# ACVIP Reduces Risk to Aviation MOSA

Bruce Lewis, Tyler Smith, Sholom Cohen, William Anderson, Alex Boydston

**Disclaimer:** This material is based upon work supported by the U.S. Army Combat Capabilities Development Command Aviation & Missile Center under contract no. W911W6-17-D-0003/W911W6-20-F-703A and Department of Defense contract FA8702-15-D-0002. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of U.S. Army Combat Capabilities Development Command Aviation & Missile Center or the Department of Defense.

**Audience:** This paper is for decision makers at Program Executive Office (PEO) Aviation and in Army Aviation Program Management Offices (PMOs). This paper assumes reader familiarity with the five principles of Modular Open Systems Approach (MOSA) and Architecture Centric Virtual Integration Process (ACVIP).

**Takeaway:** Readers should come away from this paper understanding how ACVIP provides capabilities to reduce risk for the Army MOSA.

**Executive Summary**: MOSA is a National Defense Authorization Act (NDAA) mandated systems engineering methodology.[1] The U.S. Army strategy[2] for MOSA is refined by the *"MOSA Implementation Guide"*, *"MOSA Reference Framework"*, and *"Army MOSA Initial Capability Refinement Document (ICRD)"* [2, 3, 1]. ACVIP is a process for reducing risk in development and procurement of cyber-physical systems. The *ACVIP Handbooks* define ACVIP [4] [5]. The Army MOSA strategy calls for use of standards for modularization, well-defined interfaces for component integration, integration risk reduction, and verification and validation throughout the lifecycle. ACVIP provides mechanisms for these objectives that have been extensively validated through Army Science and Technology (S&T) activities [6] [7].

## MOSA Objectives

NDAA 2017 and 2021 mandate use of MOSA. The Five MOSA Principles, described in "*A MOSA Approach to Acquisition,"* provide high-level activities for achieving modular, open systems (i.e., *Establish an Enabling Environment, Employ Modular Design, Designate Key Interfaces, Select and Implement Open Standards, Certify Conformance*) [8]. The "*MOSA Implementation Guide"* and "*Army MOSA ICRD"* provide additional guidance to refine these principles with activities and objectives for applying MOSA to the program lifecycle, including (but not limited to):

1. Capture embedded computing design architecture for modularization using standards[3]
2. Support the development and insertion of components into legacy and newly developed systems[4]
3. Reduce integration risk during initial development and sustainment[5]

---

[1] United States law. NDAA for Fiscal Year 2021 section 804, NDAA for Fiscal Year 2017 section 805.
[2] The Program Executive Office (PEO) Aviation MOSA Implementation Guide is still in review.
[3] See items 4.0, 10.0 of the MOSA ICRD, section 2.4 of the MOSA Implementation guide, and 2.4.2 of the MOSA Reference Frameworks [1, 2, 7]
[4] See item 10.0 of the MOSA ICRD and sections 1 and 2.1.3.2 of the MOSA Implementation guide [1, 2]
[5] See item 1.0 of the MOSA ICRD and section 2.1 of the MOSA Implementation Guide [1, 2]



This paper was written under US Army DEVCOM Aviation & Missile Center contract W911W6-17-D-0003 with Adventium Labs and Department of Defense contract FA8702-15-D-0002 with Carnegie Mellon University Software Engineering Institute.

4. Support verification and validation activities throughout the system lifecycle[6]

This paper describes each of these MOSA objectives and how ACVIP enables achieving each objective.

For modular embedded computing systems**, ACVIP reduces the risk of integration errors.**

ACVIP is a process for meeting these four objectives in a manner that reduces program risk in embedded systems software-hardware integration rework. Embedded systems are characterized by software enabled real time reactive control to accomplish their functionality, such as aircraft, robotics, automotive, missiles, etc. As such they are time critical, and typically safety and security critical. ACVIP was matured through a series of S&T programs for Joint Multi-Role Mission Systems Architecture Demonstration (JMR MSAD) for insertion onto Future Vertical Lift (FVL) programs with an approved Technology Transfer Agreement (TTA). This maturation occurred along with other MOSA related technologies (e.g., FACE, HOST), Model Based System Engineering (MBSE) practice, and standards [6] [7]. Through these S&T programs, aviation system prime integrators and component suppliers have become familiar with ACVIP and the Architecture Analysis & Design Language (AADL) and learned lessons that will assist them in applying ACVIP. These S&T programs supported development and maturation of ACVIP methods and analysis tools for multiple domains of architecture analysis including processor, memory, and bus utilization, latency, timing, scheduling, safety and security, plus component and system interaction behavior and interface compatibility. The methods and tools support critical embedded computing system qualities that reduce integration risks on programs such as Future Long Range Assault Aircraft (FLRAA), Future Attack Reconnaissance Aircraft (FARA) and can be applicable to upgrades to enduring fleet aircraft. ACVIP Researchers from the Carnegie Mellon University Software Engineering Institute (CMU SEI) and Adventium Labs are working under contract with the FVL PMOs to assist in the application of ACVIP.

## 1. Capture Embedded Design Architecture for Modularization Using Standards

*"… each relevant Department of Defense contract entered into after the date on which the regulations and guidance required under paragraph (1) are implemented includes requirements for the delivery of modular system interfaces for modular systems deemed relevant in the acquisition strategy or documentation … including … (iii) documentation with functional descriptions of software-defined interfaces, conveying semantic meaning of interface elements, such as the function of a given interface field;"*

NDAA 2021 (quoted above) calls for descriptions of software-defined interfaces that convey semantic meaning.[7] The Army MOSA strategy as described by the MOSA ICRD) requires effective use of standards and suggests the use of an Architecture Description Language (ADL).[8,9] Use of a standardized ADL that includes interface semantics and supports predictive real-time, safety, and security system analysis and virtual integration enables effective and efficient MOSA, supporting third party development and

[6] See item 20.0 of the MOSA ICRD and section 2.5.3 of the MOSA Implementation Guide [1, 2]
[7] See NDAA 2021 section 804.B.iii
[8] See MOSA Implementation Guide Technical Indicator B2 [2]
[9] Such analysis is required by the MOSA ICRD item 16.0 [1]

integration and lifecycle sustainment, as required by the *MOSA implementation guide*.[10] ACVIP provides a standardized ADL and the tools needed to do virtual integration of modular components. The reference ADL for ACVIP is the *SAE International Aerospace Standard (AS5506) Architecture Analysis & Design Language (AADL)*. AADL provides a set of semantics for describing the structure, dynamics and properties of embedded computing systems and an established ecosystem of tools for developing and analyzing AADL models. Without robust use of a standardized ADL to providing precise real-time semantics and without a means to evaluate models using those semantics, integration of third-party components becomes a trial-and-error process, increasing integration risk. This was evident on the JMR MSAD Capstone Demonstration in which many performers encountered integration errors due to insufficient or misunderstood informal aspects of interface definitions frustrating integration analysis.[11] ACVIP provides the capability to specify the interface in a well-defined, standard notation supporting architecture integration, as well as describing the system itself that the component is intended to integrate into, providing a basis for predictive virtual integration capable of supporting multiple domains of architecture analysis to evaluate component architectural fit. ACVIP also by providing standard semantics supporting structure, dynamics and properties, allows a richer standard context for modularity design and assessment.

## 2. Support the Development and Insertion of Components into Legacy and Newly Developed Systems

*"Begin planning the lifecycle sustainment concepts and approach for the MOSA early in the acquisition. This includes establishing how the MOSA objectives for modularity and openness will provide enhanced product support and opportunities for technology insertion and innovation and increased competition throughout sustainment and modernization."* [2]

The *MOSA Implementation Guide section 2.1.3.2* (quoted above) directs a program to establish how they will meet MOSA modularity and openness objectives. ACVIP shows how to meet these requirements through incremental refinement of models and iterative analysis to evaluate feasibility of requirements for the embedded system at successive phases of development. ACVIP through structural definition and multi-domain architecture analysis provides a means to discover and modify modularity and correct interface issues early using continuous virtual integration at each refinement of the embedded system design architecture. Trade space analysis can be used to evaluate architectural alternatives, including different components that would fit. The DARPA CASE program has demonstrated, for instance, the ability to analyze AADL expressed architecture of legacy systems for guided restructuring and insertion of security enhancing components. ACVIP builds acquisition and development practices using existing translation and analysis capabilities for predictive virtual integration of software, computer hardware, and physical devices. The ACVIP Handbooks describe these practices down to the level of selecting and planning analyses for each gate review, and guide the PMO acquisition process.

[10] See MOSA implementation guide appendix 4.5 [2]
[11] Results of the JMR MSAD Capstone demonstration have not yet been published.



This paper was written under US Army DEVCOM Aviation & Missile Center contract W911W6-17-D-0003 with Adventium Labs and Department of Defense contract FA8702-15-D-0002 with Carnegie Mellon University Software Engineering Institute.

## 3. Reduce Integration Risk during Initial Development and Sustainment

*"The PM should establish a program-wide MOSA-enabling environment by directing engineering leadership and the supportive practices needed for successful development of a modular open systems including […] Lifecycle sustainment planning and risk management*."[2]

The *MOSA Implementation Guide section 2.1* (quoted above) calls out lifecycle sustainment and risk management as MOSA objectives. ACVIP provides standard real time semantics supporting analysis and encourages practitioners to use standard properties to describe components so that multiple stakeholders can understand component integration into the embedded computing architecture at design time and throughout the lifecycle. Contractors often use customized notations which are not well defined for third party understanding or lifecycle support. ACVIP analysis tools use AADL standard semantics and properties to reduce risk by evaluating component interface behavior and emerging system qualities like timing, safety, and security. ACVIP analysis run early in the program reduces integration risk later, and ACVIP analysis run as part of sustainment efforts and upgrades reduces risk of regressions or recertification challenges. Use of AADL with ACVIP reduces risk that design artifacts will become unmaintainable due to vendor specific, custom or proprietary tools that may become unavailable over time.

## 4. Support Verification and Validation Activities throughout the System Lifecycle

Legacy systems and even new MOSA-developed systems will require change over time as the modularity style and the functionality of the components change. ACVIP allows evaluation of both the MOSA principles of the system architecture and the integration of legacy, closed interfaces, supporting the architecture and component evolution process. ACVIP tools support trade space analysis of architectural and component interface alternatives, which can be evaluated across multiple platforms. Use of a tool-agnostic AADL specification provides for reusability on those platforms, reducing the effort required to support modular components across programs with disparate tool sets. An AADL specification of a module allows effective planning for the future upgrade of systems in a manner that reduces the development, qualification, and test requirement of technology updates.

As with any tool or process, the decision to employ ACVIP requires a value assessment contrasting the effort required to develop ACVIP models and execute ACVIP analysis against the risk reduction gained from ACVIP. ACVIP is most likely to provide value on new developments or legacy system upgrades in which multiple stakeholders are collaborating to develop new cyber-physical capabilities.

## Conclusion

The MOSA recommendations provided by the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) and the Army MOSA ICRD outlines specific objectives of a MOSA implementation: use of standards for modularization, well-defined interfaces for component integration, integration risk reduction, and verification and validation throughout the lifecycle. ACVIP, as defined by the ACVIP handbooks and validated by JMR MSAD, provides defined processes, standardized ADL for real-time systems, and tools to meet these objectives.



This paper was written under US Army DEVCOM Aviation & Missile Center contract W911W6-17-D-0003 with Adventium Labs and Department of Defense contract FA8702-15-D-0002 with Carnegie Mellon University Software Engineering Institute.

[1] M. Isaacson and M. Kukla, "Initial Capability Refinement Document (ICRD) for Family of Systems Modular Open Systems Approach," U.S. Army, 2020.

[2] Office of the Chief Systems Engineer, "Modular Open Systems Approach (MOSA) Implementation Guide," ASA(ALT)/OCSE, 2020.

[3] Deputy Director for Engineering, "Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs," Office of the Under Seretary of Defense for Research and Engineering, Directory of Defense Research and Engineering for Advanced Capabilities, Washington, D.C., 2020.

[4] Adventium Labs, "Architecture-Centric Virtual Integration Process (ACVIP) Handbooks - Modeling & Analysis with the Architecture Analysis & Design Language (AADL)," 2020.

[5] N. Guertin, S. Cohen, F. Schenker, L. Figueroa and H. Levinson, "Architecture-Centric Virtual Integration Process (ACVIP) Acquisition Management Handbook," Carnegie Mellon University Software Engineering Institute, 2021.

[6] Adventium Labs, "Joint Common Architecture Demonstration Shadow Architecture Centric Virtual Integration Process Final Technical Report," 5 October 2015. [Online]. Available: https://www.adventiumlabs.com/sites/default/files/documents/Adventium_JCA_Demo_ACVIP_Shadow_Tech_Report_Distro_A.pdf.

[7] D. Johnson, W. Jacobs, A. Boydston, S. Dennis, A. Salvetti and B. Yost, "Architecture Implementation Process Demonstrations (AIPD) Final Report," U.S. Army RDECOM, 2018.

[8] Open Systems Joint Task Force, "https://www.milsuite.mil/book/docs/DOC-789030," 2004. [Online]. Available: https://www.milsuite.mil/book/docs/DOC-789030.



This paper was written under US Army DEVCOM Aviation & Missile Center contract W911W6-17-D-0003 with Adventium Labs and Department of Defense contract FA8702-15-D-0002 with Carnegie Mellon University Software Engineering Institute.