A Comparison of Avionics Open System Architectures

Joyce L Tokar, PhD
Pyrrhus Software, LCC
PO Box 1352
Phoenix, AZ 85001-1352
+1-480-951-1019
tokar@pyrrhusoft.com

ABSTRACT

Building high-integrity, safety-critical systems is one of the primary activities of the projects within the United States (US) Department of Defense (DoD). Recognizing the need for affordable and effective solutions, the DoD calls for the use of Open System Architecture (OSA) solutions in Better Buying Power (BBP) 3.0 [1], Department of Defense Instruction 5000.02 [2], and the Defense Acquisition Guidebook section 4.3.18.15 [3]. The objectives of these documents are to avoid vendor lock, enable affordable capability evolution, and promote innovation. There are several activities underway to define standards that support the development of these systems.

In the Unmanned Aerial Systems (UAS), the Unmanned Aerospace Systems (UAS) Command and Control (C2) Standard Initiative (UCI) standard has been defined to address the needs of providing an open architecture specification for unmanned aerial vehicles [4].

The Open Mission Systems (OMS) standard [5] developed by the US Air Force utilizes commercially developed Service Oriented Architecture (SOA) concepts and middleware in its definition along with the UCI standard. The Air Force is looking to extend the capabilities of the OMS standard to facilitate the rapid evolution of avionics systems.

The Open Group has constructed a consortium of government, industry, and academia experts to develop the Future Airborne Capability Environment (FACE™) [6]. FACE is an open architecture effort that is intended to standardize the development of aviation components.

The paper will present the basic definition of open systems architecture followed by a description of three of the OSA standard activities that are being conducted to address the direction from the DoD. The paper will then examine the similarities and differences between each of these initiatives. Finally, the paper will discuss the usability of OSA.

CCS Concepts

- Computer systems organization → Architectures → Other architectures
- Computer systems organization → Embedded Systems
- Computer systems organization → Real-time systems → Real-time system architecture

Keywords

Open System Architecture; OSA; Future Airborne Capability Environment, FACE™, Open Mission Systems, OMS, Unmanned Aerospace Systems, UAS, UAS Command and Control (C2) Standard, UCI

1. INTRODUCTION

At an open architecture summit November 2014, Katrina G. McFarland, then assistant secretary of defense for acquisition, said “This department is seriously engaged in trying to understand how to help our program managers and our department and our industry look at open architecture and its benefits and understand truly what our objectives are related to intellectual property and making sure that we’re doing it based on the best interest of national security relative to a business case.” [5] Recognizing the need for affordable and effective solutions, the DoD calls for the use of Open System Architecture (OSA) solutions in Better Buying Power (BBP) 3.0 [1], Department of Defense Instruction 5000.02 [2], and the Defense Acquisition Guidebook section 4.3.18.15 [3]. The objectives of these documents are to avoid vendor lock, enable affordable capability evolution, and promote innovation.

Building high-integrity, safety-critical systems are one of the primary activities of the projects within the United States (US) Department of Defense (DoD). With the guidance and direction from the DoD to utilize Open Systems Architecture (OSA) as the basis of designing systems that are modular a number of initiatives are underway to define standards that support the development of these systems.

2. OPEN SYSTEMS ARCHITECTURE (OSA)

As a starting point, an *architecture* is a set of components, connections, and rules that are used to develop systems from those components and connections. An *open systems architecture (OSA)* specifies required interfaces and presumes separation between applications and infrastructures governed by those interfaces. OSA also provides rule for constructing systems. An OSA is a contract between several groups of people. Most obviously, it is an agreement between the implementer of the standard and the organizations who use the standard, e.g., between the system software developer and the applications programmers. It is also a contract between the standards developer community and the users of the standard, and between the standards developer community and the acquisition community who specify the use of a set of standards on systems they pay for.

An *open standard* is a publically available standard, designed and developed with adherence to the key characteristics of due process, consensus, transparency, and balance. An *open architecture* is a type of computer or software architecture designed using open standards with the objectives to ease the effort associated with adding, modifying, removing, and interchanging components.

An open systems architecture is both a business and a technical strategy for developing a new system or modernizing an existing one. An open architecture is often a key component of the technical strategy of open systems architecture.

An OSA is more than a simple set of standards or a combination of business strategy and technical architecture. Key to its effectiveness are the rules by which the standards work together, and by which applications are integrated to make operational systems. These rules can constrain the choices by application developers, for instance by requiring that an option in one constituent standard be provided, or by directing that application not to use an interface in one standard (perhaps because the same functionality is provided by an alternative standard). In addition to Application Program Interfaces (APIs), many OSA include data standards, both data models and data representation standards.

Quality attributes for an OSA include, but are not limited to the following:

- Is each constituent standard/interface clearly identified (e.g., identification including version/release)?
- Are the standards/interfaces appropriate to the domain of the OSA?
- Does the OSA address the potential interactions of the constituent standards/components, including optional features and implementation freedoms? (It would be A Bad Thing if an option in one standard in the OSA caused another standard to not work.)
- Are the rules for configuring the OSA infrastructure, and for the applications/systems built on the OSA, clearly specified?
- Does the OSA provide support for testing and debugging systems built on top of it?
- Does the OSA provide conformance rules for both implementations of its infrastructure, and for what applications may and must do?
- Does the OSA provide language for how it is to be included in technical specifications and procurement documents?
- Are there multiple implementations of the OSA infrastructure?
- Is the entire OSA available from a vendor, or must the system integrator construct and verify it?
- If the system integrator assembles the OSA from different vendors, is there a means for vendors to understand and implement the OSA's requirements and rules? (e.g., a consortium or implementor's forum?)
- Is the vendor community committed to coordinating constituent updates to ensure that one vendor's update doesn't break the entire OSA infrastructure?

There are several efforts underway within the DoD to develop open systems architecture standards to address the direction specified in BBP 3.0 and other government directives. The Unmanned Aerial Systems (UAS), the Unmanned Aerospace Systems (UAS) Command and Control (C2) Standard Initiative (UCI) Standard, the Open Mission Systems (OMS) standard developed by the US Air Force, and Open Group's Future Airborne Capability Environment (FACE™) are three of examples of this work that will be examined further in this paper.

2.1 Unmanned Aerial Systems (UAS), the Unmanned Aerospace Systems (UAS) Command and Control (C2) Initiative (UCI)

The US Air Force initiated the UCI Program to establish a set of messages for machine-to-machine, mission-level command and control for airborne systems. The UCI vision is to decrease acquisition and operational costs of manned and unmanned air systems and enable interoperability by:

- Providing a standard message set for machine-to-machine communication.
- Providing an open standard to allow easy integration of new services and reuse of services between programs.

This effort started with the successful work that was done with establishing NATO Standardization Agreement 4586 (STANAG 4586) [7] as the standard definition of the interface between the ground control system and an unmanned control system (UCS) in an unmanned aerial vehicle (UAV). STANAG 4586 includes the specification of the data link, command and control, and human/computer interfaces.

During the last years, Unmanned Aircraft Vehicles (UAV) became a niche in continuous expansion within the aerospace market. With an investment that may exceed billions of dollars by 2015, it is predictable that the next generation will possess even more capabilities than today's [8]. As such, more emphasis has been put on developing an architecture that will support the development a service oriented architecture for unmanned aerospace systems command and control.

As with a large part of the existing military systems, legacy UAV systems have been designed and procured as non-interoperable "stovepipe" systems. The objective of STANAG 4586 was to begin to break down the barrier to interoperability by establishing a standard set of interfaces in the UCS to communicate with different UAVs and their payloads using a standard message set.

The UCI is taking the objective for interoperability a step further by defining a reference architecture for UAV C2 systems which incorporates the work done in developing STANAG 4586. This is a work in progress guided by the US Air Force with participants from the government and industry.

2.2 Open Mission Systems (OMS)

The US Air Force initiated the Open Mission Systems (OMS) effort with the objective of developing a non-proprietary open system architecture to drive acquisition and business models away from legacy stove-piped solutions. In addition, In accordance with BBP 3.0 and other government guidance, the OMS effort is working to influence and incentivize industry toward a capability based business model which will enhance competition and encourage rapid innovation. The OMS project is composed of members from the government, industry and academia who are working together to develop and sustain consensus for a non-proprietary architectural standard for mission systems. OMS is actively coordinating the development of the emerging OMS Standard with multiple airborne platform and sensor acquisition programs as well as the Unmanned Aircraft System (UAS) Command and Control Initiative (UCI) and the Common Mission Control Center (CMCC) program.

The objective of OMS, as well as other OSA efforts, is to identify new acquisition and architecture approaches to reduce development and life-cycle costs, while at the same time providing a viable path to upgrade and expand system capabilities. The Open Mission Systems (OMS) standard [5] developed by the US Air Force utilizes commercially developed Service Oriented Architecture (SOA) concepts and middleware in its definition. The Air Force is looking to extend the capabilities of the OMS standard to facilitate the rapid evolution of avionics systems.

The OMS Reference Architecture establishes the fundamental service-oriented design patterns and principles as well as key interfaces and modules (Figure 1). The functionality of avionics systems is characterized as a set of services and a set of clients. In some instances, a program or system may be both a client and a service. The OMS standard defines the basic behavior of clients and services as well as the Avionics Service Bus (ASB) protocols for entering and exiting the system, supporting testing, fault tolerance, isolation, and authentication.

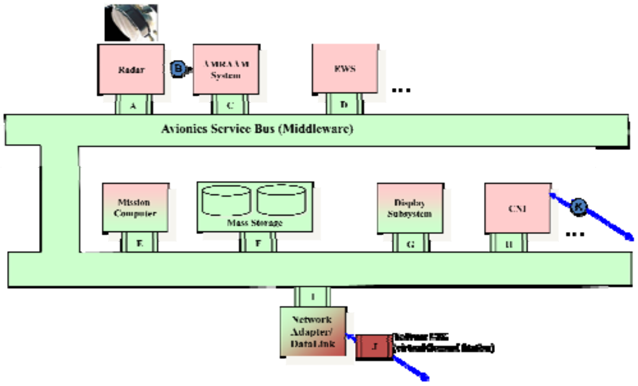

Figure 1 OMS Reference Architecture

The OMS effort specifies the test bed environment required to support the migration and development of OMS compliant systems. The OMS Standard also defines the compliance methodology and artifacts that are needed to demonstrate that a service or client is compliant with the standard.

The Air Force is pursuing the definition of the OMS Standard to improve system (of systems) capabilities in a cost effective and rapid manner. Open avionics systems are crucial to enabling the competitive, cost effective, and timely introduction of new war-fighting capabilities in platforms that will persist for decades. Service oriented concepts judiciously combined with embedded open system techniques will deliver the next generation of open avionics technologies and architectures. Open architecture test beds based on executable specifications will accelerate integration and provide the mechanism to compete new avionics technologies.

2.3 Future Airborne Capability Environment (FACE™)

The Open Group has constructed a consortium of government, industry, and academic experts to develop the Future Airborne Capability Environment (FACE™). FACE is an open architecture composed of a technical standard and a business strategy.

The FACE Technical Standard is an open avionics standard of standards developed to facilitate robust, interoperable, portable and secure avionics capabilities. The FACE Business Strategy is designed to aid in the acquisition of affordable software systems. Together these components fulfill the BBP Modular Open Systems Architecture (MOSA) goal to provide a standard mechanism to stimulate innovation in the development of components, subsystems or programs that maintain secure technical control and ownership of all the needed interfaces, including those required for software integration.

The FACE Technical Standard was motivated by the advances in mobile devices through the use of a Common Operating Environment (COE). In the commercial market, the architectural stack of the mobile device is composed of a collection of applications that access the operating system through a well defined interface. And the operating system accesses the hardware through a well defined interface. The variability in these systems comes in operating systems and the hardware, but the interfaces between these components does not change significantly (Figure 1).

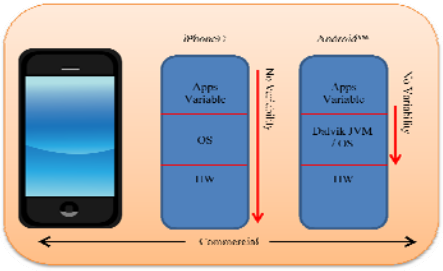

Figure 1 Mobile Computing COE

Presently, the military has considerably more variability in most aspects of the programs and systems. The objective of FACE is to provide the standards, framework, and interface definitions to enable the military to migrate to a similar COE structure while maintaining the variability at all levels to support military Avionics missions (Figure 2). This Avionics COE will reduce life cycle costs as well as the time required to integrate, test, and field new capabilities. The business strategy of FACE focuses on the conformance to the FACE standard to maximize interoperability between applications within the avionics systems.

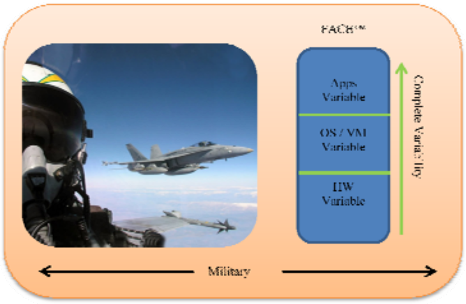

Figure 2 Military Avionics COE

The FACE strategy is to create a software environment on the installed computing hardware that enables FACE applications to be deployed on different platforms with minimal to no impact to the FACE application. The FACE architecture is composed of a set of segments where variance many occur. The FACE standard defines the horizontal (between FACE stacks) and vertical (FACE stack) interfaces. This architecture supports the development of portable applications to improve competition throughout the supply chain.

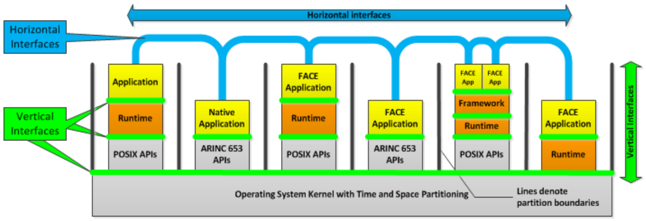

Figure 3 FACE Architecture

The segmentation of the architecture eases the impact of change by localizing the level at which change occurs. In addition, this

OSA reduces the integration costs associated with adding new capabilities. Uniform application of common open standards across DoD aviation will help to eliminate dependence on proprietary solutions.

To address the safety and security requirements of different domains of interest in FACE, the FACE Operating System Segment defines a general purpose profile, a safety profile, and a security profile. The profiles specify what resources are available based on the operational requirements.

3. COMMONALITY AND DIFFERENCES

All of the open architectures described in section 2 are collaborative efforts between industry, the government, and the user community. Yet, the approach of each is slightly different.

The UAV UCI program represents an evolution from the existing stovepipe systems toward an OSA. It is a work in progress and is working toward providing a standard systems oriented architecture for UCS UAV Control Segment. It includes the definition of the interfaces, messages, services, and clients that are applicable to supporting the C2 mission. From an OSA perspective, the UAV UCI is a partial success in that there is a large amount of programs internationally that are adopting the message set and the concept. But is not clear how far the migration has gone toward offering a full OSA with rules for interoperability, standard compliance verification, and openness to the community at large.

The OMS architecture is focused on the use of a bus abstraction to support the integration of modules into a military system through the use of the Abstract Data Bus and, if necessary, the standardized set of discrete signals. It also recognizes the need for the integration of legacy components and recommends the use of wrapper technology to achieve this migration. The standard includes some definition of compliance and utilizes existing standards such as UCI. It falls short in its definition of a data architecture. And, like UCI, it is a somewhat closed environment when it comes to accessibility from the community at large.

The FACE work is being conducted through The Open Group and uses their rules and guidelines to promote the standard development and generate consensus. The FACE consortium is working to define the business strategy, compliance process, certification process and the reusability process along with the technical architecture and the data model as part of the overall standard effort. FACE utilizes many existing standards to support the overall standard definition process.

Each of the OSA efforts described addresses the needs of a specific community. While FACE meets many of the OSA quality attributes identified early, its size and scope may be too large for some communities. The success of the UCI work in the UAV domain may help to promote this effort despite its limited domain. OMS shows is aligning with some of the quality attributes by providing an OSA targeted to the air vehicle domain.

4. USABILITY OF OSA

The key concept is 'conformance to the standard,' and the language used in the POSIX standards [9] works well to capture these concepts. Vendors provide a 'conforming implementation' when they implement all required parts of the standard. (Some vendors have claimed 'we comply with this standard' when they implement a subset of the features of POSIX; the term 'compliance' has no formal definition and means whatever the vendor wants it to mean.) The applications developer produces 'conforming applications' by using only the features of the standard, and adapting to any customizations permitted by the standard. The UAV community has had a large degree of success in moving to STANAG 4856. The next phase of the migration to an OSA is a work in progress.

Determining a 'conforming implementation', i.e., buying a system that meets the requirements of the standard, usually requires a combination of testing and of vendor documentation. Determining a 'conforming application' is a harder task, because testing does not necessarily reveal if the application uses only the facilities of the standard. An implementation may well provide extensions to the standard, including behavior within the standard interface that does things not guaranteed by the standard. As part of the Business Strategy of FACE, the Conformance Subcommittee has developed the FACE Conformance process. And the FACE Technical Committee has defined a Conformance Verification Matrix (CVM) which identifies the specific requirements, methods of verification, and associated verification evidence. OMS defines a Compliance Verification Cross Reference Matrix (VCRM) which contains all of the OMS requirements and the associated verification requirements and acceptance criteria.

A standard supports its user community when the specification is sufficient to meet the user needs, complete with respect to all parameter values, behaviors, etc., and has a well-defined conformance approach. For FACE, the FACE Trademark Licensor issues the FACE Conformance Certification Trademark for Certified Units of Conformance and Certified Unit of Conformance Packages thus allowing a third party to easily determine if a component is FACE conformant.

The real test of all of these OSA efforts will occur when multiple suppliers offer similar capabilities and these modules can be easily integrated into their target systems.

5. SUMMARY AND CONCLUSIONS

OSA systems have a large amount of appeal because of their potential to lower program costs, increase access to COTS, and ease integration. OSA programs also enable interconnectivity.

With the greater connectivity comes the potential for more vulnerability as it may provide greater access for cyber intruders. This accessibility has prompted concerns that OSA systems are more vulnerable to attack. More research is needed to demonstrate how open systems can facilitate more secure systems through the use of strict interface definition and control.

Currently, FACE has a lot of momentum in the Airborne Systems communities especially within the Navy and Army. There have been a number of demonstrations of FACE presented at FACE Technical Interchange Meeting (TIM) in January 2016 [].

OMS is in use in the Air Force and Unmanned Air UCI/STANAG 4586 has focused on the definition of the interface and message set between control stations and unmanned air vehicles. Blue Guardian has developed a platform architecture using the Air Force's OMS reference architecture and conducted a ground and flight test program of multiple payload combinations [10].

There is more opportunity to expand the use of OSA standards such as FACE and OMS for sensors system and subsystems, weapon systems, and network platform interfaces. There is a need for more development of the safety critical and high integrity aspects of these standards as well.

There is significant opportunity for better tool support for component integration and analysis as well as transitioning the use of the OSA standards into industry.

6. REFERENCES

[1] Under Secretary of Defense, Implementation Directive for Better Buying Power 3.0 – Achieving Dominant Capabilities through Technical Excellence and Innovation, 9 Apr 2015.

[2] Department of Defense, Instruction Number 5000.02, 7 Jan 2015.

[3] Defense Acquisition Guidebook, 2015.

[4] Unmanned Aerospace Systems C2 Standards Initiative (UCI) http://ucistandard.org/about-uci.html.

[5] Open Mission Systems (OMS) Initiative, http://ucistandard.org/oms.html.

[6] Technical Standard for Future Airborne Capability Environment (FACE™), Edition 2.1, 2014, https://www2.opengroup.org/ogsys/catalog/G162.

[7] STANAG 4856, Standard Interfaces of UAV Control Systems (UCS) for NATO UAV Interoperability, NATO Standardization Agency, 2012, nso.nato.int/nso/zPublic/stanags/current/4586eed03.pdf.

[8] Marques, Mário Monteiro, "STANAG 4586 – Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability," 2012.

[9] POSIX IEEE Standards

[10] Barrett, Donald A, Luke A Borntrager, David M Green, "Blue Guardian: on open architecture for rapid ISR demonstration," Proceedings of SPIE 9849, Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2016, May 2016.

[11] Fisherkeller, Kerry, "Emerging Interoperability Standards for Unmanned Aerial Systems," 19th Annual INCOSE Region II Fall Mini-Conference, Nov 2014.