2024 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
MODULAR OPEN SYSTEMS APPROACH (MOSA) TECHNICAL SESSION
AUGUST 13-15, 2024 - NOVI, MICHIGAN

A MOSA APPROACH FOR GROUND VEHICLE SYSTEM ENTERPRISE COMMONALITY

Anand Kelkar[1], Matt Rossmiller[1]

[1]Jovian Software Consulting, Grand Rapids, MI

ABSTRACT

We review architecture concepts adopted and refined in the Future Vertical Lift Architecture Framework, and their applicability to GCIA and MOSA in the ground vehicle domain, including Digital Backbone, Enterprise Key Interfaces, Enterprise Data Model, Transport Services, and Common Services. We also discuss how this MOSA approach combined with a Service Oriented Architecture (SOA) can enable Ground Vehicle System Enterprise commonality to deliver solutions for Multi-Domain Operations.

Citation: A. Kelkar, M. Rossmiller, "A MOSA Approach for Ground Vehicle System Enterprise Commonality," In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2024.

1. INTRODUCTION

Modular Open Systems Approach (MOSA) is intended to support fast fielding of capabilities, improve reuse, and reduce development costs for systems. Current ground combat systems (GCS) enterprise systems have several limiting characteristics that are relevant to MOSA goals, including: vendor-locked system architectures, unique representations of data across solutions, limited reuse of components, and interoperability challenges presented by unique architectures, communications, and data. Figure 1 provides a visualization of the current situation across enterprise systems, where each color represents unique components or interfaces. Although tactical datalinks provide well-defined communications to enable interoperability, individual weapon systems struggle to achieve reuse of components or functionality.

To keep pace with emerging threats, future formations will combine manned vehicles, unmanned/robotic vehicles, launched effects and unmanned air vehicles. These Multi-Domain Operations (MDO) will require highly integrated operations, demanding more from weapon systems and soldiers. Weapon systems will need to support a mesh of common capabilities to provide soldiers

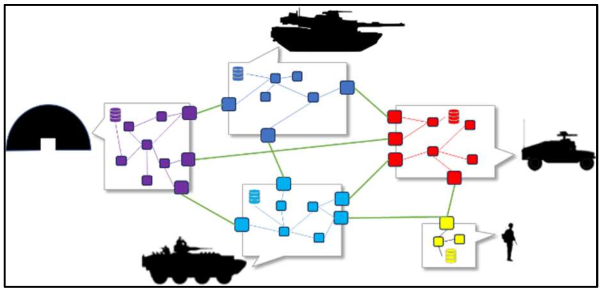

Figure 1: Uniqueness in Enterprise Systems

with the data they need. Soldiers need to train and execute missions using a consistent set of human-machine integration capabilities.

The Future Vertical Lift (FVL) Architecture Framework (FAF) [1] was designed to address these limitations for U.S. Army Aviation and beyond. This paper discusses the architecture concepts adopted and refined in the FAF, combined with Service Oriented Architecture (SOA) to satisfy the GCS Common Infrastructure Architecture (GCIA) and achieve ground vehicle system enterprise commonality.

These concepts include Digital Backbone, Enterprise Key Interfaces, Enterprise Data Model, and Transport Services, and Common Components.

2. DIGITAL BACKBONE

The Digital Backbone provides a common interconnect for weapon system components in support of key architecture properties such as adaptability and interoperability over the enterprise lifecycle.

Digital backbone defines the allocation of space for components in the system. The digital backbone also defines how power, thermal and data are distributed in the weapon system through the interconnected set of components. The Digital Backbone definition includes the following characteristics:

2.1. Government Purpose Rights

Government Purpose Rights (GPR), or less restrictive rights, are provided on descriptions of all digital backbone component interfaces, including mechanical, thermal, electrical, and data. These components may include switches, routers, power and thermal distribution modules, and infrastructure which enable core digital backbone functionality. Description of interfaces includes both the structural and behavioral aspects of components. Requiring GPR, or less restrictive, for all component interfaces ensures the government has access to information critical to future component updates or replacements.

2.2. Isolation

Isolation is provided between weapon system safety-critical and mission systems domains. This isolation is primarily intended to limit the impact of mission system changes on safety-critical system domains. Isolation between the mission and safety-critical domains allows accelerated fielding of mission capabilities which do not impact safety-critical features of the weapon system. Isolation may also provide cyber-security guard functionality to satisfy requirements identified by cyber analysis.

2.3. Installation Provisioning

Descriptions of component installation spaces within the weapon system physical structure. These descriptions define the spaces reserved for the installation of components, cables, and connectors; including any constraints on the system elements installed in these locations. Such descriptions enable component environment and suitability analysis in support of system updates.

2.4. Domain Provisioning

Identify equipment installed as part of initial weapon system manufacturing such as power or thermal distribution, equipment which support safety-critical functions of the weapon system such as drive/fly-by-wire, and equipment which supports functions of the mission system such as sensing. Together with the isolation strategy described above, this structural separation of the component architecture domains controls the impact of updates.

2.5. High-Speed Determinism

High-speed multi-access data links with support for deterministic communication, such as TSN, TTE, or ARINC 664p7, are recommended for the core of the Digital Backbone network. Having all weapon system data available on the selected core network technology, with the flexibility to support determinism when needed to satisfy real-time constraints provides necessary flexibility to support communication pattern evolution throughout the life of the weapon system. In cases where it is necessary to use components with legacy interfaces, these interfaces are adapted to communicate on the selected core network technology as close to the network edge as possible.

3. ENTERPRISE KEY INTERFACES

Key Interfaces help to drive commonality within, and between enterprise weapon systems. Key Interfaces are those interfaces which are identified, specified, and required by the government to meet MOSA, Mission, and Product Line Management objectives for the Enterprise platforms in the multi-domain battle space.

Key Interfaces are identified based upon a rigorous process, considering the need for equipment reuse, expected updatability constraints; the impact on operation, effectiveness, interoperability, or sustainment; the probability of change; and the ability to standardize. Establishing and requiring the use of key interfaces restricts the interoperability domain, simplifying reuse of components across the enterprise.

Key interfaces must be managed over the enterprise lifecycle, managing deprecated and new interfaces to coordinate support of technology changes, in support of enterprise objectives.

4. ENTERPRISE DATA MODEL

An Enterprise Data Model, realized as Domain Specific Data Models (DSDM) for the Enterprise using common conceptual and logical definitions ensures that system components will have compatible data representations. Managing the DSDM and requiring component conformance to the DSDM enables rapid integration.

Management of the DSDM is necessary to ensure the data definitions remain relevant and sufficient for developers of enterprise components. It is a continuous process, addressing feedback on existing entities, proposals for new entities, and approving updates to the DSDM. Maintaining the DSDM requires active participation from government and industry throughout the enterprise lifecycle.

Conformance to the DSDM means that components are required to base their data representations on the definitions provided in the DSDM, rather than create competing representations. Connecting component physical messages to the DSDM-provided conceptual and logical definitions facilitates integration automation, including definition of message transformations.

5. TRANSPORT SERVICES

The use of Transport Services, as defined in the FACE^{TM} Technical Standard [2], abstracts components from underlying communications, configuration, storage, and frameworks. Using transport services to connect the digital backbone, software can be moved between system compute resources with minimal integration impact. Transport Services allow the integrator significant flexibility to connect software components across new and enduring systems.

The FACE^{TM} Technical Standard allows flexible deployment of Transport Services capabilities. The following provides a summary of key capabilities which help to support the MOSA.

5.1. Type Specific Interface

The Type Specific interface provides a standard for translation of a component's data model into a runtime API. The connection to the data model provides for a common interpretation of message data across components, and enables transport services to provide data transformation when required.

5.2. Data Transformation

Data Transformation allows the Transport Services to resolve mismatches between physical interfaces without modification to the communicating components. It allows modular boundaries to be preserved when deploying components.

5.3. Transport Protocol Module

The Transport Protocol Module (TPM) allows the transport services to be easily adapted to communication on multiple types of data links. The ability to upgrade physical/data link technologies, and/or deploy transport on systems with independent data links enables reuse of transport technologies across current and future network architectures.

5.4. Data Storage

The Data Storage capability abstracts the interface to physical storage media. Storage implementations may support network and local storage resources. The capability enables independent deployment of component's compute and storage dependencies.

6. SOA

The use of Service Oriented Architecture (SOA) is a significant enabler for MOSA in enterprise systems. Using a SOA simplifies the reuse of components across different enterprise systems. Services may be developed independently, supporting a modular approach to system composition, or update. Building architectures around high granularity, loosely coupled services simplifies new technology insertion, because services may be replaced independently, without impacting the overall functionality of the existing system.

The FAF development process identified many benefits of the SOA, including: improved ability to use real system components in simulation or training environments; ability to reuse human-machine interface (HMI) across systems or visualizations; ability to define components as service product lines supporting component reuse, including reuse of major system components; and the ability to incrementally introduce technology change using existing service frameworks.

The SOA approach is aligned with Army Unified Data Reference Architecture [3] (UDRA). The service interfaces convey data products defined by a common services data model. As currently defined, services consume, aggregate, and produce data products, and are extensible to support the full range of UDRA activities.

The SOA approach defined in the FAF includes the following characteristics.

6.1. Service Interfaces

Each service interface is defined with a data definition using platform templates. Using data definitions in accordance with the FACE^{TM} Technical Standard enables use of the Transport Services capabilities, such as data transformation which allows for more flexibility in deploying services. Some services may be distributed across service nodes for availability or redundancy; others may be centralized. Using a standard Transport Services interfaces specification allows the integrator to use features of the transport services to support any required deployment pattern.

6.2. Component Specifications

The FAF approach includes defining each service needed using a Component Specification Model (CSM). The CSMs are defined and owned by the government. Service CSM implementations are required to provide GPR data rights to enable broad reuse of built services. A CSM provides component requirements, along with functional and structural architecture for the component, and interface definitions using logical query specifications. CSMs are currently defined for the services listed in section 7.

6.3. SOA Node Concept

The services are intended to be deployed into a set of SOA nodes. Within each node, various concepts are implemented as needed to support the mission capabilities implemented at that node. An overview of SOA Node elements is provided in Figure 2.

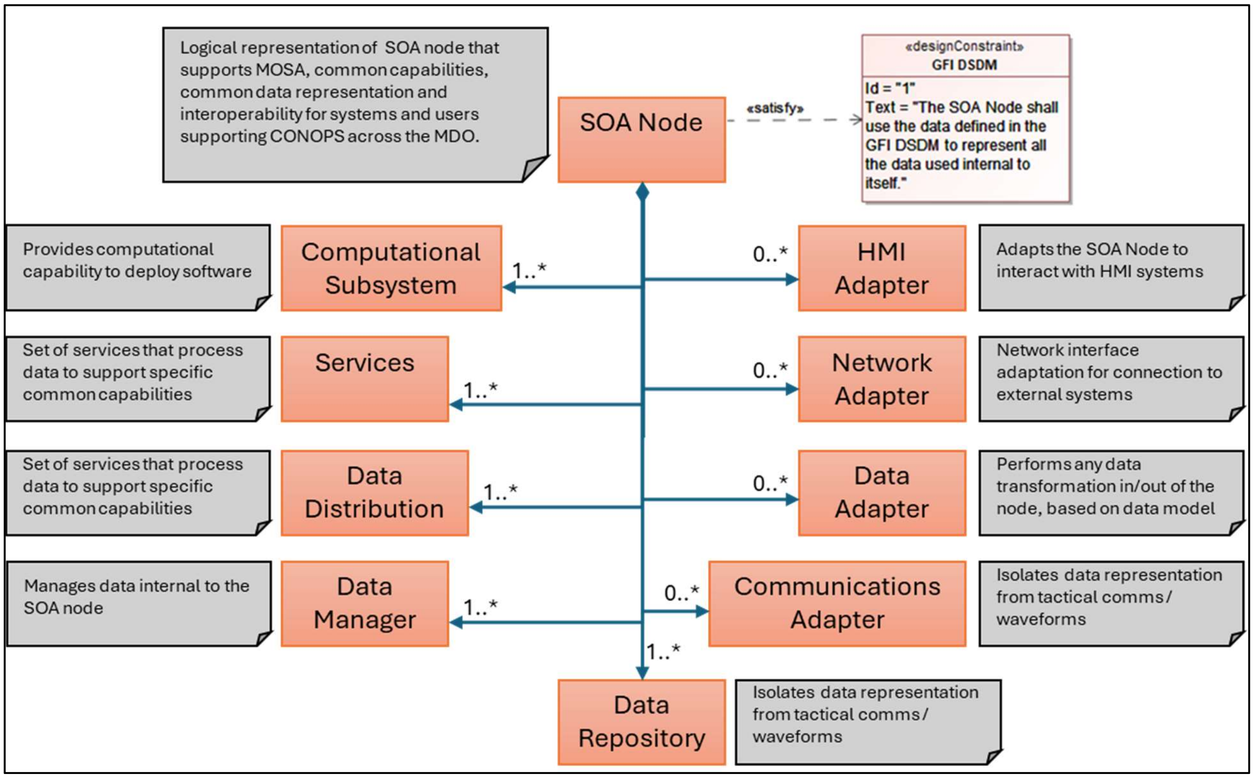

Figure 2: SOA Node Overview

7. COMMON COMPONENTS

In order to identify a general SOA for the enterprise, weapon system functionality is allocated to a common set of services, which may be deployed across enterprise systems. Each service has a defined interface which associates modeled data with a behavioral specification for the service. The enterprise common services include:

7.1. Infrastructure Services

Infrastructure services include those services which provide the basic functionality needed to support mission or vehicle services (Table 1).

Table 1: Infrastructure Services

Vehicle System Monitoring
Dataload
Data Logging
Data Storage
Operational Mode Management
Platform Configuration Data
System Capability Registry
System Health Management
System Time Information

7.2. Mission Services

Mission services include the set of services which support typical mission capabilities of a weapon system (Table 2).

Table 2: Mission Services

Area of Interest
Common Operating Picture
Element of Interest
Hazard Management
Map Data Management
Mission Data Management
Navigation Data Management
Obstacle Management
Risk Assessment
Route Management
Stores Management
Threat Management
Terrian Data Management
Track Management

7.3. Platform Services

Platform services provide access to information about the weapon system platform which are relevant to basic operation of the platform (Table 3).

Table 3: Platform Services

Position Data
Platform Performance Data

7.4. Cyber Services

Cyber services include the set of services which support run-time cybersecurity in the weapon system (Table 4).

Table 4: Cyber Services

Digital Signature
Encryption-Decryption
Key Management
Security Event Audit
User Authentication

7.5. Tactical Data Translators

The tactical data translation implements communications through adapter service nodes. Service nodes are defined for common tactical datalinks, including VMF, Link-16, UAS IOP, and AFAPD. As additional communication needs (such as UGV IOP) are identified, they can be added as additional adapter service nodes. Using services interfaces based on common DSDM enables automation in the production of data transformation definitions, simplifying integration when supporting new communication paths.

7.6. Major System Components

Major System Components can also be defined as services. For example, Advanced Teaming may be defined as a set of collaboration service nodes and communications may be defined as Data Service Nodes.

8. APPLICATION TO GROUND

Although initially consolidated in the context of FVL, the pattern defined can also bring benefits to new and enduring ground vehicle architectures. Taken together, the architectural approaches will facilitate transition toward ground vehicle systems which support enterprise-wide reuse of services and components. Building out new components and capabilities using an SOA based on a shared DSDM with defined key interfaces enables inter-domain portability of services and solutions. The defined common services may be used to bootstrap an SOA satisfying current GCIA objectives. Figure 3 provides a visualization of how systems built under an SOA pattern can be applied to benefit enduring weapon systems. As the deployed base of common capabilities grows (Figure 4), common capabilities may be

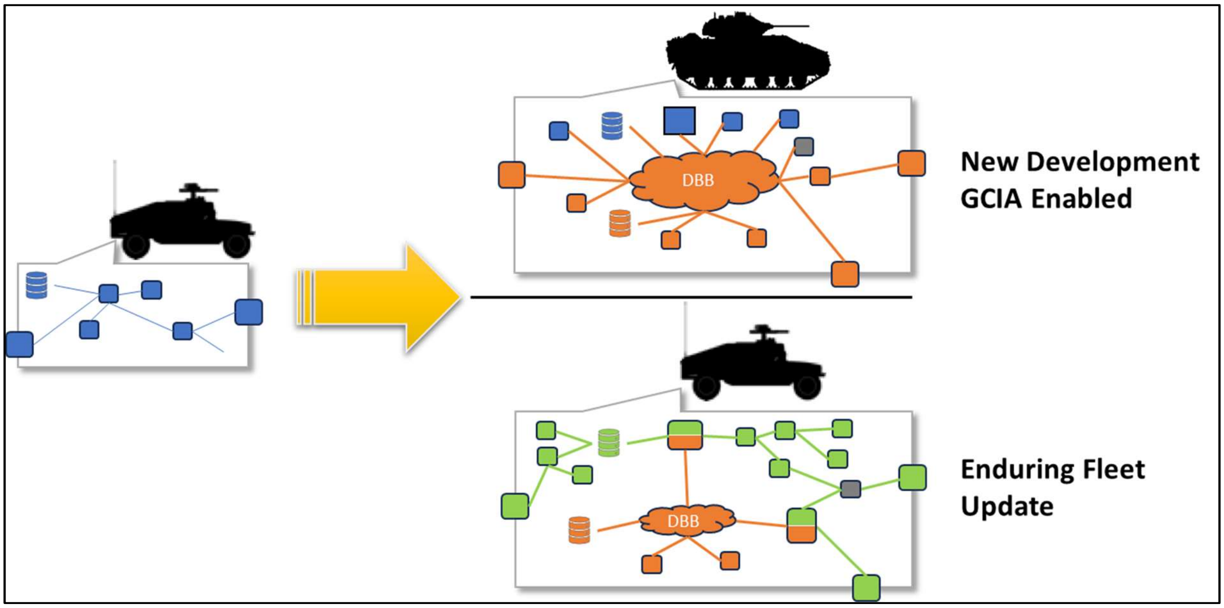

Figure 3: Transition to Common

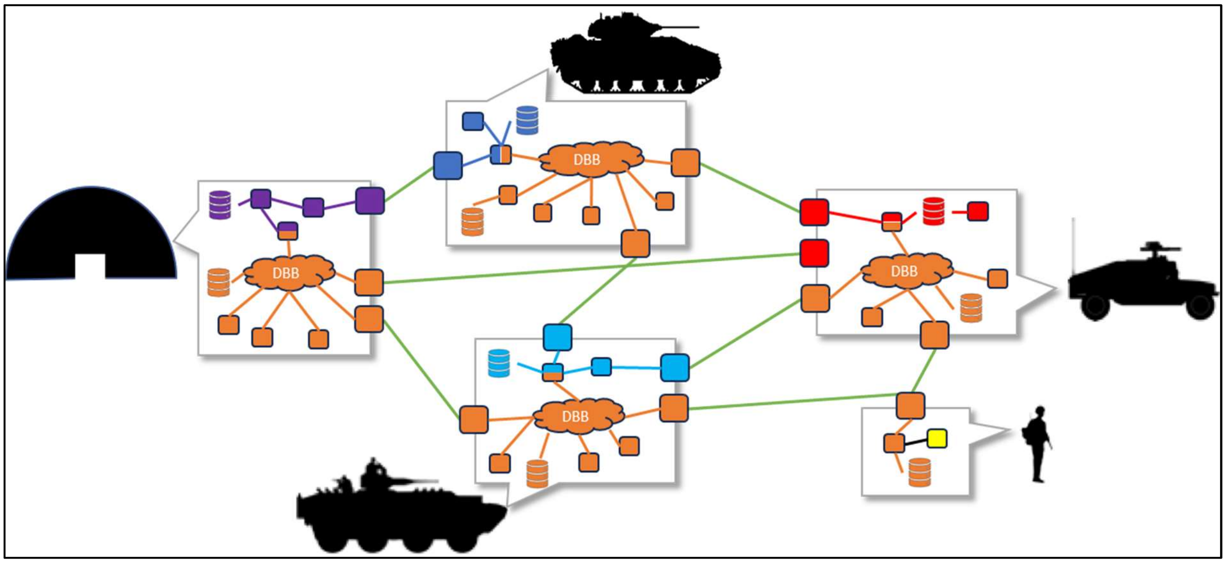

Figure 4: Enterprise Commonality

leveraged to support advanced MDO operations.

Some specific actions that would enable application of these concepts for ground vehicle enterprise systems include:

8.1. Data Synchronization

Modeling interfaces with conformance to the Enterprise DSDM will support automated generation of data transformations enabling reuse of services defined by FAF in ground vehicles. The activity should address both existing weapon system and standards-based interfaces such as VICTORY.

8.2. Data Bus Transformation

Define a Transport Protocol Module and supporting data transformations for VICTORY to support connecting service nodes based on FACE^{TM} with service nodes based on VICTORY. When combined with a transport service implementation which supports data transformation, component integration can be largely automated.

8.3. Identify Required CSMs

Ground vehicle architects can select defined CSMs which are needed to support the enterprise goals. New CSMs may also be defined using established patterns to jump-start component development.

8.4. Apply Digital Backbone

The Digital Backbone description pattern may be specified for vehicle development to ensure required data is available with necessary rights to support full-lifecycle maintenance of enterprise systems. Architects may also consider whether using high bandwidth, low latency deterministic network data link such as TSN or TTE allows reduction in use of legacy networks to meet real-time constraints.

8.5. Implement Services

The SOA can be built/deployed in government system integration labs (SIL). The common service CSMs may be used to realize the next level of decomposition of services identified in GCIA. The common services can be implemented for SIL use and shared with other component developers to help accelerate system development. Service validations may also be developed to test SOA architecture conformance.

8.6. System descriptions

Existing and new systems need to be formally described in terms of their capabilities, interfaces, functions, data, and components. An integrated view of the entire system will provide the visibility into the integration points for introduction of these concepts and components.

9. CONCLUSION

The architectural concepts developed in aviation can support reuse and commonality for ground vehicle enterprise systems.

The FAF and SOA approach can be leveraged to achieve significant enterprise commonality, satisfying GCIA, supporting MOSA objectives, and enabling advanced MDO.

10. REFERENCES

[1]FVL Architecture Framework, 4.3B U.S. ARMY DEVCOM-AVMC, Huntsville, AL, USA 2023

[2] FACE™ Technical Standard, Edition 3.2 The Open Group, [Online] https://publications.opengroup.org/c232

[3] Army Unified Data Reference Architecture, V1.0 Assistant Secretary of the Army for Acquisition, Logistics, and Technology [Online] https://api.army.mil/e2/c/downloads/2024/03/26/4b65a3b3/udra-v1-0-final.pdf