TECHNOLOGY WHITEPAPER

Why an Open Standards Approach Is Essential in Defense and Aerospace

Exploring MOSA, SOSA™, FACE™, VICTORY, and more

CURTISS-WRIGHT

DEFENSE SOLUTIONS

Read About

- Open Mission Systems/ Universal Command and Control Interface (OMS/UCI)
- Sensor Open Systems Architecture (SOSA™)
- Future Airborne Capability Environment (FACE™)
- Vehicular Integration for C4ISR/EW Interoperability (VICTORY)

Point Solutions Create Numerous Challenges

A rare event occurred early in January 2019. The Secretaries of the three main branches of the U.S. military — Army, Air Force, and Navy — issued a joint memorandum on the imperative for a Modular Open Systems Approach (MOSA) to weapons systems. The tri-services memo makes it clear that the need to rapidly share information from machine to machine requires common standards. It also notes that "MOSA supporting standards should be included in all requirements, programming, and development activities for future weapon system modifications and new start development programs to the maximum extent possible."

Figure 1: The U.S. Army, Air Force, and Navy have issued a joint memorandum on the imperative for a Modular Open Systems Approach (MOSA) to weapons systems

While developers of defense and aerospace solutions have been leveraging open standards to improve interoperability for a number of years now, the memo drove home the point that these initiatives are no longer optional. They are vital and they are mandatory.

There are many very good reasons behind the move. After decades of deploying proprietary point solutions that don't take advantage of sharedbuilding blocks, defense and aerospace organizations are facing significant size, weight, power, and cost (SWaP-C) challenges on ground, air, and sea platforms.

When each new capability or function that's added to a platform is a complete system with its own subsystems, the duplication of physical and logical components increases complexity and costs. It also increases heat generation and consumes valuable space on already-cramped platforms. It's an unsustainable approach, especially as platforms and budgets continue to shrink in size.

Interoperability is another significant issue with discrete, closed solutions. Closed solutions based on propriety technologies are designed to operate in isolation. As a result, they are very difficult and time-consuming to deploy on platforms where systems and people must work together to ensure personnel safety and mission success. Closed solutions are equally challenging to maintain and repair, especially if the vendor that provided the proprietary technology no longer supports it, or has gone out of business.

The Sensor Open Systems Architecture Is Key to Resolving Today's Challenges

The tri-services memo references several open standards:

+ Open Mission Systems/Universal Command and Control Interface (OMS/UCI)
+ Sensor Open Systems Architecture (SOSA™)
+ Future Airborne Capability Environment (FACE™)
+ Vehicular Integration for C4ISR/EW Interoperability (VICTORY)

While all of these standards are important and play a role in resolving critical challenges with solution deployments, SOSA™ is particularly relevant.

The SOSA™ Consortium creates a common framework for transitioning sensor systems to an open systems architecture. With so many existing and emerging sensor systems to consider, the Consortium's goal to "allow flexibility in the selection and acquisition of sensors and subsystems that provide sensor data collection, processing, exploitation, communication, and related functions over the full life cycle of the C4ISR system" is extremely important.

The overarching benefits of the strong push from all three main branches of the U.S. military to choose only open standards-based solutions are clear. Open solutions will improve communications and sharing across all platforms. And, they will protect investments by ensuring all systems on all platforms can be smoothly and flexibly upgraded and replaced as needed.

Increased Interoperability Offers Many Benefits

To realize the full benefits of MOSA and the associated standards, defense and aerospace organizations must select modular and ruggedized commercial off-the-shelf (COTS) solutions. These cost-effective building blocks provide the interoperability and flexibility that's needed to deploy systems across land, air, and sea platforms. COTS solutions are able to offer these advantages because they're based on open standards that leverage one another.

+ The SOSA™ standards initiative was initially developed as part of the FACE™ consortium. SOSA™ standards are compatible with FACE™ and OMS standards, and they leverage a number of VITA standards, including VITA 65, the OpenVPX standard that ensures interoperability among the COTS solutions that are used to create subsystems and systems.
+ The C4ISR/EW Modular Open Suite of Standards (CMOSS) falls under the SOSA™ umbrella. CMOSS defines sharing mechanisms across software, hardware, and network layers. To define these mechanisms, CMOSS standards leverage the:
  - VICTORY standards for network interoperability
  - OpenVPX standard for combining cards in a common chassis
  - Modular Open RF Architecture (MORA) standard for sharing RF resources
  - FACE™ standard for software portability
+ There are discussions about including FACE™ in the VICTORY Shared Processing Unit definition. If this occurs, it would be highly reflective of the goal to standardize systems and technologies across platforms. The VICTORY standard applies to ground vehicle systems, while the FACE™ standard was developed for airborne environments.

Avoiding Vendor Lock-In is Crucial

With open standards-based COTS solutions, defense and aerospace organizations are no longer forced to choose the proprietary offerings of a particular vendor. Instead, they have the freedom and flexibility to choose solutions from a far broader selection of vendors who are operating in a more competitive environment. When they're not guaranteed to win, vendors are highly motivated to showcase their competitive advantages and differentiate their offerings.

This new, more competitive landscape gives system developers access to a wider range of functionality combinations, availability timelines, and price points so they can keep programs on spec, on time, and on budget. They can also choose the optimal solution for the challenge at hand, rather than the only solution offered by the vendor to which they are tied.

In some cases, it will make sense from capability and cost perspectives to choose different solutions from different vendors and combine them. As long as each solution is designed and proven to meet the requirements in the relevant open standards, the risk in taking this approach is manageable. A multivendor strategy — whether it's applied across a subsystem, a system, a program, or a platform — also allows defense and aerospace organizations to spread risk across multiple vendors.

Once the system is deployed, open standards compliance and interoperability enable faster, easier, and more frequent technology refresh cycles. Systems, cards, and components can simply be swapped out for updated versions. And, those updated versions don't have to come from the original vendor, providing the opportunity to incorporate more sophisticated, SWaP-friendly, or cost-effective replacements.

On a similar theme, the ability to choose an appropriate solution from any vendor allows defense and aerospace organizations to immediately obtain and deploy the most up-to-date technology available to counter or overmatch a particular threat.

Finally, interoperability among system components increases operational availability levels because it's much easier to ensure a reliable, long-term supply chain for spares and replacement parts. If one vendor raises their prices for replacement parts to an unacceptable level, stops stocking particular parts, or goes out of business, it's easy to acquire compatible parts from another vendor. As a result, a total life cycle management approach can be adopted that reduces risks and increases the return on technology investments over the long term.

Interoperability in Action: Real-World Examples

Most of the interoperability benefits described in the previous section are realized by the defense and aerospace organizations that are purchasing solutions and building systems. But, interoperability also brings extremely important new capabilities and benefits to warfighters in the field. With open standards-based COTS solutions, more information can be shared faster across all systems on all platforms, leading to more informed and intelligent decision-making and increased mission success.

Here are just three examples of what becomes possible.

Easily Upgrade to More Advanced Applications

Traditional electronic warfare systems that are used to identify signals typically take a "brute force" approach to signal recognition, filtering through large numbers of signatures until they find the one that most closely matches the signal in question. This works well to a point. However, as the volume of data available for analysis continues to increase, a more sophisticated approach is needed.

A machine learning application takes signal processing and threat identification capabilities to new levels of speed and intelligence. This type of application compares real-world data from sensors to millions of examples it has been trained to identify. The application uses the result of the comparisons to make decisions, take actions, and provide warfighters with insight they wouldn't otherwise have. With faster access to more accurate intelligence from a machine learning application, warfighters are in a much better position to make the right decisions to protect people and equipment in the field.

The advanced software in a machine learning application relies on complex algorithms that can quickly process large volumes of data. To execute, that advanced software relies on the speed and processing power provided by specialized hardware that likely isn't available on the platform today.

When all system components follow MOSA, the processor card that's driving the traditional electronic warfare image identification application can be quickly and easily replaced with a more sophisticated card that can drive a machine learning application. With updated software and a simple card swap, warfighters now have access to important new threat identification capabilities with minimal disruption and no increase in SWaP.

Accelerate Every Application

While machine learning is a specific example of the need for speed in the field, the requirement to process ever-growing volumes of data from more sources, faster, applies to almost every application in use today.

With the ability to almost instantly upgrade any card type that performs any function, in any system, with a faster, more powerful replacement, warfighters have new opportunities to stay ahead of threats and increase their tactical advantage. For example, the latest:

- Field programmable gate array (FPGA) cards are optimized for radar, electronic warfare, signal intelligence, radar warning receivers, and software-defined radio applications in environments with extremely wide-ranging temperatures.
- General purpose graphics processing units (GPGPUs) bring TFLOPS of processing power to:
  - Electro-optical/infrared (EO/IR) applications that must capture and manipulate huge data streams from gigapixel cameras
  - Space-time adaptive processing (STAP) and synthetic aperture radar (SAR) systems that need floating point engines that can handle pulse compression and Doppler processing
- Single board computers (SBCs) and Digital Signal Processing (DSP) modules bring higher precision and faster results to demanding deployed applications, such as next-generation mobile mission computing systems, radar processing and imaging systems, and a wide variety of C4ISR applications

Improve Load Balancing

With applications that rely on optical sensors, huge volumes of data must be sent back to centralized data centers for processing. The challenge multiplies when optical sensor resolution is increased; doubling the resolution quadruples the amount of data that must be transmitted for processing. But, the capacity of the network links back to the data centers is typically not increased at the same pace that data volumes grow. As a result, these links can quickly become bottlenecks.

The challenge here mirrors the challenge industries outside of defense and aerospace are facing as they look to take advantage of Internet of Things (IoT) and 5G applications: It's simply not efficient or affordable to send large volumes of data across the internet for processing. Data storage and processing must be pushed out to the edge of the network, closer to where the data is collected.

When data storage and processing solutions are aligned with open standards, they can be easily added to the platform and integrated with existing systems so some of the data from optical sensors can be processed locally on the platform. Even if the local resources can only handle initial analysis tasks, there's far better ability to balance data processing loads across local and remote resources. Warfighters have faster access to preliminary processing results, and the data load on the link back to the data center is reduced, opening up link capacity for use by all applications.

Curtiss-Wright Is Dedicated to Open Standards

Curtiss-Wright understands the value that open standards-based COTS solutions bring to modern military and aerospace organizations. We also recognize that a holistic approach is essential to deliver capabilities that meet expectations and requirements. This holistic approach can only be achieved through partnership and collaboration among leading industry players to ensure that solutions are developed according to open standards.

Our strong and long-time commitment to developing modular COTS solutions that are based on an open standards architecture, along with our dedication to industry collaboration and open standards development, ideally positions our company to:

- Deliver ruggedized, reliable, and secure COTS solutions that are aligned with key industry standards, including SOSA™, VICTORY, CMOSS, MORA, and others
- Deliver solutions that align with multiple open standards
- Lead the usage of open standards and drive industry collaboration initiatives
- Give our customers faster and easier access to solutions that are aligned with open standards

Author(s)

David Jedynak
Chief Technology Officer
Curtiss-Wright Defense Solutions

Denis Smetana
Senior Product Manager
Curtiss-Wright Defense Solutions

Aaron Frank
Senior Product Manager
Curtiss-Wright Defense Solutions

Tammy Carter
Senior Product Manager
Curtiss-Wright Defense Solutions

Our solutions reduce risks, lower costs, and speed deployment of the applications warfighters need most. Some of our most sophisticated, ruggedized COTS processing solutions are developed in alignment with the SOSA™ Technical Standard, including the:

+ VPX3-1260, a high-performance 3U OpenVPX SBC featuring the latest 8th Gen Intel Xeon E processor with integrated graphics.
+ VPX3-663, a versatile building block that combines a PCI Express (PCIe) Gen 3 switch with a 10G backplane Ethernet switch in a single 3U card.
+ CHAMP-XD1S, a ruggedized, multi-core digital signal processing (DSP) engine with Xilinx MPSOC FPGA that allows High Performance Embedded Computing (HPEC) systems to take full advantage of today's leading-edge Intel Xeon processor D architecture.

We can provide these open standards-based solutions on their own, or as part of fully integrated subsystems and systems that leverage our own expertise and experience, as well as that of other leading hardware and software vendors.

For details about the open standards our solutions support, contact us at ds@curtisswright.com.

Learn More

Curtiss-Wright Open Standards Support

› Modular Open Standard Architecture (MOSA)
› OpenVPX (VITA 65) Standard
› Vehicle Integration for C4ISR/EW Interoperability (VICTORY)
› Future Airborne Capability Environment (FACE™)
› C4ISR/EW Modular Open Suite of Standards (CMOSS)
› Sensor Open Systems Architecture (SOSA™)

Curtiss-Wright Products

› VPX3-663 PCIe Gen 3 and 10G Ethernet Hybrid Switch
› VPX3-1260 3U VPX Intel Xeon Coffee Lake SBC
› CHAMP-XD1S Digital Signal Processor