Engineering a Complex Information Enterprise: A Case Study Architecting the Department of Defense Hourglass

Dr. R. Miller and Dr. R. Cherinka
The MITRE Corporation
903 Gateway Blvd., Hampton, VA 23666
Phone: 757-896-8555, Fax: 757-826-8316
drbob@mitre.org, rdc@mitre.org

Keywords: Enterprise Architecture, Enterprise Information Management, Complex Adaptive System, Web Services, Service-Oriented Architecture, Semantic Web, Agile Development

Abstract

Based on Complex Systems Theory, Net centric operations for the US Department of Defense (DoD) can be considered a complex adaptive system, representing a shift from traditional system-based interactions toward information-based web service transactions requiring highly secure, reliable, and dynamic "on-demand" information capabilities. This net centric environment must accommodate unpredictable external factors that demand rapid response and flexibility to change. Current research suggests that typical "top-down" architecture approaches are not suitable for modeling complex enterprises, and suggests that new "middle-out" approaches, focusing on simplistic information interfaces should be considered. This paper presents an ongoing case study in constructing middle-out or "hourglass" enterprise information architectures to aid in modernizing the DoD toward global net centric operations. We discuss key principles of complex systems engineering to consider, insight into the DoD Net Centric Enterprise Data Strategy, and a middle-out architecture modeling approach to on-demand information based on web service and semantic web technologies. We also discuss techniques for hands-on architecture assessment and evolution, highlighting initial lessons learned using this approach.

1. Introduction

Complex adaptive systems are characterized as having unpredictable behavior, fluid requirements, multiple competing stakeholders, and are susceptible to external pressures that can cause change across the entire system.

In many ways, thousands of loosely-coupled transactions across the web, choreographed in synchronous and asynchronous ways to represent dynamic and highly complex business models can be considered a complex system.

The US Department of Defense (DoD) net centric environment is a good example of such a system, with many unpredictable external factors that often demand rapid response and flexibility to change [1]. Net centric operations for the DoD represents a shift from traditional system-based interactions toward information-based web transactions, adding the requirement for highly secure, reliable, and dynamic "on-demand" capabilities.

XML and web services are key technologies providing a foundation for this net centric vision. However, in order for an on-demand DoD to be realized, an evolution toward intelligent information exchange based on semantic web technologies as well as enhanced policy and resource management is required. This implies an evolution of the enterprise data strategy and IT infrastructure to support it.

Current research suggests that typical "top-down" architecture approaches are not suitable for modeling complex enterprises, and suggests that new "middle-out" approaches, focusing on simplistic information interfaces should be considered [8].

This paper presents an approach to modernizing toward global net centric operations that MITRE is helping the DoD to adopt [4]. We present an ongoing case study in constructing middle-out or "hourglass" enterprise information architectures to aid in this transformation. We discuss guiding principles of complex systems engineering to consider, provide insight into the DoD Net Centric Enterprise Data Strategy, and discuss a middle-out architecture modeling approach to on-demand information based on web service and semantic web technologies. We also discuss techniques for hands-on architecture spiral assessment and evolution using Communities of Interest combined with a Developer's Environment, highlighting initial lessons learned using this approach.

2. Background

Digital information rapidly is becoming integrated into all aspects of military activities. There is a goal across the

DoD to find new and better ways of managing information and providing capabilities in response to quickly changing needs. The DoD has a large number of legacy and emerging systems that are making great strides toward achieving that goal. They fall short, however, in a number of areas. Most of them are still large, monolithic systems, each of which has to provide a full information management infrastructure (transport, network, data, interface layers, etc). Because of this, there is only limited horizontal exchange of data amongst the systems--hence interoperability is a real problem. The systems are very configuration intensive and difficult to administer. Furthermore, they are not very tailorable to a given operational environment. Finally, these systems have a very costly life cycle. Once fielded, keeping these products up to speed with the state of the art requires very costly upgrades, and replacement outright becomes cost-prohibitive. For the most part, today's systems:

- Do not share a common conceptual basis.
- Share an acquisition environment which pushes them to be "stand alone,"
- Have no common control or management,
- Do not share common funding which can be directed to "problems" as required,
- Have many "customers," and
- Evolve at different rates subject to different (generally uncoordinated) pressures and needs.

Because of the above, managing an enterprise of such systems can be considered an unbounded, unpredictable engineering activity. As such there is a need to go beyond traditional systems engineering approaches [10, 12].

For this paper, we have selected a sampling of DoD enterprise systems that fit the above characterization to provide a basis for applying the middle-out architecture approach and to experience the lessons we highlight below. We purposely selected systems that comprise a variety of business domains and user communities so that we could observe a range of complex enterprises for this work. The domains we explore include logistics, command and control, time sensitive targeting, space navigation, and sensor networks. All of these can be consider complex adaptive environments and are use cases for migration toward the net centric environment discussed in this paper.

3. Emerging concepts on complex systems

Complex Systems are constantly changing. They respond and interact with their environments – each causing impact on (and inspiring change in) the other, usually through bottoms-up affairs, not top-down designs. Change ripples through complex systems causing local "pressures" among juxtaposed systems causing those systems to respond by undergoing change themselves. This is typically referred to as co-evolution, and in this way complex systems evolve - very much like what is seen within ecosystems. Some interesting characteristics of complex systems include:

- Dynamically assembled: often integrated from existing components
- Evolving requirements: typically articulated as vision statements or broad architectures.
- Emergent functionality/behavior: from the interaction of the components themselves w/o specific direction
- Crosses program boundaries: competition for resources & alternative solutions

Previous research has been accomplished to show that traditional systems engineering approaches do not work well when applied to complex adaptive systems [2, 3]. Instead, the notion of complex systems engineering has matured over the past few years as a way to address DoD enterprise engineering. Some key principles of this approach include:

- More emphasis on capabilities, less emphasis on requirements
- Focus on early discovery and evolution of composite behavior, functionality, and performance. This usually emerges upon integration and through the use of early prototypes
- Emphasize design guidelines, such as the use of layered architecture and open standards
- Use of rapid development spirals and experimentation, supported by establishing a collaborative engineering & integration environment, developing best practices with agreed-to context, and providing incentives to collaborate

Throughout the remainder of this paper, we discuss an overall approach to enterprise engineering DoD complex systems commonly referred to as Net Centric Operations.

4. Middle-Out Enterprise Architectures

Recent Gartner research suggests a new approach to Enterprise Architectures, known as a Middle-out or "Hourglass model" architecture [8]. While projects with a single, clearly defined purpose work well with a top-down planning approach, processes such as complex enterprises, with rapidly changing requirements do not. Furthermore, "bottom-up" approaches work well when you really can't plan for the future at all; however the downside is that they are very inefficient and often fragile because

decision-making is highly decentralized and uncoordinated.

In today's complex environments, when agility is the primary goal, a better approach is a "middle-out" architecture, which defines the decentralized principles for composing diverse micro-architectures into open-ended macro-architectures.

Architecting a system that is open ended both in terms of how it will be applied over time and how it will be implemented over time is the essence of middle out. Middle-out architecture is fundamentally concerned with uncertainty and innovation: enabling systems to deal with higher degrees of uncertainty by stripping away what is assumed to be certain, thus allowing new and innovative uses to emerge.

In the “middle-out” approach depicted in Figure 1, there are several key characteristics to consider:

- Minimize the waist by specifying only a few general-purpose interface specs
- Make sure the specs can easily be implemented across a wide range of existing technology
- Define interface specs in terms of simple generic “IfaP” descriptions (Identifier, Format and Protocol)
- Ensure that identifiers, formats and protocols are easily extensible

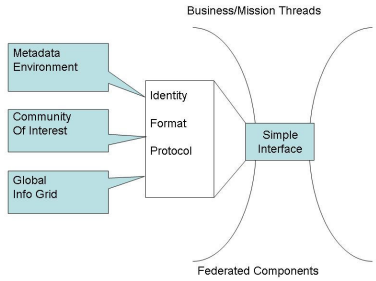

Figure 1. Hour Glass Model

5. DoD Enterprise Net Centric Data Strategy

Net-Centric Operations entails the networking of information producers (e.g., sensors), decision makers, and consumers to achieve shared awareness, increased speed and quality of decision making, and a higher tempo of dynamic operations. This concept of net-centricity motivates the following set of Enterprise Capabilities:

- Connectivity of users, applications and systems to shared, enterprise-wide services and information.
- Shared semantics and understanding of information across the enterprise.
- Unity of effort through distributed, collaborative operations and workflows.
- Predictable end-to-end performance across the enterprise.
- End-to-end secure enterprise operations.

In addition, Net Centric operations is about preparing for the unknown. We do not always know in advance what information will be needed or what collaborations must be supported, thus systems must support rapid customization, re-configuration and modification as required without significant delays to operations.

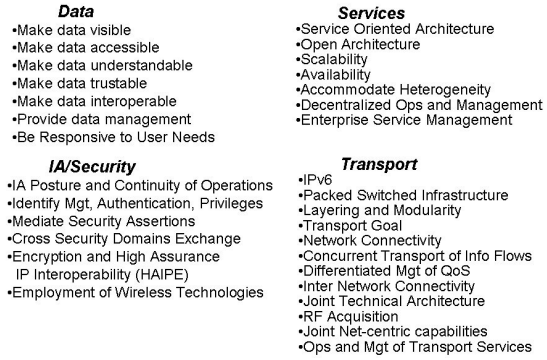

Figure 2. Net-Centric checklist

The Net-Centric Checklist shown in Figure 2 depicts the DoD’s overall strategy for achieving net-centricity across several categories: data, services, security and transport [13]. This checklist provides a basis for modernizing DoD systems and is based on several DoD and Industry best practices:

- Design application and system functionality as accessible and reusable services
- Expose service functionality through programmatic interfaces
- Maintain an abstraction layer between service interfaces and service implementations
- Describe service interfaces using standard metadata
- Advertise and discover services using standard service registries
- Communicate with services using standard protocols

A key component to this is the Data strategy which can be characterized by the following attributes:

- Ensuring that data are visible, available, and usable when needed and where needed to accelerate decision-making

- "Tagging" of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users
- Posting of all data to shared spaces to provide access to all users except when limited by security, policy, or regulations
- Protection of sensitive data to ensure that authorized users obtain reliable secure information, even in the presence of adversarial disruption
- Advancing from defining interoperability through point-to-point interfaces to enabling "many-to-many" exchanges typical of a network environment

As DoD systems migrate toward Net-Centric operations by adopting the above characteristics, it is envisioned that the enterprise as a whole will evolve as well with respect to systems adapting to this Net Centric environment. This will promote collaboration and intelligent information exchange across systems, and evolve toward seamless operational awareness via an on-demand, distributed computing environment.

6. Engineering the DoD Hourglass

In this section we discuss an approach currently being used to build "middle-out" or "hourglass" enterprise information architectures for a number of DoD enterprise programs. The fundamental steps in this approach include:

- Form a Community of Interest (COI) around the core business or mission
- Define the essential set of common "IFaPs." Map these to key information/communication products in the context of one or more mission/business use scenarios.
- Design a flexible Semantic SOA-based IT infrastructure
- Conduct hands-on agile capability development, assessment and transition to provide business value
- Incorporate enterprise architectures, strategies and agile processes into an organizational governance model

Several of these steps are discussed in more detail in the following sections.

6.1. Communities of interest (COI)

Interoperability, the ability to effectively share information and services, continues to be a difficult problem, both in the DoD and commercial endeavors. In addition, achieving a high level of interoperability is fundamental to realizing fully the benefits of Middle-out enterprise architecture. In today's complex environments organizations will communicate; build systems, services and interfaces; and transport, describe, and structure data in diverse ways. Interoperability requires that information producers and consumers come to terms with their vocabularies and manage their data and metadata so that both the provider and consumer have the same understanding of what the information means and how it is used. Interoperability also requires that these same producers and consumers define, manage, and register the service specifications to meet the requirements of an information on-demand, net-centric architecture.

Attempts at data and vocabulary management often lean towards top-down data standardization; that is require organizations and services to implement the same data definitions and knowledge representations (vocabulary). Over the years, the DoD has invested heavily in common vocabularies with some successes. But the goal of being able to share information widely remains elusive due to such factors as differences in culture and business practices. There is a large cost in designing, implementing, and maintaining standardized data structures at the enterprise level. Further, it is increasingly costly for DoD systems to keep up with the pace of change in implementing these large vocabularies.

More recently the DoD is fostering vocabulary agreement on a smaller scale through a Net-Centric Data Strategy (NCDS) [6]. This strategy, designed to support the information exchanges found in loosely-coupled, complex system environments, fits well with the Middle-Out architectural approach. The NCDS seeks to make all sharable data visible, accessible, understandable and interoperable by capturing and registering the associated metadata and posting all data to shared spaces to provide access to all users except when constrained by security, policy, or regulations.

The central component of the NCDS is the Community of Interest, or COI. DoD COIs are similar to communities of practice with in the commercial sector. COIs consist of information providers and consumers who must share information in pursuit of shared goals, missions, or business processes. Some COIs may be large functional or cross-functional groups, while others will be smaller more expedient groups focusing on some more localized mission need or process. Regardless of their size, COIs will consist of information producers and consumers, as well as system developers whose role is to implement the NCDS and specify those services required for COI participants to interoperate.

From the "hourglass" model perspective, each COI must take responsibility for the vocabulary that the community uses to share information. This is done through data dictionaries and models, and data formats such as XML schema, typically managed by the COI's

Vocabulary Panel. The vocabulary panel thus provides the format (message, container) portion of the IFaP.

Currently there are approximately 65 COI's registered within the COI Directory maintained by the DoD CIO (Assistant Secretary of Defense/Networks and Information Integration). The authors have been consulting with several DoD COI's including the Air Operations, Space Situation Awareness, Time Sensitive Targeting, Global Force Management and Maritime Domain Awareness COI's, to review their vocabulary development process [7, 9]. A major problem is variation in data/metadata specifications for common concepts (e.g., location coordinates) across various COI's, resulting in stovepipe message (XML) schemas usable only for point to point interoperability solutions. Under the Secretary of the Air Force, in order to maintain consistency, an Enterprise Vocabulary Team (EVT) has been stood up to help COI's specify and organize their vocabularies through a common methodology, the purpose being to have consistent and reusable vocabulary products. This supports the NCDS information sharing goals of making data visible, accessible, and understandable.

6.2. Metadata Environment (MDE)

One of the difficult problems in information sharing is being able to search for and discover the needed information in the first place. The identifier portion of the IFaP provides a means (address, reference, or name) to support search and discovery. A common specification for the description of information assets allows for a comprehensive capability that can locate all information assets across the Enterprise regardless of format, type, location, or classification [14]. Data must be labeled or tagged in such a way that it can be identified (made visible). Security tagging or other protection mechanisms help make sure that the right users have access to the data. Semantic metadata assists in understanding the data that is accessed.

In the net-centric enterprise, users and applications discover and access information assets through both core and mission specific services (SOA). The core services will be provided through the Net-Centric Enterprise Services (NCES) concept. Enterprise services include discovery, messaging, mediation, and collaboration services. Mission specific services will build upon these core services to provide the mission capabilities needed to support net-centric operations. As specified in the DoD Net-Centric Checklist, these services must be built on open standards (e.g., WSDL), be scalable, discoverable, accommodate heterogeneity, and support decentralized operations and management. Services must also be discoverable and accessible. Consequently, appropriate service metadata must be captured and maintained in service registries (e.g., UDDI registries).

The DoD Discovery Metadata Specification (DDMS) provides the discovery metadata requirements to support enterprise discovery of information assets. [5, 14] The DDMS provides a core set of metadata elements that are associated with each information asset to support search and discovery. The DDMS schema captures pertinent metadata as a collection of elements. These metadata categories include security (e.g., classification level), resource (e.g., title, identifier, creator, date), summary content (e.g., subject, geospatial coverage), and format (e.g., media).

DDMS metadata about an information asset is recorded through "metacards" similar to the library cards used to catalog assets (books) in a public library. These are stored in metadata catalogs that can be searched to discover sharable information. For information assets such as databases, catalogs, and services, the specification does not mandate descriptions down to the data element level, but provides for that if desired.

In developing its vocabulary, a given COI defines the metadata necessary to exchange (structural metadata) and understand/process (semantic metadata) mission information. The COI determines the mission services it needs to permit access to the community's sharable data. Description of these services is cataloged and maintained in service registries. The COI also specifies the process to record and capture discovery metadata (the metacards) about its information assets. All of this metadata is captured in federated registries for reference.

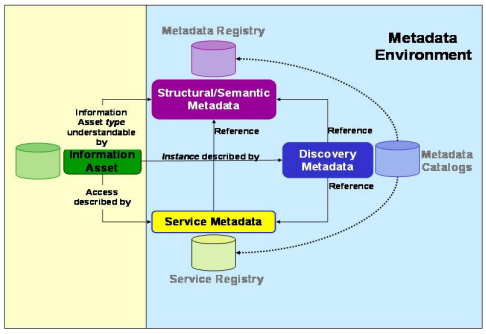

Figure 3. Metadata Environment

Figure 3 depicts a Metadata Environment to support search and discovery. This run-time environment consists of loosely coupled, federated components (registries) instantiated across the Global Information Grid. It is used to allow the COI's to express and maintain accurate (types) of metadata and metadata relationships about people, services, and available information. The environment allows users and systems to discover and use available information assets to obtain content, build a

service (orchestration) or implement a mission thread. The MDE treats all information assets the same, providing a consistent description of the asset through the same set of metadata, and managing all that metadata through a common set of services.

Several of the DoD COI's are now defining their metacard production process, but much work needs to be done to achieve a consistent approach. For example, the TST COI has documented a draft metacard population specification intended to help information asset providers, such as web service developers, produce metacards that will allow users to find those services and query for data pertinent to their area of responsibility. The basic approach is to map the COI's vocabulary (data elements and metadata) to the DDMS schema. Some DDMS elements are mandatory; the mapping for these elements must be consistent across all COI information products. Other DDMS elements are optional or extensional (i.e., unique to a particular COI. The extended portion of the metacard would typically only be useful to members of that COI and would be ignored by other communities.

For a web service developer, the COI's vocabulary is used to implement the service's information interface (how to request data and how the data is returned). Some metacard elements are populated via the elements in the service's information interface (e.g., location, description), while others (e.g., creator, date) are populated with data pertaining to the service itself. Some DDMS elements could be viewed to be populated both from the service description and from the service's interface schema; security classification is an example. More research and experimentation is needed to determine the best approaches for metadcard generation.

6.3. Semantic SOA-based IT Infrastructure

As depicted in Figure 4, it is envisioned that net centric operations across the DoD would consist of a 3-tier IT infrastructure. This provides the protocol portion of the IFaP by implementing the common protocols (e.g., IP, HTTP(S), SOAP, RSS, etc.) prescribed for use across the Global Information Grid and individual managed computing environments (nodes).

The first tier is based on the widely adopted Service Oriented Architecture (SOA). By making capabilities available in this way, they are more easily accessible to a higher number of applications and users through federated advertisement and discovery services. In addition, with capabilities transitioned to services, business processes can be modeled as portable workflows, using emerging open workflow standards. These workflows can also be registered and discovered for re-use.

The second tier is based on the addition of semantics to web services in order to achieve intelligent information exchange (IIE) across the DoD enterprise. As discussed in the literature, the additional semantics enables the use of knowledge representations (e.g., ontologies) and architectures based on publish/subscribe/query interaction to locate and transfer information objects in an optimized fashion. Investments in the SOA can be leveraged when adopting ontologies by using related open standards such as Resource Description Framework (RDF) and Web Ontology Language (OWL). These concepts combine to support an information brokering system. With a broker, information can be advertised, discovered, transformed and shared.

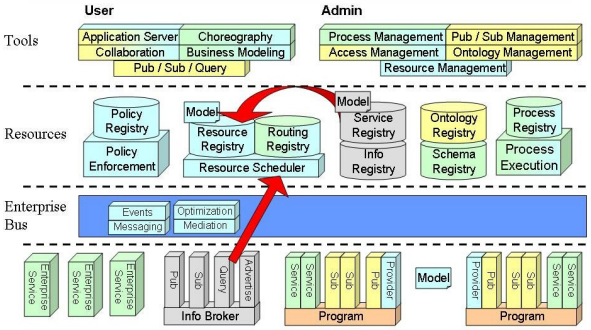

Figure 4. Managed Computing Infrastructure

The third tier, on-demand computing (ODC), enables a highly optimized and reliable service and messaging infrastructure, to include resource and policy components [11]. This will ensure overall performance across the DoD enterprise. The infrastructure required to enable on-demand computing builds on IIE and the SOA by extending the abilities of existing resource and applications while also providing new capabilities.

6.4. Agile Capability Development & Assessment

Net Centric Operations as a complex system has an effect on the DoD acquisition process, and to adequately address development and integration of complex systems, there is a shift of emphasis from building one-of-a-kind solutions to putting in place an environment and set of processes to help in the development and maturation of capabilities as they transform from innovation to fielded capability. In this section, we discuss the use of Developer's networks or environments in conjunction with user workshops to provide hands-on continuous capability assessment.

Across the DoD several developer's networks are being matured as a way to address complex systems challenges. The intent is to create an environment where researchers, developers, testers, and users can meet and exchange their ideas, code and expertise as they experiment and productize new capabilities. The focus is on creating an environment and process (rather than a

product) that facilitates 3rd party participation, eases entry and exit into the baseline of a system and minimizes integration "touch time" to achieve interoperable and integrated (loosely coupled) capabilities.

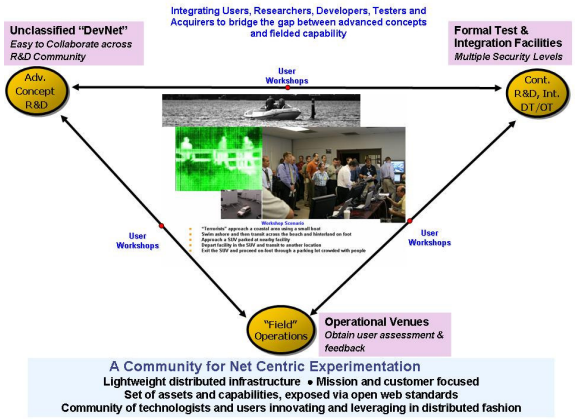

Figure 5. User Workshop Process.

Figure 5 represents the user workshop process that we are employing across several customer communities. This process relies on a maturing set of SOA-based distributed computing resources to provide an environment for community stakeholders to mature and assess capabilities from advanced concepts through test & integration and ultimately operational evaluations. The key to process is the frequent use of themed user workshops to drive integration spirals and limited objective evaluations that provide value in two important areas:

- hands-on user immersion into emerging processes, concepts and capabilities
- facilitated discussion to drive concepts, requirements and transition opportunities

The environment helps to integrate the user and developer through knowledge sharing, providing a process of evaluation, a mechanism of reward, common understanding of safety constraints, as well as rules for cooperation and competition. Typical uses include:

- Providing access to existing systems to support R&D efforts
- Providing various development levels of infrastructure, applications, and services
- Providing core services and infrastructure (e.g., service registries, brokering technologies, security) to enable rapid deployment, discovery, and usage
- Publishing guidelines for information service creation and usage based on accepted industry and government standards
- Enabling user and provider discussion and feedback channels for collaboration (e.g. forums)
- Ensuring usage and testing in operational context

Finally, this environment supports the collaborative documentation and understanding of requirements (e.g., certification) and procedures for transitioning services into production spirals for a system.

7. Lessons Learned

Based on our experience, the following observations are made about what seems to work well from adopting the approach discussed in this paper:

- Architectural frameworks, vision documents, architecture products (UML), and technical roadmaps help manage and engineer the mega-system
- Continuous involvement from COI members, and gaining consensus around infrastructure and tenets
- Active involvement of senior leadership and representative organizations
- Use of open standards, common vocabularies, capturing metadata
- Spiral development and Experimentation
- Developer's Network , integration facilities and environments (virtual and real)

Likewise, the following observations are made about what does not work so well:

- Difficulty in capturing requirements, especially in trying to describe how parts will work in context of the whole
- Implementing a common strategy across multiple stakeholders and getting everyone on a convergent path. Stakeholders need better guidance and criteria on implementing web standards & technologies
- Managing expectations and dealing with uncertainty (managing risk) across COI members, users, and senior leadership
- It still takes too long to the field capabilities, resulting in constant technology, expectation and user changes
- There is a lack of availability of core utility and mediation services
- Outdated Security policies which still serve need to know instead of need to hide approaches

Based on our experience, we can offer the following recommendations to anyone considering a similar approach:

- Need to establish a sense of community across all stakeholders

- Need buy-in and ownership from all levels of stakeholders as adopting the middle-out approach forces change across the organization
- Need to continuously educate your community members on using and embracing this approach
- Allow customers to own and influence the hands-on spiral capability assessment process
- Remember … less is more; When in doubt, leave it out so others can fill it in
- Maximize loose coupling at the edge by minimizing tight coupling at the center
- Everything via URI's and URI's for everything
- Design for the unexpected rather than immediate purpose
- Strive to take away constraints
- Empower stakeholders to innovate

8. Conclusions

Migrating to Net Centric operations will demand an unprecedented degree of cooperation and coordination among all stakeholders. Efforts will be started at different times in different places but will all need to be brought into line. While Web services standards and technologies enable interoperability, they do not guarantee it. Complex systems theory and extensive experience demonstrate that sufficiently complex systems need evolutionary engineering strategies.

In this paper, we presented an ongoing case study in constructing middle-out or "hourglass" enterprise information architectures to aid in modernizing the DoD toward global net centric operations.

In the "middle-out" approach, business drivers and strategic vision are first employed to set clear direction and priorities. Based on these, the organization takes multiple iterative steps to build out slices of end-to-end capabilities. Leveraging service-oriented architectures, this approach is focused on rapid time-to-value, and it delivers business results through iterative, incremental steps that facilitate close alignment of IT resources with changing business conditions.

We believe this approach is very promising, and does allow for an organization to start thinking about their complex environment in new ways. It also allows for a minimum essential set of architectural products to be developed that can start to document the important interfaces across an enterprise and be used to guide hands-on capability spiral development, assessment and transition.

9. References

[1] D. Albert, J. Garstka and F. Stein, Network Centric Warfare, CCRP, 1999.

[2] Y. Bar-Yam, Dynamics of Complex Systems, Perseus, 1997.

[3] Y. Bar-Yam, When Systems Engineering Fails---Toward Complex Systems Engineering, 2003 IEEE International Conference on Systems, Man & Cybernetics, October 5–8 Washington, D.C., USA, 2003.

[4] R. Cherinka and R. Miller, Lessons Learned in Using Web Services for Enterprise Integration of Complex Systems in the Department of Defense, International Conference on Systematics, Cybernetics and Informatics (SCI), July 2004.

[5] Department of Defense Discovery Metadata Specification (DDMS) Version 1.3, Deputy Assistant Secretary of Defense/ Deputy Chief Information Officer, 29 July 2005

[6] Department of Defense Net-Centric Data Strategy, ASD/NII, 9 May 2003

[7] D. Edwards et. Al., United States Special Operations Command C4ISR Enterprise IT Framework Report, The MITRE Corporation, March 2006.

[8] N. Gall, Top-down Architecture is Dead: Long Live Middle-Out, Gartner Symposium ITXPO 2006 Presentation, October 2006.

[9] R. Miller, M. A. Malloy, E. Masek, and C. Wild, Towards and Information Management Framework, Information Knowledge Systems Management Journal, Vol. 2, Number 4, Autumn 2001

[10] J. Moffat, Complexity Theory and Network Centric Warfare, CCRP, 2003.

[11] C. Nicodemos and A. Damianou, A Policy Framework for Management of Distributed Systems, PhD Thesis Imperial College of Science, Technology and Medicine, University of London, Department of Computing, London, 2002

[12] D. Norman and M. Kuras, Engineering Complex Systems, MITRE Technical Report, 2004.

[13] OSD/NII Net-Centric Checklist, Version 2.1.3, 12 May 2004

[14] H. Reed, MDE Objectives and the Enterprise Context, USAF Presentation, Dec 2006.