

# The SOA Magazine

## Feature Article



### SOA in the DoD

by Howard Cohen and Josh Taylor

Published: June 16, 2008 (SOA Magazine Issue XIX: June 2008)

[Download this article as a PDF document.](#)

*Abstract: The United States Department of Defense (DoD) understands the value of information. While this understanding is very clear, it does not yet have a fully functional or satisfactory prescription for the strategic and technical ailments that pains its communities. Service-oriented architectures are not magic but the concepts, if applied with logic, leadership and continuity, make sense. Any mission or objective must be clearly defined with planning and the use of blueprints to build solutions that have meaning to those who will be served. There is disparity in data across domains within the DoD, but there are emerging ideas and technical strategies in development to address this issue. And SOA is a key part of this solution.*

### Introduction: The Need for SOA Within the DoD

The challenges faced today in the DoD are well beyond anything that has been seen in the history of warfare. The DoD is attacked every day by foreign and domestic agents with designs on exploiting any weakness hidden in its information technology.

Information is much more than a fundamental requirement for the United States and its Allies. Information superiority is key to its success, not only in relation to the military but also for its position as a global leader. The DoD is well aware of the value of its information. The primary obstacle to successfully leveraging this data is that it has simply become detached from consumers that have the right and authority to access and use it.

This issue has been addressed at the highest levels of government by use of policy and guidance. However, these initiatives often tend to lag implementation by early adopters or experimenters. It takes more than unified policy to fix the "data service-to-consumer detachment" that is often suffered by the joint/coalition war-fighter. In this respect, the fundamental gaps have little to do with policy, which is always evolving, and almost nothing to do with technological, human or militia power. The gaps are adequate business planning, process modeling, and operational, technical and strategic communication, collaboration and cooperation across U.S. and joint/coalition forces. For the first time, the DoD has an effective technical architecture approach with SOA, along with the technologies that will facilitate the filling of these gaps.

Yet, SOA is not a "catch all". Vendors would have a consumer believe that the magical tech genie will come out of the bottle to resolve all ails, yet this is untrue. The DoD recognizes that information must be visible, accessible and understandable to the right people at the right time, which is a very serious ailment. They have to share information while compartmentalizing it, which is the historical way of doing things. SOA offers a business and engineering approach to achieving this, but it's not all perfect. Even identical technologies may not interoperate with one another based upon how they have been implemented. The likelihood of this is greatly reduced in SOA-based environments, but occasionally it still happens.

While there is also disparity in data across domains within the DoD, there are even sometimes interpretability issues within the same domain. Many of these data-related representation and context issues reach beyond ideas

established within SOA and look very much like issues the artificial intelligence community has been seeking to address for many decades. Specifically, Natural Language Understanding (NLU), Semiotics, and the original Universal Ontology efforts (which were never successful and today look more like "domain" ontology's vice a grand universal ontology).

The work being carried out in relation to SOA initiatives within the DoD that is best seeking to address this disparity is found within both the data modeling and service modeling communities, and even there not all technology and data issues are being adequately addressed. Disparity still surfaces and it is clear that there is a measure of maturation that needs to take place in both the technology and human knowledge ends.

It appears the way ahead in this maze is straight through the boundaries that contain it. DoD is taking specific actions to resolve whatever current ails are pressing in order to better prepare for the future of information warfare. The next step is to continue building improvements into current capabilities using the pieces of SOA and service-orientation that work best and passing the shortfalls back to industry and the educational community for prospective new solutions. Continuity and standards will need to be addressed along with the assignment of organizational roles and necessary policy and guidance mandates for enforcement.

Looking across the numerous efforts around SOA in the DoD, one can see the capturing of many details within the department that have been poorly understood in the past, or down right neglected.

SOA is proving quite useful in areas such as:

- the discovery and understanding of business processes that were once a mystery
- data that is highly useful to a war-fighter but was previously unknown
- the discovery of excessive redundancies and overlaps in various capabilities
- new ideas in how to use the abundance of information at a war-fighter's fingertips which never existed before

The use of SOA in the DoD is now appearing to lead to two greater rewards than these:

- the improvement in asset management
- more effective information delivery to war-fighters

There is still quite a large crevasse between current capabilities and achieving what Hollywood depicts as an über-efficient "big-brother" coordination and collaboration network of entities. But SOA is the great leap forward and we've already left the ground.

The technical aspects of SOA in the DoD are only part of the solution. The business side of a service-oriented enterprise must, of course, also be addressed. The real foundation of SOA is in the business concepts that drive the enterprise.

The Office of the Assistant Secretary of Defense Network Information and Integration division (OASD/NII) is the primary organization engaged in ensuring that the technical aspects of SOA continually meet and remain in alignment with the business requirements. The program dealing with the technical foundation and strategy for service implementation is known as "DISA Net-Centric Enterprise Services" (NCES) [REF-1]. DISA (the Defense Information Systems Agency) and the DoD are developing the technical and governance standards for use across the domains. The ultimate responsibility for all of the business and technical strategies for enterprise-wide information sharing live at the DoD CIO's office [REF-2].

### **The DoD's Approach to Service Inventories**

An Enterprise Inventory established through the Enterprise Inventory Pattern [REF-3] for SOA requires some key, well-defined, basic products that adequately capture the functions and offerings across the enterprise. These are the products that are mostly visible to the consumer and are generally comprised of:

- a canonical data model (visible in pieces through the service offerings)
- normalized services

- centralized logic (within the organization)
- business objects/entities and their definitions
- an inventory and its access point

... and other various service agents like utility and application services that may not be directly visible to the consumer but are essential for the production of automated capabilities. There are further aspects to an enterprise inventory relating to the development of different contexts throughout the organization that are seamlessly part of these basic products. However, a detailed discussion of an enterprise inventory as it relates to the Enterprise Inventory Pattern for SOA is beyond the scope of this particular article.

What is most critical to understand about this important pattern is that like every other architectural and software pattern that has been identified, it is only apropos for a relatively narrow range of possible solutions, or appropriate only at certain times when influenced by the highly dynamic, natural world we live in. The Enterprise Inventory Pattern is most suitable for those enterprises that provide a specialized range of offerings. Naturally, specialization results in a narrow expression of possible "contexts" in which your product offerings can be captured and provided to the consumer. This range of contexts under which an organization provides capabilities to its consumers dramatically impacts the prospects for implementation of the Enterprise Inventory Pattern.

On a larger scale, an enterprise as large as the DoD is far too broad in its capabilities to capture a single enterprise model and approach for all the activities it undertakes. This makes identification and implementation of an Enterprise Inventory that fits nice and neatly into a standard Enterprise Inventory Pattern impossible.

What follows then is the establishment of solutions which are implemented in the Domain Inventory Pattern [REF-4]. The Domain Inventory Pattern is an extension of the Enterprise Inventory Pattern. What happens in this pattern is the establishment of domain based inventories. The following is an excellent example that shows the need for and impact of domain inventories.

## Domains at the DoD

DoD is famous for the various "domains" under which it has conducted business for the past century or so. Domains like intelligence, special operations, command and control, battle-space awareness, situational awareness, network operations, etc. have played a natural, unintended, and surprisingly significant role in evolving the DoD's business over the years into "information stove-pipes."

These domain based stove-pipes were not intentionally designed to be so closed off from one another. They were, in fact, a natural expression of business activities that founds themselves within a massive organization. What happened over time, though, was a lack of data sharing across the domains. Recently that has been changing with the establishment of DoD's metadata registry and service registry implementations being managed by DISA, and its larger, enterprise-wide policy to become more "net-centric."

Domains are the result of at least two processes:

- people or organizations using data and services in different ways for different purposes and hence developing different contexts, and
- people or organizations using their own specific data and capabilities to address their specific needs

(These two key points might actually form the basis of two types of domain inventories as yet undiscovered and undefined.)

For example, a battlefield commander isn't going to want to use an accounting data model or services to describe what he needs to do on the battlefield, nor is he likely to use data and services specific to network operations to attack an enemy tank. He is operating in his battlefield domain. The best way to communicate within any particular domain (military or not) is to use the least amount of information in its most effective manner to accurately describe what's happening and get things done.

This is what the end-result of services being provided in a domain inventory do. What this commander would want to have at his fingertips is an inventory of capabilities that allow him to take out the enemy before the same happens to him. That inventory of capabilities might actually use something from the intelligence and situational awareness

domains, but it is spun into a battle-space awareness context for the battle-space awareness domain in which he operating.

Domain inventories capture critical divisions or groups of operations within an enterprise which are purposefully distinct from each other, enough to warrant capturing their own contexts for usage. In essence, these are "little" enterprises within the larger enterprise. There really aren't any well defined rules for determining when, where or how this happens. Generally, looking at the natural divisions within an organization can lead to clues as to how to divvy up services among the domains, but this does not mean that all services will be domain-specific nor particular to any one domain. The evolution of a large organization's domain inventories may lead to some surprising results that aren't naturally evident. It is therefore wise to be aggressive in questioning how specific services should be offered.

Within the DoD, mature domain inventories haven't fully surfaced yet, though the natural divisions among service offerings, data owners, and the contexts under which business processes occur are happening everywhere. Key activities have been in the identification of Communities of Interest (COIs), and hypercritical business activities, like those in the intelligence community.

The tools available for producers in the enterprise are mostly the Metadata Registry (MDR) and the Service Registry. Within these tools, especially the MDR, there are now partitions for domains like command and control, network operations, etc. These partitions are beginning to resemble a domain inventory that has been implemented under the Domain Inventory Pattern, but is rather more informal at this time.

## Conclusion

SOA is just now starting to spread its wings within the organization. Domain partitions are no longer comparable to the old stove-pipes of data, in that they are much more visible, accessible, and interoperable with each other than ever before. This is leading to some new, extremely exciting and effective ways to use information that simply weren't available before the advent of SOA and service-orientation.

When it comes to leveraging the what SOA has to offer, the real question is not tied up in the technical methodology used to create a mature service-oriented constructs because these methodologies are well-vetted. It is in our leadership's ability to take these methods and apply them in a meaningful way. Information superiority is the key to winning the war on electronic terrorism and overcoming future conflicts where and whenever they occur. SOA concepts empower our leaders with the potential to meet every war-fighters individual requirements. This leads to the very real opportunity to "live in the possibilities" and create services for our war-fighters that have traditionally only existed in commercial applications.

Finally, it is important to understand that all of the benefits we've be describing can be had by any organization. All it takes is a willingness to invest the proper time and resources into developing what is required for a mature SOA implementation. An important first step is recognizing and addressing the critical decision point of determining whether you will proceed with the Domain Inventory or Enterprise Inventory approaches.

## References

- [REF-1] DISA Net-Centric Enterprise Services, <http://www.disa.mil/nces/index.html>
- [REF-2] DoD Chief Information Officer (DoD CIO) <http://www.defenselink.mil/cio-nii/cio/index.shtml>
- [REF-3] SOA Design Patterns, "Enterprise Inventory Pattern", [http://www.soapatterns.org/enterprise\\_inventory.asp](http://www.soapatterns.org/enterprise_inventory.asp)
- [REF-4] SOA Design Patterns, "Domain Inventory Pattern", [http://www.soapatterns.org/domain\\_inventory.asp](http://www.soapatterns.org/domain_inventory.asp)

