WHITEPAPER

Architecting for Interoperability with MOSA

AUTHORS

Protima Banerjee
Principal Research Engineer, RTI

Joe Schlesselman
Director of Business Development, RTI

Paul Tingey
Regional Field Application Engineer Manager, RTI

OVERVIEW

Architecting systems and system-of-systems while satisfying the combined attributes of performance, scalability and reliability is hard. Adding non-functional requirements of interoperability, flexibility, modularity and portability make the problem even more difficult. So imagine the challenge defense procurement agencies such as the U.S. Department of Defense (DoD) and the UK Ministry of Defence (MoD) have taken on in recent initiatives, whereby they plan to do exactly this – and not for just one procurement requirement, but across all future procurements for systems. Furthermore, this goal is not just for systems of a similar type, but also for different mission-specific systems that need, want and use similar data.

There is a radical shift in defense procurement thinking: instead of the systems integrator, it is now up to the DoD and the MoD to define reusable and rapidly replaceable electronic and software systems to address current needs. By taking architectural ownership of these platforms, they seek to evolve the market toward open market competition for the functional subsystems. They are doing this by defining a fully interoperable, open architecture using a Modular Open Systems Approach (MOSA).

This is not simply the typical "write once, run everywhere" Open Architecture (OA) initiative. MOSA requires that different systems built at different times (potentially with different hardware, different software architectures, different suppliers, as well as different data producers and consumers) must be able to immediately integrate and deploy to different operational environments. Furthermore, system integrators still shoulder integration responsibility in this paradigm, albeit against an architectural specification governed or managed by the DoD or MoD. The primary technical objective that enables this commercial market change is the drive toward rapid deployments, software reuse and interoperability.

The main goals of creating MOSA systems are to reduce system procurement life cycle costs, increase warfighter agility, and decrease the turnaround time of change requests. As outlined in this whitepaper, programs that will reap these rewards through their adoption of MOSA principles include:

- Aircraft avionics using the Future Airborne Capability Environment (FACE™) Technical Standard and Business Approach,
- Open sensor platforms using Sensor Open Systems Architecture (SOSA™) hardware and software solutions,
- Unmanned Control Systems designed around the DoD UCS (UAS Control Segment) common architecture,
- Armored vehicles incorporating a common architecture based on the UK MoD GVA (Generic Vehicle Architecture) or the similar NATO standard referred to as NGVA,
- Unmanned maritime vehicles designed around the UMAA (Unmanned Maritime Autonomy Architecture) standard, and
- Other miscellaneous programs that enforce MOSA principles.

MOSA is the natural progression of introducing open architecture and open business market principles into a defense procurement strategy. It is designed to deliver specific benefits, and interoperability is perhaps the most important one, especially in a data-centric Joint All-Domain Command and Control (JADC2) world. MOSA drives the adoption of open standards, open systems (modularity and scalability) and commercial off-the-shelf (COTS) technologies into an open platform infrastructure that provides immediate and powerful benefits to the DoD, MoD, NATO and other defense organizations.

Term	Technical Definition	Relation to Interoperability & Commercial Context
Replaceability	One thing or person taking the place of another, especially as a substitute or successor.	While a replaceable subsystem is an asset, it does not imply that the replaced system can be enhanced or altered in any way – in fact, it's more likely that it will have to remain identical in functionality.
Interchangeability	To put each of two or more things in the place of the other, or to be used in place of each other.	An improvement on replaceability, because the subsystems are likely to be able to behave differently based on the system the subsystem is placed into. But this system context usually has to be pre-determined and fixed ahead of development time.
Extensibility	The ability to add new components, subsystems, and capabilities to a system.	There is no limit on the domino effect of change requests needed across the rest of the system to integrate the new subsystem. Nor does it imply that the new system can meaningfully exchange information with any subsystem already in the system.
Componentization	A software package, service or a module that encapsulates a set of related functions that communicates via defined interfaces.	A valuable building block in software architectures, but its interfaces are not necessarily openly defined for interoperability – therefore, it can still end up delivering stovepiped systems.
Modularity	Clarifies the functional blocks of a system, separating capability into modules.	Improves maintainability but makes no claims for interoperability, as the interfaces may still be closed and proprietary.
Portability	The ability of something, usually a software application, to be readily moved from one environment to another, usually due to a common platform.	While this aids re-use of the application, it has no association with interoperability of the application with other applications in the environment it has been moved into. It only facilitates integratability with the platform.
Open System	Provides for 'some' level of system capability that exhibits interoperability, portability and use of open standards.	There is no standard to which the level of openness is defined, nor to what interoperability relates.

WHAT IS INTEROPERABILITY?

Interoperability has become a loaded term in the defense industry. Counteracting this confusion is best achieved by defining the terms that are often used interchangeably with interoperability when they should not be. Also, given that these terms are often used to imply commercial benefits through the adoption of technical functionality, we should clarify what commercial benefits could be attributed to a system architected with a particular technical attribute. The previous table pulls together definitions from many sources.

INTEROPERABILITY AS A KEY SYSTEM-OF-SYSTEMS ATTRIBUTE

Interoperability is being brought to the top line as a deliverable requirement. And to ensure they get it, the DoD and MoD are mandating the architecture of the systems they wish to procure – not just for the next system, but with a common systems architecture across all systems of a similar type (combat vehicles, unmanned control systems, robots, etc.).

By mandating, managing and verifying interoperability, the MoD and DoD seek to more closely align the defense market with the operation of open commercial markets. The most important commercial market benefit sought is open market competition for subsystem supply. The ultimate objective is to provide the warfighter with more capability faster, decreasing the length of time needed to roll out each capability update to stay at the forefront of the technology war. The core tenet of this approach is the development of a common system-of-systems architecture that satisfies the system's non-functional requirements across all platforms. But commonality alone is insufficient; the architecture must facilitate the ability to integrate new and innovative capabilities with older 'common' functionality.

To ensure these benefits are received, the MoD and DoD are mandating an Interoperable OA and MOSA. In fact in 2019, this guidance for service acquisition executives and program executive officers was explicitly referenced in a Tri-Services Memorandum[1] with the subject heading: "MOSAs for our Weapon Systems is a Warfighting Imperative."

WHAT IS MOSA?

Based upon open standards, MOSA delivers interoperability among subsystems and applications built and procured at different times. Open standards allow defense procurement agencies to control the system architecture. Furthermore, these defense agencies have determined that the key to achieving this final critical step is to control the data.

Underpinning a MOSA platform with data creates a need for a data-centric connectivity framework based on an open standard. This open standard must include an open wire protocol for interoperability and rapid integration, as well as integrate an open programming interface for application

portability. However, while this approach provides the basis for an Interoperable OA, it is still insufficient. Communication and connectivity may have been openly standardized, but the meaning of the information flow has not.

Both the DoD with its UCS program and the MoD with its GVA program addressed this issue by defining a System Data Dictionary (SDD) that defines content and context of the data that is shared with all connected devices and systems. The SDD is not a wire protocol, but rather a full specification of the data and its meaning which can then be instantiated appropriately on interoperable and different technologies to exchange information. Included in this SDD is a set of metadata that defines the semantic information associated with every piece of data. This semantic data contextualizes it or allows it to be re-contextualized to the application using it. (see Interoperability section below).

The common approach to achieving this goal is to build an SDD (often referred to as a Data Model), which encapsulates not only the language for speaking between applications and subsystems, but also the semantic meaning of the data. Using air vehicle track data (air vehicle location data) as an example, what is height? Is this a measure from sea level, or just the distance above ground? Is it in kilometers or miles? Is a negative measure valid? More importantly, what is the human context? Who is telling me this? Where did the data originate? How old is it? What happens if I miss an update? Does the first time I see a track have any special meaning? What makes a track stale, and should I care? How fast are the updates? How much of the data update history should be available?

There are many such behaviors that, to date, have been implicitly specified and only partially understood when systems are integrated. Common errors that result are duplicated tracks, incomplete or conflicting data, inefficient use of compute resources, domino-style system integration challenges when integrating additional capability, and no gains in system interoperability.

The data context contributes to the semantic understanding of the data and provides a means to evaluate the veracity and utility of the data. When systems work upon a common semantic data model, rather than a bunch of syntactic messages, they can start to become truly interoperable.

Some open architecture programs have been focused on portability of applications. While they will deliver cost benefits in the first program, they will however also find that application portability is not the same thing as interoperability, particularly once the functionality of one application or subsystem evolves or requirements change, or a new capability is inserted. Introducing different capabilities and features for portability will have a cascading domino effect of costly change requests throughout the larger system, despite being made easy to host and run by the common platform.

Advanced programs have recognized that application portability is a goal, but that system-level interoperability is the higher-order functionality that is needed. Both benefit from using MOSA.

MANAGEMENT OF SYSTEM STATE THROUGH THE DATA

To achieve system-level interoperability, defense procurement personnel are recognizing that the system state needs to be maintained in the architecture infrastructure, and not within applications or in a specific subsystem. In fact, the entire system state has to be made explicit to every connected functional subsystem or application. This decouples not only the communication between subsystems, but also the state information — an approach that prioritizes the push toward data-centric interoperability.

Specifically, a May 2021 Memorandum[2] from the Deputy Secretary of Defense outlines the following five DoD Data Decrees to help accelerate enterprise data:

1. Maximize data sharing and rights for data use: all DoD data is an enterprise resource.

2. Publish data assets in the DoD federated data catalog along with common interface specifications.

3. Use automated data interfaces that are externally accessible and machine-readable; ensure interfaces use industry-standard, non-proprietary, preferably open-source, technologies, protocols, and payloads.

4. Store data in a manner that is platform and environment-agnostic, uncoupled from hardware or software dependencies.

5. Implement industry best practices for secure authentication, access management, encryption, monitoring, and protection of data at rest, in transit, and in use.

If these principles are followed, any subsystem or application can obtain state information from the software infrastructure rather than from another subsystem or application. This approach reduces coupling and removes stovepipes. We see evidence of this in the wide use of databases as a central 'cache' of state. Their use has been very effective in enabling client applications to get, view and manipulate the data and its state, without the need for full system connectivity. However, this implementation approach is really only practical for data-at-rest. For distributed, non-homogeneous real-time systems, a central repository of state information is impractical and introduces a single point of failure. What is needed is a fully distributed, real-time databus that maintains state information for data-in-motion.

A databus is a data-centric software framework for distributing and managing real-time data in intelligent distributed systems. It allows applications and devices to work together as one, integrated system, connecting data within applications as well as across devices, systems and networks. This simplifies application and integration logic with a powerful data-centric paradigm and enables the delivery of large data sets with microsecond performance coupled with quality-of-service (QoS) controls.

INTEROPERABILITY IN MOSA PLATFORMS

To achieve a fully interoperable MOSA environment, you need to achieve three levels of interoperability:

- **Technical Interoperability**: Bits and bytes are exchanged in an unambiguous manner via a set of standardized communication protocols.
- **Syntactic Interoperability**: A common data format is defined for the unambiguous sharing of information.
- **Semantic Interoperability**: The meaning of data is exchanged through a common information model and the meaning of information is unambiguously defined and shared.

Focusing on the data semantics will facilitate the drive towards interoperability. However, even if one enables all these capabilities in a MOSA platform, one still might not achieve interoperability. There is one more key step required – to delegate the syntactic and semantic interoperability to a software infrastructure layer, which can be common across every subsystem. In this way, interoperability can be maintained, like the state, at the system level and not between two or more interoperating applications or subsystems. The means for associating interoperability with data and information flows at the system level is to use a data-centric design approach. This is exactly the approach that the UCS, GVA, UMAA, and other open standards are implementing to drive system-wide interoperability.

IS THE SYSTEM INTEGRATOR READY?

Creating data-centric platforms is a fundamental shift in procurement strategy, and as such will have cultural, organizational and technical implications. But that does not mean the system integrators are unprepared. Many system integrators have been building out their own internal interoperable system-of-systems capabilities for the same commercial reasons that the MoD and DoD now want them. The difference is that the MoD and DoD need that interoperable environment to be open and common across suppliers of all sizes, whereas the supply chain wants it to be closed and proprietary, for obvious commercial 'lock-in' and through-life program revenue reasons.

Now, however, the non-functional system architecture will be reduced as a profit center for the supply chain, although they can compete on the efficacy of their implementations. In that context, the supply chain is not commercially ready. Therefore, the MoD and DoD are stepping forward carefully, because a commercially healthy supply chain is critical to their operational capability. Of course, private companies with no shareholders to report to are potentially able to move very quickly to take advantage of this shift. The DoD in particular is fostering greater involvement from smaller businesses, perhaps as a means to accelerate this commercial market shift.

DRIVERS OF CHANGE

The reason for this change is the economic imperative in combination with the changing warfare environment, spurred on by the more visible rate-of-change gap in technology supply between defense equipment and commercial offerings. Smartphones are a prime example: a few years ago, our phones struggled to do much more than text and dial, but now they are fully-fledged computers capable of receiving video, tracking location and orientation, and even measuring our heartbeat. The open application platform has enabled rapid accessibility of this change in compute capability. And in asymmetric warfare, the enemy is using this device quite effectively.

Contrast this with change requests that take years to bubble up to requirements, express to defense procurement, and eventually deliver by industry. But the real driver comes from the warfighter: The one flying an F16 with an iPad on their lap or sitting in a Humvee surrounded by 4 or 5 screens when one would be enough (both true feedback from the field.) That difference is felt in two ways:

1. The individual warfighters' technology expectations, in terms of capability and ease-of-upgrade, is being set by the commercial market rather than the defense industry itself.
2. The enemy is able to access sophisticated technology for less money, and those without defense industries to support them are making effective use of advanced commercial technology and access to information.

The software connectivity foundation and data modeling technologies are ready. The open-standards supply chain is ready, while the defense supply chain is up to speed with the technology and is already leveraging it. The only difference going forward will be how integration will be managed – data-centric MOSA strategies introduce a shift from the current vertical integration strategy to a horizontal one. Everyone has fully open access to the infrastructure. In fact, the infrastructure could, and perhaps should, be acquired independently from the system functional components.

The warfighter stands to gain by receiving more frequent upgrades and new technology insertions in a more agile fashion and at a pace closer to the commercial world, albeit within systems that have to be managed for 20-30 years in deployment.

The central commercial tenet that will deliver new efficiencies is competition enabled by DoD- and MoD-mandated systems interoperability.

MANDATING THE INTEGRATION STRATEGY IS CRITICAL

The lesson learned by defense procurement using OA over the last 20 years or so is that the benefits that should accrue to OA don't happen unless defense procurement also mandates the integration strategy. The traditional ICD/IDD (Interface Control Document/Interface Description Document) have been shown to be insufficient, as they only enable syntactic interoperability. The MoD and DoD are starting to define an Interoperable OA, and with that they are taking ownership of those parts of the integration strategy that are necessary to ensure the delivery of interoperable system-of-systems.

But surely this is stepping onto the suppliers' traditional turf? While true, the more forward-looking system integrators are recognizing the economic imperative and are embracing the change. Indeed, GVA would not exist today as Def Stan 23-09 unless industry had worked extremely closely with defense procurement to define the line to be drawn between the architecture and integration strategy defined by MoD versus the functional subsystems delivered by industry. Similarly, UCS has been developed with the coordination, cooperation and support of industry.

The integration strategy has to encompass:

- Modularization of subsystems
- Simple update/replacement over time of subsystems
- Innovation within a subsystem
- Insertion of innovative new subsystems
- No 'stovepipe' connectivity between any two subsystems
- The ability to 'wrap' and integrate legacy subsystems not originally built to the new Open Architecture

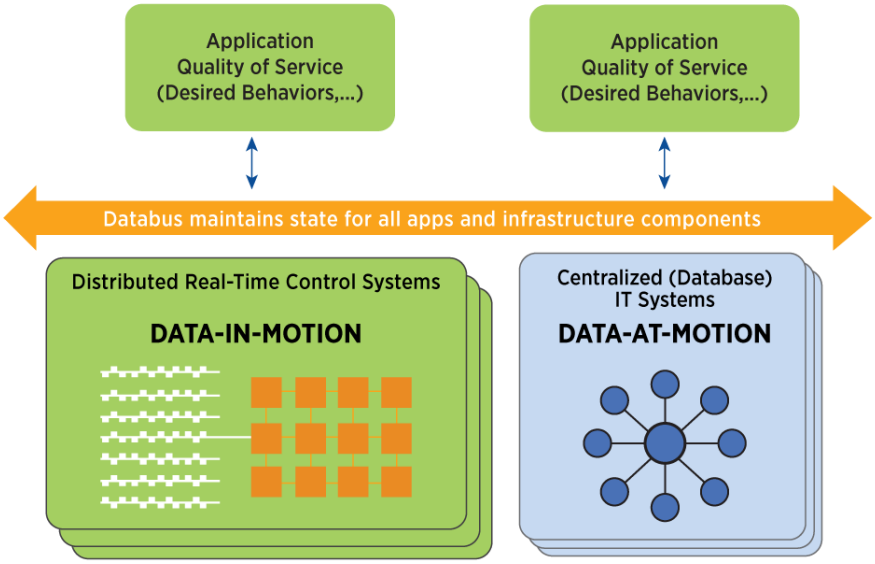

Figure 1: Decoupling system state from application and infrastructure components is critical for removing stovepipes

SELECTING THE APPROPRIATE DATA-CENTRIC CONNECTIVITY FRAMEWORK

Unfortunately, simply creating the SDD is insufficient for guaranteeing integration within an open architecture. The means to 'speak' the language has to be fully compliant with all the tenets of open architecture. The communication mechanism and state maintainer selected and mandated under GVA is the Data Distribution Service (DDS™) standard, which delivers proven vendor interoperability and for which vendor interoperability is maintained and managed by the Object Management Group® (OMG®). Under UCS, much of the test and SDD validation work was built on DDS. However, UCS does not mandate an implementation technology, as this is left for the program offices using the UCS architecture to define. This is partially because as an umbrella architecture that is, uniquely, being applied across services (Army, Navy, Air Force), it is beyond the remit of the UCS program to define the implementation approach within any one service.

It is normal for systems engineers to make design decisions that trade scalability, performance and reliability. But this is unacceptable in today's defense market — the battlefield scales in an undefined manner and performance saves lives, while unreliability costs lives. In data-centric MOSA systems, it should be possible for any system or subsystem to fail without bringing down the wider system around it. Well-architected implementations of middleware have been built with a guarantee of no single point of failure. Unlike inherently client-server based architectures, wherein a server dies and all its clients die or suffer reduced capability, a true peer-to-peer implementation of the middleware does not suffer this problem.

The middleware must also inherently support the ability to sustain a data-centric system-of-systems state on the databus; effectively, within the dataset on the move between systems at any point in time. Only one open standards-based middleware potentially delivers all these attributes, and that is DDS.

Scalability is primarily achieved by DDS's inherent decoupling of one system from another, combined with its systems communication and application-oriented QoS capabilities. Each system only talks to the system-wide databus. It either places data (from the SDD, including the semantic context) onto the databus or pulls it off. Systems talk directly to other systems as defined by their data needs. DDS manages the data-in-motion, thereby maintaining a record of the system-of-systems state and semantic interoperability.

Despite these inherent core characteristics of scalability and reliability, DDS does not sacrifice performance to achieve them. Built on DDS, RTI Connext® has consistently shown an ability to out-perform other large scale system-of-systems communications open standards middleware, whether it's across HF radios, Ethernet, satellite or a proprietary connection type.

Lastly, and perhaps most importantly, the OMG manages a process of vendor integration validation, with closely-managed control of both the API for portability and the wire protocol for integratability and interoperability. Therefore, any subsystem developer can select any DDS supplier based upon their commercial and technical needs. While DDS is standardized, the implementations are not — nor are the business terms defined. So the MoD and DoD can safely mandate DDS, secure in the knowledge that they are not undermining their own key objective of building competitiveness into their supply chain.

SUMMARY

The economic imperative is driving procurement and system integration innovation in the same way that wars tend to drive technology innovation. However, technology has advanced sufficiently to create the foundations of a fundamentally new procurement strategy. MOSA and data-centric connectivity frameworks meet the demands of the warfighter for faster and more powerful systems, while reducing costs. This approach enhances the pace of life cycle upgrades and reduces costs for logistical support.

REFERENCES

[1] Memorandum for Service Acquisition Executives and Program Executive Officers (January, 2019)

[2] Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoD Field Activity Directors (May, 2021)

ABOUT RTI

Real-Time Innovations (RTI) is the largest software framework company for autonomous systems. RTI Connext® is the world's leading architecture for developing intelligent distributed systems. Uniquely, Connext shares data directly, connecting AI algorithms to real-time networks of devices to build autonomous systems.

RTI is the best in the world at ensuring our customers' success in deploying production systems. With over 2,000 designs, RTI software runs over 250 autonomous vehicle programs, controls the largest power plants in North America, coordinates combat management on U.S. Navy ships, drives a new generation of medical robotics, enables flying cars, and provides 24/7 intelligence for hospital and emergency medicine. RTI runs a smarter world.

RTI is the leading vendor of products compliant with the Object Management Group® (OMG®) Data Distribution Service (DDS™) standard. RTI is privately held and headquartered in Sunnyvale, California with regional offices in Colorado, Spain and Singapore.

Download a free 30-day trial of the latest, fully-functional Connext software today: www.rti.com/downloads.

RTI, Real-Time Innovations and the phrase "Your systems. Working as one," are registered trademarks or trademarks of Real-Time Innovations, Inc.
All other trademarks used in this document are the property of their respective owners. ©2023 RTI. All rights reserved. 50055 V1 1123

Your systems. Working as one.

CORPORATE HEADQUARTERS
232 E. Java Drive, Sunnyvale, CA 94089
Telephone: +1 (408) 990-7400
Fax: +1 (408) 990-7402
info@rti.com

rti.com
company/rti
rti_software
connextpodcast
rtisoftware
rti_software