

Technical Reference Model for Network-Centric Operations

Bradley C. Logan
The Boeing Company

The majority of today's weapon systems are platform-centric; they work well within the same weapon system's environment, but do not readily collaborate with other weapon systems. The Strategic Architecture Reference Model (SARM) is a communication and information architecture framework based upon commercial and government interface standards. Organized to address system-wide network design issues, such as information assurance, the SARM is an enabling technology framework to allow platforms and systems to interface to the Global Information Grid as interoperable nodes on the network. This article discusses the benefits of having a SARM for platforms and systems, what is done with it, what should be in it, how to understand its structure, and how to use the SARM.

One thing agreed on among military strategists is that dominance on the 21st century battlefield will be driven by information superiority. Those who generate, manipulate, and use information in a precise and timely manner will dominate the battlefield of the future. The key to such superiority is network-centric warfare:

Network-Centric Warfare (NCW): We define NCW as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace. [1]

However, NCW is not just about connecting weapon systems together on a communications network. It is about utilizing the connectivity of the network to transform operations doctrine. This is done by rapidly gathering raw data from across the network, then fusing it together to transform data into information about the battlespace. This correlation of information from across the network transforms it into an understanding of the battlespace threats and assets. NCW is about the timely utilization of that knowledge of the battlespace state and events to rapidly make better-informed decisions, both proactive and reactive. NCW is about letting computers do what they do best, moving and manipulating data, and letting humans do what they do best, making informed decisions.

For example, recent operations in

Afghanistan and Iraq touched the tip of the iceberg for transformation with voice communications letting a soldier on the ground request and guide air strikes from air assets flying combat air patrol missions. Network-centric operations (NCO) is about speeding up that process through automation with the players as networked nodes; with intelligent software taking sensor data in, analyzing it, looking for the

“Network-centric warfare is about letting computers do what they do best, moving and manipulating data, and letting humans do what they do best, making informed decisions.”

best effector assets on the network; and dispatching tasking orders in a fraction of the time.

While this article focuses on military applications, the principles of NCW apply to civilian applications such as police and fire-first responders. For the broader application, we use the term NCO.

Stovepipe Systems

While some weapon systems can work together, most of today's deployed systems are islands of self-contained connectivity, or *stovepipe* systems. That is, those weapon systems components that were designed at the same time to work together can communicate and exchange data, but that is the extent of their network connectivity. At best, communication with

a disparate weapon system developed at a different time on a different contract is difficult and time consuming. This is a vastly different vision compared to NCW where weapon systems rapidly and easily work together in large Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems.

The proliferation of wireless communication systems using different protocols, the difficulty for coalition forces to communicate over such systems, and the difficulty of coordinating both police and fire activities on Sept. 11 are examples of the present state of stovepipe systems both military and civilian. The enabler for NCW is the *interoperability* of disparate weapon systems to form systems of systems (SoS).

Interoperability: The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. [2]

Boeing Strategic Architecture Initiative

Moving to NCW via significantly increased levels of interoperability will be a transformational process. The Boeing Strategic Architecture organization was created and chartered to integrate all of Boeing's platforms, systems, and programs into a single common communication and information framework.

The main thrust of the organization is to create, control, and disseminate the Strategic Architecture Reference Model (SARM), a communication, information, application, and presentation architecture framework. An enterprise-wide central organization that has access to all programs and a cross-program perspective

ensures a system-wide architecture to directly address key network and node design issues.

The Strategic Architecture organization is also forming an industry consortium¹ of infrastructure providers and users to promote adoption of the framework across non-Boeing products and to ensure the framework is developed and evolves with the best industry practices and products. The intention is to create open industry standards of the interoperability infrastructure lower levels via the consortium. Contractors then compete at the higher levels of the model where their application domain expertise provides added value and the open infrastructure provides a common foundation upon which the applications are built. Thus, the SARM is an enabler for SoS interoperability.

Vision to Achieve Information Superiority

The Global Information Grid

Computer networks are transforming business processes globally by allowing closer and more rapid collaboration and coordination both internally and externally among a business, its suppliers, and its customers. Timely network access to data from its business environment allows executives to correlate, fuse, and transform the data into critical operating knowledge used to make timely informed decisions, and allows using the same network to disseminate directives to effect change to achieve business goals.

This paradigm applies across organizations where data are gathered, processed, and acted upon: commercial businesses,

civil service, and the military. While networks such as the Internet may be suitable for many applications, the military has unique and stringent needs in its business environment.

The Global Information Grid (GIG) is the vision of the assistant secretary of defense for Command, Control, Communications, and Intelligence for achieving information superiority. The GIG is a single, secure grid providing seamless end-to-end capabilities to all warfighters, national security, and support users. It supports the Department of Defense and intelligence community requirements from peacetime business support through all levels of conflict. The GIG provides plug-and-play interoperability for the joint services and coalition users with high capacity network operations. It also provides interoperability at the strategic, operational, tactical, and base/post/camp/station levels [3, 4].

Operational Benefits of NCO

The power of information superiority achieved by networking assets together can be illustrated by analogy with phased array technology. A single non-directional sensor by itself may detect the presence of an object, but putting two sensors together with time-of-arrival measurement capability allows the raw data of the two sensors to be correlated to yield a direction for the object. As more and more sensors are added, the precision of the location data increases. The data have been changed into more robust information about the object, which enables refined object tracking.

In NCO, capabilities for sensing, commanding, controlling, and engaging are

robustly networked via digital data links. The source of the increased power in a network-centric operation is derived in part from the increased content, quality, and timeliness of information flowing between the nodes in the network. This increased information flow is key to enabling shared battlespace awareness, and increasing the accuracy of the information. These operational benefits are derived from having the GIG enabling technology represented by the SARM guiding the development of nodes that plug and play on the network; they are not benefits of the SARM itself.

Reference [1] provides a much more complete discussion on the benefits of NCO.

Technical Approach

Why Have A SARM?

Network System Design: To work well, the fundamental architecture of networks and their nodes are designed together as a system. Creating and managing the SARM can ensure the following:

- The components used to build up the SARM are integrated into a system-wide architecture so that fundamental network system design issues such as information assurance are addressed by the design as a whole from the beginning.
- The single consistent framework of the SARM is implemented on all platforms and systems connecting to the network.
- This system-wide architecture will enhance the ease of integration of platforms and programs as nodes on the network and the level of interoperability between them, while maintaining the precepts of information dissemination control within an information assurance doctrine.

Reusable Components: The universal use of the products in SARM instantiations will foster the creation of reusable components that provide common data and functionality across platforms and systems. This will bring the expected benefits of decreased development costs, faster time to market, extensive use of commercial off-the-shelf (COTS) products, decreased maintenance costs, open standards, and robust products suitable for many environments.

The goal is to quickly get to the point where the SARM guides node interface design based upon a product catalog of qualified and tested products that form instantiations of the framework. This will enable many programs to take the products and use them directly off the shelf.

Figure 1: *Notional Deployment of SARM With Different Implementations Suited to Each Platform*



This will free the programs from spending resources on what should be common infrastructure, and instead allow them to concentrate their assets on solving their unique programmatic challenges.

What Will You Do With a SARM?

Figure 1 provides a notional idea of what you do with a SARM: instantiate the framework across the platforms and systems that are to become nodes on the network. The photos represent the platforms and systems, while the boxes to the sides represent different instantiations of the SARM – some larger, some smaller. Realize that each of the platforms may have different needs for interoperability and therefore different instantiations of the SARM. For example, the kind and amount of information needed by a hand held device will differ from systems needed by an operations center.

What Do You Want in a SARM?

Based Upon Standards: A fundamental design decision in creating the SARM is to base it upon standards such as the Internet Protocol (IP) [5] as the basis for the infrastructure. With the rapid and far-reaching success of the Internet, this brings many benefits, including open commercial standards, multiple competing sources for compatible products resulting in reduced costs and increased maintainability, mechanisms for technology insertion, and wealth of existing application technology guidelines for robust product development. The SARM also promotes the use of government standards, including the Joint Technical Architecture [6] and the Defense Information Infrastructure Common Operating Environment [7].

Common Interface and Functionality: To be part of a network, a platform must comply with the common interfacing standards defined by the network. The Internet works because every node on the network complies with the agreed-upon standards for basic connection and data exchange. This infrastructure can be common among the nodes in the network and be the foundation upon which applications residing on the network nodes are based.

Common Ontology: Once the physical connection is made to the network and the data moves through the communications layers of a node to become IP packets delivered by the operating systems to applications, the remaining key to interoperability is the consistent syntax and semantics of data that are exchanged on the network. This is referred to as *ontology*,

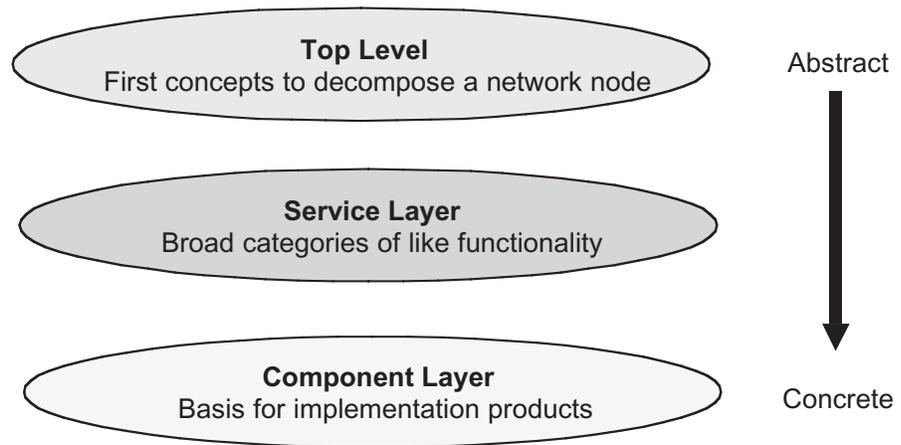


Figure 2: Discussion of SARM Structure Follows a Top-Down Design Paradigm

an explicit formal specification of how to represent the objects, concepts, and other entities that are assumed to exist in some area of interest along with the relationships that hold among them. The richness and extent of the ontology supported on a platform relates to the level of interoperability on the network supported by that node.

Understanding the SARM

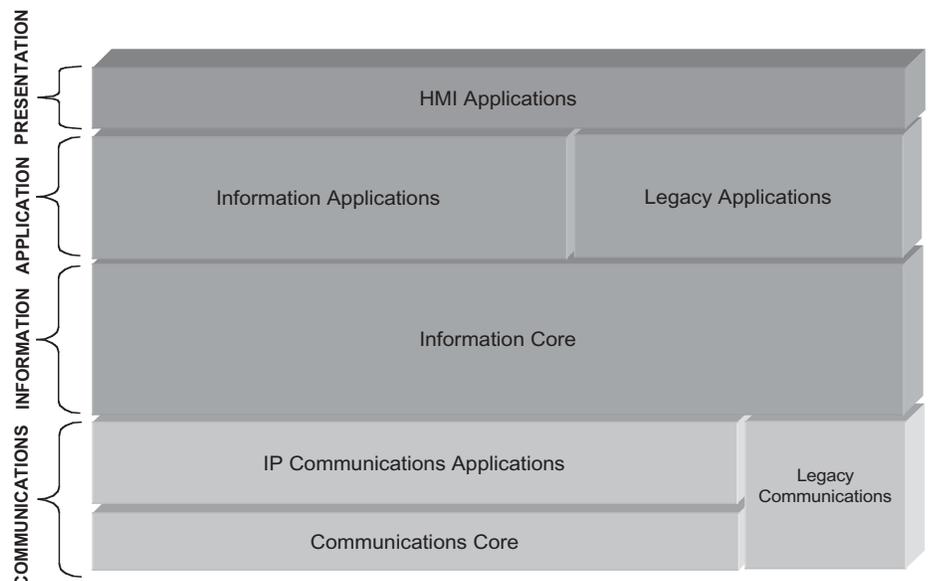
Hierarchy Diagrams: The discussion of the SARM follows a top-down approach, as shown in Figure 2, from an abstract decomposition of the functional units of a network node to specifications for the component pieces used to implement the functionality.

Top Level: The SARM is a hierarchical structure with increasing levels of detail and specificity at each successive level. The first level serves to divide the network node into broad categories of functionality and responsibility as shown in Figure 3 and as follows:

- The *communications* layer represents essential communications functions and services provided by the IP-centric network. Provision is made for legacy communications mechanisms to allow them to become nodes on the network.
- The *information* layer provides services that support the interchange and management of information between applications and the external environment. The key to this layer is a common ontology for the information flowing on the network and residing on the nodes.
- The *application* layer implements program-specific functional processing, e.g., position/navigation, sensor, control of real-time systems, and analysis of order of battle.
- The *presentation* layer implements program-specific human-machine interface (HMI) requirements.

The Strategic Architecture organization concentrates its efforts on the com-

Figure 3: Top Level of the SARM Divides the Model Into the Major Functional Areas



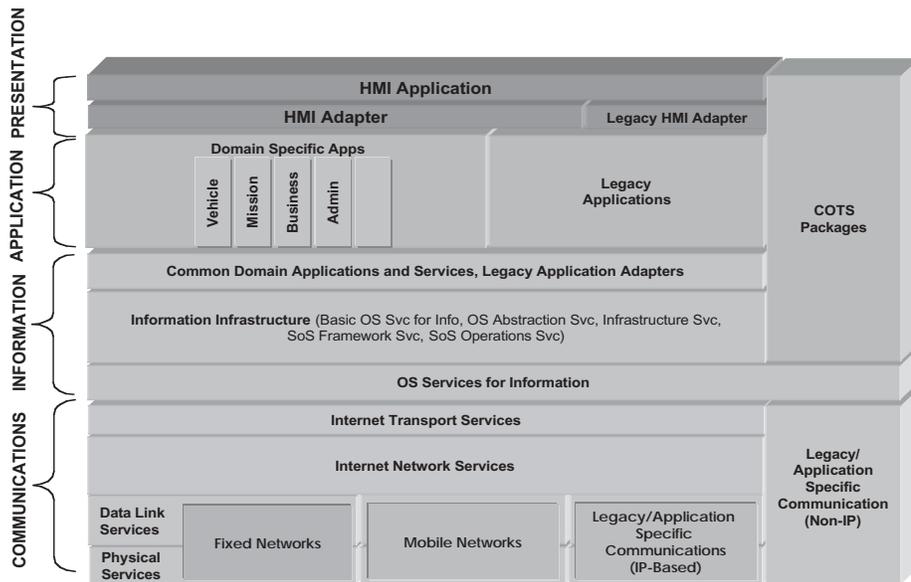


Figure 4: Service Layers Further Decompose the Framework Into More Specific Functional Categories

munication and information layers since these are the common infrastructure layers that enable interoperability between nodes. The application and presentation layers are more specific to the needs of a program. However, when application functionality that is common across programs is identified and data models and methods manipulating that data are generalized, these data and functions can be moved into the information layer for reuse across programs.

Service Layer: The next level further refines the decomposition into major services within the top-level decomposition and is shown in Figure 4.

- The *communications* services follow the layered guidelines of the Open System Interconnection (OSI) seven-layer model and the IP model, but implement only the bottom layers: physical, data link, network, and transport services. The diagram shows further decomposition into a variety of networks dependent upon the mobility of the platforms. Legacy communication systems are supported, both those that are IP and non-IP based.
- The *information* services are not strictly layered as the communication layers. The information services are application program interfaces (API) that provide operating system services, data management, information assurance, and similar services that perform fundamental control, access, and manipulation of information in a networked SoS model.
- The *application* and *presentation* services are notional in this diagram since the efforts of the Strategic Architecture organization concentrate on the other

layers and leave these layers to the programs for their value added. The intent is that program-specific processing and functionality is implemented in a network node at these levels.

Component Layer: At present, the SARM diagrams go down one more level in the communication and information layers to decompose them into compo-

“While some weapon systems can work together, most of today’s deployed systems are islands of self-contained connectivity, or stovepipe systems.”

nents. The idea is that each of the components would be implemented or mapped to COTS or government off-the-shelf (GOTS) products that provide the functionality defined by the component. The components are intended to be terminal or leaf nodes in the hierarchy tree. The software components of the SARM will have standard APIs defined for them so that applications may call the services independent of the implementation details. The common defined API will make the components independent of the underlying implementation and the hardware/software platform on which it executes. In this way, applications may be written to depend upon a platform-inde-

pendent environment provided by the SARM.

At this level of detail, the layered communications services model progresses in the protocol stack (read from bottom up) from the physical, data link, network services, and transport services. Provision is made for fixed location, mobile, and legacy systems as network nodes. Network quality of service and information assurance components exist in the layers as part of the overall design.

The structure of the information services layer progresses from basic operating system, to SoS services that provide underlying infrastructure for information management in a distributed networked environment. For example, a component provides networked directory services such as the Lightweight Directory Access Protocol.

Using The SARM

Component Catalog and Portal: Products that implement the functionality of the SARM components are being collected from COTS, GOTS, and other sources and put into a database along with tested configurations of the products that can be used to construct instantiations of the framework on different platforms. A Web portal interface is being developed to interface with the database. The portal interface will help users search for combinations of products that meet a program’s functional needs to become a node on the GIG.

SARM Evolution

The SARM is not complete and it will never be complete. It represents an expandable framework that will evolve with technology and time. Each of the layers in the reference model will expand at least horizontally to include new technologies fulfilling the same kind of functionality as existing services and components, while vertical expansion would include possibly new common functional capabilities. For example, as new communication protocols are developed with higher bandwidths, lower latency, and higher levels of information assurance, these can be added to the communication layer in the fixed or mobile networks.

Populating the SARM

One organization should be the custodian of the SARM, but it alone does not create the SARM and does not populate the component catalog solely on its own. This is an industry-wide effort that spans programs that act to supply products to implement components as well as use

those supplied by others. The NCO consortium is a critical part of proliferating this framework across the industry and will be the long-term custodian of the standards.

Conclusions

The information age is transforming business practices with the ability to network organizations internally and externally to their customers and suppliers. The military sees the need to follow similar paradigm shifts with the vision of a GIG where information flows securely between sensors, effectors, and decision-makers in the battlespace for unparalleled degrees of collaboration. To enable this level of interoperability requires a network system-wide guiding framework and products that implement that framework. The Strategic Architecture Reference Model addresses those issues and will enable NCW by providing the infrastructure for platforms and systems to become nodes on the GIG. ♦

References

1. Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. 2nd ed. (Rev.)

<www.c3i.osd.mil/NCW/ncw_0801.pdf>.

2. Joint Vision 2020 <www.kntwgs-22.ds.boeing.com/reports/OSD-Annual/jv2020b.pdf>.
3. U.S. Government. GIG. Enabling the Joint Vision. Chairman, Joint Chiefs. Jan. 2000 <www.dtic.mil/jcs/j6/enablingjv.pdf>.
4. Capstone Requirements Document. Global Information Grid (GIG). JROCM 134-01, 30 Aug. 2001 <[http://xanadu.ds.boeing.com/~moody/docs/grid/GIG_CRD_\(Final\).pdf](http://xanadu.ds.boeing.com/~moody/docs/grid/GIG_CRD_(Final).pdf)>.
5. Internet Protocol. IPv4 and IPv6, RFC 791 and 2460, respectively <www.ietf.org/rfc.html>.
6. U.S. Government. DoD Joint Technical Architecture. Department of Defense <www.jta.itsi.disa.mil>.
7. U.S. Government. Defense Information Infrastructure Common Operating Environment. Defense Information Systems Agency <<http://diicoe.disa.mil/coe>>.

Note

1. For more information on the consortium, please contact Karen Mowrey at karen.m.mowrey@boeing.com or call (714) 742-2157.

About the Author



Bradley C. Logan is a senior systems engineer with Boeing's Integrated Defense Systems where he works network-centric modeling and simulation efforts along with network infrastructure architecture definition. Previously, Logan worked both commercial and defense sectors in application domains from image and signal processing to reactive control systems. He has a Master of Science in electrical engineering from U.C. Berkeley and a Bachelor of Science in engineering from Harvey Mudd College, Claremont, Calif.

The Boeing Company
 Strategic Architecture
 Integrated Defense Systems
 3370 Miraloma Ave.
 MC 031-DB20
 Anaheim, CA 92803-3105
 Phone: (714) 762-3255
 E-mail: bradley.c.logan@boeing.com

The Sixteenth Annual
Software Technology Conference
 19 - 22 April 2004 • Salt Lake City, UT



Technology: Protecting America

Be part of the premier software technology conference in the Department of Defense

- Presentation abstracts accepted
4 August - 12 September 2003
- Exhibit registration opens
4 August 2003

Submit your abstract online or register to exhibit today!

www.stc-online.org




Source Code: CT1

Co-sponsored by:

United States Army United States Navy
 United States Marine Corps United States Air Force

Defense Information Systems Agency
 Utah State University Extension

Co-hosted by:

Ogden Air Logistics Center/CC
 Air Force Software Technology Support Center