Defense Standardization Program

JOURNAL

JANUARY–APRIL 2020

Modular Open Systems Approach

- Modular Open Systems Approach Overview and Efforts
- Making the Most of Modular Open Systems Approach Standards
- A Key Requirement to National Security
- VICTORY for MOSA

Contents

Departments

Nicole Dumm
Editor
Defense Standardization
Program Journal

Gregory E. Saunders
Director
Defense Standardization
Program Office

Defense Standardization Program Office
8725 John J. Kingman Road, STOP 5100
Fort Belvoir, VA 22060-6220
703-767-6888 | Fax 703-767-6876 | dsp.dla.mil

This issue and all previous issues of the *DSP Journal* can be found on the DSP website. To receive issues, please subscribe at the DSP website, www.dsp.dla.mil, or e-mail DSP-Editor@DLA.mil and put "Subscribe" in the subject line.

The *Defense Standardization Program Journal* (ISSN 0897-0245) is published three times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the DSP Journal are welcomed and encouraged. Send all materials to Editor, DSP Journal, Defense Standardization Program Office, 8725 John J. Kingman Road, STOP 5100, Fort Belvoir, VA 22060-6220. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means: e-mail to DSP-Editor@dla.mil. CD or DVD to DSP Journal at the above address. DSPO reserves the right to modify or reject any submission as deemed appropriate.

Director's Forum

Modular Open Systems Approach

It seems such a short time ago that I was writing my farewell message for the *DSP Journal*—but now, surprisingly—I'm back on the job. It was an unexpected development. I hired Michael Heaphy in 2017 with the intention that he would step into the role of director upon my retirement. Michael got to know the staff, the leadership, the business contacts, and, most importantly, the programs in DSPO's purview. I turned in my credentials on December 31, 2018. Later that same week, Michael, who is a naval reserve officer, was contacted by the Navy with the news that he was to return to active duty for up to one year, beginning in July of 2019. DSPO staff and leadership evaluated several alternatives—one of which was asking me if I would return to the director position for the duration of Michael's deployment. I agreed to return, so here I am, a rehired annuitant, picking up my former duties as director of the Defense Standardization Program Office. Michael has already begun to put his own stamp on DSPO, the DSP, and related programs. While proud to be of service to the Navy, I'm sure he is eager to resume his leadership of this office. I will continue to develop some of the changes that Michael initiated, and I hope that I can contribute to the sustained leadership of the DSP in so many significant areas.

As the reorganization of the Office of the Secretary of Defense evolves, there are other changes in our positioning and leadership. While DSPO is still functionally aligned with the Under Secretary for Research and Engineering (USD R&E), within R&E, there have been a few changes. Dr. Michael Griffin is the under secretary. He has established two offices—one for Research and Technology and one for Advanced Capabilities (AC). The Directorate for AC is led by Mr. Jim Faist, with Mr. Terry Emmert as principal deputy. Within AC, Dr. Sandra Magnus is the deputy director for engineering where DSPO is aligned. Dr. Magnus is a former astronaut and, more recently, was the executive director at the American Institute of Aeronautics and Astronautics. During the 1980s, Dr. Magnus worked on stealth aircraft design as an engineer for McDonnell Douglas. As an astronaut, she spent 134 days in orbit and was assigned to the crew of STS-135, the final mission of the Space Shuttle. I'm confident that Dr. Magnus will be a tremendous asset to the department and a strong supporter for the Defense Standardization Program.

Under my leadership, the Defense Standardization Program will pursue our mission goals of advancing standardization vigorously throughout DoD to reduce costs and improve operational effectiveness. There are several initiatives that are drawing a lot of attention.

Gregory E. Saunders
Director
Defense Standardization Program Office

- We continue to push for modernization of ASSIST and the Government-Industry Data Exchange Program (GIDEP). Both systems were developed many years ago and, though they have had many upgrades and patches, performance, capability, and efficiency can and will be improved through more comprehensive modernization efforts.
- The DSP logo includes the phrase, "Making Systems Work Together." There's hardly a simpler statement of interoperability—and our work at NATO focuses on this fundamental. We are looking closely at U.S. implementation of NATO standardization agreements to improve our effectiveness.
- DoD continues to pursue modular open systems approaches and the DSP supports this with a new standardization area, defining MOSA-enabling standards and standardization gaps. This issue of the journal takes you into more detail on what we mean by MOSA and what we are doing to facilitate modular approaches.
- A couple of years ago, we began to integrate parts management and diminishing manufacturing sources and material shortages (DMSMS) management into a single, holistic program. The synergies are becoming apparent and real progress is showing in both areas. There are multi-part strategic plans for each area, and they are drawing on each other's accomplishments.
- We are preparing DoDIs for DMSMS and GIDEP. Both areas have been criticized for a lack of top-down direction. The new instructions will direct compliance and reporting.

These are only a few of the most highly visible initiatives underway. DSPO works on and supports a wide range of issues. I encourage you to visit our website to see what's going on, pursue topics in more depth, and stay abreast of new developments. Among other things, stay tuned for information about our next Defense Standardization Program workshop tentatively scheduled for the first week of August 2020.

Modular Open Systems Approach Overview and Efforts

A DSPO and Office of the Secretary of Defense Perspective

Himanshu Patni

DoD has employed Modular Open Systems Approaches (MOSAs) for the last 20 years; however, recent legislation has mandated the use of MOSA in programs across DoD. The Office of the Secretary of Defense (OSD) has concluded that continued implementation and further development of MOSA-enabling standards is needed to ensure rapid sharing of information across domains with quick and affordable updates or improvements to hardware and software components. Under the direction of the Office of the Under Secretary of Defense (Research and Engineering) (OUSD[R&E]), the director, Engineering Tools & Environments and DSPO have taken the lead on MOSA efforts across DoD, based on the FY17 National Defense Authorization Act (NDAA). OSD established three MOSA tiger teams (Standards, Implementation Guidance, and Requirements and Programming Functions) and is working with the Modular Open Systems Working Group (MOSWG) to create maturity assessments, deliver MOSA-specific standards, analyze gaps, define standard profiles, and deliver a MOSA standards needs assessment. In addition, OSD established and defined a Modular Open Systems Standards and Specifications (MOSS) Standardization Area, which is to be populated with DoD-wide MOSA-enabling standards in DSPO's centralized tool, ASSIST. DoD is transitioning from monolithic closed systems and mandating the use of MOSA to facilitate technology refresh, increase competition, encourage innovation, reduce cost, and improve interoperability. In accordance with the statutory provision of Title 10, U.S. Code, Chapter 145, Sections 2451–2457 of the Cataloging and Standardization Act, DSPO, with the services and MOSA community, is standardizing MOSA using flexible, cost-effective, open, and consensus-based standards. This article discusses current and future OSD MOSA efforts across DoD and the challenges that come with them.

MOSA DIRECTION

The OSD-developed MOSA Glossary defines MOSA by referencing 10 USC 2446a.(b), Section 805, as follows: "with respect to a major defense acquisition program, an integrated business and technical strategy that—

(A) employs a modular design that uses major system interfaces between a major system platform and a major system component, between major system components, or between major system platforms;

(B) is subjected to verification to ensure major system interfaces comply with, if available and suitable, widely supported and consensus-based standards;

(C) uses a system architecture that allows severable major system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a major system platform to afford opportunities for enhanced competition and innovation while yielding—

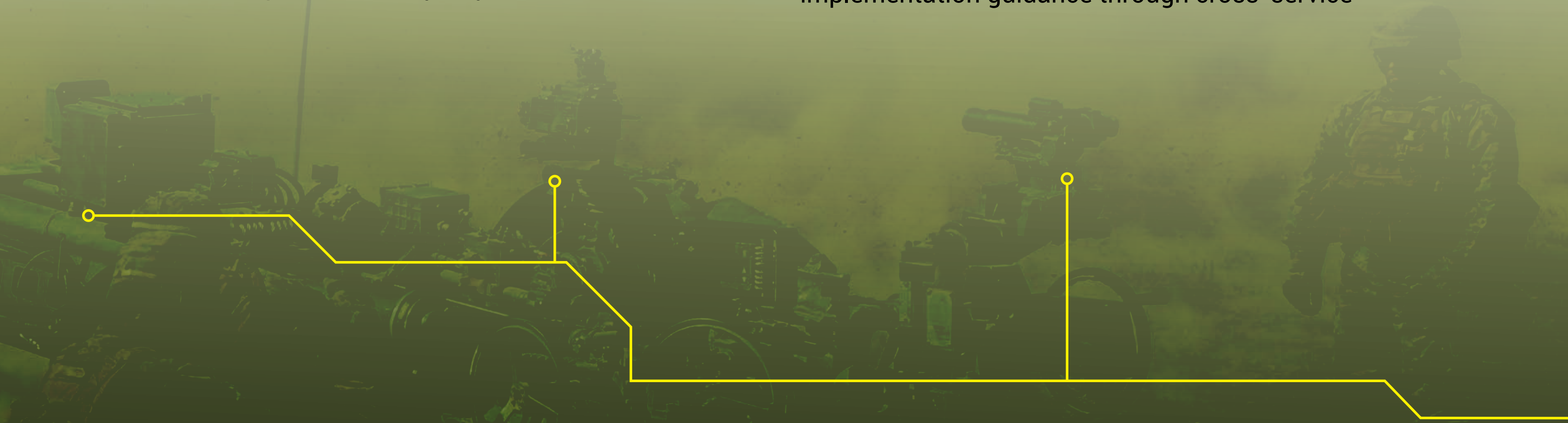
- i. significant cost savings or avoidance;
- ii. schedule reduction;
- iii. opportunities for technical upgrades;
- iv. ncreased interoperability, including system of systems interoperability and mission integration; or
- v. other benefits during the sustainment phase of a major system; and

(D) complies with the technical data rights set forth in section 2320 of this title."

Where and how do we start? In the first quarter of 2019, the service secretaries of the Army, Navy, and Air Force signed a MOSA tri-service memo, "Modular Open Systems Approaches for our Weapon Systems is a Warfighting Imperative."[1] The memo directs that MOSA standards should be included in all requirements, programming, and development activities for future weapon system modifications and new development programs to the maximum extent possible. It also cites successful MOSA efforts and standards—Sensor Open Systems Architecture™ Consortium, Open Mission Systems/Universal Command and Control Interface, Future Airborne Capability Environment™, and Vehicular Integration for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance/Electronic Warfare Interoperability standards—as "vital to our success."

APPROACH

The tri-service memo, along with the existing MOSWG, has been the driving force behind OSD's MOSA efforts in 2019, and led to the formation of three MOSA tiger teams. First, the Standards Tiger Team surveys current MOSA efforts in DoD, uncovers common standards and practices, and finds gaps. Second, the Implementation Guidance Tiger Team creates service-specific implementation guidance through cross-service



1 Office of the Secretary of the Navy, Office of the Secretary of the Army, and Office of the Secretary of the Air Force, Memorandum for Service Acquisition Executives and Program Executive Officers, "Modular Open Systems Approaches for our Weapon Systems is a Warfighting Imperative," January 7, 2019, available at https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular_Open_Systems_Approach.pdf.

collaboration to support future acquisition programs. Lastly, the Requirements and Programming Functions Tiger Team ensures MOSA is reflected in requirements and programs to enable communication and cross-domain sharing for future weapons systems.

To facilitate the inevitable sharing of MOSA-enabling standards across domains in a centralized location, DSPO worked with OSD leadership to establish a MOSA Standardization Area, and assigned ownership to the director, Engineering Tools & Environments with OUSD(R&E) as the lead standardization activity (LSA). This area, known as the MOSS, is defined in DSPO's Standardization Document 1 (SD-1) as follows:

"This AREA covers the specifications, standards, best practices and compliance testing guidance that form a framework for a Modular and Open Systems Approaches (MOSA) that can be applied to the development, operation, upgrade and maintenance of defense systems. These products include:

- Technical specifications that define system architectures that support severable and composable components, parellel [sic]
- Standards for interfaces, data exchanges, physical connections (electrical, mechanical, etc.) and data models,
- Best practices for implementing MOSA architectures and frameworks, and
- Compliance testing for implementations of standards that support the MOSA practice."

These criteria, which can be modified by the LSA, are used select the MOSA-enabling standards and specifications that are suitable for populating the MOSS in ASSIST.

CURRENT AND FUTURE CHALLENGES

MOSA was often referred to as a buzzword or fad. The definition of MOSA and what was truly modular or open presented challenges. Now that MOSA is encoded in the law (FY17 NDAA) and DoD acquisition programs are mandated to implement it, things are changing. While MOSA-related definitions have become clearer and efforts stated in the tri-service memo have gained visibility, new challenges and questions have arisen: Now that I have to implement MOSA, how do I evaluate compliance? Is there a way to measure or score MOSA? Who would establish such a metric? Should there be a metric if it might make implementing MOSA more difficult for the services, contrary to OSD's goal of using MOSA to help the services without program intervention?

One of the biggest challenges has been leveraging existing successful MOSA efforts without breaking them. Several programs are implementing MOSA in creative and useful, yet different, ways across different platforms (for example, air, land, and sea). One of OSD's goals with the MOSA tiger teams is to find MOSA lessons learned and best practices and supply a creative environment where another program, perhaps with a different service and platform, can implement MOSA. This process has brought up new questions. How can existing programs modify their change management process to incorporate MOSA? Are there situations where MOSA is not practical? Academic institutions have studied the cost of MOSA, and DSPO has created a draft MOSA document to help program managers answer some of these questions.

Additional challenges include how MOSA-enabling standards will be populated in the MOSS within ASSIST. What information will be available? Would all MOSA standards and specifications be converted into defense standard formats or should some of them be adopted by a recognized standards body, such as ANSI or IEEE, and then by DoD through a longer overall process? How important is it for one to retain ownership of a standard versus sharing it through a large standards body? Will implementation guidance be supplied? Currently, ASSIST is not a one-stop shop for implementation guidance nor does ASSIST host non-government standards. However, ASSIST modernization efforts could facilitate these improvements in the future.

To address some of these challenges, OSD has created a consolidated list of MOSA-enabling standards to aid in a gap analysis and referenced existing policy and guidance on standards, architectures, interfaces, and data rights. OSD has also facilitated numerous MOSA tiger teams with briefings from all DoD services, industry, and academia. Awareness of the DSPO, ASSIST, and LSA roles have increased, but one thing is certain—the challenges will require continued collaboration with the services while roles and responsibilities are defined at all levels.

ABOUT THE AUTHOR

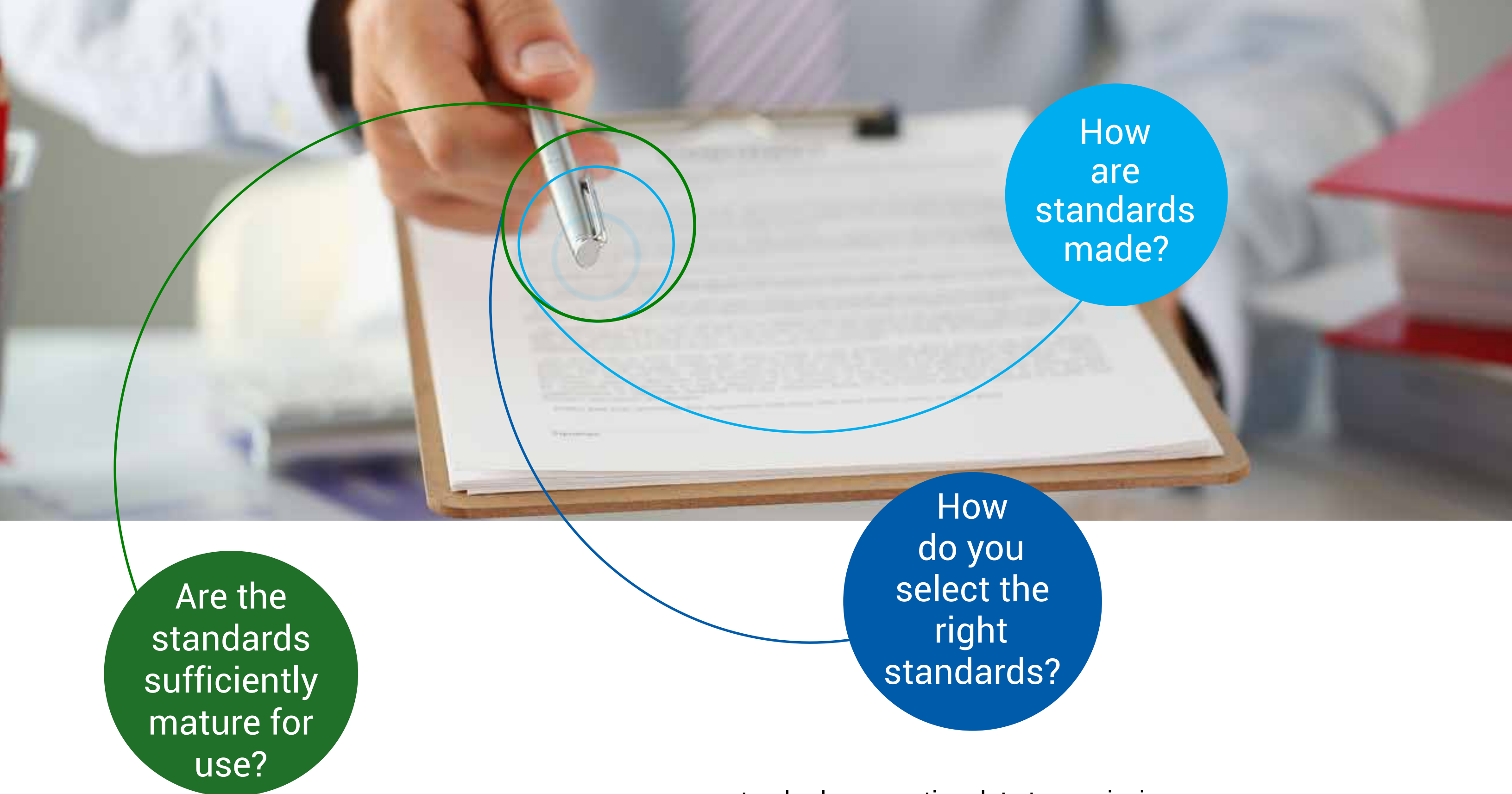
Himanshu Patni *is a MOSA standards engineer for DSPO under OUSD(R&E). He supports efforts on DSPO policy and procedures and how they pertain to MOSA standardization across DoD. He has more than 15 years of experience as an engineer, including supervisory experience with local government and 2 years of naval acquisition and systems engineering experience.*

Making the Most of Modular Open Systems Approach Standards

John Bowling

The standardization of parts, processes, and specifications enabled the industrial revolution. It should be no surprise that standardization continues to be essential for success in the information revolution. Now, we must standardize information interfaces as well as data exchange methods (syntax) and meanings (semantics). Rapidly reconfiguring and modifying systems is essential to support the emerging doctrine of multi-domain operations (MDO). Modular open systems approaches (MOSAs) can enable these capabilities by relying on open standards at key interfaces.

In 10 USC 2446c.(2), we are required to “ensure that major system interfaces incorporate commercial standards and other widely supported consensus-based standards that are validated, published, and maintained by recognized standards organizations to the maximum extent practicable.” This guidance leaves important questions. How are standards made?



How do you select the right standards? How do we know whether standards are sufficiently mature for use? This article walks through these questions to help you get the most out of MOSA standards.

HOW ARE STANDARDS MADE?

Standards are created by those who see a need for them. Standards bodies recruit members with an interest in seeing a standard developed for a business purpose; most commonly, that purpose is interoperability between vendors at a well-defined open interface. We rely on numerous open standards every day, from the Schrader valve on car tires to National Electrical Manufacturers Association 5-15 duplex electric receptacles in homes and the Institute of Electrical and Electronics Engineers 802.11ac wireless network standard in smartphones. In the cell phone industry, carriers saw a good business case for data interoperability. From 2G through 5G data standards, carriers have created common standards supporting data transmission. Common carrier interfaces and a common set of data capabilities in phones translates to lower per tower costs for carriers, cross-provider service agreements for better data coverage, and happy streaming customers.

All the services are increasing their participation in standards development, often jointly. Standards development organizations (SDOs), such as the Object Management Group® (OMG), SAE International®, and The Open Group® work with DoD on various open standards from standard languages, like OMG® Systems Modeling Language™ (SysML), to software standards, like Unmanned Systems (UxS) Command and Control Segment (UCS) and the Future Airborne Capability Environment™ (FACE) Technical Standard. One tri-service effort of note is The Open Group's Sensor Open Systems Architecture™ (SOSA) Consortium. The consortium is developing the SOSA™ technical standard as an integrative standard. This means other efforts, like Naval Air Systems Command's Hardware

Open Systems Technology and the Army's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance/Electronic Warfare Modular Open Suite of Standards are contributing content to and harmonizing with the SOSA technical standard. The consortium is aligning its effort with the FACE and Open Mission Systems standards as well as other standards.

DoD's work with SDOs has been an ad hoc process. In 10 USC 2446c.(1), service secretaries are directed to coordinate in "specification, identification, development, and maintenance of major system interfaces and standards for use in major system platforms." Such SDO participation must become an ongoing, planned part of our engineering and acquisition mission. For example, tri-service participation in development of the OMG SysML standard and the SAE International Architecture Analysis and Design Language drives better modeling for shareable systems architectures and interfaces. The widely supported, consensus-based standards development process doesn't usually occur within program execution timeframes. Thus, proactive development of open interface and data model standards is required to meet the needs of multiple future programs.

ARCHITECTURE standards

HOW DO YOU SELECT THE RIGHT STANDARDS?

In a word, architecture.

1. Capture what you know (or think you know) about your effort, such as capabilities required, constraints, and operational environments. Hire a systems architect and a modeler; you are unlikely to have the needed skills in-house.

2. Build a model and some views with the data you have and start asking questions. You'll discover actors, capabilities, connections, dependencies, flows, interfaces, modules, and requirements.

3. Iterate a few times with broader and broader reviews.

4. Send out a request for information or a draft request for proposals with the draft architecture and process the comments you get back.

5. Decide which interfaces need to be open to meet the intent of Section 2446c. Where will change occur most often? Where will maintenance responsibility change hands? Where do third parties need to quickly develop and integrate capabilities? How will the MDO doctrine affect your program? The answers to these questions will point toward the open standards you need.

So, you found a standard, but you're not sure it's right for your program. Who do you ask? That's a good question but one that doesn't always have a good answer. You can ask the SDO for assistance. Typically, some members of the SDO offer consulting services on the use of the standard. For the Air Force, the Air Force Life Cycle Management Center (AFLCMC) has established an Open Architecture Management Office (OAMO), which supplies initial consulting on standards selection and use. As a new capability with limited manning, the OAMO is supported by the engineering home office. In the Army, the Vertical Lift Consortium advances the state of the possible for rotorcraft. This includes support to open standards development (including the FACE™ and SOSA™ standards) and technology demonstrations, such as joint multi-role. The Program Executive Office Aviation and Army Futures Command Combat Capabilities Development Command Aviation and Missiles Center have employees involved with open standards. In the Navy, PMA-209, the Air Combat Electronics program, is a key point of contact for open avionics standards.

Discover who else has used the standard; ask for their advice to avoid pitfalls or mitigate schedule challenges. Try a small risk reduction effort to rapidly prototype a subsystem using the new standard. Test it out, learn about it, and supply feedback, questions, and recommendations to the SDO. This will improve your understanding of the standard and the feedback will improve the standard for future users. Create your own lessons learned to benefit the next user of the standard. Remember, despite our silos of excellence and funding segregation, we are all in the fight together.

HOW DO WE KNOW WHETHER STANDARDS ARE SUFFICIENTLY MATURE FOR USE?

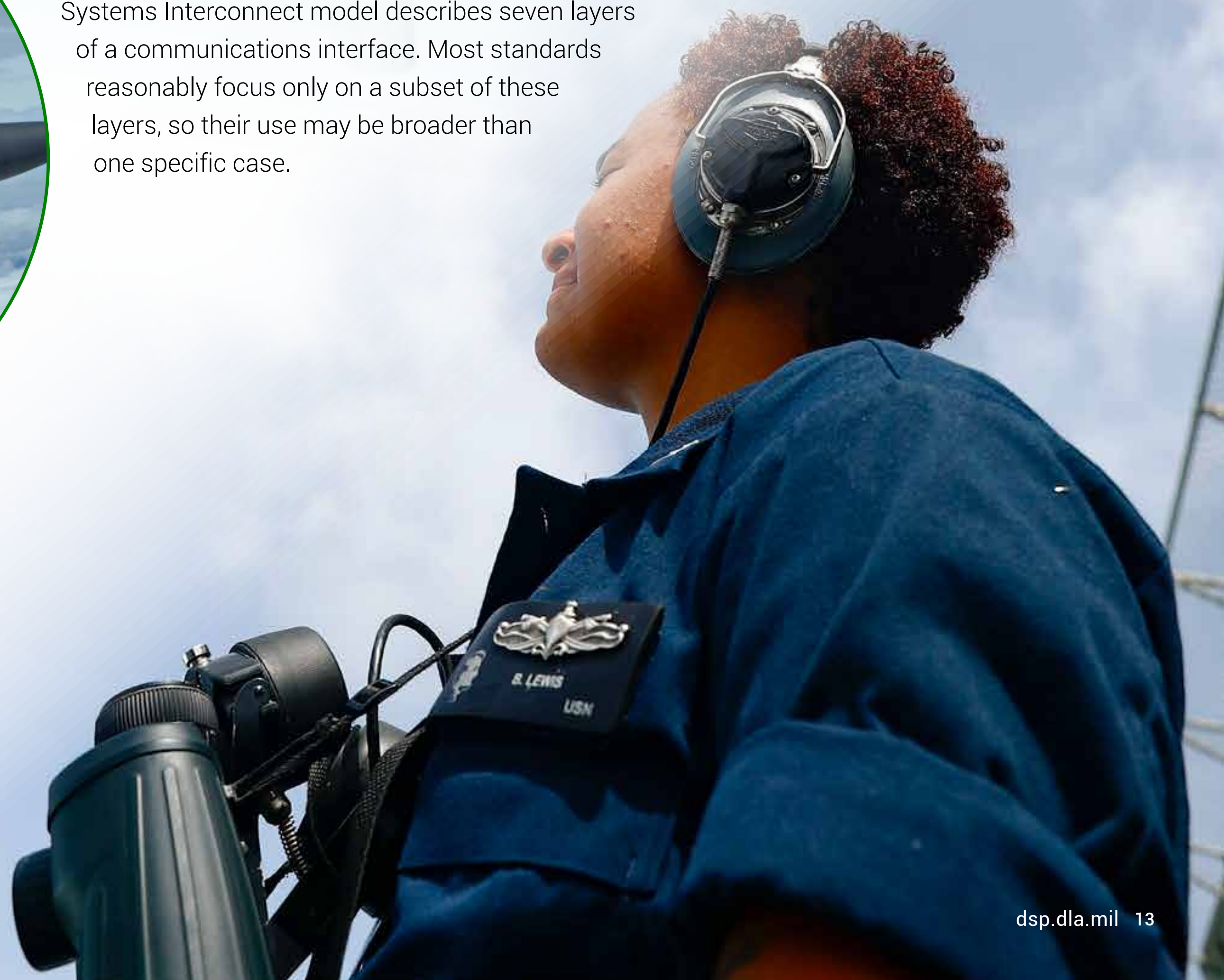
Standards maturity is an interesting and troubling concept. Standards mature through use, feedback, and revision. When is a standard mature enough? Does anyone trust version 1.0? Should we wait for versions 1.1, 2.0, or 3.0? Can parts of a standard be reliably used while other parts are less mature? Waiting is only for those

that have the luxury of time—defense programs usually don't have that luxury. It is the goal of every SDO to furnish a useful standard with each release. It's also reasonable to expect some ambiguity and imperfections in every version. We must use the tools we have, not the tools we wish we had. Standards are less than perfect, but they are still useful.

Using mature standards is preferable, but not always possible. Each program must assess the risk of using a standard versus the risk of not using the standard, remembering that MOSA is a requirement. In most cases, the risk of not using an open standard will be greater than the risk of using an immature standard. Standards reduce risk at an interface by furnishing guidance and restrictions that reduce ambiguity. System integration resolves remaining ambiguities into a working system.

Using open standards that have a well-defined conformance or compliance method further reduces program risk. If that process uses an independent third-party assessor, even more risk is mitigated. Just like standards, conformance and compliance methods are developed over time, but lag behind the standard. Resources are limited in SDOs and development of the conformance and compliance method can't be completed until the standard version is finalized. Assessment of compliance or conformance to a standard does not replace a test program. These assessments may augment your test program, but they do not assess performance.

While it's reasonable to expect open standards will reduce the burden of system integration, it's unreasonable to expect to eliminate integration in complex systems with standards. Interface standards supply specifications and guidance to limit choices, thus reducing ambiguity at the interface. Interfaces also have layers. The Open Systems Interconnect model describes seven layers of a communications interface. Most standards reasonably focus only on a subset of these layers, so their use may be broader than one specific case.



SUMMARY

Open standards come from those who get involved and develop them. You can discover which standards are applicable to your program by looking for information and asking about open standards. MOSA is a new slice to the standardization process and we all bear a responsibility for seeking out and developing standards. We'll know which standards to use by staying connected and getting involved in standards efforts. Get out there and make open standards and MOSA the new normal!

ABOUT THE AUTHOR

John C. Bowling *is an Air Force civilian electronics engineer serving as technical expert for Avionics Architectures and Interoperability in the Engineering and Technical Management/Services directorate of AFLCMC. His role encompasses participation in standards bodies, aircraft program office support, and technical support to the airworthiness process. He advises Air Force acquisition programs on open systems architecture and interoperability requirements and methods throughout the acquisition lifecycle*

A Key Requirement to National Security

A Case for Enforcing Modular Open Systems Approach Requirements

Bob Matthews, Tom DuBois, and Patrick Collier

INTRODUCTION

Our nation is standing at the precipice of a new era. Our strategic technological superiority is being eroded by nation states and asymmetric adversaries who are leveraging new commercial technologies faster and cheaper than the U.S. defense market can accommodate through traditional methods and processes. Our customers recognize the need to deliver new capabilities more efficiently but struggle to find a cohesive and effective strategy. There is a growing consensus in Congress and DoD that a modular open systems approach (MOSA) and the use of open systems architectures (OSA) can address these gaps. However, until recently, there was limited agreement on the standards and directives needed to be effective.

That situation has changed significantly with convergence efforts led by the Army, Air Force, and Navy, and from many government and industry-led OSA open and published standards efforts. This article explores the relevance of MOSA, how it is applied to these efforts, and what must happen to ensure overall success.

MODULAR OPEN SYSTEMS ARCHITECTURE PARADIGM SHIFT

Often, legacy systems have been program-specific solutions designed to address a customer need with a unique system. For most of these programs, the system architecture is derived and documented as the result of the design process and system interfaces are optimized for performance to more efficiently deliver a specific capability. This micro-performance focus is reinforced by the lack of enforceable, customer macro-performance requirements for portability, scalability, resiliency, or extensibility that drive modular architecture, are readily adapted and extended through upgrades, and leverage state-of-the-art technologies throughout the program lifecycle.

The cost and schedule of delivering, upgrading, and maintaining micro-performance systems is rising dramatically while the defense budget and more adaptive adversaries are creating immense pressure to deliver capability faster and cheaper. These pressures are forming a new market landscape with a growing desire for substantive change. The U.S. government and DoD prime contractors are advocating for increased competition, rapid prototyping, and MOSA to combat these pressures, but with unique, vague, or otherwise unverifiable requirements.

To make change effective and spur innovation in a new market, our customers must coalesce around a consistent set of verifiable standards for key interfaces, make macro-performance attributes clear discriminators in selection criteria, and be cognizant of the long-term effects from suboptimizing architectures for micro-performance at the expense of macro-performance.

To meet these requirements, suppliers need to develop high technology readiness level, modular, and affordable hardware and software solutions. Product line experts agree that successful supplier components and subsystems will demonstrate the quality attributes of portability, scalability, resiliency, and extensibility.

As a specific example, the U.S. Army Combat Capabilities Development Command (Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance) Center is advocating for adoption of the Modular Open Radio Architecture (MORA) based on ANSI/VITA standards as part of the Vehicular Integration for the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance/Electronic Warfare (EW) Interoperability (VICTORY) approach. The U.S. Air Force is petitioning the VITA standards organization to adopt new ANSI/VITA 65.0 backplane and module slot profiles that align closely with the MORA initiative. The U.S. Navy is cooperating with both initiatives for the development of its Hardware Open Systems Technology (HOST) initiative and all services are working toward convergence of hardware standards across the services. Key component suppliers (Curtis Wright, X-ES,[1] Mercury, [2] Elma, [3] and others) are investing in these OSA initiatives to influence standards and offering products aligned with these objectives to gain experience and early adopter market dominance.

MOSA RELEVANCE

The complexity and cost of DoD avionics and mission systems is increasing at an exponential rate while the time to field new capabilities remains stagnant. In contrast, near-peer and asymmetric adversaries are

---

1 VICTORY, "Participants," https://victory-standards.org/index.php/victory-part.

2 Mercury Systems, "OpenRFM: A New Open Architecture for RF," https://www.mrcy.com/OpenRFM/

3 Elma, "3U VPX 12-slot CMOSS Backplane" overview, BKP3-TIM 12-15.3.6-3 Rev5–062617; www.elma.com.

exploiting new technologies for military advantage at an accelerating rate for far less. There are myriad excuses for why our opponents have an unfair advantage, but unless we are willing to concede, it doesn't matter. The United States and its allies must find ways to delivery new and disruptive technologies faster and repeatedly. To compound the issue, capabilities must be more cost effective or we risk becoming the victim of the next economic cold war.

DoD leadership has acknowledged the imperative to maintain our nation's technological superiority. Better Buying Power encompassed multiple initiatives, including MOSA, for achieving dominant capability with innovation and integration excellence. The recent tri-service MOSA memo highlights the criticality of data interoperability across domains for achieving information dominance. Indeed, MOSA attributes are essential to unlocking our innovation in many ways:

- Breaking monolithic system architectures with open, standard, and government-controlled interfaces so no one entity can monopolize the system. This enhances competition and facilitates technology refresh while enabling cost savings.
- Defining highly cohesive, loosely coupled, and reusable components to enable the rapid insertion of commercial, competing, and innovative technologies.
- Defining verification and test requirements to ensure developers meet MOSA standards from the component- to system-level requirements.
- Supplying robustness to data interfaces to reduce integration risk significantly and improve interoperability.

An effective MOSA can ensure sustained resiliency and interoperability across domains while adapting to a continuously evolving threat.

Challenges

As technology cycles shorten, DoD integration timelines remain the same; therefore, obsolescence begins before full operational capability (FOC) is achieved (*see Figure 1*). This gives adversaries the opportunity to exploit new technologies and counter capabilities before FOC. From a development perspective, the integration timeline limits innovation. While the need for MOSA seems intuitive, achieving the benefits has been elusive. With more than 20 years of DoD programs that have attempted to implement modular open system principles, why are there only limited and anecdotal success stories? There is

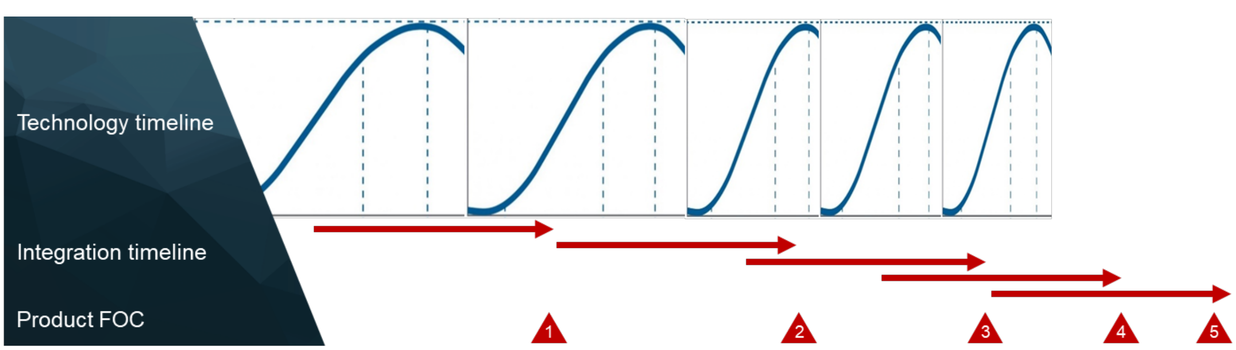


Figure 1. The VDB Architecture

something fundamentally missing from the approach. With research, a pattern forms. Common failure modes include the following:

- Failing to make MOSA a firm requirement. Using words like "to the maximum extent practicable" instead of "shall" are hallmarks of risk-adverse contracting. This is a symptom of underestimating the benefits of MOSA and overestimating the risk associated with change.
- Specifying a company, platform, or unique set of open interfaces. This occurs when deferring the decision of open standards to the contractor's selection. Many of the mission and financial benefits rely on consistent interfaces between platforms, so defining a consistent set of multi-platform, multi-domain interfaces prior to solicitation is an essential system-of-systems engineering task.
- Failing to test MOSA requirements. Anyone can pass a test with no questions. Without detailed test plans, there is no way to verify if a design is compliant or conformant to the MOSA standards.
- Trading off MOSA requirements. Even the most well-intended programs face financial pressures. Far too frequently, MOSA requirements are traded to achieve short-term gains in another performance parameter. Unfortunately, the operational effect of trading off MOSA is poorly understood and subsequently undervalued.

APPROACH

To address these shortfalls, programs must decide which of the multiple open standards to use. There are many good standards but selecting the correct one requires a deeper understanding of which standard or set of standards is applicable for the task. *Figure 2* depicts a notional Venn diagram demonstrating the relative relationships between standards and across domains. More

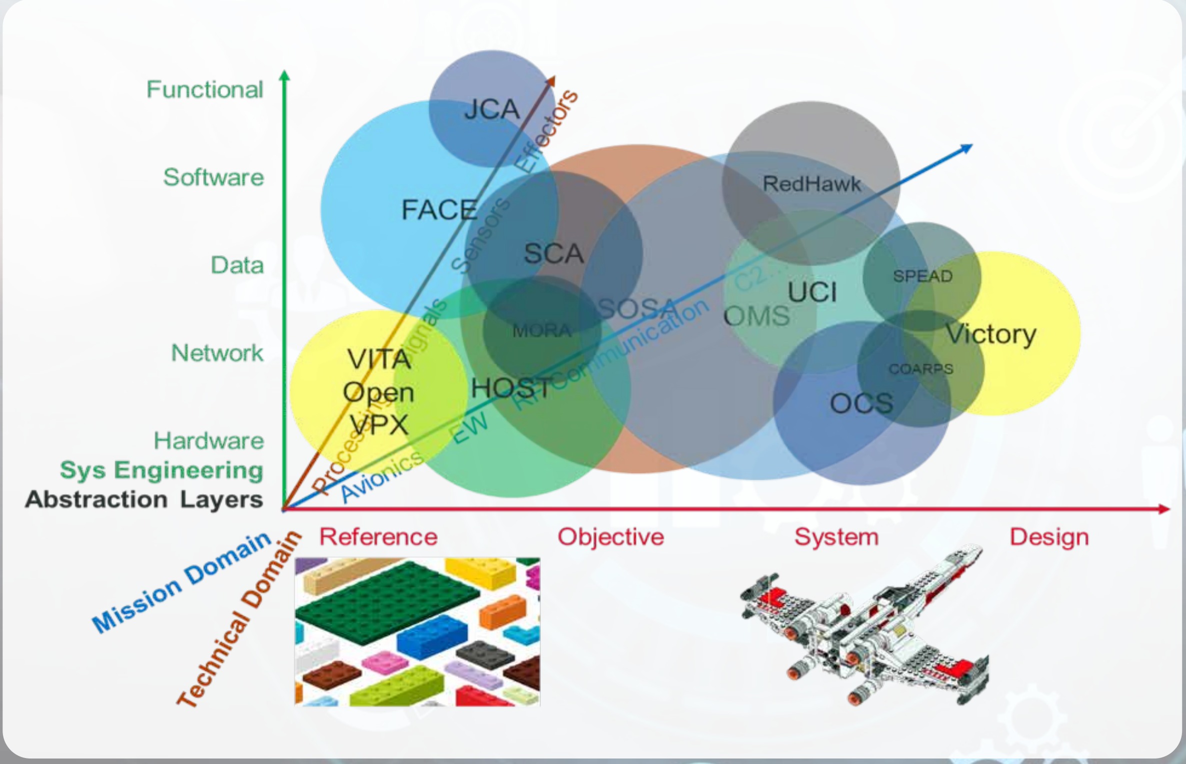


Figure 2. Ecosystem of Open and Published Standards with Systems Engineering Focus and Technical Domains

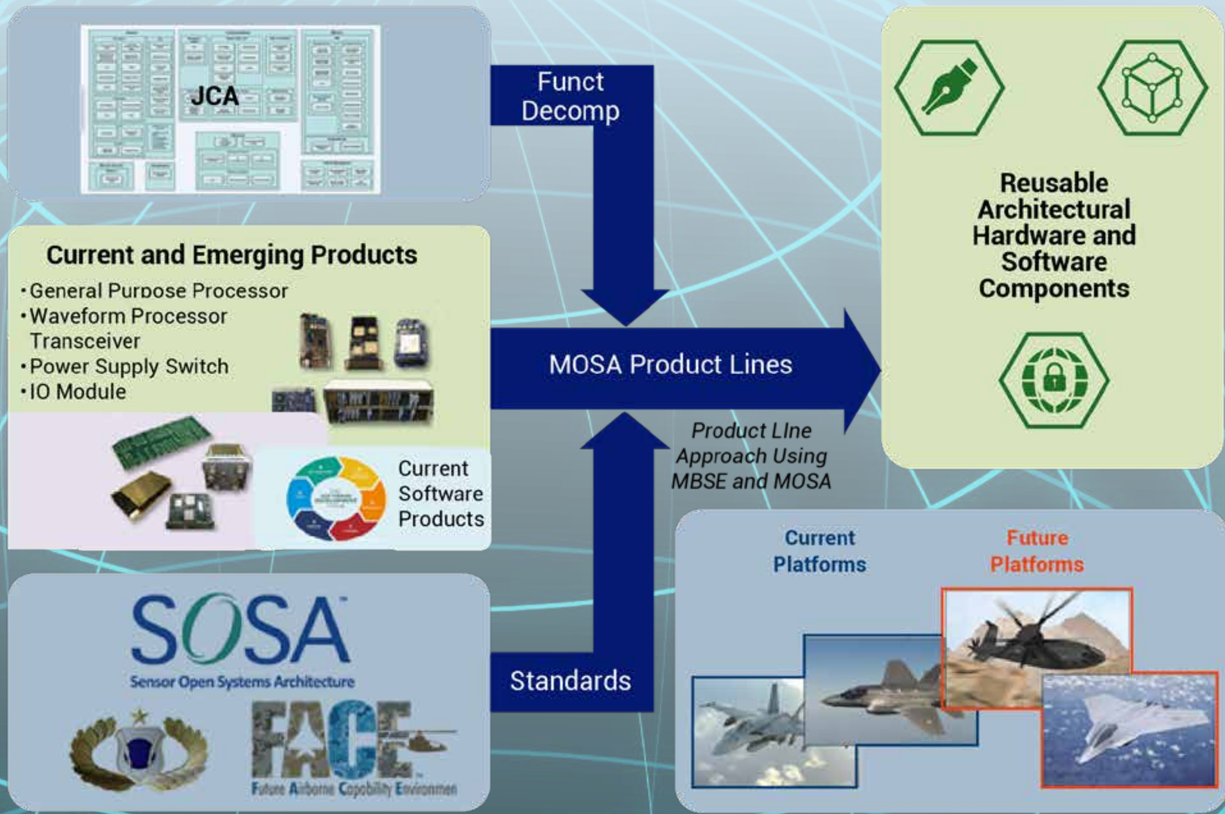


Figure 3. *Process Example to Achieve Product-Line Architecture and Balance Government and Industry Interests*

effort is required to document these relationships to supply programs with the tools to select the appropriate MOSA standards.

Creating alignment between government and industry motivations is essential to reducing friction for meaningful adoption of MOSA. A common interest to both is the desire to deliver innovative capabilities to the warfighter. Setting clear expectations that shorten development cycles and supply cost savings for reinvestment in new innovations against evolving threats will serve the interests of the public trust and shareholders.

Government and industry agree that a product-line approach balances interests while achieving MOSA principles. The government published the Joint Common Architecture (JCA) as a reference of software components developed through government-industry consensus on functional decomposition of weapon systems. Industry has the flexibility to perform its own functional decomposition based on its product offerings. A product-line approach that preserves a company's products while aligning to the JCA is one way to achieve the right balance of government and industry interests *(see Figure 3)*. But how **do the components fit together? This is where a**

With more than 20 years of DoD programs that have attempted to implement modular open system principles, why are there only limited and anecdotal success stories?

government-industry partnership on MOSA is needed. Not only does this approach need to select the right open standards, but both parties must reach agreement on implementation to avoid a lock on future business. Following an open standard without agreement enables a developer to integrate a system like fitting puzzle pieces together. The puzzle can be completed, but it is difficult to use those pieces for a different system or improve the system without significant involvement from the integrator that completed the initial system. Most suppliers have components built to fit different systems. Obtaining government-industry agreement on the implementation of MOSA can help transition integration from fitting puzzle pieces together for one system to having a set of Legos that can be used for many different systems. Transitioning from puzzle pieces to Legos can result in components that are integration ready and have fully defined and open interfaces.

The approach is a combination of preparation and perspiration. Preparation involves selecting the right standards for the right function, domain, and customer. Industry needs to manage internal building blocks to the next lower level, and then align current products to the future state to ensure that both reusable products and new innovations are integration ready. Perspiration requires a commitment to the long-term return on investment (ROI) since the solution will span more than one integrated system, encourage agreed-to MOSA enforcement, and expect competition for innovation.

Industry needs to find ROI from multiple system offers, lower development cost, and lower lifecycle cost, while steering clear of "golden screws" that can be inserted while following an open standard. Examples of golden screws are integration that can only be accomplished using the integrator's tool, proprietary interfaces used but not specified by the selected open standards, or use of an infrastructure element (e.g., operating system or middleware) that can only be swapped out at high-reintegration cost.

SUMMARY

The MOSA direction is clear, but government and industry leadership is not yet fully committed to it. Industry needs to break free of single-program ROIs and recognize the value of MOSA with due consideration of the internal process changes that will be required to address it. Government must resist the expediency of accepting proposals that check the box on following an open standard, but do not meet the full spirit and intent of what is implied by MOSA. This vision can only be accomplished with a higher degree of partnership between government and industry built from a product-line approach that is agreeable to both.

VICTORY for MOSA

Grace Qi Ping Xiang and Michael Scott Moore

INTRODUCTION

The Department of Defense has anticipated the needs of future programs, evaluated approaches and accomplishments of ongoing open system architecture (OSA) and standards efforts, and concluded that modular open systems approaches (MOSAs) for our weapon systems is a warfighting imperative. This agreement was documented in a memorandum signed by all service secretaries stating that modularity in and between weapon systems is paramount and transition to MOSA and modular systems will require common standards and guidelines for how to apply them. The memorandum listed several ongoing efforts as examples for how this may be done.

One existing effort highlighted was the Vehicular Integration for Command, Control, Communication, and Computers, Intelligence, Surveillance, and Reconnaissance and Electronic Warfare (C4ISR/EW) Interoperability (VICTORY) initiative. VICTORY defines an OSA and set of open standards for enhancing

__Disclaimer:__ Reference herein to any specific commercial company, product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States government or the Department of the Army (DA). The opinions of the authors expressed herein do not state or reflect those of the United States government or DA and shall not be used for advertising or product endorsement purposes.

interoperability in Army ground vehicles. However, transitioning to MOSA across defense acquisition programs requires more than continuing existing efforts. It is necessary to formalize existing approaches, extract patterns and lessons learned, and support the community with detailed guidance for how to apply these approaches to solve different types of problems.

In this article, we present VICTORY as an example OSA and standard effort from which to learn. We describe the effort from business (the problem space, business drivers, and objectives), technical (items being modularized, interfaces being standardized, and approach toward interoperability), and governance (organizations involved and how the work products are managed) viewpoints. We highlight lessons learned from this experience and aspects that make VICTORY distinct and a worthy exemplar.

OVERVIEW

VICTORY has defined an in-vehicle network architecture and a set of open interface standards for integrating electronics systems in military ground vehicles. The effort originated from an evaluation and analysis begun in 2008 for the U.S. Army Program Executive Office for Command, Control and Communications-Tactical (PEO C3T) Futures Office. The first version of the VICTORY architecture was published in 2009 and a government-led standards body kicked off on May 5, 2010. As of 2019, the VICTORY Standards Body has over 400 members from government, industry, and academic organizations. The VICTORY architecture and standard specifications have been developed, matured, and are supported by compliance test tools. New capabilities are added as needs evolve, but most of the scope is baselined.

Business Viewpoint

PROBLEM SPACE

Previously, electronic mission systems were integrated with military combat and logistics platforms using a bolt-on approach. As mission systems were added, the growing net size, weight, and power (SWaP) of the systems presented complexity, cost, and schedule challenges (see Figure 1). In addition, sharing

Figure 1. *The Traditional Acquisition and Integration Approach versus the VICTORY OSA Approach*

data between stovepiped systems required point-to-point communications, which resulted in limited interoperability. Interoperability between systems represents an opportunity for significant utility, increased situational awareness, simplified maintenance and sustainability, and capabilities, such as display and analysis across data sources, cross-cueing, and data fusion.

BUSINESS DRIVERS

Because vehicles and mission systems were procured separately, the mission systems included independent computing hardware, user interface devices, and interface wiring. Interoperability was an afterthought and required point-to-point interfaces. This situation was a primary driver for the architectural and technical choices made in VICTORY.

OSA and standards efforts list high-level goals, such as affordability (lower integration and lifecycle costs), increased competition (reduced vendor lock), and faster update cycles (lower cost and time to insert new capabilities and the ability to reuse capabilities across programs and services). Although valid ideas, specific details on the business and technical problems targeted are needed to uncover the relationship between the solutions and the architectural decisions, which is the key to understanding the relevance of an OSA and standards effort.

The VICTORY business goals, as paraphrased from the VICTORY architecture,[1] include the following:

- Furnish an approach to minimize stovepiped mission systems.
- Reduce the SWaP and system cost effects of adding electronics systems to vehicles.
- Simplify integration, enhance interoperability, increase capabilities, and reduce overall lifecycle costs.
- Maximize mission system portability and interoperability by defining open interface standards, data formats, and protocols for vehicle communities.
- Support current and future information assurance (IA) requirements.

[1] VICTORY Standards Support Office, *VICTORY Architecture*, Version A, April 2, 2019.

VICTORY completely defines the syntax and semantics of network messages as they will exist on the wire so that physical components of different vendors and for various systems will interoperate when plugged into the same network. This approach is practical because VICTORY defines the in-vehicle network based on ubiquitous networking technologies, such as ethernet, internet protocol (IP), transmission control protocol, user datagram protocol (UDP), and internet group management protocol. Having the freedom to choose the underlying network technologies simplifies the problem of network interface standardization. VICTORY defines the messaging interfaces, the message exchange protocol, message contents, parameter semantic, syntax, encoding, and encapsulation. Fully specifying on-the-wire network interfaces reduces the choices made when integrating a system (the design space).

TECHNICAL OBJECTIVES

These business drivers and the ground vehicle technical environment led VICTORY to first define a modular in-vehicle network architecture to support interoperability, and then define on-the-wire network interface standards by which modular C4ISR/EW entities, weapon systems, protection systems, and vehicle systems can interoperate.

VICTORY architectural tenets embody the technical objectives derived from the business drivers:

- The data bus
  - supplies shared network transport, processors, displays, and common services;
  - furnishes standard, open network-based interfaces to components and systems; and
  - integrates C4ISR/EW systems and interfaces with other electronics systems.
- The architecture
  - treats IA as vital and addresses multiple domains on a vehicle,
  - enables time-critical processing to be integrated tightly with sensors,
  - allows data bus interfaces to be secondary to internal sensor interfaces (e.g., high-rate video), and
  - must enable an evolutionary approach toward network-centric C4ISR/EW.
- VICTORY offers a roadmap from current to future architectures.

Technical Viewpoint

The VICTORY architecture defines the VICTORY data bus (VDB) as an ethernet-based, in-vehicle network through which C4ISR/EW systems are integrated and platform systems are interfaced. The VDB is made up of modular elements and instantiated in hardware and software components. *Figure 2* illustrates the VDB and its context and highlights its interactions with various groups of C4ISR/EW and platform systems.

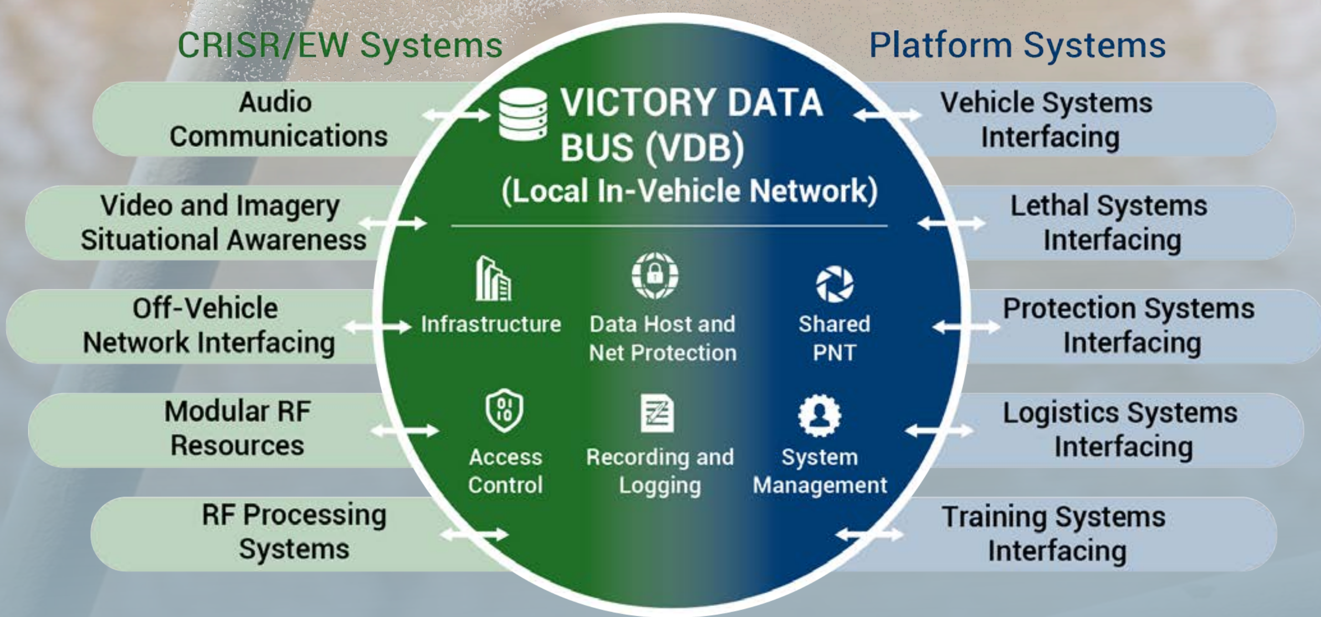


Figure 2. The VDB Architecture

The primary architectural structure, the VDB, is a normal network based on ubiquitous, open network standards, but with additional domain-specific capabilities to tailor it for military ground vehicles. More detail can be found in the VICTORY Architecture[2] and VICTORY Standard Specifications[3] documents. *Figure 2* also illustrates relationships between the VDB and various groups of C4ISR/EW capabilities and platform systems on the vehicle. The bidirectional arrows between the VDB and these elements indicate that the VICTORY standard specifications define open interfaces for the capabilities or systems indicated. This article does not go into detail about these interfaces, but highlights general characteristics, such as the types of interactions and technologies, and common functionality. The groups of interfaces can be differentiated by considering the granularity of the capabilities in each group.

SYSTEM-LEVEL INTERFACES

Note that platform systems and some of the C4ISR/EW capability groupings include the term "systems" or "interfacing." For these groupings, VICTORY defines standard data and management interfaces for high-level interoperation via the VDB but does not furnish the main transport or interfaces for integrating the system components. For example, the automotive control systems on ground vehicles are often built around serial communication protocols, such as a controller area network. The components that make up the automotive system, such as engine and transmission controllers and various types of sensors and actuators, are integrated by the vehicle original equipment manufacturer message sets standardized for those uses.

VICTORY defines system-level interfaces for data transport, configuration, control, status reporting, and fault management for systems in each of the categories shown in the figure. This enables systems to use VDB services, such as shared position, navigation, and timing and access control, and to be managed in a common way. System-level interfaces are secondary to the core system functionality and do not interfere with their operation but furnish useful interoperability between systems on the VDB.

COMPONENT-LEVEL INTERFACES

VICTORY defines component-level interfaces in addition to system-level interfaces. The VDB supplies the primary data transport and standard interfaces for components in the audio communications, video and imagery situational awareness (VISA), and modular radio frequency (RF) resources capability groups shown in *Figure 2*. Examples of component-level interfaces can be seen in the VISA capabilities group. This group is composed of video sensors, pan and tilt modules, and digital video streaming sources. VICTORY defines component-level interfaces to discover, publish, and manage data streams, configuring, controlling, and managing the health of each of these.

COMPONENT TYPES

The VICTORY architecture defines component types, which are logical modular elements that encapsulate a set of functionality and network-based interfaces that support those functions. The component type concept is equivalent to the concept of a module in other architectures, such as Sensor Open Systems Architecture (SOSA™).[4] Component types may be in hardware, software, firmware, or combinations, and can be combined in single devices or software components when implemented.

---

2 See Note 1.

3 VICTORY Standards Support Office, *VICTORY Standard Specifications*, April 2, 2019.

4 Sensor Open Systems Architecture (SOSA™), http://opengroup.org/sosa.

Some component types are inherently service-oriented—their function is to implement network interfaces that publish data or supply information upon request. Other component types imply underlying hardware, such as a switch and shared processing unit (computer). For simplicity, the term component type is used for component types whether they furnish system-level or component-level interoperability.

The VICTORY architecture defines a large set of component types which, for practical reasons, have been organized into a hierarchy of categories. The top-level categories are VDB architecture, information assurance architecture, C4ISR/EW systems architecture, platform systems architecture, and VICTORY configuration description. For brevity, we do not describe the full hierarchy. That information may be found in the VICTORY architecture document.[5]

COMPONENT-TYPE INTERFACES

Component types may include several network-based interfaces:

- **Data transport interfaces** address communication functions at the transport layer and below, including data formats, protocols, signaling, and physical media specifications.

[5] See Note 1.

- **Auto-discovery interfaces** enable components to be detected automatically on the network to support plug and play.
- **Data (publishing) interfaces** address communication functions above the transport layer, up to the application layer, including data formats and protocols. Data interfaces use a publish-subscribe pattern that enables one or more publishers to share data periodically with subscribers. The data streams are organized into channels.
- **Data logging and retrieval interfaces** enable data to be acquired from the network or generated internally to a component to be logged to a non-volatile medium, then retrieved in a standard format, and for that logging functionality to be managed from the network.
- **Health reporting interfaces** supply publish-subscribe style reporting of status and fault information.
- **Management interfaces** address configuration, control, and health (status and fault reporting) functions for systems, components, and data publishing mechanisms. Management interfaces are based mainly on a request-response model, but also include event-driven notification behaviors.
- **Security log interfaces** furnish a standard method for logging and retrieving data related to significant security events.
- **Access control interfaces** control access to other interfaces, particularly the request-response management interfaces.
- **High-volume or low-latency data transport interfaces** are data transport interfaces capable of delivering high-volume data streams (e.g., high-definition video), delivering data with low latency (end-to-end latency on the order of 1 microsecond), and offering higher levels of certainty and reliability than the normal data transport interfaces.

INTERFACE SPECIFICATIONS

We describe a subset of the interface types here, but only at a high level. The full technical details can be found in the VICTORY standard specifications document.[6] All VICTORY network interfaces are standardized for on-the-wire interoperability. The component type interface standards define the encoding of operations and parameters, encapsulation into network payloads, mapping of payloads to transport units, and binding to an underlying transport technology for the interfaces. The VDB network infrastructure standards require IP and ethernet at the network and datalink layers, and several different options for technology bindings at the physical layer. Thus, the overall standard defines all layers of the open systems interconnect network model. This implies that two components can interoperate on the VDB independent of whether they were implemented in hardware or software, what programming language was used, what compilers or tools were used, and whether the components are hosted on the same or different processors. On-the-wire interoperability may also be called implementation-level interoperability.

Note that some architectures and standards, such as the Future Airborne Capability Environment (FACE™), [7] do not target implementation-level interoperability, but instead standardize at the conceptual or logical level. These different approaches to interoperability are valid choices that

[6] See Note 3.

[7] Future Airborne Capability Environment™ (FACE), http://opengroup.org/face.

are driven by the business goals and technical realities in the application domain.[8] The top goal of FACE™ was software portability, and it is required to support a wide variety of hardware and network technologies. For that reason, FACE™ standardizes a layered software operating environment and logical-level interface definition language instead of on-the-wire interoperability.

Conceptual-Level Data Definitions: Values that are encoded into messages or application programming interfaces are described in detail in the standard specification. In lieu of a formal, machine-readable data model, VICTORY leveraged structured textual definitions supported by diagrams and tables. The standards body went to great lengths to ensure that the syntax, semantics, coordinate reference systems, units, valid values, and other constraints of each value type and data structure were described in sufficient detail so that implementers would have a common understanding of how to interpret the values passed between component types.

Defining the value and data structure types required a significant level of effort (between 20% to 40% of the work necessary to define the technical specification for a VICTORY interface). At the beginning of the effort, the percentage of work was higher but has trended lower (but not to zero) as the team gained more experience and had content. This level of effort is independent of how an effort chooses to define data types, given the appropriate level of detail is supplied.

Auto-Discovery Interfaces: VICTORY leverages zero-configuration networking for dynamic discovery of entities on the VDB. Dynamic discovery is securely operated based on the context and platform requirements.

Data Interfaces: These interfaces use data that is shared via a publish-subscribe pattern encoded in eXtensible Markup Language formatted strings, encapsulated in payloads called a VICTORY data message (VDM), and transported in UDP/IP datagrams on the network to multicast addresses. This bit-inefficient but simple approach was chosen because the types of data shared are neither wideband (hundreds of kilobits per second) or high-frequency (tens of messages per second) and do not have tight latency constraints (milliseconds end to end is acceptable). The encoding and decoding overheads are nearly negligible for these data interfaces. The high-volume or low-latency data transport interface types require a higher performance approach to encoding, encapsulation, and transport.

Management Interfaces: These interfaces configure, control, and manage the health of a VDB implementation; its devices, software components, and component types; and the platform and mission systems with which it interfaces. Management interfaces are mostly based on request-response interactions in which a user (client) sends a request message to a provider (service), and the provider sends a response message back to the sender. The request message encodes an operation and its parameters, and the response message encodes the return parameters.

Health Reporting Interfaces: These interfaces report status and health events on the VDB using a publish-subscribe pattern. Instead of

[8] Leonard Elliott, Syltinsy P. Jenkins, Howell S. Yee, and Michael S. Moore, "Potential for VICTORY and FACE Alignment—Initial Exploration of Data Interoperability and Standards Compliance/Conformance," presentation Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, August 13–15, 2019.

Adding the in-vehicle network, shared hardware resources, and open interfaces to electronics systems in vehicles facilitates interoperability, modularity, and extensibility. This also adds the responsibility to take care of these new components and their integration. VICTORY recognizes the need to address configuration management, status and fault reporting, mode and state control, health logging, and cybersecurity by creating controls and interfaces for the in-vehicle network. Each component type includes management interfaces, and the in-vehicle network supplies a system management service to support various setup, configuration, control, health tracking, and maintenance activities.

VDM encoding, the payload encoding is based on the Syslog protocol commonly for reporting and logging computer and network events.

Governance Viewpoint

One of the most important aspects of any OSA and standards effort is how it is governed. Governance includes management (how the overall effort is managed, funded, and directed), coordination (how it cordinates with stakeholder communities to ensure their viewpoints are considered and concerns addressed), work product development (how the work products are developed, matured, configured, and maintained), compliance (how the conformance and compliance of products is evaluated and certified), and program support (how it supports programs in development of mandates and requirements, and implementation of products). *Figure 3* illustrates the VICTORY governance organization.

EXECUTIVE STEERING GROUP

The VICTORY Executive Steering Group (ESG) sets the direction and priorities and supplies resources for the VICTORY initiative. PEO Ground Combat Systems is the managing partner, and membership includes PEO Combat Support and Combat Service Support, PEO C3T, PEO Intelligence Electronic Warfare and Sensors, and multiple combat capabilities development command (CCDC) centers. The Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance and Reconnaissance Center and Ground Vehicle Systems Center (GVSC) has been particularly active in VICTORY.

VICTORY STANDARDS SUPPORT OFFICE (VSSO)

The VSSO serves as the executive agent managing the VICTORY initiative under ESG guidance. The VSSO hosts and staffs the leadership of the standards body, which includes government and commercial participation. The VSSO leads the development, maturation, and maintenance of the VICTORY framework products:

- **Architecture Document:** defines common terminology, structures, component types, and interfaces.
- **Standard Specifications Document:** supplies technical interface specifications for each component type.
- **Compliance Test Suite (CTS):** furnishes the gold standard Compliance Test Plan,

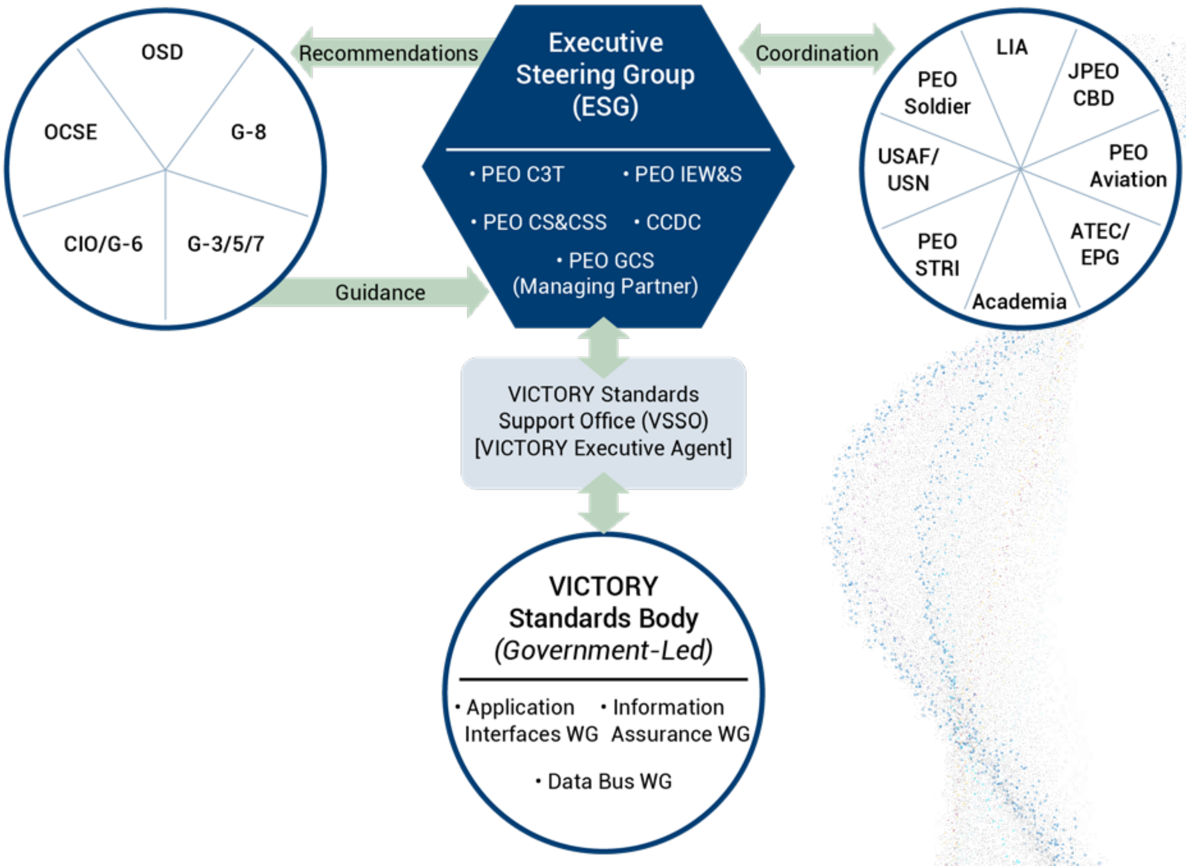


Figure 3. The VICTORY Governing Organization

Compliance Test Report (CTR) template, and the Compliance Test Tool, which automates much of the compliance testing for each component type. This ensures that the VICTORY standard specifications are testable and define a standardized method and common format for documenting the test results.

- Reference Designs: supplies samples of how to use the standard specifications on an as-needed basis.
- Validation Artifacts: furnishes documentation of the validation process and results of the initial implementation of the standard specifications along with reusable software to validate the specifications.
- VSSO Reference Software Library and GVSC libVICTORY: two government-owned (independently developed) reusable software implementations of the published specifications. Both software implementations have been verified using the CTS and made available to the VICTORY community.
- Process Document: describes the process executed to develop, mature, configure, and verify VICTORY specifications.

A subset of these core framework products is available via the VICTORY public site. The remainder are distribution limited to U.S. government organizations and contractors. Requests can be submitted to the VSSO.

The VSSO assists acquisition programs in developing acquisition language and requirements for adopting VICTORY standard specifications and reviewing CTRs delivered by vendors claiming compliance. The VSSO also assists commercial organizations in interpreting the specifications and using the artifacts to interpret, develop against, and test compliance with requirements. The VSSO explicitly does not test or certify compliance of or recommend use of products.

The ESG resourced the VSSO with a core technical team with expertise in OSA and standards, and technical understanding of the acquisition programs. This core technical team developed and manages the VICTORY framework products, supplies leadership and execution support for the standards body, and offers engineering reach-back support assisting program manager adoption of the OSA and standard specifications.

VICTORY STANDARDS BODY

The standards body consists of a set of working groups (WGs), which develop, document, and maintain the technical standard specifications. WG membership is mostly government and vendor subject matter experts (SMEs) in various technical areas. The general membership is not funded by the VSSO, so the working groups are staffed by a volunteer workforce, which is the core reason why standards take a long time to develop and mature.

STANDARDS DEVELOPMENT AND MATURATION PROCESS

The VSSO executes the process illustrated in *Figure 4* to develop and mature the VICTORY framework products.

- **Change Proposal Process:** The standards body creates technical specifications for interfaces in the architecture. Government-led task groups incorporate technical recommendations from industry participants. Change proposals (CPs) are formed and finalized through a well-documented consensus-building process. The VSSO facilitates this process to reach consensus. The detailed CP process can be found in the VICTORY process document.[9]
- **Initial Validation and Compliance Verification:** The VSSO conducts an initial validation process to mature specifications after documentation through the WG consensus process. The validation process includes development of reference software and execution of an experiment to evaluate the quality of the specification. The VSSO then creates compliance artifacts, which supply a second level of maturation for the technical standards. The findings of the initial validation and compliance artifact development process are documented as a set of recommended updates to mature the specification and furnished as feedback to the standards body. When the standards body addresses the recommendations, and the specification is fully supported with a CTS, then it is raised to the proposed standard level of maturity. The proposed standard level of maturity is considered ready for publication and adoption by acquisition programs and commercial vendors.
- **Configuration Management**: The VICTORY Configuration Control Board (CCB) manages changes to and publication of VICTORY framework

9 VICTORY Standards Support Office, *VICTORY Framework Product Development, Maturation, Approval, and Compliance Verification Process Document*, August 28, 2019.

products. The CCB governs changes in the published specifications using an engineering change proposal process. This process is critical to ensure that specifications have long-term support in the documentation and toolset. To further this goal, the VSSO created an certification authority was necessary for all implementations. Instead, the VSSO supplied the CTS to the community so that implementations could be freely evaluated by vendors, integrators, or the government. However, a certification authority may be needed in some cases,

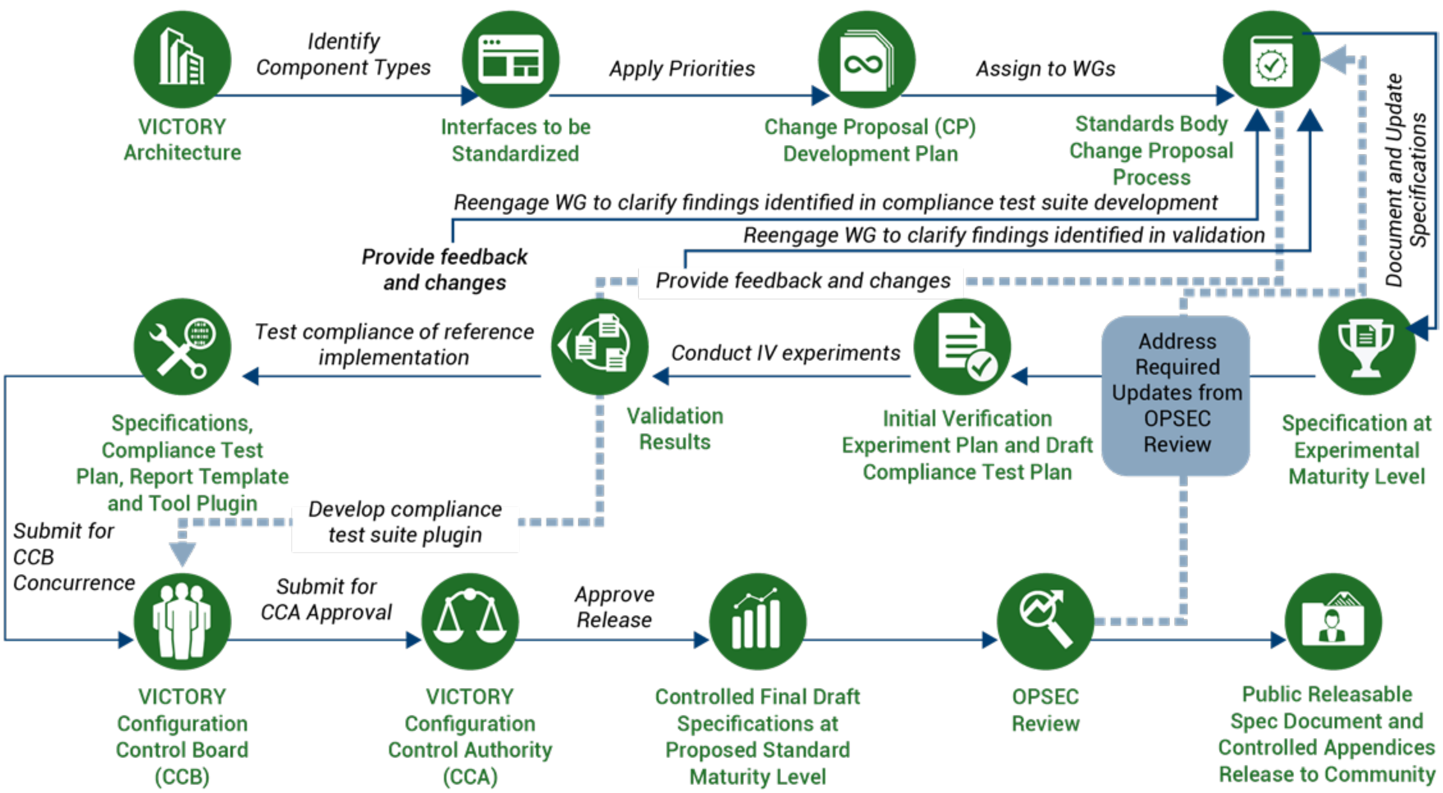


Figure 4. The VICTORY Artificacts Development, Maturation, and Change Control Processes

inter-version interoperability approach and works closely with the community to ensure programs adopting different versions of the same VICTORY specification can interoperate with each other.

- Certification Authority: There is no certification authority set up for VICTORY. The VSSO did not feel that a

so various government and commercial organizations are setting up facilities to furnish independent, third-party compliance testing services (for a fee). The use of a third-party compliance testing facility to test and document compliance of a product is up to the acquiring organization but is not required by the VSSO.

Relationships and Extensions

The VICTORY architecture and standard specifications are being extended to the RF applications domain by CCDC C5ISR Center through Modular Open Radio Frequency Architecture (MORA). MORA is, in-turn, part of a larger effort: C4ISR/EW Modular Open Suite of Standards (CMOSS). CMOSS and MORA, and thus VICTORY, are being adopted or referenced across the RF sensing communities in the Army, Air Force, and Navy through the SOSA™ effort. VICTORY data types and interfaces are being referenced by the Autonomous Ground Vehicle Reference Architecture effort in CCDC GVSC Ground Vehicle Robotics. There are many opportunities for aligning VICTORY standards with others.

CONCLUSIONS

VICTORY is a government-led OSA and standards effort that defines a network-based architecture and interface standards for how electronic components and subsystems interoperate in military ground vehicles. VICTORY supplies a set of tools to support the community in developing requirements, implementing and evaluating compliance against the standards. The VICTORY Standards Body membership includes a broad array of government, commercial, and academic organizations. VICTORY is being implemented by the Army ground vehicle and C4ISR/EW programs.

VICTORY's successes can be attributed to many people: leaders who saw the need and potential and those who formed the vision and resourced the execution as well as the hard work and commitment of the VSSO and the standards body. At least part of the success comes down to good fortune and timing, but a few aspects should be highlighted as lessons learned.

1. The business need and overall conceptual approach of VICTORY was developed by the government. Individuals in the government took ownership of the initiative to champion the idea and manage the execution. These people became the core of the VSSO, and without their personal dedication, the VICTORY Standards Body would not have gotten off the ground.

2. The VSSO is empowered and resourced by the ESG to staff leadership and direct execution support to the standards body. As technical topics are handled, task teams are formed of relevant government and industry SMEs, whose companies volunteer a small part of their time to supply the detailed technical expertise necessary to address particular topics as they come into focus. The VSSO executes much of the tedious work in the standardization process, such as facilitating and documenting technical discussions, documenting decisions, and creating and managing the standards documents. This is more time and cost efficient because the VSSO can dedicate time to these tasks while the SMEs are part-time volunteers. The VSSO has also become knowledgeable and experienced in how to guide the WG membership in the specification development and consensus-building processes.
3. The VSSO created the architecture prior to forming the standards body. The government stakeholders invested the time to evaluate the business and technical aspects of the processes and products and find the pain points from the government stakeholders' viewpoints. The government selected the problem it wanted to address, and then formulated the conceptual approach to a solution. Then, it socialized the concept in the government and provider communities and matured it based on that feedback. When the standards body was kicked off, the potential members were not asked "what do we need?" but instead "how can you help us realize this vision?" The industry representatives saw that the government had thought through the problem and had a vision of what was needed, so the membership grew quickly, and the standards body got to work immediately instead of spending valuable time debating.
4. The VSSO team began with the idea that an OSA and interface standards were the appropriate solution to the difficulties in the vehicle and equipment integration process. The VSSO would manage the architecture and a standards body would form to create technical specifications. The initial standardization process was adapted from one used in earlier efforts that was built around the concept of a change proposal. The VSSO saw that evaluating and promoting maturity (the goodness of a work product) was paramount to success. The standards must be mature before being supplied to programs for implementation or they would represent unacceptable risk to the programs. Thus, the VSSO developed the validation process to mature the standards. After the standards body produces a specification, the specification is put through a rigorous validation process (by a team that was not involved in the specification development), compliance artifacts are generated, and defects are found and documented. This process has proven more effective than predicted in detecting and fixing defects (ambiguity, conflict, and

technical errors) in the specifications. This process ensured that, when a specification is marked at the proposed standard maturity level, and thus promoted as a standard to be published, it is implementable, will operate as intended, and is likely to result in interoperability between artifacts implemented by different organizations. This process is not perfect, but the validation and compliance artifact development processes represent an invaluable lesson for other efforts.

5. Engineering reach-back support is necessary to assist acquisition programs implementing VICTORY standards. Program offices concentrate on addressing immediate operational threats and deploying capabilities. A second set of eyes helping to plan for future growth is helpful. The VSSO augments the program office teams, assisting in planning and executing their migration toward MOSA. This support included reviewing program documentation (e.g., design and acquisition documents, test procedures, and test reports); supplying technical and programmatic recommendations; creating VICTORY-related contractual language; conducting engineering analyses; developing reference designs; prototyping program-relevant, VICTORY-enabled capabilities; furnishing test procedures, reports, and programmatic recommendations; and creating government-owned engineering support tools and documents. These support tasks are crucial to maximizing implementation of VICTORY standards by programs and developing paths for future capability growth.

We are proud to supply these lessons learned from the VICTORY initiative to the wider community that is working to apply OSA and standards transitioning to MOSA. Not all approaches work for every organization, business need, or application space. However, these lessons should apply more broadly than to just the VICTORY space.

Program News

NEW DMSMS RESOURCES AVAILABLE

Two powerful new resources are now available to accelerate DMSMS resolution. In addition to the outstanding SD-22, "DMSMS Guidebook," the DoD DMSMS community has also deployed a new October 2019 edition of SD-26, "DMSMS Contract Language Guide Book," along with a compendium DMSMS Contracting Job Support Tool containing helpful contract data requirements lists and data item descriptions. Both are readily available at https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=283456.

The guide is organized around 28 different subject areas that encompass important aspects of DMSMS management, including case management and reporting, issue notification, and flow down of requirements to subcontractors. Illustrative contract language is supplied for each. Twenty-two of the subject areas are applicable to the DMSMS management portion of a contract. The remaining six are aimed at non-DMSMS portions of the contract and include configuration management or intellectual property. The guide also describes which contract language to use under different circumstances.

2019 DOD DMSMS ACHIEVEMENT AWARDS

Since 2007, the DSPO and the DoD DMSMS Working Group have recognized individuals and organizations of the military departments and defense agencies who have made significant accomplishments through robust DMSMS management. We are pleased to announce the 2019 award winners.

- **Lifetime Achievement**—*Ms. Karen Jackson*, Government-Industry Data Exchange Program
- **Individual Achievement**—*Ms. Christina Martin*, 408 Supply Chain Management Squadron, U.S. Air Force

- **Individual Achievement**—*Mr. Christopher F. Appelt*, CCDC-C5ISR Center, Product Realization Systems Engineering and Quality Directorate, U.S. Army
- **Team**—*Strategic Alternative Sourcing Program Office DMSMS Team*, U.S. Air Force
- **Team**—*Defense Logistics Agency Land and Maritime General Emulation of Microcircuits and Advanced Microcircuit Emulation Program*.

Award winners were recognized at the annual ceremony, held during the DMSMS Conference, on Thursday, December 5, 2019, in Phoenix, AZ. Ms. Robin Brown, OSD DMSMS and Parts Management Program Manager, presented the awards.

ASSIST PIV PROGRAM

DoD mandated that all common access cards (CACs) shall use a single personal identity verification (PIV) certificate to standardize access across DoD IT systems. This single certificate eliminates confusion and log in errors resulting from when users have to decide whether to log in with their CAC's existing DoD or email certificates. ASSIST websites will be PIV enabled by May 1, 2020 in accordance with the Secretary of Defense Memo "Modernizing the Common Access Card (CAC)—Streamlining Identity and Improving Operational Interoperability." This change requires users to have a PIV-enabled CAC (all CACs should be PIV enabled, if received after February 2018) and to visit the https://www.dmdc.osd.mil/self_service website for activation.

WSIT/PIN POINT USERS CLINIC

Thursday, March 5, 2020, 9 a.m. to 3 p.m.
LMI, 7940 Jones Branch Dr., Tysons, VA 22102

The Defense Standardization Program Office is sponsoring a Weapon System Impact Tool (WSIT)/Pin Point Users Clinic on March 5, 2020, from 9 a.m. to 3 p.m., at LMI in Tysons, VA. This clinic will supply an overview of the WSIT and Pin Point tools with live demonstrations, tips, and tricks for using both systems. There will be an interactive component, with simulation exercises. Attendees should bring their laptops to participate. For those that are unable to travel, a virtual option of this clinic will be available at the same times via Adobe Connect.

This clinic is open to government personnel and contractors with common access card access only. Please note the registration form is required for in-person or virtual attendance. All registration forms must be sent by February 28, 2020. Hurry, space is limited. Please visit www.dsp.dla.mil or contact Nicole Dumm at Nicole.dumm@dla.mil for more information.

Defense Standardization Program

JOURNAL

Upcoming Issues

Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

The following are our themes for the upcoming issues:

Issue	Theme
May—August 2020	Standardization Stars
September—December 2020	Modular Open System Approach continued


DEFENSE STANDARDIZATION PROGRAM
dsp
MAKING SYSTEMS WORK TOGETHER