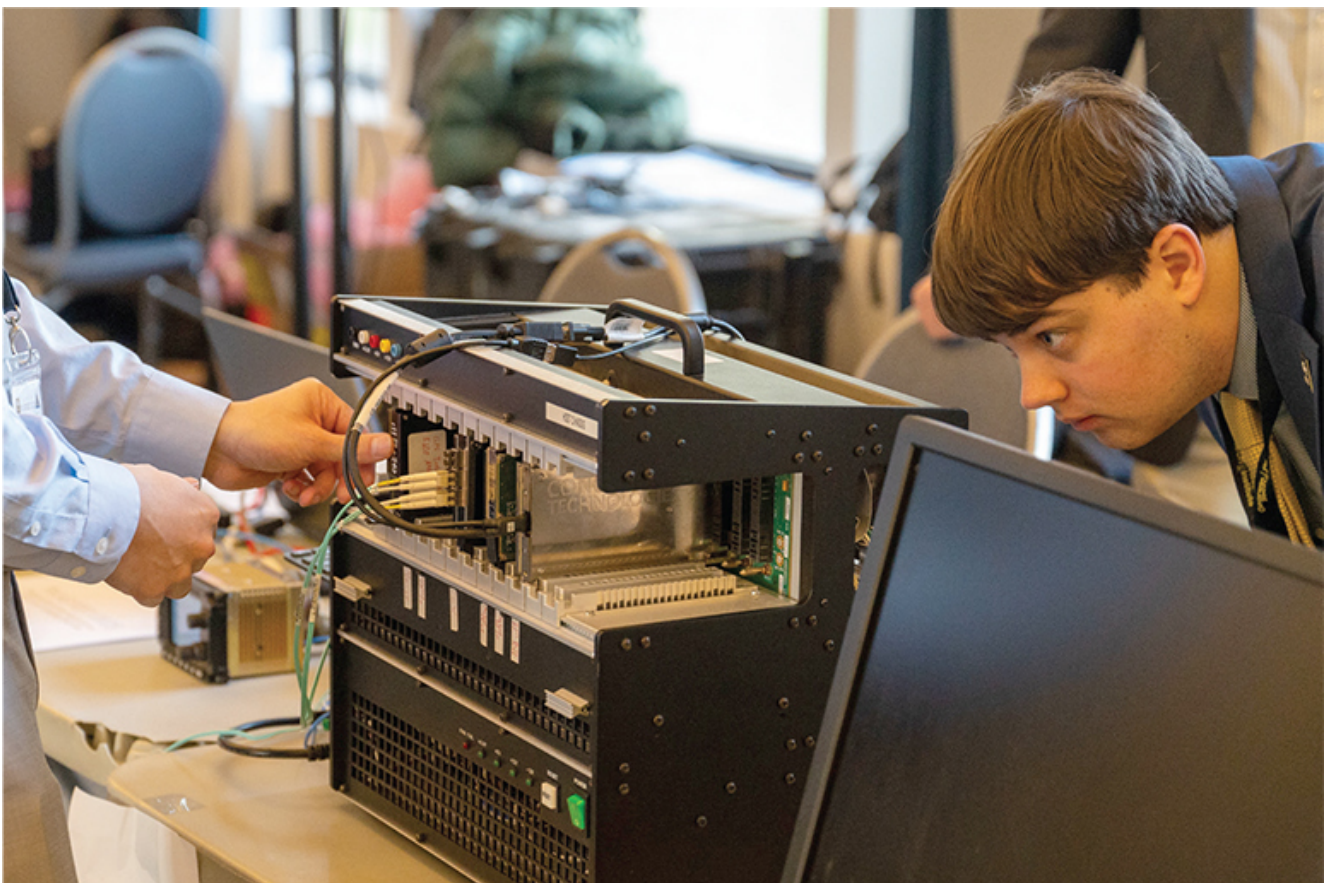
Once the performance specifications are finalized, any company developing a 3U module or hardware to meet a specific SOSA profile must undergo an independent verification process. SOSA is establishing a formal verification authority to handle this, although specific verification facilities have yet to be announced. When that process is complete and the module is approved, the vendor’s product can be listed by the SOSA Consortium as fully conformant.

In the meantime, since complete verification isn’t yet available, companies can state that their products are “SOSA aligned,” which is the only term allowed by the consortium to indicate that a product is being developed with the intent to meet SOSA standards fully. While a manufacturer could find its own test facility today to perform the testing required to confirm a product’s compliance with SOSA, it doesn’t make much sense because the company could wind up paying more now than it would when SOSA is finalized and there are more approved facilities.

Legacy system integration remains a challenge because many existing programs have selected proprietary architectures in the past that are incompatible with SOSA. Transitioning these systems requires adapter cards, protocol converters, or, in

some cases, total subsystem redesign. Nonetheless, OEMs are aligning product roadmaps with SOSA. Backplanes, embedded computing platforms, and full sensor processing modules are being revised to meet SOSA profiles, and prime contractors are investing in internal qualification programs to vet third-party components for SOSA alignment.

In addition, SOSA has created an environment for developing new tools to support SOSA-specific testing, including backplane emulation, automated compliance test suites and reference designs. Universities and research institutions also contribute by developing simulation platforms, educational curricula and rapid prototyping environments to help engineers and integrators understand and implement SOSA-based systems.



In February, the 9th Reconnaissance Wing at Beale AFB, Calif., hosted a PlugFest event where more than two dozen industry partners demonstrated their SOSA-aligned modules and chassis for various DOD organizations. The event, which was supported by Air Combat Command's Federal Laboratory, Naval Air Systems Command's Air Combat Electronics Program Office (PMA-209), and

Georgia Tech Research Institute, reflects the cooperative government-industry strategy that shapes the SOSA effort. | USAF PHOTO

RF: The Toughest Nut to Crack

RF system integration poses unique difficulties when applied to SOSA. Analog systems are less tolerant of variability than digital ones, and signal degradation, impedance mismatches and connector loss are more pronounced at RF frequencies. Hosking explains, "SOSA requires all your RF analog I/O coming through the backplane, and that's difficult to achieve while maintaining signal integrity. However, following the VITA guidelines lets you unplug a card with 20 RF connectors from the cage and plug in a new one. If they were connected to the front of the card, you'd have to find where each one goes, and human error being what it is, there's a good chance they could get mixed up."

That said, unlike digital signals, high-frequency analog signals degrade quickly over long traces, making front-panel coaxial connections a necessity in some cases. This design compromise creates tension with SOSA's modular vision. Additionally, power delivery and thermal management for high-power RF systems, such as a communications jammer or a radar jammer, remain complex. These systems often exceed the cooling and power constraints defined by VITA and SOSA, requiring customized engineering solutions that may diverge from the standard profiles. GaN RF power devices have become the choice in many RF power amplifiers. Because they have such high power density, they can generate a lot of heat that has to be dissipated from the transistor die itself through the substrate, and then outward, where it can be removed. SOSA considers this as well and allows various cooling techniques to be used.

Backplane certification is another concern, especially for small and mid-size vendors. Justin Moll gives the SOSA

development teams credit for considering this. “They didn’t want to create chaos,” says Moll, “so they allowed a degree of flexibility on the backplane because each one is a little bit different.”

“Having been involved in the original OpenVPX work and watching it evolve into SOSA, it’s clear that we’ve created something of a complexity monster,” says Ian Dunn, Chief Technology Officer at Spectrum Control. “The architecture has become significantly more intricate over time, yet there’s no direct economic return for participating in its development. Despite that, SOSA is increasingly mandated, which means vendors must implement it, whether or not it adds immediate value or revenue. As a result, the cost of compliance may have to be built into our pricing models, even though the standard itself doesn’t offer a clear path for recouping those costs.”

As SOSA becomes more prevalent, certain platforms’ size, weight, and power (SWaP) constraints raise questions about its applicability. Ian Dunn observes, “We now believe there is a strategy below 3U VPX, and we’re actively trying to figure out what that is. One of the things we’ve done – being an RF company building 3U VPX – is to work on component miniaturization. We’ve been keeping an eye on small-form-factor stuff for many years.”

Stephen Martin, Director of Marketing at Spectrum Control, points out that 3U VPX remains useful primarily for legacy upgrades. “3U VPX isn’t going away, but we see it on existing platforms where people want to upgrade but stay in the same chassis. So, we’re working to provide more mission capability for that form factor – more channels, denser modules, and fewer slots. Yet backward compatibility often takes precedence over SOSA compliance,” Martin continues. “The bulk of the market has nothing to do with SOSA interoperability – it has to do with backward compatibility. You will spend all your money trying to operate within that prior capability, not with the new standards.

“We also offer an optical transceiver platform designed for high-speed data transfer from these boards in parallel with our system-in-package platform,” Martin says. “It’s commonly used in avionics applications, particularly when high-speed data needs to be moved from an electronic warfare front end to a processing unit elsewhere in the system. The transceiver is built on a BGA platform engineered to support miniaturization and integration into compact form factors.”

Dunn is clear when asked whether SOSA makes sense for smaller, tactical platforms, like drones or missile seekers: “The short answer is probably not – at least not directly, and certainly not in the same way it’s used for larger modular systems. There will be 3U slots in a B-52 for another 30 years or more. Those might want to be SOSA-aligned, but that’s not true with drones.”

SOSA is built around a modular backplane architecture that assumes a specific chassis and slot structure. It’s best suited for environments with ample space and power, such as EW pods, ground vehicles, and ISR platforms, but it doesn’t translate well to ultra-compact, tightly integrated systems. Those platforms typically use custom boards, system-on-chip architectures, and highly miniaturized RF modules, leaving no room for the modularity SOSA requires.

Despite its limitations, SOSA represents a transformation in defense electronics. It codifies a new approach to design and procurement – one based on openness, interoperability, and competition. By adopting SOSA, the defense industry gains a framework for faster modernization, reduced lifecycle costs and greater strategic agility. Though compliance can be costly and integration complex, the long-term benefits – technical, operational, and economic – are becoming increasingly apparent.

Manufacturers are navigating the transition through architectural redesign, new test methodologies, and standards-

driven product strategies. From educational outreach and workforce development to hardware prototyping and formal certification, the ecosystem supporting SOSA continues to expand. As the DOD continues its shift toward modular open systems, SOSA will remain a key player, defining how defense systems are built and how they evolve.

There is a certain level of consternation around how long the SOSA standard will take to be finalized and testing facilities approved. However, participants in SOSA committees and subcommittees do this on their own time, without pay, and they have their own full-time jobs to do. In fact, when SOSA is compared with commercial standards, such as Wi-Fi, Bluetooth, and 5G, there's little difference between them in this respect. And if DOD employees had to do this, it would probably take even longer, and manufacturers would have to guess what they were doing. Estimates provided by people consulted for this article believe SOSA will undoubtedly be completed by the end of the decade, and some think it could even be just half that. It should be worth the wait.