PARRY LABS

SIXTH EDITION

DoD Integration Newsletter

Transforming the Integration Market

Table Of Contents

MOSA.....3

MOSA Considerations from the New Draft NDAA.....3

Digital Engineering 5

Digital Engineering: A Blueprint for Smarter Innovation.....5

Integration.....6

Implementing MOSA in DoD Programs – Implications for Real-Time Operating Systems.....6

Soldier.....8

Rapid Software Integration at the Tactical Edge: A Mission-Critical Imperative.....8

Small Business Spotlight.....9

Who'sWho?.....10

Matt Sipe.....10

USAF Dr. Bryan Tipton.....10

USN Jason Thomas.....10

US Army BG Kevin Chaney.....10

- **STAY UP TO DATE** on the latest news in the world of MOSA and Digital Engineering
- **KEEP AWARE** of key challenges in the integration community
- **DISCOVER** key leaders in the government

MOSA Considerations from the New Draft NDAA

By Matt Sipe, VP of Strategy and Open Systems, Parry Labs

The 2026 NDAA is currently working its way through congress, and it has some significant considerations relative to MOSA: Passage of industry pressure, political momentums, and a deep desire for rapid modernization. At its core, the legislation reflects a shift toward agility, openness, and commercial integration—principles long championed by emerging defense tech firms and venture-backed startups seeking to disrupt traditional procurement models.

A major catalyst was the assertive push from a handful of influential companies—new entrants to the Department of Defense (DoD) ecosystem, heavily supported by venture capital. These firms advocated for the FORGE Act as a vehicle to streamline acquisition, reduce bureaucratic overhead, and open the door for commercial off-the-shelf (COTS) solutions. Their lobbying efforts coincided with the arrival of a new administration that prioritized innovation and was notably receptive to ideas from the non-DoD commercial sector.

The legislation is also a response to longstanding frustrations within the acquisition community. There was a clear appetite to "cut the fluff" from existing laws—eliminating ambiguity and accelerating timelines without sacrificing the progress made through initiatives like the Modular Open Systems Approach (MOSA). The NDAA preserved and expanded MOSA's role, clarifying its applicability to all "covered systems," which now includes both acquisition and R&D programs aimed at delivering capabilities. This clarification removed previous uncertainty and established a firm foundation for open architecture mandates.

If the expected language is approved, here is an idea of what to expect. Before initiating a program, agencies will now have to assess and document open system objectives, aligning with Section 3102's emphasis on COTS preference. Programs will be expected to obtain software development kits (SDKs) with sufficient license rights to meet openness goals and negotiate those rights proactively.

[CONT.]

The Act also introduces several new terms to support this framework. "Incremental Standard" refers to a flexible, software-defined interface—essentially an API or Software Initial Capabilities Document (SW ICD)—that governs data exchange, even when formal standards are unavailable. This reflects an agile approach to standards: Use what's available, iterate quickly, and mature over time.

"MOSA" itself will receive a refreshed definition, emphasizing the need for a coherent architecture to describe modularity. "Module" gets clarified as a fully severable, self-contained unit, while "Module Interface" will replace the older "Modular System Interface" terminology. The distinction between "Modular Interface" and "Key Interface" acknowledges that not all programs can define modules precisely. Key Interfaces allow the government to enforce modularity at higher levels—such as separating vehicle systems, mission systems, and payloads—ensuring data transparency across domains.

Section 4401 of the Act outlines architecture requirements: It must define modules, interfaces, and openness characteristics, rely on consensus-based standards or incremental alternatives, accelerate COTS adoption, and incorporate industry input to avoid over-specification. Draft and final solicitations must reflect this architecture.

Solicitations for covered systems must also specify openness objectives, interface standards, minimum technical data packages, and desired license rights. Commercial products must procured with sufficient rights and SDKs to meet these goals. This desire for commercial products AND openness drives the government to the negotiating table to establish SNLR vs. trying to force GPR across the board.

Finally, Section 213 tasks the Director of Operational Test and Evaluation (DOTE), along with USD R&E and A&S, to review reference architectures and standards for digital engineering (DE) and recommend areas for further standardization—ensuring the FORGE Act's principles are embedded across the defense innovation landscape.

Digital Engineering: A Blueprint for Smarter Innovation

By Marisol Blank, Senior Director of Software Engineering & AI Strategy Lead at Parry Labs

WHAT DIGITAL ENGINEERING REALLY MEANS

Think of Digital Engineering as creating a smart, connected thread that weaves together data, models, and decisions throughout a system's entire life. It's not just another set of tools, it's a complete shift in how we think about building things.

BREAKING DOWN THE OLD WAYS

Over my 20+ years leading teams across aerospace, defense, finance, entertainment, I've seen the same problem everywhere: Disconnected tools and scattered data that slow everything down. Digital Engineering solves this by creating a living digital thread that connects everything from initial concept to final delivery.
This connection becomes even more powerful when you add AI to the mix. As someone who's led AI strategy initiatives, I've learned that AI without good data is just expensive guesswork. But when you build AI on top of solid Digital Engineering foundations, magic happens—tasks get automated, problems get spotted early, and systems predict their own issues before they break.

MAKING IT WORK FOR EVERYONE

The beauty of Digital Engineering is that it helps everyone, not just the technical folks. For leaders, it creates clarity—you can see how teams connect, where investments are paying off, and how programs adapt to changing requirements in real time.
Digital Engineering changes the game completely. It lets teams move from static documents that gather dust to dynamic models that evolve with your project. My leadership approach has always been about empowering teams through trust and collaboration, and Digital Engineering amplifies this by giving everyone the same clear picture.

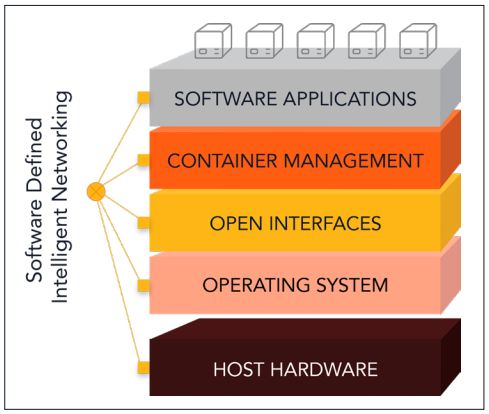
THE FUTURE WE'RE BUILDING TODAY

As we develop next-generation systems at Parry Labs, our commitment to Digital Engineering ensures we're not just keeping up, we're setting the pace. This isn't some distant future vision. **This is happening right now.** And the organizations that embrace it today will be the ones leading tomorrow's innovation.

Implementing MOSA in DoD Programs – Implications for Real-Time Operating Systems

By Greg Donahue, Technical Marketing Manager, DDC-I

In February 2025, the Office of the Under Secretary of Defense for Research and Engineering published a guidebook for the Department of Defense community. The goal of this document is to provide "information to help ensure programs incorporate a modular open systems approach (MOSA) as part of the defense acquisition program life cycle." Real-Time Operating Systems (RTOS) play a vital role in the infrastructure of embedded systems. They provide deterministic, low-latency capabilities for data processing, communications, navigation, sensor-weapon control, autonomy and more. An RTOS is also the critical connection between the system hardware and application software. It's the glue that holds the platform together so that it can perform as required.



There are several areas where an RTOS needs to support MOSA goals. Three of the most important are:

- Modularity to allow reuse and incremental upgrades to both hardware and software
- Abstracting software from hardware for portability
- Managing a wide variety of data I/O to support various sensor configurations

RTOS MODULARITY THAT ALLOWS REUSE AND INCREMENTAL UPGRADES

Many RTOS solutions compile into a monolithic binary. This is problematic when it comes to updating or changing any one component. For example, if you upgrade a sensor for improved performance, you will have to completely rebuild a monolithic RTOS from the start. With a modular RTOS, you only need to address the single software component needed to support the new sensor. You can reuse most of the executables, which accelerates upgrades to hardware components. Minimizing changes to the RTOS is the key to driving quicker updates to the warfighter.

SUPPORTING A WIDE VARIETY OF HARDWARE DEPLOYMENTS

Software performance is dependent on the hardware. A well-designed RTOS can help abstract both the kernel and application software from individual hardware needs. By employing an abstraction library that is dynamically linked, the RTOS can run on a variety of hardware solutions without the need for modification. This significantly reduces costs through software reuse.

ABSTRACTING I/O TO ENABLE RAPID SENSOR UPGRADES

There is a need for a wide variety of sensors across domains and platforms. In order to handle new sensors, the software needs to leverage libraries. In particular, an RTOS that uses I/O libraries enables modular updates.

SUMMARY

When implementing a MOSA architecture, focus on the RTOS component should consider:

- Modularity of software components
- Support of a variety of hardware
- The ability to support a wide variety of sensor input

The complete DoD guidebook can be found at https://www.cto.mil/wp-content/uploads/2025/03/MOSA-Implementation-Guidebook-27Feb2025-Cleared.pdf

Soldier

Rapid Software Integration at the Tactical Edge: A Mission-Critical Imperative

By Cory Wallace, Program Customer Liaison at Parry Labs

In modern conflict zones, the ability to rapidly integrate new software capabilities at the tactical edge isn't a luxury—it's a necessity. From 2006 to 2010, I spent 27 months deployed in Iraq, where our unit relied heavily on a tool called the BATS/HIDE camera. Its primary function was to collect biometric data from individuals encountered during missions and cross-reference that data with evidence from recent attacks.

Far too often, our cameras were inoperative—not because of hardware failure, but because of outdated software. They couldn't connect to the database or lacked the latest threat intelligence. That meant we were blind to critical information. We may have let high-priority targets walk through our checkpoints undetected simply because our systems weren't updated in time to give us the critical information we needed to act.

This experience underscores a vital truth: **software agility at the edge can directly impact mission success.** The ability to deploy updates—whether threat signatures, database patches, or new capabilities—without degrading system performance would have been a game changer. It could have enhanced our situational awareness, improved decision-making, and potentially saved lives. As the DoD continues to modernize, enabling secure, rapid software deployment to the tactical edge must be a top priority. The battlefield is dynamic. Our technology must be too.

DDC-I, Inc. is a global supplier of real-time operating systems (RTOS), software development tools, custom software development services, and legacy software system modernization solutions, with a primary focus on mission-and safety-critical applications.

DDC-I's customer base is an impressive "who's who" in the commercial, military, aerospace, and safety-critical industries. The company enables:

- A Multi-Core RTOS supporting AI/ML for multi-domain sensor fusion/data processing
- Target recognition, command & control, autonomy, and more
- Modular, reusable components for rapid updates to the warfighter
- Porting of software modules to platforms operating on different hardware

DDC-I's Deos™ RTOS employs patented cache partitioning, memory pools, and safe scheduling to deliver higher CPU utilization than any other certifiable safety-critical COTS RTOS on multi-core processors. Deos™ provides FACE® Conformant OSS Safety Base and Safety Extended Profiles and supports other MOSA initiatives like CMOSS, VICTORY and OMS.

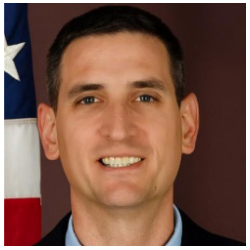
Who's Who?

Matt Sipe

Mr. Matt Sipe is the Vice President of Strategy, Open Systems at Parry Labs, where he leads the implementation of a Modular Open Systems Approach (MOSA) to deliver cost-effective solutions for government partners. He has held key leadership roles in Army Aviation, including Chief Engineer and Director of MOSA Transformation, advancing digital engineering and MOSA strategies. A former U.S. Air Force officer, Matt is also the founder of the DoD Industry Newsletter, a key resource for defense integration and open systems.

USAF Dr. Bryan Tipton

Dr. Bryan Tipton is Chief of Architecture and Engineering at the Department of the Air Force PEO for Command, Control, Communications and Battle Management (C3BM), ensuring the technical integrity of the DAF Battle Network. He leads system-of-systems integration across all C3BM acquisition programs. Previously, he was Chief Architect at the DAF Rapid Capabilities Office, guiding C2 system development for space and the Advanced Battle Management System. Earlier, he spent 15 years at MIT's Lincoln Laboratory on missile defense, ISR, and Air Force tactical systems. He holds a Ph.D. in physics from MIT.



USN Jason Thomas

Jason Thomas is the Systems Engineering Lead for the Department of the Navy in the Office of the Assistant Secretary of the Navy for Research, Development, Test and Engineering (DASN RDT&E), where he leads Modular Open Systems Approach (MOSA) efforts across SYSCOMs, other Services, and OSD. He previously spent 20 years at NAWCAD and NAVAIR in engineering, logistics, and program management. A Navy Reserve Aerospace Engineering Duty Officer, he is Joint and Information Warfare qualified with experience in space, surface, air, and cyber domains. He holds multiple engineering and defense-related degrees and is pursuing a Systems Engineering Ph.D. at the Naval Postgraduate School.

US Army BG Kevin Chaney

Brigadier General Kevin Chaney is the Program Executive Officer for Intelligence, Electronic Warfare and Sensors (PEO IEW&S), overseeing a $2.7B portfolio in intelligence, electronic warfare, cyber, force protection, and target acquisition. An Army Aviator and acquisition leader, he has served as PM for Aircraft Survivability Equipment, PM for the Future Attack and Reconnaissance Aircraft, Acting PEO for Command, Control, Communications, and Networks, and Special Assistant to the Secretary of the Army. He holds degrees in computer science, business administration, and strategic studies, and has earned the Legion of Merit and Bronze Star.