OPEN SYSTEMS: DESIGNING AND DEVELOPING OUR OPERATIONAL INTEROPERABILITY

MAJ James Ash, USA (Ret.) and LTC Willie J. McFadden II, USA (Ret.)

The need for technological innovation in the U.S. Army is continually increasing. The challenge is to institute a "change paradigm" that will allow the incorporation of new technology into existing systems to address current and future challenges, within fiscal and technological constraints. Open Systems is such an approach. An Open Systems environment facilitates a more efficient assimilation of technology. Furthermore, Open Systems would reduce the costs of technology integration and encourage efforts toward integrated training and operational readiness, using standards and protocols across our nation's warfighting enterprise. Various goals and challenges are inherent to the use of an Open Systems approach, such as Transformation Life Cycle, interoperability, physical connectivity, and political and technical solutions, which are described herein.

Keywords: *Open Systems, Open Architecture, Architecture, System, System of Systems, Transformation Life Cycle*

image designed by Derrick Powell »


OPERATIONAL
INTEROPERABILITY
U.S.ARMY
DEVELOPING
DESIGNING

A Challenged Environment

The U.S. Army is smaller today than it has been in years past, yet it takes on ever-increasing demands for its services. Furthermore, as the Army's operational tempo increases, associated increases in procurement and sustainment costs inevitably escalate. As a result, warfighter training, warfighter planning, and real-time warfighting must be conducted in a more seamless and integrated fashion.

Due to the ever-changing nature of warfare and its accompanying operational demands, the need for technological innovation is continually increasing. The challenge is to institute a "change paradigm"—a new perspective that will allow the incorporation of new technology (unmanned systems, intelligent agents, cyber assets, space systems), within the boundaries of current fiscal and technological constraints—into existing systems to address or resolve many of the challenges discussed here and more.

The Open Systems Approach

A real and possible solution to incorporate new technologies into current systems is for the Army to intensify its efforts to achieve an Open Systems environment. An Open Systems (also known as Open Architecture) environment would facilitate a faster and smoother assimilation of technology. Furthermore, Open Systems would also reduce the costs of technology integration and would encourage efforts toward integrated training and operational readiness, using standards and protocols across our nation's warfighting enterprise. The flexibility of integrating our systems, via open architectures, is a critical component to our Army's force modernization.

The idea of implementing an Open Systems approach already has the support of the Department of Defense (DoD). The Office of the Secretary of Defense established the Open Systems Joint Task Force (OSJTF) in the mid-1990s, and its charter clearly focused all Services on the future of a Modular Open Systems Approach.

Understanding Open Systems theory and how it relates to enhancing warfighting efforts is an important responsibility that is shared between DoD and corporate partners. Before beginning the development of specific solutions through the OSJTF, it is imperative that the goals and strategies be in place. This is a challenging issue due to the number of stakeholders involved in an Army Open Systems approach (Table 1).

TABLE 1. OPEN SYSTEMS ARCHITECTURE–ARMY SIGNIFICANT STAKEHOLDERS

1.	OSJTF
2.	Army G-8, Army G-3, Army G-6, Headquarters, Department of the Army
3.	Army Materiel Command (AMC)
4.	Training and Doctrine Command (TRADOC)
5.	Weapon System Technical Architecture Working Group
6.	U.S. Army Research, Development, and Engineering Command
7.	SEI Carnegie Mellon
8.	Original Equipment Manufacturers (i.e., Boeing, General Dynamics, Raytheon, Sikorsky, etc.)

CHARACTERISTICS OF OPEN SYSTEMS

Open Systems theory is a comprehensive model that describes the elements of an organization and their dynamic interrelationships (Hanna, 1988). It states that organizations are an arrangement of elements that have interdependence on one another.

William Pasmore, a leading expert in systems thinking, writes that "Systems thinking provides guidance and direction for exploration of an organization and its goals for change. It describes the complex relationships between people, tasks, and technologies and helps us to see how these can be used to enhance organizational performance" (Pasmore & Sherwood, 1978). Additional definitions are provided in Table 2.

Open Systems theory provides an important foundation for developing a comprehensive Open Systems approach. Interdependency through connectivity of Open Systems theory is a foundational layer that underpins the goals of Open Systems. However, connectivity is not necessarily hardwired or continuous; rather, it may be established through digital means when appropriate and on an as-needed basis.

FURTHER DEFINING OPEN SYSTEMS

Open Systems are about the entities, their relationship patterns, boundaries of the systems, and the environment(s) in which the systems reside. One of the best characterizations of an Open System is summarized by the frequently paraphrased statement: If you put 20 people in a room, you can find at least 20 different definitions for Open Systems.

The DoD's OSJTF defines Open Systems as "a system that employs modular design, uses widely supported and consensus-based standards for its key interfaces, and has been subjected to successful validation

TABLE 2. COMPARISON OF DEFINITIONS

Agency Institution	Definition
SEI	A system that implements sufficient open specifications for interfaces, services, and supporting formats to (1) enable properly engineered components to be utilized across a wide range of systems with minimal changes; (2) to interoperate with other components on local and remote systems; and (3) to interact with users in a style that facilitates portability.
OSJTF	A system that employs modular design, uses widely supported and consensus-based standards for its key interfaces, and has been subjected to successful validation and verification tests to ensure the openness of its key interfaces.
Webopedia	An architecture whose specifications are public. This includes officially approved standards as well as privately designed architectures whose specifications are made public by the designers. The opposite of open is closed or proprietary.
IEEE POSIX 1003.0/D15 as modified by Tri-Service OSA Working Group, Nov. 1995	A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes. An open system is characterized by the following: • Well-defined, widely used, non-proprietary interfaces/protocols • Use of principles that are developed/adopted by industrially recognized standards • Definition of all aspects of system interfaces • Explicit provision for expansion or upgrading.

and verification tests to ensure the openness of its key interfaces" (Open Systems Joint Task Force, n.d.). Further definitions of an Open Systems approach encompass several key elements and ideas associated with Open Systems. Some of these key elements are established industry protocols, standards, and interfaces. Table 3 also addresses Open Systems components. Additional characteristics of Open Systems follow (Open Systems Joint Task Force, n.d.):

- Use of developed, adopted, and recognized standards
- Well-defined, widely used, non-proprietary interfaces/protocols
- Standing governance bodies regulating Open Systems standards

TABLE 3. COMPONENTS OF OPEN SYSTEMS THEORY

Component	Explanation
Entity	A system entity can be an individual, group, technology, or a combination that comprises the organizational system.
System Boundary	The system boundary is the border that delineates it from other systems and the environment. It is permeable, allowing interaction between the system and its environment. Properly identifying the boundary helps determine the complexity of the organization's policy decision and ultimately the analysis. This boundary provides the contextual environment that the policy decision will affect.
Pattern of Relationships Between Entities	The pattern of relationships between entities interconnects all entities within the system, but all entities do not have to connect to each other. A connection or relationship does not have to be two-way.
Environment	The local environment consists of entities or systems that have a habitual association and critical effect on the system. The global environment is the larger environment that encompasses the system. It includes systems outside the parent organization. Analysts must carefully define the boundaries of local and global environments so as not to invite unwarranted complexity or overlook important interactions with the system.

- Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of application
- Explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

GOALS AND CHALLENGES

The success of Open Systems depends largely on defining, implementing, and satisfying goals at hand. The goals that are established to accomplish Open Systems must be evolutionary in nature because of the magnitude of systems and the dynamic environment of the DoD. The OSJTF charter has published goals that apply to all Services (Open Systems Joint Task Force, n.d.).

The OSJTF must oversee the military departments' transitions to Open Systems-centered acquisition and advise acquisition executives on Open Systems implementation. Also, OSJTF must act as the lead standardization activity for Open Systems weapons electronics and plan the transition of this role to a permanent activity. It must also coordinate and support DoD participation with appropriate industry standards bodies for non-Information Technology (IT) standards. For IT standards, OSJTF will support the executive agent in developing and representing the DoD position.

Other OSJTF goals include establishing sources of training in Open Systems; establishing a repository that facilitates the communication of Open Systems ideas, implementations, techniques, and technologies; designating appropriate Open Systems standards for DoD weapons systems use; and coordinating with the executive agent for IT standards and forwarding IT standards issues to the executive agent for resolution.

Some specific points from the OSJTF charter highlight various challenges that the Army faces as it works to implement Open Systems.

- Cost, interoperability, modularity, technology transparency, and supportability of the various systems create significant management demands.
- Current efforts are still somewhat fragmented and stovepiped, relatively narrow, and are limited primarily to computers and bus structures.
- The air-, land-, and sea-based communities have too little interaction.
- The intended foci of the OSJTF are weapons systems and platforms, not Command, Control, Communications, and Intelligence (C3I) systems, communications networks, or non-real-time, data-processing functions.

Another implicit goal of Open Systems is to integrate hardware, software, systems, and people within the live, virtual, and constructive training and warfighting environments. However, the OSJTF will not attempt to force the use of common hardware everywhere; rather, it will seek to standardize to each unique need while retaining the advantages of common architecture and major interfaces (Open Systems Joint Task Force, n.d.).

The OSJTF's role, as well as DoD's, is a top-down leadership role, providing guidance and resources and coordinating across Services and major agencies to establish policies. Furthermore, there is a bottom-up mandate that requires agencies to provide the daily direction, guidance, and resources required to implement an Open Systems environment.

THE TRANSFORMATION LIFE CYCLE: GOING FROM CLOSED TO OPEN

Along with establishing an Open Systems approach, the implementation of a Transformation Life Cycle is also important (Transformation Life Cycle, n.d.). A Transformation Life Cycle is an approach that can help the government and corporate entities understand, plan, and develop their systems to meet requisite standards of interoperability. Similarly, an approach of this type can help the government achieve an alignment between itself, academia, and commercial enterprise business practices. The Transformation Life Cycle will also allow for implementation that crosswalks technology (i.e., legacy, current, and future), with anticipated capabilities leading to integrated and interoperable systems results.

As previously described, Open Systems is not in and of itself a software product; rather, it is a set of protocols, standards, and a hierarchical structure from which software and hardware are built to ensure that they incorporate and pass information in an integrated and interoperable manner. Additionally, other architectures, standards, and protocols are in use throughout DoD; some of these are described below.

OTHER APPROACHES (HLA, DIS, AND SOA)

In addition to Open Systems, other architectures, protocols, and standards have been, and continue to be, widely used by DoD and industry. Some of these include DoD's High Level Architecture (HLA), Distributed Interactive Simulation (DIS), and Service-Oriented Architecture (SOA). These have, in some manner, facilitated the integration of hardware, particularly software, bringing the constructive, virtual, and live environments together into a coordinated learning environment for training, mission planning, and mission rehearsal.

HLA, developed by the Defense Modeling and Simulation Office (DMSO), was designed to support the interoperability of various DoD simulations. HLA was approved as the standard technical architecture for all DoD simulations by the Under Secretary of Defense for Acquisition and Technology in September 1996, and was later approved as an open standard by the Institute of Electrical and Electronics Engineers (IEEE) in September of 2000 (Defense Modeling and Simulation Office, n.d.).

Additionally, HLA has been an essential architecture, supporting the integration of disparate constructive simulations, as well as virtual simulators and live systems. As previously stated, HLA is not software; rather, it is a hierarchical architecture from which the adherence standards and protocols provide the integrating glue, connecting the Live, Virtual, and Constructive (L-V-C) system environments.

Furthermore, a principal element of the HLA architecture is the Runtime Infrastructure (RTI). RTI coordinates the events from each system environment, facilitating the data exchange and operations and allowing the L-V-C environment to work in a federate manner. Essentially, the simulation systems work as a collection of simulators that share information and are thus changed as a result of the shared events.

DIS is also a useful tool. DIS allows multiple users to work interactively within the same or integrated simulation environment. Examples are the distributed, Internet-based America's Army game or a federated war game, which is run at multiple locations. It is clear that a federated model using HLA can also be DIS.

DIS is built on Local Area Networks or Wide Area Networks and depends largely on the robust capability of the network to handle the data and information-exchange transmission rate. A well-designed DIS has four basic features (Qin, 2002):

- Proper interpretation of time
- Consideration of operation transmission delays
- Execution of operations in correct order
- Allowance of real-time response.

DIS is an important aspect of a simulation environment. Often, bringing each simulation system to a single location, establishing connectivity, and then running the integrated environment are not feasible or cost-effective. Thus, DIS allows simulations to interconnect via a network backbone.

The basic underlying concept of an SOA is a coupling of multiple services within an architectural structure. These services are called upon by customers to support their business requirements. The Organization for Advancement of Structured Information Standards (OASIS) defines SOA as "a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects consistent with measurable preconditions and expectations" (OASIS, n.d.).

An important aspect of SOA is that it provides a means to make services interoperable regardless of the programming language used, location, or platform of a simulation or model. This allows organizations and agencies to produce their software on an appropriate platform, using architectural guiding principles and specified standards and protocols, linking these resources in defined and spontaneous ways to produce results or information. Additionally, this promotes reuse, interoperability, and growth and can help organizations respond to ever-changing and increased demands for information in a more cost-effective manner.

Overall, the relationship of HLA, DIS, and SOA to Open Systems is that each provides a step in the right direction and expands across systems to incorporate their resident capabilities and data into a more integrated and interoperable environment.

ACHIEVING GREAT PERFORMANCE THROUGH OPEN SYSTEMS

Designing, integrating, and evaluating systems and System of Systems architectures to achieve ever greater performance and capabilities while controlling development and sustainment costs present perplexing problems for warfighters, engineers, analysts, and decision makers. Furthermore, these individuals continue to face the increasingly difficult task of integrating these complex simulations and live systems to train, plan, and rehearse—a strategy designed to make U.S. warfighting capabilities a formidable, unstoppable force against any adversary.

The preceding priorities must be accomplished in any environment along the complete spectrum of operations, from humanitarian assistance to full-scale, force-on-force operations. Current employed systems comprise legacy equipment and current technology, but must have the capacity to incorporate future technological advances as they matriculate through development and are incorporated within existing force structures. The greater introduction of space and cyber assets into our Army force structure will exacerbate even further the requirement for Open Systems that effectively and efficiently integrate these domains into the brigade combat team (BCT). Facilitating this critical integration and interoperability requirement necessitates an Open Systems approach.

INTEROPERABILITY AND PHYSICAL CONNECTIVITY

As a basic proposition, interoperability is the ability to work together (Alberts & Hayes, 2003). The importance of interoperability is not at the connectivity of systems within an L-V-C environment; rather, its importance is manifested at the information and cognitive levels.

Having physical connectivity is important. However, this is simply the starting point. And for many, this is often where the discussion stops because warfighters, analysts, engineers, and stakeholders become trapped in the details of bandwidth, platforms, cost, etc. This social standard is transferable to physical L-V-C systems.

Without interoperability, there would be no physical connection (i.e., a social wave between systems), which opens channels to pass information for sharing and allows warfighters to understand issues and situations, and consequently plan and implement courses of action designed to achieve success. With interoperability, the Army Aviation hunter-killer team is able to detach from each other, coordinate and communicate via their physical connection, and share information and understanding to hunt and kill in a distributed manner. Likewise, the Army's greater and greater reliance on commercial-off-the-shelf (COTS) technology necessitates the need for interoperability standards and protocols to better integrate these force multiplier and lifesaving technologies into operational environments.

A USEFUL BLUEPRINT

Open Systems standards and protocols provide a blueprint from which a purposeful design integrates L-V-C systems and facilitates interoperability. The true goals of interoperability are shared information and ultimately shared understanding. To achieve these goals, standards and protocols must be developed within the social structure of "humanness," which will enable the achievement of interoperability.

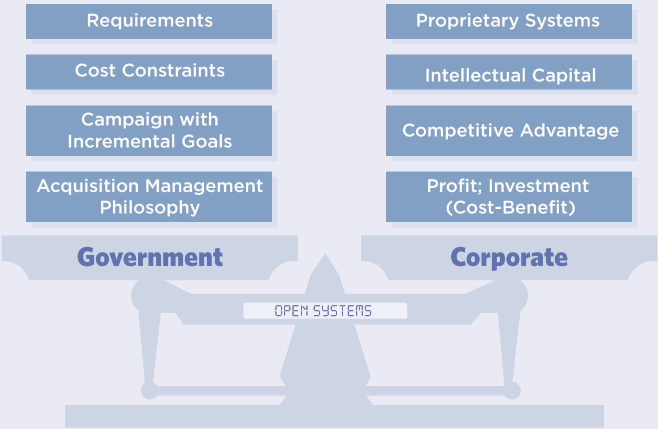
Without a common language or the ability to translate different languages so that entities can communicate, sharing information and gaining understanding would be impossible. For example, humans have developed a standard of greeting, which consists of a handshake or a wave of the hand. Both signify a non-threatening recognition and acceptance, and they open the opportunity to connect and communicate. Likewise, Open Systems provide a similar connection between entities.

OTHER ISSUES

A number of impediments with which DoD is confronted still exist, which are counter to achieving enterprise-wide Open Systems. The most prominent is cost. Open Systems architectures create a performance and cost escalation. For instance, interfaces within components that are strictly controlled to achieve performance gains often become proprietary, and thus increase the cost to the government. Additionally, the development and life-cycle sustainment costs of integrating legacy systems with future systems across DoD are prohibitive when addressed in total. This is one of the reasons that DoD leadership is tackling this requirement incrementally.

Closely associated with cost is the articulation and inclusion of requirements for the development and modification of systems to facilitate forward and backward compatibility of Open Systems standards

FIGURE. DoD AND CORPORATE BUSINESS PRIMARY NEEDS TO ACHIEVE OPEN SYSTEMS



and protocols. Without the vetted and approved requirements mandating the acquisition (i.e., government and commercial) standards that must be met during the systems development phase of a program, Open Systems will be ignored.

However, the requirements process can be a double-edged sword. Though it clearly mandates that a program manager or material developer meet the requirements, the interpretation of requirements can lead to a cost that is far beyond the intent, causing a scaling back of the requirement intent and ultimately the level of interoperability across DoD L-V-C systems. This situation starts the trade-space analysis.

Alternatively, the interpretation of requirements can lead to a cost that is far less than the intent, again thwarting the goal of achieving Open Systems. What is needed is a balance (as depicted in the Figure) between the DoD's needs and corporate business imperatives, and also the ability to deliver Open Systems.

As demonstrated, DoD must develop an environment that is designed to encourage technology development and competition within an Open Systems framework. This will require strong, earnest leadership and governance. This leadership and governance must be top-down and must have consistency over time, as DoD is a customer with high expectations.

Open Systems Solutions

The governance of the Open Systems approach must be continually reviewed and updated to provide a success-driven environment. The Army recognizes the importance of governance and thereby creates a means to implement Open Systems by socializing, formalizing, resourcing, and implementing processes to transition from closed to Open Systems.

The Army also evaluates systems throughout the acquisition process to ensure that they meet Open Systems standards. The governance of this campaign should adopt the Open Systems framework and should be the decision-making, regulatory, and enforcement structure to ensure that requirements, standards, and protocols are met. For example, new initiatives like a new architecture require that the agency either fund for the mandate or nurture a community of interest that will provide input and see benefit to incorporate such models.

Corporate entities that support the DoD are not expected to act as patriots. Rather, they should manage the customers' expectations and should work with customers to craft appropriate strategies to achieve Open Systems. They should also recognize that cost is a significant factor, and that incremental steps must be funded.

These incremental steps should be framed within an overall, larger encompassing campaign, focused on a sector of the defense industrial complex. DoD and corporate partners must come to terms with the balance of client needs and funding realities to profit, proprietary rights, and intellectual capital. The solutions are both political and technical.

At the same time, bottom-up champions who are dedicated to achieving a comprehensive, integrated L-V-C Open Systems environment are needed. Additionally, these implementers need to develop proof-of-principle facilities that work collaboratively with the materiel developers to test and validate that the systems meet Open Systems standards and protocols, and to be certain that they are truly integrated and interoperable. These champions must also be funded and empowered to make decisions within the established governance framework, and must make appropriate changes and take those changes to the executive governance body for decision.

Overall, implementing and maintaining an Open Systems approach is an involved yet essential requirement. Due to the nation's current state and the increasing demands placed upon the Army, new and innovative systems of technology are consistently needed and required. Certainly no system is without concerns or impediments, and the Open Systems approach is no exception. However, if problems are addressed as needed and if proper governance is in place, Open Systems can be achieved. The result of an Open Systems architecture is the development of an environment that provides the training, mission rehearsal, and warfighter planning that support our Army—all of which will sharpen our warfighting edge and ensure our dominance across the full spectrum of operations.

Author Biographies

MAJ James Ash, USA (Ret.), is currently the Army account manager for Booz Allen Hamilton in Huntsville, Alabama. MAJ Ash has more than three decades of experience in leading a variety of aviation and business organizations across a broad range of operational responsibilities and challenging environments. He earned a bachelor's degree from Embry-Riddle Aeronautical University and a master's degree from Central Michigan University. MAJ Ash is a former Southeast Asian Foreign Area Officer and Army Strategist.

(E-mail address: ash_james@bah.com)

LTC Willie J. McFadden II, USA (Ret.), earned a bachelor's degree from the United States Military Academy. He holds a master's degree in operations research from the Naval Postgraduate School and a PhD in engineering management from Old Dominion University. LTC McFadden is currently a senior associate with Booz Allen Hamilton in Huntsville, Alabama. He is a past president of the Military Operations Research Society and serves as president-elect for the American Society of Engineering Management.

(E-mail address: mcfadden_willie@bah.com)

REFERENCES

Alberts, D., & Hayes, R. (2003). *Power to the edge: Command…control…in the Information Age.* Information Age transformation series. Washington DC: Command and Control Research Program.

Defense Modeling and Simulation Office. (n.d.). DMSO Web page. Retrieved December 2, 2005, from http://www.msco.mil.

Hanna, D. (1988). *Designing organizations for high performance.* NY: Addison-Wesley Publishing.

OASIS. (n.d.). Organization for Advancement of Structured Information Standards Web page. Retrieved April 26, 2007, from http://www.oasis-open.org/home/index.php

Open Systems Joint Task Force. (n.d.). OSJTF Web page. Charter for the Open Systems Joint Task Force. Retrieved April 26, 2007, from http://www.acq.osd.mil/osjtf/charter.html

Pasmore, W., & Sherwood, J. J. (Eds). (1978). Organizations as sociotechnical systems. *Socio-technical systems: A sourcebook.* LaJolla, CA: University Associates.

Qin, Xiao. (2002). Delayed consistency model for distributed interactive systems with real-time continuous media. *Journal of Software.* Queensland, Australia: School of Computing and Information Technology, Griffith University.

Software Engineering Institute (SEI) Carnegie Mellon. (n.d.). SEI Web page. Retrieved May, 7, 2007, from http://www.sei.cmu.edu/.

Transformation Life Cycle. (n.d.). Booz Allen Hamilton Web page. Retrieved May 7, 2007, from http://www.boozallen.com/tlc.

APPENDIX

List of Acronyms

AMRDEC	Aviation and Missile Research, Development, and Engineering Center
DIS	Distributed Interactive Simulation
DMSO	Defense Modeling and Simulation Office
DoD	Department of Defense
HLA	High Level Architecture
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
L-V-C	Live, Virtual, and Constructive
OASIS	Organization for Advancement of Structured Information Standards
OSJTF	Open Systems Joint Task Force
RTI	Runtime Infrastructure
SEI	Software Engineering Institute
SOA	Service-Oriented Architecture