Open System Architecture as Applied to Air-Launched Weapons

Oct 2019

Jonathan Shaver
Air Force Research Laboratory

Leo Rose
Rapid Prototyping Cell, AFLCMC
Modular Open Architecture Definition

The Department of Defense’s (DoD) modular open systems approach (MOSA) is to design systems with **highly cohesive, loosely coupled, and severable modules** that can be competed separately and **acquired from independent vendors**. This approach allows the Department to acquire warfighting capabilities, including systems, subsystems, software components, and services, with more flexibility and competition. MOSA implies the use of modular open systems architecture, a structure in which **system interfaces share common, widely accepted standards**, with which **conformance can be verified**.
Weapons Open System Architecture (WOSA)

• Non-proprietary architectural standards for all munitions developed and maintained with industry consensus
  – open key-interfaces, modularity and composition requirements

• Goal to improve acquisition efficiency
  – Reduce integration cost/risk
  – Reduce Lifecycle Cost
  – Enable adaptability and reuse
  – Decouple software/subsystem from hardware
  – Decrease development and integration time
  – Reduce obsolescence impacts via competition & rapid tech insertion

• Open Architecture products needed
  – Non-proprietary architecture (Government Owned)
    • Detailed architecture specification
    • Architecture Reference Model
  – Compliance testing tools
  – Compliance verification
Government Owned Architecture
Industry/Government Consensus

• Government and Industry have worked together through voluntary consensus-based WOSA Interface Control Working Groups
  – Modular design is based primarily on widely supported, consensus-based standards for key interfaces

• Interface Control Working Group (ICWG)
  – Quarterly meetings with technical interchange meetings monthly
  – Released Ver 1.3 WOSA Specification July 2019
  – Complete Weapon Specification

• Government architecture that can be independently tested to ensure compliance with standards

Partnership through

NDIA
Weapon Open Systems Architecture
Development Team

WOSA Government Team
Chaired by AFRL/RW

Government Support
WINTEC, Inc.
ENGILITY
Space Dynamics

Prime Contractors
Lockheed Martin
Raytheon
Boeing
TEXTRON

Consensus-based
Open System Architecture Standards

MBDA, Rockwell Collins, Northrop Grumman, General Atomics, Orbital-ATK, General Dynamics
Standardized Internet as of Today

Internet (Routing, QoS, Reliable Delivery)

Facebook
Google
Amazon

Power System
Batteries
Solar Array
Cellular
Cell Tower

OSI Model

Application
Network process to application

Presentation
Data representation, encryption, conversion

Session
Interhost communication, session management

Transport
End-to-end connections, reliability, flow control

Network
Path determination and logical addressing

Data Link
Physical addressing

Physical
Media, signal and binary transmission

Application Vendor Responsible

Internet Infrastructure

= Standard Internet Interfaces
WOSA Applied to Weapons

- Munition Open Architecture Test and Evaluation Laboratory (MOATEL)
  - Evaluate performance of the Munitions Data Bus (MDB)
  - Will not evaluate performance of other domains (i.e. Seeker)
WOSA Framework

- Potential breakpoints of a system
- MDB is a message routing device (i.e. Ethernet router)
- Message header / payload formats are defined by ICD
- Most important attributes of messages are Frequency, Latency and Jitter
- Custom message formats allowed for implementation specific scenarios
System Analysis
Munitions Open Architecture Test and Evaluation Lab (MOATEL)

- Modular Test Environment
- Verification Plan
- Document review
- Real Time test tools
- Verification Report
- Architecture review
Analysis Plan

• Linearize airframe from non-linear data
  – Design stable terminal autopilot

• Frequency domain stability analysis
  – Root locus
  – Bode plots
    • Phase and Gain Margin Baseline Design
  – Nyquist plots

• Add Open Architecture data transport delay models
  – Set cycle time (update rate) requirements to maintain stability and performance

• Time Simulation for non-linear modeling and trajectory analysis
Isolated Nodal Analysis: Varied Range

- Maximum allowable delay per factor for each variant.
  - Based on when the full loop system dropped below 6 dB gain margin and 45 degree phase margin
- Using different range for each variant based on its individual baseline test
  - Range per variant was based on the larger point where:
    - Gain margin = 8 dB
    - Phase margin = 65°

<table>
<thead>
<tr>
<th>Architectural Delay</th>
<th>Variant 1</th>
<th>Variant 2</th>
<th>Variant 3</th>
<th>Variant 4</th>
<th>Variant 5</th>
<th>All Variants</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range = 293.03 m</td>
<td>Range = 134.56 m</td>
<td>Range = 247.09 m</td>
<td>Range = 109.92 m</td>
<td>Range = 46.17 m</td>
<td>Max Allowable Delay (msec)</td>
</tr>
<tr>
<td></td>
<td>Breakpoint (msec)</td>
<td>Breakpoint (msec)</td>
<td>Breakpoint (msec)</td>
<td>Breakpoint (msec)</td>
<td>Breakpoint (msec)</td>
<td></td>
</tr>
<tr>
<td>Actuator Node</td>
<td>G.M. 8.5  P.M. 7.9</td>
<td>G.M. 7.0  P.M. 16.8</td>
<td>G.M. 10.4  P.M. 6.3</td>
<td>G.M. 7.6  P.M. 4.8</td>
<td>G.M. 7.6  P.M. 14.9</td>
<td>4.8</td>
</tr>
<tr>
<td>Gyro Node</td>
<td>G.M. 33.2  P.M. 38.6</td>
<td>G.M. 5.1  P.M. 9.9</td>
<td>G.M. 44.8  P.M. 49.8</td>
<td>G.M. 33.0  P.M. 36.2</td>
<td>G.M. 18.2  P.M. 39.8</td>
<td>5.1</td>
</tr>
<tr>
<td>Accel Node</td>
<td>G.M. 27.9  P.M. 12.3</td>
<td>G.M. 219.7  P.M. 1000.0</td>
<td>G.M. 19.1  P.M. 6.3</td>
<td>G.M. 17.8  P.M. 6.0</td>
<td>G.M. 56.8  P.M. 23.3</td>
<td>6.0</td>
</tr>
<tr>
<td>AP Node</td>
<td>G.M. 17.7  P.M. 33.4</td>
<td>G.M. 401.4  P.M. 1432.1</td>
<td>G.M. 24.9  P.M. 27.7</td>
<td>G.M. 17.6  P.M. 22.7</td>
<td>G.M. 15.8  P.M. 31.5</td>
<td>15.8</td>
</tr>
<tr>
<td>Guidance Node</td>
<td>G.M. 17.7  P.M. 33.4</td>
<td>G.M. 401.4  P.M. 1432.1</td>
<td>G.M. 24.9  P.M. 27.7</td>
<td>G.M. 17.6  P.M. 22.7</td>
<td>G.M. 15.8  P.M. 31.5</td>
<td>15.8</td>
</tr>
</tbody>
</table>
Munition Data Bus Latency Requirements

### Processing

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unformatted Data Available in processor</td>
<td>WOSA MSG Ready to be sent (MSG Validity Time Mark)</td>
</tr>
<tr>
<td>1st bit transmitted over wire</td>
<td>Last bit received by transport hub for processing</td>
</tr>
<tr>
<td>Last bit received by transport hub</td>
<td>Msg Available to Hub for processing</td>
</tr>
<tr>
<td>Msg ready to transmit</td>
<td>1st bit transmitted over wire</td>
</tr>
<tr>
<td>Last bit received by target domain</td>
<td>Data Available for consumption</td>
</tr>
</tbody>
</table>

### MDB Delay

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Max Acceptable Latency (msec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actuator Node</td>
<td>0.42</td>
</tr>
<tr>
<td>Gyroscope Node</td>
<td>0.50</td>
</tr>
<tr>
<td>Accelerometer Node</td>
<td>0.56</td>
</tr>
<tr>
<td>Autopilot Node</td>
<td>1.25</td>
</tr>
<tr>
<td>Guidance Node</td>
<td>1.25</td>
</tr>
</tbody>
</table>
Interface Verification Test

Objective: Validate interface byte order and interface functionality

Test Details:
- 2 Domains – 1 Sender, 1 Listener
- 24 byte signal will be sent across the bus at 1 Hz
- 10 second test
- Repeated for all domain interface types pairings

Pass/Fail criteria:
- All 10 messages are received by listener domain for each interface type pair

*(MDB BIT/Status?)*

<table>
<thead>
<tr>
<th>Test Domain 1 Interface Type</th>
<th>Test Domain 2 Interface Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB</td>
<td>USB</td>
</tr>
<tr>
<td>UDP</td>
<td>UDP</td>
</tr>
<tr>
<td>RS-232</td>
<td>RS-232</td>
</tr>
<tr>
<td>RS-422</td>
<td>RS-422</td>
</tr>
</tbody>
</table>

*(MDB BIT/Status?)*
Interface Loading Test

Objective: Determine how the MDB will act under varying loads and see how varying throughputs affect the latency and jitter

<table>
<thead>
<tr>
<th>Rates (Hz)</th>
<th>10</th>
<th>50</th>
<th>100</th>
<th>200</th>
<th>500</th>
<th>1000</th>
<th>2000</th>
<th>10000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size (Bytes)</td>
<td>4</td>
<td>2</td>
<td>50</td>
<td>100</td>
<td>200</td>
<td>500</td>
<td>1000</td>
<td>2000</td>
</tr>
</tbody>
</table>

Test Details:
- 2 Domains - 1 Sender, 1 Listener
- 9 rates tested (10 - 10,000 Hz) with 8 msg sizes (26 - 10,000 bytes) for a total of 72 tests

Pass/Fail criteria:
- No specific pass/fail identified
- Characterization of performance limitations of MDB
Weapon System Decomposition

- CAS – Control Actuator System
- D/L – Data Link
- EIU – Engine Interface Unit
- ESAD – Electronic Safe And Arm Device
- MDB – Munitions Data Bus
- MP – Mission Processor
- OAE – Open Architecture Electronics
- WFCC – Weapon Flight Controller Computer

**Weapon Flight Controller Computer**
- Navigation Services
- Guidance Services

**Mission Processor (MP)**
- Mission Plan Management
- Dynamic MP & Re-routing
- Sensing Management
- Target Attack Management
- Test Equipment Services
- Weapon Services

**Service Distribution Layer**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**WOSA Components**
- Changeable Subsystems
- Serial Bus
- 1G Ethernet
- Power

**Changeable Subsystems**
- A/C 1760 Interface
- Test Interface/Shore power
- GPS Keys Interface
- GPS Antenna

**Power**
- Battery
- Alternator
- Fuel Pump
- EIU

**Control Power**
- Engine

**Infrastructure Services**
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**Autopilot Services**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**Dynamic MP & Re-routing**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**Sensing Management**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**Target Attack Management**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**Test Equipment Services**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services

**Weapon Services**
- Infrastructure Services
- Launch Platform Services
- Mission Planning Services
- Test Equipment Services
- Weapon Services
Acquisition Strategy Implementing Open Architecture

• Weapon designed with Open Architecture (based on WOSA)
  • Assume four major components (propulsion, GNC, effects, and seeker)
  • Government defines breakpoints
  • Government defines and owns physical and logical interfaces between components
Open Architecture Based Acquisition Strategy

• Industry’s Business Strategy that implements Open Architecture should be based on specific acquisition strategy for that particular weapon
  • Warfighter, acquisition program office, test community, and logistics must work together to establish battle rhythm for development / test / production / sustainment of weapon
  • Open architecture should enable new, more flexible modification methods to weapons throughout its lifespan
• Acquisition strategy can then be conveyed to industry to adjust their business model accordingly
• Acquisition Strategy examples (Use Cases) can be used to talk through issues or identify potential risk areas
Open Architecture Based Acquisition Strategy
Use Case #1

Premise – Weapon designed for technology refresh

• Assumptions:
  • Gov owns interface between components
  • OML / mass properties don’t change but functionality can incrementally improve
  • Interfaces have been designed to accommodate future operational growth

• Example:
  • Seeker is the component identified for tech refresh
  • Warfighter accepts a “60% performance” for first weapon variant
  • Interfaces, OML, mass properties, etc. are Gov owned and fixed
  • First weapon variant takes off-the-shelf seeker and integrates components together
  • S&T community matures next generation seeker
  • Vendor takes new seeker and integrates with existing components
  • Process is repeated until desired seeker performance is achieved

• Benefit to Gov:
  • Quickly delivers a capability to warfighter – inventory begins to grow
  • Conduct A/C integration once – first variant goes through all steps, next do not
  • Reduce logistics costs – replace old seeker with new and have only one variant in inventory
Open Architecture Based Acquisition Strategy
Use Case #2

Premise – Common component used across multiple weapons

• Assumptions:
  • Gov selects a specific function (i.e. component) within a current weapon
  • Breakpoints (i.e. interfaces) between component and rest of weapon are Gov owned/defined
  • Specific function (i.e. component) is mature (“EMD” or later)
  • Gov mandates this function to all future weapons that need that function

• Example:
  • Function (i.e. component) is a processor board that hosts the Guidance, Nav, Control, and Target State Estimator software for current weapon
  • New program starts and has a function similar to existing weapon
  • Gov will GFE component (i.e. processor board) to vendors of new program
  • Vendors will develop their own software to address new program’s specific requirements (i.e. modified TSE or Guidance algorithms)
  • Vendor that is manufacturing processor board will be required to increase production rates to satisfy both programs

• Benefit to Gov:
  • Stops re-inventing the wheel – makes use of the time and dollars already invested
  • Increases production rates – each new program added drives cost down of component
  • Lift of incremental improvements – all programs reap benefits of constant improvements
Open Architecture Based Acquisition Strategy
Use Case #3

Premise – Common weapon with 2 functionally different sub-components

• Assumptions:
  - Gov owns interface between two pieces of weapon
  - Program requires two variants of sub-component and nothing else changes
  - Two “variants” have been successfully integrated on platform

• Example:
  - Warfighter desires weapon to have two different ranges – short and long
  - Program matures two different rocket motors (i.e. two different OMLs)
  - Front end (seeker, GEU, warhead, batteries, etc) are common except for software to account for extra propulsion
  - Integrator will “tune” software to accommodate both rocket motor variants

• Benefit to Gov:
  - Warfighter flexibility – ability to select weapon range based on needs of mission
  - Incremental improvement – each portion can be upgraded separately
Open Architecture Based Acquisition Strategy
Use Case #4

Premise – Weapon has four major components and three breakpoints

• Assumptions:
  • Gov owns interface between four major components
  • OML does not change but any component within OML can
  • Gov, or their agent, is the system integrator

• Example:
  • Each of the four major components (i.e. seeker, GNC, warhead, propulsion) are competed separately
  • Interfaces, OML, mass properties, etc. are fixed within each component grouping
  • Gov issues performance parameters for all four components
  • Gov, or their agent, integrates four components
  • Production vendor builds all-up-round with four GFE components
  • As technology improves for each component, it can be quickly integrated into weapon

• Benefit to Gov:
  • Best capability to warfighter – each component is competed separately
  • Accommodates tech refresh – each component can improve as S&T delivers new capability
  • Increase competition – second-tier vendors can now compete directly
Open Architecture Based Acquisition Strategy

• Acquisition Program Manager (PM) can not predict or control:
  • Funding
  • Requirements / threat changes

• Open Architecture Based Acquisition Strategy helps mitigate issues
  • Funding Reduction
    • PM can switch tech refresh from expensive component upgrade to less expensive technology
    • PM can reduce the number of risk reduction options
    • PM can skip upgrade and wait till funding available
  • Requirements / threat changes
    • PM can change tech refresh technology to immediately address threat change
    • PM can switch technology to quickly transition from S&T community
Contact Info

• AFRL WOSA
  – Jonathan Shaver – jonathan.shaver.1@us.af.mil
  – Chris Neal – christopher.neal.8@us.af.mil
  – Patrick Bagby - patrick.bagby.ctr@us.af.mil
  – WOSA Website via APAN.ORG - https://community.apan.org/wg/wosa/
    • Contact Jonathan or Chris to gain access

• AFRL Cybersecurity
  – Nahid Gezgin – nahid.gezgin.1@us.af.mil

• Rapid Prototyping Cell
  – Leo Rose – leo.rose.2.ctr@us.af.mil
Questions