A Criteria-Based Framework for Establishing System of Systems Governance

Vaneman, W.K.

Vaneman, W.K. and R.D. Jaskot (2013).A Criteria-Based Framework for Establishing System of Systems Governance. Orlando, FL: Proceedings of the 7th Annual International IEEE Systems Conference, pp. 491-496.

http://hdl.handle.net/10945/49913

A Criteria-Based Framework for Establishing System of Systems Governance

Warren K. Vaneman
Department of Systems Engineering
Naval Postgraduate School
Monterey, CA

Roger D. Jaskot
Space and Naval Warfare Systems Command
Space Field Activity
Chantilly, VA

Abstract— **Net-centricity is forcing the evolution of system of systems (SoS). One aspect of SoS that has been essentially ignored is SoS governance. Governance is the set of rules, policies, and decision-making criteria that will guide the SoS to achieving its goals and objectives. In this paper, we join the attributes of governance practices found in the IT community with known SoS types and characteristics to develop a criteria-based framework for SoS governance.**

Keywords—System of Systems, Governance

I. INTRODUCTION

In this age of net-centricity, a premium is being placed on the interfaces and interactions among systems. As a result, there has been an increased focus on a class of complex systems known as System of Systems (SoS). An SoS is a set or arrangement of systems that results when independent, and task-oriented systems are integrated into a larger systems construct, that delivers unique capabilities and functions in support of missions that cannot be achieved by individual systems alone.

While current literature recognizes the existence of different types of SoS, no standard naming convention has been defined across the Systems Engineering community. This paper adopts the four types of systems defined by Department of Defense, *Systems Engineering Guide for Systems of Systems Engineering* [1]:

> *Virtual* – An SoS that lacks a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behavior emerges, and may be desirable, but this type of SoS must rely upon relatively invisible mechanisms to maintain it.
> *Collaborative* – An SoS where the component systems interact more or less voluntarily to fulfill agreed upon central purposes. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.
> *Acknowledged* – An SoS where component systems have recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the system.
> *Directed* – An SoS is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose.

A cornerstone of an effective SoS is governance. Governance in this context means the set of rules, policies, and decision-making criteria that will guide the SoS to achieving its goals and objectives. Governance is well represented in the IT literature [3], but a discussion of how to apply it in an SoS environment is absent. In this paper, we examine the attributes of good governance, and then use those attributes to develop a criteria-based framework for SoS governance. While these criteria would be best applied in the types of SoS defined by [1] as directed and acknowledged, SoS, we believe that it could be extended to other SoS types.

II. LITERATURE REVIEW

The definition of governance varies widely, depending on the circumstances to which governance is being referred. To avoid potential confusion throughout the entire SoS, the meaning needs to be established early and clearly. For example, within a sourcing context, governance has been used interchangeably with the term "sourcing management," which it is not.[4] Governance and management are two separate entities and need to be treated as such. Management incorporates an execution component with decision-making whereas governance strictly pertains to only decision-making. However, leveraging the elements of good governance with the best practice characteristics of service management will yield beneficial and synergistic results within the SoS.

Examining and understanding this leveraging will help in defining the SoS governance process. Coalescing and then optimizing the best attributes of governance and service management will establish the necessary foundation for a successful process.

The following are elements of good governance as defined by the United States Navy's (USN) Deputy Assistant Secretary of the Navy – Research, Development, Testing and Evaluation (DASN (RDT&E)) Chief Engineer [2]

- *Participation* – Participants must have the authority to make decisions on behalf of their organizations. Participants must be free to express themselves without retribution.
- *Regulations and Policies* – Good governance requires fair policies and regulations that are enforced impartially.
- *Transparency* – Transparency means that decisions taken and their enforcement are done in a manner that follows rules and regulations and that information is freely available and directly accessible to those who will be affected by such decisions and their enforcement.
- *Responsiveness* – Good governance requires that institutions and processes try to serve all stakeholders within a reasonable time frame.
- *Consensus Oriented* – Good governance requires mediation of the different interests to reach a broad consensus regarding what is in the best interest of the entire System of System and how this can be achieved.
- *Equity and Inclusiveness* – All members feel they have a stake and do not feel excluded from the mainstream of the decision-making.
- *Effectiveness and efficiency* – Good governance means that processes and organizations produce results that meet the needs of mission while making the best use of resources at their disposal.
- *Accountability* – In general, an organization or an institution is accountable to those who will be affected by its decisions or actions. Accountability cannot be enforced without transparency and the rule of law.

The following are elements of good governance as defined by the USN's Space and Naval Warfare Systems Command Technical Authority for IT (SPAWAR IT TA) Executable Governance Plan [3]:

- *Governance Organization* – Authoritative structure to provide guidance on the allocation of resources, coordinate and control mission area capability and promote development activity.
- *Interoperability* –Assurance of interoperability between the constituent systems at all levels to allow the necessary communication and connectivity across the system of systems. Interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment.

In order to determine useful governance principles for the four principles of service management representing best practices as defined by the Information Technology Infrastructure Library [4] are:

- *Specialization and Coordination* – The relationship between customers and service providers is defined (and varies) by specialization in ownership and control of resources and the coordination of dependencies between different pools of resources.
- *The Agency Principle* – Service agents act as intermediary agents who facilitate the exchange between service providers and customers in conjunction with users. They are typically employees of the service provider but can also be systems and processes that users interact with in self-service situations.
- *Encapsulation* – Encapsulation hides what is not the customer's concern and exposes as a service what is useful and usable to them. Customers are concerned only with utilization.
- *Principles of Systems* – A system is a group of interacting, interrelated, or interdependent components that form a unified whole, operating together for a common purpose. Two control processes used within these systems are open-looped (the value of the outcome has no influence on the process input) and closed-loop (outcome has influence). The closed-loop system depends on feedback and learning. Learning occurs from the presence of feedback as an input to a process.

III. CORRELATION OF LITERATURE

In order to determine useful governance principles for inclusion into a purposeful criteria-based governance framework, this volume of best practice elements and characteristics needs to be amalgamated along analogous threads. Binning the elements of good governance to the best practices of service management provided the best solution. This solution provides a more straightforward approach when determining how and where to apply the governance principles against the characteristics of an SoS.

Binned principles:

a) Specialization and Coordination
1. Governance organization
2. Clear regulations and policies

b) The Agency Principle
1. Participation
2. Responsiveness
3. Consensus oriented
4. Equity and inclusiveness
5. Accountability

c) Encapsulation
1. Transparency

d) Principle of Systems
1. Effectiveness and efficiency
2. Interoperability

IV. CRITERIA-BASED GOVERNANCE FRAMEWORK

The various levels of cohesion of constituent systems within the different types of SoS requires different approaches to SoS governance. For example, the loosely federated virtual SoS requires a different governance approach than the more tightly coupled directed SoS. To determine how to apply governance principles to an SoS, the characteristics of the SoS need to be considered.

Any SoS has five characteristics: autonomy, belonging, connectivity, diversity, and emergence [5]. These SoS characteristics have a range of definitions that allows them to be applied across the spectrum of SoS types. Table I defines the SoS characteristics, and represents the range of attributes for those characteristics by depicting the characteristic attributes for virtual and directed SoS.

A prerequisite to defining an SoS governance process is understanding where the SoS is in the spectrum of SoS types and characteristics. It is important to note that governance cannot be defined by SoS type alone –the characteristics must be considered as well.

Fig. 1 illustrates this point with two examples plotted on the SoS Characteristic Spectrum. For the first example, a Department of Defense (DoD) SoS is plotted, where the constituent systems are provided from different services and agencies. In this case, the autonomy and connectivity are less restrictive. Diversity and belonging are likely to be greater, because they were provided by various services and agencies who developed the systems to provide capabilities to satisfy their mission needs. Emergence will most likely occur through happenstance rather than design.

The second example is a single service acknowledged SoS. In this case the autonomy, belonging, and connectivity are likely to be more defined because they are designed to meet that service's system capability and mission needs. Since the constituent systems are being developed under a common engineering philosophy, diversity will be reduced. The emergence of good and bad SoS behavior is more likely to be known since the constituent systems may have operated or been tested together in the past. Fig. 1 also illustrates the single service acknowledged SoS.

With an understanding of the type and the characteristics of the given SoS, the governance strategy can be developed. In Section II, the elements of good SoS governance and principles of service management were defined from a few authoritative sources, then correlated for like concepts. These correlated elements serve as the foundation from which a governance strategy can be developed.

A. Criteria 1: Organizational Structure, Standards and Policies

Governance strategy must first consider the existing organizational structure and policies. While the organizational structure, standards, and policies may not be able to be

TABLE 1. SoS Characteristics

Characteristic	Definition	Directed SoS	Virtual SoS
Autonomy	The ability to make independent choices; the right to pursue reasons for being and fulfilling purposes through behaviors.	Conformance: Autonomy is ceded by parts in order to grant autonomy to the system.	Independence: Autonomy is exercised by constituent systems in order to fulfill the purpose of the SoS.
Belonging	To be a member of a group; to have the proper qualifications.	Centralize: To bring under one control; to come together to form a center.	Decentralization: Constituent systems choose to belong on a cost/benefit basis, also in order to cause greater fulfillment of their own purposes, and because of belief in the SoS supra purpose.
Connectivity	The ability of a system to link with other systems.	Platform-centric: Prescient design, along with parts, with high-connectivity among major sub-systems.	Network-centric: Dynamically supplied by constituent systems with every possibility of myriad connections between constituent systems, possibly via a network-centric architecture to enhance SoS capability.
Diversity	Noticeable heterogeneity, having distinct or unlike elements or qualities in a group; the variation of social and cultural identities among people existing together in an operational setting.	Homogeneous: Managed, that is, reduced or minimized by modular hierarchy; parts diversity encapsulated to create a known discrete module whose nature is to project simplicity into next level of hierarchy.	Heterogeneous: Increased diversity in SoS capability achieved by released autonomy, committed belonging, and open connectivity.
Emergence	The appearance of new properties in the course of development or evaluation.	Foreseen: Foreseen, both good and bad behavior, and designed in or tested out as appropriate.	Indeterminable: Enhanced by deliberately not being foreseen, though its crucial importance is, and by creating and emergence capability climate, that will support early detection and elimination of bad behaviors.

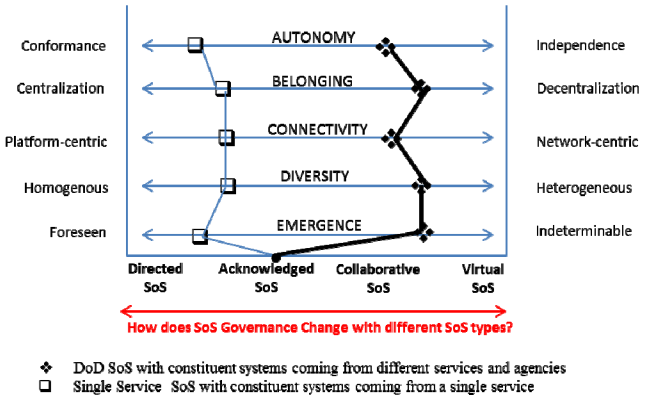

Fig. 1. SoS Characteristics Spectrum

changed, the management environment must be understood to develop effective governance.

These structures, standards, and policies can vary widely as a function of the SoS type. For example, in a virtual SoS, such as the Internet, the organizational structure is limited to the standards body. The standards and policies are only as constraining as they need to be for the very large variety of applications.

For a directed SoS, such as a ground SoS within a space architecture, the organizational structure, standards and policies are very well defined, due to the SoS residing in a single organization, and having closely aligned system development programs.

The DoD and the services have similar organizational structures, standards, and policies. Because of this, SoS are developed and assembled in similar ways. The main differences are since that in the service specific example, the SoS development and operational policies are more tightly coupled as the constituent systems are more likely to be designed to work together.

B. Criteria 2: Goverance Composition and Principles

. The second criteria determines the degree of participation, responsiveness, consensus, inclusiveness, and accountability that needs to be included in the governance strategy. When considering a governance strategy for a virtual SoS, participation is limited to a few standards committees. As a result, the average SoS participant is not included in the decisions, and they can expect a relatively low responsiveness to changes they suggest. Given the wide dispersion of user goals and missions, accountability in a virtual SoS is limited only to following the loosely defined standards and policies.

In a directed SoS, on the other hand, a higher degree of participation and inclusiveness is warranted. This participation often occurs at multiple system levels (i.e., enterprise, SoS, and systems levels), and often involves several governance forums. With a high degree of participation and inclusiveness, this governance type also realizes a high degree of responsiveness and consensus. Directed SoS are designed to work together to support a common mission and are often within a single organization; therefore, accountability is usually strongest.

In the DoD example, the constituent systems are contributed by various services: therefore, their autonomy is nearly independent due to their service specific development. As such, participation and inclusiveness are likely to reside at the enterprise and SoS levels, and not at the systems level. Responsiveness to changing mission needs will most likely be determined by the criticality of the mission: therefore, requests for SoS and system changes are likely. However, given the tightly coupled common mission, accountability of constituent systems is also expected.

In the service SoS example, constituent systems are most likely to be developed to operate together, and thus the characteristics of autonomy, belonging, connectivity, diversity, and emergence are likely to reside towards the left side of the SoS Characteristics Spectrum shown in Fig.1. Given the nature of service specific systems, the acknowledged SoS is the most common allowing for maximum mission-set flexibility. The governance strategy would then most likely focus on responsiveness, inclusiveness, participation, and accountability. As such, the governance structure will reside at the enterprise, SoS, and system levels, but will not be as tightly controlled as the directed SoS governance level.

C. Criteria 3: Encapsulation

Encapsulation refers to how transparent the governance decisions are and how enforcement is managed within the SoS. When considering a virtual SoS, the governance and decisions are made by a relatively small number of stakeholders. The SoS users are primarily concerned with utilization, and often don't care how the SoS decisions are made or the rules enforced, as long as they can achieve their missions and goals. Therefore, a virtual SoS governance strategy assumes a certain degree of transparency and exposure to SoS services without user feedback.

For a directed SoS, the stakeholders are more closely aligned, and are closer to the decisions being made. Therefore, when developing a directed SoS governance strategy, a more inclusive and transparent process is needed.

When considering the DoD and service specific examples, similar governance strategies should emerge. The transparency of decisions and the enforcement are likely to be more tightly coupled in a service specific SoS, because the service controls the technical direction, and budget for the constituent systems. On the other hand, the DoD does not control individual technical requirements or budgets, and therefore the enforcement mechanism is not as tightly coupled.

D. Criteria 4: Governance Effectiveness and Interoperatbility

The differences between the virtual SoS and directed SoS governance strategies are the most defined when considering SoS effectiveness and interoperability. Given the SoS characteristics for the directed systems, attributes such as independence, decentralization, and heterogeneous can be used as the defined the states. In a virtual SoS, the users are using

the SoS for their own goals and missions, and are essentially operating independently. As such, they don't have insights into SoS effectiveness, and don't care as long as the interoperability that they are expecting is achieved. As a result, governance for effectiveness and interoperability is limited or non-existent.

In a directed SoS, the constituent systems are designed to work together to achieve common goals and missions. Because of this, SoS effectiveness and interoperability are very well defined and controlled. Often, these systems will have common processes for establishing and controlling the baseline, with causal relationships between constituent systems both known and analyzed.

The service SoS example will closely resemble the directed SoS governance strategy. Individual systems will contribute to service mission effectiveness and will most likely share the same interoperability. Hence, a more controlled governance strategy is warranted.

The DoD SoS example also requires effectiveness and interoperability for mission success. However, services define interoperability standards, and since the constituent systems are designed for unique applications, the effectiveness will not be as pronounced as with the service SoS. The governance strategy should emphasize closer collaboration with service elements. However, while the service governance strategy can be prescriptive, the best a DoD strategy can hope for is a collaborative relationship.

V. GOVERNANCE EXAMPLE

The Chief of Naval Operations (CNO) directed that an Information Technology (IT) Technical Authority (TA) be established to enhance the integration and interoperability of information, network, and communication systems as an essential component to enable the Navy's Information Dominance (ID) vision. Subsequently, the CNO, in conjunction with the Assistant Secretary of the Navy for Research, Development, and Acquisition (ASN RDA), designated Space and Naval Warfare Systems Command (SPAWAR) as the Navy's IT TA. In that capacity, SPAWAR is responsible for establishing the overarching IT architecture requirements, identifying and defining applicable technical standards, allocating information assurance and interface requirements for Platform IT interconnection, and supporting IT certification and accreditation.

SPAWAR is defining and developing the systems engineering approach, tools, certification process and governance framework required for executing its IT TA responsibilities. A System of Systems Engineering and Integration (SoSE&I) approach is being implemented for establishing and governing the Navy's IT enterprise architecture in response to the challenges presented by the Navy's ID vision. Consequently, IT acquisition decisions and system developments will be better aligned and coordinated with mission needs to ensure the operational effectiveness of the Navy's networks and platform systems. A proper governance strategy is essential to achieving the IT TA goals.

Navy IT is an acknowledged SoS with the characteristics similar to the single service example shown in Fig. 1. Given the vast reach of Navy IT, a structure is required to govern the SoS at various levels from the Navy Enterprise to individual systems fulfilling SoS requirements. Fig. 2 depicts the IT TA Governance Environment, and will be used to explain how

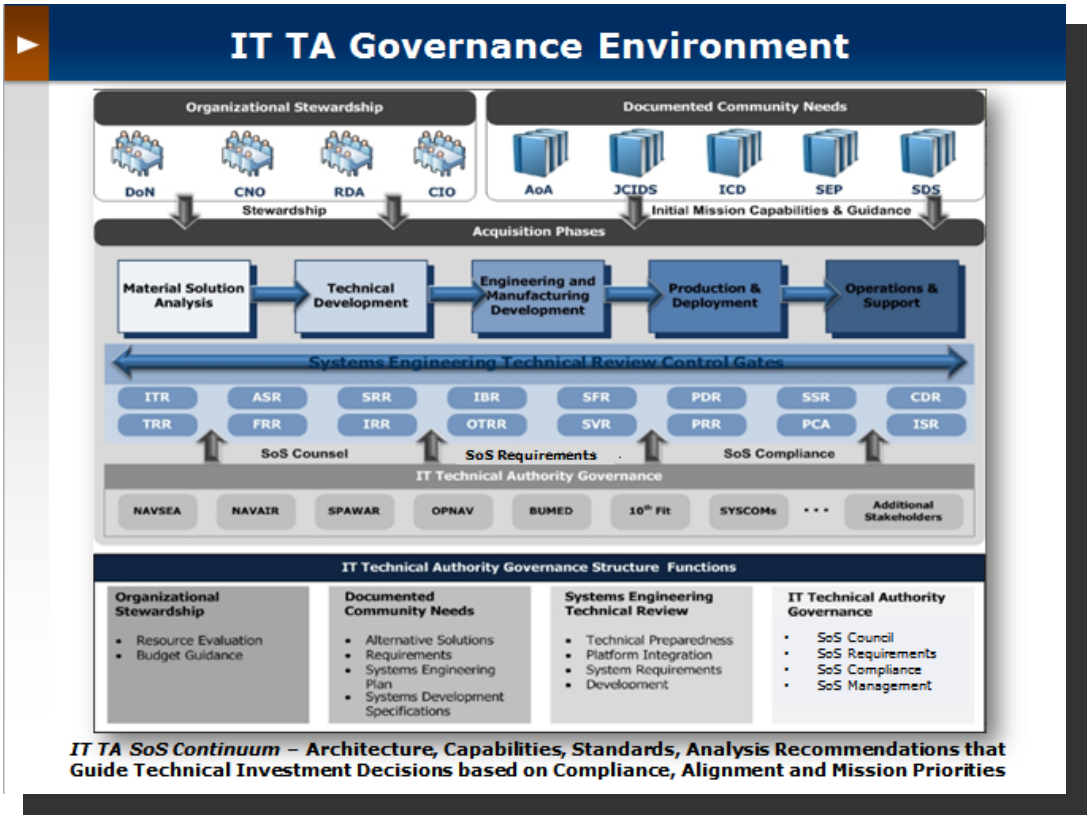

Fig. 2. IT TA Governance Environment [3].

Criteria 1-4 could be used to form a viable IT TA construct.

The Navy has a well-defined organizational structure, standards, and policies for individual system development. System requirements are allocated to individual program offices from the fleet via the Office of the Chief of Naval Operations (OPNAV). Acquisition and development authority is exercised by the various Program Executive Offices (PEO) who report to ASN RDA. As such, acquisition standards and policies are similar throughout the Navy Enterprise, but they do not address the SoS.

To be effective, IT TA governance standards and policies must be adopted at the enterprise and SoS levels. Across the Navy enterprise, standards and policies need to be developed to address cross Systems Commands (SYSCOM) SoS issues. There are current organizational bodies that could be modified to fill this void without having to establish new governing bodies.

At the SoS level, a governance structure is used to manage the SoS architecture and requirements baseline. From an SoS perspective, requirements are allocated to individual systems. These requirements may not be necessary for the system to operate autonomously, but are required for the systems to contribute functionally to an SoS. A configuration management process will allow for the baseline to be controlled, and for changes to the baseline to be analyzed according to the impact to the capability the SoS provides.

Considering Criteria 2, Governance Composition and Principles, when establishing new governance organizations, or modifying existing ones, the degree of participation, responsiveness, consensus, inclusiveness, and accountability must be considered. Given this is a single service problem, where the systems are envisioned, if not designed, to work together, collaboration among the constituent systems, and where appropriate, the SYSCOMs, is required. Therefore, when considering the governance organizations, the more inclusive and consensus oriented they are, the more effective the SoS is likely to be.

Criteria 3, Encapsulation, refers to how transparent the governance decisions are and how enforcement is managed in the SoS. Part of governance decision is the discovery of similar technical solutions across the Navy. One promising forum for this discovery is Naval Open Architecture. This concept allows for program managers to stay abreast of acquisitions occurring across the Navy [6]. This could be a beneficial governance structure, as it will consolidate the number of technical baselines, thereby making interoperability and consensus easier. The governance structure for an Open Architecture approach would require a managed and controlled central repository to house technical and acquisition data.

The Navy develops systems to provide capabilities to achieve mission success. Therefore Criteria 4, effectiveness and interoperability, is of paramount importance. Defining interface standards for interoperability needs to be one of the IT TA governance functions. Given the multiple SYSCOMs, this would best accomplished through one of the governance forums. To implement standards appropriately, an enforcement governance mechanism would be required. One existing forum which could appropriately address this with only minor considerations is the Systems Engineering Technical Review (SETR). By aligning interoperability to the SETR, the governance is enforced during major milestone reviews.

VI. CONCLUSIONS

Net-centricity is forcing the evolution of System of Systems. However, regardless of the type of SoS, some degree of governance is required. When developing governance structures, one size does not fit all. This paper serves as a first step in defining the appropriate SoS governance. The concepts introduced are theoretical in nature, but demonstrate a criteria-based guide to establishing effective SoS governance policies for a given SoS type.

The ideas presented in this paper will initiate an important dialogue among SoS practitioners on the importance of governance. While we examined one approach to governance based on the Information Technology Infrastructure Library, there are other approaches that could be incorporated with this work or used as a complimentary approach. However, whichever base governance methodology is used, applying that methodology to the correct SoS type is important.

REFERENCES

[1] Office of the Deputy Under Secretary of Defense for Acquistion and Technology, Systems and Software Engineering. *Systems Engineering Guide for Systems of Systems" Version 1.0.* [Online]. Available http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf.

[2] DASN (RDT&E) Chief Systems Engineer, "Mission Area "System of Systems" Systems Engineering Guidebook," draft 2011.

[3] Space and Naval Warfare Systems Command (SPAWAR), "Information Technology Technical Authority Executable Governance Plan," Unplublished working paper, 2012.

[4] Office of Government Commerce, "Information Technology Infrastructure Library," 2007.

[5] Office of Government Commerce, "Information Technology Infrastructure Library," 2007.

[6] B. Sauer, J. Boardman, and A. Gorod, "System of Systems Management," in System of Systems Engineering: Innovations for the 21st Century, M. Jamshidi, Ed., Hoboken, NJ: Wiley, 2009, pp. 191-217.

[7] J. Shannon, "The Imperative for Open Architecture and Innovation," Naval Institute Proceedings, February 2013, pp. 10.