Architecture: The Road to Interoperability

Dr. Raymond J. Curts, CDR, USN (Ret.)[1]
Strategic Consulting, Inc.
5821 Hannora Lane
Fairfax Station, VA 22039-1428
Voice: (703) 425-6983
Email: rcurts@erols.com

Dr. Douglas E. Campbell, LCDR, USNR-R (Ret.)
Syneca Research Group, Inc. (www.syneca.com)
P.O. Box 2381
Fairfax, VA 22031
voice/fax: (703) 876-0935
email: dcamp@aol.com

Abstract

Without a consolidated, coordinated, organized architecture there is little chance of ever attaining the elusive goal of total interoperability. Why is the process of identifying and developing architectures for the Department of Defense (DoD) so difficult, costly and time consuming? And, why, despite years of research and millions of dollars spent investigating the issues, is DoD still struggling to: define what exactly constitutes an architecture; identify what types of architectures do and/or should exist; categorize architecture concepts; or develop a long range plan for architecture development and maintenance? As will be presented here in more detail, a DoD architect must first be assigned at the very highest levels of the department and embodied with the responsibility and authority to enforce compliance with DoD architectural concepts.

1. Introduction

Over the years, several attempts have been made to "architect" various aspects of the Armed Services. Indeed, the concept is not new. Though described by a variety of titles, the United States military has been in the process of composing "Architectures" for many years. The actual process of "architecting" forces has been going on since the inception of armies and navies; in the case of the United States, that dates back to 1775. When the country was young and the militia small, the process was relatively easily handled by a small staff (in some cases one person) with paper, pen, and a firm grasp of military and/or naval tactics, seamanship, etc. As the force grew larger, however, more men, paper, pens, expertise (in both depth and breadth), and time were required to keep track of the current forces as well as to stay abreast of emergent technologies. To compound the problem, the military was split into several Brigades and Fleets, which were further divided into Battle Forces and Task Forces, etc. It took many years of evolution but the job eventually became overwhelming and continues to get more and more difficult and complex.

---

[1] The original research was partially funded under DEIS Contract Number DCA 100-94-D-0014, Delivery Order Number 061. The authors have independently continued additional research efforts.

Recently, the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD(C^3I)) commissioned a number of studies to review the status of architectures within the Department of Defense (DoD). The findings have been reported to a variety of offices and agencies within OASD(C^3I), all of which have been designated to support various aspects of architecture development for DoD as recommended in the Defense Science Board Global Surveillance Study. If true jointness and interoperability are ever to be achieved, the concept of a single unifying construct, however imperfect or incomplete, must receive support at the highest levels of DoD. Although the plan proposed by the authors is, no doubt, imperfect, it is, at least, a start and is offered as a first step toward a DoD-wide interoperable C^4I architecture. The missing ingredient seems to be a single unifying construct to lay the foundation for architectures that tie them together. Probably the most glaring deficiency lies in exactly the location that is causing the most dialogue and the need for architectures to begin with--the interface points. Almost all architectures designate some peripheral node as the "connection to" the systems, structures, architectures of other agencies. As one might expect, these are the nodes that are given the least attention (because they are generally outside the realm of the agency in question) and, therefore, are the least well-defined (Figure 1). What we have set aside as being too complicated to architect has come back to bite us.

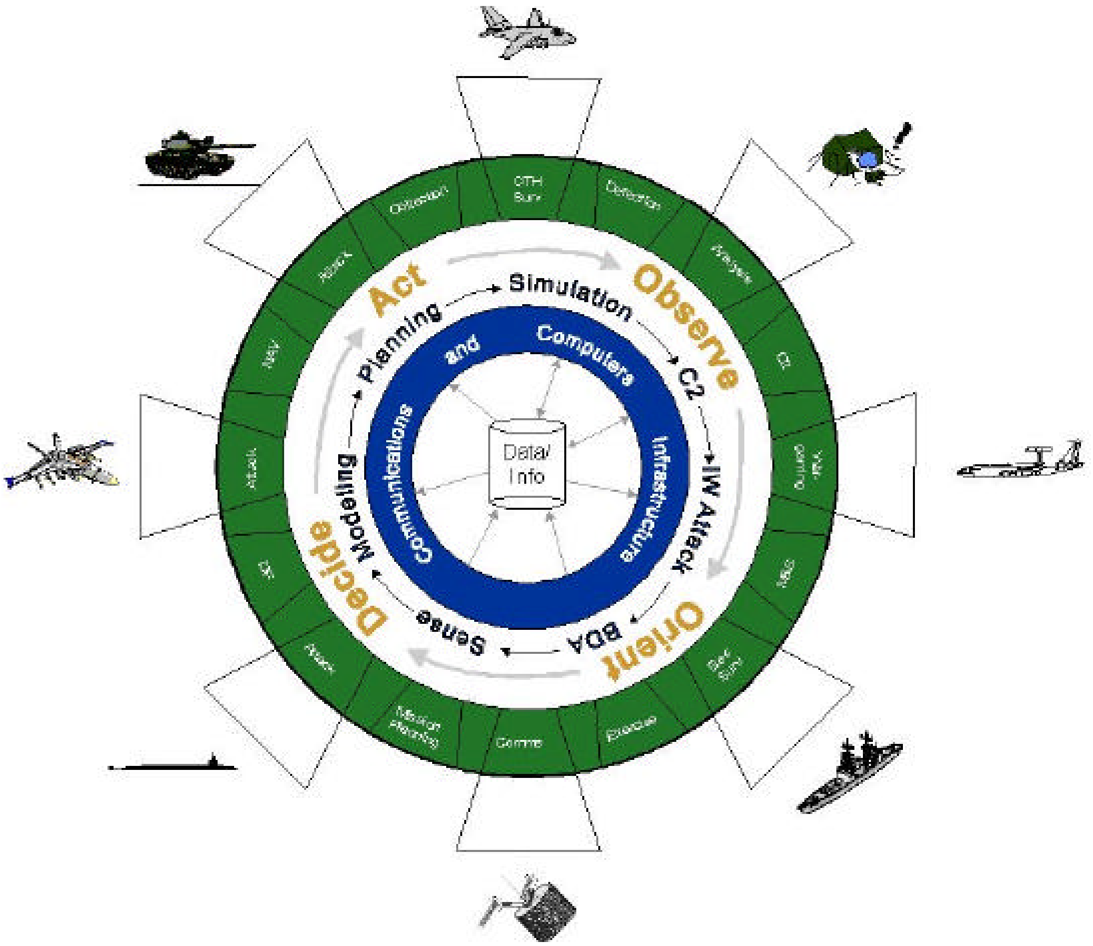


Figure 1. The Interoperability Requirement.

Still, buzz words like “jointness,” “interoperability,” and “integrated” continue to be bandied about every time United States military forces engage in any newsworthy operation. Why? Because in each successive engagement we find another instance in which our fighting men and women have been unable to adequately plan, communicate and/or coordinate multi-service activities. Sometimes the issues are new, such as the inability of the Navy, during Operation Desert Storm, to share mission planning data compiled in an Air Force system called the Contingency Tactical Air Planning System. Often the issues are much longer standing. In all cases, however, some service, agency or organization has and is actively using some system (usually a command and control system) that will not connect to, interface with or in some other fashion interoperate with other participating services, agencies and organizations. The situation has been studied at a variety of levels--from the Office of the Secretary of Defense (OSD) to individual combat units. Why then, in this age of complex, automated information systems, have we failed to achieve total connectivity and interoperability?

So what is the underlying cause of this interoperability issue? Why can't the services design, acquire and implement joint, interoperable systems? There are, no doubt, a plethora of issues; none of which are easily solvable. Many blame the procurement system. Others think that congressional oversight of military procurement is the root of the problem. At least one answer lies in requirements definition, requirements allocation and the procurement cycle itself. The process of defining what is needed, analyzing and applying alternative compromises born of conflicting requirements and budgetary constraints, and planning for a fully interoperable, joint military is very complex, disjointed and is generally not amenable to cooperative development of fully interoperable systems. All of the services and many other government agencies have begun to investigate these issues. The results are generally titled “Master Plans” or “Architectures” although other terms such as “Vision” and “Horizon” have frequently been used.

The authors examined what they believed to be the root cause of this and similar compatibility and commonality issues. The examples given in this presentation are taken from the authors personal experiences working with the architecture definition and development process within the Navy and are, therefore, primarily of Navy origin. Several other studies, however, have been conducted by and/or for numerous other services and agencies. Some of these other studies are referenced where appropriate.

2. Taxonomy

So, what exactly is architecture and what is interoperability?

2.1 *Architecture Defined*

According to Webster's II New Riverside University Dictionary the word “architecture” is defined as "... the art and science of designing and erecting ... a style and method of design and construction ... design or system perceived by humans..." [Webster, 1984]. Similarly, JCS Pub 1-02 defines architecture as: “A framework or structure that portrays relationships among all the elements of the subject force, system, or activity.” [CSC, 1995] There are numerous other definitions as well:

- Architecture: “An organized framework consisting of principles, rules, conventions, and standards that serve to guide development and construction activities such that all components of the intended structure will work together to satisfy the ultimate objective of the structure.” [CIMPIM, 1993]

- Functional Architecture: A description maintained under configuration control of the:

  (a) overall scope and mission of the functional area and its functional activities;

  (b) activity models and data models documenting the current baseline ("as is") and current target ("to be") methods, functional processes, and data structure and rules for each functional activity;

  (c) long-term objectives, performance measures, and performance targets for the functional area and its functional activities; and

  (d) functional management strategy to be followed in defining and implementing standardized and streamlined processes across the Department of Defense. [DoD8020, 1993]

- System Architecture: The structure and relationship among the components of a system. The system architecture may also include the system's interface with its operational environment. [IEEE, 1984]

2.2 *Interoperability Defined*

The ability to generate and move information has increased many thousands of times over the past 30 years. The services have all become much more reliant on information technology. Unfortunately, the current capability to generate information far exceeds our ability to control and use it effectively. To ensure information interoperability, system developers must comply with data and interface standards. Understandable descriptions of databases are the key to data interoperability [ITSG, 1998]. The Information Technology Standards Guidance (ITSG) along with the Technical Architecture for Information Management (TAFIM) and its replacement, the Joint Technical Architecture (JTA), attempt to add structure to the process.

There is a requirement to develop data metrics to assess and support system data interoperability. The C^4ISR Core Architecture Data Model (CADM) provides a foundation for addressing the tactical information architecture [ITSG, 1998].

In a paper presented at the 1997 DoD Database Colloquium, James Mathwich made the case that the seamless flow of information is one of the most ambitious visions of information warfare. “And yet within the Department of Defense, database integration and information interoperability efforts are more often characterized as false-starts rather than successes. … Commercial data warehouse programs, which are highly bounded database integration efforts, are doing no better with no more than a 50 percent success rate. … Managing information in an interoperable community will fail unless it is automated to the greatest degree possible. Automation of information management cannot be done on a community-wide basis unless there exists a community-wide policy with sufficient detail so that it can be predictably executed in an automated tool. Integrated databases bring new information interoperability challenges. The definition and management of the linkage between information and mission has in the past been lacking. Establishing this linkage will provide critical context and metrics for managing database integration and building effective interoperable systems." [Mathwick, 1997].

From a briefing given to the Department of the Navy (DoN) Chief Information Officer (CIO) in February of this year, it is obvious that we are still concerned with interoperability issues. "Data efforts are uncoordinated and there is no process in being to fix the problem. Many C^4I systems are incapable of sharing and exchanging data, an interoperability problem that could result in the possible 'loss of life, equipment or supplies'. To correct the problem requires both an information architecture and a repository of systems' databases." [Michaels, 1999].

The Joint Interoperability Test Command (JITC) performs the joint interoperability test and certification mission as prescribed in CJCSI 6212.01A. [JITC, 1998]. From JITC we have this definition of interoperability:

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

2.3 *Review*

These seem to be relatively straightforward concepts. So we will repeat the questions: Why then is the process of identifying and developing architectures for the DoD so difficult, costly and time consuming? And, why, despite years of research and millions of dollars spent investigating the issues, is DoD still struggling to:

- define what exactly constitutes an architecture,
- identify what types of architectures do and/or should exist,
- categorize architecture concepts, and
- develop a long-range plan for architecture development and maintenance?

Without a consolidated, coordinated, organized plan there is little chance of ever attaining the elusive goal of total interoperability.

3. Migration Strategy

The ultimate goal of any planning process is, of course, to build a knowledge- and experience-base upon which to formulate decisions toward shaping the future design of military forces. This is more than just managing information. Planners must be able to organize and/or re-organize the components of a large, complex system ("Force") so that it functions smoothly as an integrated whole. We must be able to manage, manipulate, and study the effort on a conceptual level so that it can be implemented on the physical level.

In the 1985 to 1987 time frame, the Space and Naval Warfare Systems Command (SPAWAR) in conjunction with the Chief of Naval Operations (CNO) formulated an initiative to perform force warfare assessments under their Warfare Systems Architecture and Engineering (WSA&E) charter. As of June 1988 the Navy had budgeted $91.5 million for the WSA&E process in ever increasing yearly increments from Fiscal Year (FY) 87 through FY 94 [WSA&E, 1988]. The purpose of these assessments, like others conducted by a variety of services and agencies, was to perform top-down analyses of platforms, weapon systems, and support systems in terms of their impact at the force level. The WSA&E process represents one of the Navy's most recent, coordinated efforts to make tradeoffs across warfare mission areas in a structured, analytical way. The process was driven by the belief that the Navy's R&D and acquisition decision process was/is inundated by a proliferation of requirements and procurements that [WSA&E, 1988]:

(1) provide a fragmented approach to Battle Force Command and Control;
(2) indicate a lack of understanding of interoperability issues; and
(3) result in programming actions taken without a full understanding of their impact on other interrelated programs.

The ultimate goal then, is to integrate and coordinate these requirements into a framework where the force is viewed as a single warfighting system.

The Navy’s plan, like many others, was well thought out and structured. Architectures were defined, at least by some, as the long-range goal, a blueprint for what was desired/expected in 10 to 20 years. In the interim, the service expressed its intermediate plans/goals in documents known as Master Plans. Master Plans generally were 5-10 year planning documents. In the near term, of course, we have the well-established Program Objective Memorandum (POM) process, a five-year plan of procurement and budgeting in general (Figure 2).

Unfortunately, the funding for architecture development in the Navy dwindled to the point of virtual non-existence long before the process was complete. There are, no doubt many reasons for this demise but one of the most prominent was the fact that architectures take a good deal of time to develop and they do not provide many answers until they are very nearly finished. In fact, some would argue that architectures are never finished because they require continual update and enhancement to account for technological advances, program adjustments, congressional actions, and a host of other variables. Architectures were originally developed, at least within the Navy, to help program sponsors make informed, timely, accurate decisions in the seemingly never ending battle of the budget. Although this effort did provide valuable insight into the procurement process and the technological issues in many warfare mission areas, the process was never completed to the point where a true migration path could be identified and pursued.

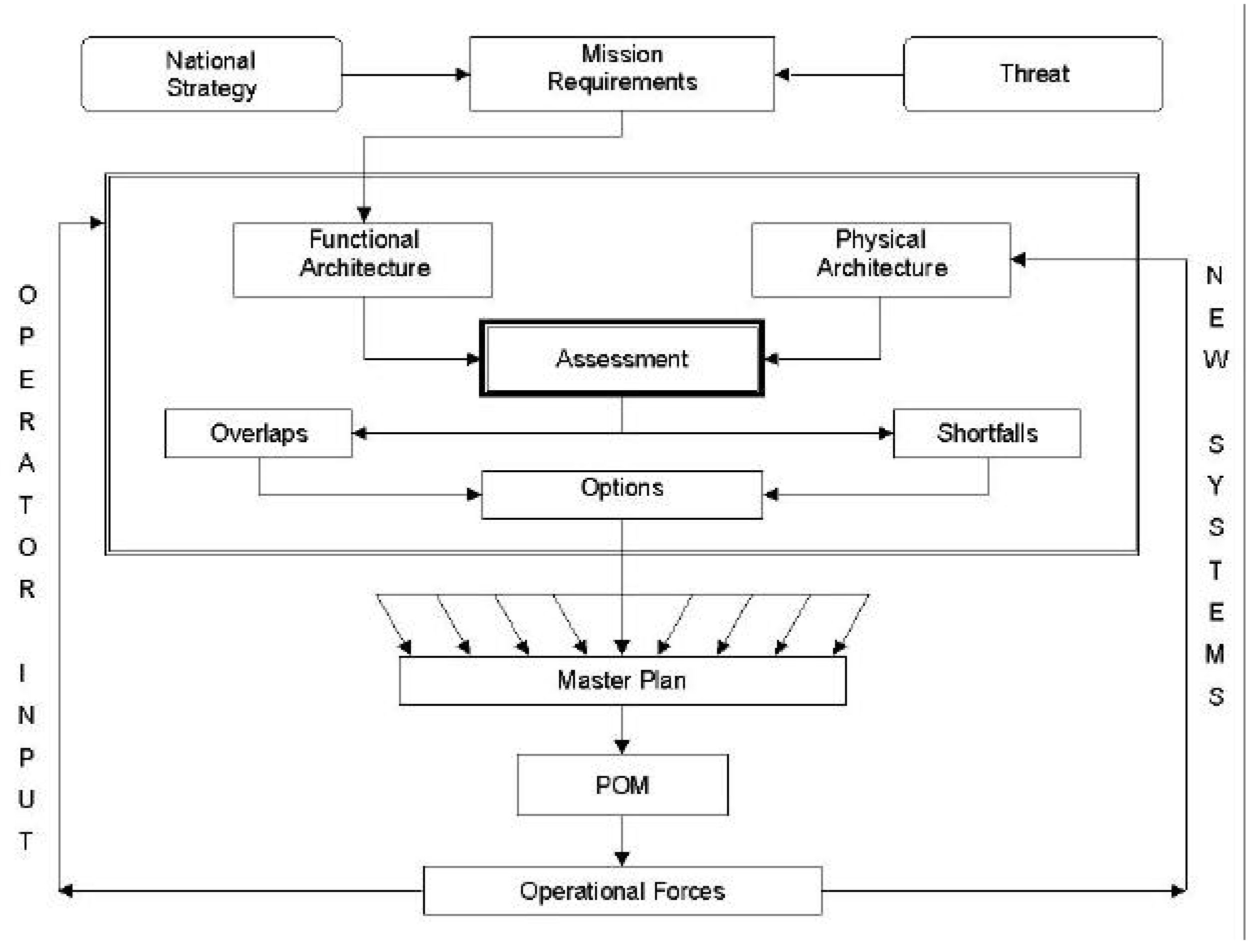


Figure 2. The Program Objective Memorandum (POM) Process.

4. Timeline of Recent Events

In December 1993 a Defense Science Board (DSB) Task Force on Global Surveillance concluded:

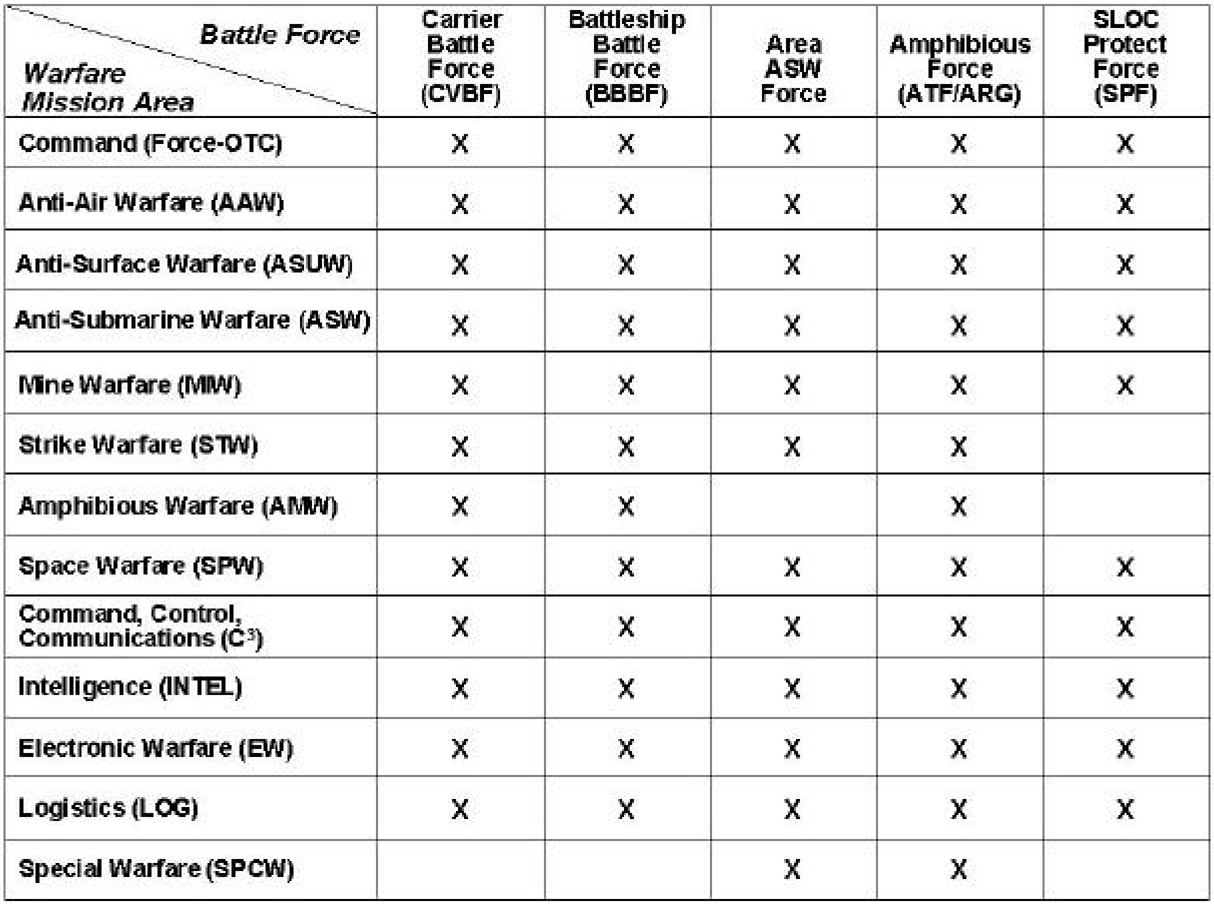
> "The Task Force believes that DoD needs an overarching 'architect' for military information systems who can work across all Department and component boundaries and reach down to the operating forces (to the combat level) to identify what is needed to better integrate military information systems into combat operations." [DSBGS, 1993]

Again in June of 1994 a DSB Task Force on Readiness reiterated the need for a long range planning process in general and an OSD "C^4I Architecture" in particular.

> "There is a need for rapid development and implementation of a joint C^4I architecture and doctrine." [DSBR, 1994]

In the summer and fall of 1994, the OASD(C^3I) commissioned studies to conduct a review of the status of architectures within the DoD and report the findings to the OASD (C^3I) Intelligence Program Support Group (IPSG). The IPSG was designated to support the development of architectures for DoD as recommended in the Defense Science Board's Global Surveillance Study.

One author of this paper, Dr. Curts, participated in a study that concluded that there are a plethora of good, useful C^3I master plans, architectures and similar documents within DoD. [CSC, 1995] All recognize the need for jointness and interoperability and contain the necessary "hooks" for such connectivity. All were researched and published by different organizations, in varying levels of detail, with several formats and for different purposes. All are useful to their developers but few, if any, can be directly combined, linked or compared to any other. Most are used for the purpose of describing existing systems (commonly referred to as "as is" architectures) rather than a rigorous analysis of requirements, capabilities, budgetary constraints and interoperability issues. (Figure 3).



Battle Force Warfare Mission Area	Carrier Battle Force (CVBF)	Battleship Battle Force (BBBF)	Area ASW Force	Amphibious Force (ATF/ARG)	SLOC Protect Force (SPF)
Command (Force-OTC)	X	X	X	X	X
Anti-Air Warfare (AAW)	X	X	X	X	X
Anti-Surface Warfare (ASUW)	X	X	X	X	X
Anti-Submarine Warfare (ASW)	X	X	X	X	X
Mine Warfare (MIW)	X	X	X	X	X
Strike Warfare (STW)	X	X	X	X	
Amphibious Warfare (AMW)	X	X		X	
Space Warfare (SPW)	X	X	X	X	X
Command, Control, Communications (C^3)	X	X	X	X	X
Intelligence (INTEL)	X	X	X	X	X
Electronic Warfare (EW)	X	X	X	X	X
Logistics (LOG)	X	X	X	X	X
Special Warfare (SPCW)			X	X	

Figure 3. Fifty-nine Architectures.

In response to these studies, ASD(C^3I) took steps to "... institutionalize the C^4I integration process through reorganization and re-tasking of the IPSG into the C^4I Integration Support Activity (CISA), all of which included the designation of an Architectures Directorate to formalize and integrate architectures initiatives." [Endicott, 95] If permitted to complete their assigned tasking with the full support and backing of ASD(C^3I), these initiatives would have made a significant, positive change in the evolution of C^4I concepts, architectures and systems.

To improve and facilitate the ability of DoD systems to support joint and combined operations, the Under Secretary of Defense for Acquisition and Technology (USD[A&T]) and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C^3I]) mandated the Joint Technical Architecture (JTA) in August 1996, specifying a minimum set of standards and guidelines for the acquisition of DoD C^4I systems and their interfaces [USD(A&T), 1996]. The JTA is mandated for all services and DoD agencies and contains performance-based standards in an attempt to apply sound technical and business practices. Supplements address technical architecture exceptions. "However, almost two years after the initial USD(A&T) memo, Navy Program Managers, who shoulder the ultimate responsibility to make it happen, still seem to have limited knowledge about the JTA." [Erickson, 1998]. At about the same time that CDR Erickson's article appeared in PM, the Commander in Chief, US Pacific Fleet, Admiral Archie Clemins asked, "Who is it that decides the technical architecture that you're going to use?" [Clemins, 1998].

Superior information has long been recognized as a force multiplier [Bjorklund, 1995]. In a more recent article, Admiral Cebrowski stated, "Value is derived from the quality and timeliness of information that moves between nodes on the net. … This value increases as information moves toward 100% relevancy, 100% accuracy and zero time delay." [Cebrowski, 1998]. The future as embodied in Network-Centric Warfare demands systems integrated at the platform level. These disciplines must be tightly and seamlessly integrated to facilitate Input/Output (IO) functions from a single integrated workstation. We can no longer afford to develop systems, tools and architectures along service specific lines. The IO systems of the future must be fully integrated. Any solution developed must be joint and interoperable. "The answer is obvious – joint architecture standards and adherence to open architectures to enhance interoperability. … This is not simply the migration of stovepipe systems, but the integration of capabilities that cross traditional functional boundaries. … System development must be accomplished in a way that results in a truly joint capability …." [GRCI, 1998].

Early in 1998 DoD drafted a revision to DoD Directive 4630.5 which requires interoperability between C^3I and interfacing systems [DoD4630, 1998].

"JCS defines interoperability as the condition achieved between systems when information or services are exchanged directly and satisfactorily between the systems and/or their users." [ITSG, 1998]

Joint Staff officials believe that, although the certification requirement is outlined in several DoD and Joint Staff guidance documents, some system managers are unaware of it [DoDD 1992], [DoDI 1992] and [CJCSI, 1995]. In a study chartered by J-6 and completed in January 1996, only 12 of 424 (less than 3 percent) surveyed acquisition managers and Defense System Management College students knew about the DoD and Joint Staff interoperability requirements. The study team found that this lack of knowledge prevented users from placing interoperability in the initial requirements documents and acquisition managers from building interoperability into approved programs. As a result, the Joint Staff began an effort in 1996 to better educate system managers about the requirement. However, the study points out that education is not a panacea for all interoperability problems.

By 1998, however, it appeared that all work toward architecture interoperability had ground to a halt. Pursuant to a congressional request on that subject matter, GAO reviewed whether DOD organizations were complying with interoperability testing and certification requirements for command, control, communications, computers, and intelligence (C^4I) systems; and what actions, if any, were needed to improve the current certification process. The GAO review was not promising.

GAO noted 15 fundamental weaknesses in the current certification process that can be summarized in six primary areas as follows [GAO, 1998]:

(1) COMMAND & CONTROL: DoD does not have an effective process for certifying existing, newly developed, and modified C^4I systems for interoperability; many C^4I systems have not been certified for interoperability and, in fact, DoD does not know how many require certification; and improvements to the certification process are needed to provide DoD better assurance that C^4I systems critical to effective joint operations are tested and certified for interoperability.

(2) COMPLIANCE: DoD organizations are not complying with the current interoperability testing and certification process for existing, newly developed, and modified C^4I systems; many C^4I systems that require interoperability testing have not been certified or have not received a waiver from the requirement; the extent of this noncompliance could have far-reaching effects on the use of such systems in joint operations; noncompliance with interoperability testing and certification stems from weaknesses in the certification process itself;

(3) GUIDANCE: While DoD guidance requires that all new systems be certified or obtain a waiver from certification testing before they enter production and fielding, systems proceed to these latter acquisition stages without being certified.

(4) RESPONSIBILITY AND AUTHORITY: The Defense Information Systems Agency (DISA) Joint Interoperability Test Command officials lack the authority to compel DoD organizations to submit their C^4I systems for testing. Although DoD guidance spells out a specific interoperability certification requirement, many DoD organizations are unaware of it; others simply ignore the requirement because it is not strictly enforced or because they do not adequately budget for such testing.

(5) PRIORITIZATION: A lack of a complete and accurate listing of C^4I systems requiring certification and a plan to prioritize systems for testing. Limited resources are not focused on certifying the most critical systems first. Prioritization is important since reviews, certifications and recertification of modified systems continually add to the number of systems requiring certification.

(6) COMMUNICATION: The process does not include notifying the services about interoperability problems, and the Test Command has only recently begun to contact the services regarding the noted problems.

5. Where Do We Go From Here?

Several good architectural and interoperability efforts exist and are producing products that are useful to the agencies that conceived them. Here's a few:

- JINTACCS (MTFs/LINKs) – message standards. They need harmonization with themselves and with C^4I databases.
- DDDS – DISA metadata repository. Not widely used by software developers.
- DII COE – Primarily hardware and software standards. SHADE is a data component, building database segments. Emphasis is on runtime avoidance.
- C^4ISR Architecture Framework – Frameworks for joint Operations, Systems and Technical standards.
- JTA – Joint Warfighter Architecture. Provides building codes. Does not provide means to define, test and configuration manage data.
- Copernicus – Naval Warfighter Architecture. Recognizes need for data interoperability.
- NWTDB – N6 management initiative/engineering methodology to implement DoD Data Interoperability Policies.
- DoN ITI and ITSG – provides DoN IT Architecture/Standards Guidance.
- INCA – Intelligence Community Architecture
- Horizon – Army Warfighter Architecture.

Do you see a pattern evolving here? You can see that there are many new initiatives underway. But so far, the authors, the General Accounting Office and others, in research independent from each other, are finding that no single product (nor consolidated set of interconnected products) has been produced which is useful from the Navy or from the DoD "Big Picture" perspective of a totally integrated, interoperable force.

Existing directives, and there are many, are very broad, general and uncoordinated within DoD, let alone between and amongst the services and agencies that make up DoD. Ongoing efforts to consolidate and simplify these controlling documents may soon remedy the situation. Still, while there is a great deal of support for interoperability concepts and much cooperation amongst agencies, there is currently little or no coordination in the detailed development of architectures.

Each agency develops architectures for their own purposes, at varying levels of detail, in their own formats, using the tools that happen to be available to them; few of which are interoperable. In general, the architectures developed by one agency are not readily comparable to those of another service or agency. Without the expenditure of a good deal of man-hours pouring through a large quantity of diagrams, tables and textual information, there is no good method of ensuring interoperability. There are few, if any, common terms of reference. Even the terms "master plan" and “architecture” are used differently amongst agencies. Terms, concepts and processes are not well defined, causing a great deal of miscommunication between agencies.

The missing ingredient seems to be a single unifying construct to lay the foundation for architectures and tie them together. Probably the most glaring deficiency lies in exactly the location that is causing the most dialogue and the need for architectures to begin with ... the interface points. Almost all architectures designate some peripheral node as the "connection to" the systems, structures, architectures of other agencies. As one might expect, these are the nodes that are given the least attention (because they are generally outside the realm of the agency in question) and, therefore, are the least well defined. These should be some of the first issues addressed by anyone contemplating a global architecture structure.

For some time now, DoD has allowed massively parallel efforts to continue, presumably in hopes that one would produce the perfect architectural construct. DoD has not yet been successful. Perhaps it is time to settle for a less perfect solution. General George Patton is said to have made the statement, "A good plan executed violently today is better than a perfect plan executed tomorrow." Similarly, Voltaire once wrote, "Best is the enemy of good."

6. Recommendations

If true jointness and interoperability are ever to be achieved, the concept of a single unifying construct, however imperfect, or incomplete must receive support at the highest levels of DoD. Although the following plan is, no doubt, imperfect, it is, at least, a start and is offered as a first step toward a DoD-wide interoperable C^4I architecture.

First, as twice reiterated by the DSB, a DoD architect must be assigned at the very highest levels of the department and embodied with the responsibility and authority to enforce compliance with DoD architectural concepts. Although the authors have not seen a charter for the newly designated CISA, presumably this agency will provide the required direction.

Next, we must compile and use a common lexicon. If architectures are ever to be interoperable, the developers of those documents must be able to communicate efficiently and effectively. Terms such as architecture, master plan, functional requirement, etc. must be defined and used consistently by all players.

Third, a standardized, a well-defined architectural process would significantly simplify the evolution of architectures while adding a certain amount of rigor, reproducibility, and confidence to the procedure. Earlier works, [Curts, 1989a], [Curts, 1989b], [Curts, 1990] and [Curts, 1995] have discussed these concepts in greater detail. The process must, as a minimum, contain well defined: authority, designated cognizant activities, processes, milestones, architectural outlines and formats, deliverables, documentation, and maintenance/update schedules.

Finally, we must define architecture development, definition, maintenance and interface standards as necessary (Figure 4):

- to ensure: interoperability and connectivity of architectures, consistency, compliance with applicable directives, and architectural information dissemination;

- to facilitate: implementation of policies and procedures, acquisition strategies, systems engineering, configuration management, and technical standards; and

- to standardize: terms of reference, modeling tools, architecture data elements, architecture data structures, hardware and software interfaces, architectural representations and architectural scope, and level of detail/abstraction.

The goal should not be forced procurement of a single, standard system that performs some specific set of functions. The real issue, at least in the near term, is not “Who is using what system?”, but rather “Are these various systems compatible/interoperable?” In other words, all that we really need, at least to start, are interface/interoperability STANDARDS. It is time to stop investigating architectural concepts and start defining/building joint, interoperable, standardized architectures.

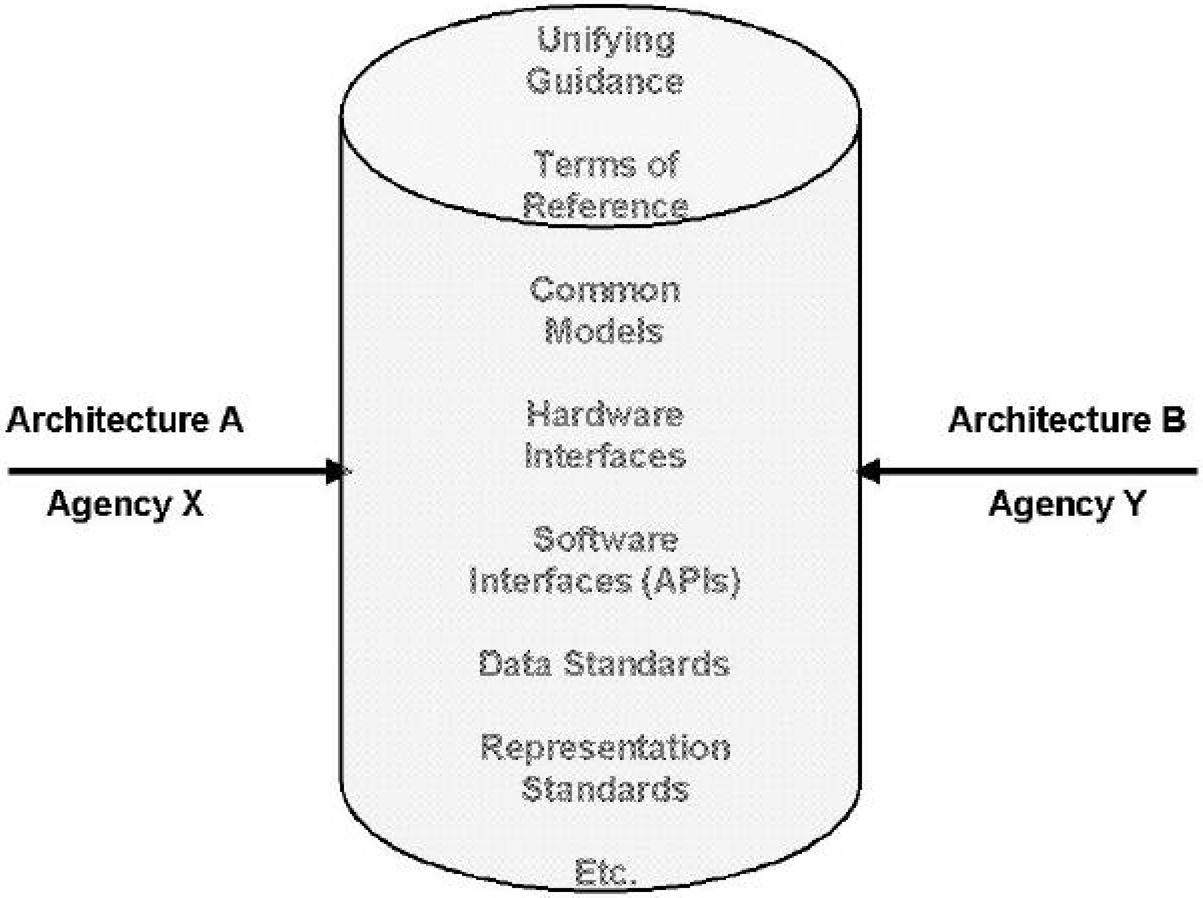


Figure 4. Interface Standards.

7. The Final Word: The Next Major Hurdle

A major technical goal of the next ten years will be the utilization of an architecture that allows interoperability between C^4I systems and Modeling & Simulation (M&S). Current technologies do not support such interoperability, without unique hardware (human-in-the-loop in many cases) and software. The goal within the next decade should be to allow the majority of military C^4I systems to "plug-and-play" to the majority of military M&S applications and exchange information without having to build unique interfaces. In other words, to give end-users the needed interoperability and reusability of M&S programs running in a common browser. This will provide an increased ease-of-use for the warfighter community. And this will promote the ability to train warfighters on the same C^4I systems that they will use in the field, at reduced training and development costs for specialized interfaces to models. Again, the Defense Science Board Task Force on Readiness:

> "Modeling and simulation technology should be exploited to enhance joint and combined training and doctrine. It offers a tremendous opportunity to leverage our existing training at all levels through enhancement or even replacement where appropriate after thorough review."

8. References

[Bjorklund, 1995] Bjorklund Raymond C. The Dollars and Sense of Command and Control. Washington, DC: National Defense University Press, 1995, pp. 73-75.

[CADM, 1997] C^4ISR Core Architecture Data Model, Version 1.0, 15 September 1997.

[CAF, 1997] C^4ISR Architecture Framework, Version 2, 18 December 1997.

[Cebrowski, 1998] Cebrowski, USN, Vadm Arthur K. "Network-Centric Warfare – Its Origin and Future." U.S. Naval Institute Proceedings, p. 31, January, 1998.

[CIMPIM, 1993] Corporate Information Management Process Improvement Methodology for DOD Functional Managers, Second Edition. Arlington, VA: D. Appleton Company, 1993.

[CJCS6212, 1995] CJCS Instruction 6212.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems. Washington, DC: Joint Chiefs, 30 June 1995.

[Clemins, 1998] Clemins USN, ADM Archie. "Remarks to AFCEA Asia Pacific TECHNET '98." Asia Pacific TECHNET Conference, Honolulu, HI, 5 Nov 1998.

[CSC, 1995] DoD Architecture Review, 2 Volumes. Falls Church, VA: Computer Sciences Corporation, 1995.

[Curts, 1989a] Curts, Raymond J. "A Systems Engineering Approach to Battle Force Architecture." Unpublished research. Fairfax, VA: 1989.

[Curts, 1989b] Curts, Raymond J. "An Expert System for the Assessment of Naval Force Architecture." Unpublished research. Fairfax, VA: 1989.

[Curts, 1990] Curts, Raymond J. "Automating the Architecture Process." Briefing/Lecture. Washington, DC: Space and Naval Warfare Systems Command, 1990.

[Curts, 1995] Curts, Raymond J. “Inference Methodologies in Decision Support Systems: A Case Study.” To be published in Information and Systems Engineering. Amsterdam, The Netherlands: IOS Press, 1995.

[DoD4630, 1998] DoD Directive 4630.5, “Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C^3I) Systems.” Washington, DC: Department of Defense, 1998.

[DoDD4630.5, 1992] DoD Directive 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C^3I) Systems. Washington, DC: Department of Defense, 12 November 1992.

[DoDD4630.8, 1992] DoD Directive 4630.8, Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C^3I) Systems. Washington, DC: Department of Defense, 18 November 1992.

[DoD8020, 1993] DoD 8020.1-M, Functional Process Improvement (Draft). Washington, DC: Department of Defense, 1993.

[DoD8320, 1994] DoD 8320.1-M, DoD Data Administration Procedures, March, 1994.

[DoD8320, 1998] DoD 8320.1-M-1, Draft DoD Data Element Standardization Procedures, February, 1998.

[DSBGS, 1993] Report of the Defense Science Board Task Force on Global Surveillance. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, 1993.

[DSBR, 1994] Report of the Defense Science Board Task Force on Readiness. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, June 1994.

[Endicott, 1995] Endicott, George. Official Electronic Mail Communication to Dr. Curts. Arlington, VA: Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C^3I)), 11 April 1995.

[Erickson, 1998] Erickson, CDR James, et al. “Impact of Joint Technical Architecture on Navy Acquisition.” Program Manager (PM), 34-38, Nov-Dec, 1998.

[GAO, 1998] Joint Military Operations: Weaknesses in DOD's Process for Certifying C^4I Systems' Interoperability (Letter Report, 03/13/98, GAO/NSIAD-98-73)

[GRCI, 1998] Information Warfare White Paper for Space and Naval Warfare Systems Command (SPAWAR), Information Warfare Program Directorate (PD-16), March, 1998.

[IEEE, 1984] Jay, Frank, ed. IEEE Standard Dictionary of Electrical and Electronics Terms. New York, NY: IEEE, 1984.

[ITSG, 1998] Information Technology Standards Guidance – Information Management. Final Draft Version 1.0. Washington, DC: Department of the Navy, 1998.

[JITC, 1998] C^4I Interoperability–JITC Certification Process. JITC Home Page, 21 Oct 1998.

[JTA, 1996] Department of Defense Joint Technical Architecture, Version 1.0, 22 August 1996.

[JTA, 1997] Department of Defense Joint Technical Architecture, Draft Version 2.0, 18 July 1997.

[Mathwick, 1997] Mathwick, James E. “Database Integration, Practical Lessons-Learned.” San Diego, CA: DoD Database Colloquium, 1997.

[Michaels, 1999] “DoN Data Interoperability.” Briefing to Mr. Dan Porter, DoN CIO. Arlington, VA: GRC International, 18 February 1999.

[USD(A&T), 1996] “Implementation of the DoD Joint Technical Architecture.” USD(A&T) and ASD(C^3I) Joint Memorandum. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 1996.

[Webster, 1984] Webster's II: New Riverside University Dictionary. Boston, MA: The Riverside Publishing Company, 1984.

[WSA&E, 1988] “Warfare Systems Architecture & Engineering.” Briefing to ADM Chang. Washington, DC: Space and Naval Warfare Systems Command, 1988.

9. Vita

CDR Raymond J. Curts, Ph.D., (USN, Ret.) was born December 2, 1946 in Philadelphia, Pennsylvania and is an American citizen. He graduated from Vandalia Community High School, Vandalia, Illinois in 1965. He received his Bachelor of Science in Aeronautical and Astronautical Engineering from the University of Illinois in 1970 and was commissioned as an Ensign in the

United States Navy. In December 1972 he earned his wings as a Naval Aviator and was assigned to the U.S. Naval Base at Guantanamo Bay, Cuba. Returning to the continental United States in 1976, he became an instructor pilot in the Navy's Advanced Jet Training Command in Beeville, Texas where he earned a Master of Arts degree in Management and Business Administration from Webster College of St. Louis, Missouri. After tours of duty in Norfolk, Virginia; Rota, Spain; and Key West, Florida, he was stationed at the Space and Naval Warfare Systems Command (SPAWAR) in Washington, DC where he spent five years as the Navy's Electronic Warfare Architect. During this time he earned a Ph.D. in Information Technology from George Mason University.

LCDR Douglas E. Campbell, Ph.D., (USNR-R, Ret.) was born on May 9, 1954 in Portsmouth, Virginia, and is an American citizen. He graduated from Kenitra American High School, Kenitra, Morocco, in 1972. He received his Bachelor of Science degree in Journalism from the University of Kansas in 1976 and was immediately commissioned as an Ensign in the United States Navy. He joined the U.S. Naval Reserve Program as an Intelligence Officer in 1980 and was transferred to the Retired Reserves as a Lieutenant Commander on 1 June 1999. Dr. Campbell received his Master of Science degree from the University of Southern California in Computer Systems Management in 1986 and his Doctor of Philosophy degree in Computer Security from Southwest University in New Orleans, Louisiana, in 1990. Dr. Campbell is president and CEO of Syneca Research Group, Inc., a certified 8(a) and a certified Small & Disadvantaged Business entity under the U.S. Small Business Administration’s program.