Advances in Applying a Model-based Modular Open Systems Approach (MMOSA) to Hardware and Software Verification and Conformance

SOSA™ Technical Interchange meeting (TIM)
Paper by:

TES-SAVi, a subsidiary of

Tucson Embedded Systems, Inc., SOSA Members since 2016 and FACE Members since 2010

Sean P. Mulholland and Ken Erickson

September 2020

Table of Contents

Executive Summary

The promise of emerging open standards, Sensor Open Systems Architecture™ (SOSA), Hardware Open Systems Technologies (HOST), C4ISR/EW Modular Open Suite of Standards (CMOSS), and the Future Airborne Capability Environment™ (FACE) are being leveraged for Modular Open Systems Approach (MOSA) system development. These "best-of-breed" technologies are being used to design, build, upgrade and deploy systems to our warfighters that are more complex and more capable with higher technology readiness levels, lower cost and reduced development and integration schedules. Adoption of open systems has been slow due to fears of delay in schedule and increases to cost in the development phase. Modern methods like MMOSA can mitigate those risks creating an environment for higher order application of open systems in new and upgraded platforms.

This paper presents TES' advances in utilizing Model-based Modular Open Systems Approach (MMOSA) in meeting the need to verify systems against the open standards they are built upon in order to achieve the high goals espoused by MOSA. TES' AWESUM® processes and tool suite enable the rapid development of hardware and software solutions for multi-organization development and integration to build complex cyber-physical systems (CPS) by creating flexible verification systems that can align with the operating environment and speed the process through test, verification and conformance.

Introduction

New and emerging standards promise to enable Modular Open Systems Approach (MOSA) system development. Some of the more important standards to MOSA are Sensor Open Systems Architecture™ (SOSA), Hardware Open Systems Technologies (HOST), C4ISR/EW Modular Open Suite of Standards (CMOSS) and the Future Airborne Capability Environment™ (FACE). These technologies hold the promise that "best-of-breed" technologies and can be utilized to build, upgrade and deploy systems to our warfighters that are more complex and more capable with lower-cost and reduced development and integration schedules. Key to interoperability of systems built utilizing these open standards is verification and conformance of the resulting systems and subsystems. Without formal verification of adherence to the open standards, it has been our experience that the resulting systems and subsystems are unlikely to be interoperable.

Formal verification is very important, but also is very difficult. We do not have to look far to see the difficulties in achieving conformance to open standards such as Unix and POSIX conformance. However, we also see many successes such as Ethernet (802.3.x), Universal Serial Bus (USB), and HDMI to name a few.

Therefore the tools and processes used for verification are key because they provide the criteria and processes necessary to assure hardware and software is developed in accordance with appropriate open standards and is much more likely to be interoperable. In addition, once conformance verification is complete, suppliers can substantiate claims of conformance to open standards and increase buyer confidence to specify and procure hardware and software that conforms to those standards.

There are several challenges to achieving verification and conformance of both hardware and software. Below we present these challenges and approaches to mitigate and remedy those challenges moving towards realizing the promise of "best-of-breed" MOSA systems.

Modular Open Systems Approach (MOSA)

The Modular Open Systems Approach (MOSA) is a strategy for the assessment and implementation of complex systems that is designed to manage the business and technical efforts that are an integral part of system development. Key to MOSA is the utilization of open standards and primarily focuses on modularity of design, identifying key interfaces, and ensuring conformance of the resultant system to standards, openness, and conformance to the open standards. Four of the open standards we will address are SOSA, HOST, CMOSS and FACE.

SOSA Technical Standard

The SOSA Technical Standard "defines a system, software, hardware and electrical/mechanical architecture that supports real-time, mission, and system-critical solutions. The SOSA Technical Standard will leverage industry standard Application Programming Interfaces (APIs) for software, common hardware pinout, and profile specifications based on VITA™, and electrical mechanical specifications based on AS6129/6"[1]. SOSA should include the tools for near term design, to an environment that will migrate quickly based on requirements and be evaluated on a flexible verification and conformance capability that will be able to work within the requirements at the time of design and the future system requirements.

Advances in Applying a MMOSA to HW and SW Verification and Conformance

HOST

The HOST standard consists of a three level open architecture framework developed and maintained by the government that supports the Modular Open Systems Approach (MOSA). It is readily available from the HOST website https://host-oa.com/host-documents/. At its top level, Tier 1, it describes basic tenets of the HOST framework, the next level, Tier 2, adds additional specificity to existing industry standards for a specific technology (e.g. 3U and 6U OpenVPX modules defined by VITA 65), and at its lowest level, Tier 3, allows modules to be specified for a particular instantiation. Thus, HOST helps to standardize the implementation of Commercial-Off-the-Shelf (COTS) components for U.S. Defense Platforms by enabling the development of interoperable, modular and upgradeable systems that leverage open standards across product families to improve defense acquisition. HOST thus supports application of MOSA for increasing the portability of different vendors computing Modules across Hardware Chassis to enable the upgradeability of I/O, processor, storage, and graphics modules.

CMOSS

C4ISR/EW Modular Open Suite of Standards (CMOSS) is an aggregate architecture and associated open standards that enables rapid insertion of planned and unplanned capabilities, along with hardware sharing and interoperability across C4ISR/EW systems. CMOSS is a layered approach which includes specifications that are individually useful and can be combined to form a holistic converged architecture. These layered standards include: Software Layer, Functional Decomposition, Hardware Layer and Network Layer.

FACE™ Technical Standard

The FACE Technical Standard focuses on software development with the goals of greatly simplifying the portability, modularity, and interoperability of software components that are conformant to the FACE Technical Standard. It achieves this by defining Application Programming Interfaces (APIs) for Operating Systems services - OSS, Input/Output services - IOS, Life Cycle services, Data and Control Transport services - Transport Services Segment (TSS) for interprocess communication, a Data Architecture for data definition, configuration, graphics, and other support services.

The MOSA Promise

The real promise of the MOSA is that systems that employ this approach will be interoperable at the varied levels of systems, hardware modules, and software components. Including legacy systems through a modeling language that encompasses historic architectures and newly integrated systems for modernization of the Defense Enterprise needs. While open standards assist in the promise of interoperability at these various levels, it is important to note, they do not guarantee interoperability.[2] Key to interoperability of systems built using these open standards are the processes and tools utilized for design, verification and conformance validation that assure that hardware and software are developed in accordance with open standards. Once conformance is proven, suppliers can substantiate claims of conformance to open standards which allows buyers to specify and procure hardware and integrated software that conforms to those standards and is more likely interoperable.

Some of the challenges that arise when attempting verification and conformance to open standards:

- Ambiguous requirements in open standards
- The difficulty of requirements traceability and coverage analysis to open standards

- Large number of possible test configurations for hardware and software such as the different chassis form factors, optional requirements, etc.
- Lack of comprehensive verification and conformance environments for open standards
- Custom program needs that may conflict with technical standards
- Lack of, or ease of access to tests, test data and conformance results
- Various and incompatible tools used by organizations
- Mismatch of tools to standards (e.g. lag in tool availability to release of standards)
- Different editions/versions of standards adherence

These challenges can be grouped and addressed collectively with a holistic approach to verification and conformance testing that supports MOSA. The primary groupings of challenges we have identified in implementing MOSA verification and conformance approaches are:

- Ambiguous requirements
- Traceability and coverage issues
- Verification and conformance tool-chain differences and incompatibilities
- Conflicting requirements of different components such as different optional requirements and versions of the standards
- Details of Multidisciplinary technical data: Electrical, Mechanical, Power, Cooling, Software, and Integration

Each of these challenges are further described in this paper, followed by proven model-based mitigation approaches used for verification and conformance of components built to the SOSA, HOST, CMOSS and FACE standards.

Primary Challenges of MOSA verification and conformance

There are many and varied challenges to achieving verification and conformance of components that are built to open standards, namely: SOSA, HOST, CMOSS and FACE. We have grouped these challenges and address collectively with an enhanced MMOSA approach:

- Ambiguous requirements
- Traceability and coverage issues
- Verification and conformance tool-chain differences and incompatibilities
- Conflicting requirements of different components such as different optional requirements and different versions of the standards, and
- Details of Multidisciplinary technical data: Electrical, Mechanical, Power, Cooling, Software, and Integration

Ambiguous requirements

The problem of poorly stated requirements is well known. While the problem is known, effective solutions have been elusive. One of the major reasons for this is that most systems still use semi-formal English text to represent the system requirements. “According to the Oxford English Dictionary, the 500 words used most in the English language each have an average of 23 different meanings. The word "round," for instance, has 70 distinctly different meanings.” [3]

This problem is exacerbated in MOSA where technical standards, such as VITA, are leveraged for high-order standard definition. The testability, ambiguity of requirements, and inconsistency in requirements format, content and structure in these standards makes implementation and testability difficult and inconsistent.

Traceability and coverage issues

In order to manage the conformance of hardware and software to open standards, particularly large standards or those that make reference to many other standards in their specification, requires a significant effort to verify coverage of the standard for verification and conformance. Ideally this would be managed with tooling and automation of the software and hardware testing, analysis of results, and verification and conformance to all applicable requirements and specifications. There are additional challenges including all the documentation, standards and specifications necessary to support the effort of fully tracing to all requirements necessary to prove conformance to complex open standards.

Verification and conformance toolchain differences and incompatibilities

Another challenge in verification and conformance of software and hardware is in the number of different toolchains that may be necessary to test a single hardware device not to mention the possible variants and optional requirements. Using HOST as an example, the sheer number of OpenVPX module profiles and slot profiles in conjunction with different module types and multiple form factors requires a large number of software and hardware test elements. To prove verification and conformance requires collecting test data from all of these test elements and collating the results. In many cases testing cannot be automated due to

excessive cost or hardware that is not available to perform testing which requires manual tests through inspection and analysis. It is also common for conformance test tools to lag behind release of open standards by many months which introduces challenges in proving conformance to new versions of open standards.

Conflicting requirements

The SOSA, HOST, CMOSS and FACE standards allow for significant flexibility in their implementation. This flexibility, while highly desirable, creates complexity in overall system integration. For example, when a system uses the FACE Technical Standard, different software components will be conformant to different parts of the technical standard. Software components conformant to the FACE Technical Standard can be conformant to different major or minor editions and may be incompatible. In addition, one Unit of Conformance (UoC) could use one or more Approved Corrections that may not be compatible with other UoCs. These UoCs while each conformant to their specific configuration of the FACE Technical Standard edition, tooling configuration, compilation environment, and selected Approved Correction(s), collectively may not be compatible when integrated together into a system.

Another area of incompatibility is in the semantic data model. For instance, a Platform Specific Service (PSS) UoC can be implemented on one vendors TSS and be integrated with another vendors Portable Component Service (PCS) UoC that was developed using a different TSS. The data model used for these components may even be different. The power of the FACE Technical Standard is that it was built to support this type of integration where optional TSS features can be used to effectively perform FACE conformant integration between the software components.

Multidisciplinary technical data

This challenge is focused more on our traditional solutions than on the problem itself. Stated another way, systems are so complex that we have developed methods to divide the problem into well understood engineering disciplines and coordinate the integration points between the engineering designs with the hope of developing a cohesive, buildable design. This method works for most systems, except, when the complexity of interactions becomes too great. The methods of integrating the modules need to adapt to manage this high complexity.

Methods to Mitigate the Challenges of MOSA verification and conformance

A Holistic Approach

A holistic approach to Model-based Modular Open System Approach (MMOSA) verification and conformance validation consists of addressing the entire process of conformance validation to the open standard specifications. TES has made advances in utilizing MMOSA to develop a holistic verification and conformance solution that is used to build and verify MOSA hardware and software solutions for multi-organization development and integration to build complex cyber-physical systems.

In order to tackle the problem, we must first address the problem of **ambiguous requirements** of the open standards themselves. That is, the open standard normative specifications must be clear and concise without undue ambiguity. It is imperative to ensure the structure and semantics of the specifications are well written and understandable, so consistent implementations of the specifications are possible.

In addition, the problem of **conflicting requirements** is one area where the use of our AWESUM MMOSA modeling tool suite can aid in integrating multiple FACE data models and with the assistance of the AWESUM data model validation, export a FACE data model that can succeed in passing FACE conformance with the Conformance Test Suite (CTS).

AWESUM model-based tool suite is purposely designed to align with the FACE Technical Standard, to DO-178C guidance, and to US Army's airworthiness to AR 70-62. The tool helps prepare the artifacts for FACE Certification and for US Army airworthiness qualification efforts. These life cycle design artifacts are submitted to a sanctioned FACE Verification Authority (FACE VA) per the FACE Conformance Policy guidelines and to authorized airworthiness directorates. The TES-SAVi AWESUM model-based tool suite has been used to develop and certify 33% of the FACE Conformant products listed in the FACE library today and is being used to develop additional FACE Conformant UoCs on three different contracted program efforts. [4]

The success of a MOSA implementation relies heavily on the ability to prove conformance to the open standards on which the MOSA is based. Because of this, it is very important to show that all of the applicable requirements are met. Traditionally, this is accomplished in requirements management through tool automation and supporting processes. Tools such as IBM's DOORS and TES' AWESUM that implement robust **requirements and test traceability** to ensure complete **coverage** is achieved. The results of the traceability analysis can be reported to conformance authorities for independent conformance assessment

As mentioned above, the different methods and tools required to **verify** complex hardware and software systems can be daunting and very expensive. A holistic approach to managing and combining disparate test data and test methods into one unified **conformance toolchain** can greatly simplify conformance management including manual inspection and demonstration. In addition, analysis of large test data sets can be standardized across the various toolchains.

This holistic approach is focused on unifying all of the various normative standards into one unified model to manage all of the specifications, test cases, tests procedures and test results. This includes all

multidisciplinary technical data where electrical, mechanical, power, cooling, software, and integration data is captured, traced and verified.

Application of MMOSA Toolchain

HOST is an important example of a successful SBIR project, described in more detail in Past Projects below. During the HOST SBIR, TES leveraged its AWESUM MMOSA modeling tool suite to develop a HOST Conformance Test Suite called "HARMONY". HARMONY has applicability in its current form but more importantly the tools that were used to develop the capability can be used to extend the capabilities beyond conformance and into the system development from requirement to specification to product to conformance to upgrade. HARMONY can also be used support verification and conformance of other open standards such as SOSA and CMOSS.

The benefit to using HARMONY for conformance is the management of conformance from start to finish. HARMONY provides access to the full suite of standards on which conformance is based upon along with full traceability between those standards. The HOST Tier 3 Component Specification(s) can be produced in HARMONY or easily imported along with the Tier 3 CVM then traced to the appropriate Tier 2 Standard, CVM and Tier 2 Conformance Verification and Applicability Matrix (CVAM). Conformance tests can be executed, results imported from internal or external test execution, status dashboard reports on conformance status, management and analysis of conformance and conformance reports generated and exported both locally and on the web.

Past Projects

In this section, selected past projects utilizing the AWESUM process and toolchain are introduced. Described are efforts that have led TES to a key position supporting the US Army Aviation Community and the Navy's NAVAIR group.

HOST (Hardware Open System Technologies) SBIR Topic N162-0086, Phase I/Phase II

Hardware Open Systems Technologies (HOST) [5, 6] is an Open Systems Architecture (OSA) which defines virtual and physical interfaces to hardware such that interoperability and reuse of hardware components can be realized. The HOST standards leverage commercial technology combined with form factor such as the VITA Standards Organization™ OpenVPX 6U standard [5, 6, 7]. In this example the OpenVPX standard allows flexibility such that vendor lock can still be accomplished. HOST constrains the use of the OpenVPX standard such that vendor lock is preventable. The intent of HOST is to establish performance and interface requirements that are open, enforceable, and testable. As diminishing supplies and obsolescence become more impactful, HOST will facilitate addressing obsolescence and diminishing supplies as well as capability growth from new and/or evolving requirements.

HOST Conformance is defined as 100 percent compliance with all HOST requirements and identifies two products to be verified for conformance: Tier 3 Specifications and products developed to those specifications. All new Tier 3 Specifications will be verified conformant to applicable Tier 1 and 2 Standards. All developed products will be verified conformant to the applicable Tier 3 Specification. This provides a challenge for conformance due to the need to map new Tier 3 specifications to the standards and to validate the product against the provided Tier 3 specification.

The FACE approach to conformance to the FACE Technical Standard is two-fold, an automated test suite, and a Conformance Verification Matrix (CVM). First, FACE utilizes a test suite which ensures conformance of software Unit of Portability (UoP) interfaces to the Operating System Segment (OSS), the Transport Services Segment (TSS), the UoPs application segment: Portable Component Segment (PCS) or Platform Specific Services Segment (PSSS); and to the UoPs' chosen application profile: Security, Safety Base, Safety Extended, or General Purpose.

Second, each of the requirements in the technical standard that are applicable to the UoP must be identified as to how the requirement is met to show conformance. This effort requires the UoP submitter to provide a Conformance Verification Matrix (CVM) to the FACE VA for review. A sanctioned FACE Verification Authority (FACE VA) reviews the CVM and runs the Conformance Test Suite against the UoP to ensure it passes conformance.

TES believes that this two-fold approach for conformance will be effective for ensuring HOST conformance through the HOST verification methods of Inspection, Analysis, Demonstration, and Test. By utilizing an automated conformance test suite executed against the hardware we can ensure that the interface and performance requirements of the computing hardware functions correctly, is timely, and adheres to the HOST interface specifications. It is highly preferable to utilize automated testing, where possible, over other methods.

At TES we always strive to achieve 100% automated testing, there are always some requirements that cannot be tested. For these requirements we recommend a formalized approach whereby the submitter identifies for

each conformance requirement how they believe they meet the requirement as well as the method and justification for meeting the requirement be it through Inspection, Analysis, or Demonstration. An example is for requirements for operating temperature; this would be performed by a qualified lab, whereby documentation provided by the vendor would satisfy the requirement.

TES has developed several tools performing automated hardware and software conformance. To support our Commercial and Military airworthy customers, TES-SAVi developed a MMOSA model tool suite named AWESUM® (AirWorthy Engineering Systems Unified Modeling).

AWESUM is based on an architecture for tool development utilizing the Eclipse Environment. The AWESUM architecture enables rapid development of plugins that come together to create a cohesive set of integrated tools. These tools are cross-platform (Windows, Linux, and OS-X), richly functional providing for systems development, software development, software verification, and ensuring conformance to requirements and specifications. Currently AWESUM supports mapping FACE specification conformance requirements to UoP development plans, requirements, design, and test result. Combined with the FACE conformance tool suite the environment for development of conformant, FACE UoPs are realized.

TES leveraged the AWESUM tool suite to develop a HOST Conformance Test Suite called "HARMONY". We leveraged the existing AWESUM plugins and augmented them to provide a conformance management suite supporting both automated HOST conformance testing and a fully traceable conformance verification matrix. As part of the automated conformance tests, we also interface directly with third party test tool vendors such as National Instruments LabView to automate HOST interface and performance test procedures in addition to the internal HARMONY test procedure development environment. The current supported test procedures methods are Python, Java, C/C++, and a drag-n-drop "Scripts" test development environment.

For additional information on TES-SAVi AWESUM, see https://tes-savi.com/awesum-products/

The Army's R2C2, now A2E2 ARCM

ARCM was formally called "R2C2." R2C2, short for Reusable Radio Control Component, is a FACE™ communications domain application. R2C2 completed the US Army's FACE Verification efforts in 2016. R2C2 is written to FAA's DO-178B Design Assurance Level (DAL) 'C', is aligned to the FACE™ reference architecture standard edition 2.1. It also aligned to the FAA's AC-20-148 guideline for reusable software components. R2C2 was the U.S. Army's first FACE Verified product, completing the Army's sanctioned FACE Verification Authority (FACE VA) in July 2016. R2C2 was developed following Army Guidelines. [Handbook - "Developer's Handbook for Airworthy, Reusable FACE Units of Conformance", Carter, Simi, Tompkins; 2014, US Army AMRDEC-SED.]

R2C2, now known as A2E2 ARCM, [Aviation Architecture and Environment Exploitation (A2E2) for Airborne Radio Control Manager Software Application] is a set of five (5) FACE Units of Conformance. This software suite is aligned to the FACE Technical Standard with a FACE aligned Capability Data Model [i.e., more in model-based description sense than a FACE data model]. It supports multiple US Aviation radios, 14 abstracted open communications capabilities, including over 500 radio functions. It represents a real-world implementation of radio control capabilities in the Army Aviation domain. Under the new A2E2 ARCM contract, its design requirements have been updated to align with the Army's most current guidance, specifically: DO-178C DAL 'C', FACE Technical Standard Edition 3.x [8], and AR 70-62 [9]. ARCM will be delivered to the US Army's sanctioned FACE Verification Authority (Army FACE VA) and verified for correctness to FACE requirements. Then the products will be sent for Flight Qualification to Combat

Capability Development Command-Aviation/Missile Command System Readiness Directorate – Airworthiness (CCDC-AvMC SRD-AW) for the U.S. Army's Airworthiness efforts for integration and flight on an Army PM Office's Utility helicopter, UH-60M model.

In addition, this product suite has been positioned for reuse on other U.S. Army aircraft (Aviation Platform Programs (e.g., PM Apache, PM Cargo, PM UAS, and fixed-wing fleet)). To do this, we have introduced special provisions for reuse into our design and development processes per the AC 20-148 RSC guidance. In the 2014 to 2015 timeframe the US Army's Aviation Directorate (ADD) funded a Science and Technology (S&T) research study called Improvements and Modernizations of Programs Affecting Capabilities and Technologies (IMPACT). [10]. The objective and intent of IMPACT was to prepare the US military aviation community for using improved tools and processes to modernize the design and development capabilities for applications on its fleet of modern aircraft [11].

Conclusion

The emergence of new open standards such as FACE and SOSA are enabling a new generation of Modular Open Systems Approach (MOSA) systems. MOSA holds the promise of utilizing "best-of-breed" technologies to build, upgrade and deploy highly complex systems to our warfighters that are more capable with lower-cost and reduced development and integration schedules.

Over the past three (3) years, Tucson Embedded Systems, Inc. (TES) has tackled the difficult problem of providing multidisciplinary formal verification for MOSA systems. TES developed an MMOSA system for HOST and FACE conformance. The result of these efforts is TES' HARMONY conformance and verification product.

Tucson Embedded Systems leveraged its extensive experience in reusable systems development, MBE tools and tool development, test automation, FACE conformance, and FACE Verification Authority experience, to determine our approach of utilizing AWESUM as a foundational technology for the HARMONY conformance and verification product. HARMONY can be readily applied to SOSA, CMOSS and other open standards for development support, verification, and conformance testing.

TES' work on the HOST Phase I/II SBIR has proven HARMONY Conformance Verification is in fact a feasible approach to reduce the effort to prove OEM hardware verification and conformance and thereby reduce development and integration costs and enable faster hardware upgradability for U.S. Defense Platforms.

Works Cited

[1] The Open Group (2019), Technical Standard for SOSA™ Reference Architecture, Edition 1.0, Version 2 (Snapshot); retrieved from www.opengroup.org/library/s180

[2] M. S. Moore, "Success Factors for Modular Open System Architectures," 8 April 2015. [Online]. Available: https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2015/grcce/Moore.pdf.

[3] "Gray Area," [Online]. Available: http://www.gray-area.org/Research/Ambig/.

[4] IMPACT in Action - Conducting multiple FACE™ development efforts aligned to DO-178C, DO-331, AC 20-148, and AR 70-62 for US Army Airworthiness, 3 June 2020, FACE & SOSA CETIM Sept. 2020 paper

[5] Hardware Open Systems Technologies Tier 1 Standard, HOST00001-10, Version 4.0, April 22, 2019

[6] Hardware Open Systems Technologies OpenVPX Core Technology Tier 2 Standard, HOST00002-10, Version: 4.0, April 22, 2019

[7] OpenVPX Tutorial: http://www.vita.com/Tutorials

[8] "The Open Group (2017), FACE™ Technical Standard, Edition 3.0," [Online]. Available: www.opengroup.org/library/c17c. [Accessed 2017].

[9] “Airworthiness Qualification of Aircraft Systems,” US Army Regulation AR 70-62, Research, Development, Acquisition, HQ Department of the Army, 21 May 2007.

[10] “Innovation and Modernization Projects Affecting Capabilities and Technology (IMPACT): The Airworthiness of Complex Systems”, Final Report v1.0, US Army Aviation Development Directorate (ADD), January 2015, Contract W31P4Q-10-D-0092 DO84, prepared by The University of Alabama in Huntsville.

[11] "Aviation 2050 Vision - Technology for Tactics", 2013, Dr. Bill Lewis, Director of the AMRDEC's Aviation Development Directorate.

References

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- The Open Group (2019), Technical Standard for SOSA™ Reference Architecture, Edition 1.0, Version 2 (Snapshot); retrieved from www.opengroup.org/library/s180
- "RTCA DO-178C – Software Considerations in Airborne Systems and Equipment Certification," RTCA Dec. 2011.
- "Advisory Circular AC 20-148 – Reusable Software Components," US Department of Transportation, Federal Aviation Administration, December 2004.
- "Method and Apparatus for Interfacing with Multiple Objects using an Object Independent Interface Protocol," US Pat No 8,239,586, Tucson Embedded Systems' Capability Driven Architecture (TES' CDA).
- "Capability Driven Architecture: An Approach to Airworthy Reusable Software," Tucson Embedded Systems, American Helicopter Society 63rd Annual AHS International conference, Virginia Beach, Virginia, May 2007.
- "Developer's Handbook for Airworthy, Reusable FACE Units of Conformance," Carter, Simi, Tompkins; 2014, US Army AMRDEC-SED.
- Hardware Open Systems Technologies Open Architecture Standards Framework website https://host-oa.com/

About the Author(s)

Sean P. Mulholland *is a co-founder of Tucson Embedded Systems, Inc. Sean has a B.S in Computer Science and Systems Design from the University of Texas at San Antonio. Sean currently serves as TES CEO and President. Sean has 31 years of experience in software intensive system development, design, integration and testing, especially as it relates to mission critical and safety critical systems. Sean has designed and built several product lines that produced significant advancements in the areas of Geographic Information Systems, Military Ground Systems, Unmanned Ground Vehicles, Unmanned Aerial Vehicles, and Manned aircraft systems. Sean is a contributing author to the FACE™ technical reference architecture and has been active serving as a key resource in FACE Data Architecture development. Sean's current work is focusing on the development of a process and supporting tool suite for optimizing the system development of safe and secure systems for military and commercial systems.*

Ken J. Erickson *is a Principal Engineer with Tucson Embedded Systems and has been with TES for over 22 years. Ken has a B.S. in Computer Science and Bachelor of Computer Engineering from the University of Minnesota, Duluth. Ken has 29 years of experience in real-time and embedded software and systems requirements, design, development, integration and test, including both mission and safety critical systems. He is an active participant in the FACE TWG Transport Services Subcommittee, FACE SECURITY CRADA Working Group, FACE TWG Security Subcommittee, FACE Integration Workshop Standing Committee, and Integration Workshop – Getting Started Guide Subcommittee, a member of SOSA, as well as a member of the TES-SAVi FACE Verification Authority team. Verification work includes conformance testing of FACE 2.0, 2.1 and 3.0 TSS, PSSS, Data Models and OSS'.*

About The Open Group SOSA™ Consortium

As sensor systems increase in number, applications, cost, and complexity, users need to address issues such as affordability, versatility, and capabilities. Sensor systems should be rapidly reconfigurable and reusable by a greater number of stakeholders. The 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, non-proprietary standards for key interfaces.

Further information on 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. Our diverse membership of more than 750 organizations includes customers, systems and solutions suppliers, tools 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.