# PLUGFEST 2025

## Event Summary

***PlugFest 2025 Hosted by***

ACC Fed Lab and Booz | Allen | Hamilton

***Supported by***

NAVAIR/PMA-209

***Coordinated by***

Event Summary presented by Cody Cox
Research Engineer, Georgia Tech Research Institute

June 2025

## Table of Contents

## List of Figures

# 1. Executive Summary

PlugFest 2025 was a groundbreaking technical event that showcased the usage and implementation of Open Architecture (OA) principles in the defense sector. Hosted at Beale Air Force Base (AFB) in collaboration with Air Combat Command (ACC) Federal Laboratory and Naval Air Systems Command (NAVAIR) PMA-209, PlugFest served as a proving ground for industry and government partners to evaluate open systems hardware and software aligned with standards such as the Sensor Open Systems Architecture® Technical Standard, the Future Airborne Capability Environment® Technical Standard, HOST (Hardware Open Systems Technologies), MORA (Modular Open Radio Frequency Architecture) and CMOSS (C5ISR/EW Modular Open Suite of Standards).

The Department of Defense (DOD) continues to prioritize the adoption of Modular Open Systems Approach (MOSA) to reduce integration of emerging technologies, reduce vendor lock-in, and promote mission modularity. However, aligning industry solutions with open standards remains a complex challenge. PlugFest was designed to provide a real-world environment in which vendors, integrators, and government stakeholders can work together effectively to validate system interoperability, modularity, and capability in a practical defense-oriented environment.

PlugFest 2025 was a collaborative effort involving over 30 industry and government organizations. The event was hosted at Beale Air Force Base in California on February 10–11, 2025. Two pre-event integration activities supported PlugFest readiness: the first pre-integration event was held at Georgia Tech Research Institute (GTRI) Headquarters in Atlanta, GA (Dec 2–4, 2024), followed by the Integration Workshop at Antara Teknik in Roseville, CA (Feb 6–9, 2025). These events allowed participants to validate basic compatibility, finalize containerized deployments, and coordinate test activities prior to arrival for live demonstrations at Beale Air Force Base (AFB). PlugFest brought together representatives from key government entities including Naval Information Warfare Center (NIWC) Atlantic, Naval Surface Warfare Center (NSWC) Crane, US Army Aviation Mission Systems and Architecture (AMSA), Air Force Life Cycle Management Center / Cryptologic and Cyber Systems (AFLCMC/HNCA), NIWC Pacific and US Army Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.

At PlugFest, defense primes and technology vendors demonstrated a wide range of capabilities such as Graphical Processing Unit (GPU)-accelerated AI processing, containerized FACE® applications, SOSA® hardware interoperability, Bandwidth Efficient - Common Data Link (BE-CDL) waveform processing, cross-domain data filtering and in-band/out-of-band system management. Notable outcomes included the successful integration of NVIDIA's RIVA speech-to-text AI with Software Defined Radio data, multi-vendor chassis testing, and containerized applications aligned to the FACE® Technical Standard and deployed over Red Hat Device Edge.

The results can be used to inform acquisition strategies, guide future RFI/RFP development, and educate program offices on MOSA compliance in upcoming DOD programs. The lessons learned from PlugFest 2025 will enhance the effectiveness of future PlugFests and contribute to the broader goal of advancing Open Architecture (MOSA) principles within the defense sector. A more extensive report for DOD personnel and authorized DOD contractors, labeled CUI // SP-CTI // FEDCON DISTRIBUTION STATEMENT D, may be requested: PMA209-AAT@us.navy.mil

# 2. Scope of the Report

The report provide a comprehensive review of PlugFest 2025, detailing the findings, technical insights, and recommendations derived from the integration activities and demonstrations conducted. It is structured to offer insight into integration efforts and informs program offices, acquisition leaders, and industry stakeholders on the strengths and challenges observed during the event.

Specifically, the report:

- Summarize the objectives of PlugFest for advancing Open Architecture adoption.
- Detail the participation of DOD and Industry, including the systems and capabilities brought to the event.
- Provide an overview of test group activities, organized by integration tiers, which include:
  - Tier 1: Hardware Validation (ex. power-on testing and interface functionality)
  - Tier 2: Capability Execution (ex. running applications and demonstrating system-level functionality)
  - Tier 3: Interoperability and Modularity (ex. cross-vendor integration and multi-system interoperability)
- Provide summarized reporting of the test group activities based on the integration tiers.
- Highlight technical successes, failures, integration challenges and lessons learned.

The report serves as a reference for future PlugFest planning and collaboration, open standards development, and acquisition strategies to accelerate the implementation of modular and interoperable defense technologies. The insights and results from PlugFest will help reduce technical risk, expand collaboration across the defense community, and drive the transition toward truly open, innovative and adaptable systems to the warfighter.

## 2.1 Purpose of PlugFest

The PlugFest is dedicated to advancing Open Architecture standards such as the SOSA® Technical Standard, the FACE® Technical Standard, HOST, MORA and CMOSS in MOSA objectives. Hosted by ACC Fed Lab, supported by NAVAIR PMA-209 and coordinated by GTRI, with the shared goal of proving out hardware interoperability, modularity, and testing real-time integration across platforms. By bringing together leading defense innovators, PlugFest helps accelerate technology maturation, enhance cross-domain interoperability, and identify integration challenges early in the development cycle. The event directly supports warfighter capability advancements by enabling real-time hardware and software validation, ensuring systems align with future military needs, open architecture mandates, and rapidly fielding objectives.

## 2.2 Summary of Participation

**Major DOD Standards Plugged: SOSA®, FACE®, CMOSS, HOST, MORA, VICTORY**

30 Participants from military services and industry

**ACC Federal Laboratory** **NAVAIR/PMA-209** **AFLCMC** **US ARMY C5ISR Center**

## Industry

- AEGIS Power Systems
- AirBorn Inc.
- Annapolis Micro Systems
- Behlman Electronics
- Booz | Allen | Hamilton
- Concurrent Technologies
- Curtiss-Wright Defense Solutions
- EIZO Rugged Solutions
- Elma Electronic Inc.
- Epiq Solutions
- General Electronics Aerospace
- Georgia Tech Research Institute
- Herrick Technologies Laboratories
- L3 Harris
- LCR Embedded Systems
- Leidos
- Northrop Grumman Mission Systems
- OAR Corp
- Pacific Defense
- Pixus USA
- Red Hat
- Real-Time Innovations
- Sciens Innovations
- Tucson Embedded Systems , Inc
- VICOR
- WOLF Advanced Technology

## 2.3 Impact to the Warfighter

### 2.3.1 A Proving Ground for Interoperability Across Platforms

PlugFest 2025 served as a testbed for evaluating the interoperability of SOSA® aligned hardware and open architecture software solutions across diverse platforms. By integrating and demonstrating vendor-agnostic systems, PlugFest provided real-time validation of modular solutions that align with MOSA. Participants assess how well their hardware and software components function across different military and industry platforms, showcasing compatibility, scalability, and ease of integrating systems. PlugFest provided a collaboration environment for vendors to communicate with integrators and government stakeholders.

### 2.3.2 Empowering Joint Operations

PlugFest strengthens cross-service collaboration, enabling the exchange of data and resources across the Air Force, Navy, and Army through standards such as those demonstrated, i.e. the SOSA® Technical Standard, the FACE® Technical Standard, HOST, MORA, VICTORY and CMOSS. By fostering collaboration and aligning with Open Architecture principles, PlugFest exemplifies conformance with tri-service memorandum directives for a Modular Open Systems Approach for Defense Weapon Systems published on December 17th, 2024.

### 2.3.3 Open Solutions for Emerging Threats

PlugFest demonstrations highlighted the advantages of Open Architecture (OA) systems in addressing modern battlefield challenges through modular, scalable, and secure technologies. Capabilities include edge computing for real-time speech-to-text translation, secure BE-CDL waveform processing, containerized application deployment, and cross-domain data filtering were showcased, providing valuable insights into modular system design and implementation strategies.

**Figure 1** illustrates three approaches to system modularity and scalability. First, an extensive modular open system, where key functions are fully isolated into independent modules. Second, a selective modular approach, which prioritizes modularization of essential components with open interfaces. And third, a proprietary, non-modular design which relies on rigid, vendor-specific connections. This visualization underscores how selective or partial modular adoption allows platforms to gradually integrate OA principles based on mission priorities rather than requiring a complete system overhaul.

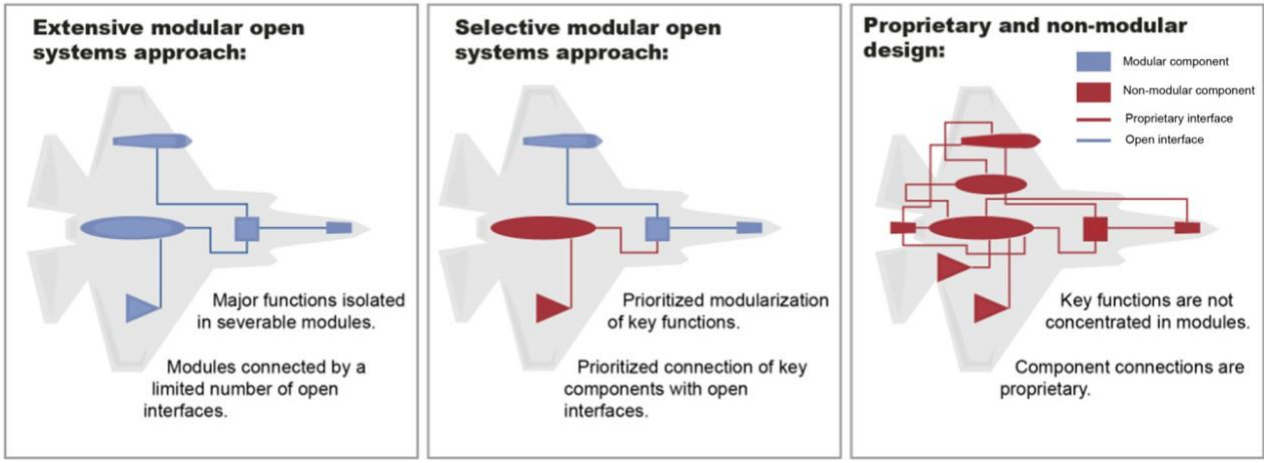


Figure 1: System Modularity Approaches

### 2.3.4 Enhancing Combat Readiness Through Open Standards

Adopting open architecture principles enhances combat readiness by allowing rapid system upgrades, increasing platform flexibility, and improving interoperability across joint and coalition forces. Open systems allow for scalable and mission-adaptable solutions, whereas proprietary, non-modular designs hinder adaptability and increase costs.

- **Reduces Proprietary Lock-in**: Open systems minimize vendor dependency, allowing seamless integration of new technologies without extensive redesigns.
- **Increases Platform Flexibility**: Modular solutions enable multi-mission capabilities, allowing for quick adaptation to emerging threats.
- **Promotes Interoperability**: Standardized interfaces promote cross-service and industry integration efforts, ensuring systems can communicate effectively.
- **Accelerates Deployment and Cost Efficiency**: Open standards reduce the time and expense of developing and fielding new defense technologies, ensuring warfighters receive cutting-edge capabilities faster.

By showcasing these principles at events such as PlugFest, participants can demonstrate the importance of Open Standards in defense systems, reinforcing the need for continued investment in modular and interoperable technologies for the modern battlefield.

# 3. Event Overview

## 3.1 Dates and Location

**Pre-Integration 1**
**Date**: December 2–4, 2024
**Location**: Georgia Tech Research Institute Headquarters

The first preparatory milestone was the Pre-Integration event at GTRI, designed to bring vendors and system integrators together under a controlled environment to establish hardware connectivity, perform debugging, and confirm initial chassis card compatibility. This event marked the beginning of cross-vendor technical collaboration to address early-stage electrical and software issues prior to the formal PlugFest 2025 event.

Vendors brought their SOSA® aligned Plug-in Cards (PICs), chassis, power supplies, and other hardware to test against shared chassis platforms provided by a mix of vendors. Testing focused on validating card power-on, validating interfaces, management compatibilities, and system interconnects. This pre-integration event was also highlighted in an official press release by GTRI, detailing the value and benefits of early testing and showcasing industry collaboration. PR link: https://gtri.gatech.edu/newsroom/integration-demonstration-event-prepares-february-2025-plugfest

**Pre-Integration 2**
**Date**: February 6–9, 2025
**Location**: Antara Teknik

The second event was hosted at Antara Teknik's facility in Roseville, California, and served as a software-focused collaboration effort. Key objectives included containerization of software packages, integration of Red Hat Device Edge, and co-development of solutions between Tucson Embedded Systems (TES-i), Leidos, Real-Time Innovations (RTI), and Red Hat that aligned to the FACE® Technical Standard.

Leidos led efforts to containerize the NVIDIA HoloScan and RIVA AI frameworks, validating PXE boot deployment workflows and GPU driver configuration on Red Hat Enterprise Linux (RHEL). Antara Teknik provided an environment conducive to agile software development and quick turn testing, enabling vendors to finalize configurations prior to PlugFest.

**PlugFest Main Event at Beale Air Force Base**
**Date**: February 10–11, 2025
**Location**: Community Activity Center, Beale Air Force Base

The culmination of the pre-integration and testing events occurred at Beale Air Force Base in California, where the PlugFest main event was held. Hosted by the U.S. Air Force's 9th Reconnaissance Wing and by ACC Fed Lab, the event featured participation from government stakeholders, system integrators, and over a dozen hardware and software vendors.

Keynote remarks were delivered by senior government representatives, and the event was documented by Beale Public Affairs in an official article further detailed in the next section.

## 3.2 Major Participants and Stakeholders

The PlugFest event at Beale Air Force Base served as a collaborative platform, bringing together government agencies, invited industry partners and technical experts to evaluate the interoperability of open systems components. The 2025 event opened with a keynote address from the 9th Reconnaissance Wing Chief of Staff, followed by remarks from the ACC Scientific Advisor and ACC Senior Engineer, emphasizing the critical role of open architecture standards in defense modernization.

Keynote Representatives:

- **9th Reconnaissance Wing:** U.S. Air Force Lt. Col. Nathan Maertens, Chief of Staff of the 9th Reconnaissance Wing, provided opening remarks, highlighting PlugFest's focus on interoperability testing to enhance mission capabilities. He emphasized that PlugFest is an event "focusing on testing the interoperability of modules and sensors within open standards."
- **Air Combat Command (ACC):** Dr. John D. Matyjas, Scientific Advisor to the ACC Commander, addressed attendees during the opening session, stressing the role of scientific research in advancing open systems. His participation highlighted the importance of integrating scientific insights into the development of interoperable systems.
- **Air Combat Command (ACC):** Dr. Ilya Lipkin, Senior Engineer at the ACC Federal Laboratory, delivered opening remarks underscoring the significance of open architecture standards in system development. He highlighted that PlugFest serves as a platform to "promote open architecture standards and aid in the development of systems through testing."

PlugFest 2025 had participation from key government organizations, including:

- Naval Information Warfare Center (NIWC) Atlantic
- Naval Surface Warfare Center (NSWC) Crane
- Naval Air Systems Command (NAVAIR)
- U.S. Army Aviation & Missile Systems Architecture (AMSA)
- U.S. Army C5ISR Center
- Air Force Life Cycle Management Center (AFLCMC/HNCA)
- Naval Information Warfare Center (NIWC) Pacific

These agencies attended PlugFest 2025 as observers, with a focus on understanding OA principles and their potential applications in defense modernization. Their participation highlights the importance of Section 4401 of Title 10, United States Code Title 10 directive, which emphasizes the adoption of MOSA for future DOD acquisitions. PlugFest delivered a learning environment where government organizations engaged with industry partners, asked questions, and gained insight into how open systems enable interoperability and lifecycle cost savings.


Figure 2: PlugFest keynote, featuring Lt. Col. Nathan Maertens and the GTRI team

The Beale Air Force Base Public Affairs Office attended PlugFest to document the event through press coverage and photography. Their coverage highlights the significance of PlugFest in advancing DOD open architecture initiatives. The article on the event's outcomes and key takeaways can be found here:

https://www.beale.af.mil/News/Article-Display/Article/4079405/plugfest-at-beale-tests-conformance-and-performance-of-open-systems-components/


Figure 3: Dr. Ilya Lipkin and Lt. Col. Maertens observing a demonstration of the BALSA and ARCM applications aligned to the FACE® Technical Standard.

### 3.3 PlugFest Integration and Preparation

PlugFest required some preparation and coordination between government, industry, and research institutions to perform successful demonstrations of open architecture capabilities. Leading up to the main event, GTRI hosted a pre-integration event that allowed participating vendors to validate initial hardware compatibility, troubleshoot technical issues, and refine their planned demonstrations. This was instrumental in establishing a foundation for PlugFest, encouraging industry to address potential integration roadblocks prior to arriving at Beale Air Force Base for the main event.


Figure 4: Rich Lucente presenting on Red Hat Device Edge at the pre-integration event

The pre-integration event at GTRI was a key milestone in the PlugFest preparation phase. It allowed vendors to bring their hardware together in a controlled environment, identifying and resolving potential issues before the main event. As shown in the image above, Red Hat provided a technical briefing to a room full of vendors, outlining the benefits of containerized deployment of applications and Red Hat Device Edge (RHDE) for edge operating systems. Key activities included:

- Initial Power-On Testing – Ensuring processing and networking plug-in cards functioned correctly within SOSA® aligned chassis.
- Network Configuration and Connectivity Checks – Verifying Ethernet and PCIe-based interconnections between components.
- Software Deployment and Containerization – Testing software deployment of FACE® applications using containerization and Red Hat-based solutions.
- Validation of System Management Interfaces – Testing communication between Management software and hardware monitoring tools.

Leading up to the pre-integration(s) and PlugFest main event, weekly coordination meetings with industry partners facilitated structured planning and execution of the demonstrations. The sessions focused on defining test objectives, determining hardware and software configurations, and orchestrating cross-vendor collaboration for testing at PlugFest. Vendors worked closely to align their efforts with the five MOSA principles, ensuring that their demonstrations properly utilized SOSA®, FACE®, CMOSS, and HOST standards.

During the pre-integration events and at these meetings, vendors coordinated on which test groups they would participate in and how their hardware would integrate into the PlugFest vision, goals and environment. Despite meticulous planning, the event itself demonstrated that integration efforts were often more organic than anticipated. Many vendors adapted their test setups on-site, leveraging opportunities to validate interoperability with hardware they had not previously planned to test against.


Figure 5: Pre-Integration PlugFest event in Atlanta, GA

While pre-integration planning laid the groundwork for successful demonstrations, the organic nature of PlugFest proved to be a valuable aspect of the event by driving real-time innovation and fostering deeper interoperability among participating vendors. Lessons from the 2025 event will inform future PlugFest iterations, further refining integration methodologies and enhancing the effectiveness of modular open systems within defense applications.

# 4. Technical Findings and Results

## 4.1 Overall Performance by Tier

Each participating group was evaluated on their level of performance to PlugFest objectives based on a three-tier system. These tiers measured the degree of integration, functionality, and interoperability demonstrated during the event. This section outlines the tiered criteria for each demonstration, along with a summary of the key technical demonstrations..

### 4.1.1 Tier 1 (Hardware Validation)

- The hardware successfully powers on without failure(s). Plug-In-Cards and chassis interfaces safely and correctly.
- Electrical interfaces for SOSA®, HOST, or CMOSS hardware function as intended.
- Basic system-level connectivity and initialization are confirmed (ex. Ethernet ping).

### 4.1.2 Tier 2 (Capability Execution)

- An application or capability is successfully executed on the hardware.
- The system processes data, performs computations, or demonstrates a key function.
- Performance metrics for the capability are captured and assessed.

### 4.1.3 Tier 3 (Interoperability and Modularity)

- The hardware and application demonstrate interoperability with other open hardware and software components. (ex. Containers installed on multiple Single Board Computers (SBCs)).
- The capability is integrated into a vendor agnostic system showing cross-vendor compatibility.
- Modularity is validated by swapping components or running multiple configurations successfully.

## 4.2 Executive Summaries of Demonstrations

### 4.2.1 US ARMY CMFF System Management

The U.S. Army's Open Innovation Lab (OIL) team participated in PlugFest to validate the interoperability and operational readiness of the CMOSS Mounted Form Factor (CMFF) architecture. The primary focus was on integrating the CMFF System Management software and the System Management Interface for Test Execution (SMITE) software with CMOSS hardware solutions across various chassis configurations. The secondary focus was to see that additional cards could be run in the system.

**Tier 1 - Hardware Validation**

- The Pacific Defense CMFF 9-slot and 2-slot chassis were tested with a range of CMOSS-aligned plug-in cards (PICs).
- Initial power-on tests successfully validated power integrity, mechanical fit, and electrical connections within the OpenVPX chassis.

**Tier 2 - Capability Execution**

- The CMFF System Management and SMITE software was deployed across different system configurations to evaluate its ability to monitor and manage chassis health.
- Multiple SBCs and networked processing units were integrated, revealing software compatibility issues with non-standard MORA implementations.
- The chassis management features were evaluated for fault detection and reporting, with mixed success due to VICTORY port mismatches and MORA inconsistencies in CMOSS implementations across different vendors.

**Tier 3 - Interoperability and Modularity**

- Several third-party PICs were introduced into the CMFF architecture, including radio, networking, and processing cards.
- Interoperability challenges were identified, particularly with inconsistent VPX interface implementations and port mismatches from different vendors.

### 4.2.2 Northrop Grumman's Single Module Radio Type 1 (SMRT)

Northrop Grumman's Single Module Radio Type 1 (SMRT) was demonstrated to validate its SOSA® aligned, BE-CDL waveform processing capability. The SMRT module was integrated with a Kratos Kestrel BE-CDL radio, aiming to establish high-bandwidth Ethernet-over-RF connectivity.

**Tier 1 - Hardware Validation**

- The SMRT module was installed in an LCR DK3 development chassis, alongside Abaco, Curtiss-Wright, and Concurrent Technologies SBCs.
- Initial power-on and link verification tests confirmed full electrical and mechanical compatibility with the OpenVPX chassis.
- Network link tests using ping utilities and packet inspection tools validated successful connectivity.

**Tier 2 - Capability Execution**

- The BE-CDL waveform was configured through a web-based GUI, establishing real-time RF communications.

- File transfer and VLC-based video streaming were conducted over the BE-CDL link, demonstrating effective data transmission and reception.
- Network latency and throughput measurements confirmed stable low-latency, high-bandwidth connectivity which is crucial for tactical data links.

**Tier 3 - Interoperability and Modularity**

- The SMRT module was tested with multiple SBCs, verifying hot-swappable functionality without requiring reconfiguration.
- Successful integration achieved with the Kratos Kestrel radio validated modularity in a multi-vendor OpenVPX environment.
- Future PlugFest iterations to focus on automated reconfiguration of waveform settings to enhance interoperability between BE-CDL radios and additional mission systems.

### 4.2.3 Northrop Grumman's Multi-Level Switch (MLSW)

The Multi-Level Switch (MLSW), developed as part of the Next Generation Cross Domain Solutions (NGCDS) Multi-Level Security Subsystem (MLSS), was evaluated for its cross-domain networking capabilities in handling secure multi-domain traffic.

**Tier 1 - Hardware Validation**

- Two configurations were tested: LBSA Configuration (Setup A) and Mission Operational Configuration (Setup B).
- Power-on validation confirmed optical link integrity via 10G-BaseSR connections.

**Tier 2 - Capability Execution**

- The MLSW was configured to enforce multi-domain traffic policies, utilizing CIPSO-labeled IPv4 routing.
- Data transmission test cases were conducted to validate network policy enforcement.
- Security enforcement policies successfully blocked unauthorized transmissions, ensuring secure, policy-driven data flows.

**Tier 3 - Interoperability and Modularity**

- The MLSW was tested with Curtiss-Wright, L3Harris, GE Aerospace, and SMRT vendor hardware.
- While basic interoperability was achieved, some vendors had incomplete data link connections that limited full integration.

### 4.2.4 Northrop Grumman's Open Sensor Platform (OSP) and Open Edge Processing (OEP)

The Northrop Grumman Open Sensor Platform (OSP) and Open Edge Processing (OEP) demonstrated full alignment with SOSA® principles, proving scalability, modularity, and interoperability across compute, RF, and networking domains. The L1310 chassis successfully integrated multi-vendor PICs, while OEP facilitated dynamic mission processing, reinforcing the DOD's vision of a Modular Open Systems Approach (MOSA).

**Tier 1 - Hardware Validation**

- Validated power-on, mechanical, electrical, and data plane compatibility for 11 of 12 PICs.
- Successfully booted SBCs into a Kubernetes cluster, enabling dynamic compute scaling.
- Integrated NVIDIA GPUs and RF transceivers, proving mission-readiness.

**Tier 2 - Capability Execution**

- Executed compute, RF, and networking workloads across multiple chassis.
- Remotely configured SDRs and transceivers, demonstrating modular RF control.
- Enabled real-time AI and ISR processing on NVIDIA GPUs.

**Tier 3 - Interoperability and Modularity**

- Achieved multi-vendor interoperability with seven PICs.
- Demonstrated dynamic reconfiguration of mission workloads in a distributed computing environment.
- Identified key interoperability challenges with BIOS settings, Layer 3 Ethernet, and RF clocking.

### 4.2.5 GE Aerospace's Cross-Domain Solution (CDS) and Time-Sensitive Networking (TSN) Switch

GE Aerospace evaluated their Monitoring and Inspection Device (MIND) Cross-Domain Solution (CDS) and VNetS-3320 Time-Sensitive Networking (TSN) Switch for baseline conformance with SOSA® and HOST standards. The effort focused on Tier 1 - Hardware Validation, assessing power-on functionality, mechanical fitment, electrical compatibility, and network link establishment across multiple vendors in nine (9) test environments.

**Tier 1 - Hardware Validation**

- Successfully powered on and validated baseline network connectivity in an X-ES XPAND1007 chassis using an X-ES VITA 62 power supply.
- Verified mechanical and electrical fitment, ensuring alignment with SOSA® aligned backplanes and slot profiles.
- Identified power supply compatibility issues with alternative VITA 62 PSUs, resulting in system reset failures due to voltage mismatches and keying differences.
- Confirmed basic control and data plane operation via SSH, ping, and initial Ethernet link tests.

### 4.2.6 BALSA and ARCM FACE® Applications

The Basic Avionics Lightweight Source Archetype (BALSA) and Aviation Radio Control Manager (ARCM) FACE® applications test group focused on integrating FACE® Units of Conformance aligned with the FACE® Technical Standard across multiple SBCs.

**Tier 1 - Hardware Validation**

- Validated vendor-agnostic SBCs with Curtiss-Wright, Concurrent and Kontron.
- SBCs experienced PXE booting issues, requiring manual BIOS reconfiguration.
- Serial console access was necessary to troubleshoot firmware inconsistencies.

**Tier 2 - Capability Execution**

- BALSA and ARCM applications were containerized and deployed across SBCs.
- RTI Connext FACE® Certified Conformant TSS enabled secure communication between application containers.
- Firewall and IGMP snooping configurations were adjusted to ensure continuous system stability.

**Tier 3 - Interoperability and Modularity**

- The BALSA EGI Unit of Conformance (UoC) was migrated to a separate SBC container.
- The addition of SOSA® Health Management Messaging enhanced real-time application monitoring.

### 4.2.7 SOSA® Containers

At PlugFest, Red Hat Device Edge (RHDE) was evaluated to demonstrate secure, scalable, and modular containerized execution across SOSA® aligned mission systems utilizing containers. The testing showcased RHDE's ability to support containerized workloads in a MOSA, showcasing cross-vendor integration, rapid deployment, and security compliance.

RHDE was tested in collaboration with multiple PlugFest test groups, including:

- FACE® Group – Enabled seamless execution of FACE® aligned applications across plug-in cards.
- GPU Group – Validated high-performance, AI/ISR workloads on NVIDIA GPUs within ELMA chassis.
- Communications and Security Group – Focused on zero-trust security compliance and modular container deployments.

**Tier 1 – Hardware Validation**

- Successfully deployed RHDE on SOSA® aligned SBCs with hands-free provisioning of both operating systems and container workloads.
- Validated compatibility with SBCs from Curtiss-Wright and Concurrent Technologies, including GPUs from Wolf and EIZO, housed within multiple chassis.

**Tier 2 – Capability Execution**

- Preinstalled drivers and applications executed for a containerized RIVA speech-to-text applications on vendor-agnostic SBCs working with NVIDIA GPUs, proving the feasibility of AI and sensor processing workloads.
- Enabled seamless container execution of FACE UoCs including BALSA, across multiple SBCs.

**Tier 3 – Interoperability and Modularity**

- Achieved full interoperability across multiple vendor platforms, proving workload portability and dynamic execution.
- Demonstrated hot-swappable container execution, allowing applications to be updated or reconfigured without system reboots.

### 4.2.8 GPU Group Report

The GPU group was led by Leidos with representatives from EIZO and WOLF. The objective of this group was to utilize multiple GPUs for running the same applications on multiple SBCs. Ideally, the only configuration that would need to be done on the SBC is to ensure the drivers are enabled in the RHEL image and the Riva and Holoscan demonstrations can run. Extremely successful test group integrating ten separate vendors inclusive of hardware, including chassis, cards and applications.

**Tier 1 – Hardware Validation**

- EIZO provided 2 GPUs and WOLF provided 2 GPUs. Each was able to be properly inserted, powered up and communicated with over Control and Expansion Plane.

**Tier 2 – Capability Extension**

- RHEL images preinstalled with drivers and applications were independently able to be booted to SBCs and confirmed to recognize GPUs connected over expansion plane.
- Riva and Holoscan demonstration and utilization shown on each GPU.

Tier 3 – **Interoperability and Modularity**

- The same PXE-booted RHEL image was used successfully on 2/3 SBCs provided to communicate with each GPU. One did not contain enough memory for the full image but was interfaced to the GPUs correctly.
- The group was able to remove the cards and run applications successfully in a different chassis live in front of PlugFest attendees

### 4.2.9 Chassis Management Group Report

The Chassis Management Group at PlugFest conducted a series of tests to evaluate the functionality of Chassis Managers and Intelligent Platform Management Controllers (IPMCs) using the SMITE tool. The focus was on verifying session setup, authentication, IPMI command responsiveness, and integration with in-band management software to assess the modularity and interoperability of chassis management solutions across different vendor platforms.

The SMITE tool was used to establish remote communication with chassis managers via Ethernet (RMCP), allowing for out-of-band device discovery and system monitoring. Additionally, an in-band system management demonstration was conducted, leveraging a HOST System Management Interface implementation to enable REST-based hardware monitoring and network configuration management. This in-band capability was also demonstrated on the Army CMFF chassis.

**Tier 1 – Hardware Validation**

- Successful chassis manager session setup and command executions were observed across multiple test platforms.
- Baseline IPMI and system discovery functionality was validated using the SMITE tool.
- Power supply compatibility issues were identified, affecting IPMB communication and causing session failures in some chassis.
- In-band management validation was conducted, demonstrating REST-based chassis monitoring and network diagnostics.

**Tested Chassis and Results**

- LCR Chassis (NAI Chassis Manager): Successfully initialized but became unresponsive after the first day, which prevented further testing.
- Concurrent Dev Chassis (ELMA Chassis Manager and Concurrent Payload SBC): Passed all session and IPMC validation tests with 80% Tier 2 IPMI command implementation; Tier 3 testing was not performed.
- AMS Chassis (AMS Chassis Manager): Passed session setup but encountered power supply-related failures affecting IPMB communication.
- Pixus Chassis (Crossfield Chassis Manager): Experienced session initialization failures which prevented testing.

# 5. Conclusion

PlugFest 2025 served as a pivotal platform to advance Open Architecture principles within the defense sector, facilitating collaboration among over 30 industry and government organizations. As the outcomes of this event are analyzed, several practical lessons emerge that can enhance future planning and execution of Concept of Operations (CONOPs).

A primary lesson learned is the necessity for comprehensive pre-event integration activities. While the two preparatory events were beneficial in establishing initial compatibility among systems, unforeseen challenges arose during the main event. And although structured planning meetings were held, the dynamic nature of interactions during PlugFest 2025 highlighted the need for enhanced adaptability. Future CONOPs should prioritize comprehensive checklists, clear communication channels and establish designated points of contact who can facilitate immediate troubleshooting and decision-making during live demonstrations. That approach would serve to minimize downtime and increase efficiency.

Networking configurations and infrastructure proved to be another area requiring attention. Many participants encountered connectivity issues that stemmed from inadequate network setups which were exacerbated by the transition from pre-event environments to the PlugFest venue. To mitigate such risks in future events, CONOPs should include detailed network architecture plans that account for potential vulnerabilities. Additionally, having backup solutions readily available can provide a safety net against unforeseen failures.

Moreover, the significance of documentation and knowledge sharing cannot be overstated. Future CONOPs should emphasize comprehensive documentation practices, ensuring that lessons learned, best practices, and technical insights are recorded and made accessible to all stakeholders. Establishing a repository for this information would assist in learning and preparation for future events.

To enhance the effectiveness of future PlugFests, it is crucial to secure adequate support from the Department of Defense (DOD). This includes fostering buy-in from program offices regarding their specific needs and expectations for Electric Warfare capabilities. Engaging with these offices early in the planning process will help to ensure the objectives of PlugFest align with the strategic goals of the DOD, leading to more relevant demonstrations and outcomes overall.

In conclusion, the experiences gained and learned from PlugFest offer valuable insights into improving the integration of Open Architecture systems within the defense sector. By focusing on thorough pre-event preparations, enhancing communication, ensuring robust networking infrastructures, embracing operational flexibility, and prioritizing effective documentation, future CONOPs can be significantly refined. These practical lessons, coupled with strong DOD support and engagement from program offices, will contribute to the successful implementation of modular and interoperable defense technologies, thereby enhancing the operational readiness and effectiveness of U.S. military forces in the realm of electronic warfare and beyond.

## 6. About the Author

Cody Cox, a Research Engineer at the Georgia Tech Research Institute, has been instrumental in advancing open architecture systems in military technology. Cody served for five years in the United States Navy as an Aviation Electronic Technician, Intermediate level (AT-I), where he calibrated and maintained Advanced Targeting Forward-Looking Infrared (ATFLIR) Pods for F/A-18 aircraft aboard the USS Dwight D. Eisenhower (CVN-69) during Operation Enduring Freedom. After his military service, he earned a B.S. degree in Mechatronics Engineering at Kennesaw State University.

Cody played a pivotal role in the MQ-9 Reaper's sensor modernization project, which used MOSA and the SOSA® Technical Standard to enhance the MTS with advanced computing capabilities. This upgrade facilitated rapid hardware updates, improved image scanning, and better system interoperability. The project's success ensured the MQ-9 could efficiently adapt to evolving technology requirements.

Since joining GTRI's Open Systems Development Branch (OSDB) in 2020, Cody has played a crucial role in supporting Department of Defense (DoD) sponsors through the development and implementation of Open Architectures. In 2021, he began directing the MQ-9 program at GTRI, spearheading efforts to modernize the MTS in alignment with the SOSA® Technical Standard. The primary mission of GTRI's OSDB is to assist DoD sponsors in integrating Open Architecture designs that meet Title 10 Initiatives, including developing OA standards, prototyping OA systems to align with these standards, and advising on published standards to demonstrate advanced capabilities.

In 2024, Cody took on a leading role in organizing and executing PlugFest, a multi-organizational interoperability event focused on validating modular open systems across the defense community. Under his direction, PlugFest brought together vendors and government stakeholders to demonstrate real-world system integration based on SOSA®, FACE® and other open standards. Cody was instrumental in defining test group objectives, guiding participants through pre-integration requirements, and ensuring a smooth execution of the event.

In 2025, Cody currently serves as Program Director for the Small Form Factor (SFF) Advanced Multi-purpose Multi-size Color Display (AMMCD) program at GTRI. In this capacity, he is overseeing the development and integration of a SFF feasibility prototype aimed at modernizing cockpit display systems that comply with MOSA standards.

GTRI's OSDB operates an Open Architecture System Integration Lab (SIL) in Atlanta, where SOSA® aligned hardware is integrated and tested across various programs. The OSDB also collaborates with prime contractors on DoD-sponsored projects, acting as the lead system integrator to ensure the use of OA designs and providing technical ownership to government sponsors. The MTS Chassis modernization effort is a prime example of OSDB's successful collaboration with industry partners, ensuring OA designs and government technical ownership.

**About The Open Group FACE® Consortium**

The Open Group Future Airborne Capability Environment® Consortium (the FACE® Consortium), was formed as a government and industry partnership to define an open avionics environment for all military airborne platform types. Today, it is an aviation-focused professional group made up of industry suppliers, customers, academia, and users. The FACE® Consortium provides a vendor-neutral forum for industry and government to work together to develop and consolidate the open standards, best practices, guidance documents, and business strategy necessary for acquisition of affordable software systems that promote innovation and rapid integration of portable capabilities across global defense programs.

Further information on the FACE® Consortium is available at www.opengroup.org/face.

**About The Open Group SOSA® Consortium**

The Open Group SOSA® Consortium enables government and industry to collaboratively develop open standards and best practices to enable, enhance, and accelerate the deployment of affordable, capable, interoperable sensor systems. The SOSA® Consortium is creating open system reference architectures applicable to military and commercial sensor systems and a business model that balances stakeholder interests. The architectures employ modular design and use widely supported, consensus-based, nonproprietary standards for key interfaces.

Further information on the SOSA® Consortium is available at www.opengroup.org/sosa.

**About The Open Group**

The Open Group is a global consortium that enables the achievement of business objectives through technology standards and open-source initiatives by fostering a culture of collaboration, inclusivity, and mutual respect among our diverse membership of more than 900 organizations. Our membership includes customers, systems and solutions suppliers, tool vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open-source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.