

Open Architecture, The Critical Network Centric Warfare Enabler

**First Edition
March 18, 2004**

Captain Richard T. Rushton, USN
Chief, Network Systems and Integration Branch
Surface Warfare Directorate (N76)
Chief of Naval Operations Staff (OPNAV)

Mr. Michael McCrave
Senior Systems Engineer
ANTEON International Corp

Mark N. Klett
President & CEO
Klett Consulting Group, INC

Timothy J. Sorber
Senior Systems Engineer
Klett Consulting Group, INC

Acknowledgements

The authors wish to acknowledge the efforts of the following individuals for their valuable contributions to this project.

- Bridget M. Rushton – Communications Specialist for NAVSEA-62 (DTI Associates, Inc.) - Grammatical and content editing
- Joseph M. Veneziano – Senior Systems Analyst (Klett Consulting Group, INC) – Technical research and content editing
- Kari S. Lindell – Corporate Administrator (Klett Consulting Group, INC) – Administrative support, content and grammatical editing

Preface

A tremendous amount of ink has been expended over the past several years, describing Information Technology (IT) based warfare concepts. Predominately, the debate has been aimed at the technology or business drivers that reflect the enhancements that IT technology offers. When the argument does wander into the lexicon of warfare, it is mostly in the context of top level notions of the Global Information Grid (GIG) and FORCENet. Most military leaders in general, and naval warriors particularly, exhibit little patience grappling with the acronym laden, technical jargon used in IT. This paper describes the imperatives of the modern battlefield that demand Network Centric Warfare (NCW) and why Open Architecture (OA) is the most critical enabler. It attempts to place the architectural constructs of GIG and FORCENet into warrior context and terms that relate. Finally, a significant effort is made to describe how the current family of integrated combat systems the U.S. Navy is being transformed so they can be maintained and improved with the flexibility required in an uncertain world. Enjoy.

CAPT R.T. Rushton, USN
Chief, Network Systems and Integration Branch (N766)
Surface Warfare Directorate (N76)
Chief of Naval Operations Staff (OPNAV)



"The truly transformational things, conceivably, might be in information technology and information operations and networking and connecting things in ways that they function totally differently than they had previously...Possibly the single most transforming thing in our force will not be a weapon system, but a set of interconnections and substantially enhanced capability because of the awareness it provides."

Secretary of Defense Donald H. Rumsfeld, Town Hall Meeting, Washington DC, August 9, 2001

Executive Summary

Information technology (IT) based warfare capabilities have been vigorously written about and debated during the past several years. The discussion on this subject typically focuses on the technology offered to today's maritime forces, or the business based opportunities modern computing technologies provide. These topics are not the crucial ones to examine. The true imperative for embracing modern open systems architectures is driven by the technical conditions required to support full enablement of network centric warfighting capabilities (NCW). Open Architecture (OA), allows maritime tactical integrated combat systems (ICS) to establish the conditions required to net sensors, achieve full joint interoperability, and provide seamless information relationships to the Global Information Grid (GIG).

The requirement for NCW is driven by the complexities of the joint-coalition battlespace in which maritime forces must operate. The physics of the environment, urban setting, severe terrain and extended inland operations all contribute to this issue. Moreover, these battlespace challenges are complicated by traditional, non-traditional and asymmetric threats. Maritime forces increasingly perform operations in the littoral environment.

Unfortunately, current tactical ICS capabilities fail to meet the threats of these agile opponents. Present integrated weapon systems (IWS) were initially developed with "platform-centric" capabilities to regain the battlespace time constraints of the Cold War threat. As a result, they were optimized for tight platform collocated sensor to weapons pairing, encased in the main-framed computing technology of the times. Since then, the rapid technology explosion of the 1990's moved the commercial IT sector far ahead of these DoD unique computing systems supporting weapons employment. This gap widens at an increasing pace every year. Fortunately, maritime and joint capabilities at the operational and strategic levels were developed in the modern Internet Protocol (IP) based technologies. These capabilities constitute a significant segment of the presently fielded operational planning and mission execution IT, and include the lion's share of the force's computing requirements.

The Department of Defense (DoD) recognizes the power of the IP based information environment, and is defining both the capstone warfare requirements and concepts needed to exploit the Global Information Grid (GIG). The U.S. Navy has expanded upon these requirements and concepts to develop the maritime information environment called FORCEnet. Embracing the concepts of these information environments unlocks the underpinnings of joint interoperability and with it NCW. Auspiciously, the key to this unlocking is Open Architecture (OA). It provides the framework that can adapt and exploit open system design principles, standards, and architecture. It facilitates a new approach in acquiring and managing reusable software components, while taking maximum advantage of the commercial off-the-shelf (COTS) market place.

The Global Information Grid (GIG) provides the enabling foundation for NCW: information superiority, decision superiority and, ultimately, full spectrum dominance. The information gained through the use of NCW allows a warfighting force to achieve dramatically improved information positions, in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and resulting in combat power. For naval forces, the success of exploiting the GIG in NCW depends in large part on how well it achieves interoperability and force-wide information sharing through the implementation of FORCEnet.

Meeting the Sea Power 21 challenges to seamlessly connect Sea Strike, Sea Shield, and Sea Basing with the enabling pillars of Sea Trial, Sea Warrior, and Sea Enterprise, FORCENet must support relationships between three dimensions of the information space:

- *Data Domain* - facilitates warriors' focus on decision making and planning
- *Time Domain* - allows warriors to reach out to data from a grid of netted sensors and fuse it with federated information coming from non-real time reach back support capability
- *Operational Level of Command* - provides widespread situational awareness so that commanders are able to more effectively execute command and control over their assigned forces

To enable NCW, FORCENet will operate efficiently throughout this multi-dimensional information space.

The first step moving toward an OA environment is base-lining current systems. A thorough understanding of what degree fielded software based ICS and associated C2 capabilities comply with the engineering standards and functional allocations of OA is essential. A top-level review establishes that none of the Navy's in-service ICS backbones are currently compliant with OA. However, a more detailed assessment reveals several that are technically positioned to support the infusion of OA conditions, so a detailed migration plan can be formulated and investment resources allocated to achieve migration. They are:

- AEGIS Baseline Seven for CG/DDG
- Ship Self Defense System Mark Two for CVN/LPD/LHD

The Navy faces a daunting task in transforming its high fidelity sensor, command and decision, and weapon fire control software based capabilities into Open Architecture, and once there, incorporating the new capabilities demanded by "Sea Power 21." It requires two distinctive processes:

- The "Open Architecture Transformation Roadmap" is a temporary, specifically focused process that takes the Navy to an initial OA condition by 2008
- The "Rapid Capability Insertion Process/Advanced Processor Build (RCIP/APB)" will complete the transformation and provide the agile modernization structure to allow for new capability insertion for the foreseeable future.

These two processes will be sequential, but overlapping, and are the essential muscle movers to achieve and maintain network-centricity.

Fundamentally, the Defense Department has no choice in moving its archaic, monolithic, main-framed, integrated combat systems into OA. The commercial market place made the decision for the department over a decade ago. The DoD embraced the decision when it shifted much of its capabilities out of military standard computing environments and into COTS hardware. Unfortunately, it didn't move to embrace the modern software structures, companion to COTS, and, as such, retains much of its capabilities in archaic conditions. The only decision for the DoD remaining is, when it will make the remaining shift to OA software designs.

The world has entered an era of rapid, technological globalization, marked with the new threat of asymmetrical warfare. It is necessary to seize and utilize the available tools provided by NCW to achieve joint interoperability of military forces on a global scale

in order to successfully combat future asymmetric terrors. Now is the time to embrace the power of OA and move aggressively to align Navy and DoD investment, acquisition policy, and budget execution to support it.

"A key element of our military technological superiority is our capability to command the high ground of space for early warning, intelligence, weather, surveillance, navigation, and command, control and communications."

General Colin L. Powell, U.S. Army
Chairman, Joint Chiefs of Staff, 1991



Table of Contents

Acknowledgements.....	ii
Preface	iii
Executive Summary.....	iv
Introduction	1
Two Revolutions in Warfare since World War II.....	1
The First Revolution – Platform Sensor to Weapon Integration.....	2
The Second Revolution – Multi-Platform Network Centric Integration.....	3
Adversarial Exploitation of Modern Technology	4
Defense Department loss of Computing Technology Leadership.....	4
Open Architecture in a Warrior’s Terms	7
Categorizing Compliance with Open Architecture	7
Open Architecture Computing Environment (OACE).....	8
Functional Capabilities Architecture	10
OACE/OAFA Relationship	12
Today’s Software Based Integrated Combat Systems Challenges.....	13
Base-lining Current Capability	13
AEGIS Integrated Weapon System v. modern technology and network centric warfighting imperatives.	14
Tactical and Operational Commander’s Operational Needs v. Weapon System.	15
Identifying Open Architecture Migration Options.....	16
Integration of Weapon Systems Functions into the FORCENet Environment	18
FORCENet as an integrated part of the Global information Grid	22
FORCENet’s seamless information to knowledge building imperatives depends on Open Architecture.	23
Web Based Command and Control.....	24
Bandwidth.....	25
Detect, Control, and Engage in a Web Based C2 Environment.....	25
Human Systems Integration Challenges	26
Challenges of Moore’s Law.....	27
Equipping the Warrior vs. Manning the Equipment	28
How Do We Get There?	29
The Open Architecture Roadmap	29
Element 1: Harnessing Future Platform Development	30
Element 2: Joint Track Management – Key to Interoperability.....	31
Element 3: Establishing OA Functional Architecture Migration.....	31
Element 4: Transformation Risk Mitigation	31
Element 5: Establishing the Conditions for Future Capabilities	32
Rapid Capability Insertion Process/Advanced Processor Build	34
SSDS MK2 for CVN/LHD/LSD	36
AEGIS Baseline 7 OA for CG/DDG	37
CNI Enabled ACDS for LHA/LHD.....	38
Conclusion.....	39
Glossary	40
Glossary	41
Abbreviations and Acronyms	41
Definition of Terms	44

Table of Illustrations

Tables

Table 1 OA Compliance Categories	7
Table 2 BMC2 Trackers & Displays	11

Figures

Figure 1 Why Open Architecture?	5
Figure 2 OA Computing Environment	9
Figure 3 OA Functional Architecture	10
Figure 4 OACE/OAFA Relationship	12
Figure 5 AEGIS Baseline	14
Figure 6 Multiple Track Displays	15
Figure 7 Evolution of OAFA Combat Systems	16
Figure 8 Information Dissemination Management (IDM)	20
Figure 9 Joint Command and Control Operational Vision	25
Figure 10 Open Architecture Transformation Roadmap	29
Figure 11 AEGIS Spiral Developments	33
Figure 12 Technology Lifecycles	34
Figure 13 OA RCIP/APB Surface Transformations	36

Introduction

The requirement for Network Centric Warfare (NCW) is driven by the complex joint and coalition battlespace in which maritime forces must operate for the foreseeable future. It is characterized by the objectives of modern combat operations, the physics of the environment, urban setting, severe terrain, and extended inland operations. These battlespace challenges are further complicated by traditional, non-traditional and asymmetric threats. Balancing these threats against the innovation of new tactics and procedures, enabled by available technology, is the revolutionary driver for NCW. The warfare case for this revolution is made by a brief trip into the history of naval warfare, from a computing technology perspective, by examining two of the most challenging battlespace defining developments that occurred from World War II to the present. They are:

- The introduction of the low altitude anti-ship cruise missile that effectively reduced reactive battlespace to the horizon.
- The collapse of the Soviet Union and shift of the maritime battlespace into littoral and inland operations.

Once NCW is justified as the key to establishing and maintaining effective battlespace today, understanding the importance of its foundational concept of Open Architecture (OA) is essential in working to shape maritime forces capable of operating in its environs. Much has been written in the recent past about OA as a business imperative, this paper is specifically challenged to make the case for OA in the context of maritime warfare NCW contributions. In the process of doing so, effort is made to place OA in relation with significant information technology architectures of the Global Information Grid (GIG) and FORCEnet, as well as relating it to some of the common technical standards descriptions like Network Centric Enterprise Services (NCES). Once these relationships are defined, an evaluation of today's "in service" capabilities is undertaken and placed in context of development synergies with the Navy's future capabilities. This assessment results in the establishment of two significant processes that together create a path to the future. They are:

- The establishment of an "OA Transformation Roadmap" that defines some specific objectives essential to executing the migration of the U.S. Navy's high end integrated weapon systems into an open systems environment.
- Transitioning the initial transformational effort into a flexible, sustainable, and continuous modernization methodology that meets the Navy's needs into the future. It is called the "Rapid Capability Insertion Process/Advanced Processor Build (RCIP/APB)."

Two Revolutions in Warfare since World War II

The seeds of today's combat systems were planted with the introduction of digital computing technology into maritime combat systems early in the Cold War. The pivotal role the Defense Department played in early Naval Tactical Data Systems (NTDS) development proved to be the lead influence in early development efforts and remained so into the early 1990's. The introduction of NTDS was motivated by some profound, but evolutionary changes introduced by an increasingly challenging array of threats posed by the Soviet Union. Their defining dimensions were kinematics of airborne threats, ever increasing in speed and maneuverability,

and numbers. They required much greater automation to keep up with higher data rates, like target positions and identification, and the ability to keep track of and make decisions on large quantities of threats. In short, the World War II based procedures of manually plotting target locations and locally assigning weapon systems to targets was being overwhelmed by the speed, complexity, and scope of the battle.

However, two watershed developments produced revolutionary challenges, both driven by breakthroughs in technology and the latter by a corresponding change in objectives of maritime operations. They were, as mentioned in the introduction, the deployment of the low altitude (sea skimming) cruise missile and the fall of the Soviet Union with its corresponding shift of both the character of the threat and the maritime battlefield. Each of these are worth treating in some detail because of their profound impact on the development and application of digital computing in the Navy's combat capabilities.

The First Revolution – Platform Sensor to Weapon Integration

In the 1960's, the U.S. Navy was in the forefront of developing digital computing technology for weapons systems. Although these efforts resulted in computer-based capabilities that were effective with manned air threats, the introduction of the sea-skimming ASCM effectively reduced the reaction time to a level that could not be accomplished with individual sensors and weapons, coordinated by human evaluation and decision.

The answer was the integration of sensors, computer based command and decision, and weapons employment at the platform level. This was the development of the AEGIS Weapon System and it required a complete rethinking of tactics, techniques, and procedures as well as the harnessing of emerging technologies. The computing technology the AEGIS system relied upon was the state of the art in the early 1970's. It adapted second generation digital computers¹, then in use by NTDS systems, called



AN/UYK-7's, and connected them together using a point-to-point wire backbone that enabled the direct information flow between its computer based radar, AN/SPY-1, a command and decision capability that included rudimentary decision producing doctrine statements, and the missile system. This platform integration restored the effectiveness of a ship's combat power to a level that was effective and restored the U.S. Navy's maritime dominance into the 1990's.

The computing technology of this era was still led by the U.S. Defense industry and included the latest in main-framed computing techniques, modern computer languages of the time and military standard processing plants. The monolithic or mainframe software structure included innovative ideas like "shared memory" to optimize the loading of 16 kps processors and limited memory modules. Although the continued evolution of technology improved processing

¹ Boslaugh, David L. *When Computers went to Sea: The Digitization of the US Navy* (Piscataway: IEEE, 1999) 361.

speeds and memory into new military standard computers in the 1980's, the monolithic software design structure of the AEGIS Weapon System remained virtually unchanged with add-on modifications supporting each additional change to systems.

The Second Revolution – Multi-Platform Network Centric Integration

Two significant changes occurred, in close succession that again jeopardized the effective warfighting capability of the U.S. Navy. First, the fall of the Soviet Union at the beginning of the 1990's caused a fundamental shift in the battlefield environment and the character of the threat. Simultaneously, an information technology business explosion occurred seizing the leadership of computing technology from the U.S. Defense Department and placing it firmly into the hands of commercial industry, driven by a mega-civilian market share on a global scale.

In the DoD led era, the evolution of software based Cold War maritime warfare capability was carefully tailored to counter the symmetric "blue-water" threat of the Soviet Navy which allowed for extending the decision timing by defense-in-depth. With the demise of the Soviet Union, the U.S. Navy quickly found itself without a global maritime competitor and increasing drawn into a battlespace defined by the littoral environment. Furthermore, maritime warfare was challenged with:

- Asymmetric threats of swarm boats
- Land launched sea-skimming ASCM's in the clutter of the sea-land interface
- Uncertain tactics of para-military operations
- Emerging demands for deep power projection



The Navy's sensors, computer command and control systems, and weapons employment however, remained optimized to win the Cold War. Further, the ability to rapidly seek out new technology and integrate it into existing warfighting systems to combat these new threats was limited, both by current defense procurement practice and by weapon system development philosophies. In short, the Navy was ill equipped to meet all of these modern warfare challenges.

The challenges encountered fundamentally re-shaped the time-speed-distance dimensions of maritime battlespace. As examples:

- Littoral operations, forced much shorter reaction times.
- Neutral air and shipping activity became realities of the littoral battle-space clutter
- Geography and environment challenged systems optimized for open ocean operations
- Threats were masked from platform co-located sensors and weapons.

Additionally, the destabilization of large areas of the world formerly under the influence of the Soviet Union, the emerging hostile powers that control the energy rich regions of the earth, and

most profoundly the rapid expansion of terrorism as means to influence global security moved the United States and its allies into a world dominated by asymmetric warfare. These conditions led to the requirement for NCW, where sensor information and weapons can be integrated across high capacity seamless networks. However, the challenge of getting these required capabilities into all of the nodes across the maritime portion of the architecture now is problematic with the closed, tightly coupled computing systems of the platform integrated combat systems.

Adversarial Exploitation of Modern Technology

While the U.S. Navy struggled with the effects of this new battlespace, terrorists and guerrilla insurgents have taken immediate advantage of the information technology explosion. They have the agile and compact infrastructure to take immediate and full advantage of every newly developed state-of-the-shelf technology. Terrorists have effectively utilized the Internet, for example, as “Cyber-planning” and command and control tools². Most notably, IT was utilized in this capacity during the planning of the successful 9/11 attacks. Further, terrorists have used the Internet as an intelligence tool to gather information on potential targets and assess their vulnerability. One captured al Qaeda computer contained engineering and structural architecture data of a dam, enabling precise mission planning to be conducted on this target³.

Defense Department loss of Computing Technology Leadership

Computers will change our lives more in the next 10 years than they have in the last 20.

Bill Gates, Chairman, Microsoft 25 Feb 2004

In the backdrop of these battlespace-defining revolutions, the Defense Department dominance of information and computing technologies was lost. Two profound effects resulted from this fall from influence:

- The DoD could no longer demand characteristics and capabilities in computing technologies that were optimized to its needs. In actuality, the market share the DoD represents is dwarfed to insignificance when compared to the global IT market place.
- The carefully developed and tailored information infrastructure that supports the legacy DoD information environment has becoming increasingly more expensive and less reactive to user needs with each passing year. It includes “government-unique” message standards for data systems, land based software development sites for the archaic monolithic software designs, and government only computer languages.



Meanwhile, the commercial sector has taken firm hold of IT and has driving it at a breath taking pace, powered by the emergence of internet protocols, computing speeds that have grown exponentially and a world-wide public demand for increasing capability. The business base that has emerged not only dwarfs the U.S. Defense Department

² Timothy L. Thomas, *Parameters*, (Spring 2003) 112-113.

³ Gellman, “FBI Fears Al-Qaeda Cyber Attacks,” *San Francisco Chronicle*, (28 June 2002) 1+

(DoD) acquisition influence in magnitude, but also has significantly increased the speed with which the gap is widening. The net effect makes virtually, all of the tactical data and software based weapon systems of U.S. Navy ships and aircraft unaffordable to maintain, much less adding new capabilities (see Figure 1). Further, since current and potential adversaries are not required to conform to accepted technology development and procurement processes, they realize a level of agility, cost-efficiency and a technological advantage that is, in some way, far superior to the today's national defense establishment.

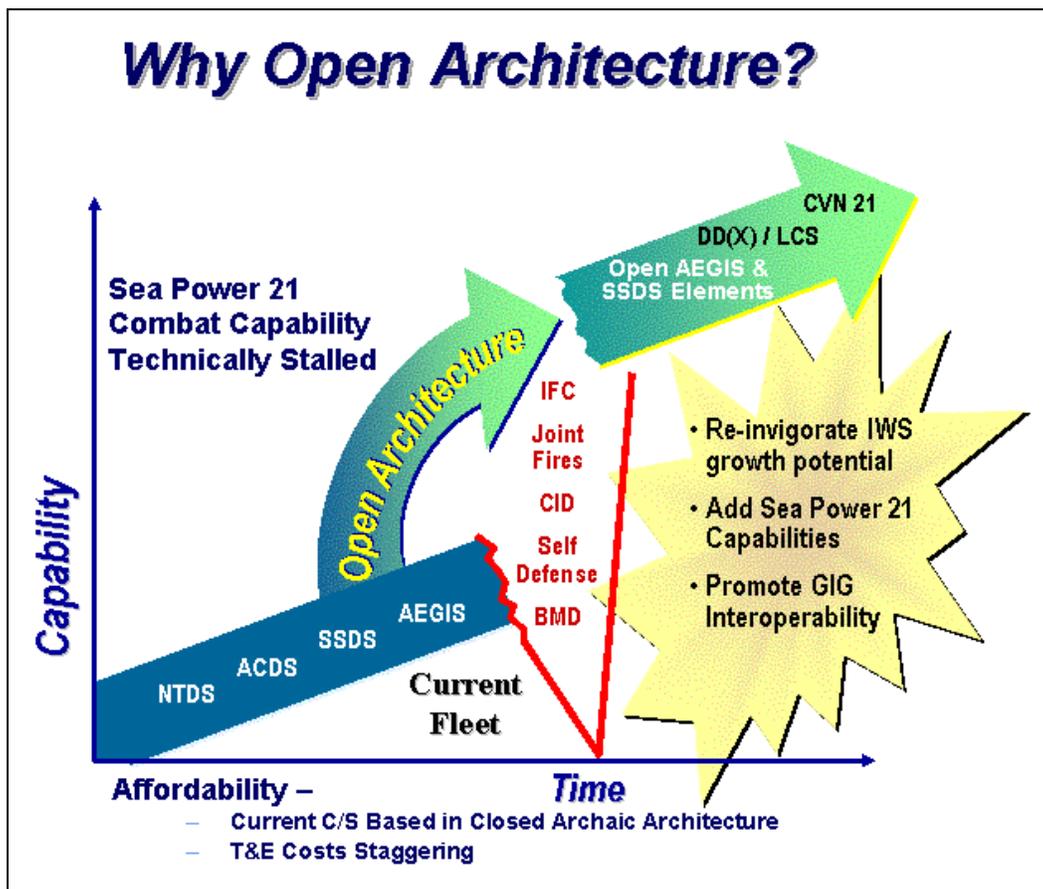


Figure 1 Why Open Architecture?

There is good news in this otherwise bleak situation. Fundamentally, maritime and joint planning and operational level capabilities were developed in the modern Internet Protocol (IP) based technologies. They constitute a significant bundle of capabilities for operational planning and mission execution and, most significantly, include the lion's share of the computing requirements of the force. Additionally, they are the basis for these emerging concepts:

- Web-based command and control
- Timely sharing of intelligence
- Off-board surveillance and reconnaissance information
- Time critical focusing of combat power

Capabilities such as the Global Command and Control System-Maritime (GCCS-M) and the Theater Battle Management Control System (TBMCS), used to plan offensive strike operations, are compatible with "publish and subscribe," data basing, and internet transmission control

protocols that leverage open commercial standards. Moreover, the Defense Department has recognized the power of the IP based information environment and is aggressive in defining both the capstone warfare based requirements and concepts that need to be embraced in the Global Information Grid (GIG). These conditions have been defined in the Global Information Grid Capstone Requirements Document⁴ (GIG CRD) and the architectural documents defined by the Assistant Secretary of Defense for Network Information and Integration⁵ (ASD (NII)). The Navy has taken, expanded on, and tailored the requirements and concepts defined in the DoD documents to develop the maritime information environment called FORCENet⁶. FORCENet, as an extension of the GIG, requires a seamless and timely flow of data to be transformed into executable information. It provides the knowledge building protocols through the tactical, operational, and strategic levels of warfare. To achieve that condition, the real-time weapon systems must be in the same IP based technology as the operational systems. Succinctly, it means that getting systems like the AEGIS Weapon System and the Ship Self Defense System Mark II (SSDS MK2), transformed aggressively out of their current archaic, monolithic, proprietary software conditions and into modern applications that conform to open commercial standards is essential to meeting the FORCENet vision. Further it is an operational imperative to ensure that the fundamental tenets of joint interoperability are realized in order to achieve a robust Network Centric Warfare capability.



⁴ USJFCOM, *Global Information Grid Capstone Requirements Document*. (JROCM 134-0130 Aug 2001)

⁵ DoD CIO, *DoD Architecture Framework Version 1.0* (15 Aug 2003)

⁶ DoN, *Transformation Roadmap: Power and Access...From the Sea*. (2003) 4.

Open Architecture in a Warrior's Terms

OA is multi-faceted, providing a framework for developing joint interoperable warfare systems⁷ that adapt and exploit open system design principals, standards and architectures. The two fundamental elements of OA are a Technical Architecture defining the Standards and Guidance for the Open Architecture Computing Environment (OACE) and a Functional Architecture (Oafa), embracing of an agreed upon framework of functional allocations, common/standard applications and services. OA enables a new approach in acquiring and managing reusable software components while taking advantage of standards-based computing technologies from the commercial off-the shelf (COTS) market place. These two elements depend on coordinated implementation guidelines and instructions, and involve the use of widely accepted and available specifications, standards, products, and design practices to produce systems that are interoperable, easy to modify, and extensible.

Categorizing Compliance with Open Architecture

The starting point in understanding the tenets of OA, for evaluating the conditions that exist in current computing environments, and finally, defining compliance targets for future systems requires definitive criteria. Table 1 has been derived from the OACE Technologies and Standards document⁸.

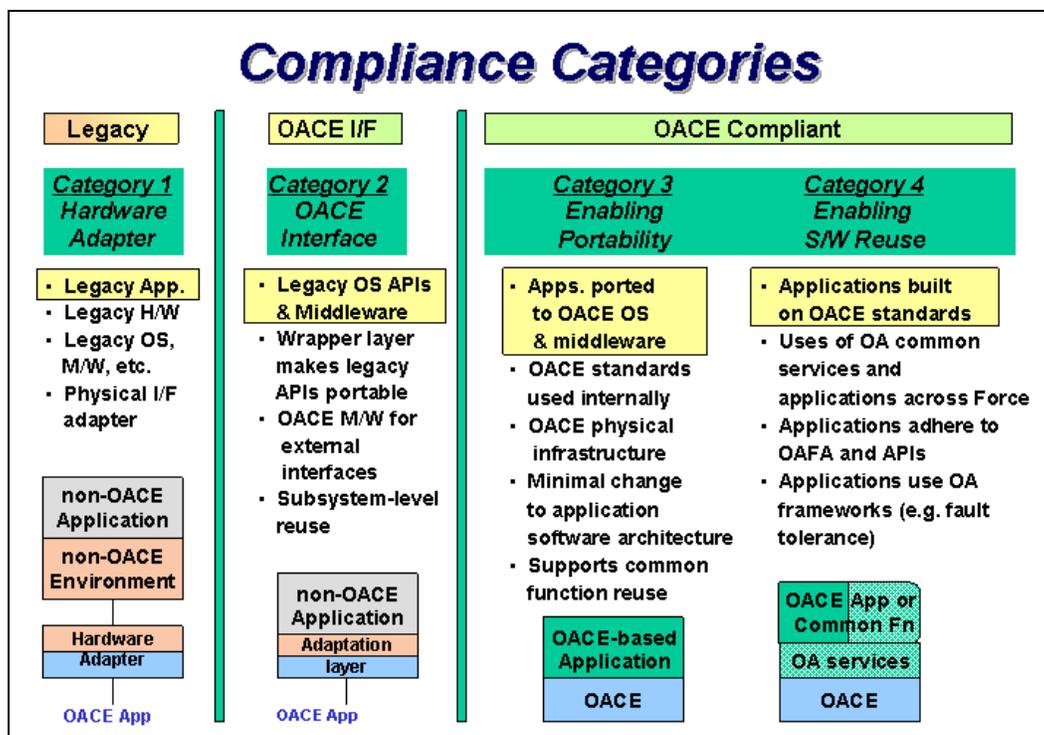


Table 1 OA Compliance Categories

⁷ All shipboard tactical systems, and tactical mission support systems, such as weapons, sensors, command and control, navigation, aviation support systems, mission planning, intelligence, surveillance and reconnaissance, interior and exterior communications, topside design, and warfare system networks.

⁸ Naval Surface Warfare Center, Dahlgren Division. *Open Architecture Computing Environment Technologies And Standards* (04 Sept 2003)

The significant distinctions are as follows:

- Most current combat & weapon systems are Categories 1 & 2, which are system designs that are precursors to true modular (de-coupled) hardware & software condition.
- Category 3 is the first OACE design, which allows change of hardware infrastructure without requiring change to software design (example: a MS Windows 95 version could be used on more modern Pentium PC than the 486 available when introduced).
- Category 4 is a maturation of the OAFE to allow cross platform use of common applications (example: an identical word processing application running on LINUX, Windows, Apple, etc. operations systems). Selected platforms could also add a dynamic resource management schema to provide shared optimization of computing design performance.

Relationships between technical community definitions in the computing environment, like DII/COE levels or the more recent construct Network-Centric Enterprise System (NCES) standards, are only loosely related to OA categories. The conundrum is that the majority of combat/weapon systems are not yet in an Internet Protocol configuration. OA enables the transition of these systems into a technology base that can conform to these definitions.

Open Architecture Computing Environment (OACE)

The Open Architecture Computing Environment (OACE) architecture is based on a commercial distributed services model that decouples software from hardware. Commercial industry computer designs exceed militarized integrated hardware and software designs in performance and reduced expense. Technological limitations prior to the 1990s required innovative and efficient use of memory. Integration was, by definition, platform system-centric in order to achieve the performance efficiencies of weapon systems. The OACE (see Figure 2) provides the technical design for the computing infrastructure that will provide⁹:

- A flexible foundation for rapidly introducing new warfighting capabilities into the combat system to pace the threat
- Interoperability across diverse joint battle management command & control systems
- A system design that fosters affordable development and life-cycle maintenance
- A system design that reduces upgrade cycle time and time-to-deployment for new features
- An architecture that allows technology refresh despite rapid COTS obsolescence
- Improvements in Human Systems Integration

⁹ OACE Technology and Standards

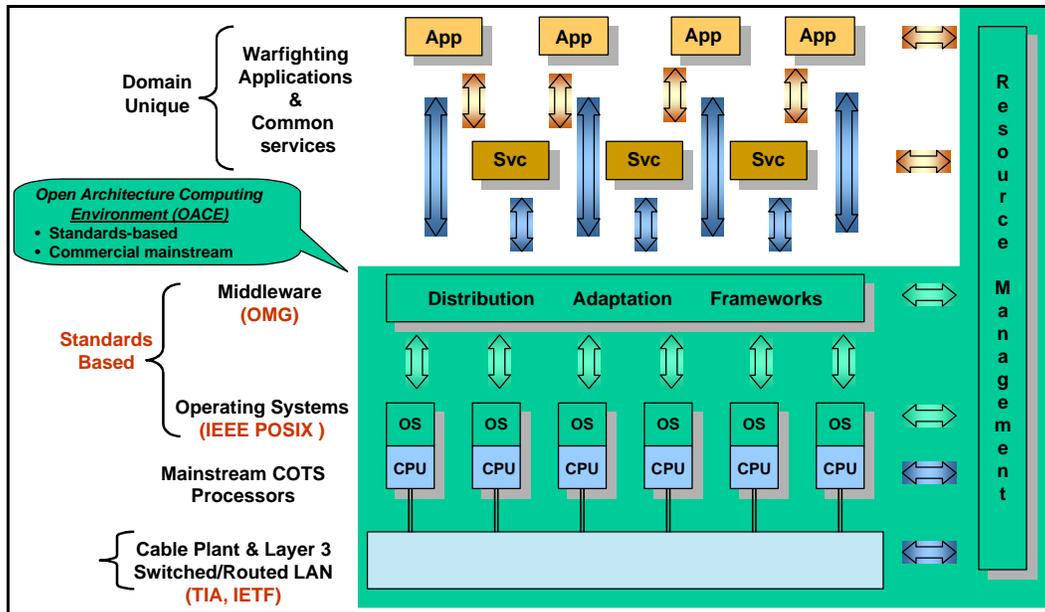


Figure 2 OA Computing Environments

Transitioning to OACE, by physically decoupling the tight dependencies between computer system hardware and software applications, does not in and of itself add warfighting capability. However, parsing the hardware and software infrastructure design into discrete components provides modularity mandatory for innovation flexibility. Only after rebuilding the current integrated warfare system (IWS) designs into OA technical infrastructure at the physical cable plant, processor, operating system and middleware layers, are they unconstrained for independent upgrade.

As each layer of the technical infrastructure is now loosely coupled by internationally recognized standard interfaces, flexibility in procurement and extensibility in performance is possible. The ability to reuse warfighting application technology across the Naval and Joint enterprise provides easily connected LANed interoperable components that provide new warfighter mission capabilities with minimal development effort and without requiring detailed knowledge of the internal workings and implementation. The distributed services approach will allow developers to wrap legacy allied/coalition applications for compatibility and the opportunity to explore multi-level security implementations will enable efficient and secure sharing of information.

The modular independence with each component, occupying a well-defined space and purpose, inherently supports flexibility in designing complex and varied systems. Replacing individual components of a layer, due to obsolescence or new capabilities, can be effectively managed and scheduled appropriately. The opportunity to rapidly insert new and enhanced capabilities is predicated on a modular design. The flexibility of an OACE has significant economic and capability value because physical hardware obsolescence occurs in a different timeframe than middleware and software applications. As an example, empirical data from the commercial industry indicates the cable layer should last 10 years plus, whereas operating systems are updated about every 3 years. This maintenance scheduling flexibility will be described further in the Rapid Capability Insertion Process/Advanced Processor Build (RCIP/APB) section.

Functional Capabilities Architecture

The OACE provides the technology conditions required for updating the combat systems into the IP computing system design. The Open Architecture Functional Architecture (OFA) is the functional characterization of warfighting and ship/control systems. This framework of functional allocations includes the performance requirements, information exchange standards. It also defines common services (e.g., time and navigation) and warfighting capabilities (e.g., track management, identification, training, etc.). Initially the OFA consists primarily of the identification of naval combat system functionality and their initial logical partitioning. The OFA provides the functional partitions (see Figure 3) and the information exchange between those partitions.

This OFA effort is far more complex than changing the computing hardware infrastructure. The warfighting capabilities resident in current combat system designs are intermingled and tightly coupled with the hardware design. Many of the application processes using shared memory designs (AEGIS) are duplicative (multiple trackers and displays such as AEGIS, GCCS-M, Tomahawk, etc. (see Table 2)) or service-specific (air, sub, surface, land). Because of these issues, gaining agreement has been time consuming yet crucial. The core effort has been focused on gaining agreement on common services of time & navigation for data registration, followed by establishing a core, common, joint track manager application. Accurate tracking and reporting of physical objects, both within the platform combat systems and across interfaces is key to joint network-centric decision making. All current efforts for Combat Identification (CID) and Integrated Fire Control (IFC) are predicated on an accurate, timely and coherent display.

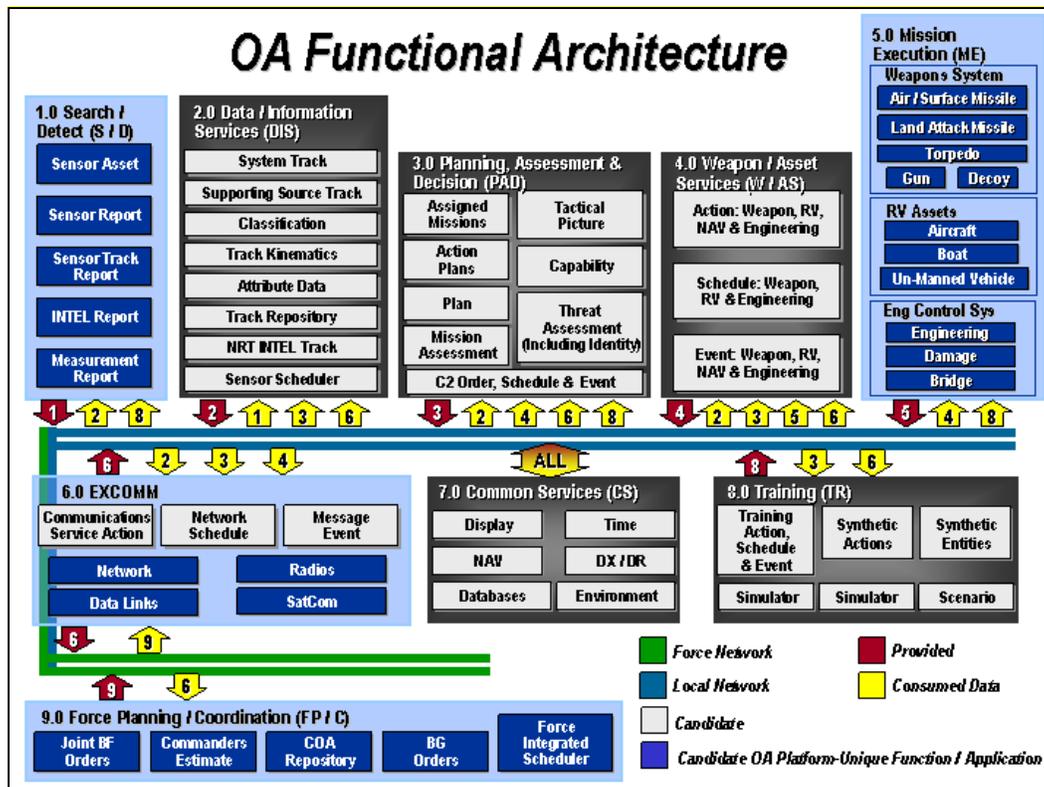


Figure 3 OA Functional Architecture

Acceptance of the joint track management application acknowledges the significant value added by the collaborative effort. For example, battle flags and the Allied Tactical Signal publication (ATP-1) and International Maritime Signals (HO 102) are early instantiations of interoperability for communicating and relaying mutually agreed standard signals for action or information between decision nodes. The use of standard phraseology reduced confusion in understanding the message content and was designed for flexibility, independent of the communication medium.

Too Many BMC2 Trackers & Displays	
Shipboard Internal	External & Joint
◆ SPY / Radar	◆ GCCS
◆ C & D	◆ DJC2
◆ CEC	◆ E-2C & Advanced Hawkeye
◆ ADS	◆ P-3C
◆ NFCS	◆ F/A-18 (USN & USMC)
◆ ATWCS/TTWCS	◆ CAC2 (USMC)
◆ SQQ-89	◆ AFADTS (USMC & Army)
◆ GCCS-M	◆ FCS (Army)
◆ C2P / CDLMS / CLIP	◆ AWACS (USAF)

Table 2 BMC2 Trackers & Displays

Establishing an equivalent common set of applications for tracking and reporting objects, concurrently functionally independent of the external communication medium, is required for the joint interoperability across battle management command & control computing systems.



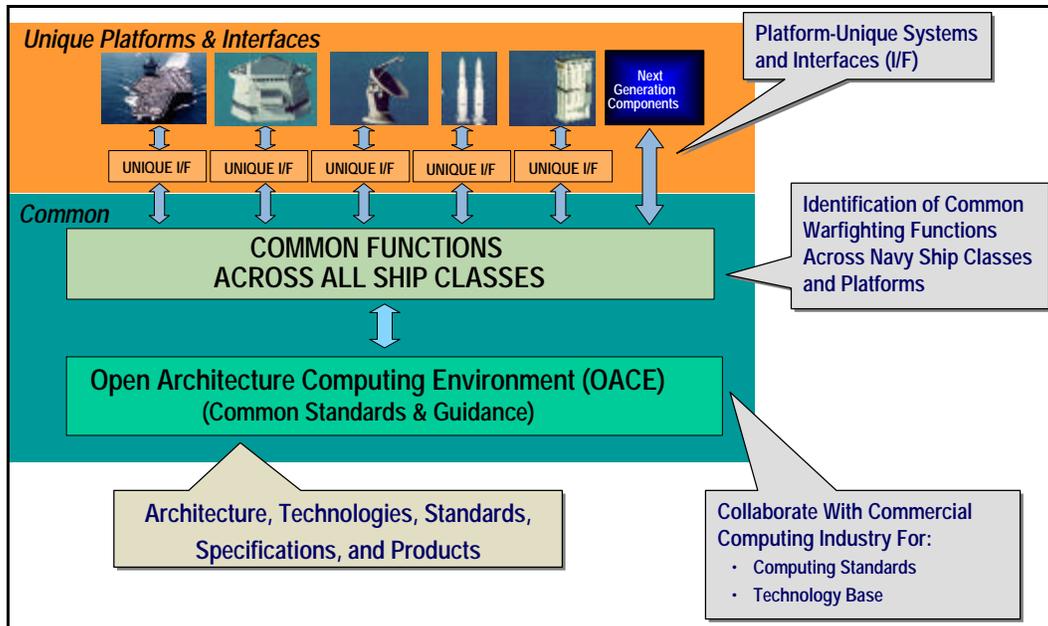


Figure 4 OACE/OAFA Relationships

OACE/OAFA Relationship

The development of OA requires a comprehension of the relationship between the OACE and OAFA. As illustrated in Figure 4, and shown previously in Figure 2, the OACE consists of standards-based middleware and operating systems, mainstream commercial-off-the-shelf (COTS) processors and technologies, and guidance for commonality. The OAFA primarily defined to:

- Identify Navy warfighting functionality across platforms and systems that may include commonality of function, processing, design, interface, and/or data/information exchange; and
- Further identify those systems, functions, or interfaces that are unique to particular Navy platforms. The OACE must be capable of executing the performance requirements for the warfighting capabilities in the proposed OAFA.

Today's Software Based Integrated Combat Systems Challenges

As discussed previously, base-lining to what degree fielded software based integrated weapon systems and associated C2 capabilities comply with the engineering standards and functional allocations of Open Architecture today is essential. Presently none of the in-service and fielded integrated combat system backbones are fully compliant to OA Category 3 and, as such, are not prepared for immediate acceptance of open system applications. However, several systems have been modernized using COTS technology and provide advantageous foundations from which to migrate to an open environment. Selecting which of the integrated combat system backbones can be used to support a migration strategy is an essential first step. Once the selection of integrated backbone is accomplished, a detailed migration plan can be established and investment resources organized to support it.

Base-lining Current Capability

The Navy's premiere integrated combat systems are all heavily reliant on the DoD-specific tactical information standards of Navy Tactical Data Systems (NTDS) Model 4 (LINK 11/M series data message standard) or NTDS Model 5 (LINK 16/J series data message standard) conditions. Specific systems include:

- AEGIS Integrated Combat System (both Model 4 and 5 versions)
- Advanced Combat Direction Systems (ACDS)(both Model 4 and 5 versions)
- Ship Self Defense System (SSDS) Mark 1 and 2
- Hawkeye Air Early Warning mission control system
- Mission control software for F-14 (NTDS Model 4)
- F-18 (NTDS Model 5)

All of these systems were designed when the Defense Department's military specifications for computer systems were state of the art. They were also optimized for "platform-centric" integration and weapons employment. They continue to have software structures that are monolithic in nature, and incorporate design features based on the DoD led computing technologies of the 1980's.

These conditions set up two challenges. First, many of the design concepts embraced during this era were and are unique to the Defense Department. Examples of these concepts include, message standards used in LINK 11 and LINK 16 information dissemination structures, NTDS software organizational structures supporting combat identification processing, mil-standard physical connector interfaces, and deterministic design criteria once considered essential to high priority weapons control. When the information technology explosion took off in the 1980's, it left the DoD with a



compounding and expensive requirement to maintain unique infrastructure for monitoring and maintaining niche software based capabilities. The financial weight of supporting this infrastructure is bleeding off significant portions of DoD investment sorely needed to deliver new capabilities in the battle-space of the future. Second, the mainframe integrated software design of these systems makes adding new capabilities, or even improving performance, tremendously expensive and very challenging from an engineering perspective. Software designs were optimized to gain maximum effect from the limited processing capacity of military standard computing plants. For instance, the shared memory design is problematic, especially for modern software applications, because it is specifically dependent on the host computing plant's performance characteristics. This "hard coupling" of software to hardware requires improvements in one be matched with significant design adjustments in the other.

AEGIS Integrated Weapon System v. modern technology and network centric warfighting imperatives.

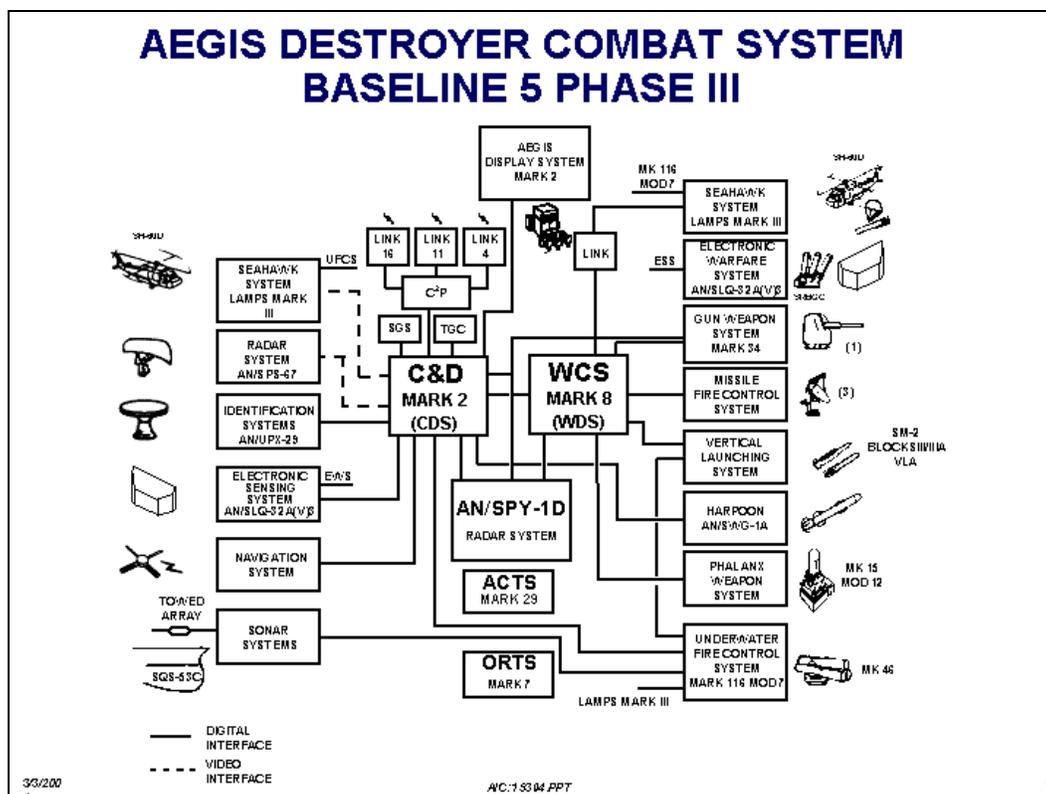


Figure 5 AEGIS Baseline

The AEGIS Combat system provides the most significant and difficult example of the challenges presented by these legacy conditions. It is the Navy's most successfully integrated ship and weapons system at sea. The system design provided for robust defense of the CVBG in blue-water operations against the Soviet fleet, in particular defending the carrier from aircraft and cruise missiles. Gaining detect-to engage time in the reduced battlespace of supersonic missiles required a very deterministic point-to-point interface between sensors and weapons control. The tight integration between the SPY radar, Command & Decision (C&D), and Weapons / Launcher / Fire Control was achieved in 'real-time' by optimizing the relationships of hardware and software applications. This tightly integrated combat system also fostered a proliferation of individual component track files (SPY, C&D and AEGIS Display System),

which optimized performance at that particular system. Since then, computing architectures have transitioned and evolved to support a stronger and broader market than the military.

The optimization of the AEGIS IWS design has become a double-edged sword with the addition of enhanced capabilities, such as Tomahawk, CEC and GCCS-M. These enhancements have caused adjunct relationships in handling sensor data and the elements of the common tactical data picture. The net result has been to establish a challenging correlation problem across multiple track databases, see Figure 6. Moreover, interoperability across the battle force using TADILs and CEC became more precise, yet less coherent (due to dual-designations, etc.) as the various mechanisms for reporting track objects failed to coalesce into a common picture. Finally, command support from ISR and distributed is collaborative planning tools not fully integrated, forcing warriors to manually correlate and transfer information between information and weapons systems.

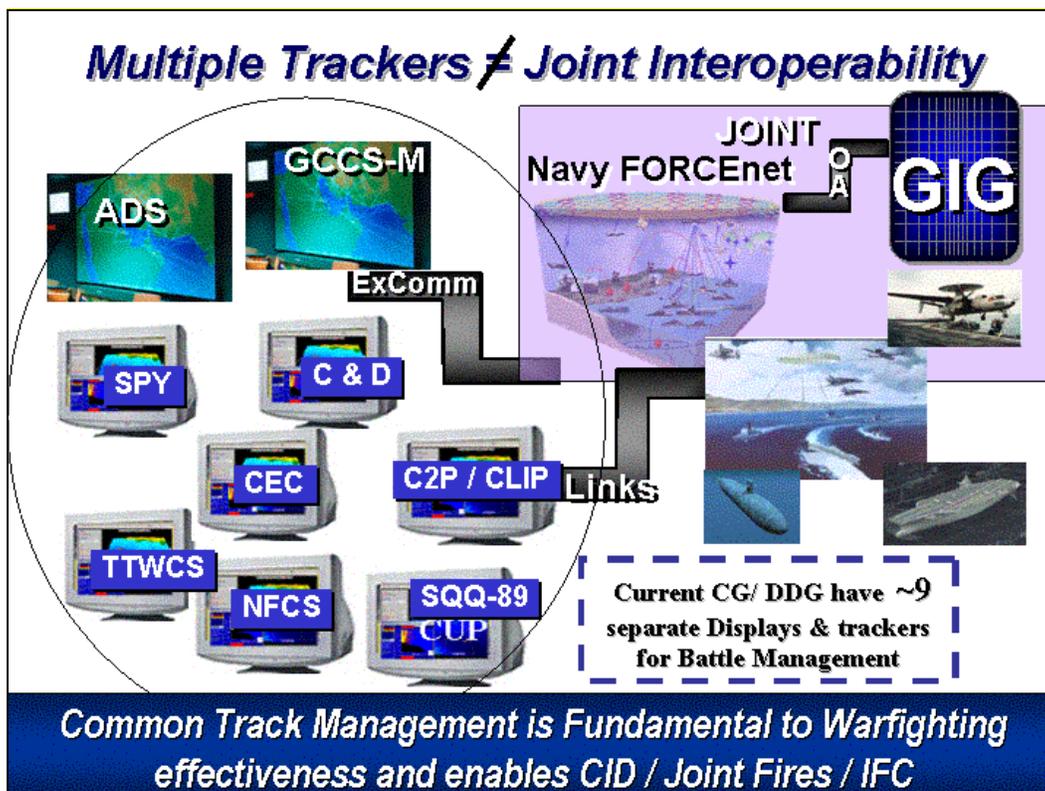


Figure 6 Multiple Track Displays

Tactical and Operational Commander's Operational Needs v. Weapon System.

A commander's battlespace is a unique perception of time, speed and distance affecting his responsibilities. A Tactical Commander requires a "hard real-time", closed-looped quality of service support for weapons employment once an imminent threat is revealed. Integrated combat systems that evolved in a main-framed software structure, such as AEGIS IWS, are optimized specifically to support these requirements. Conversely, the Operational Commander's focus relies on situational awareness (SA) for the near and far-term objectives of planning and resource management. These capabilities as well as the C4ISR community requirements are supported by the existing COTS-based planning systems such as GCCS.

The net effect of these diverse requirements has been the development of software based capability technology instantiations. Weapons system computing environments remain essentially locked in the archaic structures in which they were originally designed, despite the transition of hardware into COTS. This transition caused “niche-specialized” COTS products that are tailored to monolithic software structure. The customizing of these COTS products largely negates the advantages they traditionally bring.

Identifying Open Architecture Migration Options

Fortunately, the most recent instantiations of in-service IWS backbones establish migratory opportunities into the OACE. Careful review of these backbones provides three basic potential paths to exploit:

- AEGIS IWS Baseline 7 for CG/DDG
- Ships Self-Defense System (SSDS) MK2 for CVN/LHD/LSD
- Common Network Interface (CNI) for LHA/LHD

The first two are based on the significant investments in modern computing plants. The third opportunity takes a step approach that modernizes selected portions of the computing environment in the CDS backbones of selected ships on a periodic cycle.

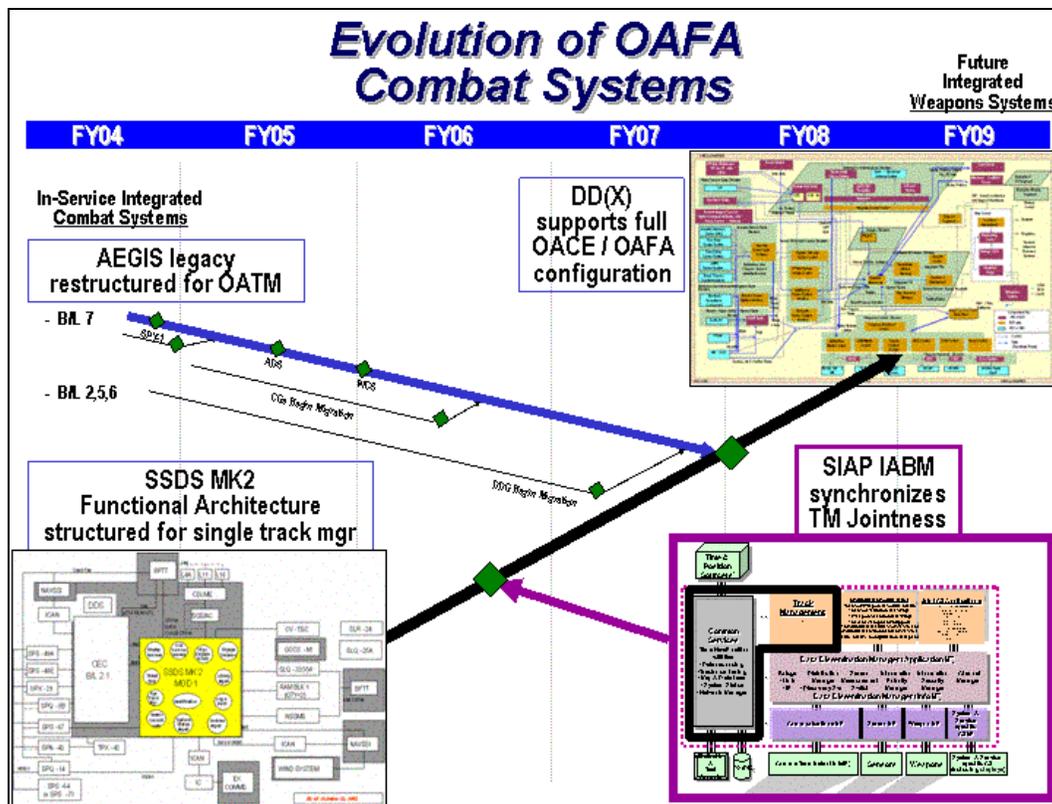


Figure 7 Evolution of OAFA Combat Systems

What makes AEGIS Baseline 7 and SSDS MK2 key are in the relatively modern COTS based computing plants on which they reside. Both have migrated to network backbone elements that embrace “fast Ethernet” switching technologies. This “cable layer” condition allows for use of modern transmission control protocols and much greater efficiency in sharing data across multiple nodes. Next, it causes the weapon systems backbone to converge on new

ship control backbones introduced in the SMART SHIP technology improvements. AEGIS and SSDS computing plants abandoned the military standard processors of their earlier predecessors and adopted similar COTS processors, encased in VME¹⁰ chassis incorporated “citadel cabinets” that both provided the “shock hardened” environments required for warships, but also providing conditions for rapid upgrades of processors without extensive ship alterations. Finally, SSDS MK2’s design incorporated the key features of a modern functional architecture, required to meet key tenants of network-centric capability (see Figure 7 above), as well as the tenants of “common re-use applications.”



Finally, the CNI opportunity leverages the advantages outlined in the BL7 and SSDS MK2 in all but the reliance on leveraging completely modernized computing plant. As such, it is specifically targeted at those CDS systems that are in the older “mil-standard” aligned platforms, which remain critical nodes in the joint network-centric architecture. It allows for gradual migration of software-based capabilities that are OA compliant, by adding a scaled modern computing plant to support the modern applications, along with modern to legacy interface capabilities to retain functions within the unaffected legacy computing plant.

¹⁰ VME bus (Versa Module Europa) is a flexible open-ended bus system, which makes use of the Eurocard standard. It was introduced by Motorola, Phillips, Thompson, and Mostek in 1981. VME bus was intended to be a flexible environment supporting a variety of computing intensive tasks, and has become a very popular protocol in the computer industry. It is defined by the IEEE 1014-1987 standard.

Integration of Weapon Systems Functions into the FORCEnet Environment

“Joint Vision 2020’s view of future warfighting includes complex, higher-operational tempos that demand unprecedented distribution of information, rapid warfighter interaction, and joint/coalition interoperability. The increased lethality, mobility, and range of weapons, coupled with a smaller and more dispersed force structure significantly increase the three-dimensional battlespace over which an individual force element must maintain awareness and control. The challenge of the warfighters’ command, control, communications, and computers (C4) requirements will be further complicated by the need for our forces to work in concert with allied and coalition forces, and to maintain connectivity in a post-nuclear environment.”

USJFCOM JROC Approved Information Dissemination Management Capstone Requirements Document

The Global Information Grid (GIG) will provide the enabling foundation for Network Centric Warfare (NCW)¹¹, information superiority, decision superiority, and ultimately full spectrum dominance. The information advantage gained through the use of NCW allows a warfighting force to achieve dramatically improved information positions, in the form of common operational pictures that provide the basis for shared situational awareness and knowledge, and a resulting increase in combat power. The ability to achieve shared situational awareness and knowledge among all elements of a joint force, in conjunction with allied and coalition partners, is increasingly viewed as a cornerstone of transformation to achieve future warfighting capabilities. For naval forces, the success of exploiting the GIG in NCW depends in large part on how well it achieves interoperability and force-wide information sharing through the implementation of FORCEnet. The purpose of this portion of the discussion is to establish the relationship between these top-level architectures and NCW with OA.

The key element essential to the success of future warfighters is a highly responsive, high-capacity GIG that allows them to integrate and synchronize their capabilities within the multitude of fluid, rapidly changing military operational environments that must respond to ever-changing missions. With accurate, timely, secure, and assured information, commanders and their staffs are able to gain and apply superior knowledge and understanding of the battlespace. Further it provides the ability to collaboratively formulate and disseminate plans and orders, synchronize forces, exert effective control over the battlespace, sustain a high velocity of action, and help achieve full-spectrum dominance over the enemy.

The focus of future Command, Control, Communications, Computers and Intelligence (C4I) capabilities¹², and by extension NCW, is embodied in three essential prerequisites needed to meet emerging warfighter requirements. First and foremost, the user must be preeminent in defining what information is needed. Second, to use the limited available bandwidth efficiently, the information transmission and retrieval scheme must only transmit information that the

¹¹ An in-depth treatment of NCW is provided in the book: David S. Alberts, John J. Garstka and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised) (C4ISR Cooperative Research Program, Aug 1999)

¹² USJFCOM. *Information Dissemination Manual Capstone Requirements Document (IDM CRD)* (JROCM 015-01 22 Jan 2001)

warrior specifically needs or requests. Third, the identification, shipping instructions, and retrieval options must be sufficiently flexible to meet the warrior's rapidly changing mission requirements.

The Department of Defense established its exploitation of the GIG¹³ as:

- 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, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. The GIG provides interfaces to coalition, allied, and non-DoD warriors and systems¹⁴.
- Any system, equipment, software, or service that meets one or more of the following criteria:
 - Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
 - Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
 - Processes data or information for use by other equipment, software, and services¹⁵.

The GIG is a key enabler of NCW and is essential for information and decision superiority. It will enable C4I integration of joint forces, improve interoperability of systems, and increase optimization of bandwidth capacity thereby dramatically improving the warfighting capabilities. The NCW tenets of netted sensors, automated battle management, and integrated fire control all depend on providing GIG enabled common operational environment. In particular, the GIG will support¹⁶:

- Warfighters' ability to operate with reduced forces at high operational tempos where dynamic planning and redirection of assets is the norm.
- Delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets to joint commanders, their forces, and the President and SecDef within specified time frames.
- Warfighters' ability to obtain and use combat and administrative support information from national, allied, coalition, and other widely dispersed assets.

¹³ Definition of A DoD Chief Information Officer (CIO) memorandum, dated 22 September 1999, established the definition of the GIG, which subsequently was revised on 2 May 2001, by agreement among the DoD CIO, the Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L), and the Joint Staff/J6.

¹⁴ GIG CRD

¹⁵ IDM CRD

¹⁶ Ibid.

- Collection, processing, storage, distribution, and display of information horizontally and vertically throughout organizational structures across the battlespace.
- Rapid and seamless flow and exchange of information around the globe to enable collaborative mission planning and execution from widely dispersed locations and at different levels (to include strategic, operational, tactical, and business).
- Timely, assured connectivity and information availability for decision makers and their advisors to support effective decision making.
- Integrated, survivable, and enduring communications for the President and SecDef, Integrated Tactical Warning and Attack Assessment (ITW/AA), and strategic forces.

Essential to the warfighter's decision-making capability is having the right information, arrive at the right place, to the right person, at the right time, over the right communications path, and in the right (usable) format (as seen in Figure 8 IDM OV-1). Meeting this goal requires the entire GIG to be thoroughly integrated and synchronized, highly responsive to a changing operational environment, and resistant to system malfunction and deliberate attack. Working within the GIG, IDM addresses the awareness of available information and knowledge of changes to that information, the ability to access the information without having to know its exact location and format, and the efficient delivery of information. Through improvements in these areas made possible by the development of IDM tools, the commander at each echelon will be able to take advantage of the emerging capabilities that are envisioned to be integral to the GIG.

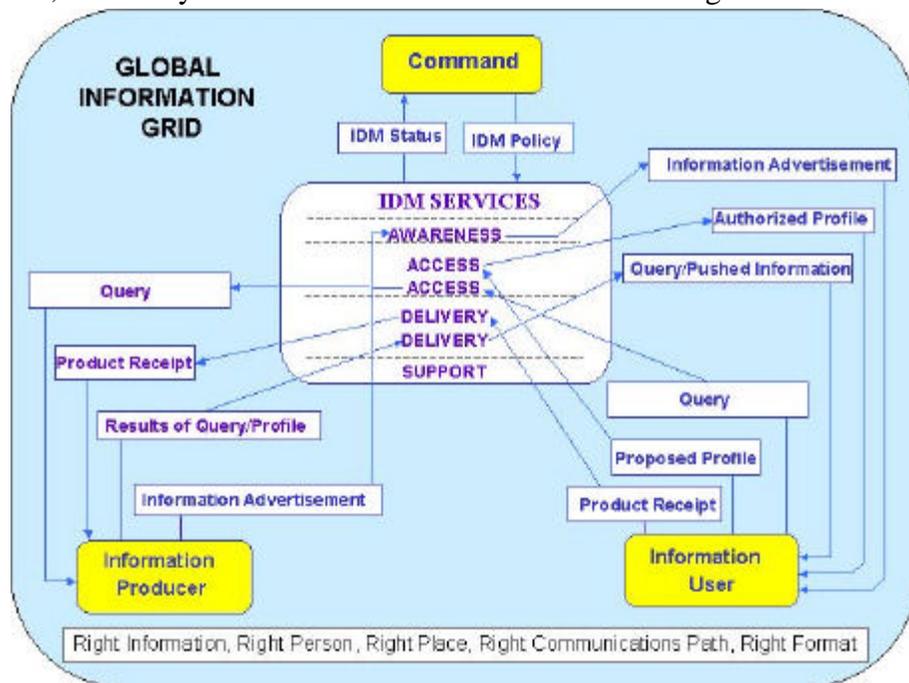


Figure 8 Information Dissemination Management (IDM)

In addition to being thoroughly integrated and synchronized, IDM must be capable of supporting the

dissemination of critically time-sensitive information to designated warriors in as close to real time as technically possible to meet the requirements of their operational situation. The dynamic nature of these urgent information dissemination requirements necessitates adopting a new paradigm for dissemination based on identifying those information elements requiring real-time/near-real time delivery to specified warriors as distinct from all other information requiring

less-urgent delivery. This new IDM paradigm will drive the dissemination of extremely time-critical information to those warriors, who need it, by identifying the time-critical information elements and matching them with specific warriors' identified (and possibly dynamically changing) information needs. For these warriors, the identified time-critical information elements are called "survival" information because they convey one of the following three basic factors:

- Information that requires the recipient to take immediate action to avoid danger or hostile action
- Information that is essential to enable the recipient to take immediate action to destroy, nullify, or defeat a hostile entity, weapon, or force
- Information that will prevent the recipient from causing fratricide

The paradigm also addresses the requirements of the majority of warriors and information elements that do not meet the above described survival criteria. For these warriors, information is characterized as "planning" information because, even though in some cases, it can be time-sensitive, it is used to support some action in the future (including the near future). While it is true that some planning information requires time-sensitive dissemination for some warriors, it still does not meet the life-threatening time-critical survival information requirements. Determining whether a particular element of information meets the survival or planning criteria is dependent on the warrior's operational situation, the commander's information dissemination policy, and the information content. In which category an information element fits, is governed by the warrior's information requirements profile. Consequently, categorizing an information element as being either survival or planning identifies the relative urgency of its delivery requirements from the warrior's operational perspective. Survival information will typically be characterized as a critical Information Exchange Requirement (IER) in Operational Requirements and Capstone Requirements Documents. The GIG must be sufficiently responsive to ensure the timeliness specified for critical IERs is achieved, and effective use of information management dissemination processes are crucial to making these operational imperatives a reality.

The concept of survival information is best described as follows:

- It is a subset of the information required for battlespace situational awareness, implying that all survival information is relevant to situational awareness. However, not all information used for situational awareness can be considered as survival information.
- It pertains to perceived threats in the area of operations that are geo-spatially related to the individual warfighter or the fighting platform. Hence it informs about objects and events in the immediate geo-spatial region around a warfighter that can cause destruction of life and property.
- It prompts either an immediate action or a decision from the recipient and is generally of short duration.
- Survival information is also dependent on the context determined by current mission, operating environment, and commander's intent.
- In most circumstances, survival information is predetermined on the basis of perceived threats and is immediately disseminated to the warrior when available.

It is unique and distinct to each individual and fighting platform in the battlespace. This implies that the same information element may be treated as survival information for one warfighter and as planning information for another.

The importance of information to, and in many respects the information needs of, the warfighter have not changed over time. What has changed is the increased access to information and the technology that permits greater manipulation and transfer speeds for the increasing amounts of information. While this has enhanced the warfighter's capabilities in many areas, advancements in information technology have also created new challenges in the form of information paralysis and/or information overload. How much information is enough to make a good decision? If decision makers wait, can they get additional information to improve their understanding and make a better decision? If they have too much information and are unable to determine critical elements, does the information have the same value?

FORCENet as an integrated part of the Global information Grid

FORCENet includes all aspects of communicating; sharing relevant valid information in near real-time (some time constraints) using expanded networks; sensing everything with information gathered from multiple spectrum and types of sensors; being capable of precise location in four dimensions; and maintaining security of those linkages and networks that allow joint and coalition forces to share timely, relevant information¹⁷. Knowledge can be created or lost due to the processing of data and information. Having real-time, accurate information that can be shared and assessed creates knowledge. Knowledge is a force multiplier. As naval forces progress to 2009, there will be increased efforts to provide secure, reliable networks that support joint and coalition command and control.



One of the fundamental objectives of FORCENet is to support situational awareness throughout the battlespace, improve combat identification, and reduce the risk of fratricide. Critical to this objective is the linking of all the sensors in the battlespace to provide a timely, accurate, continuous picture of the situation. Initiatives focus on improving data management and utilization of available information exchange links. Massing effects of widely dispersed forces requires fast, reliable communications that can support the transfer of pertinent, relevant data and communications. Investigating and investing in new technologies that protect networks, communications and precision navigation, promote spiral development to meet emergent operational/informational demands. In short, the imperative is to transform from a platform centric to network centric Navy.

The FORCENet architecture describes the construct and the framework for Naval Warfare in the Information Age transforming the Navy and Marine Corps to make NCW a reality. FORCENet integrates Warriors, Sensors, Networks, Command & Control, Platforms, and Weapons into a networked, distributed joint combat force, scalable across the spectrum of

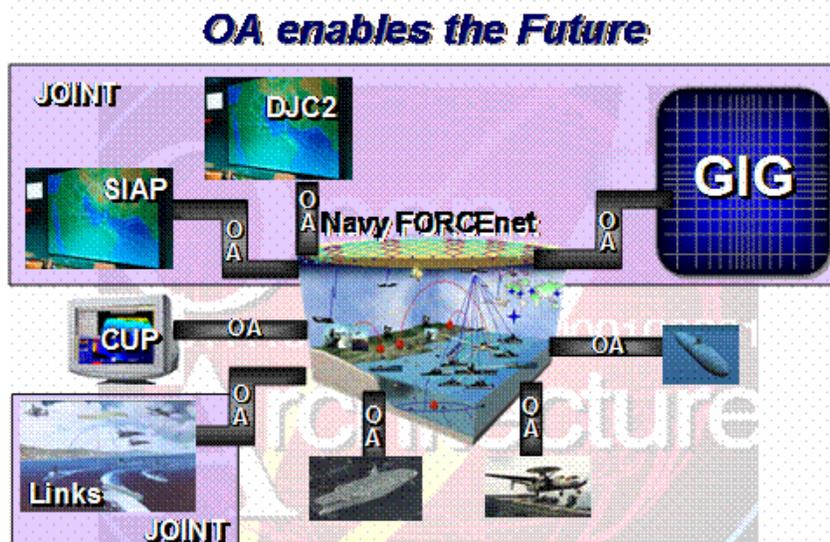
¹⁷ Space and Naval Warfare Systems Command. *FORCENet Architecture and Standards Document* (Ver 1.1 3 Nov 2003)

conflict from seabed to space, from sea to land. The FORCENet architecture will contain the enabling elements for the Naval Transformation Roadmap and Seapower 21 Pillars of Sea Strike, Sea Shield, and Sea Basing¹⁸, and for the supporting initiatives of Sea Warrior, Sea Trial, and Sea Enterprise. The architecture will also be coordinated with Service transformation initiatives in the Army, Air Force, and Coast Guard. A fundamental FORCENet objective is the development of a Naval networking infrastructure and integrated applications suite with full interoperability among the service components, joint task force elements, and allied/coalition partners.

The FORCENet architecture is based on a commercial distributed services model. This offers the ability to reuse technology across the Naval and Joint enterprise by providing components that can be easily connected in a wide variety of ways to provide new warfighter mission capabilities with minimal development effort and without requiring detailed knowledge of the internal workings and implementation. The distributed services approach will allow developers to wrap legacy allied/coalition applications for compatibility. Proposed multi-level security implementations will enable efficient and secure sharing of information required as an ICD functional requirement.

Open Architecture is the fundamental enabler for the FORCENet capability that allows a broad and rapid exchange of information and the ready assimilation and use of this information by the warfighter to enhance decision making.

The goal of the Open Architecture Computing Environment (OACE) is to provide technical performance, architecture, and design guidance for the computer programs and computing infrastructure of future Naval Combat Systems (NCSs) and Naval Warfare Systems (NWSs).



FORCENet’s seamless information to knowledge building imperatives depends on Open Architecture.

Meeting the Sea Power 21 challenges to seamlessly connect Sea Strike, Sea Warrior and Sea Shield, with the enabling pillars of Sea Basing, Sea Trial and Sea Enterprise, FORCENet must support relationships between three dimensions of the information space. The first dimension is the data domain: data, information and knowledge. The next dimension is the time

“FORCENet is an initiative to tie together naval, joint, and national information grids to achieve unprecedented situational awareness and knowledge management...FORCENet will be central to commanding joint operations from the sea.”

Admiral Vern Clark, Chief of Naval Operations, Naval War College, June 12, 2002

¹⁸ Admiral Vern Clark, U.S. Navy, “Sea Power-21: Projecting Decisive Joint Capabilities”, *Proceedings*, (Oct 2002)

domain: real-time, near real-time and non-real-time. The last dimension is the operational level of command: tactical, operational, and strategic.

To enable NCW, FORCEnet must operate efficiently throughout this multidimensional information space, providing quick access to data, allowing common registration of data to speed processing, and supporting decision cycles within time requirements. FORCEnet must automate the processing of data into information and to knowledge, so that warfighters can then focus on decision making and planning, which are better suited tasks for humans to perform. FORCEnet must allow warfighters to reach out to data from a grid of netted sensors, and fuse it with federated information coming from non-real time reach back support capability. FORCEnet must provide wide spread situational awareness, so that commanders are able to more effectively execute command and control over their assigned forces.

Today's integrated combat and weapons systems are fundamentally isolated by their monolithic archaic tightly coupled hardware and software designs. For example, legacy sensors tend to work in classic stovepipes that do not share data outside of the domain of the host system. When data is shared in a netted environment, data registration, information subscription and timeliness are inconsistent across a diverse family of networks. Additionally, to share sensor data with joint and coalition forces requires layers of ancillary processes. The data must be filtered into a manageable condition and then posted onto another system that is networked across the battlespace. These processes add time latency. As the numbers and types of sensors continue to proliferate, the fidelity and volume of data to be evaluated about the battlespace grows exponentially. The end result is the sheer volume of sensor data inundates the Observe-Orient-Decide-Act (OODA) cycle, many times with data that is not relevant.

Open Architecture is the critical enabler in the modern computing environment that can ensure combat power through information superiority and decision superiority, because of its open internationally recognized standards, flexibility, adaptability and modularity. FORCEnet and GIG architecture designs leverage open standards to efficiently transport data across the networks without accumulating latency at the interfaces. Automating the creation of knowledge and providing web-based information dissemination management processes, FORCEnet provides a means to dramatically reduce the volume of information to the warrior and improve shared awareness with joint and coalition units. As an example, Operation Iraqi Freedom and the Global War On Terrorism demonstrated how adversary tactics create emerging requirements to transport and process information in new ways. Naval units had to share digital pictures taken during maritime interdiction operations with commanders in theater and other agencies like CIA, FBI, and Homeland Security. OA's extensible architecture supports plug-and-play interoperability of new and existing sensors and combat systems, thereby allowing warfighters to reorganize to best perform their mission.

Web Based Command and Control.

Figure 9 shows the Operational Vision for the Global Information Grid and FORCEnet. Web basing is the command and control environment that the GIG provides to manage information and knowledge. The drivers in the web environment are:

- Bandwidth
- Detect, Control, and Engage in a Web Based C2 Environment.
- Human to System Integration

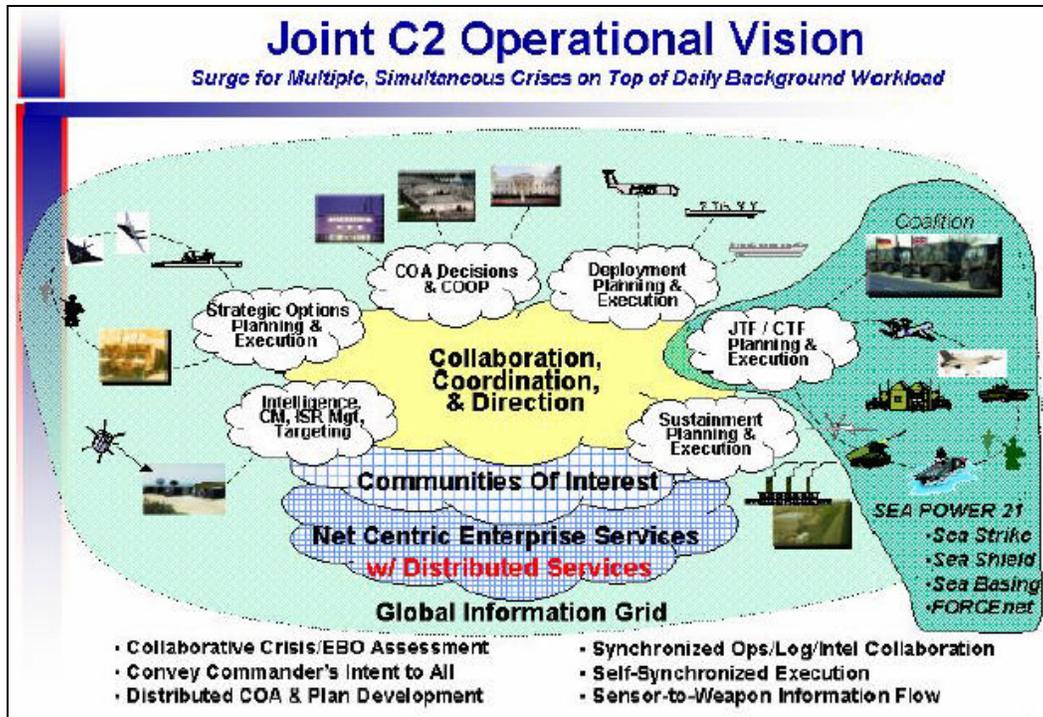


Figure 9 Joint Command and Control Operational Vision

Bandwidth

Prior to the introduction of the web-based environment, traditional information networks such as radio circuits, telephones systems and discreet data linkages were individually isolated and tailored to their specific needs. Modern information structure that includes web-basing consolidates information paths to a broadband environment. As an example, bundling the satellite circuits together with the digital data networks and satellite data links reduces the number of physical satellite connections and antennas required. However, this consolidation establishes a new set of challenges in apportionment, efficiency limited by the boundary of physics and resources.

The solutions to the bandwidth challenge are in techniques such as dynamic reallocation, which allow for more efficient use of the total bandwidth allocated. Using open standards and formats like Voice Over IP (VOIP), in a digital data environment eliminates dedicated bandwidth requirements characteristic of older analog circuits.

Detect, Control, and Engage in a Web Based C2 Environment

Web-centric warfighting presents the means to achieve Battlespace dominance, as a result of information superiority supporting decision superiority. Leveraged by network centric technology, whereby our forces operate inside our adversaries OODA execution cycles, the most critical warfighting processes of detection, control and engagement are optimized. The web based C2 environment allows for distributed asynchronous command and control while providing the means to synchronize multiple disparate actions based on superior information about the battlespace environment, enemy course of action, and disposition of own forces and logistics tail.

Web-based technologies let a netted sensor grid seek out the warfighter throughout the battlespace and notify them of detections of the enemy. Internet Protocols provide broadcast

addresses, whereby information may be pushed out to an unknown number of recipients by only sending the data once, termed multicast. This commercially available technique is used to push information like stock market tickers and news feeds. Multicast really helps the efficiency of the network by reducing the volume of data, since the broadcaster does not have to make a connection with each receiver and send the same data multiple times. The sensor grid can push both raw sensor data to promote horizontal fusion processes and notifications of activity to support an indications and warning network.

Employing collaborative web tools, like Chat, Knowledge Web (KWEB) and Sametime™, warfighters today are realizing the huge benefits that web centric warfighting provides for controlling engagements within the battlespace. Chat, one of the main web-based C2 tools, is more prevalent at the watch station than a radio handset. Its benefits include extended ranges using satellite with better connections than voice, information persistence on the display avoiding having to repeat communications, and integration with other tools on the computer desktop. Chat is one of the simplest tools to use and as such saw extensive use during Operations Enduring Freedom and Iraqi Freedom.

Knowledge management tools like KWEB simplify the workload by allowing the warfighter to concentrate on important issues and not having to sort through the mountains of mundane data. It promotes wide spread shared awareness while evening out bandwidth demands. With a few clicks, warfighters of various disciplines have access to both status and plans information. Monitoring KWEB, Intelligence, Logistics, Legal and Planning staffs can simultaneously begin to assess changing situations and develop courses of action to support the commanders' decision making process.

Other collaborative tools like Sametime™, email and VTC also support the planning and decision making cycle. They allow commanders and their staffs to focus on the hard points to develop and decide on new courses of action. These tools also allow more support staff to monitor the thought process behind the planning and decision making, allowing them to better the process.

Web-based tools promote more decisive engagements. Sharing the same sensor data that has a common registration speeds the transition from detection to engagement by the weapon system. Web-basing allows fusion of knowledge and information from multiple sources, i.e., sensor, intelligence, weapons system, and knowledge, etc., into Common Operational Pictures creating a higher foundation for decision making and reducing the fog of war. Quicker detection notifications allow more time to ascertain the threat and develop courses of action, and then support better decisions based on more complete knowledge of the situation.

Since each unit's commander has better situational awareness through access to the sensor grid and shared knowledge, and better access to the campaign plan and his commander's intent they can make better decisions locally to achieve their mission and support the overall objectives.

Human Systems Integration Challenges

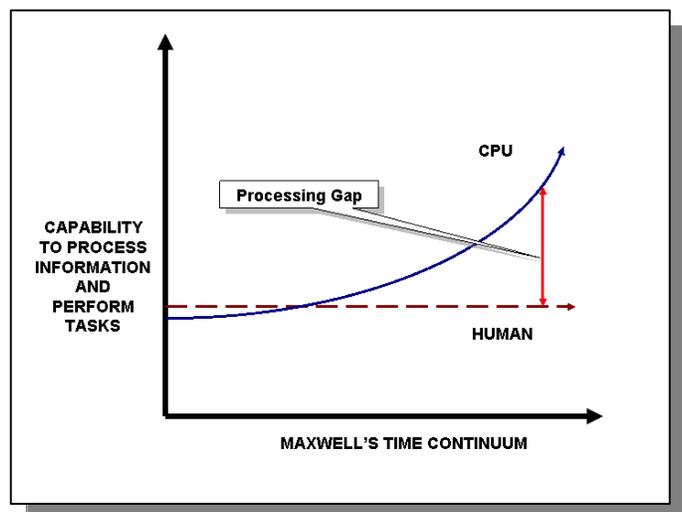
In addition to the problem of uncertainty, a commander will always have to deal with the problem of time. Gathering and processing information takes time. In military operations, time is a precious commodity for three reasons. First, the information we gather, and the knowledge we derive from it, is perishable; as we take the time to collect new information, previously collected information may

become obsolete. Second, since war is a contest between opposing wills, time itself is a resource shared by both sides. While we are trying to gather information about a particular situation, the enemy already may be taking new actions-and changing the situation in the process. Third, the rapid tempo of modern operations limits the amount of information that the commander can gather and process before having to make another decision. Command and control thus becomes a race against time. The more time a commander spends processing information trying to reduce uncertainty, the slower his tempo of operations becomes. If taken to extreme, the pursuit of more and more information can lead to operational paralysis. A naval commander, therefore, must ensure that his decision making and execution are swift-at least swifter than those of his adversary.

Naval Doctrine Publication (NDP) 6, Naval Command and Control

Challenges of Moore's Law

Technology follows an empirical rule called Moore's Law¹⁹: The density of transistors on a chip will double every 12 to 18 months, which is usually accompanied by the computer chips' speed doubling in that same time frame. Information inundation accelerates. The problem is that our nation's warfighter's ability to process information has not seen any improvements. Their training and understanding of the equipment and Tactics, Techniques and Procedures (TTP) improves, but this does not help them cognate any faster or more. Figure shows that the processing gap between humans and computers continues



to grow as computers get more complex. Human Factors Specialists and Human Systems Engineers recognized this problem and have devoted extensive study and task analysis to address this issue, now recognized under the term Human-System Integration (HSI).

One way to realize improvements in human performance has been to reduce the amount of time that they spend doing repetitive tasks. Software automation tools, called agents, have been developed to perform administrative tasks, leaving the cognitive and decision making task to the human. The agents can be trained to seek out information that is gathered routinely, and then notify the warrior and post it into a knowledge store. Smart agents will be the next generation tools that will have the ability to fuse information together and to create new searches based on the information found.

Another way is to optimize the Human Systems Interface. Ergonomics looks for ways to reduce the stress of performing tasks on the Human. They reduce the number of clicks, or the distance the mouse or track ball has to travel to accomplish the most common tasks, that are the ones that have not already been automated. Additionally, the equipment is made to better fit the human form and to minimize fatigue when performing repetitive manual tasks.

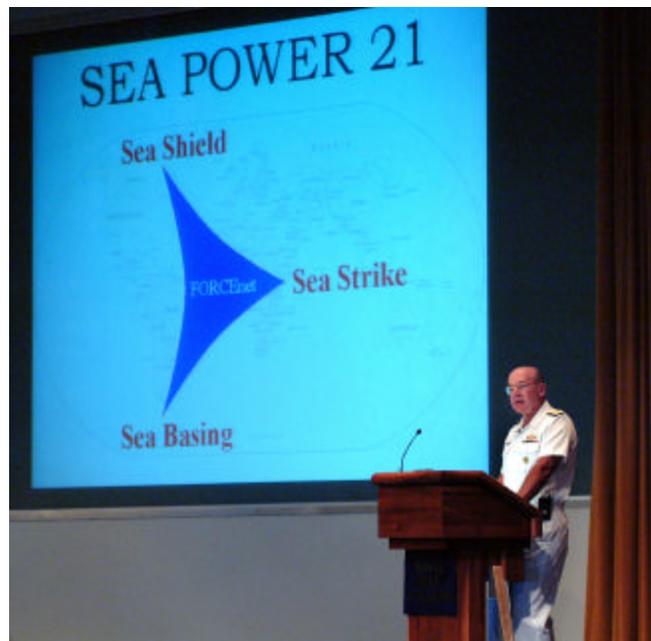
¹⁹ Gordon Moore, "Cramming More Components Onto Integrated Circuits," *Electronics* (Volume 38, Number 8), April 19, 114-7

Driving the HSI effort has been the shortfalls of legacy Combat System's design to optimally support the warfighter in their emergent tasks from the information revolution. Chatting, emailing and browsing just weren't part of the design equation. Each system was optimized for the human warrior to perform specific tasks, but in aggregate they induce stress and fatigue. Engineers have done superb jobs to co-locate as much as possible those systems that are used to perform groups of tasks, but the warfighter must still switch between systems to perform their jobs. To reduce the footprint of the warfighter's workstation, the use of Keyboard, Video and Mouse (KVM) switches have been incorporated to allow sharing of equipment between systems that employ standard PC equipment displays. The use of KVM switches, while a step in the right direction, did not anticipate the need to move information between system, like cutting and pasting pictures and text between systems like GCCS-M, KWEB, Chat and email.

Open Architecture enables improved HSI. Using open web standards, warfighters tailor their workstations to perform their usual tasks, like operating radars, weapons systems, reading message traffic, and monitoring the common operational picture, that which they must perform routinely. Then when unique events occur, they can use the network to gain access to additional web-based information and services as required, like researching a SCONUM, identifying an unknown vessel or aircraft, or recommending a new scheme of maneuver to the commander using a collaborative tool. Instead of having multiple consoles and displays that display only one kind of information on each, the warfighter can compose their console on two or three displays that are tailored to their needs. They warfighter no longer will have to sub-optimize to get the job done; and will be more confident in their work product.

Equipping the Warrior vs. Manning the Equipment

It has been understood that Human System Integration must improve if our combat forces are to achieve Information Superiority and maintain combat edge. Driving home this new direction in acquisition, CNO says that we will focus on 'equipping the warrior' vice 'manning the equipment'. Our people give us the advantage in combat, and human systems integration makes them more effective at their jobs. Without it our adversaries will use off the shelf technology to gain the asymmetric advantage while our people become fatigued from performing numerous tasks processing information with sub-optimized workstations. It truly is a new era in Quality of Service for our sailors and Open Architecture leads the way.



How Do We Get There?

The Navy faces a daunting task in transforming its high fidelity sensor, command and decision, and weapon fire control software based capabilities into Open Architecture. It is the necessary pre-condition to achieving Network-Centric capability. Once the OA pre-condition is achieved, the process must then be able to support the incorporation of the essential foundation capabilities of network-centric operations. The “Open Architecture Transformation Roadmap” and the “Rapid Capability Insertion Process/Advanced Processor Build (RCIP/APB)” are the essential muscle movers in achieving this network-centricity and maintaining them through the next decade.

The Open Architecture Roadmap

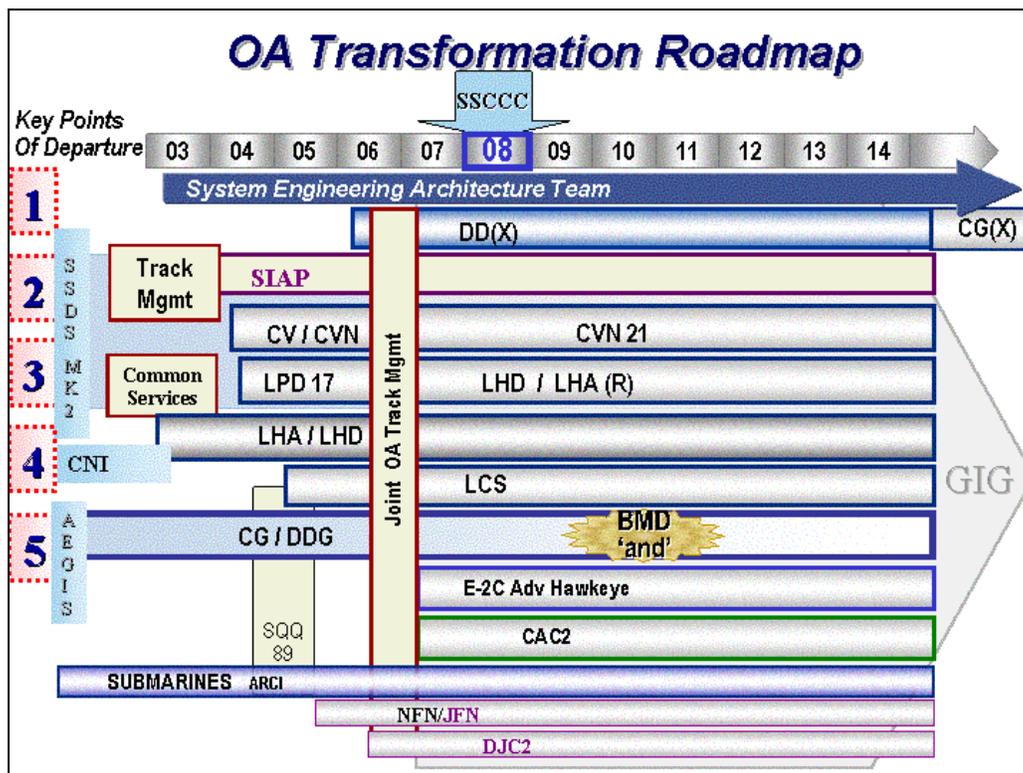


Figure 10 Open Architecture Transformation Roadmap

The Navy’s Open Architecture Transformation Roadmap (Figure 10) is targeted to achieve open architecture software design conditions to category 3 (uncoupling of software from hardware reliance) for capital ships and aircraft by Fiscal Year (FY) 2008. It is established on five major foundation elements. The first maximizes the development investment in future ship classes and aircraft presently in development. The centerpiece of this family of ships is DD(X), however, it also includes LCS, CVN21, and the Advanced Hawkeye (AHE) Air Early Warning Aircraft. The second element establishes a path in current programs that will shape the development of those common service and applications, like joint track management, navigation, time, and command and control elements that will go into what is being described is the “Single Scalable Core Combat Capability (SSCCC).” The development and acquisition programs of record targeted are Cooperative Engagement Concept (CEC) and Common Network Interface (CNI). The third element recognizes there is a relationship between the objective OAF, which defines the software capability organization in the future, platform family and in service

integrated warfare systems of current ships and aircraft. The program of record, providing the beginning of the OAF migration, is SSDS MK2. The fourth element recognizes that the littoral combat ship (LCS) will precede the future family of ships and becomes the ideal risk mitigation opportunity in a robust operational environment. Finally, the fifth element realizes the backbone combat capability of the fleet for the next 40 years is resident in the family of AEGIS IWS baselines in the TICONDEROGA and ARLEIGH BURKE Class ships. They have critical software based capabilities in both sensors and weapons control that must be migrated to modern software architectures that support emerging and urgent capabilities, like ballistic missile defense, integrated fire control, and enhanced joint tactical interoperability. These elements, represented in Figure 10, will be discussed in some detail.

Element 1: Harnessing Future Platform Development

The family of future ships and aircraft provide a significant opportunity for the Navy to synergize several significant realities in achieving network-centric combat capability. First, there is significant development investment focused on developing these platform's software based capabilities in modern, modular, software and hardware conditions. DD(X) specifically, is uniquely positioned in its development effort to produce many of the modern software application based capabilities on a timeline that is in step with the OA Transformation Roadmap effort. LCS and AHE are further along in their developments, but still are well positioned to influence OAF boundary establishment and provide risk mitigation opportunities in their fielding plans. Second, they are each pursuing advanced concepts, like Total Ship Computing Environment (TSCE) and modular capabilities that provide opportunities for incorporation across the force. DD(X), again, is in the van of these shaping concepts with its TSCE.

DD(X) is on a development path that has the first ship contract award in FY-05, launching in FY-09, and delivery to the U.S. Navy in FY-13. It is not only an innovation driver in ship operations; it is also blazing new trails in development and ship acquisition paradigms. Characteristic of these new concepts is the procurement of the first ship in research and development funds (RDTE) and advanced concepts in software-based capabilities, leading to greatly reduced crew sizes and automation of shipboard functions. Overlaying the development timeline required to meet DD(X) delivery with the OA Transformation Roadmap establishes a relationship that provides early off ramps for software applications for use in migrating in-service ships and aircraft, which, if properly managed, provides significant risk reduction to DD(X) fielding as well as leveraging DD(X) development funding for software capabilities resident in the SSCC for fleet-wide use.

However, in DD(X)'s early program development, it retained some traditional views that have become problematic as the Navy embraces the revolution from "platform-centric" to "network-centric" combat capabilities. Specifically, sensor, command and control, and weapons control functions were being optimized for platform relationships without sufficient sensitivity for many of the basic underpinnings of joint interoperability and network-centric drivers in sensor netting and integrated fire control. These underpinnings are key influences that "all" platform nodes in the net-centric architecture must embrace to provide coherent capabilities. It has required some reshaping of the software-based capability efforts in the DDX Program.

The DD(X) Total Ship Computing Environment (TSCE) influence on determining the objective organization of the OA functional architecture is significant. That influence works back toward the starting functional architecture, largely influenced by SSDS MK2, to provide a

migratory path that in service ships and aircraft can “on ramp” at points that make sense in their individual pre-planned product improvement (P3I) plans.

Element 2: Joint Track Management – Key to Interoperability

First, causing initial alignments at the center of the sensor, C2, and fire control relationship to the top level OA functional architecture, is a must. It is not only essential for OA migration, it is the one portion of the functional allocation of software based capabilities that is critical to joint interoperability and the establishment of conditions for “common re-use applications” or the SSCCC. Thus, the second element of the Transformation Roadmap is opening the common services required to register data and minimally processed information to the network, and the applications that provide the capabilities to develop and manage vehicular track information in what the Navy defines as the Joint Track Manager (JTM). The Navy has embarked on an aggressive partnership with the Joint Single Integrated Air Picture (SIAP) Systems Engineering Organization (JSSEO) to develop an Integrated Architecture Behavior Model (IABM) defining the critical design elements to be incorporated in the applications of “common services” and vehicular track establishment, management, and identification. This behavior model is being developed in a format which will support conformance by all joint information systems in the network-centric environment to establish and maintain a single coherent tactical command and control environment.

Element 3: Establishing OA Functional Architecture Migration

This element supports the essential uncoupling of the hardware to software reliance and furthering the migration of software boundaries in C2 to align to the OA functional architecture. It is being executed initially by “re-reporting” the C2 and self-defense weapons capabilities resident in SSDS MK2 to OA Category 3. SSDS MK2 is the integrated backbone of choice for this migration for the hardware conditions it provides, as previously described, and most importantly because it’s C2 capability is already organized in a modern functional architecture condition that includes its reliance on a largely single, fully integrated track management application bundle, used by the Cooperative Engagement Processor (CEP) of CEC. It not only migrates the SSDS MK2 configured platforms to OA Category 3, but prepares it to receive the JTM as the first element of the OA category 4 compliant SSCCC which places these ships in strict compliance with joint interoperability requirements in the tactical battle-space. It is also intended that the C2 software applications will become the basis for displacing the non-compliant “Command and Decision” software in AEGIS Baseline 7.

Element 4: Transformation Risk Mitigation

Future ship participation in the OA Transformation Roadmap re-surfaces here as the fourth element, in the form of the Littoral Combat Ship (LCS). The Navy’s approach to LCS is revolution for several factors, including, among other things, its rapid development schedule and modularity. It becomes an inviting participant in the OA transformation effort, both in risk mitigation in bridging software capability migration between DD(X) and in-service platforms and in the opportunity to field an OA compliant integrated combat capability in advance of huge challenges presented by DD(X), CVN21, and CG(X). Because of it’s rapid development and fielding schedule, LCS must push aggressively into the OA COTS environment, purchase significant capabilities “off the shelf” from defense contractors, use commercial IT technology, and leverage some existing DoD owned capabilities. It’s “mission module” design will drive many of the OA hardware conditions that will be useful in both forward and backward fit efforts.

Finally, LCS Flight 1, planned for delivery in FY-09 will debut the first OAFAs complaint capability.

Element 5: Establishing the Conditions for Future Capabilities

The fifth and final element of the OA Transformation Roadmap addresses the essential migration of the AEGIS Integrated Combat System (IWS). The initial challenge here is getting the AN/SPY-1 (series) radar into OA Category 3 that will allow for immediate improvements to support near term warfare capability demands, the most pressing of these being littoral operations and ballistic missile defense. The tightly coupled relationship of the radar control computer program (RCCP) with its



customized “niche” COTS computing plant has seamless incorporation of these improvements unachievable because of its maxed out processing capacity. Uncoupling this software to hardware design reliance will put the radar computing plant into a condition where it can be scalable to the processing requirement of these added capabilities.

The present condition of the AEGIS IWS presents some additional challenges as well as some opportunities. The challenge in the C2 portion of AEGIS is two fold. First, its adjunct relationship with CEC is problematic in the preparation for incorporating the SSCCC into the IWS. The SSCCC will provide both the JTM developed in thread 2 of the Roadmap as well as commence the migration to the OA Functional Architecture. Secondly, AEGIS incorporated a concept called the “Common Display Kernel” (CDK) into the AEGIS Display System (ADS). It is problematic in migrating the ADS as well as defining the requirements for display in the SSCCC.

The third challenge of the AEGIS IWS is getting the weapons control capabilities resident in the Weapons Control System (WCS) portion of the IWS into a condition that would not only uncouple it from its “niche” COTS processing environment, but would also be reusable in any platform expected to shoot the area air defense missile family resident in Standard Missile (SM). The Navy presently expects to incorporate the SM2 in DD(X) and desires to retain the option of migrating the SM3 and SM6 versions of this missile into CG(X). It means that the weapons control applications that support this missile family in AEGIS must be modernized into OA Category 4 to support re-use in these future ships.

To achieve these objectives, the AEGIS 3 Spiral migration plan was developed and is depicted in Figure 11. This plan provides detailed execution under the auspices of the CG Modernization Program. Picked to mitigate risks that have long made OA migration in the new construction DDG program untenable, the CG Modernization effort is uniquely suited by both schedule and improvement objective to be the centerpiece of this effort.

The first spiral will open the AN/SPY-1B radar RCCP by the first ship to enter CG Modernization in FY-06. The second spiral is targeted to achieve two additional objectives. Primarily, it will build on the work done in the SPY-1B radar to get the destroyer’s SPY-1D/V

radar into the OA condition. Secondly, it will re-organize and open the ADS to remove CDK and establish an OA framework for display, which may be reused across the force. This spiral will be introduced via the DDG “new construction” program with DDG-103 and will be incorporated in the CG’s by the 4th ship in the modernization program in FY-08. The third spiral will open the weapons control software required for standard missile as well as other weapon interfaces. It will also be introduced via the CG Modernization program in the 4th ship. All of these capabilities will be migrated back to all AEGIS Baseline 7 ships via ordnance alteration (ORDALT) at their first “obsolescence” computing plant upgrade.

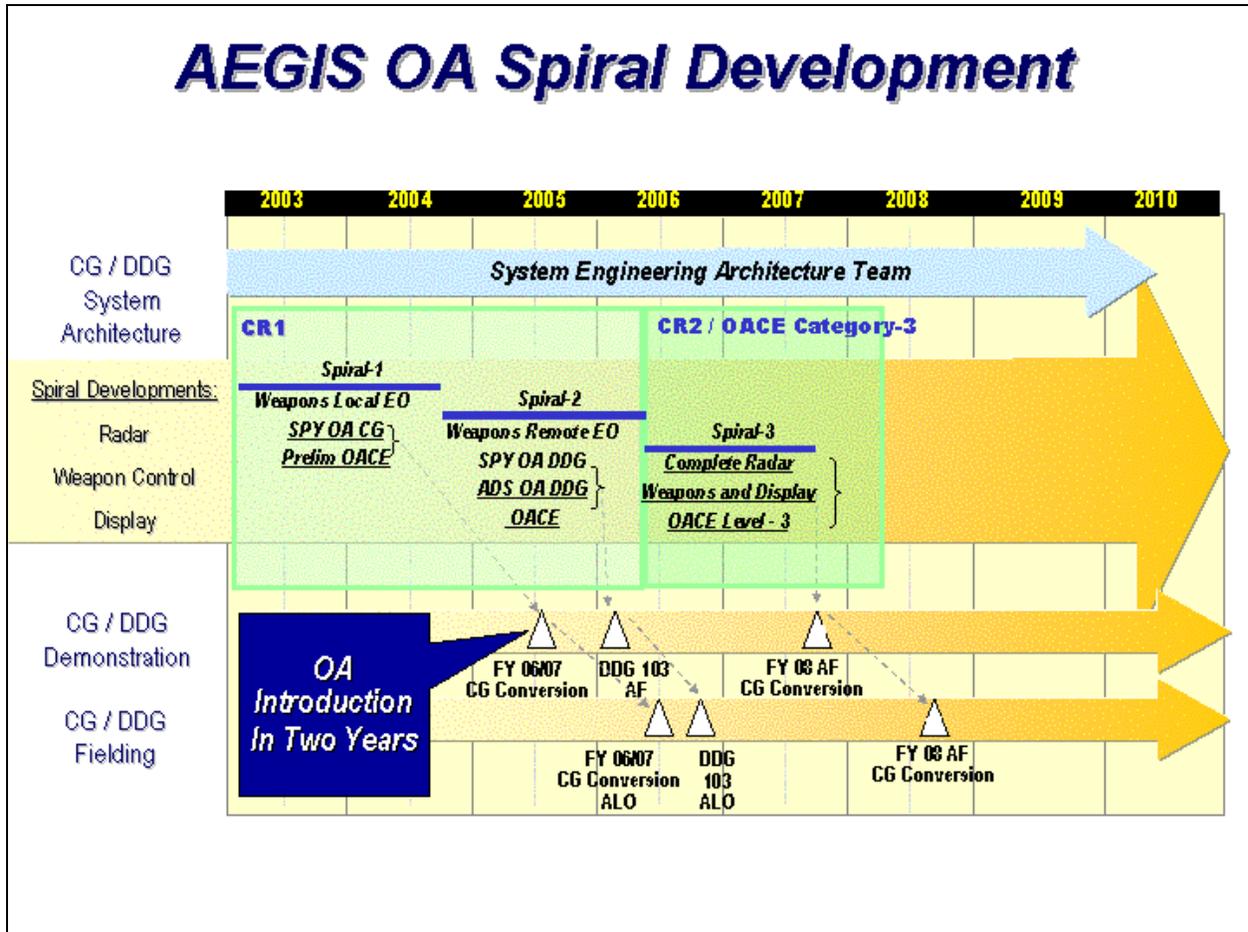


Figure 11 AEGIS Spiral Developments

Rapid Capability Insertion Process/Advanced Processor Build

The Open Architecture Transformation Roadmap was carefully crafted to provide the specific OA conditions needed for the addition of future software based capabilities. As such it was limited to only those tasks that were essential and it has a definite end point in FY-08. It did not provide for significant war-fighting improvements beyond those provided by the joint interoperability characteristics resident within the initial deployment of the SSCCC. Once in this condition however, a sustainable process for continuing capability insertion, based on priorities established by the Navy's Mission Capabilities Package (MCP) effort and the immediate requirements forwarded by the Fleet is essential. Equally important, the process must provide for the necessary technology hardware obsolescence updates and "pace of technology" driven software design improvements that are characteristic of the OA COTS computing environment. The Rapid Technology Insertion Process (RCIP/APB) has been established to meet these needs.

The RCIP/APB concept is driven by five significant influences. They are:

Driver 1: Pace of Technology. The "pace of technology" is shaped primarily by the speed in which processing power has been compounded over recent years shown in Figure 12. Known principally as "Moore's Law," it surmises that computer processor speeds will continue to double about every 18 months. This thesis drives both affordability and sustainability of computing environment hardware, as well as impacts peripherals, cable layer technology, and software design. Recent experience with the "Moore's Law" impact on major computing environment manufacturers reveals that, on average, they maintain supportability of their major products only for about three years. The Navy has been successful in extending this obsolescence trend another year by organizing repair part lifetime buys or "buy outs." It is this driver that has been used to establish a goal in RCIP/APB of replacing major elements of the COTS computing environment on major warfare platforms approximately every four years.

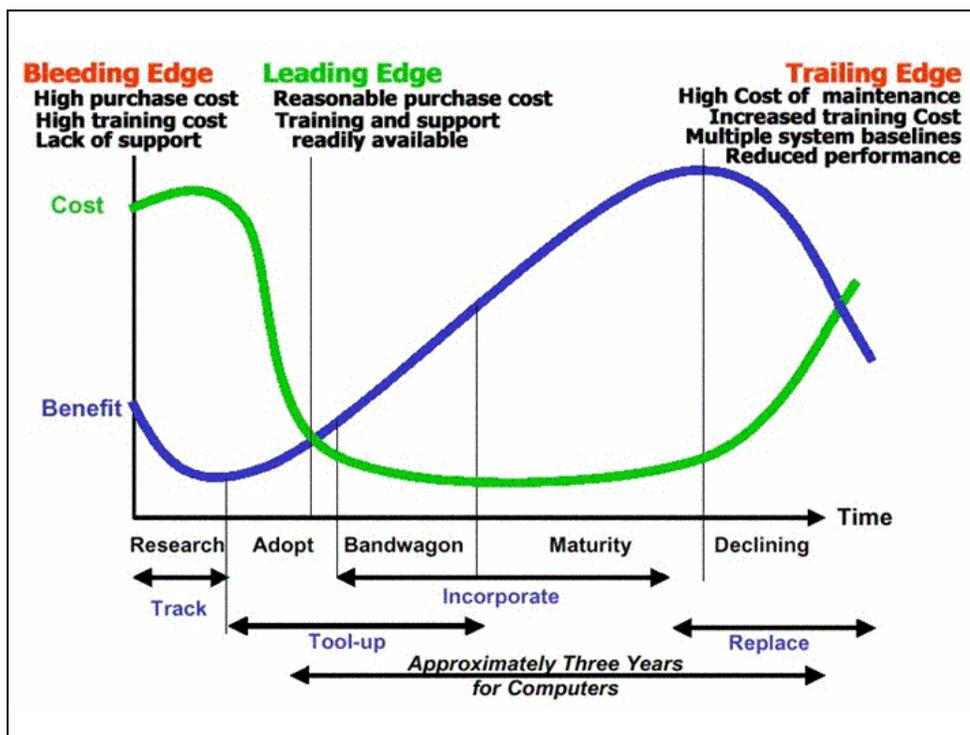


Figure 12 Technology Lifecycles

Driver 2: Naval Capabilities Process (NCP)/Mission Capabilities Package (MCP).

The next most significant influence on RCIP/APB is the Navy's MCP Process, used by senior leadership to generate an understanding of war-fighting requirements based on future battle-space driven capabilities assessments. The MCP process uses a variety of war gaming and warfare system modeling techniques to get at the investment decisions required for the future. It is executed on a cycle that provides decision opportunities annually, aligned to the federal budget submission. It is the principle means for identifying warfare improvement options for inclusion in the RCIP/APB cycle.

Driver 3: Federal Planning, Programming, Budgeting, and Execution (PPBE). The PPBE process is the third driver for establishing time boxes in which to organize improvements. The policy guidelines shaping PPBE require the budget to be shaped in two-year blocks with an attendant follow on 4-year target investment; called the "Future Years Defense Plan"(FYDP). The net effect of PPBE is that major shifts of investment can only occur on a two-year cycle.

Driver 4: Systems Engineering Effort. A fourth driver is the systems and software engineering it takes to get new capabilities integrated into the OA functional architecture. The integrated backbones of capital combatants and aircraft are challenging environments, not only because of the complexity and magnitude of their software relationships, but also because of the quality of service demands of high-end weapon systems, time critical actions in the supported battle-space, and challenging data structures. In short, a methodical systems engineering (SE) approach remains critical. Experience in the level of effort effective SE takes defines 24 months as about as quickly new software-based capabilities can be properly engineered, tested and fielded.

Driver 5: Small Business Innovation Research (SBIR). Finally, the Submarine Warfare Community recognized the requirement to get acoustic capabilities migrated to modern software/hardware conditions some time ago and in the process were able to harness the power of SBIR contracts to redefine the development effort required for new capabilities. This effort, called the Acoustic Rapid Capabilities Improvement (ARCI) program, provided an early model relevant to the challenges of establishing RCIP/APB.

The net result of the convergence of all of these drivers was the establishment of RCIP/APB with the following characteristics. Hardware upgrades and improvements will be established on a four-year pattern. The actual upgrade of the computing environment on a given ship will be dependent on when it was last subjected to a hardware upgrade, adjusted to its next major industrial availability. Software improvements will be targeted for a two-year cycle. The software-based warfighting improvements will be targeted by prioritizing capability needs identified by the MCP process or fleet input and the maturity of the software developed to support it.

Application of the RCIP/APB across the many "platform nodes" of the network-centric environment is no small task. Each of these "nodes" contributes capabilities that are required for the collective success of the battle forces in the net-centric battlefield as well as unique contributions specifically attributed to their character. For example, an AEGIS Cruiser provides sensor data and information that contributes to the overall situational awareness of a collection of command and control points across the battle-space and it uniquely provides both operational air defense command and control as well platform specific area air defense weapons employment. An E-2 Advanced Early Warning "Hawkeye" aircraft also contributes to the sensor grid of the battle space as well as providing platform specific tactical control of fighter and attack aircraft

and in both air defense and strike missions. Similar examples can be made regarding CVN operational command and control contributions, submarine undersea picture contributions, and the sensor contributions of a host of manned and unmanned air, surface and sub-surface vehicles. On the whole, RCIP/APB must be tailored to each of these major nodes to meet the tasking assigned; that of organizing the continuous software based capability improvements required for their specific mission contributions. RCIP/APB is powered by the information backbones that emerge from the OA transformation roadmap. They are:

- SSDS MK2 for CVN/LHD/LSD
- AEGIS baseline 7 OA for CG/DDG
- CNI enabled ACDS for LHD/LHA

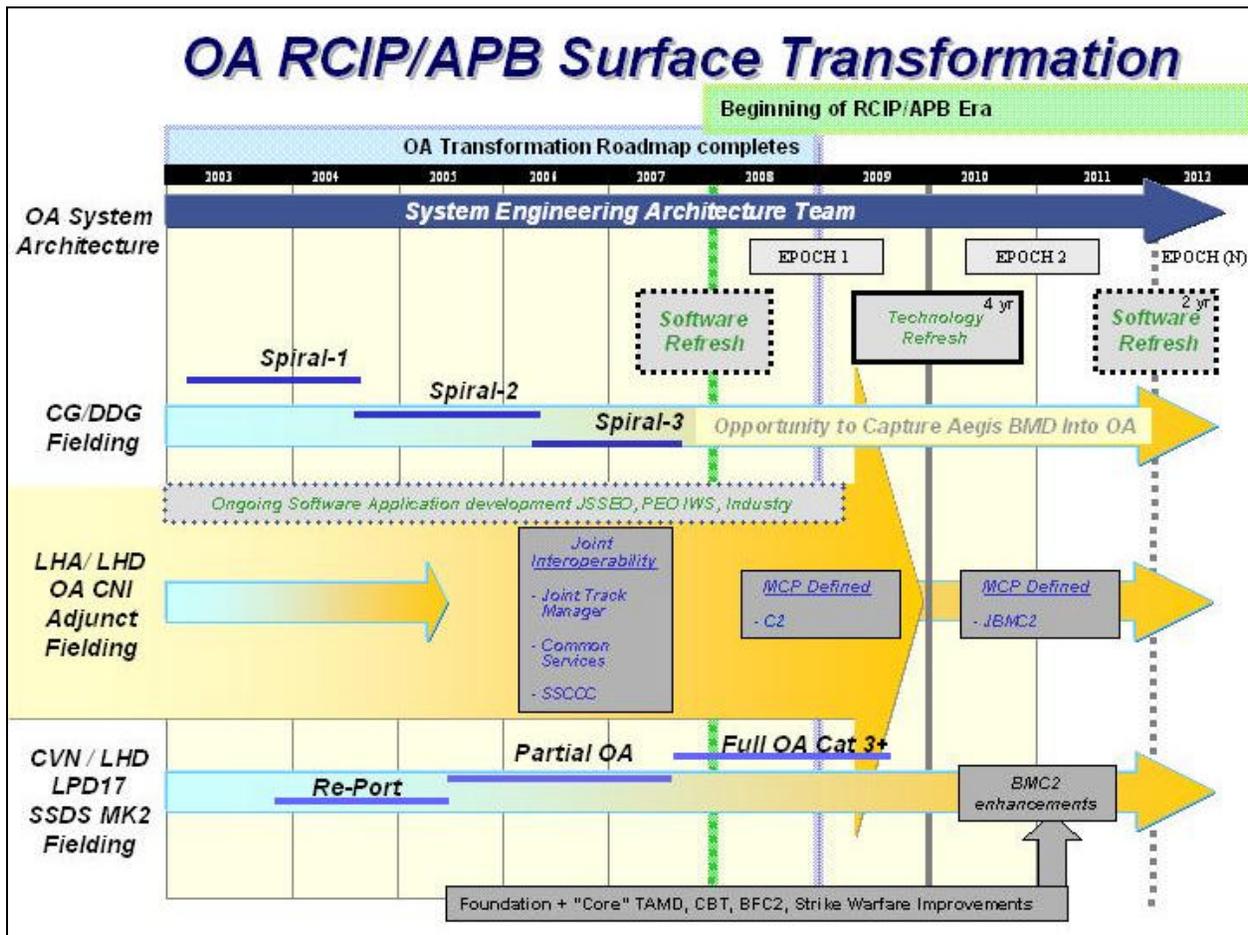


Figure 13 OA RCIP/APB Surface Transformations

SSDS MK2 for CVN/LHD/LSD

At the heart of the Navy's Sea Power 21²⁰ articulated concept of maritime power and force application are the Carrier Strike Groups (CSG) and Expeditionary Strike Groups (ESG). These groups are formed around the platform nodes of the "big deck" aircraft carriers (CVN) and helicopter assault ships (LHA/LHD). The CVN OA transformation follows the migration of SSDS MK2 to OA as depicted in. It is specifically tailored to mitigate and manage the

²⁰ Admiral Vern Clark

technology obsolescence needs of the SSDS MK2 COTS computing environment as well as support for the insertion of critical interoperability improvements being forwarded by the IABM design of the SIAP SE. Follow on epochs show themes anticipated by the Navy's MCP process and some of the characteristics that support them.

There are three software based capability improvements that could be proposed for integration into the SSDS OA backbone. The process of selecting which of these specific solutions is based on a prioritization by the warrior of their importance in meeting his/her needs and application of resources via the PPBE process. The end result is intended to be a bi-annual integration effort that will package improvements in these two-year epochs.

AEGIS Baseline 7 OA for CG/DDG

The same process applied to the capital ships of the surface force is shown in AEGIS Spiral Development Figure 11. The AEGIS cruiser and destroyer force represents a significant portion of the CSG and ESG combat power for the next 40 years. These ships are vested in the software-based capabilities of the AEGIS Baseline 7 IWS and their "open" conditions are



established by leveraging the Baseline 7 migration via the OA Transformation Roadmap. The command and control portion of the AEGIS system was specifically ignored during the transformation to give the joint interoperability conditions included in the SIAP IABM time to reach maturity. The first epoch of RCIP/APB for these ships incorporates the IABM design as its first theme, and as is essential, matches the first epoch of the CSG and ESG Flag ships. This first epoch is a good example of the criticality of constant synergy of the shared capabilities resident in the SSCCC across all of the nodes of the network-centric environment. Figure 11 drills down into the software resident capabilities forwarded by the POM-06 Theater Air and Missile Defense (TBMD) MCP that established ballistic missile defense (BMD) as a significant gap in capabilities. The themes for the next two epochs deal as priority the capabilities

required to fill those gaps. These themes are excellent examples of where RCIP/APB must be tailored to meet the needs of unique contributions of platforms as well as shared needs. Many of the applications that must be developed to support C2 in the CGs and DDGs, are also applicable for integration into the CVNs and LHD/LHAs as situational awareness information for operational commanders.

CNI Enabled ACDS for LHA/LHD

Migrating the LHA/LHD combat system backbone migration follows the step approach of CNI, as previously described and is therefore, seamless in shifting to the RCIP/APB approach. The epochs of improvements mirror those planned for the CVNs; however, because the computing plant was not completely replaced, but rather upgraded in increments, the hardware improvements for the near term would be included with each two-year epoch. Figure 13 depicts this model.

As future ships and platforms, like DDX, LCS, and CVN21 come on line, they too will require tailored RCIP/APB based plans to keep them on pace with evolving capability requirements. These ships have added drivers and concepts that must be incorporated as well. First, they are distinctly different in design than in-service capabilities. Concepts of minimal manning, total ship computing environments, and modular flexibility will significantly influence the character of their tailored RCIP/APB plans.

It is also essential to expand the application of RCIP/APB to airborne nodes like the Advance Hawkeye (AHE) AEW aircraft and, as significantly, the high performance fighter and attack aircraft. Most of these platforms are in the latter stages of development or at the beginning of their fielding. Most of them have been designed with significant attributes of Open Architecture. They are vital contributors to the network-centric environment and must be evolved in step with the many other elements. Ultimately, RCIP/APB is the paradigm of future modernization.



Conclusion

The assertion in the introduction of this paper was that NCW is the essential condition required to meet the challenges expected on the littoral and inland battlespace encountered today and into the future. The breakthroughs in computing technology that drove the character of the battlespace also brought profound changes in opportunities and limitations facing the Defense Department in attempting to develop and field NCW. Open Systems or OA is at the heart of those opportunities. The architectural constructs of the GIG and FORCEnet are the frameworks within which the OA based opportunities must be applied.

Supporting this general conclusion, are some specific take aways. They are:

- Network Centric capabilities are essential to meeting the requirements of the littoral and inland battlespace in which maritime forces must operate for the foreseeable future.
- The Defense Department no longer leads or even significantly influences developments in information technology.
- The commercial, non-DoD, market place drives the pace and character of information technology and it has embraced OA.
- Key tenants of the GIG and FORCEnet, such as web based command and control, information dissemination management, and modern human systems integration depend on OA in COTS based products.

In summary, the net effect of these take aways is that the Defense Department has no choice in the matter of moving its archaic, monolithic, main-framed, integrated combat systems into OA. The commercial market place made that decision for the department in the early 1990's. The DoD embraced the decision when it shifted much of its capabilities out of military standard computing environments and into COTS hardware. Unfortunately, it didn't move to embrace the modern software structures, companion to COTS and, as such, retains much of its capabilities in archaic conditions. The only decision for the DoD remaining is when it will make remaining shift OA software designs.

"The need for military transformation was clear before the conflict in Afghanistan, and before September the 11th...What's different today is our sense of urgency."

President George W. Bush, Remarks at The Citadel, December 11, 2001

Fortunately, most of the departments significant IT based planning and operational command and control systems were developed in an IP based technical condition. Systems like Global Command and Control System (GCCS) have evolved largely into open standards and are compliant to at least OA Category 3 today. These systems represent an overwhelming portion of the DoD's software based capabilities, in relation to IWS systems. Transforming the IWS systems is both essential to meeting the operational requirements of GIG and FORCEnet, as well as an imperative in rescuing the Department out from under its very expensive and unique IWS supporting infrastructure. Executing the OA Transformation Roadmap will place the Navy's family of IWS on that path, using the financial resources already programmed to support them.

Lastly, OA provides an entirely new dynamic in building, improving, and maintaining software based IWS. It provides the modularity, flexibility, interoperability, and tailorable

options required to meet the Department's warfare capability needs in modern technology. However, it requires a new modernization paradigm. RCIP/APB is the model that provides the framework for the future paradigm. RCIP/APB must be supported by an investment framework that matches its flexibility, deals with the reality of the pace of COTS obsolescence, and can be properly programmed in the rigid policies of the Federal Governments PPBE process.

It is time to embrace the power of OA and move aggressively to align DoD investment, acquisition policy, and budget execution to support it.



"Good ideas are not adopted automatically; they must be driven into practice with courageous impatience."

ADM Hyman G. Rickover

Glossary

Abbreviations and Acronyms

A

ACDS – Advanced Combat Direction System
ADS – AEGIS Display System
AHE – Advanced Hawkeye
APB - Advanced Processor Build
ARCI – Acoustic Rapid Capabilities Improvement
ASCM - Anti-Ship Cruise Missile
ASD - Assistant Secretary of Defense
ATP – Allied Tactical Signal Publication

B

BMD – Ballistic Missile Defense

C

C&D – Command and Decision
C2 - Command and Control
C4I - Command, Control, Communications, Computers and Intelligence
C4ISP - Command, Control, Communications, Computers and Intelligence Support Plan
C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CDK – Common Display Kernel
CEC - Cooperative Engagement Capability
CEP – Cooperative Engagement Processor
CID - Combat Identification
CJCS - Chairman of the Joint Chiefs of Staff
CJCSI - Chairman of the Joint Chiefs of Staff Instruction
CNI – Common Network Interface
COP - Common Operational Picture
COTS - Commercial Off-The-Shelf
CRD - Capstone Requirements Document
CSG - Carrier Strike Group

CVN - Multipurpose Aircraft Carrier, Nuclear
CVN 21 - The Future Multipurpose Aircraft Carrier Class

D

DII/COE - Defense Information Infrastructure/Common Operating Environment
DoD - Department of Defense
DoN - Department of the Navy

E

ESG – Expeditionary Strike Group
EW - Electronic Warfare

F

FY – Fiscal Year
FYDP – Future Years Defense Plan

G

GCCS-M - Global Command and Control System-Maritime
GIG - Global Information Grid

H

HSI - Human Systems Integration

I

IABM – Integrated Architecture Behavior Model
IDM - Information Dissemination Management
IER - Information Exchange Requirement
IFC – Integrated Fire Control
IP – Internet Protocol

ISR - Intelligence Surveillance and
Reconnaissance
IT - Information Technology
IT21 - Information Technology for the 21st
Century
IWS – Integrated Warfare Systems

J

JROC - Joint Requirements Oversight
Council
JSSEO – Joint SIAP Systems Engineering
Organization
JTM – Joint Track Manager

K

KPPs - Key Performance Parameters
KWEB – Knowledge Web

L

LCS – Littoral Combat Ship

M

MCP – Mission Capabilities Package

N

NCES – Network Centric Enterprise
Services
NCP – Naval Capabilities Process
NCS – Naval Combat Systems
NCW – Network Centric Warfare
NDP – Naval Doctrine Publication
NII – Network Information and Integration
NSS - National Security System
NTDS - Navy Tactical Data Systems
NWS – Naval Warfare Systems

O

OA - Open Architecture
OACE - Open Architecture Computing
Environment

OAFA – Open Architecture Functional
Architecture

OODA – Observe-Orient-Decide-Act

ORDALT – Ordnance Alteration

OV-1 - High Level Operational Concept
Graphic

P

P3I – Pre-Planned Product Improvement

PC – Personal Computer

PPBE – Planning, Programming, Budgeting
and Execution

Q

QoS - Quality of Service

R

RCIP/APB - Rapid Capabilities Insertion
Process/Advanced Processor Build

RDTE – Research, Development, Test and
Evaluation

S

SBIR – Small Business Innovation Research

SE – Systems Engineering

SIAP - Single Integrated Air Picture

SM – Standard Missile

SSCCC – Single Scalable Core Combat
Capability

SSDS – Ship Self Defense System

T

TADIL - Tactical Digital Information Link

TBMCS – Theater Battle Management
Control System

TBMD – Theater Ballistic Missile Defense

TSCE – Total Ship Computing Environment

U

UAV - Unmanned Aerial Vehicle

V

XYZ

VOIP – Voice Over Internet Protocol

W

WCS – Weapons Control System

Definition of Terms

<p>Air Warfare</p>	<p>Air defense against airborne weapons including theater ballistic missiles. Operations include surveillance, offensive counter air, defensive counter air, and electronic warfare.</p>
<p>Architecture</p>	<p>(1) The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. (2) A high level design that provides decisions made about: the problem(s) that the product will solve, component descriptions, relationships between components, and dynamic operation description. (3) A framework or structure that portrays relationships among all the elements of the subject force, system, or activity.</p>
<p>Architecture Views, Software²¹</p>	<p><i>Conceptual Architecture.</i> The purpose of the conceptual architecture is to direct attention at an appropriate decomposition of the system without delving into details. Moreover, it provides a useful vehicle for communicating the architecture to non-technical audiences, such as management, marketing, and users. It consists of the Architecture Diagram (without interfaces) and an informal component specification (which we call CRC-R cards) for each component.</p> <p><i>Logical Architecture.</i> The logical architecture adds precision, providing a detailed "blueprint" from which component developers and component users can work in relative independence. It incorporates the detailed Architecture Diagram (with interfaces), Component and Interface Specifications, and Component Collaboration Diagrams, along with discussion and explanations of mechanisms, rationale, etc.</p> <p><i>Execution Architecture.</i> An execution architecture is created for distributed or concurrent systems. The process view shows the mapping of components onto the processes of the physical system. The deployment view shows the mapping of (physical) components in the executing system onto the nodes of the physical system.</p>

²¹ Presented by Malan and Bredemeyer at Comdex 98

Architecture, Functional	The hierarchical arrangement of functions, their internal and external (external to the aggregate itself) functional interfaces and external physical interfaces, their respective functional and performance requirements, and design constraints.
Architecture, Software²²	(1) The software architecture of a program or computing system is the structure or structures of the system, which comprise (1) software components, (2) the externally visible properties of those components, and (3) the relationships among them. (2) The structure and relationships among the components of a computer program. The software architecture may also include the program's interface with its operations environment.
Architecture, System	(1) A logical, physical structure that specifies interfaces and services provided by the system components necessary to accomplish system functionality. (2) The structure and relationship among the components of a system: The system architecture may also include the systems interface with the operational environment.
Asset	Any sensor, weapon, aircraft, boat, unmanned air vehicle (UAV), etc., directly controlled by own ship.
Associated Measurement Report (AMR)	A sensor measurement that has been processed by the originating sensor for clutter rejection and meets defined signal-to-noise parameters, and has been associated to either a local sensor track or a global composite track.
Association	(1) The automatic or manual establishment of a relationship between two or more tracks when the information on them is deemed to pertain to the same contact. (2) The process of identifying and linking data sets that may correspond to the same object while retaining each track as an individual entity.
Attribute Data	Any non-kinematic data provided by a sensor for a track. Examples include IFF mode codes, INTEL data (e.g., imagery), EW data (e.g., parametric data), non-cooperative target recognition (NCTR) data, etc.

²² Bass, Clements, and Kazman. *Software Architecture in Practice*, Addison-Wesley 1997

Baseline, Allocated	The initially approved documentation describing a system's functional, performance, interoperability, and interface requirements that are allocated from those of the system or higher level subsystem; interface requirements with interfacing subsystems; design constraints; derived requirements (functional and performance); and verification requirements and methods to demonstrate the achievement of those requirements and constraints.
Baseline, Functional	The initially approved documentation describing a system's or configuration item's functional performance, interoperability, and interface requirements and the verification required to demonstrate the achievement of those specified requirements.
Battle Force	A standing operational naval task force organization of carriers, surface combatants, and submarines assigned to numbered fleets. A battle force is subdivided into battle groups.
Combat Identification (CID)	CID is the process of attaining an accurate characterization of detected objects in the joint battlespace to the extent that high confidence, timely application of military options and weapons resources can occur. Depending on the situation...this characterization may be limited to 'friend', 'enemy', or 'neutral'. In other situations, other characterizations may be required – including, but not limited to, class, type, nationality, and mission configuration.
Command and Control	The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.
Component, System	A basic part of a system. System components may be personnel, hardware, software, facilities, data, material, services, and/or techniques that satisfy one or more requirements in the lowest levels of the functional architecture. System components may be subsystems and/or configuration items.
Composite/Collaborative Track	A representation of an entity that is formed by combining individual instances of measurement data or a collection of measurements from one or more sensors into a single composite/collaborative track state vector and combined attribute information.

Condition	A variable of the operational environment or situation in which a unit, system, or individual is expected to operate that may affect performance.
Correlation	(1) The determination that a locally derived track represents the same object or point as another track and/or the process of combining two such tracks/data under one track number. (Logicon) (2) The process of identifying tracks believed to represent the same object and replacing them with a single track, combining the data from the duplicate tracks as appropriate.
Decorrelation	The determination that locally held track data for a given track number does not represent the same object or point as track data being received in a remote track report for the same track number.
External Time Source	Synchronizes internal clocks across BF platforms and represents the source of UTC time for the above system time.
Force	(1) An aggregation of military personnel, weapon systems, vehicles, and necessary support, or combination thereof; (2) A major subdivision of a fleet.
FORCEnet	An operational construct and architectural framework that integrates the SEAPOWER21 concepts of Sea Strike, Sea Shield and Sea Basing by connecting warriors; sensors, networks; command and control; platforms and weapons; providing accelerated speed and accuracy of decision; and integrating knowledge to dominate the battlespace. FORCEnet provides the following capabilities: Expeditionary, multi-tiered, sensor and weapon grids; distributed, collaborative, command and control; dynamic, multi-path survivable networks; adaptive/automated decision aids; and human-centric integration.
Functional Analysis	Examination of a defined function to identify all the sub-functions necessary to the accomplishment of that function; identification of functional relationships and interfaces (internal and external) and capturing these in a functional architecture; and flow down of upper-level performance requirements and assignment of these requirements to lower-level sub-functions.
Functional Requirement	Specifies actions that a system must be able to perform, without taking physical constraints into consideration. These are often best described in a Use Case Model and in Use Cases. Functional requirements thus specify the input and output behavior of a system.

<p>Global Command and Control System – Maritime (GCCS-M)</p>	<p>GCCS-M [AN/USQ-119E(V)], previously the Joint Maritime Command Information System (JMCIS), is the Navy's primary fielded Command and Control System. GCCS-M receives, processes, displays, and manages data on the readiness of neutral, friendly, and hostile forces in order to execute the full range of Navy missions (e.g., strategic deterrence, sea control, power projection, etc.) in near-real-time via external communication channels, local area networks (LANs) and direct interfaces with other systems.</p>
<p>Global Information Grid (GIG)</p>	<p>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, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.</p>
<p>Group</p>	<p>(1) A flexible administrative and tactical unit composed of either two or more battalions or two or more squadrons. The term also applies to combat support and combat service support units. (2) A number of ships and/or aircraft, normally a subdivision of a force, assigned for a specific purpose.</p>
<p>Identification (ID)</p>	<p>(1) Identification is the Identity, Category, Platform, Type, Activity, and Nationality/Alliance of the track. (2) The process of determining the friendly or hostile character of an unknown detected contact.</p>
<p>Identity</p>	<p>Identity refers to the nature or attributes of the track: Friend, Assumed Friend, Neutral, Unknown, Pending, Suspect, or Hostile.</p>
<p>INTEL-Generated Track</p>	<p>Track based on INTEL data that is of sufficient quality for correlation/association to a System Track.</p>

Joint	Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate.
Joint Composite Tracking Network (JCTN)	Generic title for a joint telecommunications network and processing capability to enable composite tracking among joint, heterogeneous mixes of sensors and to support appropriate levels of cooperative engagement of targets by weapons systems. It is envisioned as real-time, sensor fusion system, which distributes and fuses sensor measurement data into composite tracks that create a high fidelity, coherent air picture. The JCTN is a concept rooted in the Navy's experience with Cooperative Engagement Capability (CEC). It includes common software and a communications element that allow participating units to share fused sensor data. The communications structure as currently envisioned includes wide-band line-of-sight communications, satellite links, and other communication systems.
Joint Data Network (JDN)	A collection of near-real-time communications and information systems used primarily at the coordination and execution level. It provides information exchange necessary to facilitate the Joint/Service Battle Manager's comprehension of the tactical situation, and also provides the means to exercise command and control beyond the range of organic sensors. The JDN carries near-real-time tracks, unit status information, engagement status and coordination data, and force orders; JDN information is used to cue radars as well. The backbone of the JDN is Link-16. However, other data links such as TADIL A/B/C, Link-22, and VMF (Variable Message Format) will exchange information with the JDN through gateways at various platforms to ensure that disadvantaged users are included in the JDN. Satellites link geographically dispersed users in near real-time without consuming limited tactical bandwidth.
Joint Force	A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander.
Joint Planning Network (JPN)	A collection of non-real-time and near real-time communication and information systems. It provides a distributed collaborative planning capability, automated decision aids, and a means for distributing plans within theater. The core of the JPN is the Global Command and Control System (GCCS) operating in the Defense Information Infrastructure Common Operating Environment (DII COE).

Joint Task Force	A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub-unified commander, or an existing joint task force commander.
Kinematics	Position, Velocity, and Acceleration.
Manual Track	A track that is entered and updated by an operator. It may represent an object not seen by current sensors or provide a different representation of an entity than is currently being depicted by the sensors. In addition to system track correlation, the operator has the ability to associate or correlate this track with other tracks.
Measurement	A sensor-derived detection, contact, hit, or observation at a given point in time.
Measurement Report	A detection from a single sensor which has not yet been subjected to an association process.
Mission	The task, together with the purpose, that clearly indicates the action to be taken and the reason for that action.
Mission Essential Task (MET)	A task selected by a force commander from the Universal Navy Task List (UNTL) deemed essential to mission accomplishment.
Mission Essential Task List (METL)	A list of tasks considered essential to the accomplishment of assigned or anticipated missions. A METL includes associated conditions and standards and may identify command-linked and supporting tasks.
Model 4	TADIL A Taxonomy (Link-11)
Model 5	TADIL J Taxonomy (Link-16)
Multi-Sensor Correlated Track	A representation of an entity that is formed by correlating track reports using various methods based upon time latency of the given tracks. These multiple tracks are correlated to form one representation of the track.
Navy Tactical Task List (NTTL)	The comprehensive list of Navy and Coast Guard (Department of Defense related missions) tasks at the Tactical level of war

Near-Real Time (Tracks)	(1) Near-Real-Time Tracks are generated by real-time sensors on remote units, whose delivery latencies are sufficiently large that while they can be used to help decide to engage on the target, they cannot be used to fire on the target. The data is primarily used for situational awareness. (2) The timelines of the data or information have been delayed by the time required for electronic communications and automatic data processing. 7P1 SS
Non-Functional Requirements	Requirements that are not functional, such as the ones below, are sometimes called non-functional requirements. Many requirements are non-functional, and describe only attributes of the system or attributes of the system environment. Although some of these may be captured in Use Cases, those that cannot may be specified in Supplementary Specifications. Non-Functional requirements are those that address issues such as Reliability, Performance, Supportability, Constraints, and Physical Matters.
Non-Real Time (Tracks)	(1) Non-Real-Time Tracks have latencies that nominally range from 15 seconds up to days. (2) The timelines of the data or information have been delayed such that the data or information has questionable utility beyond situational awareness. 7P1 SS
Other Tactical Data	Data of a non-kinematic, non-sensor-processed nature including intelligence, imagery, voice, context information (e.g., commercial air and shipping lanes, political boundaries).
Quality of Service (QoS)	A defined level of performance that adapts to the environment in which it is operating. QoS may be requested by the user of the information and the level of QoS provided will be assigned based on the request, the available capabilities of the provider, and the priority of the user.

Real Time (Tracks)	(1) Real-Time Tracks are generated by sensors whose delivery latencies are sufficiently small to enable them to be utilized to participate in anti-air warfare (AAW), i.e., to form composite tracks for situational awareness and also of sufficient quality to engage and fire on the target (“quality” is weapon dependent). The key issue is the latency of the arrival and subsequent usage of the track data. Periodicity is also a component of track quality. (2) Pertaining to a system or mode of operation in which computation is performed during the actual time that an external process occurs, in order that the computation results can be used to control, monitor or respond in a timely manner to the external process.
Request for Information (RFI)	Any specific time-sensitive ad hoc requirement for intelligence information or products to support an on-going crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A RFI can be initiated to respond to operation requirements and will be validated in accordance with the theater command’s procedures.
Requirement	Describes a condition or capability to which a system must conform; either derived directly from user needs, or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system. A capability that the system must deliver.
Sea Basing	Projecting Joint Operational Independence through the extended reach of networked weapons and sensors. Capabilities include: Enhanced afloat positioning of joint assets; Offensive and defensive power projection; Command and control; Integrated joint logistics; and Accelerated deployment and employment timelines.
Sea Shield	Takes Naval defense beyond unit and task-force defense to provide the nation with sea-based theater and strategic defense. Capabilities include: Homeland defense; Sea and littoral superiority; Theater air missile defense; and Force entry enabling.
Sea Strike	Describes the capabilities of naval forces to project decisive and persistent offensive power anywhere in the world. Capabilities include: Persistent intelligence, surveillance, and reconnaissance; Time-sensitive strike; Electronic warfare/ and information operations; Ship-to-objective maneuver; and Covert strike.

Supporting Source Track	A composite/collaborative track, a multi-sensor correlated track, a manual track, or an INTEL-generated track that is the basis for declaring the existence of a system track.
Supporting Task	Specific activities that contribute to the accomplishment of a joint mission essential task. Supporting tasks are accomplished at the same command level or by subordinate elements of a joint force (i.e., joint staff, functional components, etc.)
System Time	Represents the time standard used within the combat system, including the local source of Universal Coordinated Time (UTC), a system-wide monotonically increasing reference time, as well as other representations of the system-wide reference time.
System Track	A platform-specific representation of an individual entity, identified by a unique system track number, containing one or more track state vectors and uncertainties, as well as associated attributes, attribute uncertainties, and data valid time.
Task	A discrete event or action, not specific to a single unit, weapon system, or individual that enables a mission or function to be accomplished.
Track	(1) A set of detections, contacts, hits or observations, generated by the same real object in the environment. It is identified by a track number, and has intrinsic and derived attributes associated with it. (2) A series of related contacts displayed on a data display console or other display device. (3) To display or record the successive positions of a moving object.
Track Kinematics	A track state vector that represents the best understanding of the entity's position and movement at a defined point in time with the objective of predicting the entity's future position if it maintains a consistent direction of movement.
Track Number	The unique or alphanumeric identifier associated with a specific set of track data representing a vehicular object, point, line of bearing, fix, or area of probability.
Track Quality (TQ)	A numerical value assigned to a track computed from data related to the past tracking performance on the track, representing the accuracy of the track position.

Track State	Smoothed position and velocity representation of an individual object, which minimizes the RMS errors in estimates of the closest point of approach and time of closest point of approach.
Track, Local	A track established within a unit based on sensor measurements derived from the local platforms sensors.
Track, Remote	A track established by a remote unit, or group of units, and supplied to the local platform.
Unassociated Measurement Report (UMR)	(1) A sensor measurement that has been processed by the originating sensor for clutter rejection and meets defined signal-to-noise parameters, but has not been associated to a track. (2) A Measurement Report from a single sensor that has not been successfully associated with an existing composite or single-sensor track and which may be the initial detection of a new entity.
Universal Joint Task List (UJTL)	The comprehensive list of tasks at the Strategic and Operational levels of war. A menu of capabilities (mission-derived tasks with associated conditions and standards, i.e., the tools) that may be selected by a joint force commander to accomplish the assigned mission. Once identified as essential to mission accomplishment the tasks are reflected within the command joint mission essential task list.
Universal Navy Task List (UNTL)	UNTL = UJTL + NTTL
Use Case	Describes a sequence of actions, performed by a system, that yields a result of value to a user. A description of a set of actions, including variants, that a system performs that yields an observable result of value to a particular actor. (UML)
Use Case Survey	A list of names and perhaps brief descriptions of use cases associated with a system, component, or other logical or physical entity.
Use-Case Model	A model that describes a system's functional requirements in terms of use cases. Consists of all the actors of the system and all the various use cases by which the actor interact with the system, thereby describing the totality of the functional behavior of the system.

Warfare System	All shipboard tactical systems, and tactical mission support systems, such as weapons, sensors, command and control, navigation, aviation support systems, mission planning, intelligence, surveillance and reconnaissance, interior and exterior communications, topside design, and warfare system networks. Source: N00178-04-R-2010, <i>Aircraft Carrier Warfare Systems Support</i> .
-----------------------	--