2026 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
MODULAR OPEN SYSTEMS APPROACH (MOSA) TECHNICAL SESSION
AUGUST 11-13, 2026 - NOVI, MICHIGAN

Reformed MOSA for Ground Combat Vehicles

Macam Dattathreya, PhD

US Army DEVCOM GVSC

ABSTRACT

Ground combat vehicles traditionally remain in service for decades, yet their rigid architectures make them costly to upgrade and slow to adapt to evolving threats. While the Department of War's 2025 Modular Open Systems Approach (MOSA) mandate aims to address this challenge, implementation barriers persist inconsistent vendor interpretations, physical and logical interoperability gaps, and IP complexities hinder progress. This paper proposes a reformed MOSA framework for ground vehicle Portfolio Acquisition Executives that redefines the government's role from system architect to ecosystem governor. The framework comprises four pillars: tiered standards balancing mandatory physical integration with vendor innovation, digital validation pipelines accelerating compliance verification, dynamic IP rights preventing vendor lock-in, and strategic portfolio management aligning investments with ground vehicle capability priorities. Special emphasis addresses integrating AI capabilities. This reformed approach enables rapid fielding of advanced ground vehicle capabilities at commercial innovation speed.

Citation: M. Dattathreya, "Reformed MOSA for Ground Combat Vehicles," In Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 11-13, 2026.

1. INTRODUCTION

The lifecycle of ground combat vehicles spans decades, making them costly to upgrade, difficult to sustain, and slow to adapt to evolving threats. The Department of War's 2025 acquisition reform mandate to implement a Modular Open Systems Approach (MOSA) represents a pivotal shift in strategy, aimed at breaking this cycle. MOSA promises to deliver fleets that are more lethal, adaptable, and easier to maintain.

However, implementing MOSA has proven challenging due to inconsistent vendor interpretations, physical and logical interoperability gaps, and intellectual property (IP) complexities. The rapid integration of Artificial Intelligence (AI) capabilities further complicates the landscape, as AI systems require dynamic modularity and continuous upgrades.

This paper proposes a reformed MOSA framework that redefines the government's role from system architect to ecosystem governor. By leveraging industry consortia, digital validation pipelines, and strategic portfolio management, this approach accelerates vendor-driven innovation while ensuring interoperability and affordability. Special emphasis is placed on integrating AI capabilities, which demand new approaches to modularity, testing, and sustainment.

The following sections outline the challenges of traditional MOSA, introduce the reformed framework, and provide actionable recommendations for Portfolio Acquisition Executives (PAEs) to implement this strategy effectively for ground combat vehicles.

2. THE REFORMED MOSA

MOSA represents more than a technical methodology. It is a strategic fusion of systems engineering principles with acquisition policy, designed to fundamentally transform how the Army develops, sustains, and modernizes complex defense systems [1]. By elevating system architecture from a purely technical exercise to a core business imperative, MOSA shifts the focus from optimizing initial performance to ensuring long-term adaptability and affordability [2]. Understanding this strategic foundation is essential before examining what makes the current MOSA approach "reformed."

2.1. The Core Tenets of MOSA

At its foundation, MOSA applied well-established systems engineering principles to create flexible, competitive, and sustainable systems. The approach begins with a fundamental architectural decision: partitioning the system into discrete modules that are both "highly cohesive" and "loosely coupled" [3].

High cohesion means each module performs a single, well-defined function with all internal components contributing to that purpose. A sensor module, for example, focuses exclusively on data collection rather than mixing sensing with processing or communication functions. ***Loose coupling*** ensures modules interact only through well-defined, standardized interfaces, minimizing dependencies between them. A properly designed sensor module can be replaced without requiring changes to the processing or display modules it connects to.

This architectural discipline makes interfaces the cornerstone of MOSA strategy. Unlike proprietary interfaces that lock users into specific vendors, MOSA interfaces are based on widely supported, consensus-driven standards that are thoroughly documented and accessible to multiple vendors [4]. The most critical activity in MOSA implementation is identifying and defining these ***Key Interfaces*** the boundaries where modules connect and exchange data.

The strategic value becomes clear when the government secures ***intellectual property*** and ***data rights*** for these interface specifications. With these rights, the government can competitively source modules from any vendor whose product conforms to the standard, rather than being locked into the original equipment manufacturer. This approach mitigates vendor lock-in, reduces lifecycle sustainment costs, and fosters a ***more dynamic and innovative industrial base***. New technology can be inserted rapidly and affordably by replacing a single module with an upgraded version that conforms to the same interface standard a process that has demonstrated significant reductions in system modification time and cost.

2.2. Challenges of Traditional MOSA

Despite its strategic promise, MOSA implementation has encountered significant barriers that limit its effectiveness. These challenges fall into three categories:

Technical Challenges

1. Designing cohesive, loosely coupled modules requires deep system knowledge, and poor decomposition decisions can undermine modularity.
2. Publicly available interface specifications may expose vulnerabilities, necessitating robust cybersecurity planning.
3. Validating vendor compliance with open standards is complex, especially for hardware-software integration.

Financial Barriers

1. Retrofitting MOSA principles to legacy systems is cost-prohibitive due to the lack of modularity in existing platforms.
2. Acquiring proprietary interface data rights requires substantial investment, which is difficult to justify within near-term budgets.

Organizational Obstacles

1. Traditional stovepipe acquisition processes conflict with MOSA's enterprise-wide approach, leading to missed opportunities for component reuse.
2. Workforce shortages and inadequate planning hinder effective MOSA implementation.
3. Programs often lack formal portfolio-level coordination, resulting in redundant efforts and inefficiencies.

These challenges emphasize the need for a reformed MOSA approach that addresses technical, financial, and organizational bottlenecks while fostering innovation and adaptability.

2.3. What Makes the Approach "Reformed MOSA"?

The challenges of traditional MOSA highlight the need for a deliberate evolution in the government's role. The "reformed" MOSA strategy addresses these bottlenecks by redefining the government's role from system architect to ecosystem governor. This shift enables the government to focus on strategic oversight while empowering industry consortia to develop and manage open standards.

Earlier MOSA implementations often relied on specific, government-controlled or government-defined architectures. The government would develop detailed technical reference architectures, specify exact interface standards, and maintain configuration control over the entire system design. While these approaches promoted openness and modularity, they created unintended consequences. The government became a bottleneck that vendors had to wait for government-approved architecture updates before innovating, and the architecture themselves struggled to keep pace with rapid commercial technology advancement. This centralized control, though well-intentioned, inadvertently slowed the very innovation MOSA was meant to accelerate. However, some of these could be stemmed from the misunderstanding of the role of the government.

The reformed MOSA fundamentally redefines the government's role from **system architect** to **ecosystem governor as depicted in Figure 1**. Rather than prescribing detailed technical solutions or specifications, the government establishes strategic direction, sets mandatory baseline

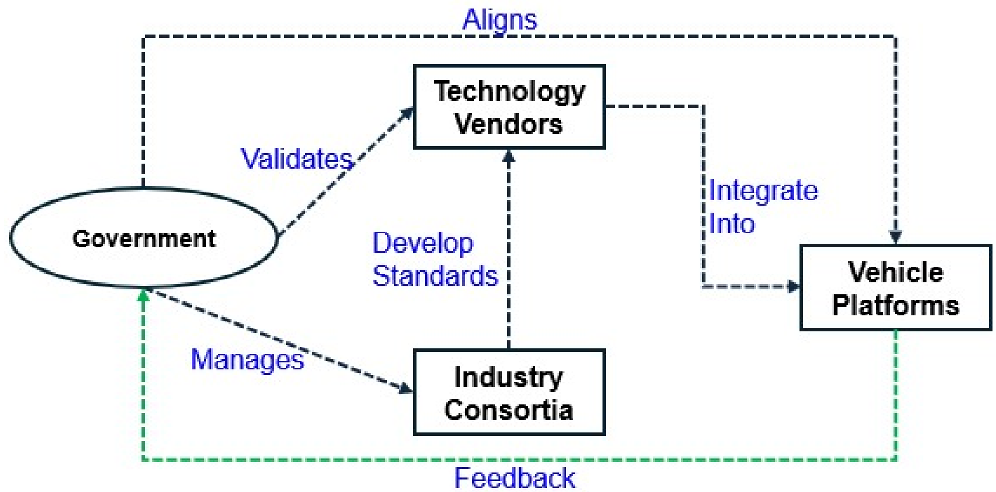

Figure 1: Reformed MOSA: Government as Ecosystem Governor. A dynamic, collaborative ecosystem where the government provides strategic guidance and enables competition.

requirements, and creates the conditions for a competitive, innovative ecosystem to flourish. The development and management of detailed open standards are delegated to industry consortia organizations like the National Advanced Mobility Consortium (NAMC), the Object Management Group (OMG), or the Sensor Open Systems Architecture (SOSA) Consortium. These consortia possess the technical expertise, industry participation, and organizational agility to develop and maintain standards that keep pace with commercial innovation.

This **USG-industry partnership** creates a clear division of responsibilities. The government sets strategic directions by identifying capability gaps, establishing non-negotiable baseline requirements for physical, logical and electrical integration, and providing oversight to ensure standards serve warfighter needs, more importantly interoperable integration. Industry executes technical details, developing consensus-based interface standards, creating reference implementations, and driving continuous improvement based on emerging technology and operational feedback. This approach has been identified as a key enabler for agile acquisition in complex technology domains, where the pace of innovation exceeds the government's ability to maintain detailed technical control.

Effective governance of multi-firm consortia is a critical success factor. These organizations must balance competing interests, large defense primes and small innovative firms, hardware and software vendors, domestic participants while maintaining technical rigor and preventing any single entity from dominating the standards process. The government's role as **ecosystem governor** includes ensuring these consortia remain open, transparent, and aligned with strategic objectives.

The goal is to create a **self-sustaining innovation ecosystem,** where the new capabilities, whether a next-generation radio, an advanced sensor, or even a more efficient weapon system can be integrated into a vehicle platform without triggering a multi-year, cost-prohibitive redesign effort.

By removing the government as a technical bottleneck, the reformed MOSA model accelerates innovation while maintaining interoperability and affordability.

3. THE FRAMEWORK FOR MOSA IMPLEMENTATION

The reformed MOSA framework operationalizes the government's role as ecosystem governor through four interconnected pillars:

Tiered Standards and Architecture

- Establish a tiered model balancing mandatory integration requirements with vendor innovation freedom.
- Tier 1 defines non-negotiable physical and electrical integration profiles.
- Tier 2 delegates logical interface standards to industry consortia.
- Tier 3 allows vendors to innovate within standardized boundaries.

Digital Integration and Validation Pipeline

- Provides a Government-Furnished Digital Environment (GFDE) for automated compliance verification and virtual integration testing.

Dynamic IP and Data Rights Framework

- Balances government access to critical data with vendor protection of proprietary technology.
- Introduces tiered rights aligned with the standards model and data escrow mechanisms for long-term sustainment.

Strategic Portfolio and Technology Management

- Aligns vendor innovation with Army priorities through a technology roadmap and enterprise-level incentives.

By systematically addressing technical, financial, and organizational challenges, this framework enables rapid fielding of advanced capabilities while ensuring long-term adaptability.

3.1. Piller 1: Tiered Standards and Architecture

This pillar resolves the tension between vendor flexibility and interoperability through a **tiered standards model** as depicted in **Figure 2**, that applies governance where most critical while preserving vendor innovation freedom.

Tier 1: The PAE defines a minimal, non-negotiable ***Vehicle Integration Profile (VIP)*** not a comprehensive architecture like Ground Combat Systems Common Infrastructure Architecture (GCIA) [5], but a slim profile of absolute requirements for any module to integrate into a given platform. For example:

1. ***Physical Form Factors & Mounting***: Standardized dimensions and mounting patterns per Standardized A-Kit/Vehicle Envelope (SAVE) [6] to ensure modules physically fit into pre-allocated vehicle slots.
2. ***Key electrical interface requirements:*** Specified power standards e.g., MIL-STD-1275 and connector families e.g., MIL-DTL-38999 for power and network backbone access.
3. Baseline shock, vibration per MIL-STD-810, and thermal management requirements for vehicle chassis integration.

This eliminates **"physical vendor lock"** where modules are logically compliant but physically incompatible with the platform.

Tier 2: ***Consortia-Managed Logical Interface Standards***: The PAE delegates detailed logical and data-level interface standards to industry consortia e.g., NAMC, OMG, SOSA. Guided by the PAE's strategic technology roadmap as described in Section 3.4, these consortia establish consensus-based standards for data models, network protocols e.g., Time Sensitive Networking (TSN), and domain-specific Application

Programming Interfaces (API)s. This leverages industry expertise and ensures standards remain current while the government provides strategic oversight.

Tier 3: ***Vendor-Specific Module Innovation:*** Within Tier 1 and 2 boundaries, vendors have maximum freedom to innovate. Internal design, algorithms, and technologies remain proprietary, allowing companies to bring best-of-breed commercial solutions and differentiate offerings while fostering competition focused on performance within a common framework.

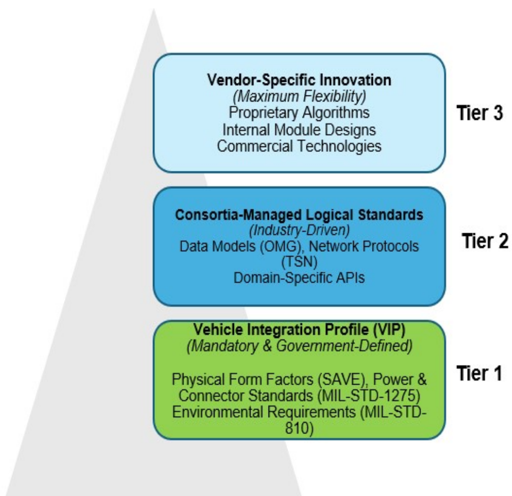

Figure 2: Tired Standards Model: Balances governance with innovation by layering standards. The base layer is mandatory and government-defined to ensure interoperability, while the upper layers provide increasing flexibility for industry and vendors to innovate.

The ultimate success of MOSA depends on creating a vibrant industrial base. The Army is actively fostering this by pairing flexible acquisition models with a transformative digital engineering approach.

1. ***Collaborative Acquisition Models****:* Utilizing OTAs through consortia like GVSC, NAMC and prize competitions such as xTechSearch to lower barriers for small businesses and non-traditional contractors.
2. ***Digital Engineering Transformation****:* Mandating "born-digital" approaches like the XM30, requiring contractors to deliver detailed Model-Based Systems Engineering models before physical prototypes, creating a "digital thread" connecting requirements through sustainment. Product Lifecycle Management (PLM) tools enable real-time multi-vendor collaboration and virtual prototyping for early soldier feedback at reduced cost.

3.2. Pillar 2: The Digital Integration & Validation Pipeline

This pillar addresses validating multiple vendor solutions without creating bottlenecks through a ***Government-Furnished Digital Environment (GFDE)*** serving as a common "digital proving ground.".

1. ***GFDE***: The PAE provides cloud-based GFDE including standardized digital engineering tools, mandated common data formats, secure collaboration spaces, and a centralized repository for validated models enabling enterprise-wide reuse.
2. ***Automated Interface Compliance & Validation***: The GFDE hosts an automated pipeline answering: **"Does this module conform to Standard Y?"** Vendors continuously submit digital models for programmatic validation against machine-readable Tier 1 and Tier 2 standards, receiving rapid iterative feedback to correct issues early and accelerate compliance.
3. ***The Reference Integration Model (RIM)***: The GFDE contains a government-owned digital twin of each vehicle platform. Before building physical hardware, vendors must virtually integrate their module into the RIM, enabling:

- Physical-fit and clearance verification
- Electrical load and thermal impact analysis
- Functional interoperability testing through co-simulation
- Virtual **"Vendor A for Vendor B" swap testing** proving interfaces are truly open and vendor-agnostic, de-risking integration before physical prototypes

3.3. Pillar 3: The Dynamic IP & Data Rights Framework

This pillar, as depicted in **Figure 3**, balances the government's need for data to enable vendors' need to protect proprietary technology through a predictable, transparent IP framework.

Explicit IP Value Negotiation: IP and data rights must be separately priced Contract Line Items (CLINs), forcing explicit negotiation on data value, providing vendor clarity, ensuring fair compensation, and enabling informed government trade-offs.

Tiered Rights Aligned with Tiered Standards: The IP strategy is directly aligned with the tiered standards model to create a cohesive and logical approach:

Standard Tier	IP/Data Component	Minimum Government Rights
Tier 1 & 2	Interface Specifications & Data	Government Purpose Rights (GPR)
Tier 3	Module Internals, Algorithms, Software	Limited/Restricte Rights
Sustainment	Build Instructions, Diagnostics	Data Escrow (Trigger-based release)

Figure 3: Pillar 3 - The Dynamic IP & Data Rights Framework: Standards tiers with the corresponding intellectual property rights.

1. ***Tier 1 and 2 Interfaces***: The government asserts minimum Government Purpose Rights (GPR) for all interface data a non-negotiable participation condition essential for sharing specifications with other vendors, enabling competition, and preventing vendor lock-in.
2. ***Tier 3 Module Internals***: Protected under Limited/Restricted Rights or Specifically Negotiated Licenses, safeguarding vendors' core intellectual property and competitive differentiation.

Data Escrow for Long-Term Sustainment: Vendors deposit critical sustainment data such as diagnostics, software build instructions with trusted third-party escrow agents. Data remains confidential but releases to the government under pre-defined trigger conditions such as vendor ceasing support, bankruptcy, providing long-term supportability guarantees without exposing day-to-day competitive information.

Training Data Rights: The government must secure rights to government-collected operational data from deployed vehicles, synthetic training data generated in the GFDE for augmenting real-world datasets, and data sharing protocols enabling vendors to access government data for model development while protecting classified or sensitive information.

Department of War (DoW) IP Strategy Framework: Building on the established practices

- **IP Strategy Document**: Programs proactively identify technical data and software rights early in lifecycle.
- **Funding-Based Data Rights Model (DFARS):** Rights

determined by funding source, enabling strategic investment in critical interface rights.

- **Flexible Contractual Frameworks**: "Black box" licensing, OTAs for tailored negotiations, and "right to repair" initiatives emphasizing organic sustainment capabilities.

3.4. Pillar 4: Strategic Portfolio & Technology Management

This pillar aligns decentralized vendor innovation with strategic Army priorities while preventing duplication through active portfolio management.

PAE-Maintained Technology Roadmap: The PAE develops a strategic technology roadmap identifying critical capability gaps, technology maturity timelines, cross-platform reuse opportunities, and modernization windows. Sharing this roadmap provides clear direction to industry consortia and vendors, guiding R&D investments toward pressing operational needs and preventing redundant efforts.

Incentivizing Enterprise-Level Behavior: To overcome conflicts between upfront MOSA investment and near-term program budgets, the PAE uses policy levers:

Program Incentives: Programs reusing enterprise repository modules receive award fees, budget relief, or accelerated approvals.

Vendor Incentives: Vendors whose modules achieve multi-program adoption receive preferred vendor status, financial incentives, or public recognition, creating market-driven alignment between vendor business interests and government strategic objectives.

4. AI-Specific Extensions

The integration of AI capabilities into ground combat vehicles introduces unique challenges that require tailored approaches to modularity, validation, and sustainment. AI modules often demand high-performance computing hardware, such as GPUs, neuromorphic processors, or specialized accelerators, which require substantial power and advanced cooling systems. To accommodate these needs, Tier 1 standards must define physical integration profiles that address high-bandwidth data interfaces, thermal dissipation, and unique form factors.

AI systems are dynamic and probabilistic, necessitating specialized logical interface standards to ensure interoperability. Tier 2 standards should include model interchange formats, such as Open Neural Network Exchange (ONNX), to enable cross-vendor compatibility. Additionally, data pipeline APIs for sensor data preprocessing and fusion, inference service protocols for querying models and receiving predictions with confidence scores, and model management interfaces for versioning, deployment, and performance monitoring are essential for seamless integration.

Validation of AI systems requires a continuous and adaptive framework due to their evolving nature. The digital validation pipeline must include standardized test datasets representing diverse operational scenarios, such as varying terrains, weather conditions, and threat signatures. Automated benchmarking tools should measure accuracy, latency, robustness, and computational requirements, while virtual integration with the Reference Integration Model (RIM) enables testing of AI modules under simulated operational conditions. Furthermore, a continuous validation framework should support regression testing to ensure new model versions maintain or improve performance, operational performance monitoring to detect degradation in deployed systems, and rapid update pathways for deploying updated models in response to new threats or feedback.

Given the rapid evolution of AI capabilities, active portfolio management is critical to align innovation with Army priorities. The PAE's technology roadmap should identify high-value AI applications, such as autonomous navigation, target recognition, and predictive maintenance, while also highlighting opportunities for shared AI infrastructure, including computing platforms, data pipelines, and model management tools. Enterprise-level incentives can further encourage cross-platform reuse of AI models and infrastructure, as well as contributions of high-quality operational data to enterprise repositories for AI training.

By consolidating AI-specific considerations into a dedicated subsection, the framework ensures a cohesive approach to integrating dynamic AI systems into ground combat vehicles. This approach not only addresses the unique challenges posed by AI but also maintains interoperability and adaptability, enabling the Army to leverage cutting-edge technologies effectively.

5. CONCLUSIONS

The Department of War's 2025 reformed MOSA mandate transforms ground vehicle acquisition by shifting the government's role from system architect to ecosystem governor. This paper's four-pillar framework tiered standards, digital validation pipeline, dynamic IP rights, and strategic portfolio management enables PAEs to harness vendor-driven innovation while ensuring interoperability and affordability.

To achieve these outcomes, PAEs must:

- Establish Vehicle Integration Profiles to standardize physical and electrical integration.
- Invest in digital infrastructure to accelerate compliance verification and virtual integration testing.
- Engage industry consortia strategically develop and maintain open standards.
- Mandate explicit IP negotiations to balance competition and innovation.
- Implement enterprise-level incentives to align vendor behavior with Army priorities.
- Develop AI-specific guidance to address the unique challenges of integrating dynamic, evolving systems.

The urgency of adopting this framework cannot be overstated. By acting now, the Army can deliver advanced capabilities to warfighters at the speed of relevance while ensuring platforms remain adaptable throughout their decades-long service lives.

6. REFERENCES

[1] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Modular Open Systems Approach (MOSA) Implementation Guidebook," Version 1.1, U.S. Department of Defense, Washington, D.C., 2019.

[2] J. A. Z-M. Gao, "A Systems Engineering Perspective on the Business Case for Modular Open Systems Architecture," *IEEE Systems Journal*, vol. 14, no. 3, pp. 4075-4083, Sept. 2020.

[3] E. Yourdon and L. L. Constantine, *Structured Design: Fundamentals of a Discipline of Computer Program and Systems Design*. Upper Saddle River, NJ: Prentice-Hall, 1979.

[4] U.S. Government Accountability Office, "Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems," GAO-25-106931, Jan. 2025.

[5] NAMC consortium URL, https://www.namconsortium.org/article/news/ground-combat-systems-gcs-

common-infrastructure-architecture-gcia-community.
[6] URL: https://www.lcrembeddedsystems.com/save-standard/

7. ACRONYMS

AI	Artificial Intelligence
API	Application Programming Interface
CLIN	Contract Line Item
DFARS	Defense Federal Acquisition Regulation Supplement
DoW	Department of War
GCIA	Ground Combat Systems Common Infrastructure Architecture
GFDE	Government-Furnished Digital Environment
GPR	Government Purpose Rights
IP	Intellectual Property
MBSE	Model-Based Systems Engineering
MOSA	Modular Open Systems Approach
NAMC	National Advanced Mobility Consortium
OMG	Object Management Group
ONNX	Open Neural Network Exchange
OTA	Other Transaction Authority
PAE	Portfolio Acquisition Executives
PLM	Product Lifecycle Management
RIM	Reference Integration Model
SAVE	Standardized A-Kit/Vehicle Envelope
SOSA	Sensor Open Systems Architecture
TSN	Time Sensitive Networking
VIP	Vehicle Integration Profile