Net-centricity

What is net-centricity? Everyone is talking about it. What do we really mean when we attach “net-centric” to other terms such as net-centric architecture, net-centric value added, net-centric engineering, net-centric operations, net-centric transformation, or net-centric warfare? How much is real and what is still a dream? All of these expressions are used by our authors in the articles appearing in this issue. For them, perhaps, the meaning is obvious, but for many of us (software professionals) it is not crystal clear. What does it mean for something (a system, or maybe, a component) to be “net-ready”? One definition of Net-centricity is:

“the extent to which a system or group has at its center the complex connection of people with common interests via communications and computer networks.”[1]

This definition suggests that, although technology is an essential element, there is a strong emphasis on the connection of people. Technology becomes the essential enabler of net-centricity when complexity is operative[1]. The term “network” has multiple meanings [1]:

1. A system of lines or channels that cross or interconnect: a network of railroads.
2. A complex, interconnected group or system: an espionage network.
3. An extended group of people with similar interests or concerns who interact and remain in informal contact for mutual assistance or support [a social or professional network]
4. In Computer Science, a system of computers interconnected by telephone wires or other means in order to share information. Also called [the] net.

The key attributes of a network are: a system, some degree of complexity, people with common interest, and technology. The notion of net-centricity embodies all of those meanings within it, not just the meaning used in computer science.

In the context of our national security we understand that net-centricity means digital networks carrying digital information from the systems (applications, repositories, etc.) and people that have it to those that need it [1].

The GIG

What about the Global Information Grid (GIG)? In its lexicon document [2], the Network Centric Operations Industry Consortium (NCOIC), describes the GIG as: 

“a DoD-wide program”, managed by OSD(NII) and integrated by DISA with the tasking to support all DoD missions with information technology, …, that offers the most effective, efficient, and assured information handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices.”

In Wikipedia the GIG is defined as follows [3]:

“The Global Information Grid (GIG) is defined as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), system data, security services, and other associated services necessary to achieve information superiority for the United States military. It is the physical manifestation of the network-centric warfare doctrine.”

What is interesting about the Wikipedia definition is that it asserts that the GIG (which started out as a concept):

• Is, in fact, the manifestation of achieving a level of net-centricity
• Encompasses much more that the elements we typically associate with a technical network, or even a network-of-networks.

The NCOIC description implies that there needs to be some alignment with the best practices that industry can offer as well.

Software Architecture

Now to the key question --- What does Software Architecture have to do with net-centricity? The architecture is the structure of the software system; it is typically described using multiple views in much the same way as the architecture of a house is described with multiple blueprints, each representing a particular view, or emphasizing a particular aspect of the building, using the language and symbols of the various builder roles (electrician, plumber, carpenter, mason, etc.). The architect must ensure that all of these views work together ---- that is, that the space provided for wiring does not conflict with the space provided for plumbing, and so on. The building architect has a rich set of standards and ‘building codes’ to follow to ensure compatibility of all components.

Establishing the software architecture and making sure it is the right architecture is a complex and critical task performed by experienced designers who work with the domain experts, consider all possible uses of the software and all possible...
Tech Views: Working Through the Maze!
Continued from page 1.

constraints. There is often more than one software architecture that addresses the software need and designers must make trade-offs among them.

Net-centric software architecture is about creating architectures for software at all levels of operation (from the lowest level embedded software component, such as a sensor, to high level user applications) that can be deployed and will perform on demand in an ever changing operational environment. Software architecture is usually not singled out but rather is developed as part of a larger system development effort. The term "Net-centric Software Architecture" is not a commonly recognized term among net-centric experts. It is used in the context of this issue to encompass the role that architecture in general plays in achieving net-centricity. The particular architecture construct that supports the GIG is services oriented architecture (SOA).

The Maze

As a software professional, I find myself caught in a maze of concepts, terminology, technology, organizational entities, programs and initiatives (see Figure 1). The items in this small section of the maze come from the three articles in this issue and the path from software architecture to Net-centricity is challenging at best. The maze extends far beyond what is pictured here.

I think that most of us (software professionals and managers) understand the concept of net-centricity and that the GIG is our mechanism for making that concept a reality. It makes sense that we need to cross both organizational and cultural boundaries to make this happen. It also makes sense that DoD has such a massive undertaking to develop the infrastructure for the GIG. However, it is not clear how we as individuals (managers, technical leads, quality experts, testing experts, etc.) fit in with our respective projects here and now. It is not clear where the line is drawn between net-centric software and software that is not relevant. Is the entire collection of DoD user applications going to be scrutinized for accessibility in a net-centric environment? One definition of the GIG targets all software (including applications) necessary to achieve information superiority. Does that mean that anyone who is involved in designing or integrating software for any DoD sponsored system or application, and perhaps some non-DoD systems, is, by definition, involved in achieving net-centricity. If so, how do we start? Suppose, as an example, I am managing a software project focused on planning weapons munitions production and control. The operational (user) environment consists of two highly skilled analysts, who are also domain experts in a branch within a division within … within … several layers on an Army organization chart. I probably should be thinking about the plug and play capability of this software package but my customer needs this application yesterday. Should I be concerned with net-centricity or not? Where do I go to get...
Tech Views: Working Through the Maze!
Continued from page 2.

the answer? Do I simply say “let the network people worry about how to make this application (and its data) accessible on demand” somewhere in the GIG? There are so many pieces to the puzzle that we each need to be selective in choosing what to learn about. As program managers and project managers and technical leads we are accountable for critical architectural decisions. How do we get on the right path to do our part toward achieving net-centricity? How do we find our way through the maze?

Overview of Articles

We, the DACS, asked our authors to write articles about net-centric software architecture from their perspective. They have done their job well. After all, they are the experts. They have provided a plethora of information about the architecture, standards, processes and strategies, and organizations needed for the United States to achieve a state of information superiority that will enable better decision making in our defense initiatives (supporting the warfighter, protecting our country). I think this is called “net-centricity”.

In the first article, the author, Dave Chesebrough, helps us navigate the maze by describing the role that architecture plays in moving DoD into an net-centric environment. He has also provided several sidebars to minimize the complexity of content that is inherent to the subject of net-centricity.

In the 2nd article, authors Mark K. Bowler, Hans W. Polzer, and Sheryl S. Sizelove, all members of the Network Centric Operations Industry Consortium (NCOIC), describe NCOIC’s role in fostering interoperability, which is another perspective of net-centricity. To quote them, “The missing element has been a common technical approach that could be adopted by all designers and manufacturers so that their products would carry the inherent capability to interoperate with other systems on a global network, as desired.”

NCOIC (formally chartered in 2004) has also developed some tools to aid our progress in achieving interoperability; namely, a lexicon to ensure that everyone speaks the same language; the NOCIC Interoperability Framework (NIFTM), which describes the building codes or standards and components to select when building, organizing, and relating applications, data, and communications—and how to put them together for an interoperable system; and the Network Centric Analysis Tool (NCAT™), which allows analysts to answer the question, how net-centric is a given system? --- a measure of interoperability.

The final article, authored by Chris Gunderson, Brian O’Neill, and Stephen R. Macdonald, discusses the need for a business model to achieve and sustain net-centricity. It proposes establishing “a marketplace for certified net-ready tools that enable trusted transactions of valuable information at the right time by investing in an open not-for-profit environment that enables intellectual property distribution, open collaboration and commercial risk mitigation through adaptive validation, verification and certification processes.” They assert that success depends on imagination and leadership and propose the formation of some organizations (and processes) that can function without the current restraints of the DoD bureaucracy.

In conclusion, if you read all three articles, you may feel the walls of the maze closing in. The task is daunting. For those of us on the fringes, or lost somewhere in the maze, we need a living map. We need to quickly see how each and every item (term, concept, organization, technology, architecture, etc.) contributes (and to what degree) to net-centricity. I started to build a cause and effect (Ishikawa) diagram identifying contributors to net-centricity based on the content provided by our respected authors (See Figure 2). It probably needs several other branches such as people, process, acquisition, culture, education, program management, and project management.

In fact, is there anything about software acquisition and development that does not impact net-centricity? Can any software professional, say comfortably that their role has nothing to do with achieving net-centricity --- that none of this applies to them?

Figure 2: Contributors to Net-centricity

continues on page 4
I have only started this net-centricity map. It has a long way to go. Perhaps there is a better visual tool for making such a map. I ask you, the software development community, to help me build it and strengthen it so that it can help all of us find our way through the maze as we move forward. I welcome your emails or phone calls.

References

About the Author
Ellen Walker, Interim DACS Deputy Director and Managing Editor of the DACS Software Tech News, is currently developing a series of publications on software “best practices” as part of the DACS Gold Practice Initiative. She has spent the past 20 years as a software developer in various roles spanning the entire software life cycle including project management of multiple business process re-engineering efforts within the DoD community. She is also experienced with assessment initiatives such as the Capability Maturity Model for Software (CMM-SW) and the quality management practices of the New York State Quality Award program. Ellen has an MS in Management Science (State University of New York (SUNY) at Binghamton), and bachelor degrees in both Computer Science (SUNY – Utica/Rome) and Mathematics (LeMoyne College).

Author Contact Information
Phone: 315-334-4936
Email: ewalker@dacs.dtic.mil
ellen.walker@itt.com
The DACS Gold Practice Initiative:

- Promotes effective selection/use of software acquisition & development practices
- Defines essential activities/benefits of each practice
- Considers the environment in which each practice is used
- Addresses the timeliness of practice benefits
- Recognizes interrelationships between practices that influence success or failure
- Contains quantitative and qualitative information
- Includes discussion forums, case studies and survey opportunities
- A continually evolving resource for the DoD, Government, Industry and Academia
- Free to use/free to join

Current Gold Practices:

- Acquisition Process Improvement
- Architecture-First Approach
- Assess Reuse Risks and Costs
- Binary Quality Gates at the Inch-Pebble Level
- Commercial Specifications and Standards/Open Systems
- Ensure Interoperability
- Formal Inspections
- Formal Risk Management
- Goal-Question-Metric Approach
- Integrated Product and Process Development
- Model-Based Testing
- Plan for Technology Insertion
- Requirements Management
- Requirements Trade-Off/Negotiations
- Statistical Process Control
- Track Earned Value

Learn More About the DACS Gold Practice Initiative:
http://www.goldpractices.com

Become a Registered Member!
http://www.goldpractices.com/registration/register_step1.php

Data & Analysis Center for Software
P.O. Box 1400
Rome, NY 13442-1400

http://iarc.dtic.mil/dacs

Data & Analysis Center for Software
Are you getting All you can from your software investment?

The DACS ROI Dashboard

Impact on Quality (% defect reduction)

75th Percentile: 90

Oklahoma City Air Logistics Center, Test Program Set and Industrial Automation line observed the defect density decrease 91%, from 3.3 to 0.3 Defects per KSLOC, while achieving CMM Level 4.

Access the DACS ROI Dashboard!
http://www.thedacs.com/databases/roi/

Technologies Covered:
- SEI CMM/CMMI
- SEI Team Software Process (TSP)
- SEI Personal Software Process (PSP)
- Inspections
- Reuse
- Cleanroom
And Many More!

Graphs Showing Impact Of Software Technologies On:
- ROI
- Productivity
- Quality

Summarizes Facts From Open Literature

Data & Analysis Center for Software
P.O.Box 1400
Rome, NY 13442-1400
http://iac.dtic.mil/dacs
The Role of Architecture in Moving DoD to a Net-Centric Environment

By Dave Chesebrough, President, Association for Enterprise Integration (AFEI)

DoD – A Department on the Move

The Department of Defense is an organization on the move. A restless wind blows through the halls of the Pentagon, and it’s not just a lot of hot air! Across the Department initiatives have sprung up that are aimed at integrating information and data across various areas of Defense Agencies and Military Services. Net-centricity has become a sort of mantra for the new Defense establishment. What is going on, and why? Blame it on Reagan and Gorbachev. That’s right. If the Soviet Union had not dissolved, DoD would not have had to re-adjust to a new reality in the 21st century.

But there is enough blame to go around. Vint Cerf, Steve Jobs, Bill Gates, Tim Berners-Lee and other innovators also bear some responsibility for the state that DoD finds itself in. They and others constructed a world where information can be created by applications and sensors, and then exchanged easily through complex networks of computers, routers and wireless devices. This has broken many cherished, hierarchical models of information control and distribution. Now, with the right systems in place, a soldier on the battlefield can now know as much, even more, than the commander at headquarters about the action taking place. This, of course, turns some things upside down. But that’s the way it is, and the way it will be.

The Growing Role of Architecture

The impact of information technology on business and government has barely begun, and the pace of change is accelerating. Today we recognize that, as with any journey, project or enterprise, it helps to have a plan. Enterprise architecture is now recognized as the plan for aligning technology with strategy. It helps you respond much more effectively to a changing business environment, and allows organizations to coordinate structure, business functions, and processes to achieve their missions.

Over the next decade, organizations, including DoD, will experience increasing pressure to find new and better ways to perform in an information-rich world. Information management is moving from an infrastructure support function to becoming the essential foundation of performance. Enterprise architecture forms the skeletal structure for the future knowledge-centric organization.

In computer science the term ‘architecture’ has traditionally been applied to software and information systems (see SIDEBAR 1). Enterprise architecture is associated more broadly to the practice of business optimization, in that it addresses business processes, performance, information and organization. The Wikipedia entry for Enterprise Architecture defines it as the application of a well-defined, consistent, comprehensive and rigorous method to describing current and future structures and behaviors for an organization’s processes, information systems, personnel and configuration, aligning them with core missions and strategic direction. Ross, Weill and Robertson in their recent book, Enterprise Architecture as Strategy, propose enterprise architecture as a key enabler of corporate strategy (see SIDEBAR 2). They eschew the more “traditional” (ad hoc and uncontrolled) approach to IT in favor of one more closely aligned with providing capabilities that enable strategy achievement. They describe enterprise architecture as:

“…the organizing logic for business processes and IT infrastructure, reflecting the integration and standardization requirements of the company’s operating model. The enterprise architecture provides a long term view of the company’s processes, systems and technologies so that individual projects can build capabilities – not just fulfill immediate needs.”

SIDEBAR 1: What is Architecture?

Ar•chi•tec•ture: In computer science the structure and organization of a computer’s hardware or system software.

There are many definitions of software architecture. The Software Engineering Institute at Carnegie Mellon offers a comprehensive collection of definitions. The common thread amongst them is structure. Architecture is the guiding construct against which a software development can be executed, and provides a roadmap and measuring stick for achieving the desired outcome (capability).

Today the concept of architecture in information technology has expanded beyond hardware, software and even networks into the processes and organization of the concern itself. So it is today with service-oriented architecture (SOA). SOA is an IT strategy that organizes applications into interoperable, standards-based services that can be combined and reused to meet changing business needs and in so doing can separate applications and data, making data understandable, visible and accessible.

Architecture can be elusive because it involves subjective elements. While objective elements such as blueprints, specs, materials list, etc. can be easily quantified, the user’s experience, the utility, and the harmony of the thing being architected within its environment can not.
The Role of Architecture
Continued from page 7.

Enterprise architecture is becoming a common practice within the U.S. Federal Government as part of the Capital Planning and Investment Control (CPIC) process. The Federal Enterprise Architecture (FEA) reference models serve as a framework to guide Federal Agencies in the development of their architectures. The primary purpose of creating enterprise architecture is to ensure that business strategy and IT investments are aligned. As such, enterprise architecture allows traceability from the business strategy down to the underlying technology, and guides investment in capabilities necessary of the enterprise. Companies such as AOL, BP, Intel and Volkswagen AG have applied enterprise architecture to improve their business performance activity.

Architecture for Net-centricity

Architecture was used in computer science to address the growing problem of managing software development. By choosing the right data structures, algorithms, etc. developers were able to overcome problems in large projects. Through the 80's and 90's software architecture grew as a discipline and was centered on the idea of reducing complexity through abstraction and breaking a program up into functions with as little overlap as possible. The current problem with this traditional approach to software is that every program is unique and optimized to perform its particular set of requirements. The highly interconnected nature of today's environment drives us to seek more integrated ways of developing capabilities, of allowing for the unanticipated, and of driving efficiency across the enterprise.

In this environment, DoD architecture is being driven by the strategy of net-centricity, coupled with a “services” approach to applications and data. That is, making both available through web and internet technology. This is commonly referred to as a service-oriented architecture (SOA). SOA makes use of the concept of web services. This is viewed as a key foundation to achieving the Global Information Grid (GIG). OASIS defines web services as services that allow applications to communicate across platforms and programming languages using standard protocols based on XML.

The GIG encompasses all of DoD’s warfighting, combat support, and business processes. Building an architecture that supports this vision is a daunting task. As you might expect from a large, complex organization architectures exist in various forms. The GIG approach will leverage the existing architectures, even those still in progress. It is organized into three interrelated track activities, or lanes:

- the Joint Operational Architecture (JOA),
- the Combat Support and Business Area Architectures,
- and the Communications and Computing System Architecture.

Providing a means to use existing architectures in a “plug and play” manner is essential to building this global enterprise view. This approach is called “federation”, and is at the heart of the OSD strategy for enterprise architecture. The following diagram (see Figure 1) illustrates the relationships of architectures and DoD mission areas.

![Global Information Grid Enterprise Architecture Diagram](image)

Figure 1: Global Information Grid Enterprise Architecture

continues on page 9
The Role of Architecture
Continued from page 8.

The GIG enterprise architecture will be a blueprint of a current or postulated future configuration of resources, rules, and relationships. To achieve compatibility, flexibility, and interoperability, the GIG elements will be made available in a manner that allows components to be assembled into the required system configuration. This building blocks approach is becoming more common in commercial business as service-oriented architectures become more available.

The enterprise architecture should be substantive and comprehensive, but not prescriptive. This will allow flexibility to accommodate local needs and innovation (see SIDEBAR 2). For example, the enterprise architecture would specify a lowest common denominator of interoperability through technical standards, protocols and data models, but would not prescribe the data elements, processes or representation of a specific function like a target track. These are left to functional architectures developed by communities of interest such as maritime domain awareness or time-sensitive targeting.

**Transitioning Architectures**

One of the more difficult, but absolutely essential, aspects of developing an enterprise architecture is to describe adequately how the architecture process accommodates both the ‘as-is’, intermediate increments, and the ‘to-be’ environment. Tackling this architecture transition starts with a rigorous, top-down, traceable approach to defining required capabilities for both the ‘as-is” and ‘to-be” time frames. The basic DoD architectural landscape is identified in the DoD Architecture Framework (DoDAF). Within this framework operational views (OVs) provide the context for deriving and developing system views (SVs), which identify potential solutions (see SIDEBAR 3).

To be of value to the Office of the Secretary of Defense (OSD), joint, and service decision makers, the OVs must delineate required joint warfare capabilities both now and in the future. This will enable DoD to develop valid SVs and procure the correct, capabilities-based systems.

Defining the target architectures will require high-level, long-range OSD and military guidance and direction – in short, a consistent strategy. Definition of the target architecture will involve multiple iterations of current architectures. In the end, this systemic enterprise approach is a process that repeats itself as new

**SIDEBAR 2: The DoD Enterprise Strategy**

The Quadrennial Defense Review (QDR) is the DoD Strategic Plan. National Defense strategies flow from the QDR and are reflected in the programs the military executes regarding structure, equipping, training and operations. The 2006 QDR defines the following fundamental imperatives for the Department of Defense:

- Continuing to reorient the Department’s capabilities and forces to be more agile in this time of war, to prepare for wider asymmetric challenges and to hedge against uncertainty over the next 20 years, and
- Implementing enterprise-wide changes to ensure that organizational structures, processes and procedures effectively support its strategic direction.

The vision represented by the QDR is one of a more agile, integrated DoD whose systems are aligned with its strategies.

Viewing DoD as an enterprise, with enterprise-wide transformations, is a significant departure from past defense planning perspectives. Accomplishing these objectives will require enterprise architecture, governance processes for compliance, and a continual evolving of defense systems and acquisitions.

The GIG enterprise architecture will be a blueprint of a current or postulated future configuration of resources, rules, and relationships. To achieve compatibility, flexibility, and interoperability, the GIG elements will be made available in a manner that allows components to be assembled into the required system configuration. This building blocks approach is becoming more common in commercial business as service-oriented architectures become more available.

The enterprise architecture should be substantive and comprehensive, but not prescriptive. This will allow flexibility to accommodate local needs and innovation (see SIDEBAR 2). For example, the enterprise architecture would specify a lowest common denominator of interoperability through technical standards, protocols and data models, but would not prescribe the data elements, processes or representation of a specific function like a target track. These are left to functional architectures developed by communities of interest such as maritime domain awareness or time-sensitive targeting.

**SIDEBAR 3: DoD Architecture Framework (DoDAF)**

DoDAF is being managed from the Office of the DoD CIO/ASD NII. DoDAF was formerly named C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) Architecture Framework. Other derivative frameworks based on DoDAF include the NATO Architecture Framework (NAF) and Ministry of Defence (United Kingdom) Architecture Framework (MODAF).

DoDAF is organized around a shared repository to hold work products. The repository is defined by the Core Architecture Data Model 2.0 (CADM - essentially a common database schema) and the DoD Architecture Repository System (DARS). DoDAF views are organized into four basic view sets: overarching All View (AV), Operational View (OV), Systems View (SV), and the Technical Standards View (TV).

The DoDAF has come under some criticism because of its focus on representational view, and not underlying data. DoD has in the past made unsuccessful efforts to develop common data dictionaries. DoD is evolving the Core Architecture Data model to provide a common approach for organizing and portraying the structure of architecture information, and is designed to capture common data requirements.

continues on page 10
requirements and missions, defined by changing global realities, are revealed. Therefore, the most effective enterprise architecture provides for accommodating change, avoiding technical and process lock-in. This approach to architecture development will contribute to development of a robust enterprise architecture based on future warfare requirements (see SIDEBAR 4).

**GIG Enterprise Architecture**

The GIG enterprise architecture will be used to prioritize the information technology issues and investment strategies for the future, integrate extant architectures and develop the methodology for maintaining architectures. The GIG architecture will be used by various commanders, services, and other government agencies to assist in the formulation of their mission-specific applications (communities of interest, or COIs) and required infrastructure support; to assist in meeting their Clinger-Cohen Act (see SIDEBAR 5) requirements; and to formulate budget strategies for planning, programming, and budgeting system (PPBS) and program objective memorandum (POM) activities. Although the GIG enterprise architecture will not be the sole tool required to guarantee interoperable DoD information systems, the architecture goes a long way in providing the missing enterprise roadmap necessary for enabling interoperability among DoD systems.

**Industry Support of DoD Architecture Efforts**

The Association for Enterprise Integration (AFEI) has jointly chartered with ASD (NII) several working groups to bring industry views and input to the development of policy and approaches to various aspects of net-centric capability. Two of the AFEI working groups are addressing architecture. The following figure shows the current AFEI working groups.

One of the most active is the Data Strategy and Shared Services Working Group, which supports the Director for Information Management in ASD (NII) in the area of SOA and shared services. In October this group published its third paper, DoD

---

**SIDEBAR 4: The Global Information Grid Challenge**

In a January 2006 GAO report entitled DoD Management Approach and Processes Not Well-Suited to Support Development of Global Information Grid, 14 GAO states:

“Department of Defense (DOD) officials currently estimate that the department will spend approximately $34 billion through 2011 to develop the core network of the Global Information Grid (GIG), a large and complex undertaking intended to provide on-demand and real-time data and information to the warfighter. DOD views the GIG as the cornerstone of information superiority, a key enabler of network-centric warfare, and a pillar of defense transformation. A high degree of coordination and cooperation is needed to make the GIG a reality. In prior work GAO found that enforcing investment decisions across the military services and assuring management attention and oversight of the GIG effort were key management challenges facing DOD.”

The GAO found that while the vision for the GIG was commendable, DoD has significant implementation challenges that are rooted in the processes, structure and culture of the Department. GAO opined that the DOD management approach for the GIG, in which no one entity is clearly in charge or accountable for results, is not optimized to enforce investment decisions across the department. The DOD Chief Information Officer has lead responsibility for the GIG development effort, but this office has less influence on investment and program decisions than the military services and defense agencies, which determine investment priorities and manage program development efforts.

The department’s three major decision-making processes – budgeting, acquisition and requirements - are not structured to support crosscutting, department-wide development efforts such as the GIG. This is also a finding of the Defense Acquisition Performance Assessment (DAPA) conducted in 2006. 15

The full report, GAO-06-211, is available at www.gao.gov or from the AFEI web site. The DAPA Final Report is available at http://www.acq.osd.mil/dapaproject/
The Role of Architecture
Continued from page 10.

SIDEBAR 5: The Clinger-Cohen Act of 1996

Clinger-Cohen Act, formally the Information Technology Management Reform Act of 1996, provides that government information technology organizations be operated in the same manner as an efficient and profitable business would be. Acquisition, planning and management of technology are now treated as a “capital investment.” Within the DoD, certain mission or system-specific investments have been exempted from the provisions of the act.\(^1\)

Clinger-Cohen generated a number of significant changes in the roles and responsibilities of various Federal agencies in managing acquisition of IT. The act established Chief Information Officers for Federal Departments and Agencies, and gave them significant oversight for IT acquisitions. It elevated oversight responsibility to the Director, OMB. In the Department of Defense, the Assistant Secretary of Defense for Networks & Information Integration (ASD (NII)) has been designated as the DoD Chief Information Officer and provides management and oversight of all DoD information technology, including national security systems.

Clinger-Cohen emphasizes an integrated framework of technology aimed at efficiently performing the business of the Department. The act takes aim at proliferation and duplication in IT investments across the Government, attacking “impulse purchases” that are not in accordance with an overall plan or that are unnecessary investments.

The operative Clinger-Cohen principles include: planning major IT investments, improving processes before investing in systems, enforcing accountability for performance, using standards in ways that promote integration, and increasing the acquisition and incorporation of commercial technology and products. The Clinger-Cohen Act also mandates the use of a formal process for all Federal agencies, the Federal Enterprise Architecture.

In this context, ‘services’ were defined as applications or data sources presented as web-services by a service provider to achieve results for the user. Sharing web-services inherently enables data sharing because the same data and underlying processes are used by many. To increase data sharing, or more precisely information sharing, DoD seeks to employ shared-services across the enterprise to assist in the response to the new threat environment.

There are numerous constraints described in their first report. These include:
- Challenges in acquisition planning, funding and scheduling with the associated business models for service oriented architectures (SOAs)
- Differences in agency and Military Service requirements
- Programmatic interdependencies that accrue as services are cooperatively developed
- Lack of vendor neutral specifications in the current interoperability standards limiting the ability to provide a heterogeneous enterprise
- Lack of processes to assist in defining and sharing semantics among the COIs
- Lack of common or shared security C&A mechanisms; uncertain service scaling or load balancing of shared-services
- Undeveloped business incentives that encourage, rather than just enforce, shared-services

Figure 3 illustrates the tension that exists between the driving forces for shared services, and existing restraints.

Performance Metrics to Support Industry Confidence in Shared Services.\(^6\) The group has involved as many as 44 companies in developing positions on SOA issues. The working group has also published other reports on various aspects of DoD SOA implementation. In the initial report industry was asked to analyze the issues surrounding shared-services, and recommend strategies and policies that will provide incentives to industry for the implementation and adoption of shared-services within DoD.

Figure 3: Driving Forces and Existing Restraints

continues on page 12
Shared services require a shift from existing concepts of idiosyncratic requirements, into an environment where organizations understand and embrace cross-community development. Moving to a heterogeneous infrastructure for the DoD net-centric environment means being able to move away from a single master vendor or “winner-takes-all” contracting environment, to an environment of many vendors operating according to common standards tailored for net-centric SOAs. This environment of cooperation provides best of class services and enables DoD users to access mission-relevant services and technology capabilities that keep pace with change.

The performance metrics paper identifies significant shifts to new kinds of metrics definition that must occur in this unprecedented dynamic environment, and provides guidance for ongoing evolution in development of shared service performance metrics.

To address the new challenges of shared services (new risks, new accountabilities, new business strategies, etc.), shared services performance governance will be a critical foundation.

DoD Enterprise Architecture Congruence Community of Practice

AFEI is also bringing industry input to the effort by DoD to bring its architecture into alignment with the Federal Enterprise Architecture. The DoD Architecture Framework (DODAF) is the current avenue of DoD compliance with the Clinger-Cohen Act and Office of Management and Budget Circulars A-11 and A-130.

The Enterprise Architecture Congruence (EAC) Community of Practice (CoP) is working to align the relationships between the DoD Enterprise Architecture and the Federal Enterprise Architecture (FEA). This is important from the perspective of satisfying OMB requirements. However, the greater value lies in the opportunity to accelerate enterprise architecture development across the DoD in ways that promote interoperability of architectures at the enterprise level with military service architectures and program/system architectures.

The Federal Enterprise Architecture’s (FEA) purpose is to identify opportunities to simplify processes and unify work across the executive agencies and within the lines of business of the Federal government. The FEA is entirely business-driven, as opposed to the DODAF approach. Its foundation is the Business Reference Model, which describes the government’s Lines of Business (LOB) and its services to include Defense and National Security.

The transition strategy for DoD is the DoD Enterprise Architecture Reference Model. It consists of a set of reference models that parallel those of the FEA, and serve as a transition from the DODAF to the FEA. Figure 4, from the Army Enterprise Solutions Competency Center, shows the relationship flow from the FEA reference models through the DoD reference models to the GIG architecture and DoD mission areas.

These reference models provide universal definitions and constructs for the business, services, performance, and technology of the DoD. The DoD EA RM serves as a foundation to leverage existing processes, capabilities, components and technologies as DoD and other government organizations build target enterprise architectures. The DoD EA RM is designed to facilitate cross-organizational analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within DoD and across Federal agencies and other government organizations. DoD plans to leverage presentation of the DoD architecture and other information resource attributes in reference model style as well as leverage the use of the accompanying management processes to gain improved efficiency and effectiveness in the DoD by using EA to improve results.

Conclusion

Architecture is quickly becoming a tool for converting vision into reality. To be sure, architecture is an abstraction of what we want to create. A set of builder’s blueprints and specifications are not a house, nor does a set of enterprise architectures give desired information capabilities. But without an enterprise approach to architecture, our chances of creating the net-centric Department of Defense or the Information Sharing Environment for homeland security that we desire are very, very small. The world that Reagan, Gorbachev, Cerf, Lee and many others have given us is one that demands a different approach. We all know that Einstein and Lincoln told us that to get something new we need to do something different. We would be wise to heed their advice.

continues on page 13
The Role of Architecture
Continued from page 12.

SIDEBAR 6: Association for Enterprise Integration

The Association for Enterprise Integration (AFEI) has its roots in the problems of sharing information among defense logistics information systems in the mid 80's. In the 80's we were in the era of batch processing and tapes. Today we have the Internet, SIPRNET, NIPRNET, the web and cell phones. However, the nature of the problems with information sharing remains the same, but the technologies involved have changed dramatically. The mission of AFEI is to create the framework for collaboration between industry and government on these problems. AFEI sponsors working groups and information exchange meetings and conference targeted towards meaningful exchanges of information between government and industry. To paraphrase and old commercial: we don't make the solutions – we make the solutions better! AFEI is a subsidiary of the National Defense Industrial Association, a not-for-profit educational group whose motto is Strength Through Industry and Technology. Visit AFEI at http://www.afei.org.

References
1. This definition is a paraphrase of one found on Wikipedia. It contains the essential elements of an enterprise architecture as defined by many authors, and reflects the intent of the Federal Enterprise Architecture in providing a framework for guiding the development of software capabilities that improves the ability of an agency to perform its mission, vice effectively completing a function of that mission. (http://en.wikipedia.org/wiki/Enterprise_architecture).

About the Author

David E. Chesebrough, P.E.

Dave became the second President of AFEI on November 6, 2001. During his tenure the association has redefined itself to become the premier industry group dealing with net-centric operations and enterprise integration. The Association for Enterprise Integration is an affiliate of the National Defense Industrial Association.

Mr. Chesebrough has over 30 years experience with technology, business management and strategy, including Defense acquisition, international information technology consulting, aerospace, nuclear power, and education.
He has lectured, taught, and consulted extensively in the US, Asia, Europe and Africa. He founded and operated a strategic e-business consultancy for B2B and B2G e-commerce.

His experience in Defense work began upon entering the U.S. Air Force in 1976, where he served four years as an Astronautical Engineer. His responsibilities included the integration of experimental payloads with the Minutemen I ballistic missile.

Prior to entering the Air Force he was an engineer with Babcock and Wilcox, designing fuel and control components for commercial nuclear power generation plants. Mr. Chesebrough re-entered industry in the Washington, D.C. area providing technical and management support to a variety of military programs, including underwater acoustics systems, Army telecommunications, and Navy command and control installations. He owned and operated a small information technology firm for nine years, providing technical and management support to government and industry in electronic business practices. His interest in the application of information technology to improve information sharing in enterprises began in the mid – 80’s, and he has pursued that passion ever since.

Today he is guiding the NDIA family of associations into a central position as the leading industry-wide advisory body to government on net-centric operations.

Mr. Chesebrough has had numerous international consulting engagements throughout Europe and Asia, including contracts with the Royal Saudi Navy and the U.S Army in England. He has conducted training courses for the NATO Maintenance and Supply Agency and industry in South Africa, and has completed numerous studies for companies in Japan and Korea. He has lectured extensively in the US, Europe and Asia.

He is a registered Professional Engineer in the Commonwealth of Virginia.

Mr. Chesebrough is married to the former Diane Wev of Arlington, Virginia and has three sons. They reside in Woodbridge, Virginia.

Author Contact Information
Office phone: (703) 247-2597
e-mail: dchesebrough@afei.org
Spurring NCO by Fostering Interoperability

By Mark K. Bowler, Hans W. Polzer, and Sheryl S. Sizelove

Recent events highlight the critical need for agencies and organizations to share information in real time and create a common operational picture during a situation. Fulfilling this need is the goal of network-centric operations (NCO).

NCO—“an information superiority-enabled concept of operations”—is best enabled and supported by systems that interoperate. Although NCO is still in its formative stages, the value of an NCO approach is quickly gaining recognition given the realization that such an approach eliminates standalone systems—those systems that can operate only with like systems—and thus enables all systems and platforms to interoperate on a global network. The ability to interoperate on a global network ensures access to information, and, armed with access to information, government agencies are positioned to make more effective decisions.

The Network Centric Operations Industry Consortium (NCOIC) is working collaboratively with stakeholders from governments, industry, and academia globally to define and promote open standards, system engineering tools, commercial building blocks, and education that will contribute to a network-centric environment across all government departments, from first responders and local authorities to regional and nationwide or federal military services. The consortium is the only organization of its kind dedicated to these goals.

NCO Today

Operation Iraqi Freedom, the responses to Hurricane Katrina and the Sept. 11, 2001 terrorist attacks in the United States provide examples of decisions taken in the absence of complete information. Increasingly, defense and military agencies have sought NCO capabilities to enhance situational awareness, information sharing and, in turn, decision making. Other types of agencies (such as “blue-light” first responders and space agencies) are gravitating toward the NCO vision as well.

Certainly, today's advanced network technology, information management, and data fusion techniques are up to the challenge. It is easier than ever for systems and platforms to share information over a global network. The missing element has been a common technical approach that could be adopted by all designers and manufacturers so that their products would carry the inherent capability to interoperate with other systems on a global network, as desired. A common technological basis for designing like systems results in less engineering specialization and, thus, avoids over-specialized and closed architectures. This not only reduces program cost, it also accelerates delivery of the final product.

Only through far-reaching collaboration on open, standards-based interoperability will the goal of achieving NCO-enabled government transformation be fully realized. Consider the example of the Internet. Had many companies not collaborated 15 years ago and agreed upon the Internet Protocol (IP), then the World Wide Web as we know it today might never have been established. In the same way, NCOIC hopes—by fostering open, standards-based interoperability—to spur creation of a dynamic infrastructure and capitalize on the vast potential of network-centric technology.

“How we get there is through close cooperation,” said Mark Bowler, chair of NCOIC’s Architectures and Standards Analysis Team. “Governments can’t simply go out there and specify that interoperability occurs. It needs industry to make it happen, and industry needs the government’s support and input. It really does take both entities.”

NCOIC’s Origin, Mission and Operations

NCOIC’s mission is to facilitate global realization of the benefit inherent in NCO. The organization was formed as a not-for-profit international corporation with a vision of “industry, working together to provide its customers a network-centric environment where all classes of information systems interoperate by integrating existing and emerging open standards into a common, evolving global framework employing a common set of principles and processes.”

The first formal meeting of NCOIC membership took place Aug. 27, 2004, but the concept goes back to 2000, when Carl O’Berry, vice president of Boeing Strategic Architecture, initiated informal discussions about the NCO concept and the role industry could play with customers. O’Berry served as the consortium’s first elected executive chairman, but the consortium from the start operated independently, governed by neither Boeing nor any other individual member company. Every member is treated equitably. From October 2005 to October 2006, Lorraine Martin of Lockheed Martin chaired NCOIC’s executive council, with Harry Raduege of Deloitte & Touche serving as vice chair. Raduege became the chair in October 2006, and Martin now serves as chair emerita.

Membership in the consortium is open, and NCOIC draws representatives from across the spectrum of joint, interagency, intergovernmental, and multinational industrial and commercial operations. With more than 600 technical experts from member organizations participating, the technical work of NCOIC is divided into domain-focused functional teams:

- The Architectures and Standards Analysis Team develops NCO system “building codes” that provide engineering, architectural, and standards guidance for the developers.

continues on page 16
Spurring NCO by Fostering Interoperability

Continued from page 15.

of NCO systems. The building codes are designed to complement existing reference models and other architectural specifications.

• The Building Blocks Team identifies fundamental NCO-enabling components that have been assessed by interoperability guidelines recommended by NCOIC.

• The Customer Requirements Team analyzes customer architectures, capability needs, and mandated standards to identify commonalities, synergies, conflicts, gaps, and areas for improvement.

• The Education and Outreach Team promotes awareness, adoption, and use of NCO principles and interoperability guidelines.

• The Engineering Processes Team promotes uniform systems-engineering methods, tools, and processes for the development and use of NCOIC engineering deliverables.

Defense companies, large-scale systems integrators, information technology providers, government agencies, and academia have joined to work in concert with advisory bodies of government officials, standards groups, and other stakeholders to develop a standardized technical approach emphasizing existing standards and commercial, off-the-shelf (COTS) technologies.

Though departments and ministries of defense around the world have been the earliest adopters of NCO capabilities, the consortium from the outset committed itself to taking into account the needs also of non-military national security, intelligence, first responders, law-enforcement ministries, and other civilian agencies, as well as, eventually, vertical markets such as finance and merchandising.

Furthermore, NCOIC sought from the start to serve a global audience of stakeholders. Membership in NCOIC is open to virtually the entire international community, and, in fact, a substantial portion of the consortium’s membership is headquartered in Europe.

“When we first started out, there was some thought that we had to create country-specific areas and keep some documents separated by nation,” said Sheryl Sizelove, current chair of NCOIC’s technical council. “But we quickly came to realize that was not the way to go. To really interoperate, we must all share in the same information and, in this way, break down the barriers that have kept systems from interoperating. …

“We must live the network-centric vision. NCOIC is effectively a laboratory, an experiment, that is beginning to make a real difference.”

Complementary Efforts, Unique Results

Various working groups and standards bodies have been working for many years on aspects of NCO, but NCOIC competes with none of them. Rather, the consortium complements the other organizations’ valuable efforts and is committed to affiliating with them so that collective NCO activities continue to advance.

NCOIC occupies a previously unfulfilled niche. No other organization has a charter of bringing together commercially available technology, processes, and standards to recommend a unified technical approach that all of industry and government may use, free of charge. NCOIC is a unique forum in which any product based on open standards may be brought to the table for engineering analysis.

NCOIC develops specific engineering tools based on network-centric principles (e.g., enhancing interagency synergy and mission success requires secure information exchange) as opposed to solution-centric architectures that were engineered to meet an agency’s specific needs for a particular, ultimately “stove-piped” system.

With more than 85 member organizations and growing, NCOIC’s broad base of technical experts has been able to leverage exponentially an array of experience, intellectual capital, and domain expertise as one cooperative entity with the ability to educate, formulate, and—most importantly—deliver.

NCOIC Deliverables

Over the course of less than three years, NCOIC has rolled out a series of deliverables that work together to define a unified approach within which industry can create network-centric systems and solutions that all interoperate.

NCOIC crafted a lexicon document—openly available and free of charge as a downloadable file at www.NCOIC.org—as its initial deliverable to enable companies to speak the same language and engage in meaningful discussions. There previously existed a wide disparity of ideas about these definitions.

Even the definition of NCO itself was reviewed and approved by NCOIC: “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 greater degree of self-synchronization. NCO is the application of the fundamental tenets of Network-Centric Warfare to aspects of national security, especially industry support for the missions of both the DOD and the Department of Homeland Security (DHS).”

“One of the interesting things that we found was that all of the good words are already taken,” said Hans Polzer of Lockheed Martin, a Tier 1 member of NCOIC. “And most of the interesting terms had more than one meaning, in different contexts and domains. … But we had to get people on the same page up front, and the lexicon was a means of doing that.”

continues on page 17
Spurring NCO by Fostering Interoperability
Continued from page 16.

Subsequently, NCOIC released two interrelated deliverables, NCOIC Interoperability Framework (NIF™) and Network Centric Analysis Tool (NCAT™), that comprise a unique offering for system designers, engineers, and integrators responsible for ensuring systems seamlessly interoperate with other components in a multi-vendor procurement environment.

**NOCIC Interoperability Framework (NIF™)**

The NIF describes the building codes or standards and components to select when building, organizing, and relating applications, data, and communications—and how to put them together for an interoperable system. Future NIF releases will go further to contain the actual building codes or protocol functional collections that will enable net-centricity for specified missions.

The NIF addresses the entire spectrum of interactions among network-centric system elements—from infantry soldiers to back-office operations, from the physics of transmissions over wires or antennae to the semantics of information models. In the NIF Technical View shown in Figure 1, horizontal elements represent protocol layers in a manner analogous to the Internet Reference Model. The dashed-line box illustrates the pervasive nature of the “Global Aspects,” properties of the communications environment (e.g., information assurance, mobility, Quality of Service) that apply to many different system elements. The vertical elements represent “Protocol Functional Collections,” application-specific collections of protocols chosen from each protocol layer.

Figure 2 illustrates how a typical wide-area network (WAN) router might be described using the NIF. This particular router has two Ethernet interfaces, eth0 and eth1, where each makes use of the 802.3 Logical Link Control (LLC) data link protocol. The router also contains a tdm0 T1 WAN interface that uses the High-Level Data Link Control (HDLC) data link protocol. The two Protocol Functional Collections, Ethernet with 802.3 and T1 with HDLC, have null network, transport, infrastructure and application protocols layers. The NIF shows that the router can be attached to Open, Shortest Path First (OSPF), Routing Information Protocol (RIP)/RIPv2 and Border Gateway Protocol (BGP) networks and can forward packets using either IPv4 or IPv6.

**Network Centric Analysis Tool (NCAT™)**

The NCAT (Figure 3), available to NCOIC member companies and selected government agencies by contacting the consortium, answers the question, how net-centric is a given system? Either during the design phase or once a legacy system is selected for a network-centric environment, the NCAT tool continues on page 18
### II. Information Assurance/Safety

#### Design Te net : Net-Centric IA Strategy

1. [F] Does the program have a documented Net-Centric Information Assurance Strategy?

<table>
<thead>
<tr>
<th>N/A</th>
<th>The program is not aligned with a documented Net-Centric Information Assurance Strategy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>The program is aligned with the Net-Centric IA Strategy only in 25% of the objectives (Identity Mgmt., Confidentiality, Threat Mgmt., Availability).</td>
</tr>
<tr>
<td>N/A</td>
<td>The program is aligned with the Net-Centric IA Strategy only in 50% of the objectives.</td>
</tr>
<tr>
<td>N/A</td>
<td>The program is aligned with the Net-Centric IA Strategy only in 75% of the objectives.</td>
</tr>
<tr>
<td>N/A</td>
<td>The program is fully aligned with the Net-Centric Information Assurance Strategy.</td>
</tr>
</tbody>
</table>

To ensure there is a documented Net-centric Information Assurance Strategy and to evaluate how well the program is aligned with it. Explain how the program is aligned with the documented Net-Centric Information Assurance Strategy. If not, when is it programmed to be aligned?

Planned Ans: 0 - N/A  
Achieved Ans: 0 - N/A

**Rationale:**

#### Design Te net : Net-Centric IA Posture and Continuity of Operations

2. [F] Has a Mission Assurance Category and Confidentiality Level been identified for this program and is it documented in the capabilities document?

<table>
<thead>
<tr>
<th>N/A</th>
<th>A Mission Assurance Category and Confidentiality Level has not been identified for this system, nor is it documented in the capabilities document.</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>A Mission Assurance Category is identified but not a specific level of confidentiality but it is not documented.</td>
</tr>
<tr>
<td>N/A</td>
<td>A Mission Assurance Category and Confidentiality Level has been identified for this system and but is not documented in the capabilities document.</td>
</tr>
<tr>
<td>N/A</td>
<td>A Mission Assurance Category and Confidentiality Level has been identified for this system and but is only partially documented in the capabilities document.</td>
</tr>
<tr>
<td>N/A</td>
<td>A Mission Assurance Category and Confidentiality Level has been identified for this system and is fully documented in the capabilities document.</td>
</tr>
</tbody>
</table>

To evaluate how Mission Assurance Category and Confidentiality Levels are identified for this system and the status of appropriate documentation in the capabilities document.

Planned Ans: 0 - N/A  
Achieved Ans: 0 - N/A

**Rationale:**

3. [F] Is the assigned Mission Assurance Category and Confidentiality Level appropriate for this system in context with the Net-Centric operational, systems architectures and technical standards within which it will function?

<table>
<thead>
<tr>
<th>N/A</th>
<th>The assigned Mission Assurance Category and Confidentiality Level is not appropriate for this system in context with the Net Centric operational, systems architectures and technical standards within which it will function.</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>The assigned Mission Assurance Category and Confidentiality Level has been determined to be only partially appropriate for this system in context with the Net Centric operational, systems architectures and technical standards within which it will function.</td>
</tr>
<tr>
<td>N/A</td>
<td>The assigned Mission Assurance Category and Confidentiality Level is appropriate for this system in context with the Net Centric operational, systems architectures and technical standards within which it will function.</td>
</tr>
</tbody>
</table>

To evaluate how appropriate Mission Assurance Confidentiality and Confidentiality Levels are for this program’s net-centric environment (architecture, compliance with technical standards and operational functioning). Failure to ensure these system characteristics are identified in capabilities documents will adversely impact all Information Operations in a Net-Centric environment.

Planned Ans: 0 - N/A  
Achieved Ans: 0 - N/A

**Rationale:**

---

**Figure 3:** Sample of NCAT Interface  
*continues on page 19*
measures its interoperability. This provides critical information to weigh in deciding, for example, whether to upgrade or mature a particular legacy platform. The NCAT is flexible, adaptable, and customizable for specific requirements.

“The initial version of the NCAT had a tightly coupled set of net-centric assessment criteria from the DOD net-centric checklist,” Polzer said. “What we ran into was that the DOD checklist was not one that many European agencies or even U.S. civilian agencies would agree to use. ... How people want to measure net-centricity depends on what those people in particular are trying to achieve. So we decided we had to separate the criteria set from the assessment tool itself.” That determination helped lead to a third element of the NCOIC suite that is currently in development.

**Systems Capabilities Operations Programs and Enterprises (SCOPE) Model**

The SCOPE Model will enable a system architect to assess a broad range of interoperability requirements before system design begins. SCOPE could be used to assess the qualities of a set of capabilities as they currently exist or to define the objectives for a set of capabilities to be built or evolved in the future. Currently in the final stages of development, the SCOPE Model will complete the consortium’s review and approval process in the first quarter of 2007. Interested organizations can track its progress by visiting www.NCOIC.org or arranging with NCOIC to contact the chairs of the appropriate working groups.

**Conclusion**

As customer requirements evolve, NCOIC will continue to mature its tool set. And with each new member, advisor, or affiliate, the effectiveness of NCOIC multiplies. For example, in October, NCOIC added its first government member, the U.S. Defense Information Systems Agency (DISA), “and we have statements of intent from other agencies,” Sizelove said.

This is an especially important milestone in the consortium’s evolution. With government agencies collaborating directly, the consortium is even better positioned to meet its goal of accelerating the development and deployment of NCO solutions that fit government and industry needs alike. Some agencies have, indeed, openly stated intentions to incorporate NCOIC criteria in their acquisition processes and decisions.

“In my thinking, the ultimate measure of NCOIC’s impact would be reading an RFP from a civilian or government agency and see that the system it will acquire must be shown to be NCOIC compliant to achieve what it needs to do,” Bowler said. “That doesn’t mean we have to get to that point to be successful. Certainly if all the people who respond to an RFP are compliant, then that, too, is helping ensure interoperability and further NCO.”

Already, NCOIC is helping government address the challenges of our time and enhance the competitiveness of its member companies.

**About the Authors**

Mark K. Bowler, NCO Strategist, NCO Architecture Engineering Org., The Boeing Company

Mark Bowler is chair of the NCOIC Architectures and Standards Analysis team (ASA), where he works with the chairs of ASA’s five technical Working Groups to manage their activities and to insure that Consortium’s deliverables are progressing according to plan. Mr. Bowler is employed by the Boeing Company, where he is a manager and the Network Centric Operations Strategist for Boeing’s Advanced Systems - NCO Architecture Engineering organization. There, he is responsible for creating strategies for the development and implementation of NCO systems. Mark has been involved with the NCOIC since its inception.

Mark has more than 25 years of experience in the development of advanced systems, including battle management command and control systems, space-based infrared surveillance, infrared sensors and guidance systems, laser communication systems, tactical air-to-air missiles, signal processing, optical system design, and cryogenic systems. Recent assignments have included assessment and development of core technologies for missile defense command & control systems. He has held various management and principal investigator positions in systems engineering and technology development since joining the Boeing Company in 1997.

Mark has a bachelor’s degree in physics from the University of California, Irvine, with graduate studies in systems engineering, electro-optics, infrared technology, and linear systems.

Hans W. Polzer, Net Centric Integration, Integrated Systems and Solutions business areas, Lockheed Martin

Hans is a Lockheed Martin Fellow, working for the Net Centric Integration organization within Lockheed Martin’s Integrated Systems and Solutions business area. In that capacity, Hans is responsible for developing, implementing, and evolving a net centric assessment framework to apply to major Lockheed Martin programs. These assessments are aimed at facilitating and improving interoperability within and among systems delivered by Lockheed Martin to its customers. Hans is also the lead Lockheed Martin technical representative to the Network Centric Operations Industry Consortium (NCOIC), acting as vice-chair for the NCOIC Services and Information Interoperability Working Group.

continues on page 20
Spurring NCO by Fostering Interoperability
Continued from page 19.

Hans previously was manager of the Horizontal Integration Technology Team at Lockheed Martin Mission Systems, responsible for a number of joint ACTD programs and joint interoperability initiatives. Hans was director of engineering on the Global Transportation Network (GTN) program, responsible for all engineering staff and processes and managing the development of the initial delivered system. Prior to that he was Lockheed Martin's director of the DARPA Software Technology for Adaptable, Reliable Systems (STARS) program. He joined Lockheed Martin in 1985 as Chief Engineer on the Integrated Automated Intelligence Processing System (IAIPS), a large scale operational intelligence system for the US Navy.

A 1969 graduate of Massachusetts Institute of Technology, Hans has a BS degree in physics. He received an MS degree in physics from Rutgers University in 1971. He joined the US Army that year and reached the rank of captain before leaving the Service in 1976. While in the Army, Hans was assigned to the US European Command Intelligence Data Handling Division where he was instrumental in implementing a number of distributed intelligence computer system initiatives. He joined Logicon in 1976 and managed a number of national-level intelligence and command and control software implementation projects before coming to Lockheed Martin.

In April 2003, Sizelove was named Chief Engineer for Strategic Architecture, the Boeing organization chartered with developing and integrating network-centric architectures and operations across the Boeing enterprise and for demonstrating Boeing's NCO vision at the Boeing Integration Centers (BICs). In 2005, Strategic Architecture was realigned after having laid Boeing's technical strategy for network-centric operations (NCO).

Previously, Sizelove supported Connexion by Boeing, initially as Software Architect, and later as Information Architect. From 1993 to 1997, Sizelove worked overseas in Australia, supporting the integrated combat system of the Royal Australian Navy's new submarine program, holding the positions of Software Architect, Team Lead and Software Development Manager.

From 1979 to 1992, Sizelove owned and operated a software consulting firm, Sizelove Computer Systems, Inc., serving clients within the aerospace industry.

She received a bachelor of arts degree in Mathematics from California State University, Long Beach, and a master of science degree in Computer Science from the University of Southern California.

Originally from Joplin, Missouri, Sizelove and her husband, Phillip, currently reside in Newport Coast, California. She enjoys cooking, hiking, exercising, and watching Pacific Ocean sunsets.

Author Contact Information
Mark Bowler: global-architectures-chair@global.ncoic.org
Hans Polzer: hans.w.polzer@lmco.com
Sheryl Sizelove: sheryl.sizelove@ncoic.org
Two Great Reliability Solutions from the RAC & DACS

System Reliability Toolkit

The RIAC/DACS System Reliability Toolkit provides technical guidance in all aspects of system reliability, allowing the user to understand and implement techniques to ensure that system and product designs exhibit satisfactory hardware, software and human reliability, and to minimize the inherent risks associated with deficiencies in system reliability.

To purchase, please contact:
The Reliability Information Analysis Center
6000 Flanagan Road
Suite 3
Utica, NY 13502-1348
1-877-363-RIAC http://theRIAC.org

The DACS Software Reliability Sourcebook

This first edition of the DACS Software Reliability Sourcebook provides a concise resource for information about the practical application of software reliability technology and techniques. The Sourcebook is divided into nine major sections, plus seven supporting appendices.

To purchase, please contact:
The Data & Analysis Center for Software
775 Daedalian Drive
Rome, NY 13441-4909
1-800-214-7921 http://iac.dtic.mil/dacs/
DoD Netcentricity... a Buzzword or a Business Model?
By Chris Gunderson, Brian O’Neill, and Stephen R. Macdonald

Abstract
The U.S. Department of Defense can jump start a marketplace for certified net-ready tools that enable trusted transactions of valuable information at the right time by investing in an open not-for-profit environment that enables intellectual property distribution, open collaboration and commercial risk mitigation through adaptive validation, verification and certification processes. The concept has worked for other government agencies, and the pieces are in place for DoD to capitalize on their lessons learned. There is no lack of understanding of the issues or the desired outcome. What is required for success is imagination and leadership to execute.

Executive Summary
DoD leaders recognize that their vision for Netcentric Operations enabled by the Global Information Grid (GIG) is stymied by DoD’s current slow, hierarchical, conservative, acquisition process. E.g. Lt Gen Croom, Director of DISA, advocates adapting a commercial e-business model for fielding the GIG [1].

Ms Payton, then Deputy Undersecretary of Defense (DUSD) for Advanced Systems and Concepts (AS&C), has advocated adapting “Open Technology Development” by following the commercial open source model [2]. Both therefore agree that DoD needs: (a) a flat, innovative, acquisition model for information processing capability; and (b) a more open and agile architectural model based on Internet best practice that is not as adverse to risk.

The former requires focus on trusted transactions of valuable information at the right time; the latter requires an open infrastructure providing for a modular “value off-the-shelf” approach and a “just try it” mentality. Emerging DoD policies that, after all, intend to bring about change, should be used to develop a lightweight acquisition process that enables this progressive approach to information architecture. The issue is that a conservative hierarchy like DoD is not equipped to develop rapid, flat, innovative process models that embrace risk and accept failure.

An external agent is required to help government catalyze that change. Industry can and has partnered with government to provide such catalytic agents in other market sectors (e.g. medicine, weather, distance learning). The common elements are: broad lucrative commercial market for off-the-shelf offerings that also serve government interests; an independent non-government not-for-profit organization, the World Wide Consortium for the Grid (W2COG) Institute [4], chartered as a Government/Industry Collaboration; a government regulatory activity to mitigate commercial risk through certification of commercial offerings; an open license model that channels intellectual property, developed by government research, efficiently to industry.

There is a potentially lucrative commercial market for artifacts that support the DoD’s net-centric objectives. These objectives rely on trusted transactions of valuable information at the right time. For example, the current commercial market does not adequately address privacy, security, and the information value chain. Search engines and associated portals, like Google and Yahoo, represent the state of the art in information processing on the Internet. However they do not efficiently filter information or provide a truly private and/or secure environment for transactions. Further, the commercial state of the art in the necessary semantic and security technology is immature. Nevertheless, all agree that there is a value proposition for Internet offerings that manage information overload while simultaneously improving security. One could realize this value by providing, an e-portal that provides government-approved “consumer reports,” and an online catalog to connect developers and consumers of off-the-shelf products and services that enable trusted exchanges of valuable information.

The Joint Interoperability Test Command (JITC) [visit http://jitc.fhu.disa.mil/] has been given a recent mandate to create a test and evaluation methodology to accelerate delivery of Service Oriented Architecture (SOA) based information processing capabilities. As a working capital major test range, JITC is chartered by US Title X to work closely with, and accept resources from industry for test and evaluation (T&E) [3]. JITC will use that Title X authority to serve as a single point of contact, i.e. a low friction netcentric certification office for industry to seamlessly collaborate with a distributed network of government laboratories. The product will be an adaptive certification process and an easy to use “consumers’ report” that documents comparative characteristics of various information processing products and services.

The Office of Secretary of Defense (OSD) has created a non-government not-for-profit organization, the World Wide Consortium for the Grid (W2COG) Institute [4], chartered as follows:

Conduct ~90 day projects that:
• Deliver studies, demonstrations, and prototypes in an environment compliant with Title 10, but not constrained by the Federal Acquisition Regulation
• Bundle off-the-shelf capabilities
• Include self-selected expert teams of operators, developers, and testers

continues on page 23
DoD Netcentricity...a Buzzword

Continued from page 22.

• Protect participants with an intellectual property rights (IPR) policy that allows both open source and open standards licenses
• Demonstrate trusted delivery of valuable information at the right time
• Perform, document, and post all the above in an open, collaborative, dynamic, run-time “GIG-lite.ORG” environment

JITC and the W2COG Institute have joined forces to embed distributed adaptive, collaborative, validation and verification in a rapid SOA deployment process: a netcentric “sandbox”.

Government and industry experts, frustrated by the undue cost and complexity of the status quo, can actualize an Acquisition Lite process for accelerating the delivery of the GIG promise.

The Issue

The director of the Defense Information Systems Agency (DISA), Lieutenant General Charlie Croom, frequently explains that netcentric operations are essentially equivalent to excellent e-business practices. After all, “netcentric operations” means innovative, ultra efficient, horizontally distributed (i.e. flat rather than hierarchical) process similar to that employed by Google, e-Bay, Linux, Amazon.Com, FedEx, et al [5]. General Croom and his senior staff use these examples from e-business to describe a vision of DISA as a superb GIG Service Provider partnering, netcentrically, as a peer of the best industrial experts in information processing/sharing [6]. His implication is that companies interested in capturing a share of the multi-billion dollar DoD annual spending on information processing should sniff the change in the wind.

Then Deputy Undersecretary of Defense for Advanced Systems and Concepts, Ms. Sue Payton, commissioned a road map plan for open technology development [7]. This report exhaustively and compellingly makes the case that collaborative open source and open standards approaches to software development are prevalent among the most successful commercial enterprises and must be adopted by the Defense Department to achieve information superiority. The report suggests a number of actions the DoD should take within its acquisition process to adopt those e-business best practices. Executing these actions will require adaptive, cross-program collaboration, i.e., netcentric engineering, among the Defense Acquisition Community and others. The implication is that senior OSD leadership demands a change in the defense acquisition landscape.

Frankly, the DoD and the Defense Industry, constrained by a bureaucratically stifling acquisition practice, simply do not collaborate netcentrically with each other. Together, they forged a rigid relationship around a marketplace they created to deliver major weapon systems like tanks, ships, airplanes and missiles. In this environment, procurement spending generally occurs in programmatic stovepipes. Large improvements in capability are fielded as expensive new pieces of equipment over the course of several years. Science and technology research, requirements formalization, engineering, and acquisition occur in rigid serial sequence. Information processing capability, e.g. software, is treated as a lesser included element in this process. It is therefore not surprising that the defense industrial marketplace has very little impact on the development of commercial information processing technology [8]. If DoD and the Defense Industry are to collaborate netcentrically, they will need new process models. In fact, they need a completely new arena, a net-ready marketplace, where they can develop and consume continuously improving information processing/sharing components on Internet time scales.

Some Success Stories

Very few insiders in the DoD acquisition community would dispute this analysis. These insiders cynically doubt that government is capable of making the necessary deep changes in process to emphasize “doing vs. knowing” [9], and improving the status quo. Cynicism notwithstanding, government/industry behavior models to create this new marketplace exist today. Strong leaders have deliberately executed these models to bring about the requisite transformation. Here are some examples of government/industry partnerships that have succeeded in accelerating innovation for the public good:

1. The Food and Drug Administration (FDA) exerts huge influence over the vastly profitable Pharmaceutical Industry. FDA mitigates commercial risk by providing a government certification process. The first firm to get to market with an FDA approved medicine is virtually guaranteed huge profits. The FDA certification also mitigates the threat of law suits. Further, the government invests heavily in medical research, effectively seeding pharmaceutical industrial innovation. The Pharmaceutical Research and Manufacturers of America (PhARMA) web site quotes the Wall Street Journal and other sources to make the case that United States governmental policy offers pharmaceutical companies an environment that “reward[s] innovation” through a “comparatively free medical market.” [10]

2. Government and industry have partnered as peers in the Advanced Distance Learning initiative. Together, in a public/private not-for-profit forum they have agreed on standard formats for digital “learning objects.” The result is a commercial market for tailored just-in-time, training and education products. The vendors in this industry all have access to multi-domain data sources provided by the

continues on page 24
government. They profit by adding value to the way the information is processed, packaged, and delivered [11].

3. The relationship between the National Weather Service (NWS) and the Weather Industry at large is instructive. Not so many years ago, the Weather Service was the main source of weather forecasts in the United States. The US government created the US Weather Industry, virtually overnight, by getting the NWS out of the specialized forecast business, and restricting it to delivering government certified data instead. Now the NWS invests heavily in scientific research and delivers continuously improving digital data as “open source” to the public. Industry adds value and re-packages it in countless profitable applications. Government, industry, and private citizens have all benefited from quantum improvement in over-all forecast capability generated by government and industry contributing what each does best [12].

A Way Ahead

DoD sustains a defense industrial market geared toward fielding complex, specialized, rugged, pieces of equipment on 5-10 year cycles. Within that defense industrial market, the Government and its prime contractors behave as ordinary retail consumers of commercial information technology. As the examples above show, the Government could choose to catalyze a complementary new market sector, aimed at rapid innovation. What’s needed is a net-ready market for continuously improving digital data as “open source” to the public. Industry adds value and re-packages it in countless profitable applications. Government, industry, and private citizens have all benefited from quantum improvement in over-all forecast capability generated by government and industry contributing what each does best [12].

R&D investments and regulatory efforts to incent information assurance and distribution of valuable information at the right time. After all, the US Government’s requirement for better information processing/sharing capability is especially compelling; its investment in IT scientific research is large compared to its overall market share; and it has a mandate to appropriately regulate and incentivize industry at large.

Success with such an approach requires two architectural imperatives.

1. Deliver Trusted Valuable Information at the Right Time (VIRT): an approach to the increasingly vast market place of data that encourages careful choices regarding how valuable time is spent “buying” and “consuming” information. We get competitive advantage from finding opportunity and acting quickly. We gain if we can quickly achieve the trust that allows us to partner quickly and share valuable information. We lose competitive advantage if we waste time processing insignificant data or keeping potentially synergistic information in a stovepipe. Expediting decisions on critical information makes money and wins battles. A decision made too late is not a useful decision [16].

2. Reuse Value Off The Shelf (VOTS): an approach to delivering “good enough” capability fast enough to take advantage of the rapid advances taking place in the information technology market. This approach emphasizes reusing and bundling interoperable off-the-shelf components in an architecture optimized for Trusted VIRT. (See Figure 1.) We get competitive advantage from finding opportunity and acting quickly. We lose our advantage if we waste time on processes that are inherently too slow to exploit current opportunities. Expediting delivery of capability makes money and wins battles. A system fielded after the battle is not a valuable capability [17].

See SIDEBAR-1 for a discussion of the characteristics of a VIRT architecture and VOTS delivery platform. Notice that, consistent with the e-Bay example discussed in the sidebar, the Trusted VIRT and VOTS architectural imperatives depend on an entrepreneurial market and behavioral model. Neither DoD’s operational nor acquisition doctrine address entrepreneurial market models. As previously explained, both dictate disciplined hierarchies with associated rigid behavior models. Net-centric transformation requires change and adoption of this value-oriented approach focused on behavior across the enterprise. A pre-deterministic architectural approach that aims to carefully define and build toward a concrete future state of the enterprise is doomed to failure. Static, formal, architectural documents...
SIDEBAR 1: Trusted Valuable Information at the Right Time (VIRT) Architecture and Value Off the Shelf (VOTS) Delivery Model

Trusted VIRT architecture improves effectiveness by increasing the fraction of time spent processing valuable information. Important characteristics of Trusted VIRT-based architectures include the following:

- Enables Operators to request “bids” from various potential providers to satisfy information requirements for specific tasks and desired outcomes
- Performs authentication, authorization, and audit to ensure sensitive information can be shared in real-time on the basis of dynamic risk/reward considerations
- Provides multi-faceted computer network defense [i]
- Delivers context-sensitive information culled by intelligent agents that detect significant changes in the state of important parameters
- Rewards information providers whose products tangibly enhance productivity
- Includes automated and multi-faceted computer network defenses that discover and punish malicious activity
- Pressures operators to make effective selections of information and information sources
- Applies pressure to operators and information providers to reinforce and improve productive choices
- Decomposes mission performance threads into information value delivery chains, comprising essential tasks, desired outcomes, and information exchange elements
- Analyses mission threads to determine objective value characteristics of information exchanges
- Determines productivity based on mission outcomes, where “productivity” = value/bit exchanged
- Establishes specifications and associated performance metrics based on this definition of productivity
- Continuously implements and improves all of the above

[continues on page 24]


Data & Analysis Center for Software (DACS)
DoD Netcentricity...a Buzzword

Continued from page 25.

SIDEBAR-1: (continued)

A VOTS delivery process continually increases the productivity of employed systems by drastically reducing the time, cost, and bureaucratic friction for implementing improvements. This process:

- Delivers Trusted VIRT products and components that work immediately, “out of the box,” in standard computational environments
- Allows customers to shop for Trusted VIRT products and components from various potential providers to satisfy specific information requirements for specific tasks and desired outcomes
- Tangibly rewards providers of Trusted VIRT products and components that tangibly enhance productivity.
- Pressures program managers to make effective selections of Trusted VIRT-enabling components
- Values products or components only on their ability to enhance operators’ productivity where productivity ~ effect/effort.
- Establishes metrics and performance criteria that depend on the ability of a product or component to deliver information in ways that demonstrably enhance value
- Continuously implements and improves all of the above

There are impressive examples of VIRT architectures and VOTS delivery processes in the commercial marketplace. These propagate quickly and allow trusted exchanges across widely distributed communities of interest, but within the bounds of relatively static partnerships. The on-line auction house e-Bay is one such example. Developers at eBay continuously improve methods to reach across the Internet and connect widely disparate providers and consumers of valued commodities. The e-Bay auction shows the power of VIRT operational architecture. Recall the VIRT productivity model: Productivity ~ Value/Bit. Multiple buyers and sellers who were previously unknown to each other, but who have defined their individual conditions of interest to the market at large, all learn of an emergent opportunity associated with their mutual interests immediately. They agree on the value parameters in a short sequence of low bit exchanges; execute a trusted transaction immediately upon agreement of value parameters; and learn lessons about how to improve their outcome the next time. The e-Bay development method shows the power of a VOTS delivery process. Globally distributed and disparate software service providers share an on line development environment. This environment employs the same family of tools and methods (e.g. subversion open source configuration management software) that allow huge open source collaborative projects to discover existing capabilities, form partnerships among developers, check out code offerings, and bundle and/or improve those offerings. Consequently, the e-Bay experience continuously improves for all its community members as a result of facilitated collaboration among those community members.

Given this landscape, the DoD can achieve its goals by nurturing a net-ready marketplace for products and services that deliver trusted VIRT. Two appropriate governmental activities are necessary: (a) mitigate commercial risk through a carefully designed government certification process; and (b) make government-owned intellectual property readily available to potential developers of net-ready capability. To be successful, this net-ready marketplace must provide a convenient means for government and the Defense Industry to evaluate, compare, and consume continuously improving off-the-shelf net-ready offerings. In addition, the strategy should recognize that there are thousands of other organizations worldwide that have similar concerns. These organizations need better ways to share information, make more effective decisions, and perform Internet transactions with reduced security risks. The Government should deliberately tap the innovative energy of this large, motivated, global community.

Study of the government/industry process models that have successfully fostered targeted commercial innovation reveals three key success factors:

1. A government process mitigates commercial risk by verifying, validating, and certifying valued capabilities
2. A collaborative government/industry merit based process evaluates candidate solutions
3. An industry process identifies and propagates best practices

Because the goal is to accelerate availability of better information sharing and decision-making capabilities, these processes should be woven together netcentrically. That is, all three processes should be concurrent, rapidly innovative, and deliberately focused on critical opportunities and threats. Fortunately there is a new project that aims to create the government/industry partnership necessary to do just that. It is called the Netcentric Certification Office initiative and is sponsored by DISA’s Joint Interoperability Test Command (JITC) (http://jitc.fhu.disa.mil/) as part of their effort to help developers and consumers accelerate fielding of net-ready capability bundles. This collective effort is nicknamed the netcentric “sandbox”. See SIDEBAR 2.

To support the sandbox concept, JITC is designing a new flavor of rapid, adaptive, collaborative, and distributed validation and verification appropriate for SOA. The approach will team operators, developers, and testers in rapid innovation spirals. Test and evaluation will be a distributed service across many

continues on page 27
laboratories and will share cumulative lessons learned. Rather than an onerous milestone on a traditional system delivery pipeline, net-ready certification process will be flexible “living” engineering implementation guidance that grows from mutual agreement by operational customers, developers, and testers. This adaptive collaborative validation and verification will use mission-models in pre-deployment simulations [21] followed by post-deployment audits, i.e. on line tests of bundled VOTS components. This approach to validation of requirements and verification of their satisfaction eliminates formal, detailed, documentation of requirements and subsequent testing against rigid specifications. Instead, operators, developers, and testers explore the art of the possible in context and together discover ways to enhance information value chains associated with important use cases [22]. (See SIDEBAR 2) The results of the test and evaluation will be readily available on line in a comparative format, i.e. a “consumers’ report” metaphor.

SIDEBAR 2: Community of Interest in the Netcentric Sandbox

The Office of the Secretary of Defense has introduced the notion of “Communities of Interest” to flesh out the details associated with these imperatives, but has not yet defined the specifics of the community activity [i, ii]. The netcentric “sandbox” initiative suggests a method.

To field netcentric capability, communities must understand netcentric requirements, i.e., define the specific characteristics of information “value” for a given application. The value of information depends on its ability to improve productivity. Often we struggle to define “productivity” in the context of information processing activities. One proxy for productivity is “speed to better decision.” After all, “speed to better decision” correlates directly to “time not wasted evaluating irrelevant information.” By analyzing specific, critical, recurring, mission threads, communities can quantify both “speed” and “better” in terms of the information exchange elements associated with particular families of recurring decisions, and thereby define the Trusted VIRT requirement.

Consider this hypothetical scenario. A commander wants to find and kill an elusive mobile target. The operational use case, i.e. “mission thread” or “kill chain” might be as follows: receive “tipper” on SECRET tactical circuit; confirm validity of tipper via TOP SECRET network information (3 hrs); evaluate risk of collateral damage with coalition members via UNCLAS and SECRET network (1 hr); evaluate and select weapon options with coalition members via SECRET and UNCLAS network (3 hrs); kill target (2 hrs); assess and report results with coalition members via various networks and circuits (9 hrs). (Times are notional and arbitrary examples.)

This analysis might lead to measures of effectiveness as follows. (All service levels are notional and arbitrary examples):

**Acquisition objective:** Decrease time required to field increment of new capability (Target Service Level = 90 days to service level upgrade)

**Operational objective:** decrease kill chain cycle time (Target Service Level = 66% ); increase probability of kill (Target Service Level = 80%)

**Information Assurance objectives:** Unintended disclosures do not occur (Target Service Level = 0 disclosers); Malicious denial of service does not occur (Target Service Level = 0 unscheduled down time)

**Technical objective:** Fielded artifacts have adequate performance and reliability characteristics (Target Service Level = Carnegie Mellon Software Maturity Level 2-3)

A community of interest could pool resources in the GIGLite.org netcentric sandbox to:
- Digitally model and simulate the mission thread(s) of interest. Register the mission thread(s) in the GIGLite.org library.
- Search dynamic GIGLite.org library for existing capability bundles that might add value.
- Invite innovative suggestions from a GIGLite.org community of developers about how to bundle various collaborative, security, and information processing services in ways that might achieve the service level targets.
- Analyze options
- Compose demos
- Perform rapid, adaptive, collaborative verification and validation based on modeled mission threads and targeted measures of effectiveness. Team developers, operators, and testers and adapt requirements as appropriate.

DoD Netcentricity...a Buzzword

Continued from page 27.

SIDEBAR-2: (continued)

- Develop prototypes.
- Perform Operational test of prototype by deploying it and auditing actual performance with respect to targeted measures of effectiveness.
- Certify reference implementation. Document hardware, software, interfaces, doctrine, training, and caveats required to achieve demonstrated capability.
- Deliver certification detail to e-portal marketplace to allow comparison shopping.
- Purchase COTS products as necessary to scale capability across domain of interest.

This entire process will take about one year. When mature, increments of increased capability will be fielded quarterly.

The not-for-profit World-Wide Consortium for the Grid (W2COG) Institute, (www.w2cog.org), is helping to create the netcentric sandbox. The W2COG Institute was created by a Secretary of Defense project designed to accelerate progress on the Global Information Grid (GIG). The idea was to capture successful practices from Internet interoperability consortia like the Worldwide Web Consortium, the LINUX open source community, the Internet Task Force, etc. Accordingly, the W2COG Institute has introduced a non-hierarchal process and open intellectual property rights model for rapidly identifying experts and selecting netcentric project teams that include members from industry, academia and government. These projects employ open source and open standards methods to bundle government and commercial software to solve compelling information processing problems. This activity is carefully designed to comply with US Title 10 rules for industry and government interaction, but to fall deliberately outside the boundaries of the Federal Acquisition Regulations (FAR). The result is a framework that allows government and industry to pool resources and learn lessons quickly [23].

Taking a cue from the way successful businesses rapidly and adaptively employ SOA, and applying the transformational intent of emerging GIG policy, the netcentric sandbox will enable a lighter weight version of the DoD Acquisition process, call it “Acquisition lite” that will:

- Collaboratively adapt information processing requirements and doctrine with science and technology on-the-fly
- Team up operators, developers and testers
- Capture and share best practices
- Re-use off-the-shelf information processing capability
- Certify on the basis of demonstrated measurable improvements in mission outcome
- Field netcentric capability bundles in 90-day spirals;

The potentially disruptive innovation here is that government “study money” can be applied, and government intellectual property contributed, in an environment that complies with U.S Title 10, but is outside the bounds of Federal Acquisition Regulations [24]. Prototype capability bundles will be certified in that environment based on use cases that demonstrate netcentric value added. Vendors and labs will then independently productize their COTS and GOTS versions of the certified capability. These VOTS products will be offered in a commercial e-market portal where consumers can easily evaluate the products’ certification and customer feedback pedigrees. The DoD procurement dollars for SOA enabled information processing capability can then be spent, under the Federal Acquisition Regulations, to buy and integrate those off-the-shelf capability bundles (See Figure 2).

Figure 2: The not-for-profit “open consortium” model can provide an independent platform, GIGLite.org, for government and industry to pool resources, including intellectual property, in rapid discovery cycles that deliver government certified capability bundles. A small office, NetCert.gov, serving as single point of contact for all related government activities will streamline the process. continues on page 29
The sandbox concept will be manifested in a W2COG Institute sponsored “GIGlite.org” runtime environment. GIG-lite will use a distributed global community of experts and an open source and/or open standards model to continuously expand and improve a shared SOA foundation. Artifacts hosted in this SOA foundation will address security services for trusted data exchange; semantic and geospatial services to provide context; network monitoring services for network protection and optimization; and adaptive collaborative business services to support rapid innovation. GIG-lite will use tools and methods similar to those explained in the e-Bay sidebar as well as a suite of modeling and simulation tools. (See Figure 3.) The GIGLite.org intellectual property rights regime will carefully address the license models necessary to support cross domain development in an open architecture. A community of government, industry, and academic members has formed to build Spiral 0 of GIG-lite in the first quarter of FY07 [25].

There are clearly underserved government and industry participants in today’s expensive and complex DoD acquisition process. Capturing them, that is convincing them to try a new approach, will require attractive value propositions. For example, Government laboratories would appreciate a low friction, pre-approved method to channel their intellectual property to the marketplace and an easy pre-approved method to receive funding for industrial studies. Commercial companies would like visibility and use of government intellectual property, and convenient government certification and a channel to market to “level-the-playing field” for their off-the-shelf products and services. Operational customers need better net-ready tools specifically designed for and by them and convenient and timely delivery of those tools.

The target audience for early adoption, i.e. the underserved communities of interest, can be the producers and consumers of products and services that they consider to be “netcentric best of breed”, but have not yet been widely adopted. The bait is the opportunity to have those excellent products and services certified as net-ready, and to be the first to market in a lucrative new sector.

There are many government initiatives that meet these excellence criteria. Many information technology vendors also meet these excellence criteria. Members of both groups are frustrated by the firewall between their innovative capability, and the operational customers imposed by the rigid government major procurement model.

……Are you one of the frustrated?……Want to do something about it?

The authors invite your correspondence and involvement in our initiative.

References
DoD Netcentricity...a Buzzword

Continued from page 29.


About the Authors

Chris Gunderson

Gunderson is a Research Associate Professor of Information Science at the Naval Post Graduate School. He is on a special assignment in Reston VA sponsored by the Defense Information System Agency (DISA) Joint Interoperability Test Command (JITC) to establish a Netcentric Certification Office (NCO). The NCO will link distributed DoD laboratories in partnership with industry to create a public/private e-Business portal for delivery of government certified “net-ready” software products and services.

Prior to this assignment, Professor Gunderson managed an initiative sponsored by the Office of the Secretary of Defense to create the World Wide Consortium for the Grid (W2COG), a global network of collaborative experts committed to rapidly fielding network centric tools for enhancing global security and peaceful commerce.

Gunderson retired from the US Navy in October 2004 as a Captain following 27 years’ service.

His last assignment in the Navy was as Commanding Officer of Fleet Numerical Oceanographic & Meteorological Center, a super computer network operation center in Monterey, Calif.

Prior to command of Fleet Numerical Meteorology and Oceanography Center, Gunderson served as Deputy Oceanographer of the Navy, and helped develop Department of Defense policy for enhancing information system interoperability. He holds a BS from the U.S. Naval Academy, an MS (with honors) from the Naval Postgraduate School, and is a Fellow of the American Meteorology Society.

continues on page 31
Brian O’Neill

Mr. Brian O’Neill has developed a depth of experience in Information Technology, systems integration, and web services working as a project manager and technical architect. Brian O’Neill is currently a Technical Architect for Gestalt, LLC, a leading provider of collaborative technology for governments and Fortune 500 customers. Mr. Brian O’Neill has held numerous technical and managerial roles encompassing both strategic and tactical scope. Most recently, Mr. Brian O’Neill was Vice President of Engineering at a startup in the IP communications industry, where he was originally chief architect and lead developer of an IP telephony solution for service providers.

Brian sits on JAIN (Java APIs for Integrated Networks) expert groups within the Java Community Process and was instrumental in the design of the JAIN SIP API v.1.1 (JSR 32). Prior to that, Brian was Chief Technical Officer at another small company where he managed the development of a J2EE based SIP Server.

Mr. O’Neill also worked for one of the large Systems Integrators as a technology architect where he designed and implemented a dialog management server and development platform for VoiceXML. Brian holds a B.S. in Computer Science from Brown University and has a strong history of designing and delivering technically demanding solutions using J2EE, SIP, XML, and SOAP.

Mr. Brian O’Neill has been a featured speaker at numerous conferences for both the VoIP and java development industries, speaking on such topics as the Session Initiation Protocol (SIP) and the JAIN SIP API v.1.1. Mr. Brian O’Neill was also granted patents in the areas of artificial intelligence and natural language processing. Finally, Mr. O’Neill was selected by Sun Microsystems to host a web log on the Java.Net website regarding “Java in Communications”.

Stephen R. Macdonald

Mr. Macdonald has developed a depth of experience in Information Technology, systems integration and web services as founder, technology investor and key contributor to multiple companies seeking to provide web services. Mr. Macdonald joined Collabnet, Inc. as Director, Public Sector in February of 2006.

Prior to joining Collabnet, Mr. Macdonald served various corporations providing Federal Sector Business Development and Key Account Management on behalf of Sendmail, Inc., Tangible Software, SAIC, Pictometry International, SRM, Ltd., OTG Software (now EMC) and BDS, Inc. since 1990.

Author Contact Information

Chris.Gunderson@w2cog.org 703 262 5332
Brian.ONeill@gestalt-llc.com 215 588 6024
ssmacdonald@collab.net 540 226-374
The first 50 people to send in a completed survey will receive a FREE DoD/IT Acronym CD from the DACS.

This valuable CD-ROM contains over 9,000 Department of Defense and Information Technology acronyms. There are hundreds of acronym lists available but none are as well done as this CD AND specifically targeted towards DoD and Information Technology. This unique-shaped CD-ROM plays in your computer’s regular, hub-mounted, CD drive. You’ll use this great resource over and over again. It’s FREE, just for filling out our brief survey on the next page!

Data & Analysis Center for Software (DACS)

http://iac.dtic.mil/dacs/
Software Tech News Feedback


2. When did you receive the newsletter?  (month/year)

3. How satisfied were you with the CONTENT of the newsletter? (Article Quality)
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

4. How satisfied were you with the APPEARANCE of the newsletter?
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

5. How satisfied were you with the OVERALL QUALITY of the newsletter?
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

6. How satisfied were you with the ACCURACY of the address on the newsletter?
   - Very Satisfied
   - Satisfied
   - Neither Satisfied nor Dissatisfied
   - Dissatisfied
   - Very Dissatisfied

7. Approximately how much of the newsletter do you read?
   - The entire issue
   - Most of the content
   - About half the content
   - Briefly Skimmed
   - Didn’t Read

8. Would you read this newsletter in an E-mail newsletter format?
   - Definitely
   - Probably
   - Not Sure
   - Probably Not
   - Definitely Not

9. How did you request the product or service?
   - Phone Call
   - E-mail
   - DACS Website
   - Subscription Form
   - Other

10. Would you recommend the Software Tech News to a colleague?
   - Definitely
   - Probably
   - Not Sure
   - Probably Not
   - Definitely Not

11. What topics would you like to see this newsletter devoted to?

    Comments (Optional)

Register for the first time      Update current subscription

Name:                          Position/Title:

Organization:                 Office Symbol:

Address:

City:                         State:             Zip Code:

Country:                      E-mail:

Telephone:                    Fax:

Functional Role:

Organization Type:  Air Force  Army  Navy  Other DoD
                     Commercial  Non-Profit  Non-US  US Government  FFR&D  Other

*Note: You must give us your address to receive the CD.
About This Publication:
The *Software Tech News* is published quarterly by the Data & Analysis Center for Software (DACS). The DACS is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC). The DACS is technically managed by Air Force Research Laboratory, Rome, NY and operated by ITT, Advanced Engineering and Sciences Division.

Article Reproduction
Images and information presented in these articles may be reproduced as long as the following message is noted:

“This article was originally published in the *Software Tech News*, Vol. 9, No. 4.”

STN Spotlight
The DACS has reserved this space to highlight those who contribute to help make this excellent publication possible, or have made a significant contribution to the software domain.

Morton A. Hirschberg,
DACS STN Editorial Board Chairman

Mort has had a long and rewarding career spanning nearly 50 years within the defense community. His work began with missiles at Douglas Aircraft Company and aerospace applications at North American Aviation. In 1964 he began working at General Research Corporation modeling ballistic attacks. In 1973 he joined the Ballistic Research Laboratory at Aberdeen Proving Ground, Maryland. He became a DARPA agent in 1985, initially, for the Army/DARPA Air/land Battle Management Program, ALBM. Later, he was given more DARPA projects with academe as well as contractors. During this time he was appointed to represent the Army on Tri-Service and International software and computer projects and committees. Mort’s association with the DACS began in the mid 1990’s serving on the DACS Steering committee. Although he retired from the Federal Service in 1999, Mort continues to assist the DACS as Chairman of the Editorial Board for the DACS Software Tech News.

Mort’s formal education includes a BA in Mathematics, from UCLA, in 1957 and an MA in Experimental Psychology, from UC Santa Barbara, in 1972. He has authored or co-authored over 50 papers as well as contributing to numerous corporate papers.

Mort has this message for our readers: “The SoftwareTech News is an important part of the DACS. We strive to bring current and exciting articles of the highest caliber to our readers. So, as Chairman, I urge you and your colleagues to contribute articles.

In my career I was fortunate to have many mentors who took an interest in me. When I became a supervisor myself it was my goal to develop the people who worked under me to the fullest extent. I feel I largely succeeded in that. Now it’s your turn.”

DACS
P.O. Box 1400
Rome, NY 13442-1400
Phone: 800-214-7921
Fax: 315-334-4964
E-mail: dacs@dtic.mil
URL: http://www.thedacs.com/
In This Issue

Tech Views .................................................................1
The Role of Architecture in Moving DoD to a Net-Centric Environment ..........6
Spurring NCO by Fostering Interoperability ..............................................14
DoD Netcentricity...a Buzzword or a Business Model .................................20

Advertisement

The Software Tech News is now accepting advertisements for future newsletters. In addition to being seen by the thousands of people who subscribe to a paper copy, an electronic version is available at the DACS website, exposing your product, organization, or service to hundreds of thousands of additional eyes.

For rates and layout information contact: news-editor@dacs.dtic.mil

Cover Design by Dorene Foundos, ITT
Illustration by David Minton, Chief Engineer of the W2COG Institute.