Software Engineering Institute

System-of-Systems Governance: New Patterns of Thought

Ed Morris
Pat Place
Dennis Smith

October 2006

TECHNICAL NOTE
CMU/SEI-2006-TN-036

Integration of Software-Intensive Systems Initiative

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Tables

Acknowledgment

This work on this technical note was partially supported by funding from the Secretary of the Air Force/Acquisition (SAF/AQ).

Abstract

Systems of systems introduce complications for information technology (IT) governance because their individual system components exhibit considerable autonomy. This technical note examines the ways in which six key characteristics of good IT governance are affected by the autonomy of individual systems in a system of systems. The characteristics discussed are (1) collaboration and authority, (2) motivation and accountability, (3) multiple models, (4) expectation of evolution, (5) highly fluid processes, and (6) minimal centrality. This report examines each characteristic in detail and, where possible, provides guidance for the practitioner.

1 Introduction

Many software systems fail to meet expectations in capability, cost, and timeliness for a variety of factors.[1] A significant number of failures result from poor management and control of information technology (IT)[2] projects and faulty procedures that do not keep systems operating as expected.

Better structures are needed for identifying objectives, encouraging desired behaviors, establishing appropriate relationships, and monitoring and achieving accountability. Generally, support structures for those activities are part of an organization's IT governance.

Even when constructing and operating "in-house" systems that execute within the boundaries of a single project and organization, IT governance is difficult. When systems cross organizational boundaries, the development problems—and, by extension, IT governance problems—are multiplied due to conflicting structures, policies, and expectations.

This paper considers the impact that a system-of-systems context[3] has on IT governance. For the most part, we highlight governance issues without being able to suggest solutions in every instance. Further work will be required before all such issues can be resolved. Traditional acquisition, development, and operational models are predicated on a single-system (or single-organization) notion. Even though we know that systems do not operate in a stand-alone manner, we tend to acquire and develop them that way. This simplifying assumption leads to the approach in which each program has a program office that controls a system. Because a system-of-systems environment requires interaction between a number of different systems and organizations, it requires a rethinking of traditional assumptions about IT governance.

The rest of Section 1 characterizes both IT governance and systems of systems and outlines the need for change in governance practices. Section 2 discusses six characteristics of good system-of-systems governance. Section 3 briefly summarizes the paper and recommends further investigation.

[1] Even though the number of software system failures is a matter of recent debate, there is little doubt that the number is still significant. The initial [Standish 1994] and updated versions of the *Chaos Report* are frequently cited sources. However, a recent article by Glass suggests that objective research study findings reach different conclusions. Glass suggests that the Standish findings could possibly be biased toward failure and requests more openness regarding the data and data collection process [Glass 2006].

[2] While the subject of this paper is governance for IT systems (where more data is available), we do not expect that the issues we raise are altered substantially if we extend our comments to weapons systems.

[3] Investigators in the Integration of Software-Intensive Systems Initiative at the Carnegie Mellon® Software Engineering Institute (SEI) start with the view that a system of systems is radically different from a system and cannot be treated as though it were simply a much bigger system. (Carnegie Mellon is registered in the U. S. Patent and Trademark Office by Carnegie Mellon University.)

1.1 IT GOVERNANCE

KPMG International[4] defines IT governance as

- an integral part of corporate governance
- the responsibility of board members and executives
- a mechanism to deliver value, manage performance, and mitigate risk
- a method to assign accountability for decisions and performance
- dynamic in alignment to business goals
- composed of policies, procedures, management committees, performance metrics, and related management techniques working in unison toward common business goals [KPMG 2004]

According to the IT Governance Institute, the "overall objective of IT governance . . . is to understand the issues and the strategic importance of IT, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims at ensuring that expectations for IT are met and IT risks are mitigated" [ITGI 2003].

A common thread running through these and most definitions is that IT governance involves policies for the control and coordination of IT resources, enforcement of those policies, and measurement of the outcome. Also central to these definitions, and illustrated in the preceding KPMG definition, is the corporation (or enterprise) whose board members and executives decide on business goals.

1.2 IT GOVERNANCE OF SYSTEMS OF SYSTEMS

Systems of systems introduce a new set of issues that have significant implications for governance. The following list of characteristics provided by Maier captures the essence of how a system of systems differs from a system [Maier 1998]:

- **operational independence** of the systems
  Each system within a system of systems has a "life of its own" and can function acceptably and provide useful service without necessarily interacting with other systems.
- **managerial independence** of the systems
  The individual systems within a system of systems are under different authorities. For example, within the U.S. Department of Defense (DoD) different service branches will own different systems in the context of a system of systems.
- **evolutionary development**
  The different systems within the system of systems are developed and upgraded on uncoordinated schedules. While current policies can coordinate the schedules for a relatively limited number of systems within a system of systems, it is unlikely that such a policy can scale to a size of the Global Information Grid (GIG).

[4] KPMG International is a global network of professional firms providing audit, tax, and advisory services.

These highlighted characteristics[5] lead to the conclusion that the systems within a system of systems exhibit a high degree of autonomy. Because of that autonomy, the system-of-systems perspective overturns the assumption upon which most of the traditional IT governance practices are founded (i.e., IT governance involves policies for the control and coordination of IT resources, enforcement of those policies, and measurement of the outcome).

Distributed ownership of individual components represents a thorny problem for any system of systems. Governance becomes significantly more complicated and must change to accommodate the realities of a system of systems. Many different organizations own pieces of the system of systems, yet it is unlikely that a single organization will own the entire system of systems.[6] Without an overall system-of-systems governance policy, it is likely that the individual system owners will develop policies according to their localized priorities, resulting in negative effects on the system of systems.

1.3 IMPACT OF DYNAMIC SYSTEMS OF SYSTEMS

Where systems of systems are intended to be dynamically composed, even an overall governance policy will be difficult to fashion. A number of current DoD goals focus on large associations of systems connected over a network, for which the concept of an enterprise is ephemeral. The enterprise may exist only notionally and for the time that various systems are interconnected. As a result, no single board or set of executives identifies the enterprise or business goals, and no one is made to adhere to any individual set of goals that are defined. In fact, there may be many sets of boards and executives with a variety of different and, perhaps, competing goals. If we look at the formation of a battle group or a typical expeditionary force, we can see that they are, indeed, ephemeral entities.

Thus, the community is quickly moving from a situation where an individual organization can govern its IT resources to one where an organization's systems will be increasingly interconnected with those of other organizations. These connections will be dynamic—quickly constituted to complete a particular task and just as quickly dissolved.

---

[5] At times, Maier has also included emergent behavior and geographic distribution in his system-of-systems characterization.

[6] Anecdotal evidence suggests that in the rare cases where a single organization does own the entire system of systems, the owning organization is too far removed from the details to exert control over the component providers.

2 Characteristics of Good System-of-Systems Governance

Following the example of Maier, we considered characteristics of good governance, instead of creating yet another definition of governance. Our initial list came from an examination of governance issues in a service-oriented architecture (SOA), and we modified it to account for the distinctions between a system of systems and an SOA. While it may expand in the future, the following list includes several necessary characteristics:

- collaboration and authority
- motivation and accountability
- multiple models
- expectation of evolution
- highly fluid processes
- minimal centrality

2.1 COLLABORATION AND AUTHORITY

When developing a single, stand-alone system, the program managers for both acquirer and contractor have control and authority within their organizations and can effectively enforce IT governance over the components they "own." Even when multiple organizations are involved, we often observe contractual relationships that define governance in a hierarchical manner. It is certainly true that within a system of systems, managers still can control what they own. However, as discussed by Carney and colleagues, ownership in a system of systems is a complex matter, with no single organization being in any position of ownership (and by extension authority) over the whole [Carney 2005a]. If some part of IT governance is about control, how can control be established across systems of systems that have distributed ownership? If authority is essential to the enforcement of IT policy, then without sufficient authority what will encourage independent organizations to adopt shared policies?

It is difficult to establish control over a large system of systems precisely because no individual or organization can have total authority—even when it appears that a single authority does exist. For example, the DoD may create a program with authority for the integration of constituent systems into a system of systems. Theoretically, this new program has some authority over the constituent systems and their associated stakeholders. But, in instances like that, the owners of the constituent systems inevitably have primary allegiance to their particular stakeholders. Even if owners of constituent systems are unusually committed to the system of systems, a single authority is likely to be ineffective since the size of the overall capability makes it virtually impossible to understand the nuances involved in effective control.

Thus, the only alternative is to facilitate community identification and adherence to a shared set of governance policies. As stated by Zadek (in addressing the problem of interaction between various governmental, nongovernmental, and private organizations), collaborative governance is

> *deliberative multi-stakeholder collaboration in establishing rules of behavior governing some or all of those involved in their development and, potentially a broader community of actors. . . . Collaborative governance could cover one or more of the elements of rule-setting, for example design, development, and implementation, including enforcement. The means of enforcement, importantly, might be non-statutory or statutory, or some combination that changes over time* [Zadek 2005].

Collaborative system-of-systems governance involves abandoning the notion of rigid top-down governance of IT processes, standards, and procedures and adopting peer-to-peer approaches. Such collaborative system-of-systems governance is clearly at odds with the natural tendency of business and military organizations, because it means that the "chain of command" must evolve to a "web of shared interest." Collaborative system-of-systems governance requires cooperation between separate authorities, even when there is no formal agreement. Carney and associates observed in a case study on infrastructure replacement that distrust between the two government organizations led to initial difficulties in the relationship between contractors [Carney 2005b]. [7]

In addressing the characteristics of collaborative governance among public and private sector entities, Freeman provides a model that we have adapted here to system-of-systems governance:

- **a problem-solving orientation**
  This viewpoint brings relevance and focus to the system-of-systems governance activities.
- **participation by interested and affected parties in all stages of decision-making processes**
  This democratic process facilitates effective problem solving and buy-in.
- **provisional solutions**
  Policies are recognized as being subject to revision, which requires willingness to move forward under conditions of uncertainty and to reconsider goals and solutions.
- **accountability**
  Traditional top-down oversight may be supplemented or replaced by self-disclosure and monitoring through community and independent (third-party) organizations.
- **a flexibly engaged agency**[8]
  A flexibly engaged agency works in many roles, as appropriate—including convener and facilitator of negotiation processes, provider of incentives for participation and sharing, technical resource provider, and funding source [Freeman 1997].

Freeman's model suggests how collaborative system-of-systems governance must differ from traditional authoritative IT governance. The model suggests new responsibilities for system owners

---

[7] The case study is indicative of problems that can arise without suitable governance.

[8] Use of the word *agency* here is not meant to imply a government agency, but some individual or group operating within a system of systems.

that will participate in the system of systems; it also argues for flexibly engaged "conveners" that represent the traditional authority figures in systems-of-systems development.

System-of-systems governance processes must take into account the governance policies of many, primarily autonomous, organizations. This allowance will require the adoption of more democratic governing processes, as suggested by Zadek and Freeman. Adopting those processes will not be easy, because individual systems are often components of multiple systems of systems. In these cases, an organization may be a party to negotiations for multiple system-of-systems governance policies.

To further complicate the issue, it is possible (and even easy) to create a system of systems where the owners of some of the participating systems are unaware of their participation. A simple example of this condition is the use of Global Positioning System (GPS) technology in a system-of-systems context. In this example, where use of GPS doesn't really affect GPS itself, the GPS owners are unlikely to become involved in collaborative governance. As a result, those constituents actively involved in the system of systems have to depend on the good nature of nonparticipants over which no authority can be exerted.

Since no single person or organization owns the entire system of systems, hierarchical control for the entire system cannot be enforced. Given this, no single person or organization will own the governance. Instead, governance will be created by the participating organizations in a collaborative manner and will be followed because it is in each organization's best interests to do so.

2.2 MOTIVATION AND ACCOUNTABILITY

Donahue distinguishes between **extensive** and **intensive** accountability [Donahue 2002]. Extensive accountability refers to making decisions and taking actions that reflect the diverse and possibly competing interests of many stakeholders. This contrasts with intensive accountability where decisions are made with a limited set of stakeholders in mind. Developers of component systems for use within a system of systems often have extensive responsibility; individual system owners typically have a narrower or more intensive accountability.

Most hierarchical organizations enforce accountability through imposed standards and coercion. In highly dynamic environments, these approaches can work initially, but they are hard to sustain. The challenge in those environments is to devise a structure in which the extensive accountability for the system of systems and the intensive accountability of individual system owners both can be accommodated. In a structure like that, individual system owners can choose to collaborate by building consensus.

Zadek identifies five learning stages that organizations go through to achieve the benefit of consensus through voluntary collaboration [Zadek 2005]. Key to Zadek's stages is the assumption that collaboration is not just a worthwhile goal (i.e., recognition of shared interest) but is essential to sustainable participation. Table 1 shows Zadek's stages, with the actions and motivations that typify them in a system-of-systems governance context.

Table 1: An Organization's Learning Stages and Corresponding Typical Actions and Motivations in a System-of-Systems Context

Stage	Action	Motivation
Defensive	Deny relevance of system-of-systems governance practices, outcomes, and responsibilities.	Defend against attacks to reputation in short term.
Compliance	Adopt system-of-systems governance policies as cost of doing business.	Defend against erosion of value in the medium term.
Managerial	Embed system-of-systems governance policies into core managerial practices.	Mitigate in the medium term and achieve longer-term gains by integrating into daily practices.
Strategic	Integrate system-of-systems governance into core strategies.	Enhance long-term value and gain first-mover advantage.
Civil	Promote broad participation in system-of-systems governance.	Overcome others' first-mover advantages and realize gain through collective action.

Table 1 not only shows what motivates organizations at different stages but also reveals what they may need to learn. For example, a defensive organization that claims common system-of-systems practices are irrelevant may need to be educated about threats to its reputation due to its lack of voluntary compliance. Or, an organization that has embedded consensus system-of-systems practices into its managerial practices but is not actively participating in the consensus process may need different incentives to move toward more active involvement.

At all stages, we need policies to give individuals and organizations the incentive to do the right thing. Until incentives are created for the system-of-systems viewpoint, existing incentives will discourage appropriate system-of-systems behavior. For example, incentives for program managers are based on bringing their systems in on schedule and within budget. Even reporting requirements (such as those in U.S. Code of Federal Regulations Title 10) are grounded in a **system-by-system view**. The incentives we need to develop may differ for different organizations—variances in the structure of award fees, for example. At the operational level, service level agreements (SLAs) can be useful as a basis for measurement, where performance against an SLA earns system-of-systems incentives.

Creating and enforcing[9] policies on incentives to promote the system of systems encourages individuals and organizations to take the wider view. At the same time, it is possible to create performance measures (e.g., a measure of the failures in interoperation between systems in the system of systems) that discourage poor system-of-systems behaviors. Making such performance

[9] Enforcing policies may be difficult in the system-of-systems context, particularly because no one group will have power of enforcement—hence the argument for making behavior visible.

measures visible[10] to all participants will discourage poor behavior, if only out of self-interest by the individuals and organizations.

2.3 MULTIPLE MODELS

While system-of-systems governance policies will certainly differ by role,[11] there might be additional variations. For instance, there could be a shift in focus from governance primarily at design-time (e.g., "Use standard X," "Document design by standard Y") to governance for deployment and use of capabilities. The U.S. Army software blocking policy (SWB) [JITC 2001] offers one instance of this aspect. It follows that there is also need for a model of governance at runtime, providing policies on how capabilities can, or should, be used.

The importance of acknowledging different types and levels of governance might arise from the relationship of the individual components to the entire system of systems. For instance, consider a relatively contained system of systems contracted and integrated by a single entity, Mack Trucks. Mack gets parts from many sources—it builds some parts, others suppliers build parts to Mack specifications, and still other suppliers build parts to their own specifications that Mack has adopted (e.g., Mack uses Bendix stability control systems, which are also used by International Truck and Engine, Kenworth, Volvo, and other truck builders). This situation is repeated across the automotive industry and in many other sectors.

An organization facing Mack Truck's situation cannot enforce a single governance model across all sources of parts. Instead, it could adopt a matrix view of system-of-systems governance capabilities for its parts supply. The matrix potentially needed for the Mack Trucks example could include

- the type of source for a part (internal, internally controlled but externally supplied, and external)
- phases in a part's life cycle (development, deployment, and runtime)

Classification by the source of components, however, might not be the best approach for highly dynamic systems of systems, such as those required to achieve the DoD concept of network-centric warfare via the GIG. The GIG provides ubiquitous connectivity throughout the military—including infantry soldiers, ground vehicles, command centers, aircraft, naval vessels, and spacecraft. This improved networking is expected to enable all elements to share information and collaboratively create a coherent, accurate picture of the battlefield. Because each unit "sees" the sum of what all other units "see," all enjoy a greatly increased awareness.

Within this sort of environment, concepts such as neighborhood (close collaboration by components around a particular task or mission thread) call for a more flexible classification. A single governance model might not be appropriate for all systems within a neighborhood or between neighborhoods of components in a system of systems. Without doubt, these neighborhoods will

---

[10] Publishing such data has technical difficulties that would need to be resolved. For example, there is a question of whether so doing would disclose proprietary performance data.

[11] An analogy to roles in a system of systems can be seen in SOAs, where the roles of infrastructure provider, service provider, and service user have been defined. For more information, see *Three Perspectives Required of Service-Oriented Architectures* at http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2006/01/eye-on-integration-2006-01.htm.

develop governance approaches tied to important requirements such as mission survivability and trustworthiness of information and information providers.

2.4 EXPECTATION OF EVOLUTION

Two forms of evolution must be considered within a system of systems: (1) evolution of the components and (2) evolution of the system of systems itself.

As we stated in Section 1.2, a fundamental characteristic of a system of systems is that its component systems will change at different rates and in an uncoordinated manner. An organization might impose system synchronization (e.g., with the SWB), but that authority can extend only to the limit of control. We have argued (see Section 2.1) that control is rarely established over the entire system of systems. Indeed, when an organization controls a large number of systems, it is unlikely that a synchronization policy can even be enforced over the entire span of control.

If governance cannot eliminate the independent evolution of components within the system of systems, we must use it to reduce the harmful effects of uncontrolled evolution by the component systems. Thus, policies must be created and enforced to provide rules and guidance for components as they change. In an infrastructure replacement case study, Carney and colleagues observed that no thought was given to the system of systems during the early development of the replacement for a legacy system. Specifically, though the developers of the replacement were instructed simply to develop the replacement, they knew that they were replacing most of the interfaces of the legacy system. Had the legacy system been replaced directly, the entire system of systems would have been unable to function. While the people who maintained that legacy system initiated the appropriate engineering to ensure that the replacement would not halt the functions of the system of systems, there was no requirement or guidance for them to do so [Carney 2005b].

At a minimum, governance for evolution should include rules and guidelines for

- informing other components systems (when known) [12] of the changes in the interfaces to and functionality of one system
- coordinating schedules with other component systems so that those that have to change can do so together (when backward compatibility of interfaces cannot be maintained)
- maintaining multiple versions of the system when schedules cannot be coordinated
- developing each system to insulate it from changes in other component systems
- minimizing the perturbations to interfaces when changing a system

The other form of evolution is that of the system of systems itself. While this may be directed, it will also occur, by default, when some new component system is added. If systems are simply added to the system of systems without forethought, sooner or later the unanticipated interactions between the various systems will create behaviors that are unanticipated and undesirable.[13] It is unclear exactly what policies are needed or how they can be enforced, particularly given that gov-

[12] It may not be necessary to inform all other systems of the changes in interfaces, but a minimum would be the other component systems known to be using the interfaces.

[13] In one case, the accumulation of systems into a system of systems led to a situation where, unintentionally, a sheriff's department gained access to medical records from a local hospital.

ernance must be distributed among the various owners. However, we would expect that some modeling of the pieces of the system of systems would be used to assess the effect of adding the new system.[14]

2.5 HIGHLY FLUID PROCESSES

Future systems of systems are expected to adapt quickly to different contexts and requirements and be highly dynamic—characteristics that will require flexible system-of-systems governance processes.

Planning for rapid changes in system-of-systems governance is needed. For example, governance strategies may provide a mechanism for adapting to rapid policy change, such as a way to relax security policies to achieve some urgent goal and then tighten them up again. Some notion of flexible enforcement of governance may also be useful in responding to a need for the rapid verification and deployment of an updated component or some critical situation.

Multilevel models (see Section 2.3) allow for the rapid adaptation of functional capabilities and governance policies at one level of a system of systems, while they support more carefully controlled evolution at other levels. System-of-systems governance policies for neighborhoods, then, might support the use of rapid processes for reaching local consensus and implementing changes. For example, a neighborhood of closely related systems might be the first to notice a problem with a current component or process and will need to respond quickly. At the extreme, where neighborhoods of related systems are themselves fluid, some details of system-of-systems governance policies might be negotiated. Other neighborhood governance policies might support wider dissemination of information about local changes to more remotely connected components.

Still, stability beyond the immediate neighborhood must be maintained. We would expect other portions of system-of-systems governance to support wider consensus and more stable policy, reflecting a larger and more diverse set of "neighbors" involved in determining appropriate governance for these issues. For example, we would not expect a global decision to migrate to IPv6 (Internet Protocol version 6) to be made in haste or in response to a rapidly developing condition. (Such a decision represents the relatively stable core of system-of-systems governance discussed in Section 2.6.) However, we can imagine local neighborhoods being allowed to respond to local conditions by moving to IPv6, as long as they maintain the agreed interface (i.e., IPv4) to more distant neighbors.

2.6 MINIMAL CENTRALITY

To this point, we have argued for a decentralized approach. However, there are two cases where centrality is likely to occur: (1) where there is a dominant system or organization in the system of systems and (2) in the system-of-systems infrastructure.

The first case can obviate the need for system-of-systems governance. For instance, a company that dominated a local market changed its business practices and then required all suppliers to comply with the new practices—under the threat of losing the company's business. Though many

[14] Modeling for systems of systems is, unfortunately, not yet a widespread practice.

systems were involved, the dominance of the one company meant that the system of systems behaved like a single system under the control of the dominant company.

In the second case, some level of centrality for infrastructure makes sense; without it, we recreate the Tower of Babel, with individual systems no longer able to communicate with each other. The infrastructure provider[15] provides governance by

- setting rules for becoming a part of the system of systems (e.g., the protocols to be used for communication)
- creating metadata repositories or system registries where the capabilities of a system are discoverable (such repositories and registries define the extent of a system of systems)

Of course, there can be more than one infrastructure provider in a system of systems. Consider the early days of the Internet when multiple providers (and nations) provided localized networks (e.g., Arpanet in the USA and the experimental packet switching system in the UK). In those days, each infrastructure defined the extent of the possible system of systems and enforced policy rules such as the structure of system names (which were ordered differently in those two systems). As networking technology improved, gateways were introduced that could route messages from one network to the other, even though the name structures were still different. Technology continued to advance, and today there are seamless connections between infrastructure providers. In the sense of governance, we have seen the various infrastructure providers progress from enforcing independent policies to enforcing a set of policies agreed by federation.

It is not clear what a system-of-systems infrastructure should be. However, if we extend our thoughts to a system of systems as large as the GIG, we can see that already we have three infrastructure providers (FORCEnet, LandWarNet, and C2 Constellation Net), each of which will be responsible for setting and enforcing policy for "their part" of the GIG. If the governance history of the Internet is a suitable analogy, we should expect to see separate policies for each of these components at the outset, with gateways connecting the various components. As time progresses and the various policies are tested in practice, we expect to see policies converge to a single model that is still governed by the three distinct governing bodies.

[15] In SOAs, one integration mechanism for systems of systems, the infrastructure provider identifies the network and communications protocols and standards to be employed. For more information, see *Three Perspectives Required of Service-Oriented Architectures* at http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2006/01/eye-on-integration-2006-01.htm.

3 Summary

The underlying purpose of system-of-systems governance is to ensure that the interoperation between the component systems will achieve the goals of the enterprise. However, when those goals become more diffuse as we expand our notion of the enterprise, we see that governance must change in nature.

We have presented a number of ways in which traditional governance models must change when acquiring, developing, and operating a system of systems. As such, the characteristics and, more importantly, the changes discussed provide measures of effectiveness by which existing, or proposed, governance strategies may be tested. The next steps in pursuing system-of-systems governance would be to

- explore each characteristic defined in Section 2 in greater depth, particularly with respect to developing true measurements of each characteristic
- look for additional characteristics of system-of-systems governance
- examine the governance strategies proposed by COBIT [ISACA 2006], OASIS [OASIS 2006], ITIL [OGC 2005], the Mercury IT Governance Center [ITG 2006], and others to be identified within the confines of all characteristics[16]

Finally, we should not expect to set out system-of-systems governance practices immediately. The IT community is only taking its first steps in the system-of-systems world and will make mistakes. As a community, we need to look at other disciplines—such as complex system engineering—to determine which governance strategies can be adapted for our use.

[16] COBIT stands for Control Objectives for Information and related Technology; OASIS is the Organization for the Advancement of Structured Information Standards; and ITIL is the Information Technology Infrastructure Library.

References

[Carney 2005a]
Carney, D.; Anderson, W.; & Place, P. *Topics in Interoperability: Concepts of Ownership and Their Significance in Systems of Systems* (CMU/SEI-2005-TN-046, ADA447053). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tn046.html.

[Carney 2005b]
Carney, D.; Smith, J.; & Place, P. *Topics in Interoperability: Infrastructure Replacement in a System of Systems* (CMU/SEI-2005-TN-031, ADA444901). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tn031.html.

[Donahue 2002]
Donahue, J. D. Ch. 1, "Market-Based Governance and the Architecture of Accountability," 1–26, *Market-Based Governance: Supply Side, Demand Side, Upside, and Downside*. Washington, DC: Brookings Institution Press, 2002 (ISBN: 0815706286).

[Freeman 1997]
Freeman, J. "Collaborative Governance in the Administrative State." *UCLA Law Review 45* (1997): 1–98.

[Glass 2006]
Glass, R. L. "The Standish Report: Does It Really Describe a Software Crisis?" *Communications of the ACM 49*, 8 (2006): 15–16.

[ISACA 2006]
International Systems Audit and Control Association. *COBIT 4.0*. http://www.isaca.org/template.cfm?Section=COBIT6 (2006).

[ITG 2006]
Mercury Interactive Corporation. *Mercury Project and Portfolio Management Center*. http://www.mercury.com/us/products/it-governance-center/ (2006).

[ITGI 2003]
IT Governance Institute. *Board Briefing on IT Governance, 2nd Edition*. http://www.itgi.org/Template_ITGI.cfm?Section=About_IT_Governance1&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=4667 (2003).

[JITC 2001]
Joint Interoperability Test Command. *Army Software Blocking Policy*. http://jitc.fhu.disa.mil/vmf_conf/2004_jul/docs/010918_armyblocking_approved.doc (2001).

[KPMG 2004]
KPMG International. *Creating Stakeholder Value in the Information Age: The Case for Information Systems Governance*.
http://www.kpmg.com.au/aci/docs/info-age.pdf (2004).

[Maier 1998]
Maier, M. "Architecting Principles for Systems-of-Systems." *Systems Engineering 1*, 4 (1998): 267–284.

[OASIS 2006]
Organization for the Advancement of Structured Information Standards. *OASIS Reference Model for Service Oriented Architecture V 1.0—Official Committee Specification approved August 2, 2006*.
http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf.

[OGC 2005]
Office of Government Commerce. *Introduction to ITIL*. Norwich, Norfolk, UK: August 2005.

[Standish 1994]
The Standish Group. *The Chaos Report (1994)*.
http://www.standishgroup.com/sample_research/chaos_1994_1.php.

[Zadek 2005]
Zadek, S. *The Logic of Collaborative Governance: Corporate Responsibility, Accountability, and the Social Contract*. (The Corporate Social Responsibility Initiative Working Paper Series: Working Paper #3.) Boston, MA: Harvard University Center for Business and Government, August 2005.
http://generativedialogue.org/documents/Logic%20of%20Collaborative%20Governance%20-%20Published%20PDF%20-%202005.pdf.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	October 2006	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
System-of-Systems Governance: New Patterns of Thought	FA8721-05-C-0003

6. AUTHOR(S)
Ed Morris, Pat Place, Dennis Smith

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2006-TN-036

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)
Systems of systems introduce complications for information technology (IT) governance because their individual system components exhibit considerable autonomy. This technical note examines the ways in which six key characteristics of good IT governance are affected by the autonomy of individual systems in a system of systems. The characteristics discussed are (1) collaboration and authority, (2) motivation and accountability, (3) multiple models, (4) expectation of evolution, (5) highly fluid processes, and (6) minimal centrality. This report examines each characteristic in detail and, where possible, provides guidance for the practitioner.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Governance, system of systems	22

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL