NPS-SE-06-005

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Coalition FORCEnet Implementation Analysis

by

Ted Berger
Michael Gonzales
Brian Nguyen
Gary Perkins
Tony Russell
Rick Tahimic
Paul Choate
Christine Liou
Eugene Park
Duncan Peterson
Eric Shebatka
Greg Whalin

September 2006

Approved for public release; distribution is unlimited

Prepared for: Deputy Chief of Naval Operations for Warfare Requirements and Program (OPNAV N71), 2000 Pentagon, TTCP MAR Group, Action Group 6, Washington, DC 20350-2000

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 93943-5001

COL. David A. Smarsh, USAF
Acting President

Leonard A Ferrari
Associate Provost

This report was prepared for the Chairman of the Systems Engineering Department in partial fulfillment of the requirements for the degree of Master of Science in Systems Engineering.

This report was prepared by the Masters of Science in Systems Engineering (MSSE) Cohort Four from the Space and Naval Warfare Systems Center, San Diego:

Authors:

Ted Berger	Paul Choate
Michael Gonzales	Christine Liou
Brian Nguyen	Eugene Park
Gary Perkins	Duncan Peterson
Tony Russell	Eric Shebatka
Rick Tahimic	Greg Whalin

Reviewed by:

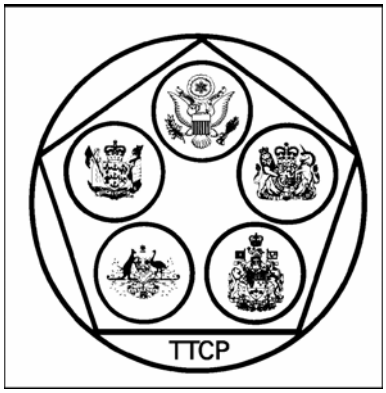
David H. Olwell, Ph. D.
Chairman, Department of Systems Engineering

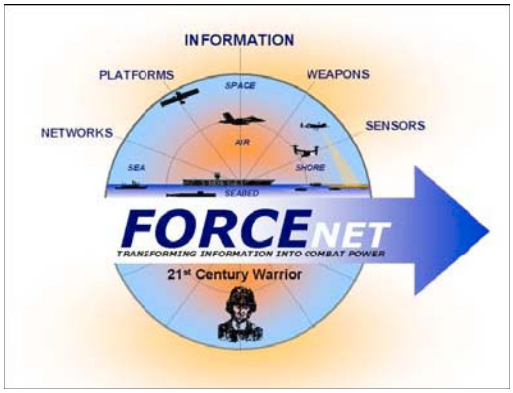
Released by:

Dan C. Boger, Ph. D.
Interim Associate Provost and Dean of Research

CAPABILITY DEVELOPMENT DOCUMENT
FOR
FORCEnet FOR COALITION
JOINT TASK FORCE

Focus on Expeditionary Strike Group (ESG)





Prepared for the Naval Postgraduate School (NPS)
MSSE Capstone Project, SI0810 2006-1

Prepared by:
San Diego, California, Cohort:

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Technical Report	
4. TITLE AND SUBTITLE: Coalition FORCEnet Implementation Analysis			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ted Berger, Paul Choate, Michael Gonzales, Christine Liou, Brian Nguyen, Eugene Park, Gary Perkins, Duncan Peterson, Tony Russell, Eric Shebatka, Rick Tahimic, and Greg Whalin			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT

In January 2006, the San Diego Naval Postgraduate Cohort was tasked to evaluate a FORCEnet scenario which involved a Humanitarian Support Mission which escalated into an Expeditionary Warfare Mission in and around the Philippine Islands, employing AUSCANNZUKUS Coalition forces. The task was to study the impact of Coalition forces participating in the United States Navy FORCEnet (Fn) program. The goal of this study is to provide options, perspective, technical and tactical insight to each nation in identifying opportunities to participate in FORCEnet and the operational benefits that result. The San Diego Naval Postgraduate Cohort developed an architecture and modeled it in an effort to demonstrate enhanced collaboration capability between U.S. and Coalition partners with an improved ability to collect, process and share information for joint decision making and joint tactical employment of resources between U.S. and Coalition countries, and to fully integrate Coalition operations. The modeling approach focused on integrating a Sensor grid, C2 grid, and Engagement grid. As a result, enabled Network-Centric warfare for Coalition Forces shows a significant increase in capabilities. Joint employment of FORCEnet demonstrated Coalition enhancements by providing a scalable and composable Joint force structure.

14. SUBJECT TERMS FORCEnet, Coalition Forces, AUSCANNZUKUS, Network-Centric Warfare (NCW), Data Mining, EXTEND Modeling, Expeditionary Strike Group (ESG), Integrated Fire Control (IFC).			**15. NUMBER OF PAGES** 209
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

ACAT	Acquisition Category
ADNS	Automated Digital Network System
AEHF	Advanced Extremely High Frequency
AG-1	Action Group 1
AI	Artificial Intelligence
AMA	Automated Management Aids
Ao	Availability
AOSN	Autonomous Oceanographic Sampling Network
ASCM	Anti-Ship Cruise Missle
ASG	Amphibious Strike Group
ASMD	Anti-Surface Missile Defense
ASN	Assistant Secretary of the Navy
ASuW	Anti-Submarine Warfare
ASW	Anti-Surface Warfare
AUSCANNZUKUS	Australia, Canada, New Zealand, United Kingdom, United States
AV	Architecture View
AWACS	Airborne Warning And Control System
BACN	Battlefield Airborne Communication Node
BF	Battleforce
BG	Battlegroup
BLOS	Beyond Line-of-Sight
C2	Command and Control
C3N	Command, Control, Communication Network
C4ISR	Command, Control, Communication, Computing, Intelligence, Surveillance, Reconnaissance

CADM	Core Architecture Data Model
CART	Classification and Regression Tree
CDD	Capability Development Document
CDP	Cumulative Detection Probability
CEC	Cooperative Engagement Capability
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFE	Combined Enterprise Regional Information Exchange System (CENTRIXS) Four Eyes
CG	Guided Missile Cruiser
CHAID	Chi Square Automatic Interaction Detection
CID	Combat Identification
CIO	Chief Information Officer
CIS	Coalition Information Sharing
CISMOA	Communications Interoperability and Security Memorandum of Agreement
CJCSI	Chairman of Joint Chief Staff Instruction
CJTF	Coalition Joint Task Force
CMI	Classified Milityary Information
CNFC	Combined Naval Forces Central Command
CNO	Chief of Naval Operations
COA	Course of Action
COCOM	Combatant Commander
COI	Community of Interest
COMSPAWARSYSCOM	Commander, Space and Naval Warfare Systems Command
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture
CRD	Capstone Requirements Document
CSG	Carrier Strike Group

CTP	Common Tactical Picture
CVN-21	Carrier Vessel Nuclear number 21
DADS	Deployable Autonomous Distributed System
DD	Destroyer
DDG	Guided Missile Destroyer
DDX	Destroyer, Experimental (US Navy next generation ship)
DE	Discrete Event
DFRM	Data Fusion Resource Manager
DISR	DoD Information Technology Standards Registry
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoN	Department of Navy
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DRM	Distributed Resource Management
DTUSD(P)PS	Deputy to the Under Secretary of Defense (Policy) for Policy Support
E3	Effective Engagement Envelope
EHF	Extremely High Frequency
EoC	Engage on Composite
EoR	Engage on Remote
ES	Enterprise Services
ESF	Expeditionary Strike Force
ESG	Expeditionary Strike Group
FCP	Fire Control Picture
FFG	Guided Missile Frigates
FIFO	First-In, First-Out
Fn	FORCEnet
FnFC	FORCEnet Functional Concept

FNMOC	Fleet Numerical Meteorology and Oceanography Center
FOC	Full Operational Capability
FOS	Family of Systems
FRP	Fleet Response Plan
FY	Fiscal Year
GCTF	Global Counter Terrorism Task Force
GIG	Global Information Grid
GIG ES	Global Information Grid (GIG) Enterprise Services
GIS	Geographical Information System
GPS	Global Positioning System
GWOT	Global War On Terror
HA-DR	Humanitarian Aid and Disaster Relief
HAIPIS	High Assurance Internet Protocol Interoperability Specification
HFE	Human Factors Engineering
HFIP	High Frequency Improvement Program
HSCC	Health, Status, Configuration, and Capability
HSI	Human Systems Integration
HUMINT	Human Intelligence
I/O	Input and Output
IABM	Integrated Architecture Behavior Model
IC	Intelligent Community
ICD	Initial Capabilities Document
ID	Identification
IEEE	Institute of Electrical & Electronics Engineers
IFC	Integrated Fire Control
INCOSE	International Council on Systems Engineering
INMARSAT	International Maritime Satellite
INT	Intelligence

IOC	Initial Operational Capability
IP	Internet Protocol
ISNS	Integrated Shipboard Network System
IT	Information Technology
JCTF	Joint Coalition Task Force
JDL	Joint Directors of Laboratories
JFCOM	Joint Force Command
JITC	Joint Interoperability Test Command
JSSEO	Joint Single Integrated Air Picture (SIAP) Systems Engineering Organization
JTA	Joint Technical Architecture
JTM	Joint Track Manager
JV	Joint Version
JV2020	Joint Vision 2020
LCS	Littoral Combat Ship
LHD	Amphibious Assault Ship
LoC	Launch on Composite
LoR	Launch on Remote
LOS	Line-of-Sight
LPD	Amphibious Transport Dock Class
LST	Landing Ship, Tank
M&S	Modeling and Simulation
MA	Mission Area
MA ICD	Mission Area Initial Capabilities Document
MAR	Maritime Systems
Mbps	Milibits per Second
MCFI	Multinational Coalitional Forces Iraq
METOC	Meteorological and Oceanographic
MNIS	Multi-National Information System

MOA	Memorandum of Agreement
MOE	Measure of Effectiveness
MOP	Measure of Performance
MOU	Memorandum of Understanding
MSSE	Masters of Science, Systems Engineering
NAMRAD	Non-Atomic Military Research and Development
NATO	North Atlantic Treaty Organization
NCEP	Naval Capability Evolution Process
NCES	Net Centric Enterprise Services
NCID	Net-Centric Information Document
NCMW	NetCentric Maritime Warefare
NCOW RM	Net-Centric Operations and Warfare Reference Model
NCW	Network-Centric Warfare
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organizations
NOC	Network Operation Center
NPS	Naval Postgraduate School
NSA	National Security Agency
NTR	Naval Transformation Roadmap
OASD(NII)	Office of the Assistant Secretary of Defense, Networks and Information Integration
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
ONI	Office of Naval Intelligence
OOB	Order Of Battle
OPNAV	Chief of Naval Operations
OSD	Office of the Secretary of Defense
OV	Operational View

P2P	Peer-to-Peer
PAO	Public Affairs Office
PCP	Peer Computing Programs
Pd	Probability of Detection
Pk	Probability of Kill
PSD	Preferred Shooter Determination
QFD	Quality Function Deployment
QoS	Quality of Service
RDML	Rear Admiral
RDT&E	Research, Development, Test and Evaluatoin
RF	Radio Frequency
RMP	Recognized Maritime Picture
ROC	Receiver Operating Characteristics
RP	Republic of the Philipines
SA	Situational Awareness
SAG	Surface Action Group
SATCOM	Satellite Communication
SBR	Spaced-Based Radar
SHF	Super High Frequency
SIAP	Single Integrated Air Picture
SIGINT	Signal Intelligence
SLA	Service Level Agreement
SOS	System of Systems
SOW	Statement of Work
STANAG	NATO Standardization Agreement
SubNet	Sub-Network
SV	System View
TDL	Tactical Data Link

TTCP	The Technical Cooperation Program
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Arieal Vehicles
UCP	Unified Command Plan
UHF	Ultra High Frequency
UNTL	Universal Navy Task List
US	United States
USN	United States Navy
USW	Under Sea Warfare
UUV	Unmanned Undersea Vehicle
VHF	Very High Frequency
WAN	Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The target of this project is to resolve a scenario in and around the Philippine Islands, employing AUSCANNZUKUS Coalition forces, and to study the Coalition impact of participating in the USN FORCEnet (Fn) program. The goal of this study is to provide options and perspective to each nation in terms of identifying opportunities to participate in FORCEnet and the operational benefits that might result. The second goal is to assist each nation's decision-making process by demonstrating improved Coalition effectiveness with the implementation of FORCEnet.

The framework for this study is derived from the Operation Philippine Comfort – CJTF scenario. The scenario is based around a natural humanitarian disaster (volcanic eruption) creating international sentiment which requires relief action on the part of each nation. Each AUSCANNZUKUS nation has naval and/or military assets with some dual use capability (naval/humanitarian relief) as well as inherent warfighting capability in the vicinity of the disaster. Due to a change in government, the Philippines are experiencing political unrest due in part to Muslim factions in the southern province of Mindanao, whose intent is to use the chaos as an opportunity to achieve their goal of a separate secular state. The mission of the CJTF evolves from humanitarian relief to one that also includes peace-keeping and law enforcement. The U.S. dispatches an Expeditionary Strike Group (ESG) with an amphibious component to ensure that disaster relief is not impeded by the previously covert, but now openly aggressive support of the separatists by a Southeast Asian country with their naval units (SAG and SSK), as they attempt to oppose ESG access to the Sulu Sea .

Lack of a single, multinational information sharing environment exists among the AUSCANNZUKUS Coalition. Additionally, insufficient standardization and interoperability of C4ISR systems exists between U.S. and Coalition forces. To overcome these shortcomings, a fully functional agreement on standards creating a common CONcept of OPerations (CONOPS) and agreement in Tactics, Techniques and Procedures (TTPs) is required by all participating countries.

A key component to enhancing Joint Coalition Force operations is the strengthening of the collaboration between multinational partners, with the ultimate goal to improve the ability to collect, process, and share information. Operational experience has demonstrated shortcomings in Department of Defense (DoD) arrangements for multinational information sharing with Coalition partners.

This project proposes a candidate operational and systems architectures and modeled them in an effort to demonstrate the following:

- Enhanced collaboration capability between U.S. and Coalition partners
- Improved ability to collect process and share information between U.S. and Coalition countries
- Fully integrated Coalition operations and synchronization

Platforms that are Partially Net Enabled or Fully Net Enabled show a higher rate of survivability. Secondary goals of the study were to model and identify if Coalition FORCEnet architecture improves:

- Communication to all nodes
- Accuracy and timeliness of information on friendly, environmental, neutral and hostile units
- Storage and retrieval of authoritative data sources
- Knowledge management capability with direct access ability to raw data
- User-defined and shareable Situational Awareness (SA)
- Distributed and collaborative command and control
- Automated decision aids to enhance decision making
- Information assurance
- Cross-domain access and data exchange
- Interoperability across all domains and agencies
- Autonomous and disconnected operations
- Automatic and adaptive diagnostic and repair

The modeling results demonstrate that these attributes in a Coalition architecture made a considerable difference.

The preliminary results show:

- Network-Centric warfighting is value added to Coalition Forces
- Sensors - 5% improvement in number of threats detected
- C2 - 42% improvement in tracking via precision cue
- Engagement - 25% improvement in threat neutralization
- Non-FORCEnet forces sustain higher casualties

The modeling assumes implementation of common Concept of Operations (CONOPS) and agreement in Tactics, Techniques, and Procedures (TTPs). Essential among these are:

- Releasability Policy
- Unity of Command and Control (C2)
- Adequate Peace-Time Training

Enabled Network-Centric Warfare for Coalition Forces shows a significant return on investment. FORCEnet lends itself to accommodating Coalition enhancements providing a scalable and composable force structure. Implementation of Level-3 and 4 FORCEnet capabilities is recommended.

I. CAPABILITY DISCUSSION

In an effort to identify capabilities required to improve United States and Coalition warfighting effectiveness in a network-centric environment, this project will:

- Examine the tenets and capabilities provided by FORCEnet as described in existing literature and policy documents
- Examine Command, Control, Communications, Computers, and Intelligence (C4I) capabilities and their desired attributes to understand how they contribute to improved Situational Awareness (SA) and warfighting effectiveness
- Examine both materiel and non-materiel solutions to develop recommendations for continued analysis, and
- Conduct a Modeling and Simulation (M&S) analysis to quantify the potential warfighting improvement associated with the implementation of recommended capabilities

A. INTRODUCTION – NETWORK-CENTRIC WARFARE AND FORCENET

The concept of Network-Centric Warfare (NCW) emerged in the late 1990s and is a key element of the Department of the Navy's (DoN) effort to transform itself to meet the 21st Century military challenges[1]. NCW focuses on using advanced information technology (IT) – computers, high-speed data links, and networking software – to link U.S. Navy ships, aircraft, and shore installations into a highly integrated combat force through the implementation of local and wide-area networks. As has been seen, networking has affected society in many significant ways. The World Wide Web and Internet have profoundly affected the global economy, as well as our personal lives. An extension of this technology to the realm of military operations is therefore an undertaking well worth consideration. The DoN believes that NCW will dramatically improve naval combat capability and efficiency[2].

[1] For more on naval transformation, see CRS Report RS20851, Naval Transformation: Background and Issues for Congress, by Ronald O'Rourke. Washington 2003. (Updated periodically) 6 p.

[2] For discussions of NCW, see Alberts, David S. et al. Network-Centric Warfare, Developing and Leveraging Information Superiority. Washington, Department of Defense, 1999. 256 p;

FORCEnet is the process of making Network-Centric Warfare (NCW) and Net-Centric Operations a reality.

- FORCEnet is:
  - The operational construct and architectural framework for Naval Warfare in the Information Age which integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force, scalable across a spectrum of conflict from seabed to space and sea to land[3].
  - The naval Command and Control (C2) component for Sea Power 21 and Expeditionary Warfare.
  - The future implementation of Network-Centric Warfare in the naval services.
  - An enterprise alignment and integration initiative to serve as a change agent and engine for innovation, potentially touching every naval program.
- What is the value-added of the FORCEnet Functional Concept (FnFC)?[4]
  - It provides critical shared direction, guiding principles, and projected evolutionary objectives for the Navy and Marine Corps development of future C2 capabilities, to ensure Naval Forces will be ready in the future security environment.
  - The FnFC serves as a vital and necessary bridge between the FORCEnet vision and the capabilities that the Navy and Marine Corps must develop to ensure national security goals are met.
  - Additionally, the FnFC provides:
    1. Coherence and alignment of FORCEnet development efforts
    2. Acceleration in Fleet implementation of C2 capabilities
    3. Transformation of Navy operations in a warfighting or business role
    4. Front and center position for the warfighter in FORCEnet development

---

Cipriano, Joseph R. a Fundamental Shift in the Business of Warfighting. Sea Power, March 1999; 39-42;

Cebrowski, Arthur K, and John J Garstka Netwrk-Centric Warfare: Its Origins and Future. U.S. Naval Institute Proceedings, January 1998; 28-35.

3 CNO's strategic Study group – XXI definition from 22 July 02 CNO Briefing. Network-Centric Warfare, 2nd Edition, by D.S. Alberts, J.J. Garstka, and F.P. Stein

4 FORCEnet: A Functional Concept for the 21st Century, February 2005

- The 15 specific capabilities that the FnFC has identified have been articulated to support the development of architectures and future experimentation, and to drive Navy and Marine Corps programmatic requirements.
    1. Provide robust, reliable communication to all nodes, based on the varying information requirements and capabilities of those nodes.
    2. Provide reliable, accurate and timely location, identity and status information on all friendly forces, units, activities and entities or individuals.
    3. Provide reliable, accurate and timely location, identification, tracking and engagement information on environmental, neutral and hostile elements, activities, events, sites, platforms, and individuals.
    4. Store, catalogue and retrieve all information produced by any node on the network in a comprehensive, standard repository so that the information is readily accessible to all nodes and compatible with the forms required by any node, within security restrictions.
    5. Process, sort, analyze, evaluate, and synthesize large amounts of disparate information while still providing direct access to raw data as required.
    6. Provide each decision maker the ability to depict situational information in a tailorable, user-defined, shareable, primarily visual representation.
    7. Provide distributed groups of decision makers the ability to cooperate in the performance of common command and control activities by means of a collaborative work environment.
    8. Automate certain lower-order command and control sub-processes and to use intelligent agents and automated decision aids to assist people in performing higher-order sub-processes, such as gaining situational awareness and devising concepts of operations.
    9. Provide information assurance.
    10. Function in multiple security domains and multiple security levels within a domain and manage access dynamically.
    11. Interoperate with command and control systems of very different type and level of sophistication.

12. Allow individual nodes to function while temporarily disconnected from the network.
13. Automatically and adaptively monitor and manage the functioning of the command and control system to ensure effective and efficient operation and to diagnose problems and make repairs as needed.
14. Incorporate new capabilities into the system quickly without causing undue disruption to the performance of the system.
15. Provide decision makers the ability to make and implement good decisions quickly under conditions of uncertainty, friction, time, pressure, and other stresses.

- The FnFC also identifies six dimensions of development effort:
  1. Physical – platforms, weapons, sensors, etc.
  2. Information Technology – communications and network infrastructure
  3. Data – structure and protocols for information handling
  4. Cognitive – interfaces that support judgment and decision making
  5. Organizational – new structures and working relationships that will be made possible by FORCEnet
  6. Operating – new methods and concepts by which forces will accomplish missions with the new, FORCEnet-provided capabilities

The concept of FORCEnet operations will generate increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

B. CAPABILITY GAPS

Recent operational experience with allied nations demonstrated shortcomings in the Department of Defense (DoD) arrangements for multinational information sharing with Coalition partners[5] including the efforts during Operation Enduring Freedom (OEF) where the operational area force was comprised of thirty-one (31) U.S. Navy ships and

[5] DoD Instruction 8110.1 Subject: Multinational Information Sharing Transformation Change Package of 6 February 2004.

sixty (60) Coalition platforms from eleven (11) countries[6]. Some of these shortcomings are based on the fact that the communication systems used by each nation are not interoperable with one another. Therefore they cannot share battlefield information as it is acquired. There is a lack of a single multinational information sharing environment and there is insufficient standardization in systems to enable interoperability between U.S. and Coalition forces.

To overcome this interoperability gap the United States Navy is developing and implementing FORCEnet, not only to enable communication with multiple U.S. platforms, but also to utilize the information gathered from all the platforms, creating a Common Operating Picture (COP). Distribution of the COP would allow all platforms in the theater to have the same comprehension and understanding of what actions and plans are in effect for an area.

The implementation of the FORCEnet architecture can, and should, be extended beyond United States forces, to include any allied or participating nations, but in particular, the Coalition forces of AUSCANNZUK. It must be remembered that FORCEnet is not a system or a collection of systems, but an architecture under which the systems from the Coalition forces must become interoperable in order to take advantage of the capabilities FORCEnet provides.

C. REQUIREMENT FOR NETWORK-CENTRIC WARFARE

Reiterating, FORCEnet is defined as the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms and weapons in a networked, distributed combat force[7]. This integration requires that systems be networked such that data can be shared between platforms and countries. Additionally, the information obtained would be capable of being synchronized and delivered in a timely manner so that it can be fully taken advantage of in order to be able to supply COP to the Coalition force. This concept of shared information is the foundation of Network-Centric Warfare (NCW). The term Network-Centric Warfare broadly describes the combination of strategies, emerging

6 The Technical Cooperation Program (TTCP) Brief, 9 January 2006

7 FORCEnet: A Functional Concept for the 21st Century, February 2005

tactics, techniques, procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage[8].

This "networking" utilizes information technology via a robust network to allow increased information sharing, collaboration, and shared situational awareness, which theoretically allows greater self-synchronization, speed of command, and mission effectiveness.

The theory has four basic tenets:

1. A robustly networked force improves information sharing
2. Information sharing enhances the quality of information and shared situational awareness
3. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
4. These, in turn, dramatically increase mission effectiveness[9]

D. EVALUATION OF FORCENET FOR COALITION FORCES

Network-Centric Warfare brings together a powerful set of warfighting concepts and associated military capabilities that enable the warfighters to exploit information in order to bring assets to bear in a rapid and flexible manner. This is the basis behind the possible benefits to the AUSCANNZUKUS Coalition force. This paper reviews those benefits and models them based on the sample scenario.

---

[8] John J. Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal, May 2003, p. 58.

[9] Wikipedia,, on-line, available at http://en.wikipedia.org/wiki, accessed August 2006

II. LITERATURE REVIEW

A. FORCENET C4ISR

One of the main goals for future joint operations with U.S. and Coalition forces is to increase data sharing through networking technologies. Through the use of networking technologies, a group of individual platforms can function as one large, netted battle force. With a netted battle force, all platforms have the same tactical picture and platform resources such as sensors and weapons are available for use by the entire battle force. Conducting military operations more efficiently and effectively by using these integrated and distributed resources is the ultimate goal of the network-centric warfare concept.

The purpose of Section 2 is to describe the enabling technologies that make it possible to conduct network-centric warfare. The topics in this section include Integrated Fire Control, the Joint Track Manager, future Tactical Data Links (TDL), the Global Information Grid (GIG), and underwater networking technologies. A description of the C4ISR technical challenges, limitations and gaps is also provided in the concluding sections.

As previously stated, one major goal of the network-centric battle force is to increase data sharing. One of the early systems that made it possible to conduct network-centric operations was the Cooperative Engagement Capability (CEC) system. CEC combines a high-performance sensor grid with a high-performance engagement grid. The sensor grid rapidly generates engagement quality measurement data which allows the engagement grid to neutralize targets over a larger area than was previously possible. The CEC sensor grid fuses data from multiple sensors to develop engagement quality composite tracks, creating a higher quality fire control picture than was previously possible using with stand-alone sensors. The ability to cooperatively engage targets increased both the lethality and survivability of the battle force.

One capability that is possible through network-centric warfare is Integrated Fire Control (IFC). IFC could only be realized through a netted battle force. A netted battle force will be able to effective track and efficiently used its weapons resources. The

concept of integrated fire control is to use the sensors and weapons of multiple platforms to engage targets more effectively than was possible using the sensors and weapons of a single platform. IFC is described in Section 2.2.2.

The goal of the Global Information Grid (GIG) is to provide the means for data sharing between geographically separated nodes such as the battle force, command centers, intelligence organizations, etc. The GIG should greatly increase data sharing among all participants. The GIG is faced with many challenges, i.e. quality of services, bandwidth, and timeliness, to name a few. Section 2.2.3 explains the purpose of the GIG and its core services.

As the battle force makes the transition to a network-centric capability, tactical data links will continue to support the exchange of command and control information between legacy units. Information exchange between TDLs and network-centric units will be possible using gateway units. The TDLs will also server as a backup to the netted battle force as well as another source of information. Section 2.2.4 describes the role of tactical data links in the network-centric warfare concept.

The Joint Track Manager (JTM) performs several functions. The JTM is responsible for processing tactical information and producing a common tactical picture. The JTM also manages and allocates the battle force resources (sensor, weapons, and C2 systems) based on threat assessment results. A behavior model concept is designed into all JTM units, which if given identical data to process produces identical results at each unit. Section 2.2.5 describes components and functions of the JTM including data fusion, the integrated behavior model, the resource manager, and data mining.

Section 2.2.6 looks into underwater networking technology in a system called Seaweb. This system enables network-centric warfare in the subsurface environment.

B. FORCENET ENABLING TECHNOLOGY

1. Sensor Networking Technology

a. Introduction

The U.S. military operational architecture consists of three grids: the Sensor grid, the Communications and Control (C2) grid, and the Shooter grid. In a Naval platform-centric architecture, the sensor grid is generally utilized and managed to support

a single weapon or combat system. Platform-centric sensor system consists of single intelligence stovepipes to support an individual platform's needs. Figure 2-1[10] depicted a sensor platform with a dedicated C2 node.

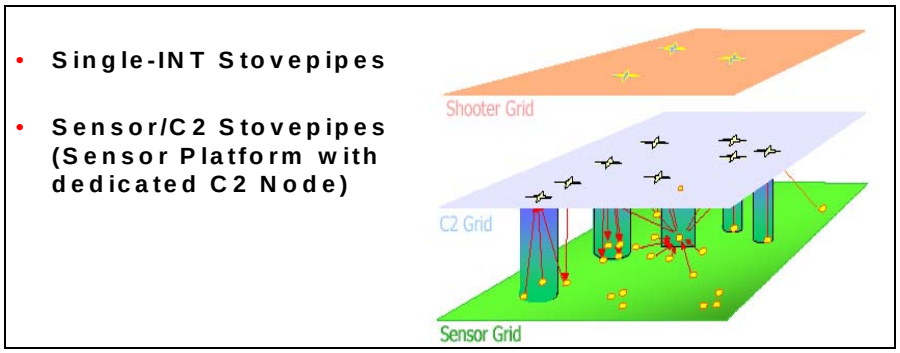


Figure 2-1 Platform-Centric Sensor Grid

In the Naval platform-centric architecture, sensors and weapons have not been used to their full capability. This is illustrated in Figure 2-2, Platform-Centric Engagement Envelope. In this figure, the sensing envelope is represented by the green-shaded circle. The maximum weapons employment envelope is represented by a blue-shaded circle. In platform-centric operations, combat power is projected only when a platform's onboard sensor provides engagement quality data to the weapons system and the target is within the weapon's maximum employment envelope. The effective engagement envelope is the area defined by the overlap of the area where engagement quality data is available and the maximum employment envelope of the weapon. The effective engagement envelope (E^3) is portrayed as the red-shaded area of the diagram. Consequently, the instantaneous combat power for a platform-centric engagement is proportional to the effective engagement envelope. As is apparent from the diagram, in platform-centric operations, combat power is often marginalized by the inability of the platform to generate engagement quality data at ranges greater than or equal to the maximum weapons employment envelope. This situation occurs frequently in platform-

10 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000.

centric air engagements, as a result of the inability of an aircrew to positively identify as friend or foe the objects that they can detect and track at the full range of their sensors[11].

The right-hand-side of Figure 2-2[12] shows that the point in time when a weapon can actually be fired comes later in the sensor-to-shooter timeline than the time when the weapons launch could have made full use of the weapon's maximum range.

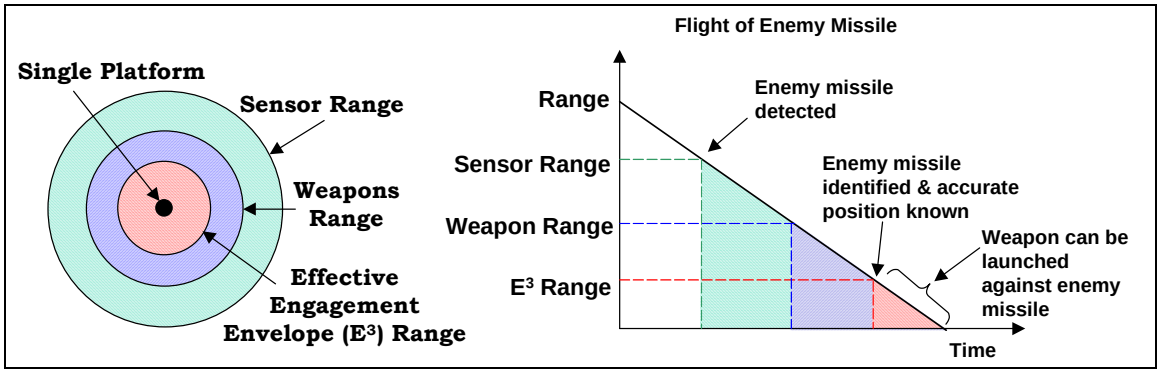


Figure 2-2 Platform-Centric Engagement Envelope

The ultimate goal is to make the transformation from a number of platform-centric sensor systems to a network-centric sensor system. This should provide benefits to the platforms in the battle force such as increased detection ranges, improvements in engagements with less resource depletion, and decreased sensor-to-shooter timelines. Figure 2-3[13] depicts the increase in E^3 with a network-centric sensor system.

11 Network-Centric Warfare by D.S. Alberts, J.J. Garstka, and F.P. Stein, 2nd edition, February 2000

12 Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

13 Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

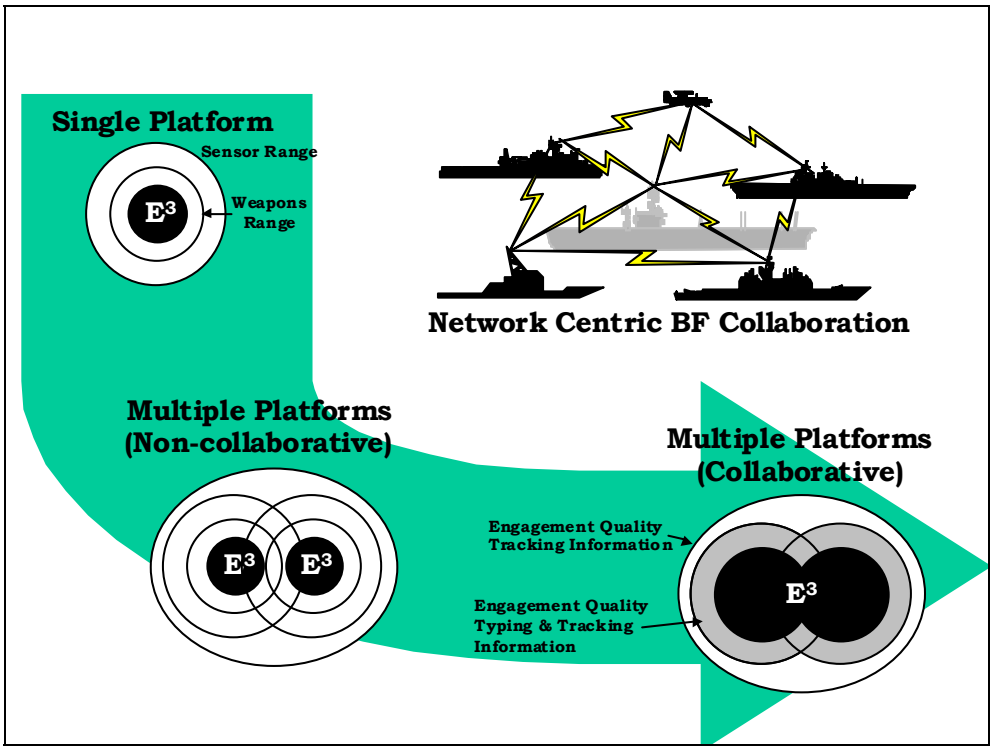


Figure 2-3 The Ultimate Goal

The ultimate grid would network the three grids from the sensor to the shooter grid and would remove the stovepipes in the platform-centric architecture as shown in Figure 2-4[14].

[14] Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

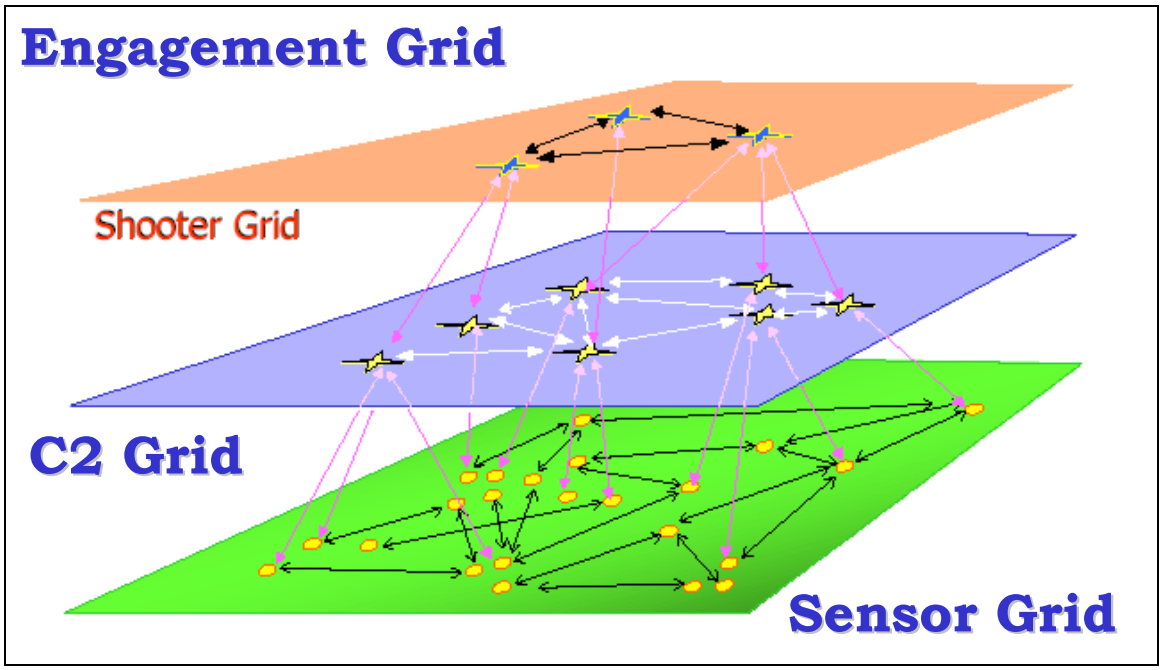


Figure 2-4 The Ultimate Grid

b. Advantages of Network-Centric Sensor system

The following are some examples of the benefits of network-centric sensor system. First, network-centric sensor enables detection of low-signature targets such as submarines shown in Figure 2-5[15]. Low-signature targets are difficult to detect, classify, and engage. By combining sensors and sources in numbers, types, and locations, low-signature targets can then be detected and classified.

15 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000

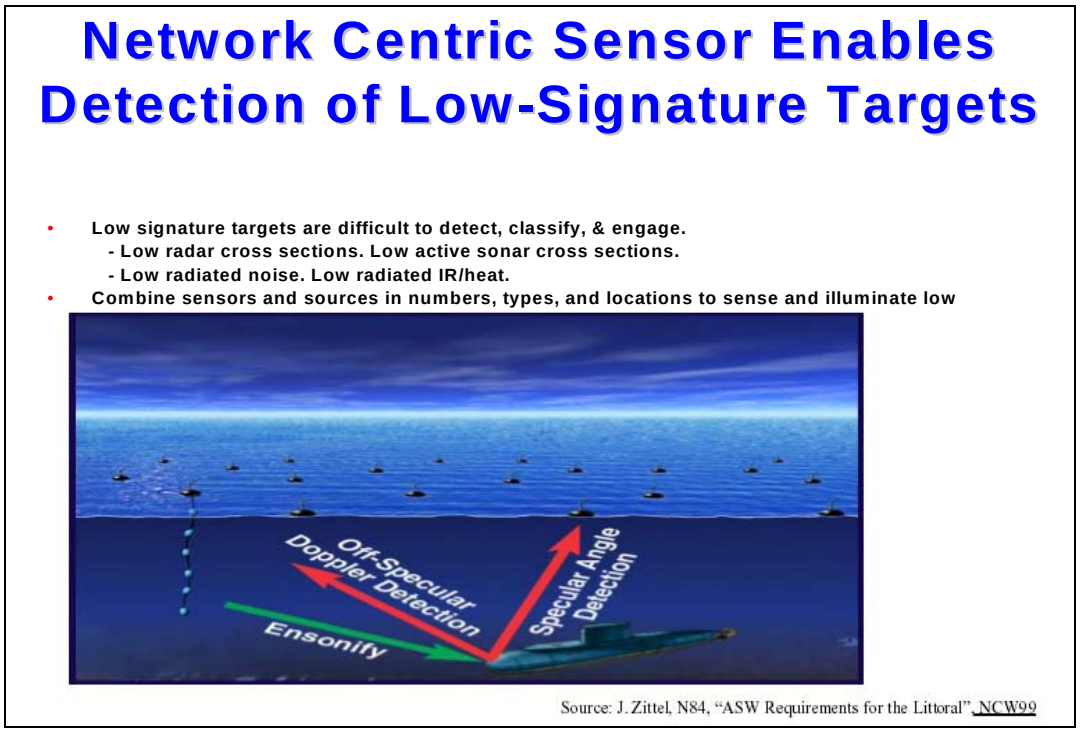


Figure 2-5 Low-Signature Targets Detection Example

The second benefit is that network-centric sensors reduce the area of uncertainty in target tracking as shown in Figure 2-6[16]. As shown in this example, the area of uncertainty for Radar Y and B is shown in the yellow and blue areas around the target. By combining sensors from different positions or with different frequency ranges, the area of uncertainty is reduced significantly as depicted in the green area around the target of Figure 2-6.

16 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000

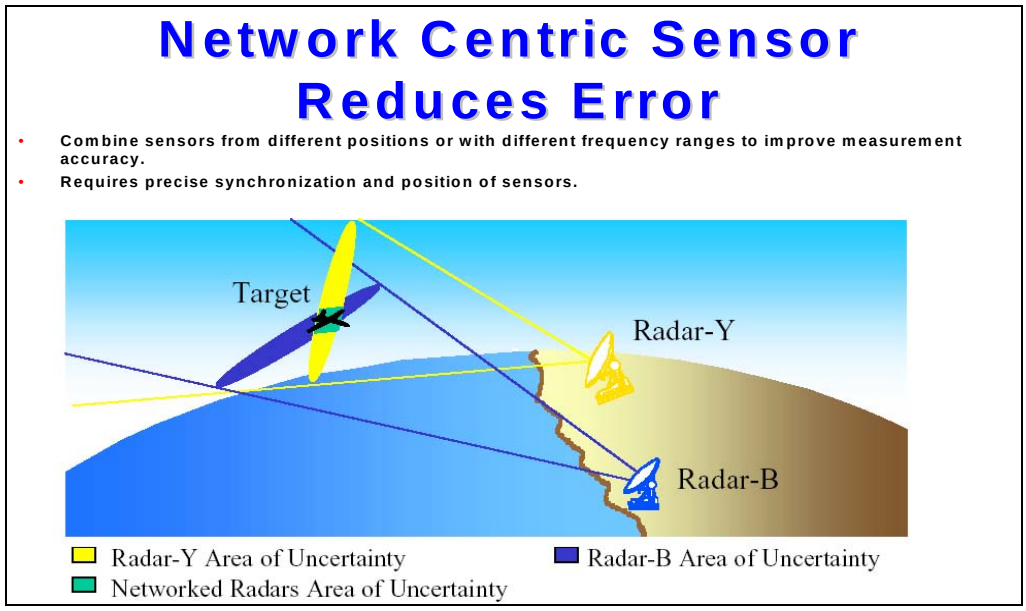


Figure 2-6 Error Reduction Example

Third, network-centric sensor systems improve targeting using sensor data fusion. Certain classes of objects cannot be tracked, located, or identified with sufficient accuracy using a single type of sensor or sensing technique. This deficiency can sometimes be overcome by linking sensors of different types to achieve a multiple source capability. Figure 2-7[17] shows the significant reduction in position uncertainty that is possible with sensor data fusion.

17 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000

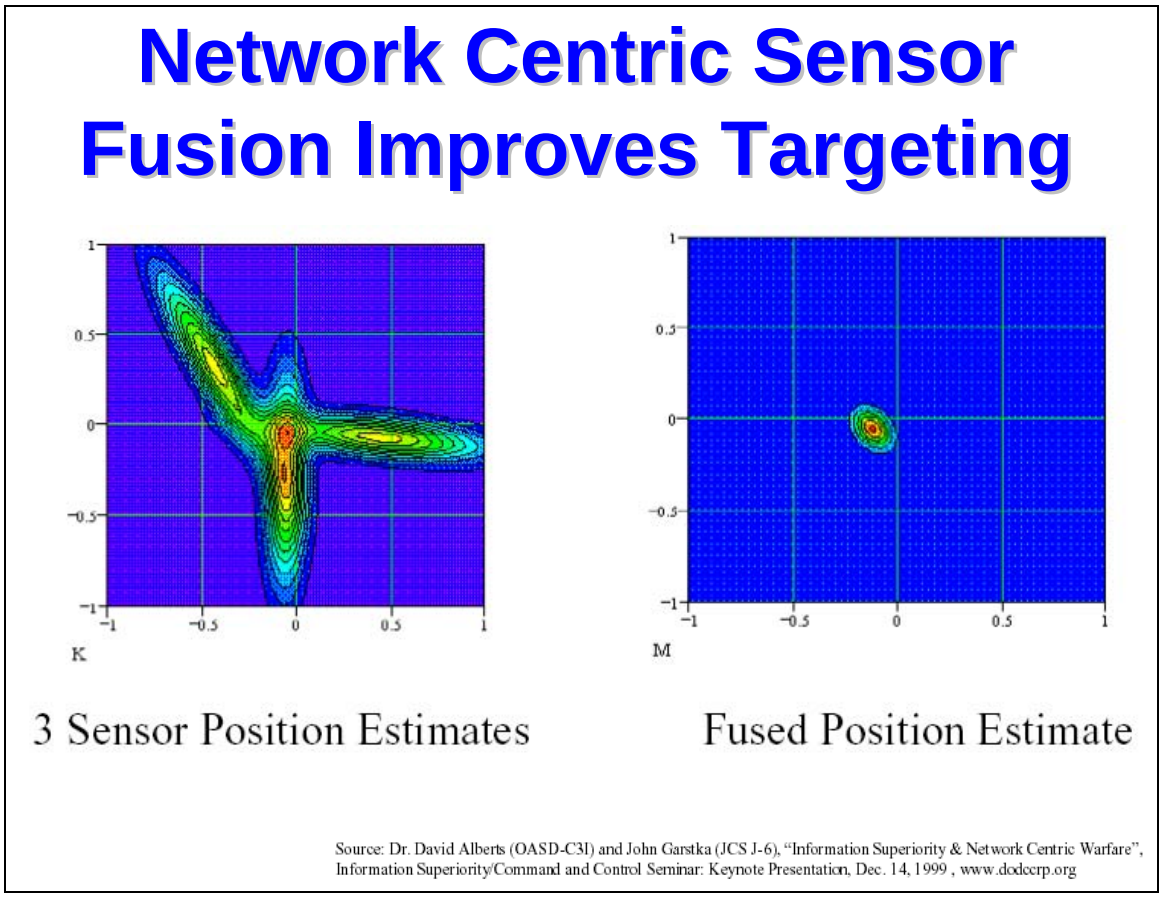


Figure 2-7 Targeting Improvement Example

In addition, sensor data fusion also provides improvement in target tracking as portrayed in Figure 2-8[18]. As shown in this figure, individual stations or elements do not have a complete track picture due to interference such as fade zone, rain, multi-path, jamming, etc. With sensor data fusion, a complete composite track of the target is possible.

18 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000

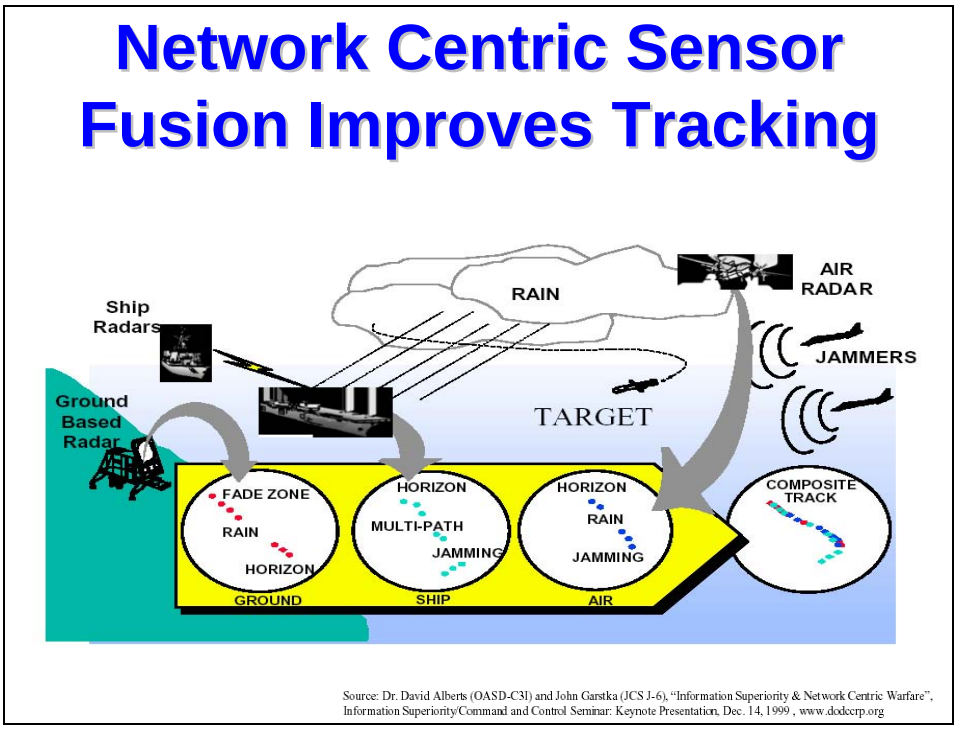


Figure 2-8 Tracking Improvement Example

Fourth, network-centric sensors increase awareness of the battle field. Network-centric sensors enable commanders to rapidly generate battle space awareness and to synchronize operations with platforms in the battle force as depicted in Figure 2-9[19].

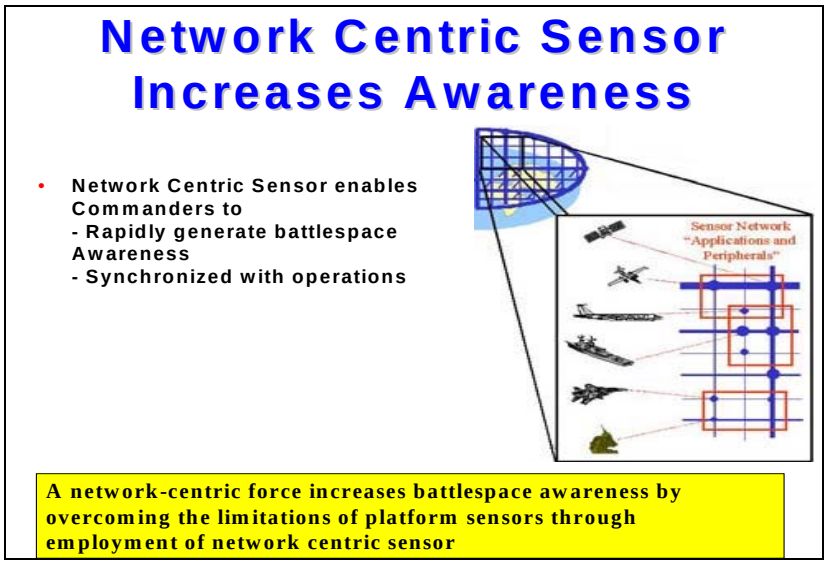


Figure 2-9 Battlespace Awareness Example

19 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000

In summary, network-centric sensors can decrease time to engagement as shown in the time domain plot of Figure 2-10[20]. In addition, network-centric sensors can improve tracking accuracy and continuity, target detection and identification, and extended detection ranges. The robust networking of sensors provides the force with the capability to generate shared awareness with increased quality.

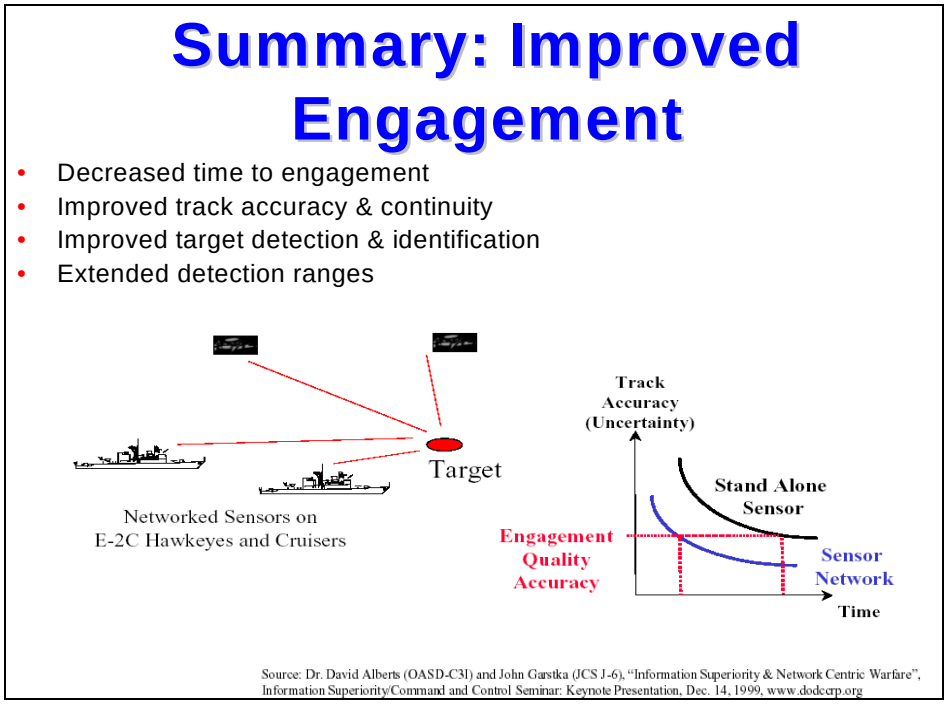


Figure 2-10 Network-Centric Sensor Improvement

c. Enablers for Network-Centric Sensor Concept

The networking of sensor systems from different platforms creates an information architecture in which sensor management can shift to a battle force focus. In such a network-centric paradigm, individual sensors address the need of the battle force as a whole. In order for this to work, there is a need for an automated sensor resource manager that tasks sensors to address battle force needs. Network-centric resource management relies on the achievement of battle force information superiority. Information concerning the tactical battle space and battle force resources must be timely, accurate, and consistent across the battle force in order to enable optimized sensor command and control.

20 Sensor Network for Network-Centric Warfare by John Walrod, Network-centric Warfare Conference, October 30-31, 2000

Enabling a network-centric sensor resource manager requires: an information database, automated link management, and human-machine interaction[21].

(1) Information Database

An information database is the first enabler for a network-centric sensor resource management concept. This information database in turn enables the creation of shared battle space awareness and knowledge. There are three realms of battle force information: the Common Operational Picture (COP), the Common Tactical Picture (CTP), and the Fire control Picture (FCP). Figure 2-11[22] depicts the three realms of information.

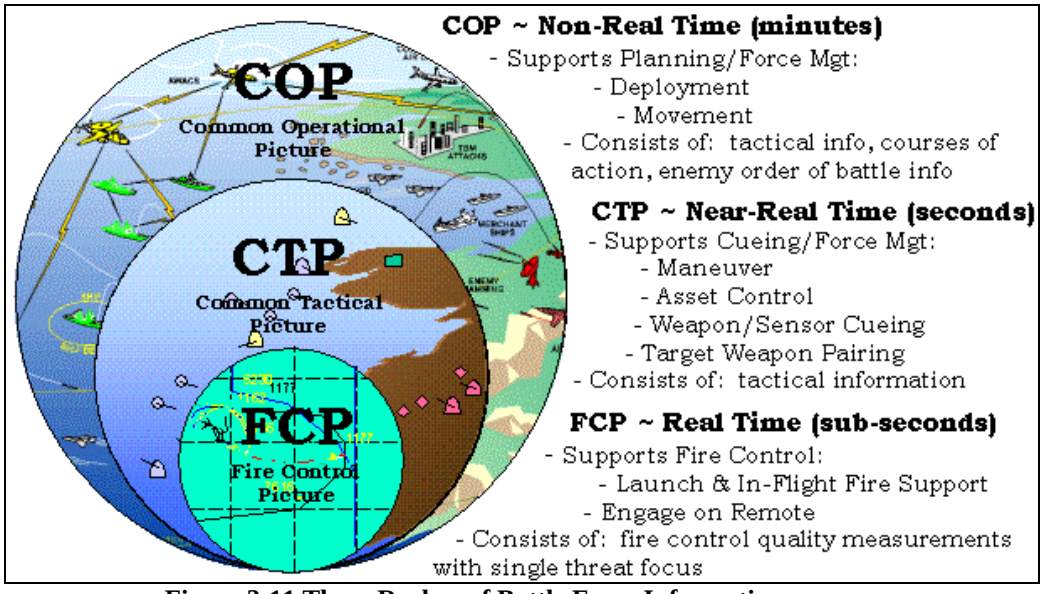


Figure 2-11 Three Realms of Battle Force Information

The COP consists of non-real-time tactical information used for mission planning and force management, such as blue and red Course of Actions (COAs), a priori knowledge of the enemy, and cultural, political, and geographical features. The CTP consists of near-real-time tactical data and information used for cueing and managing battle force resources (such as sensors, communications, and weapons). The FCP is the

21 Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

22 Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

collection of real-time fire control quality data/measurements used to support weapons during launch and in-flight. Information from all these three categories is relevant to the effective and efficient management of battle force resources as well as addressing battle force threats and operations[23].

(2) Automated Link Management

A second enabler for network-centric sensor management is the automated link management for distribution of data throughout the battle force. This automated link management allows for inter-platform data communications and exchange. Due to the bandwidth constraints of the communications devices, the battle force must intelligently distribute data and information between decision nodes based on the needs of the battle force information users, which dynamically change as the operations and missions changes. For example, during remote engagements, the sensor resource manager will require interplatform throughput priority for the FCP data to support the closing of the fire control loop[24].

The automated link management concept is shown in Figure 2-12[25]. As shown in this figure, the Link Interface module handles the necessary protocol for establishing communications with other platforms. In addition, the Link Interface module must also interface with the information database to send and retrieve data from this database to allow synchronization between the platforms in the battle force. Another element of the automated link management is the Link Manager. The Link Manager module handles the following tasks:

1. Determines the needs of the information-recipient users or decision nodes.
2. Keeps track of what data and information is available.

[23] Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

[24] Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

[25] Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

3. Determines the feasibility of transmission (whether the decision nodes are within transmission distance, whether the communication links can support transmission, whether the transmission will support the user's timeline, etc.).
4. Sends commands to other link managers within the BF to control and manage transmissions and transmission modes.
5. Transmits data and information as required.

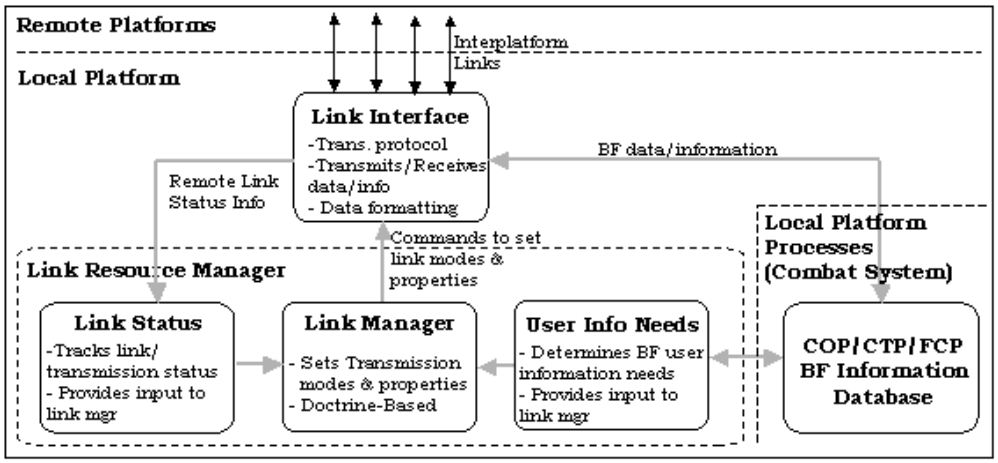


Figure 2-12 Automated Link Management Concept

(3) Human-Machine Interaction

In any system, a human has to be involved in the final decision making. In the sensor system, a human (the operator) forms an integral link in providing feedback between tracking performance and future sensor behavior. With the increasing complexity of information in the network-centric sensor system, the sensor resource management system must process all the information and provide only concise information that allows the operator to make a quick decision and to perform manual override if necessary. This is called the Automatic Sensor System, which provides the following benefits[26]:

1. **Reduced Operator Workload:** Automatic Sensor System alleviates the need for the operator to specify each sensor operation or future behavior. The automated sensor manager is responsible for controlling future sensor behavior while the

[26] Naval Network-Centric Sensor Resource Management by B.W. Johnson and J.M. Green, April 2002

operator exercises control by negation. Hence, the operator's role can simply just provide the following actions: override a track's priority, establish degree of allowable active radiation, request special data collection, etc.

2. **Sensor Tasking based on finer detail:** An operator's control ability is based on information shown on a display and the ability to assimilate information into the human decision- making process. This limits the amount, types, and degree of detail of information feeding the sensor control decisions. On the other hand, automating sensor tasking allows more amounts, types, and finer degrees of detailed information to support the decision-making process.
3. **Faster Adaptation:** Automatic sensor system allows much faster adaptation to the changing environment, i.e., earlier detection of tracking performance degradation.

2. Integrated Fire Control (IFC)

a. Introduction

Integrated Fire Control (IFC) refers to the participation and coordination of multiple non-collocated warfare assets in tactical engagements of enemy targets. IFC is defined as the ability of a weapon system to develop fire control solutions from information provided by one or more non-organic sensor sources; conduct engagements based on these fire control solutions; and either provide mid-course guidance (in-flight target updates) to the interceptors based on this externally provided information or in specific cases, have them provided by a warfare unit other then the launching unit.[27] Table 2-1 highlights the benefits of Integrated Fire Control:[28]

Table 2-1 IFC Benefits

• Selection of the best shooter from a set of geographically distributed weapons
• Improved chance of interception by selecting the optimal engagement geometry

[27] Single Integrated Air Picture (SIAP) Operational Concept document (July 2002)

[28] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

- Improved economy of weapon resources by reducing redundant shots
- Earlier launch decisions are possible through remote detection and precision tracking
- Decoupling of local sensor/weapon pairing constraint
- Sharing engagement control – forward pass
- Off-board engagement support for guidance relay and target illumination
- Enhanced defense against complex threat environments (sophisticated or significant numbers of aerospace targets) – IFC may be a necessity

b. IFC Capabilities

There are a variety of techniques for collaboration between warfare elements in order to execute integrated engagements. Collaboration can be as simple as receiving an early warning cue from a satellite source to the complex collaboration required to pass engagement quality data and control to a remote source. The following paragraphs outline IFC capabilities from an operational construct:

- Precision Cue is an IFC capability where a threat cue from a remote source (sensor, Intel, TADIL, etc.) is received and acted upon by the local combat system. The cue is used to provide the local sensor with acquisition information in order to narrow the search and is typically comprised of general location, track data and/or identification assessment. Figure 2-13[29] below illustrates the precision cue concept.

[29] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

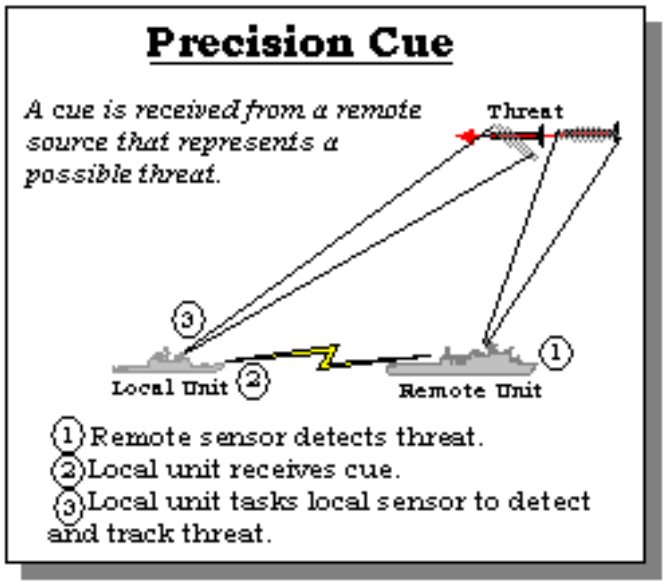


Figure 2-13 Precision Cue

- Launch on Remote (LoR) is an IFC capability that uses a remote sensor to initiate a local missile launch even though the local unit does not hold a local sensor track. LoR is predicated on the local sensor providing in-flight guidance after missile launch. Launch on Composite (LoC) is a close variant where composite data developed from multiple remote sensors is used to initiate the missile launch. Figure 2-14[30] below depicts a LoR scenario where the initial launch is based on remote sensor data with in-flight guidance provided by the shooter.

30 Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

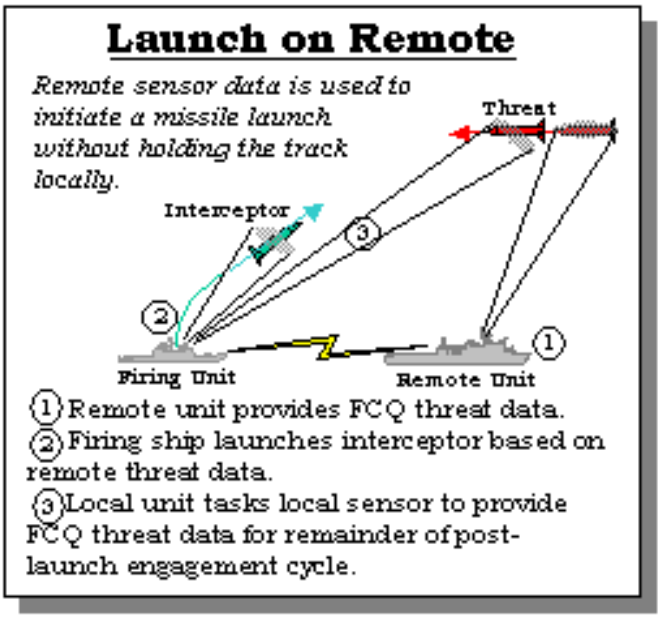


Figure 2-14 Launch on Remote

- Engage on Remote (EoR) is an IFC capability where the remote sensor plays the primary role in providing pre and post launch Fire Control quality sensor data up to and including terminal illumination. Engage on Composite (EoC) is a like variant where composite Fire Control Quality data from multiple remote sensors is used to support missile launch and engagement. Figure 2-15[31] below is illustrative of an EoR engagement scenario.

[31] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

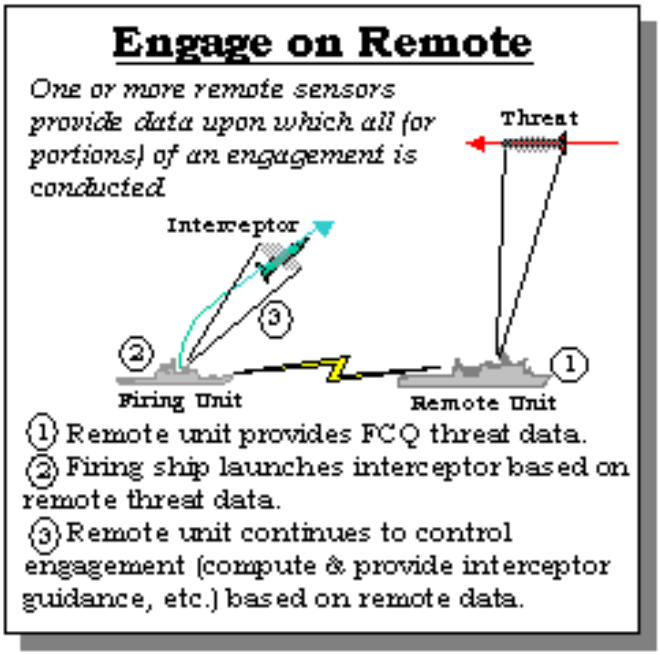


Figure 2-15 Engagement on Remote

- Forward Pass is an IFC capability where in-flight missile control can be transitioned or forward passed to another unit to complete the engagement. Forward Pass is a redundancy technique that allows an engagement to be completed when the originating unit becomes constrained by system limitations or the environment. Forward Pass may also be a tactical technique to exploit an adversary's defense or to gain more refined terminal guidance from a better positioned unit. Figure 2-16[32] below is representative of a Forward Pass scenario where the remote unit assumes control of the in-flight missile.

[32] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

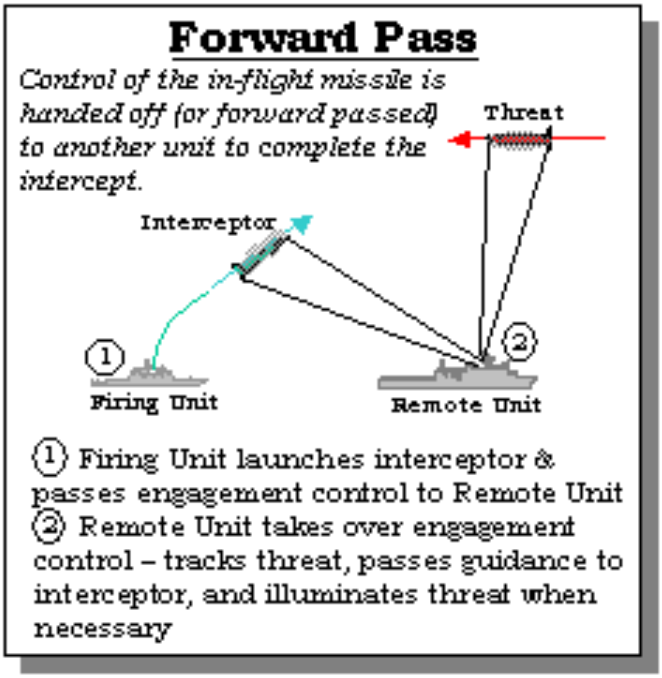


Figure 2-16 Forward Pass

- Remote Fire is an IFC capability where the launch decision is made by the remote unit. After launch, in-flight guidance can be either retained by the remote unit or passed to the local unit. Figure 2-17[33] below is representative of a Remote Fire scenario where the remote unit initiates the launch and retains control of the target engagement.

[33] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

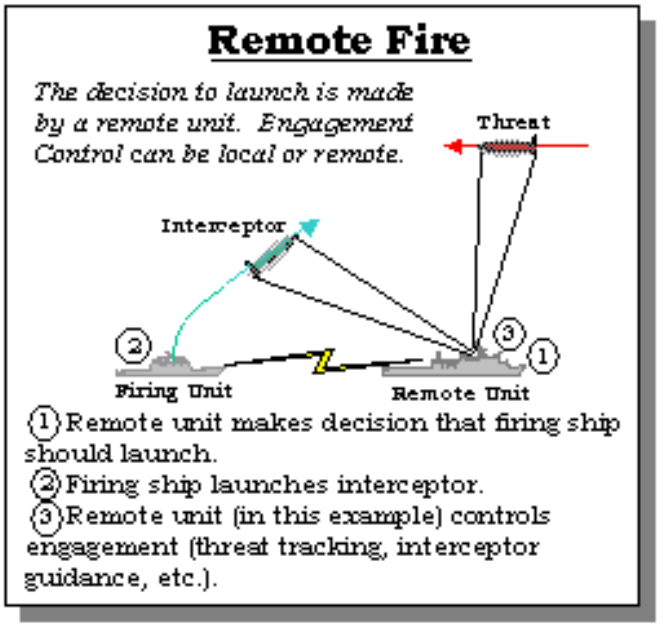


Figure 2-17 Remote Fire

- Preferred Shooter Determination is an IFC capability where the optimum weapon is collaboratively selected from a group of warfare units for target engagement. Optimal geometry and engagement characteristics are used to determine the preferred unit. This capability can be used in parallel with the other IFC capabilities and truly encapsulates, Force-centric weapon-target pairing[34]. Figure 2-18[35] below depicts a Preferred Shooter Determination scenario comprised of five platforms sharing data in a collaborative environment in order to select the optimal platform for threat engagement.

[34] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

[35] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

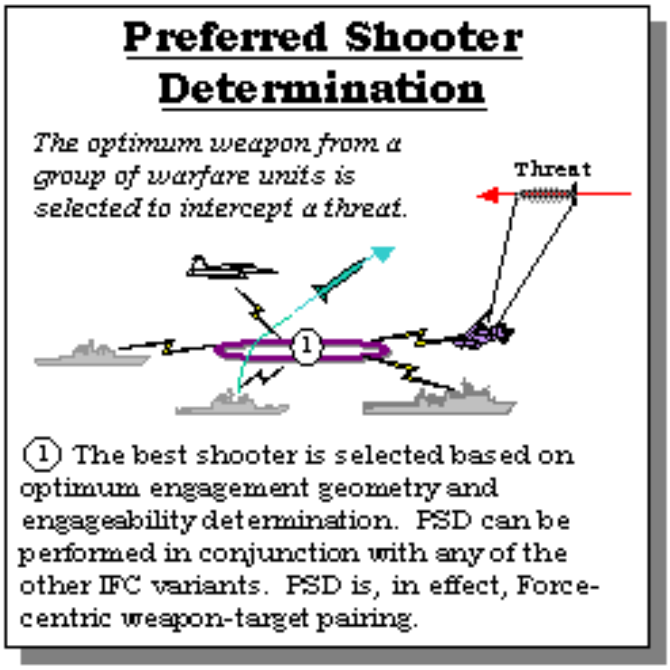


Figure 2-18 Preferred Shooter Determination

c. IFC Process

Figure 2-19[36] below outlines the conceptual IFC flow built on Integrated Architecture Behavior Models (IABMs) that function collaboratively as a distributed system using common processing to facilitate shared situation awareness. The highlighted data fusion blocks (level 1- 4) will be discussed in greater detail later in the Data Fusion section. Table 2-2[37] lists decision products provided by IFC, Automated Management Aids (AMA) and Data Fusion working in a collaborative environment.

[36] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

[37] Young, B. W. (2004). Integrated Fire Control for Future Aerospace Warfare

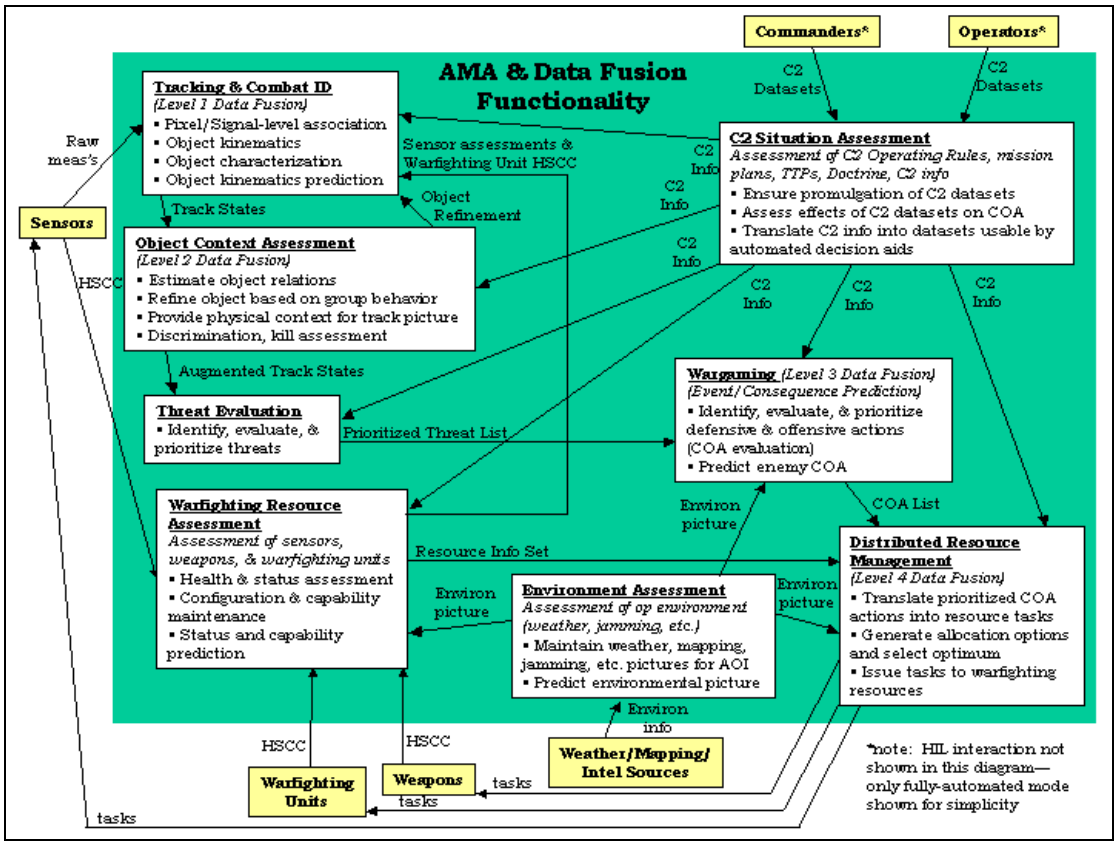


Figure 2-19 Functional IFC

Table 2-2 List of IFC Products

• Preferred shooter determination • Weapon to Target Pairing • Sensor support for engagements • Engagement control strategy (Forward Pass) • Engagement preferences

3. Global Information Grid (GIG)

a. Introduction

The Global Information Grid (GIG) provides the ability to organize, transform, and manage information technology (IT) throughout the DoD. GIG policy, governance procedures, and supporting architectures are the basis for developing and evolving IT capabilities, IT capital planning and funding strategies, and management of legacy (existing) IT services and systems in the DoD. In discussing the GIG and how a

particular program interacts with, supports, or relies upon the GIG, it is useful to think of the GIG from three perspectives – its vision, its implementation, and its architecture.

b. Overview

In the Department of Defense (DoD) Directive 8100.1, the GIG and its assets are defined as:

> The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, 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 as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, national security, and related intelligence community 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[38].

c. Vision

The vision of the GIG is to enable users, in any conditions and with attendant security, to have easy access to information at anytime and anyplace. Program managers, sponsors and Domain Owners can use this vision to help guide their acquisition programs. This vision requires a comprehensive information capability that is global, robust, survivable, maintainable, interoperable, secure, reliable, and user-driven. The goal is to increase the net-centricity of warfighter, business, intelligence, DoD enterprise management, and enterprise information environment management operations. Making these operations more network-centric will increase information access by GIG users, provide the information and expertise to support operational decisions, allow more rapid access to vital information, and will provide information to tactical edge users in any theater.

38 Department of Defense (DoD) Directive 8100.1

d. Mission

The mission for the GIG is to provide assured net-centric end-to-end services seamlessly in support of the DoD's full spectrum of warfighting, intelligence, and business missions. The objective of net-centric services is to ensure that information flow can be optimized and quickly accessed by decision makers. Rapid access to timely information will help theater decision makers to more effectively carry out their mission. The effectiveness of the GIG will be measured in terms of availability and reliability of net-centric services, across all domains, in compliance with specified service levels and polices. The method for service assurance in a net-centric collaborative environment is to establish operational thresholds, compliance monitoring, and a clear understanding of the capabilities between enterprise service/resource providers and consumers through Service Level Agreements (SLAs).

e. Description

As stated in Joint Vision 2020 (JV2020), the demand for the GIG has been driven by the requirement for information and decision superiority to achieve full-spectrum dominance. JV 2020 also highlights the importance of a Net-Centric Warfare environment, which is enabled by the GIG to improve information sharing through the robust networking of warfighting forces. The Joint Staff prepared a pamphlet called *Enabling the Joint Vision* that envisions the GIG as:

- A single, secure grid providing seamless end-to-end capabilities to all warfighting, national security, and support users
- Supporting DoD and Intelligence Community (IC) requirements from peace time business support through levels of conflict
- Joint, high-capacity netted operations
- Fused with weapons systems
- Supporting strategic, operational, tactical, and base/pots/camp/station
- Plug-and-play interoperability
- Guaranteed for United States and Allied forces
- Connectivity for Coalition users
- Tactical and functional fusion a reality

- Information/bandwidth on demand
- Defense in depth against all threats

To ensure that systems that constitute and use the GIG interoperate in a net-centric manner, the OASD(NII)/DoD CIO prepared the "Net-Centric Checklist" (12 May 2004, Version 2.1.3), which requires programs to address the following issues:

- Ensuring that data are visible, available, and usable when needed and where needed to accelerate decision making.
- Tagging of all data (intelligence, non-intelligence, raw, and processed) with metadata to enable discovery of data by users.
- Posting of all data to shared spaces to provide access to all users except when limited by security, policy, or regulations.
- Advancing the Department from defining interoperability through point-to-point interfaces to enabling many-to-many exchanges typical of a network environment.

The GIG Net-Centric Information Document (NCID) is a compilation of the enterprise-level functionality that must be achieved if GIG programs are to satisfy the policy and technical directives contained in these documents and the needs of the users as described in the GIG Mission Area Initial Capabilities Document (MA ICD).

f. Global Information Grid (GIG) Enterprise Services (GIG ES) Capability Development Document

The GIG ES Capability Development Document (CDD) focuses on nine enterprise services provided by the Net-Centric Enterprise Services (NCES) Program. The Defense Information Systems Agency provides these enterprise services to establish the foundation for the initial net-centric capabilities. The Global Information Grid Core Enterprise Services Strategy Document[39] describes the overall set of services in detail.

The NCES program will develop the core enterprise services incrementally. Each program that is dependent upon the core services being developed by the NCES program should address the impact of the incremental NCES schedule on

[39] Global Information Grid (GIG) Core Enterprise Services Strategy document can be found at http://www.defenselink.mil/nii/org/cio/doc/GIG_ES_Core_Enterprise_Services_Strategy_V1-1a.pdf

their program. The Net-Centric Operations and Warfare Reference Model (NCOW RM) provides a basis for discussing issues associated with these core services. The table below (Table 2-3) shows the relationship of the nine Core Services articulated in the GIG ES Capability Development Document to the services articulated in the NCOW RM.

Table 2-3 Mapping of GIG ES/NCES Core Services to Net-Centric Operations and Warfare Reference Model Services

GIG ES Capability Development Document/NCES	NCOW RM Activity
Application	A316 (Provide Applications Services)
Collaboration	A312 (Provide Collaboration Services)
Discovery	A311 (Perform Discovery Services)
Enterprise Services Management/NetOps	A33 (Environment Control Services) and A5 (Manage Net-Centric Environment)
Information Assurance/ Security	A33 (Environment Control Services) and A5 (Manage Net-Centric Environment)
Mediation	A314 (Perform Information Mediation Services)
Messaging	A313 (Provide Messaging Services)
Storage	A315 (Perform Information Storage Services)
User Assistance	A2 (Perform User Agent Services)

g. Compliance with the Global Information Grid (GIG)

Compliance with the GIG means that an information technology-based initiative or an acquisition program demonstrates compliance in the following areas:

1. **DoD Architecture Framework (DoDAF)**[40] – Identifying and meeting the requirement in order to produce the architectural products. A complete integrated architecture can be developed using the specified products described in the

[40] DoD Architecture Framework (DoDAF) found at http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf

DoDAF document. This document can assist in generating requirements such as capability definition, process re-engineering, investment decisions, and integration engineering.

2. **Core Architecture Data Model (CADM)**[41] – Using the CADM architecture data, this would enable developing integrated architecture.
3. **DoD Information Technology Standards Registry (DISR)**[42] **–** Enabling GIG users to meet requirements in selecting technologies and standards. This requirement is met by defining and implementing capabilities, based on technologies and standards contained within the JTA/DISR. Meeting this requirement should be validated at every milestone.
4. **DoD Net-Centric Data Strategy**[43] - Providing the associated metadata, and defining and documenting the program's data models can be met by:
    a. Describing the metadata that has been registered in the DoD Data Metadata Registry for each data asset used and for each data asset produced (i.e., data for which the program is the Source Data Authority).
    b. Providing the documented data models associated with the program.
5. **GIG Capstone Requirements Document**[44] **(CRD) -** Using this document to verify an overall degree of conformance and to identify and address issues and risks.
6. **Use of Standards** – Enforcement of IT and architecture standards is an essential element for achieving interoperability across the GIG.
    a. **Compliance.** GIG systems should be implemented in accordance with the latest versions of the *DoD JTA*[45] unless waived in accordance with the

41 Core Architecture Data Model (CADM), *Baseline Version 1.1* is the current official version of the CADM as published by DoD. There have been several versions of this model since 1996 until it was placed under configuration control in 2003.
http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/116.pdf

42 DoD Information Technology Standards Registry (DISR) found at https://disronline.disa.mil/DISR/index.jsp

43 DoD Net-Centric Data Strategy found at http://www.defenselink.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf

44 GIG Capstone Requirements Document found at http://handle.dtic.mil/100.2/ADA408877

45 DoD JTA found at http://www.tricare.osd.mil/policy/tma00/techarch.htm

waiver process described in DoDI 5000.2-R[46]. Systems that are part of host nation and bilateral agreements should be checked for their ability to interface with the GIG.

b. **Interoperability Testing and Certification.** Interoperability testing and certification should be addressed as an integral part of the requirements generation process prior to production, fielding, and life cycle support, as required, of GIG systems regardless of ACAT level, in accordance with CJCSI 6212.01B[47].

c. **Technology Insertion.** The GIG should apply open-system design strategies to enable the insertion of new and emerging technologies while maintaining interoperability with existing GIG systems and architectures. However, emerging technologies, for which standards do not exist, may be incorporated with an appropriate waiver to the JTA, only if they can integrate in a seamless and efficient manner (i.e., without compromising interoperability or GIG functionality requirements). Such JTA-waived technology insertions should be reviewed for feasibility of replacement with standards-based technology when appropriate.

d. **Data Standards.** All GIG systems should support standardized semantic tagging of data, unless it is not feasible to do so (such as may be the case with certain legacy systems). Both the syntax and semantics of GIG data and semantic tagging mechanisms should comply with applicable DoD standards. In cases where standards do not exist for a class of data, the developer should unambiguously define the syntax and semantics.

4. Tactical Data Links

A portion of the analysis performed for this project was to quantify the benefits of Coalition participation in FORCEnet. The statement of work (SOW) and scenario description provided descriptions of the various Coalition FORCEnet participation levels

46 DODI 5000.2-R found at http://exploration.nasa.gov/documents/TTT_052005/DoD50002R.pdf

47 CJCSI 6212.01B found at http://www.army.mil/howwewillfight/references/9%20CJCSI.pdf

to facilitate comparisons. In one of the options, the battle force is evaluated when the Coalition Forces are at FORCEnet level zero. Level zero is defined in the following manner:

> No FORCEnet. Vessels use voice radio and Link 11 or 16 to share situational awareness and C2 data. Platform-centric in character.

While the SOW defines tactical data link operations as no FORCEnet, other documents, such as the the Naval Transformation Roadmap (NTR), describe a role for the tactical data links in FORCEnet. This section describes the role of tactical data links in FORCEnet.

The FORCEnet portion of the NTR contains a section entitled *Transformational Network Concepts and Capabilities – Near-and Mid-Term (2005-2015).*[48] This section contains the following paragraph:

> Naval forces have unique mobility requirements that limit access to available network capacity, despite rapid technology advancements. The FORCEnet communications and network architecture includes alternative communications paths for essential networks to provide the required operational throughput to the warfighters. The centerpiece is the global secure, interoperable family of afloat and ashore IP networks. Allied and Coalition networks will be included within this federation through connectivity provided via various gateways and guards, both afloat and ashore. Non-IP Tactical Data Link networks will be included in the federation through the creation of a gateway. Critical warfighting information, such as track data, will be able to flow seamlessly between the IP network infrastructure and the tactical links.[49]

In the role described by the NTR, gateways will allow data to flow between tactical data links and the FORCEnet communications network. In this capacity, tactical data links will be capable of supporting FORCEnet in the following areas:

- Supplementing the common operating picture and common tactical picture by providing: information such as intelligence, imagery, surveillance data, weather, threat warnings, etc.

---

48 Naval Transformation Roadmap 2003 Assured Access & Power Projection From the Sea (Department of the Navy, [2003]), 65.

49 Naval Transformation Roadmap 2003 Assured Access & Power Projection from the Sea (Department of the Navy, [2003]), 66.

- Providing a backup for the FORCEnet communications network for those functions that are supported by the tactical data links. Functions such as exchanging real-time targeting information are not supported by the tactical data links and will not be available, but providing a lesser quality common tactical picture will be supported.
- Providing tactical data link formatted information, such as J-series messages, to legacy systems on the GIG.
- Providing a data path from the GIG to tactical data link equipped legacy platforms. GIG nodes could reach these legacy platforms with information such as free text, imagery, or intelligence data.

5. Joint Track Manager

a. Introduction

The Joint Track Manager (JTM) is a key component of the Cooperative Engagement Capability (CEC) system. The JTM function is to create a common operation picture of sufficient quality to support fire control application for each combat control system. JTM attributes consist of integrating track picture, providing high quality track data with low distribution latencies, sensor-to-weapon thread management, multi-dimensional (not warfare domain specific), and common communications links. To achieve optimum interoperability across the battleforce, the JTM consist of sensor measurement fusion and track management algorithm solutions. In the article, "Open Architecture: The Critical Network-Centric Warfare Enabler[50]", identifies the JTM is a key component in supporting the re-architecting of battle force functionality in order to support the Navy's Open Architecture functional architecture. The Navy's Open Architecture vision is to establish a common functional framework across Navy programs and platforms to reduce development cost by promoting software reuse and to promote interoperability by allowing functionality to be consistently engineered across the battleforce.

Several organizations have been tasked to define a Joint Track Management (JTM) Architecture which supports different approaches for processing

[50] Captain Richard T. Rushton, U.S. Navy, Open Architecture: The Critical Network-Centric Warfare Enable, http://kcg-inc.net/OPNAV_766/open_architecture_proceedings.htm

sensor measurement, attributes, and track related data which forms and identifies tracks. The JTM must also be able to support data communication over diverse communications channels into different host systems in order to achieve a common tactical track picture, and to provide data exchange architecture to integrate the Common Tactical Picture (CTP) and Common Operational Picture (COP). The JTM (see Figure 2-20[51]), besides registering and managing vehicular track information, consists of core common services which allows it to fused data from different sources, manage and task resources (weapons and sensors), ensures all JTM platforms behave alike, and allows for the discovery of movement patterns.

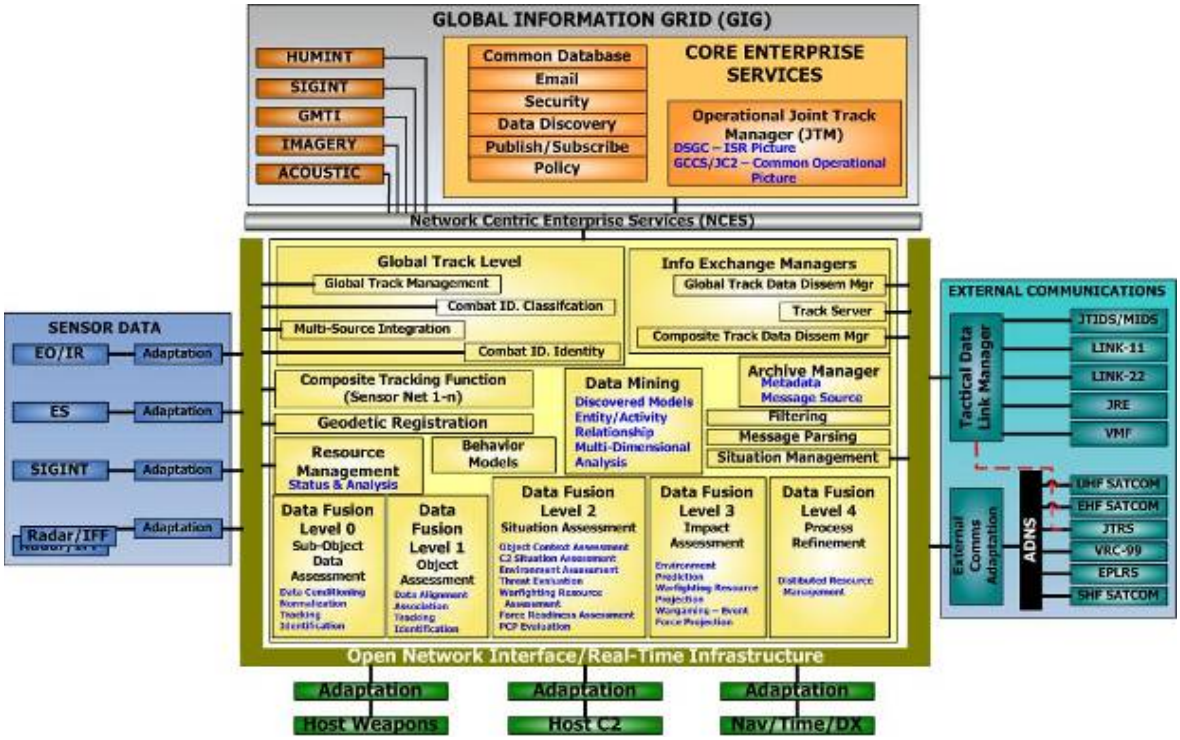


Figure 2-20 Joint Track Manager

Young's article, *"A C2 System for Future Aerospace Warfare[52]"*, summarizes the Single Integrated Air Picture (SIAP) distributed system, which lays the foundation upon which advanced forms of Joint C2 are built. Young states, "*Advanced forms of collaboration among distributed Joint warfighting units require a basic NCW foundation comprised of an information architecture that promotes information sharing*

51 Open Architecture Track Manager/Joint Track Manager Brief; given by Capt J.M. "Ike" Locovetta, diagram was modified to include other enabling technologies, reference slide 7

52 A C2 System for Future Aerospace Warfare, Bonnie W. Young

among distributed units and processing resident at each unit to enable shared knowledge." To accomplish this, Young's article presents advanced concepts such as SIAP distributed system, data fusion, distributed resource management, integrated architecture behavior model (IABM). This section summarizes Young's advanced concept.

b. SIAP Distributed System

The SIAP Distributed System is composed of a network of distributed Peer Computing Programs (PCPs) interacting in a collaborative manner over the Peer-to-Peer (P2P) network. The SIAP concept (Figure 2-21[53]) illustrates multiple peers interacting in the context of an operational scenario. Figure 2-21 also shows these peers interfacing with external non-SIAP entities. An individual peer is shown as a single PCP and associated warfare resources.

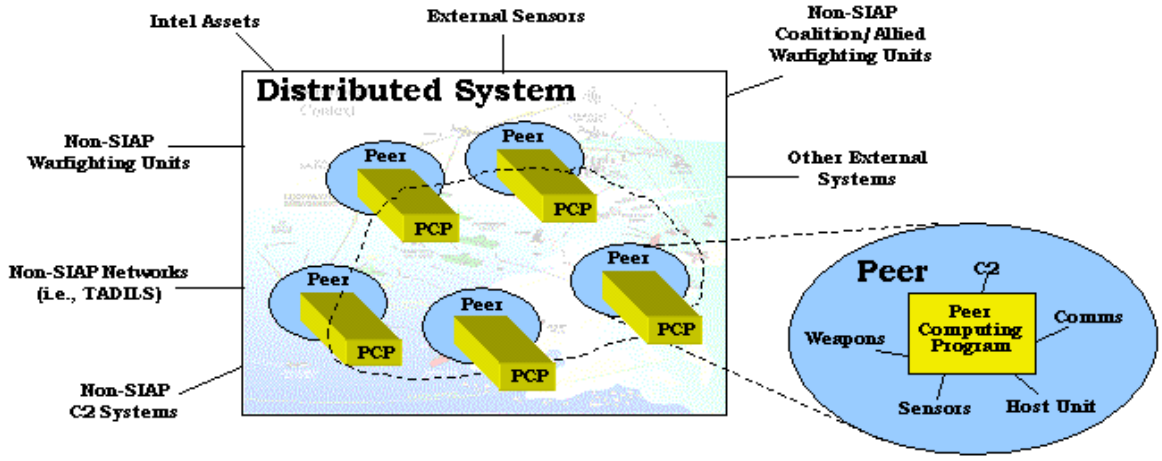


Figure 2-21 SIAP Distributed System Context Diagram

In the SIAP concept, each PCP will use common processing techniques including common computational methods and algorithms. Since each PCP is provided with identical data inputs and uses common processing, each will produce the identical picture, assessment, and decision results (see Figure 2-22[54]). These identical pictures are

53 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

54 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

derived from real time and near real time data, and consist of correlated track objects and associated information (such as Combat Identification (CID) information). The PCP system fuses real-time and near real-time data to support situation awareness, battle management, and target engagement. The core capabilities of the PCP system include target detection, target tracking, and target identification. The core functions are responsible for: receiving and transmitting sensor measurement data, processing the sensor data to generate the single integrated air track picture, and making CID determinations for each track object in the identical picture.

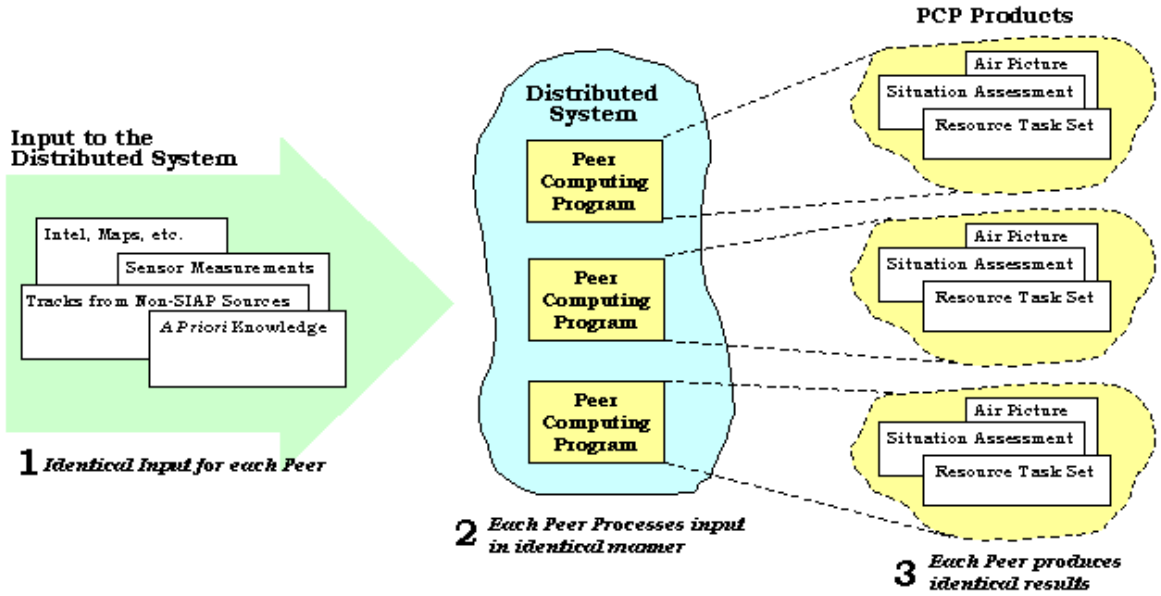


Figure 2-22 SIAP Common Processing Concept

Figure 2-23[55] shows the external interfaces of a single PCP unit. PCPs interface with a warfighting unit's resident sensors, weapon systems, relevant operator displays, and C2 systems. PCPs interact with each other over the Peer-to-Peer (P2P) network communications architecture. PCPs communicate with legacy systems (warfighting units without PCPs, C2 systems, etc.) over tactical data links.

[55] Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

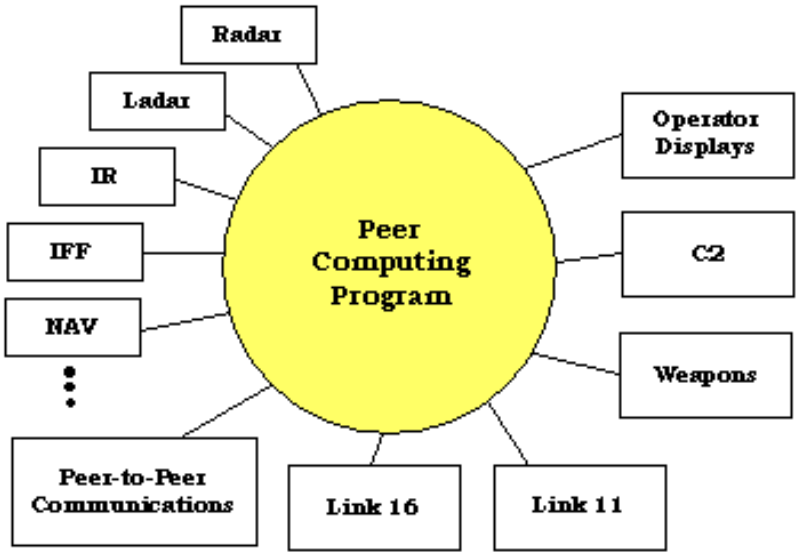


Figure 2-23 PCP Context Diagram

The PCP core architecture processing flow is illustrated in Figure 2-24[56]. The track management function is capable of fusing data from several different sources including peer-to-peer networks, tactical data links (Link-11/Link-16), and sensors and is designed to reduce the likelihood of dual tracking, track blooming, and tracking conflicts.

56 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

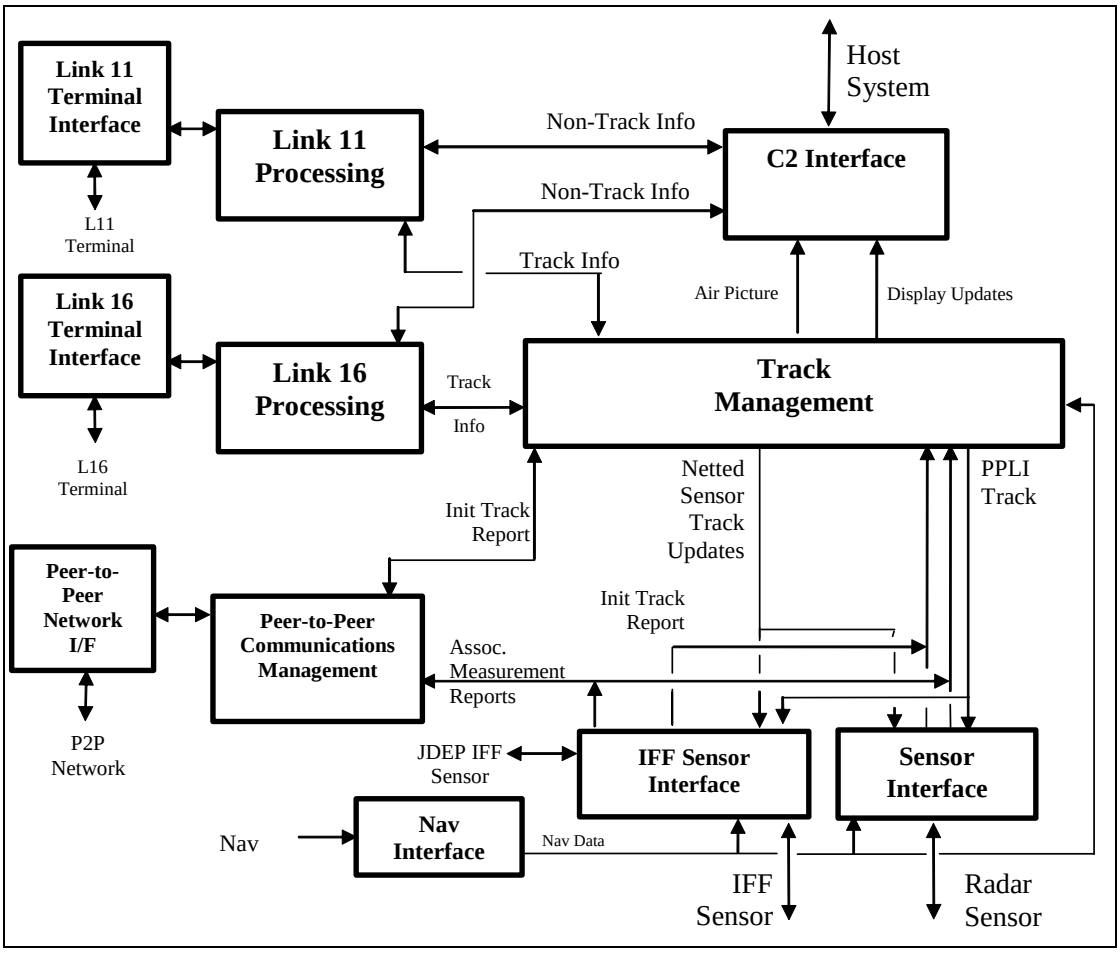


Figure 2-24 PCP Core Architecture

The two key PCP capabilities that support future Joint C2 concepts are:

1) To automate the composition of a shared, accurate, and complete situational awareness picture
2) To automate the decision-making process involved in most effectively managing warfare assets (resources).

c. Data Fusion

The Data Fusion model was originally introduced by Joint Directors of Laboratories (JDL) in 1991. Data Fusion is defined as the process of combining data to refine state estimates and predictions. The JDL data fusion model illustrates the primary functions, relevant information and databases, and interconnectivity necessary to perform data fusion. JDL further defines data fusion as a "multi-level, multifaceted process

dealing with the automatic detection, association, correlation, estimation, and combination of data and information from single and multiple sources ". The word "multi-level" refers to the five levels of data fusion in the functional model as shown in Figure 2-25[57].

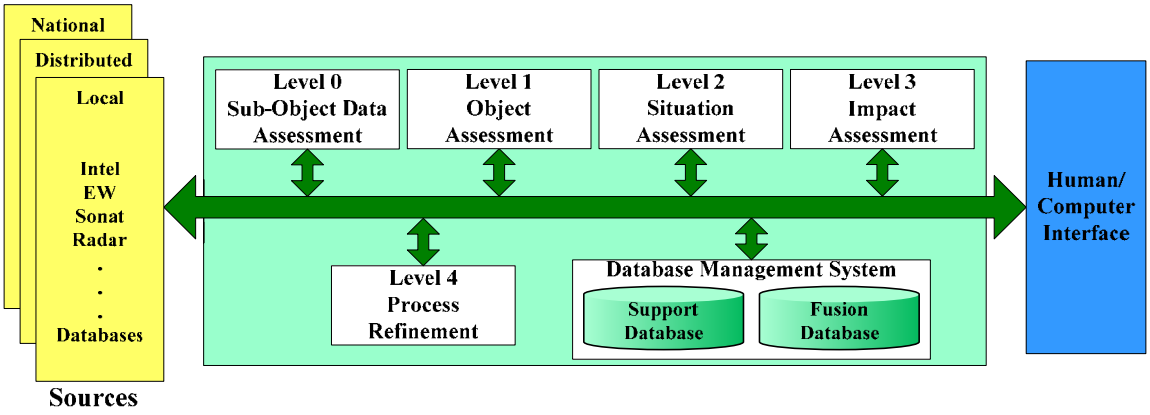


Figure 2-25 Data Fusion - 5 Levels

The definitions of JDL's five levels of Data Fusion Model are provided in the bullets below.

- (Level 0) Sub-Object Data Assessment and Estimation: pixel/signal level data association and characterization.
- (Level 1) Object Assessment: observation-to-track association, continue out state estimation (e.g. kinematics) and discrete state estimation (e.g. target type and ID) and prediction. At this level, fused data is used to determine the identity and other attributes of entities. The term entity refers here to a distinct object. A track is usually directly based on detections of an entity, but can also be indirectly based on detecting its actions. The product from this level is called the situation picture. That is, Level 1 tries to determine the what (identification), where (position) and when (time) of a detected object. Level 1 is usually partitioned into four functions: data alignment, association, tracking and identification (Hall, 1992). The data alignment function is used to project data into a common reference frame. Association tackles the problem of sorting or

[57] Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

correlating observations into groups, with each group representing data related to a single entity. Tracking refers to the estimation of the position and velocity of the entity. Identification seeks to better describe the entity.

- (Level 2) Situation Assessment: object clustering and relational analysis, to include force structure and cross force relations, communications, and physical context, etc. The iterative process of fusing the spatial and temporal relationships between entities to group them together and form an abstracted interpretation of the patterns in the order of battle data.
- (Level 3) Impact Assessment: threat intent estimation, event prediction, consequence prediction, susceptibility and vulnerability assessment. At this level, iterative process of fusing the combined activity and capability of enemy forces to infer their intentions and assess the threat that they pose. The product from this level is called the threat assessment.
- (Level 4) Process Refinement: adaptive search and process (an element of resource management), tasking. Level 4 performs "process refinement", which is an ongoing monitoring and assessment of the fusion process to refine the process itself and to regulate the acquisition of data to achieve optimal results (Klein, 1993)[58]. Level 4 interacts with each of the other levels.

Figure 2-26 shows how objects flow through the levels of Data Fusion. At level 0, objects, depicted as alerts, are picked up and processed by sensors. The object information is then passed to the feature extraction process (level 1) for identification. The pattern processing then determines the intent of the object by comparing it against known patterns. The information is then analyzed in the situation assessment process (level 2) and finally passed to the decision making process (level 3).

[58] L. A. Klein. Sensor and data fusion concepts and applications. Tutorial texts, vol. TT 14, SPIE Optical Engineering Press, USA, 131 p., 1993

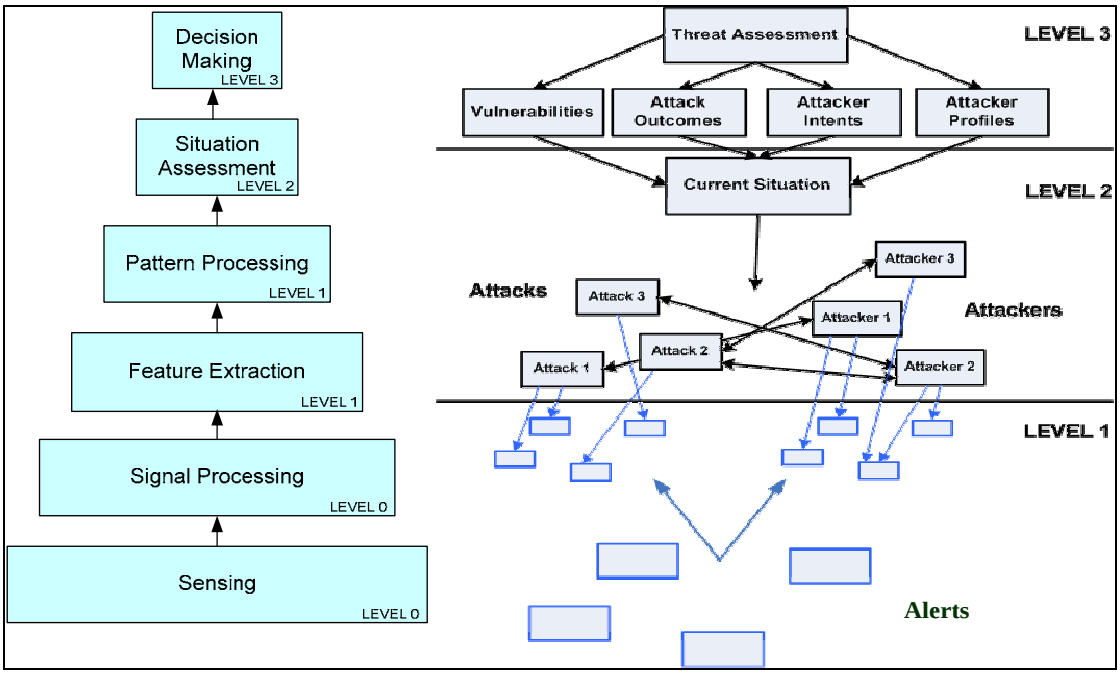


Figure 2-26 Data Fusion Levels 0-3

The diagrams and descriptions in the previous paragraphs cover the levels of data fusion in the JDL model. One important aspect of using the model is to understand that not all functions at each level are used in every evaluation. For example, if a detected object undergoes object assessment/feature extraction during level 1 data fusion, it is certainly possible to make a threat assessment and determine a course of action without performing any pattern processing. One should not infer that there is a rigid structure to performing data fusion where all activities of a lower level must be completed prior to moving to the next level.

(1) Functional Requirements

Figure 2-27[59] shows the flow of the JDL Data Fusion Model. The figure shows entities external to the peers such as sensors, weapons, decision-makers, Intel/weather data sources, and the other warfighting units. The diagram does not show communications interfaces or peer functionality involved in communications.

Beginning with the sensors, raw measurement data is passed to both the tracking and combat ID function and the warfighting resource assessment function. The objective

[59] Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

of the tracking and combat ID (CID) function is to assess the kinematics and other characteristics of detected objects. Once enough information is obtained for the object (kinematics, characterization, and kinematics prediction), it is then passed to the object context assessment function as a real track. The tracking and CID functions constitute levels 0 and 1 in the JDL fusion model.

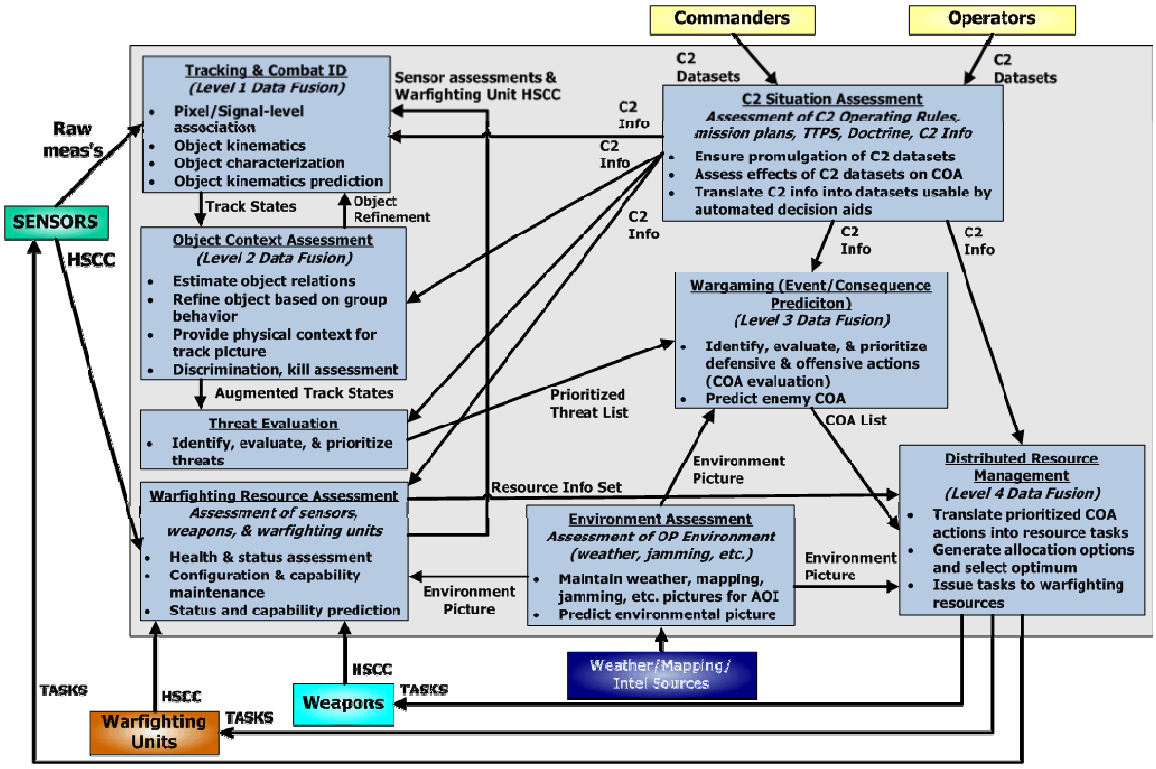


Figure 2-27 Data Fusion Process

Several of the function sets shown in Figure 2-27 provide situational awareness—object context assessment, threat evaluation, warfighting resource assessment, environment assessment, wargaming, C2 situation assessment, and Distributed Resource Management. These functions support the development of a higher level of awareness of the operational situation by fusing or associating non-kinematic data sets with the track picture.

(a) Data Fusion (Level 2) Situational Assessment

Bonnie Young, in her article, "A C2 System for Future Aerospace Warfare[60]", provides detailed information on the JDL Data Fusion Process. This section summarizes the key points about data fusion from Young's article.

Situational Awareness (SA) is the act of understanding the totality of the tactical situation, including the threat, the defended assets, the readiness of warfighting resources, and command and control constraints within which the systems must operate. There are various aspects of the operational situation (see Figure 2-28[61]) that comprise SA. Each peer will effectively create and maintain a "picture" of each of these aspects including a track picture, object context, threat picture, defended assets picture, warfighting resources, environment picture, and the C2 situation. The pictures are really sets of information that are products of the data fusion process.

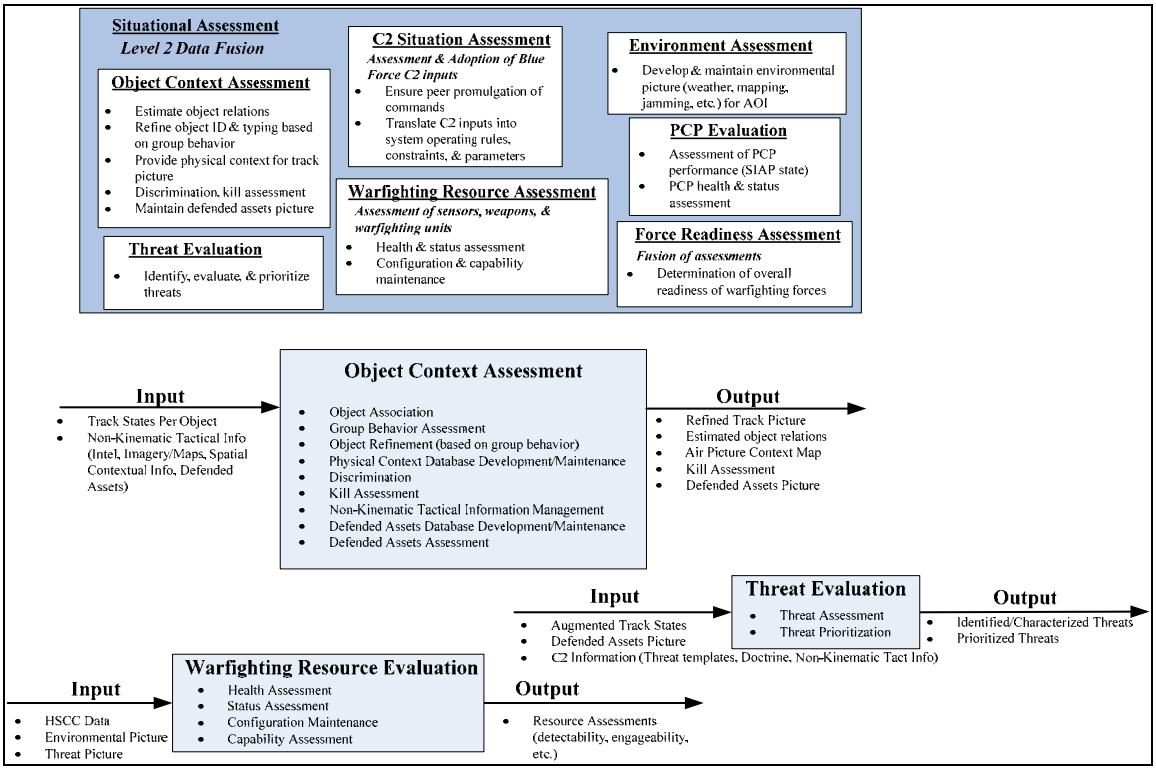


Figure 2-28 Data Fusion - Level 2

60 Bonnie W. Young, A C2 System for Future Aerospace Warfare

61 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

Object Context Assessment

Object context assessment examines the group behavior of the objects and the operational context of the objects. This process estimates and predicts relationships among entities to include force structure, cross-force relations, communications, and physical context. The input to this functional domain includes track datasets or states on a "per object" basis and types of C2 dataset information applicable to providing the operational context to the area of interest. Prior to object context assessment, each object has been examined individually—the kinematics and characterization have been assessed for each individual aerospace object. Within the object context assessment domain, the kinematics and characterization of the group behavior of a set of aerospace objects is assessed. From this assessment, individual object characterizations may be refined and additional information concerning objects may be attained. Table 2-4[62] shows the functionality of object context assessment as well as the input and output.

Table 2-4 Object Context Assessment Functions

Function	Description
Object Association	Object association develops hypotheses for associations among aerospace objects. Associations among objects are estimated based on relationships including temporal relationships, geometrical proximity, communication links, and functional dependence. Examples of object associations include: a set of tracked aerospace objects representing ballistic missile deployment phase targets and penetration aids; a set of tracked objects representing a squadron of fighter aircraft; and a set of blue force aerospace objects that are part of the defended assets picture.
Group Behavior Assessment	Group behavior assessment analyzes the behavior of a hypothesized group of associated objects. Assessments include group and object characterization by comparisons of the kinematic behavior to templates. Also includes event/activity aggregation, which establishes relationships among diverse entities in time to identify meaningful events or activities.
Object Refinement	The refinement or modification of a particular aerospace object's characterization or identification based on the results of group behavior assessment.
Physical Context	The development and maintenance (updating) of a database or "picture" of the

62 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

Function	Description
Database Development	operational situation based on the fusion and association of the track picture with non-kinematic tactical information. This capability also includes contextual interpretation/fusion, which provides an analysis of an individual aerospace object's or group's relationship with the evolving contextual situation including weather, terrain, sea-state or overland conditions, enemy doctrine, and socio-political considerations. Context correlation fuses multi-source (kinematic, ID, parametric and geographic) information.
Discrimination	Discrimination refers to the set of algorithms and methods involved in distinguishing the re-entry vehicle in a complex missile threat from chaff and penetration aids.
Kill Assessment	Kill assessment assesses the effectiveness of an intercept of an enemy aerospace object based on real-time sensor input (i.e., kinematic change, change in signature). Related functionality includes: engagement status tracking (which monitors the progress of the current engagement situation) and battle damage assessment (which analyzes post-engagement and offensive action data to determine the effectiveness of blue force battle damage inflicted on red forces or red force defended assets).
Non-Kinematic Tactical Information Management	"Non-Kinematic Tactical Information" includes tactically-relevant information that is non-kinematic and of a non-sensor-processed nature. It may include intelligence, imagery, voice data, and context information (e.g., commercial air and shipping lanes, political and cultural boundaries (observed countries of threat origin and countries of over flight, etc.), geographical items of interest, etc.). This functionality manages and fuses this information into forms that support tactical operations.
Defended Assets Database/Assessment	This functionality develops a defended assets "picture" within the area of interest that includes all defended aerospace objects and zones as well as points or areas on the ground. A "defense level" or prioritization is assigned based on established doctrine and/or operator input. The purpose of keeping track of all defended assets in the air and on the ground is to feed into the process of prioritizing threats, which ultimately supports the optimized use of warfighting resources. The defended assets information set can also be displayed to operators and commanders in order to allow them to easily change prioritizations as necessary. This information set also supports wargaming functions, which evaluate proposed blue and red force courses of action.

Threat Evaluation

The threat evaluation process determines what objects are candidates for engagement or defensive action, determines whether engagements or actions are allowed, and assigns priorities to those objects designated as threats. The threat evaluation process uses a number of inputs including the following: augmented track states that include a track's characterization (track category, type, and ID information), the track's kinematic profile, overt behavior exhibited by the track, and non-kinematic tactical information such as intelligence data.

Warfighting Resource Evaluation

Another aspect of situational awareness is the evaluation of warfighting resources. This involves the management of information related to the sensors and weapons of each unit and the assessment of their capabilities in particular operational situations. Specifically, this evaluation provides the health, status, configuration, and capability (HSCC) of these resources. Table 2-5[63] describes this data in more detail. In addition to the HSCC data, this evaluation of warfighting resources requires the environmental picture, the threat picture, and resource task sets.

Table 2-5 Health, Status, Configuration, and Capability (HSCC) Information

HSCC Dataset	Description
Health	Information regarding a resource's ability to perform optimally. (For example, a sensor's health data may include its current registration, alignment, and calibration information as well as information regarding whether its operation is degraded.)
Status	Information regarding a resource's current tasking and thus, availability for future tasking.
Configuration	Information regarding a resource's mode and configuration. (For example, a resource may be on, off, in standby, etc.; additionally a sensor may be in a search or track mode, etc.)
Capability	A static information set that includes a resource's capabilities (functional and performance) and limitations based on various environments, configurations, and threats or tasks.

63 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

Warfighting resource evaluation is performed by every participant unit in the battle force. This important capability is a critical part of developing effective and timely resource tasking for network-centric warfare missions. Each unit must assess the health, status, configuration and capability of each resource. Each unit then uses this information to fulfill operational missions.

Command and Control Situation Awareness

C2 situation awareness is the capability to maintain a shared awareness among the entire battle force. Every participant unit would be aware of various levels in the warfighting chain of command involved in battle management and force command. Basically, it involves the creation of a picture or awareness of the current C2 situation. The C2 picture focuses mainly on the state of affairs of friendly forces and warfighting resources. It depicts the deployment or mission status of units showing aircraft on strike missions or land or sea based units in surveillance modes, for example. It will also show the status of which units are operating as a distributed system and which are stand-alone.

PCP Evaluation

PCP evaluation is the ability of a set of distributed peers to monitor the individual and group performance of a peer or set of collaborating peers. The performance of PCPs and PCP collaborations constitute an important aspect of the operational situation.

(b) Data Fusion (Level 3) Impact Assessment

In the impact assessment process, all participant units will perform threat intent estimation, event prediction, consequence prediction, and susceptibility and vulnerability assessments as shown in Figure 2-29[64].

64 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

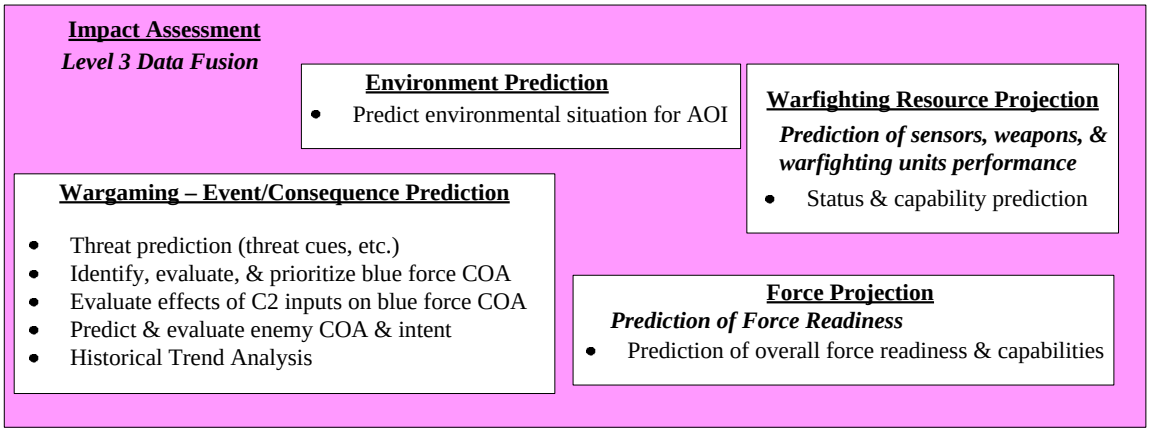


Figure 2-29 Data Fusion - Level 3

Data Fusion (Level 3) Situation Prediction

Figure 2-30[65] shows the functions associated with situation prediction. Situation prediction is used to estimate the enemy course of action (COA) and the potential impacts of the COA on the plans of the battle force. Situation prediction is performed using Automated Management Aids (AMA) to predict real-time, near real-time and non-real-time operational situations based on blue and red hypothesized COAs. The following functions are used in the situation prediction process: environment prediction, warfighting resource projection, wargaming, and force projection.

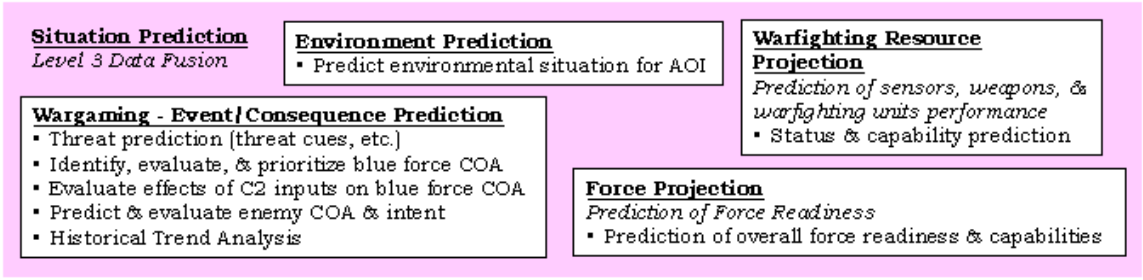


Figure 2-30 Data Fusion Level 3 - Situation Prediction Functionality

Environmental Prediction

Environmental Prediction produces Meteorological and Oceanographic (METOC) weather forecasts based on current and historical conditions. The forecast is used to estimate the effects of weather on weapon and sensor performance and to determine the feasibility of their use for potential operational missions.

65 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

Warfighting Resource Projection

The projection of warfighting resource capabilities into the future based on hypothesized COAs is an important part of wargaming. This function set maintains an information database of resource capabilities in various operational and environmental conditions.

Wargaming or Event/Consequence Prediction

The ability to predict enemy COAs provides great advantage to the warfighter. Assigning quantitative confidence values to potential COAs will support other advanced C2 capabilities such as collaborative planning and resource management.

(c) Data Fusion (Level 4) Process Refinement

At Level 4 of JDL Data Fusion model, the Distributed Resource Management (DRM) function monitors and allocates the battleforce's resources (sensors, weapons, and C2) based on the situation (Figure 2-31[66]). The Distributed Resource Management function is further discussed in section Resource Managing and Tasking.

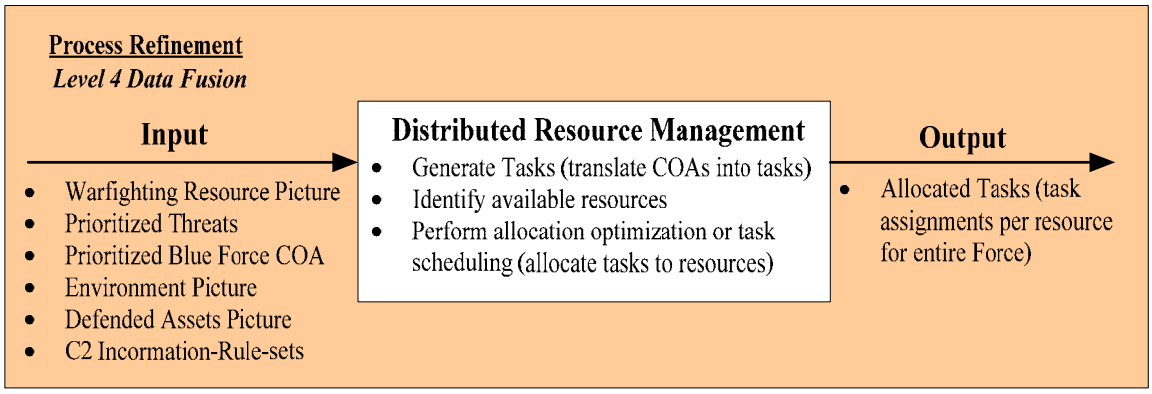


Figure 2-31 Data Fusion - Level 4

d. Resource Managing and Tasking

The Resource Manager operates in Level 4 of the Data Fusion Model, but because of the importance of this capability this section is devoted to describing it. As stated in Young's article, *Integrated Fire Control for Future Aerospace Warfare*, "the Resource Manager is the key to enabling and optimizing the use of distributed resources for collaborative and integrated fire control". The Resource Manager is the function that

66 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

prioritizes tasks and selects the optimum sensor and weapon resources to that task. To perform this task, the Resource Manager requires the outputs of the situation assessment and situation prediction functions. Using these outputs, the Resource Manager selects the most suitable resource for a specific task. This selection is based on the prioritized threats, the best estimated blue force COA, and operational situation (i.e., environment, defended assets locations, etc.).

If the Resource Manager is unable to assign a resource to a task, based on the availability of the resource at that given time, the Resource Manager must reprioritize the task list. The main advantage of the Resource Manager capability is that it enables each distributed unit to determine the best use of each resource in the "force" (or within a set of collaborating peers) and to make this determination in a near-simultaneous manner. In this way, resources can be used for force needs rather than just for the needs of an individual unit. The basic concept of the Resource Manager is that every participating warfighting unit will effectively be able to produce the same decision results; given that each unit receives similar information.

The Resource Manager is the key that enables the Integrated Fire Control (IFC) concept. The Resource Manager determines the best sensor and weapon systems based on several factors including available resources, weapons characteristic, and sensor capabilities. The Resource Manager will construct a list of primary and backup resources. Each Resource Manager must compare their results with the results of the other units to identify and correct any discrepancies. This step is necessary to ensure that each unit generates the same decision recommendations, particularly when the commitment of distributed resources is critical, as is the case for IFC.

Traditionally, the control of the weapons and sensors systems has been the responsibility of the officer in charge of the local units in the battle group. The Resource Manager distributes this command authority to all individual units. Every participating unit's Resource Manager will generate a list of all available resource for assignment but there will still be an ability for an individual unit to override the resource availability and tasking if need so.

e. Integrated Architecture Behavior Model (IABM)

Since all participating units are exchanging sensor and status data, the expectation is that each U.S. and Coalition unit will generate the same Operational Picture and will make the same threat assessments and resource assignments. To accomplish this goal, each platform must process information in the same manner. The Joint Single Integrated Air Picture (SIAP) Systems Engineering Organization (JSSEO) has been tasked to develop a behavior model, known as the Integrated Architecture Behavior Model (IABM). JSSEO is defining the IABM's critical design elements to be incorporated in the applications of "common services" and vehicular track establishment, management, and identification. The IABM will be developed in a format which will support all joint information systems in the network-centric environment to establish and maintain a single coherent tactical command and control environment. The IABM will reside on each participating unit or peer and will ensure each unit uses common computational methods and algorithms. The concept is that each participating unit is given identical sets of data/information and will produce the identical picture, threat assessments, and resource allocations.

As illustrated in IABM PCP Network diagram (see Figure 2-32[67]) the distributed system consists of multiple peers interacting and interfacing with external non-SIAP entities such as legacy systems. An individual peer is shown as a single PCP with associated warfare resources.

67 Bonnie Young, article "The Power of Information Age Concepts and Technologies: A C2 System for Future Aerospace Warfare", 2004 Command and Control Research and Technology Symposium

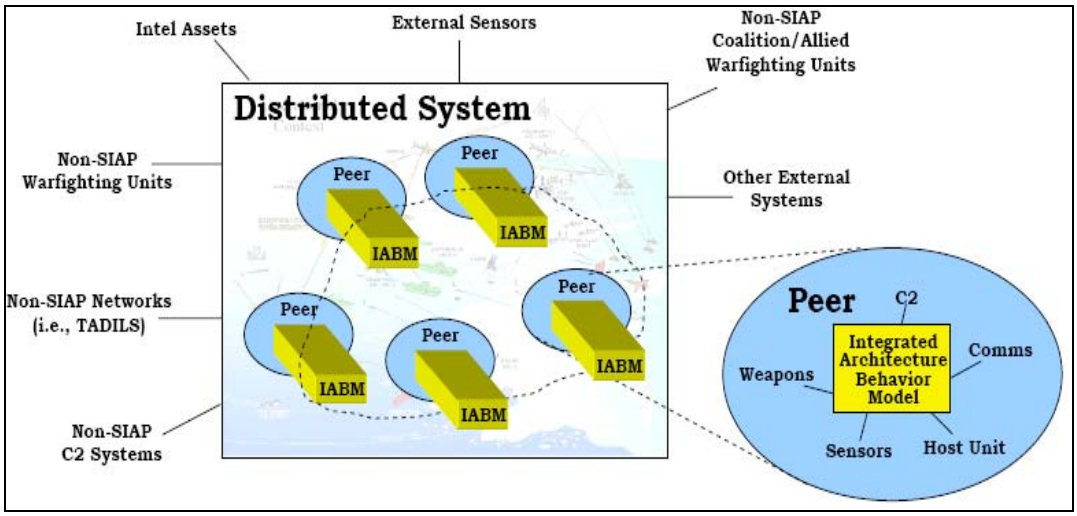


Figure 2-32 IABM PCP Network

JSSEO's plans are to take the relevant elements of the IABM, specifically those associated with common services and joint track management, and couple them with maritime tracking requirements in surface (land and sea) and sub-surface vehicles to form the "Open Architecture Joint Track Management" capability.

f. Data Mining

During military operations, all contacts (tracks) that are potential enemy targets are carefully monitored. This function is tedious but very important for the Joint battle force. Knowing the position of enemy tracks allows the U.S. and Coalition Forces to strike quickly and ensure the success of their mission. During a major operation, the number of tracks that must be monitored can be significant. Determining the intent of an enemy track with an operator display that is saturated with tracks is even more difficult.

One possible way to address the issue of determining an enemy track's intent is by implementing artificial intelligence (AI) into the JTM. Such an approach has been proposed by the JSSEO group. The AI feature would automatically determine the intent of the enemy track based on known patterns. If it is determined the enemy track has hostile intentions, the U.S. and Coalition Force would be placed on high alert. This capability is known as data mining.

Data mining, sometimes referred to as knowledge discovery, is the process of analyzing data from different perspectives and summarizing it into useful information.

The data mining process, shown in Figure 2-33[68], accepts inputs from multiple databases. These databases are integrated into the data warehouse. Data warehousing is defined as a process of centralized data management and retrieval. Data warehousing represents an ideal vision of maintaining a central repository of all organizational data. Centralization of data is needed to maximize user access and analysis. Potential enemy tracks are analyzed against known patterns and any new patterns would be considered hostile and given immediate attention. Automated discovery of previously unknown patterns helps to assure that U.S. and Coalition Forces have an advantage over their adversaries.

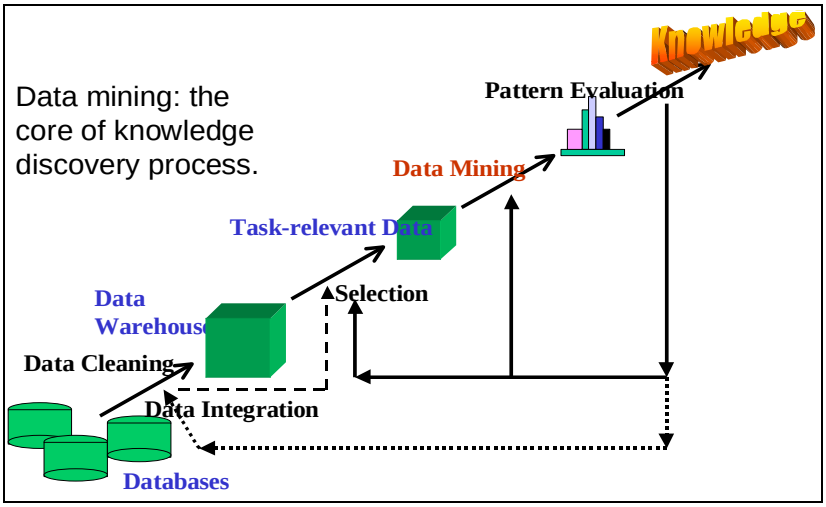


Figure 2-33 Data Mining Process

The most commonly used techniques in data mining are:

- Artificial neural networks: Non-linear predictive models that learn through training and resemble biological neural networks in structure.
- Decision trees: Tree-shaped structures that represent sets of decisions. These decisions generate rules for the classification of a dataset. Specific decision tree methods include Classification and Regression Trees (CART) and Chi Square Automatic Interaction Detection (CHAID).

68 Waltz, Edward L., "Information Understanding: Integrating Data Fusion and Data Mining Processes", IEEE International Symposium on Circuits and System, 1997

- Genetic algorithms: Optimization techniques that use processes such as genetic combination, mutation, and natural selection in a design based on the concepts of evolution.
- Rule induction: The extraction of useful if-then rules from data based on statistical significance.

(2) Data Fusion and Data Mining Operations

Edward Waltz, in his article titled *Information Understanding: Integrating Data Fusion and Data Mining Process*,[69] show the functional processes of an integrated data mining and fusion model. This model is shown in Figure 2-34[70]. Real-time data, represented by the three sources lines, build three operational databases. This is the first level (level 0) of the data fusion model. The output of the process is a real-time visualization of the present situation. Relevant data is then extracted, transformed and loaded into a long-term data warehouse. The data from the warehouse data goes through the data cleaning and transformation process to a common multidimensional data set to allow entity-relationship clustering by a data mining engine. The mining process allows faint and complex signatures to be discovered, modeled and validated for insertion back into the data fusion pipeline.

[69] Waltz, Edward L., "Information Understanding: Integrating Data Fusion and Data Mining Processes", IEEE International Symposium on Circuits and System, 1997

[70] Waltz, Edward L., "Information Understanding: Integrating Data Fusion and Data Mining Processes", IEEE International Symposium on Circuits and System, 1997

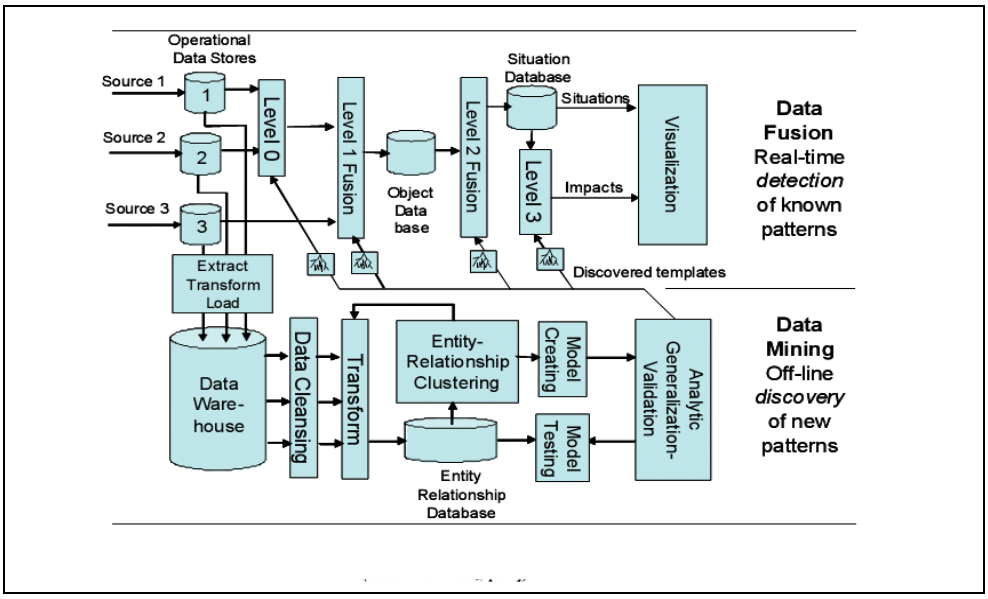


Figure 2-34 Co-processing of Abductive/Inductive (Data Mining) and Data Fusion Operations

James Llinas and Christopher Bowman, in their article *Revisiting the JDL Data Fusion Model II*[71], state that there are several challenges to incorporating Waltz's abductive/inductive techniques into a robust and automated data mining-fusion system. One concern is the development of a reliable method for automated discovery of relevant patterns in the flow of real-time data. Even if that capability exists, there is still a concern whether the decisions and/or actions would be taken on the basis of the discovery of such a pattern – this is a concept of employment issue, and is related to the reliability of such discoveries.

6. Acoustic Networks Undersea FORCEnet Connectivity Using Seaweb

a. Introduction

When the submarine is operating in the domain of a deployed Seaweb infrastructure, Undersea FORCEnet connectivity can be maintained through Seaweb. Seaweb is networked undersea acoustic communications involving submerged submarines, deployable autonomous distributed sensors, and Racom (radio

[71] Llinas, James & Bowman, Christopher etc.., Revisiting the JDL Data Fusion Model II

communication) gateway buoys linked to an ashore command center[72]. The principle for FORCEnet below the ocean surface is to provide the submarine Fleet with two-way networked connectivity when operating at tactical depth and speed[73]. Undersea FORCEnet is a broad spectrum of technology enablers, including advanced acoustic and acoustic-RF (radio frequency) communications, high-bandwidth satellite communications across all frequency bands. Seaweb enables future naval capabilities in littoral ASW and undersea autonomous operations. A significant dual-use of Seaweb is C3N for oceanographic surveys and environmental assessment. Certainly, a major potential benefit of the technology is cross-system, cross-platform, cross-mission interoperability, providing enormous added value to otherwise solitary systems. Seaweb is the underlying fabric of an undersea expeditionary sensor grid, and is imperative for dynamic interoperable connectivity[72].

b. System Description

"Seaweb is a distributed grid of interoperable telesonar (i.e. telecommunications sound navigation ranging) modems supporting low-power, low-bandwidth networked undersea communications and node-to-node ranging (Figure 2-35). The Seaweb network consists of sensor nodes, repeater nodes and gateway buoys. Gateway buoys are equipped with radios for satellite communications (Iridium), line-of-sight communications (FreeWave), and GPS. The Seaweb architecture enables the submarine to communicate and navigate at speed and depth in as much the same way the telephone infrastructure supports mobile users terrestrially. Seaweb will link U.S. and Coalition/Allied submarines to the GIG and provide the following capabilities[74]:

- Global service to meet information exchange requirements anytime, anywhere.
- High availability to support 24/7/365 operations
- Multiple security levels with information protection and assurance

72 J. A. Rice, C. L. Fletcher, R. K. Creber, J. E. Hardiman and K. F. Scussel, "Networked undersea acoustic communications involving a submerged submarine, deployable autonomous distributed sensors, and a radio gateway buoy linked to an ashore command center" Proc UDT Hawaii 2001 Conf, 30 October, 1 Nov 2001.

73 D. Richter, "The Art of the Possible", Undersea Warfare Spring 2006.

74 J. A. Rice and B. Marn, "TASWEX04 Seaweb Test Plan, Draft 7.1".

- An end-to-end security architecture providing defense in depth across the enterprise
- Adaptable and self-configuring to operate in mobile environments
- Hosting of applications and data;
- Warfighting information transmitted directly to naval users"[75].

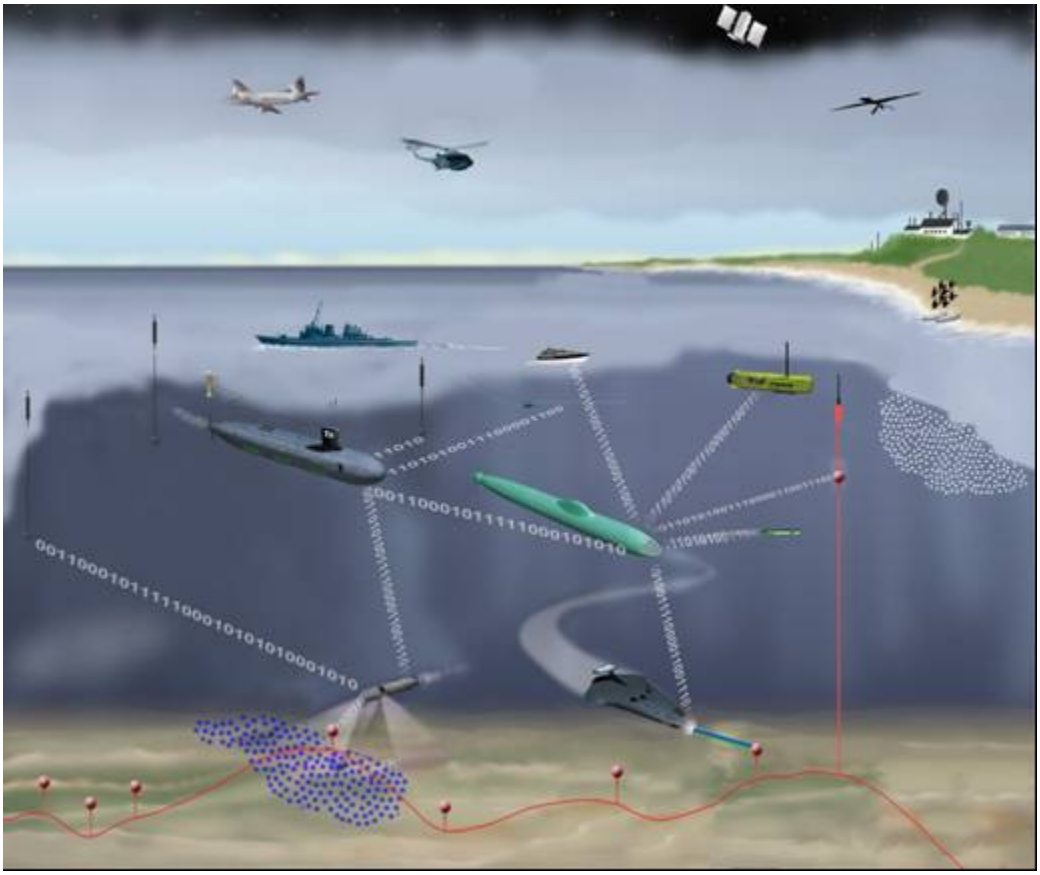


Figure 2-35 Seaweb Distributed Network

c. System Employment

Seaweb is deployed in a grid much like a net, the grid is scaleable and its relatively short links permit physical-layer communications at high enough frequencies to support useful bandwidth, small transducers, directivity, deployable packaging, low battery power, and inherent transmission security[76].

[75] Office of the FORCEnet Chief Engineer SPAWAR 05, "FORCEnet Technical reference Guide For Program Mangers", Version 0.9.4.2. , 4, April 2005

[76] J. A. Rice and B. Marn, "TASWEX04 Seaweb Test Plan, Draft 7.1"

Seaweb networks support asynchronous data communications from autonomous nodes to command centers. On the backlink, Seaweb allows remote command and control of instruments associated with the autonomous nodes. Additionally, network activity supports acoustic navigation and geolocalization of undersea nodes as a natural by-product of telesonar ranging signals. More generally, Seaweb networking permits wireless acoustic transmissions between member nodes in the network using established routes or via an intervening cellular node. Seaweb technology provides an undersea C3N infrastructure for various applications[77].

The initial motivation for Seaweb is a requirement for wide-area surveillance in littoral waters by the DADS application, and by related surveillance applications involving autonomous undersea sensors. These sensors typically operate in 50- to 300-m waters with node spacing of 2 to 5 km. Sensor nodes in a DADS grid generate concise ASW contact reports that Seaweb routes to a master node for field-level data fusion[78]. Primary network packets are contact reports with about 1000 information bits[79]. DADS sensor nodes asynchronously produce these packets at a variable rate dependent on the receiver operating characteristics (ROC) for a particular sensor suite and mission. The master node communicates with manned command centers via gateway nodes such as a Racom sea-surface buoy linked with space satellite networks. Following ad hoc deployments, DADS relies on the Seaweb network for self-organization including node identification, clock synchronization on the order of 0.1 to 1.0 s, node geo-localization on the order of 100 m, assimilation of new nodes, and self-healing following node failures.

As a fixed grid of inexpensive interoperable sensor nodes and repeater nodes, DADS is consistent with the most fundamental Seaweb operating mode based on a stable topology that periodically adjusts itself to optimize overall network endurance and

[77] J. A. Rice, C. L. Fletcher, R. K. Creber, J. E. Hardiman and K. F. Scussel, “Networked undersea acoustic communications involving a submerged submarine, deployable autonomous distributed sensors, and a radio gateway buoy linked to an ashore command center” Proc UDT Hawaii 2001 Conf., 30 October, 1 Nov 2001

[78] E. Jahn, M. Hatch, and J. Kaina, “Fusion of Multi-Sensor Information from an Autonomous Undersea Distributed Field of Sensors,” Proc. Fusion ’99 Conf., Sunnyvale, CA, July 1999

[79] S. McGirr, K. Raysin, C. Ivancic, and C. Alspaugh, "Simulation of underwater sensor networks," Proc. IEEE Oceans '99 Conf., Seattle WA, Sept. 1999

quality of service (QoS). The fixed Seaweb topology provides an underlying cellular network suited for supporting an autonomous oceanographic sampling network (AOSN)[80], including C3N for autonomous operations with UUV mobile nodes. The cellular architecture likewise provides seamless connectivity for submarine operations at speed and depth in a manner not unlike terrestrial cellular telephone service for automobiles[81].

d. Coalition Force Utilization

The goal of the Undersea FORCEnet when utilized by Coalition forces is to multiply the effectiveness of the submarine platforms in support of Coalition, Joint Task Force (CJTF), Expeditionary Strike Group (ESG) and Global War On Terror (GWOT) warfare by enabling two-way communications and network-centric warfare while optimally engaged in the assigned mission. Seaweb will increase the operational capabilities of the submarine platforms by allowing it to maintain its stealth posture while supporting these various missions all while linking the allied or Coalition force to the Global Information Grid allowing all participants to draw on a common operational picture. Undersea FORCEnet is the link to increased operational capabilities of undersea Coalition operations that will include combined Special Operations Missions (SOF) combined anti-submarine operations and provide decisive firepower. Undersea FORCEnet will increase the ability to protect allied and Coalition force navies by assuring information and fire control systems are in sync and conducting the most effective warfare operations. Undersea FORCEnet will increase the U.S. and Coalition forces by ensuring the following[82]:

- Projecting and sustaining combined force operations in distance access or area- denial environments and defeating anti-access and area-denial threats.

---

[80] T. B. Curtin, J. G. Bellingham, J. Catipovic, and D. Webb, "Autonomous

[81] J. A. Rice, C. L. Fletcher, R. K. Creber, J. E. Hardiman and K. F. Scussel, "Networked undersea acoustic communications involving a submerged submarine, deployable autonomous distributed sensors, and a radio gateway buoy linked to an ashore command center" Proc UDT Hawaii 2001 Conf, 30 October, 1 Nov 2001

[82] D. Richter, "The Art of the Possible", Undersea Warfare Spring 2006

- Denying enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement with high-volume precision strike, through a combination of complementary engagement methods against critical targets both mobile and fixed in all weather and terrains.

e. Seaweb Summary

Seaweb is the undersea FORCEnet connection to the GIG. Seaweb is a foundational FORCEnet capability. Dynamic, interoperable connectivity will be achieved through provisioning of a secure backplane of communications systems. Capabilities such as data networks and information systems that form a global Naval Information Grid will be fully integrated with the other Services and Countries into the GIG. As previously stated, FORCEnet is the Navy's link to the GIG. This Naval grid is envisioned as a ubiquitous network that provides a host of services with high availability, reliability, and survivability across the Naval enterprise in airborne, afloat, ashore and undersea domains. U.S. and Allied/Coalition Interoperability can be made more effective by using Seaweb in undersea/submarine operations[83].

Seaweb can help meet the U.S. Allied/Coalition diverse Warfighter communications needs through networked acoustic transmissions between member nodes using established routes or via an intervening cellular node. Seaweb technology provides an undersea C3N infrastructure for all applications that will provide seamless communications among Warfighters data across the U.S. military services, and with Coalition forces and allies. These attributes are supported by the physical infrastructure and the data link protocols that combine to provide FORCEnet communications and specific network applications (e.g., ISR networks, weapons networks etc.) that comprise the networks that ride on the communications framework along with required routing, access and authentication[84].

---

83 Office of the FORCEnet Chief Engineer SPAWAR 05, "FORCEnet Technical reference Guide for Program Mangers", Version 0.9.4.2. , 4, April 2005

84 Ibid

C. LIMITATIONS AND GAPS OF NETWORK-CENTRIC WARFARE

John Luddy discusses limitations of Network-Centric Warfare in his article[85], "The Challenge and Promise of Network-Centric Warfare." Mr. Luddy identifies seven areas where limitations exist, but only three (technical, operational, and intelligence) are of a concern to C4ISR. The other limitations deal with doctrines, training, and strategic employing of NCW. Mr. Luddy identifies bandwidth is a technical limitation. As was stated, "*bandwidth is the information-carrying life blood of any network, and network-centric operations devour signal bandwidth."* As demand for information increases, network-centric operations will constantly require more communication bandwidth. Bandwidth will have to be managed more efficiently, and will require better communication technology.

Another technological concern for the network of sensors is the vulnerability to jamming. Enemy forces will make every attempt to disable the battle force network either through deception or denial. Because technology is always vulnerable, and frequently fragile, networks must be durable, flexible and redundant.

Another operational limitation, ironically, is too much information. Generally more data is better but too much data can also lead to difficulties. A flood of information from different sensors and sources can be overwhelming and as Mr. Luddy states, "too much information may cause commanders to tune out."

One of the greatest limitations facing NCW is the constant challenge to obtain continuous up to date intelligence information. Luddy states that network-centric operations will depend on comprehensive intelligence collection, management and analysis. One noted shortfall in recent operations was the lack of persistent (day/night, all-weather) battlespace sensor coverage. It has been a challenge to make UAVs better and equipped with more capable sensors to improve this shortfall.

Ultimately, a constellation of spaced-based radar (SBR) satellites may provide the most significant sensor improvement in decades. The Pentagon still has to prove that SBR can be integrated with other assets, tasked effectively and responsively by warfighters, strategic analysts and planners, and acquired on a realistic schedule and

85 The Challenge and Promise of Network-Centric Warfare, written by John Luddy, Feb. 2005 http://www.lexingtoninstitute.org/docs/521.pdf

budget. Finally, no advance in technology or its efficient use can compensate for inadequate human intelligence (HUMINT). In the drive toward increased network-centric operations, and better and faster sensors, the need for accurate HUMINT should not be neglected.

D. C4ISR SUMMARY

As stated by Admiral Arthur K. Cebrowski and John J. Garstka, in their article "*Network-Centric Warfare*[86] *: Its Origin and Future*," Network-Centric Warfare derives its power from the strong networking of a well-informed but geographically dispersed force. The enabling elements are a high-performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command-and-control (C2) processes--to include high-speed automated assignment of resources to need--and integrated sensor grids closely coupled in time to shooters and C2 processes."

Network-centric warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography.

As the U.S. Armed Forces increases their network-centric focus, the failure of our Coalition to do likewise could prove a serious obstacle to the success of future Coalition efforts. A few of the Coalition nations have explored networked operations in one form or another. Some have changed their forces to a network-centric organizational concept, but these efforts are very limited. Coalition members are changing to provide "niche" capabilities rather than trying to match the U.S. system for system. Future Coalitions will have to incorporate varying levels of technological sophistication, and support it with training, exercises, doctrine and resources. If U.S. forces become unable to reliably communicate with Coalition forces, U.S. leaders might well be justified in fighting alone. This dilemma must be avoided. The U.S. must make every effort to encourage its allies to pace their network-centric modernization with its own, perhaps with carefully constructed joint ventures between U.S. and Coalition governments. A "NATO

86 Network-Centric Warfare: Its Origin and Future, By Vice Admiral Arthur K. Cebrowski, U.S. Navy, and John J. Garstka, Proceedings, January 1998 http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm

standard" for communications protocol and software would be a good start. From there, procurement and deployment benchmarks should be established.

Future advances in Joint aerospace warfare depend largely on Network-Centric Warfare (NCW) solutions that enable new and enhanced forms of Command and Control (C2). The role of C2 in aerospace operations is to optimize the use of offensive and defensive resources to combat aerospace threats. NCW-enabled C2 will enhance time-critical aerospace operations by enabling the use of *distributed* warfare assets in collaborative missions that optimize their use for Force-level priorities. A primary example of a collaborative C2 capability is Integrated Fire Control (IFC) or the tactical engagement of aerospace threats using distributed warfare assets. Selecting the best shooter from a set of geographically distributed firing units improves the chances of intercepting targets (by selecting optimal engagement geometries) and improves the economy of weapon resources (by eliminating multiple redundant shots). For complex threat environments in which many aerospace targets exist, collaborative fire control may be a necessity for victory.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY AND ANALYSIS

The analysis focuses on determining a system architecture, what benefit FORCEnet (Fn) will provide to Coalition forces, and also the benefit of Fn to a joint Coalition task force (AUSCANNZUKUS). Identification of the requirements for implementing FORCEnet is also analyzed.

To show the improvement between Fn and the traditional platform-centric operation, a model must be built to simulate this new Fn concept. The objective of the modeling and simulation is to model FORCEnet enabling methods and concepts. These methods and concepts include netted sensors with cueing, data fusion and resource management, and integrated fire control. In the research conducted, the Fn modeling for the three vignettes in the scenario are: Anti-Submarine Warfare (ASW), Anti-Surface Warfare (ASuW), and Anti-Surface Missile Defense (ASMD) and are summarized in Table 3-1. The scenario involves both the United States (U.S.) and the Coalition forces.

Table 3-1 FORCEnet Composition

Scenario	Objective	Blue Force	Red Force	Fn Level
ASW	ESG/CSG aims to localize the Red force submarines	1 MPA, 1 SSN, LFAS and deployable barrier sensors laid by LCS (3), 1 Coalition SSK	2 Kilo submarines	U.S.: 4 Coalition Forces: 0-2
ASuW	Monitor and shadow Red force SAG	3 LCS, 1 SSN, 2 DDG, 2 Coalition FFG/DDG, MPA/AWACS/UAV/helos , 1 LHD, 1 LPD, NGO vessels	2 Parchim Corvette, 3 Van Speijk FFG	U.S.: 4 Coalition Forces: 0-2
ASMD	To defend ESG/CSG against air/missile attack	3 LCS, 2 DDG, 2 Coalition FFG/DDG, 1 U.S. E-2C, 1 LHD, 1 LPD	2 Parchim Corvette, 3 Van Speijk FFG, 2 Kilo submarines	U.S.: 4 Coalition Forces: 0-4

The modeling and simulation performed shows the benefit to the United States Navy, and Coalition forces if they were to implement FORCEnet into their navies. This report explores the possible benefits for Coalition forces, as well as the United States Navy, in terms of Measures of Effectiveness (MOE) and Measures of Performance (MOP) as they relate to an operational scenario. Discussion of the possible capability

improvements for Coalition forces, provided through the implementation of FORCEnet, and how it would benefit their navies in a non-Coalition exercise follow.

Steps for the implementation of the FORCEnet capabilities so that Coalition forces can interact as a single force in the planning and execution of the force protection and force projection requirements are stated. The Coalition force addressed within this study is bounded by the AUSCANNZUKUS Coalition, made up from the forces of Australia, Canada, New Zealand, the United Kingdom and the United States navies.

The implementation of FORCEnet for Coalition forces through the development of a Coalition Force Architecture and the use of policy and procedures for implementing the architecture is also discussed. The identification of specific systems was minimized so that the focus of the study would be on the Coalition FORCEnet architecture itself.

A. NETWORK-CENTRIC WARFARE

Many current National and Naval policy documents notionally describe the improvement in warfighting effectiveness which will be achieved through the implementation of network-centric Command and Control (C2) capabilities. It has been further suggested that expanding these net-centric C2 capabilities to our Coalition partners is a necessary component for the success of the CNO's vision of a "1,000 ship" Navy. The overall goal of this study is to provide a Modeling and Simulation (M&S) based analysis of these improvements in warfighting effectiveness as provided by network-centric Command and Control capabilities. By evaluating the warfighting effectiveness of a given force in a common scenario and altering the attributes of their C2 capabilities, we will be able to quantitatively assess the direct contributions of these C2 capabilities to the overall effectiveness of the force.

B. SYSTEMS ENGINEERING

No system, System of Systems (SoS), or Family of Systems (FoS) should exist or come into being without a definition of need. The need should drive technology and the solution, not the inverse, trying to make square pegs fit into round holes. Developing a system only when a need is identified is the primary tenet of Systems Engineering.

> Traditional engineering design methods are based on a bottom-up approach. Starting with a set of known elements, design engineers create the product or system by synthesizing a combination of system elements.

> However, it is unlikely that the functional need will be met on the first attempt unless the system is simple. After determining the product's performance and deviation from what is required, the elements and their combination are altered and performance determined again. This bottom-up process is iterative, with the number of iterations (and design efficiency) determined by the experience and creativity of the designer, as well as by the complexity of the product of system.[87]

For this study, the need is to determine if FORCEnet provides a measurable benefit to Coalition partners, and measured improvement in performance of a joint Coalition task force.

Systems engineering implements a top-down approach in designing a system and the process for this project is shown in Figure 3-1[88]. With a need identified, requirements of system behavior are documented. These requirements not only come from customers, but also from users, maintainers, managers, developers, etc…, any stakeholder of the system. The requirements identified must be testable and measurable. If they are not, then the requirements are worthless, and the end system will not have correctly implemented the systems engineering discipline. Additionally, required performance is needed, not just required capabilities. For example, a system capability is to navigate a platform, but how accurately the navigation must be is also needed.

87 Blanchard, Benjamin S., Fabrycky, Wolter J., Systems Engineering and Analysis, 3rd edition; pg. 28

88 http://www.gmu.edu/departments/seor/insert/robot/robot2.html - accessed 8/7/06

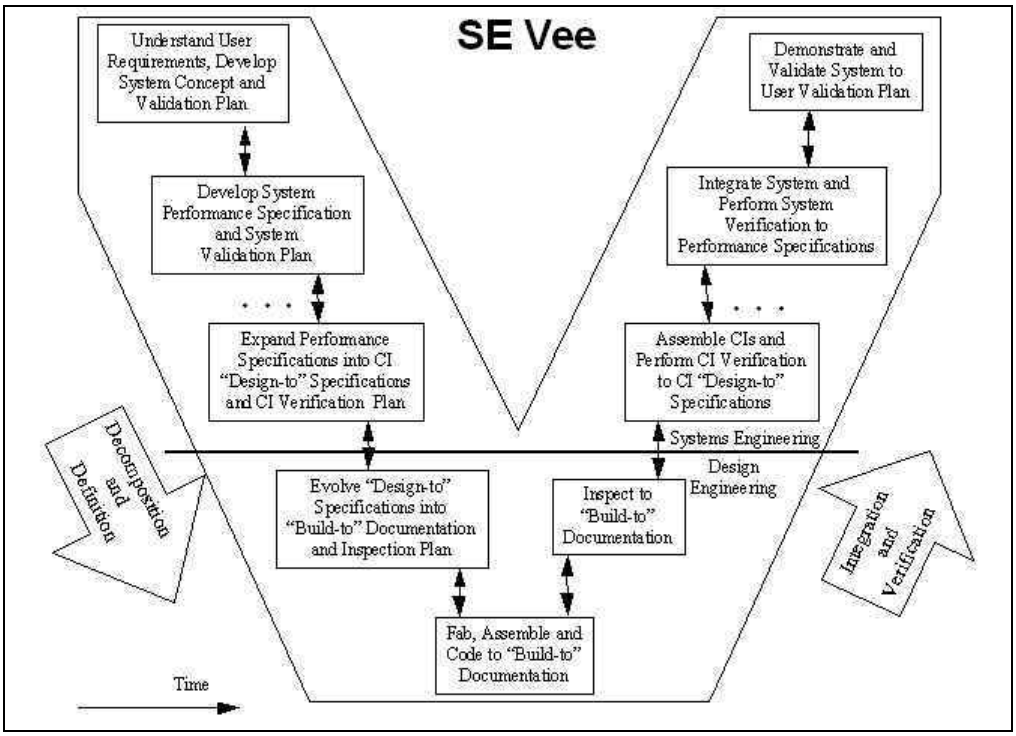


Figure 3-1 Systems Engineering Vee Model

Next, the requirements are decomposed into functions, which are then allocated to subsystems. The decomposition continues until the functions are allocated at the lowest level elements or components. "The use of functional elements is the essential difference in systems engineering methodology compared with systems integration."[89] This is followed by the final step of the decomposition and definition sequence is the detail design of the components.

Once the detail design of the system components is accomplished, the integration and verification sequence can begin. To verify the system design, the prototype must be demonstrated to satisfy client acceptance as well as user satisfaction. This begins the integration and verification sequence of systems engineering.

Another basic tenet of systems engineering is that the process of developing the system is an iterative one, comprised of the endless loop of Synthesis, Analysis, and Evaluation as shown in Figure 3-2[90].

89 Blanchard, Benjamin S., Fabrycky, Wolter J., Systems Engineering and Analysis, 3rd edition; pg. 28

90 Ibid.

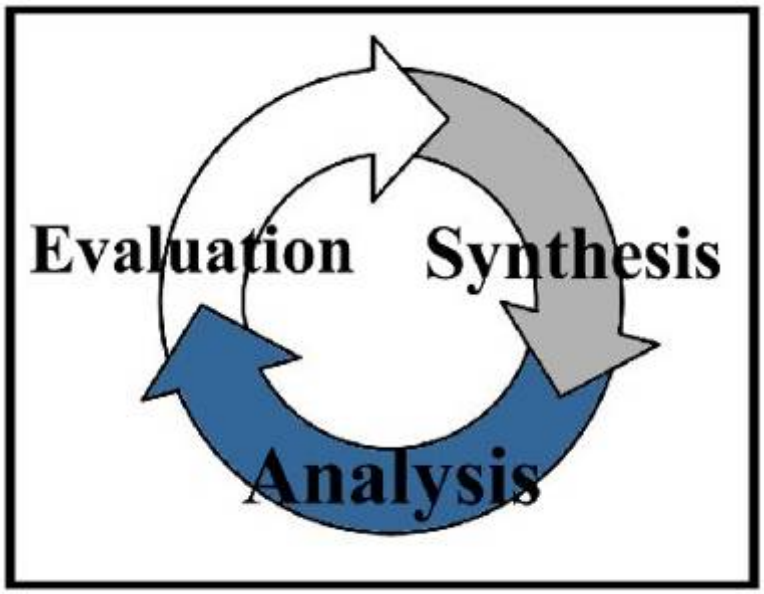


Figure 3-2 Systems Engineering Process

First, synthesis (design) of the problem to be solved is performed, then an analysis of the functional characteristics and finally an evaluation of the current output. If the desired results have not been achieved at this point, the process of synthesis, analysis, and evaluation is repeated until success is attained.

1. Develop Architecture

For this project, the need is for seamless, near-instantaneous synchronization and exchange of information in order to maximize the effectiveness of an Expeditionary Strike Group (ESG) comprised of Coalition forces (AUSCANNZUKUS). An architectural approach to the problem is implemented vice a non-system engineering method that would select a system design based upon current technology.

The selected architecture is based upon a self-synchronizing, self-healing, fully netted battleforce. The battleforce is dependent on the process of data fusion, where data from several sources are fused and stored in a single integrated database. Compilation, retention and distribution of the database and the data fusion process, is the responsibility of designated Super-Nodes and Auxiliary Super-Nodes. The Integrated Architecture Behavior Model (IABM), data mining, and Integrated Fire Control (IFC) are all key components in realizing this netted battleforce architecture. Implementation of the proposed components of the architecture will result in an increased speed of command,

more effective use of battleforce resources (sensors, weapons, etc…), which in turn assures information superiority for the Fn platforms. Ultimately, Fn will succeed in minimizing blue force losses and maximizing the potential of any Coalition force structure.

From a technological perspective today, the United States is fully capable of performing the tasks required in defeating most any naval threat, from blue water operations to littoral combat and support. The issue is that the fighting piracy and conducting Noncombatant Evacuation Operation (NEOs) and humanitarian relief as well as Coalition operations requires support from the Coaltion. Politics and common sense will not allow, except in a rare instance, the United States to act unilaterally. Thus, buy-in and implementation of FORCEnet (Fn) among allied and Coalition partners are mandatory.

The analysis and modeling show that US-only platforms that implement FORCEnet have a significant advantage over non-FORCEnet capable platforms (US or Coalition). Analysis of the model also shows a decrease in capabilities when non-Fn units are added to a Fn environment.

Criteria or the Measures of Effectiveness (MOEs) considered in the modeling process include:

MOE 1 – Engagement Quality

MOE 2 – Target Detection

Additional MOEs to be considered for future efforts may include:

- Connectivity
- Track Integration
- Data Exchange
- Data Registration
- Information Management
- Unit Tactical Situational Awareness (SA)
- Battleforce SA / Common Operational Picture(COP)

Numerous Measures of Performance (MOPs) were provided in the scenario and supporting documentation. The MOPs used in modeling the selected architecture are listed in Table 3-2.

Table 3-2 Measures of Performance

Grid	Measure of Performance (MOP)
Sensor (Detection)	**# (targets) detected** **# (targets) not detected**
Command and Control (C2)	**total # identified (enemy ship)** **# identified (non-hostile)** **# subs identified** **# subs not (detected on slide) identified** **# missiles identified** **# missiles leakers** **# tracked via precision cue (all threats)**
Engagement	**total # missiles engaged via IFC** **# engaged (platform-centric)** **# enemy killed** **total # of leakers** **# blue hits suffered (if only one engagement)**

The modeling and simulation results show that Fn provides the following improvements:

- Sensors - 5% improvement in number of threats detected.
- C2 - 42% improvement in tracking via precision cue (sensor tasking).
- Engagement - 25% improvement in threat neutralization.

The analysis shows an increased quality of the information acquired, a robust situational awareness shared by the distributed combat elements within the network, and improved neutralization of threats to the Joint Coalition Task Force.

For the purposes of the analysis, M&S efforts were limited to the ASW, ASuW and ASMD vignettes. In each vignette selected for modeling and simulation, decomposition of each of the identified missions into their respective functions and tasks was necessary. OPNAV INSTRUCTION 3500.38A, the UNIVERSAL NAVY TASK LIST (UNTL), Figure 3-3[91], was used, focusing on the Operational and Tactical levels outlined in red below.

91 OPNAV INSTRUCTION 3500.38A, the UNIVERSAL NAVY TASK LIST (UNTL)

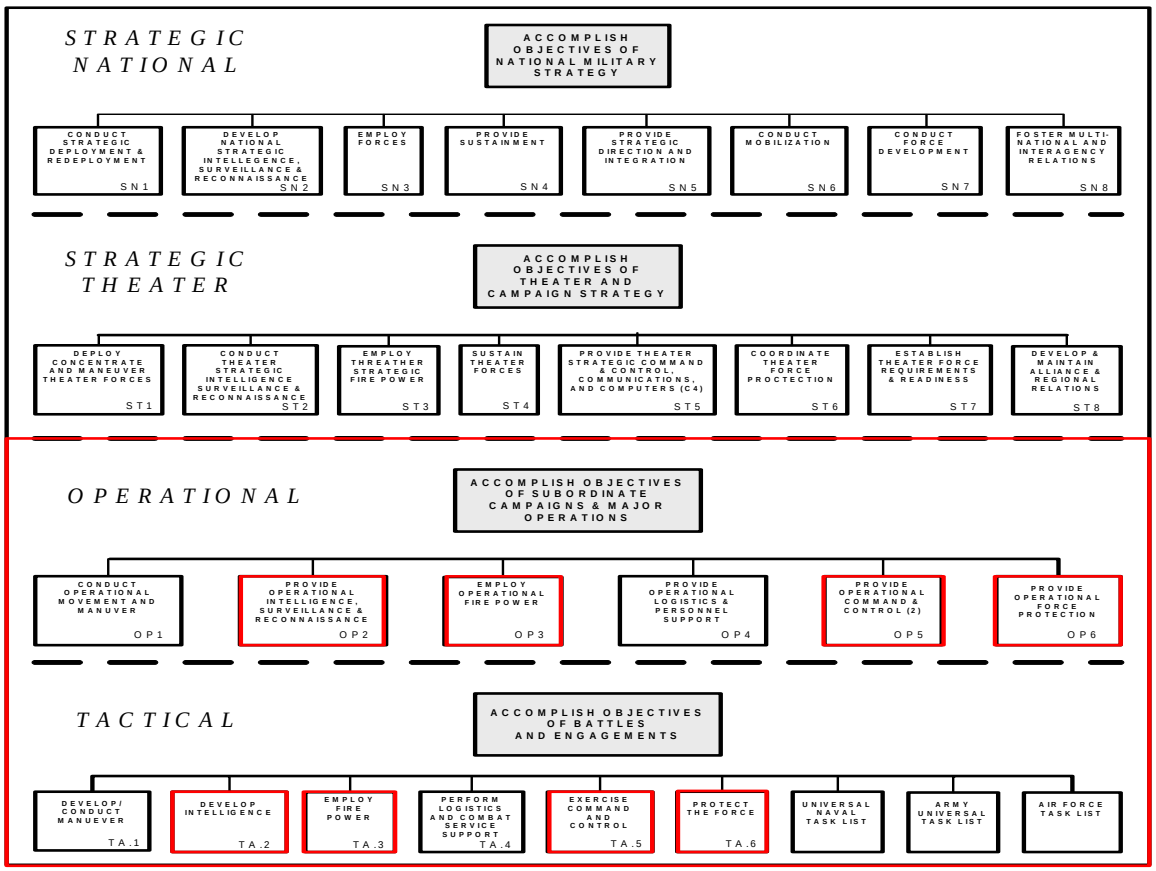


Figure 3-3 Universal Navy Task List

Each of the selected tasks was further decomposed to the next level. An example demonstrating the decomposition of Operational Task 5 – "Provide Operational C2" is shown in Figure 3-4.

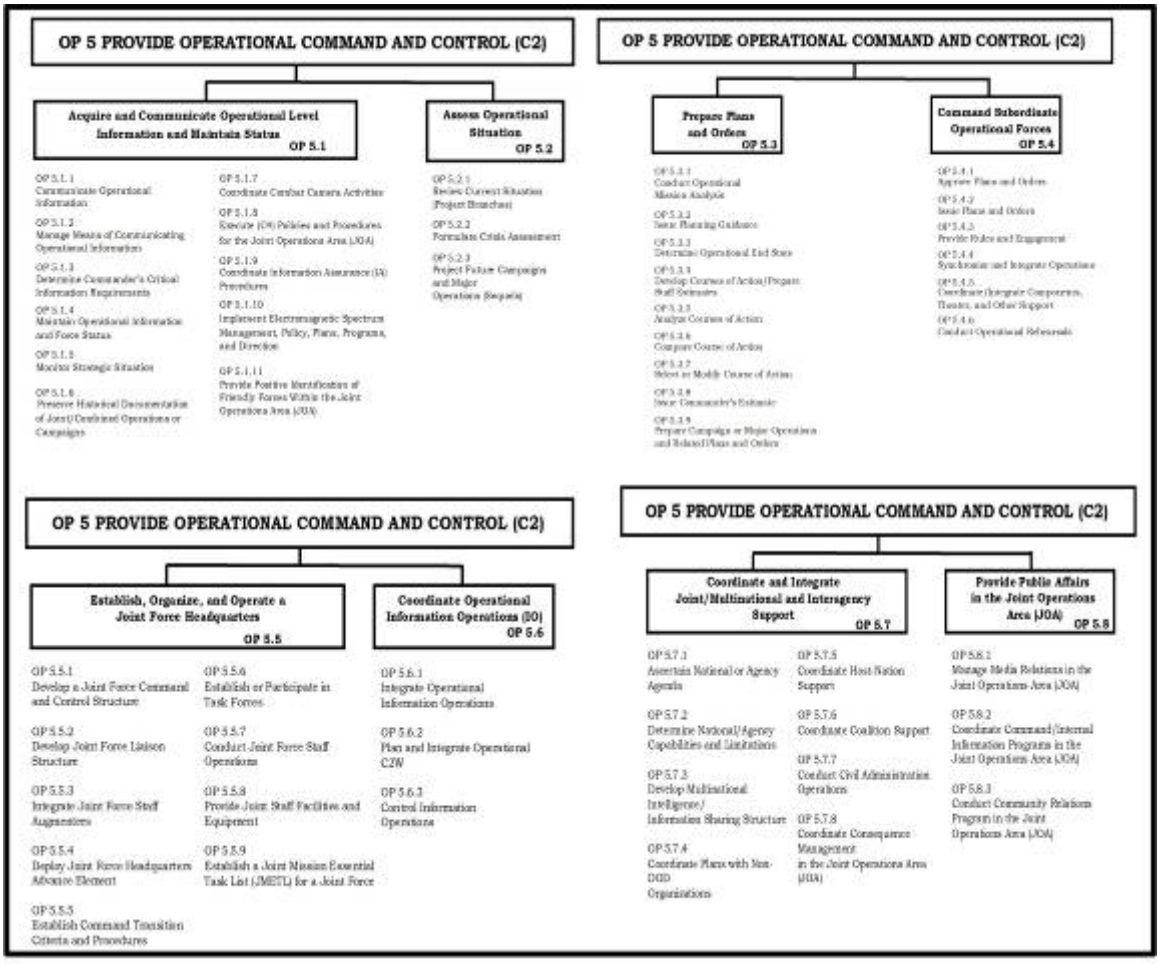


Figure 3-4 Lower Level Universal Navy Task List

Given a representative set of required functions and tasks, these required functions and tasks were allocated to the platforms identified in the given force structure with the goal of identifying gaps and overlaps in providing the required capabilities. The approach consisted of a subset of the Quality Function Deployment (QFD) method (Figure 3-5)[92] as described in the International Council on Systems Engineering (INCOSE) Systems Engineering Guidebook[93] and the ASN(RDA) Naval Capability Evolution Process (NCEP)[94]. In this approach, the outputs of one matrix become the inputs of the subsequent matrix, continuing until the desired output has been attained.

92 Naval Capability Evolution Process Guidebook, Volume 1. ASN(RDA). Version 1.1, May 2005

93 Systems Engineering Handbook. International Council on Systems Engineering. Version 2a, June 2004

94 Naval Capability Evolution Process Guidebook, Volume 1. ASN(RDA). Version 1.1, May 2005

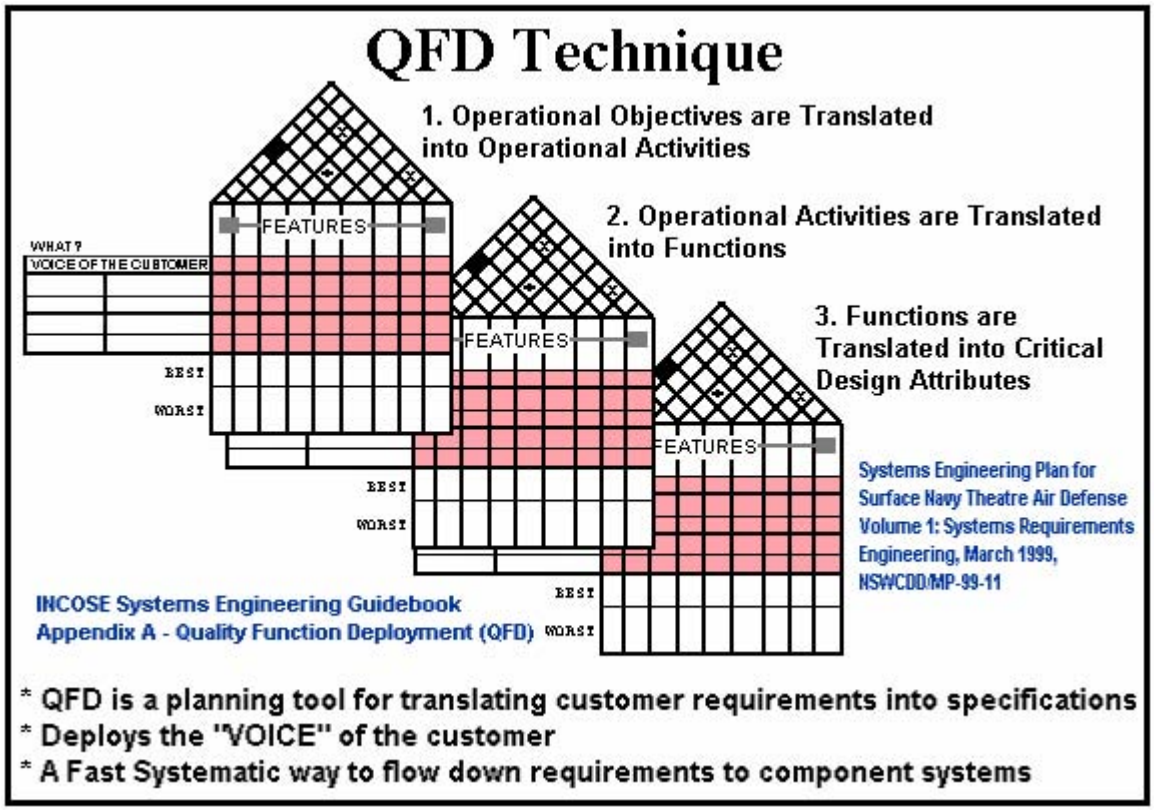


Figure 3-5 Quality Function Deployment Technique

As described in the NCEP guidebook, QFD matrices can be constructed for each of the pairing shown in Figure 3-6[95].

95 Naval Capability Evolution Process Guidebook, Volume 2. ASN(RDA). Version 1.1, December 2005

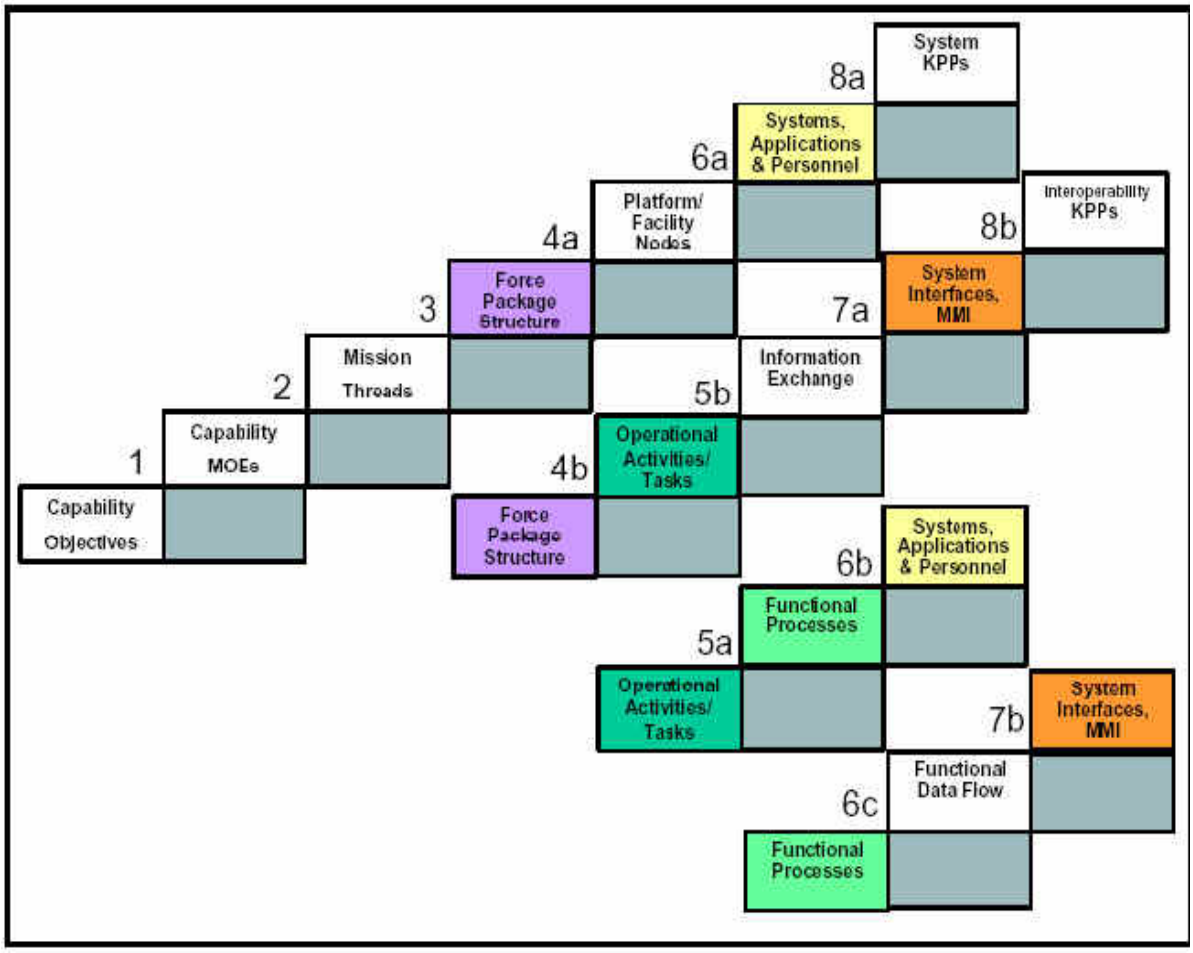


Figure 3-6 QFD Matrices for Capability-Based Planning

For demonstration purposes, pairs comparing Platforms versus Tasks is depicted in Table 3-3. This is not intended to provide a detailed analysis of individual platform capabilities. Obviously, smaller platforms are indeed capable of performing each of these tasks to varying degrees. It is rather intended to illustrate that larger platforms will likely be required to possess enhanced capabilities to coordinate these tasks between numerous platforms spanning great distances across the theater and beyond.

Table 3-3 Platforms vs. Tasks

	Function	OP 2.2 Collect & Share Info	OP 2.3 Process & Correlate Info	OP 2.5 Disseminate Intel	TA 5.4 Determine Actions	TA 5.5 Direct Forces	OP 3.1 Conduct Targeting	OP 3.2 Attack	TA 2.3 Assess Attack
US	LHD	X	X	X	X	X			
	LPD	X	X	X	X	X			
	LSD	X	X	X	X	X			
	LCS	X			X		X		X
	DDG	X	X	X	X	X	X	X	X
	CG	X	X	X	X	X	X	X	X
	SSN	X	X		X		X	X	X
	TAGOS	X			X		X		X
	UAV	X					X	X	X
	Helos	X			X		X	X	X
	Harriers	X			X		X	X	X
	MPA	X			X		X	X	X
AUSCANNZUK	FF	X			X		X	X	X
	FFH	X			X		X	X	X
	FFG	X			X		X	X	X
	DD	X	X	X	X	X	X	X	X
	DDG	X	X	X	X	X	X	X	X
	LPD	X	X	X	X	X			
	LSD	X	X	X	X	X			
	AOR	X			X				
	SSK	X	X		X		X	X	X
	P3	X			X		X	X	X
	Helos	X			X		X	X	X

Given this high-level list of required functions and tasks, the attributes of the C2 capabilities required to support these functions and tasks were identified. An embedded list of desired capabilities and attributes is shown in Table 3-4 and explained below. Capabilities identified in green exist today. Capabilities identified in blue are currently planned to exist in 2014. Capabilities identified in red are desired and/or required but are not currently planned for fielding. It is these specific capabilities that need to be pursued in order to fully realize the improved warfighting effectiveness of net-centric C2. While again not intended to provide a detailed analysis concerning to what degree a particular platform may possess each of the desired traits, this is intended to illustrate the enhanced traits required of large, theater-level, C2 platforms.

Table 3-4 Capabilities

	Capability	Publish	Subscribe	Cross-Domain	Level 4 Fusion	Theater Database	Self-synchronyzing	Disconnected Ops	LOS	BLOS	Reach-Back
US	LHD										
	LPD										
	LSD										
	LCS										
	DDG										
	CG										
	SSN										
	TAGOS										
	UAV										
	Helos										
	Harriers										
	MPA										
AUSCANNZUK	FF										
	FFH										
	FFG										
	DD										
	DDG										
	LPD										
	LSD										
	AOR										
	SSK										
	P3										
	Helos										

2. Desired Command & Control (C2) Traits

This section describes the C2 capabilities listed in Table 3-4, identified as critical in supporting FORCEnet. Some capabilities apply to the Coalition Joint Task Force and Global Information Grid participants, while others are primarily CJTF-centric.

a. Publish

To publish is to have the ability to expose organic sensor, C2, and weapon information for examination and use by other entities attached to the CJTF and the GIG. This includes the ability to advertise the data's availability, as well as the data's type, quality, time, location, and other significant identifying traits.

b. Subscribe

Subscribing is the ability of consumers (CJTF or GIG) to collect and assemble remote data based on pre-defined data traits. Data would be automatically retrieved based on its type, quality, time, location, and other significant identifying traits.

c. Cross-Domain

Cross-domain references the ability to publish, subscribe, process, and store data of differing classification and releasability levels. Data security and

availability is automatically governed by business rules determined by each user's roles, clearances, and affiliations.

d. Level 4 Data Fusion

Data fusion is the ability to conduct ongoing monitoring and assessment of the overall fusion process, to refine the process itself, and to regulate the acquisition of data to achieve optimal results[96].

e. Theater Database

Positioned aboard the Super-Node, the theater database provides the ability to maintain a comprehensive database of all data published or subscribed to by theater units is essential to FORCEnet. This CJTF-based database would, by proxy, serve as the repository for all data published by smaller tactical units. The database is also the repository and service provider for many subscription requests from the lesser equipped platforms (disadvantaged users). Should elements outside the theater subscribe to tactical sensor data, the theater database would service these requests, precluding the need for multiple or redundant requests to the tactical edge platforms and the associated bandwidth loading required by those requests. Likewise, this database would, by proxy, subscribe to the superset of data requested by other theater platforms. Should multiple 'Tactical Edge' platforms subscribe to similar data, these requests would be serviced by the theater-database, again precluding the need for multiple redundant requests by 'Tactical Edge' platforms and the associated bandwidth loading.

f. Self-Synchronizing

This ability allows Super-Nodes to automatically synchronize among multiple theater databases. While the most capable unit would normally be assigned the role of Super-Node, maintaining the primary database, other similarly equipped platforms (Auxiliary Super-Nodes) would maintain duplicate, synchronized, theater-databases allowing them to assume the Super-Node role in the event of a casualty to the previously assigned master. Synchronization would occur automatically, using underutilized bandwidth on existing circuits based on availability.

---

96 L. A. Klein. Sensor and data fusion concepts and applications. Tutorial texts, vol. TT 14, SPIE Optical Engineering Press, USA, 131 p., 1993

g. Disconnected Operations

Disconnected operations refer to the ability of individual platforms and theater-level forces to operate for periods of time without access to the GIG. In the event of a casualty to SATCOM or other reach-back connectivity to the GIG, theater forces must be able to continue operations until connectivity is restored. The self-synchronizing theater-databases previously described could provide this capability.

h. Line-of-Sight (LOS) Communications

IBGWN (Intra Battle Group Wireless Network) is an example of a system currently demonstrated to provide this capability. It is the ability to communicate among theater platforms using interoperable protocols (including Internet Protocol (IP)) and waveforms over various Radio Frequency (RF) paths providing LOS connectivity.

i. Beyond LOS (BLOS) Communications

Also known as Extended LOS, this includes the ability to communicate among theater platforms using interoperable protocols (including Internet Protocol (IP)) and waveforms over various RF paths providing BLOS connectivity within the theater. Examples of systems currently demonstrated to provide this capability include High Frequency Improvement Program (HFIP), SubNet Relay, and BACN (Battlefield Airborne Communication Node).

j. Reach-Back

The ability to communicate among global platforms using interoperable protocols (including Internet Protocol (IP)) and waveforms over various RF paths providing connectivity beyond the theater is known as reach-back. Reach-back provides theater assets their primary connectivity to the GIG.

Examples of systems currently demonstrated to provide this capability are Super High Frequency (SHF) Satellite Communications (SATCOM), Advanced Extremely High Frequency (AEHF) SATCOM, and commercially on Ku/Ka SATCOM systems.

C. CONCEPT OF OPERATIONS (CONOPS)

This section describes the relevant parts of the Family of Joint Future Concepts, CONOPS and/or Unified Command Plan (UCP) assigned missions to which the desired

capabilities contribute, what operational outcomes they provide, what effects they must produce to achieve those outcomes, how they complement the integrated joint warfighting force and what enabling capabilities are required to achieve the desired operational outcomes.

1. Coalition Scenario

The scenario was provided in a series of documents each further refining the force structure and platform participants. The most recent of these documents "Coalition FORCEnet Study – Operation Philippine Comfort Scenario" Version 0.g dated 20 January 2006[97], describes the initial scenario as follows:

"The scenario opens with an internationally compelling natural humanitarian disaster -public sentiment requires relief action on the part of each nation. Each nation has in the vicinity assets with some dual use capability (naval/humanitarian relief) so their initial response can be measured in days not weeks. The trade space for modeling the force is that some portion of the U.S. ESG will not be available. The injection of the Indonesian Naval threat will be evolutionary and will begin after the Nations have already very publicly committed to the humanitarian mission, thus removing the opportunity to just not participate.

The Philippines are affected by two large volcanic eruptions affecting the centre of the country (Luzon), and the overall disruption leads to a political crisis and change of government. Other nations provide support with humanitarian and disaster relief, but whilst this effort gathers pace, Muslim factions in the southern province of Mindanao use the opportunity to foment trouble and achieve their own goal of a separate secular state. The Coalition support then widens to include peace making/peace enforcement, and the U.S. dispatch an Expeditionary Strike Group (ESG) with an amphibious component to ensure that disaster relief is not impeded, and to provide additional land support to Philippine ground forces facing the insurgents. In turn this triggers increased support by other Southeast Asian countries (previously covert) to the separatists, and their naval units (SAG and SSK) attempt to oppose access by the ESG."

97 The Technical Cooperation Program (TTCP). Coalition FORCEnet Study – Operation Philippine Comfort Scenario, v0.g. January 2006

2. Vignettes

The scenario as presented was described in terms of eight independent vignettes beginning with 'Assembly Training Planning and Rehearsal' and concluding with 'Recovery and Regeneration' as shown in Figure 3-7[98].

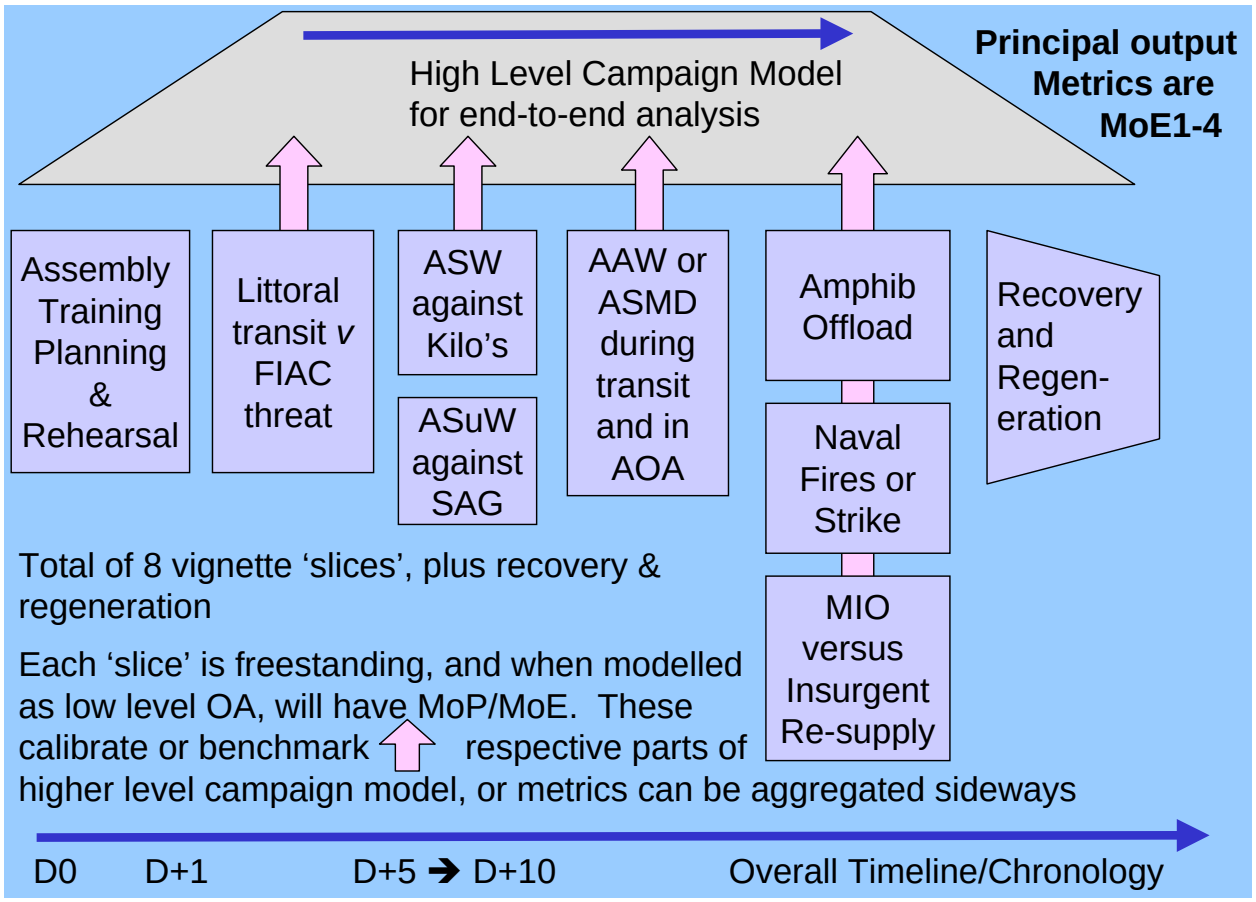


Figure 3-7 Vignettes

D. FOUR LEVELS OF FORCENET

FORCEnet maturity has been defined in terms of four specific levels of capability. These levels and their associated capability traits are shown in Figure 3-8[99].

98 The Technical Cooperation Program (TTCP). Coalition FORCEnet Study – Operation Philippine Comfort Scenario, v0.g. January 2006

99 TTCP MAR AG-6 Brief to Commander, Naval Network Warfare Command. April 24, 2006

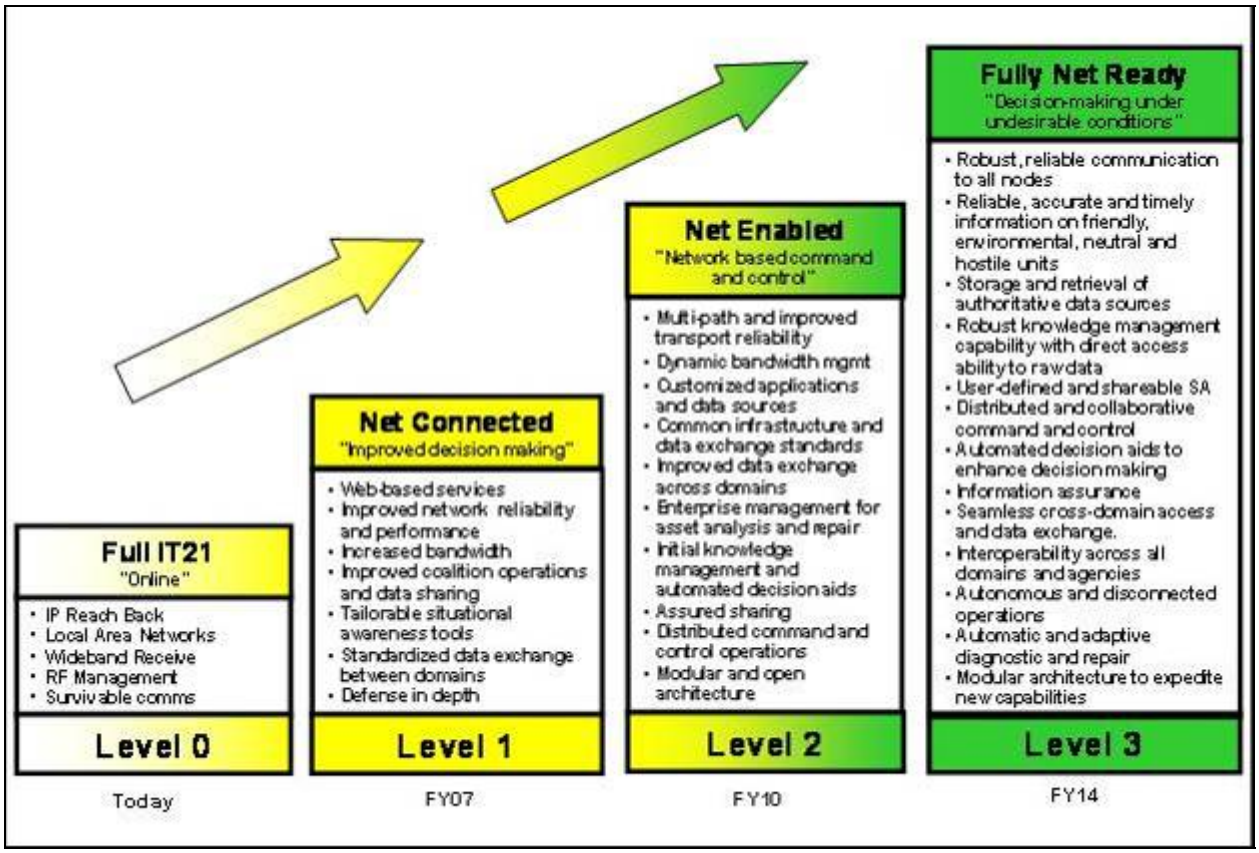


Figure 3-8 Levels of FORCEnet Capability

Alternative definitions, used for modeling and simulation purposes in this project, were provided in the scenario and are listed in Table 3-5[100].

Table 3-5 ESG composition and FORCEnet levels

Fn Level	Benefits/Characteristics:
0	No FORCEnet**.** Vessels use voice radio and Link 11 or 16 to share situational awareness and C2 data. Platform-centric in character.
1	Filtered, delayed, low bandwidth (dialup) FORCEnet (like 'no FORCEnet', but higher fidelity/faster updates). ESG/CSG has access to reach back and has the ability to distribute intelligence information gained from that to all ESG/CSG members. Information from organic sensor and intelligence data is available with some time delay throughout ESG/CSG. Recognized Maritime Picture (RMP) which fuses organic and other ESG/CSG data is distributed with minor time delays.
2	Real-time targeting information gained from any U.S. or Coalition asset/source (when latter is technically capable) is available to all ESG/CSG vessels as required. Access to targeting information is assured within understood

100 The Technical Cooperation Program (TTCP). Coalition FORCEnet Study – Operation Philippine Comfort Scenario, v0.g. January 2006

	limitations. Information accuracy, timeliness and coverage continuity are assured up to predefined levels. Rapidly updated RMP is available to all ESG/CSG vessels.
3	Weapons systems are networked but are only able to be controlled by national authority.
4	Vessels of all Coalition nations are technically and politically/militarily able to offer weapons systems as a network service for command by approved authorities from any of the nations within the ESG/CSG/CJTF.

E. COMBINED JOINT TASK FORCE (CJTF) COMPOSITION

Four force compositions are considered based on the technology and political policies implemented by members of the U.S. and Coalition forces. These four options are shown in Table 3-6[101].

Table 3-6 Four Options to be Considered

Option	Description	Map to Levels in Table 3-5
I (do nothing)	Small size (all US) ESG force, fully Fn capable	US (level 3) No Coalition
II (do minimum)	Added Coalition ships, but not Fn capable (i.e. larger overall force)	US (level 3) Coalition partners (level 0)
III	Intermediate Fn capability to the additional Coalition ships	US (level 3) Coalition partners (levels 1 or 2)
IV	Full Fn capability to entire force	US and Coalition Units (level 4)

F. THREAT SUMMARY

1. Threats

Discussion has identified the requirement for a feasible Coalition scenario, to act as the framework for the various modeling efforts and that the *Operation Philippine Comfort – CJTF* scenario, already used for U.S. demonstrations of Fn components, might be appropriate.

Volcanic eruptions in Philippines have caused widespread civilian distress, and Naval and Marine forces from the Essex ESG (originally transiting South East Asia en-

101 The Technical Cooperation Program (TTCP). Coalition FORCEnet Study – Operation Philippine Comfort Scenario, v0.g. January 2006

route to the Arabian Gulf) are diverted. The U.S. has committed the force to Humanitarian Aid and Disaster Relief (HA-DR) tasking, involving airlift, medical and material requirements.

Fundamentalist rebels (ASG) remain active on southern Philippine islands, and increased force protection measures are applied to all units within the vicinity. The ESG is briefed to anticipate the possibility of providing assistance to U.S. and RP ground forces.

Southeast Asian nations announce support for ASG. To show its support of Mindanao, these countries announce that they will send a naval force northward (SAG) to the Sulu Sea, the likely location for a Coalition sea base.

They do not announce what that force will do once it arrives in the area, but it is likely to be based on their recent major sea exercise off the south-eastern point of Borneo. This featured:

- 2 cruisers. 5 frigates, and 1 amphibious ship have been operating as a single force, conducting anti-submarine operations against the 2 Kilo submarines for about five days
- The Kilo's appear to be fairly proficient. National sensor support confirms that the submarines have not returned to port near Jakarta, there is no Signal Intelligence (SIGINT) information to confirm their whereabouts, and the Kilo positions have been unknown for about 50 hours[102].

2. Red Order of Battle (OOB)

2008: The discovery of new oil deposits in the disputed Spratly Islands has led to renewed and escalating political tension between the five nations (China, Taiwan, Indonesia, Vietnam, Philippines) that have staked claims in the region.

2010: International arbiters award the majority claim to the Philippines. Indonesia publicly denounces the decision, stating that improper U.S. influence tainted the result and tilted the proceedings towards the U.S. ally. Anti-U.S. Islamic Fundamentalist movements in Indonesia continue to grow in intensity.

2015: Two volcanic eruptions on the main Philippine island of Luzón have resulted in a humanitarian crisis and the collapse of the government. In the midst of the

[102] Note: Blue forces refer to Coalition forces. Red forces refer to the enemy.

ensuing international disaster relief movement, separatist Muslim factions on the southern island of Mindanao, utilizing heretofore covert aid, capitalize on the opportunity to stage a revolt.

In support of the Muslim rebels, a Southeast Asian nation dispatches a naval force composed of several frigates, corvettes, patrol boats, an amphibious assault vessel, and two diesel-electric submarines.

The Van Spijk Frigate is a multi-purpose ship that can be deployed in anti-submarine, anti-aircraft, or surface action roles. Armament consists of one 76 mm gun and 8 SS-N-14 anti-ship cruise missiles that have both anti-ship and anti-air capabilities[103].

The Parchim Corvette is an advanced anti-submarine patrol ship. Armament consists of 2 quadruple SA-N-5 (24 missiles), 2 twin 16-in torpedo tubes (400-mm), 4 KH-35 anti-ship missiles, and several medium caliber machine guns[104].

The Patrol Boat PSK-M is a fast patrol boat whose primary armament consists of 4 KH-35 anti-ship missiles. It possesses excellent capabilities in the littorals.

The Tacoma LST is an amphibious landing ship equipped with two .50 caliber machine guns. Overall military lift capabilities provide for transport of two-hundred troops or 1,700 tons of cargo/vehicles[105].

The Kilo SS is a diesel-electric submarine of Russian origin equipped with 8 Strela-3 (SA-N-8 Gremlin) anti-ship missiles and 18 VA-111 torpedoes. Primary missions include anti-submarine and anti-surface warfare. The Kilo is considered to be one of the quietest diesel-electric boats operating today[106].

---

103 Jane's Fighting Ships, http://jfs.janes.com.libproxy.nps.navy.mil/docs/jfs/search.jsp

104 Ibid

105 Ibid

106 Ibid

Table 3-7 Southeast Asian Nation Naval ORBAT

Type	Status	Armament	ty	Location
Kilo SS	Operational	8 Strela-3 (SA-N-8 Gremlin) 18 VA-111 Torpedoes		At Sea
Parchim Corvette	Operational	2 quadruple SA-N-5 (24 missiles) 2 twin 16-in torpedo tubes (400-mm) 4 KH-35		6 At Sea 2 in Surabuya
Fatahilah Corvette	Operational	2 twin 16-in torpedo tubes (400-mm)		2 At Sea 4 in Surabuya
Van Spijk Frigate	Operational	1 76mm gun 8 SS-N-14 ASCM		2 At Sea 1 in Surabuya
Kihajar Dewantara Frigate	Non-operational	1 76 mm gun		In Surabuya
Patrol Boat PSK-M	Operational	4 KH-35	2	At sea
Tacoma LST	Operational	2 .50cal		1 At Sea 2 In Surabuya

Given the nature of the Philippine insurgency, there exists the possibility that separatists will augment the above listed naval support with their own asymmetric techniques. Suicide bombings via dhows or light single-prop planes are the likeliest scenario.

G. BATTLEFORCE TRANSFORMATION

The U.S. Department of Defense is undergoing a rapid transformation in its operations it conducts abroad. With the downsizing of U.S. Armed Forces, the need to conduct warfare will often consist of both U.S. and Coalition Forces. The need to communicate effectively is of high importance. To accommodate this transformation, the development of Network-Centric Warfare (NCW) has begun. NCW promises to deliver an unprecedented situational awareness through a network community. For the Navy, the NCW concept has evolved into the definition of FORCEnet. This research seeks to determine of the FORCEnet concept, through modeling and simulation efforts, demonstrating an improved capability for the CJTF.

Built on results and findings of AG-1 and AG-6, this study of Coalition FORCEnet implementation examines the way ahead, realizing Coalition capabilities that are compatible with current and future U.S. Navy's FORCEnet initiatives.

This report seeks to define, in functional terms, the various levels of Coalition interoperability with FORCEnet and to assess the incremental value of higher levels of interoperability to provide input to national balance of investment studies.

A trans-national need is also recognized to harmonize national Network-Centric Maritime Warfare (NCMW) functional and technical roadmaps to support effective netted Coalition capabilities and assessment of priorities. Similar to the series of studies sponsored by the TTCP MAR AG-1 and AG-6, the goal of this project is to analyze the application of techniques for performing quantitative analysis, and the benefits of a network-centric Coalition force using FORCEnet. The FORCEnet functional concept[107] defines FORCEnet as "the operational construct and architectural framework for Naval Warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force."[108]

This strategic definition can be shared by Coalition Forces. Primarily this study aims to prove that Coalition FORCEnet can accomplish three goals. First, it will provide conceptual, top-down guidance for engineering Coalition FORCEnet. Second, it provides integrated guidance for identifying, justifying, and prioritizing Coalition FORCEnet investments both outside and within the Naval Enterprise. Third, it models the alignment and integration effort that could be implemented in coordination with other Service transformation initiatives and with other efforts across Joint, Department of Defense (DoD), Inter-agency, and Multi-national arenas. The San Diego Study Group used, developed and applied parametric techniques, and specific modeling and simulation of the assigned scenario for analyzing network-centric warfare. Using the data derived from the modeling and simulation, the value of Coalition utilization of FORCEnet is demonstrated as a force multiplier.

Topics discussed within this document include:

1. FORCEnet Enabling Technology
2. Advantages of Network-Centric Sensors
3. Advantages of Integrated Fire Control

107 FORCEnet: A Functional Concept for the 21st Century, February 2005

108 USN/USMC. *FROCEnet A FunctionalConcept For The 21st Century*

4. The Global Information Grid (GIG) Enterprise Services
5. Tactical Data Links
6. Data Fusion
7. Acoustic Networks
8. Limitations and Gaps of Network-Centric Warfare

H. FAMILY OF SYSTEMS (FOS)/SYSTEM OF SYSTEMS (SOS) SYNCH

As stated by Admiral Vern Clark, *"FORCEnet is the "glue" that binds together SEA STRIKE, SEA SHIELD, and SEA BASE. It is the operational construct and architectural framework for naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force."*[109]

FORCEnet will provide the architecture to increase substantial combat capabilities through the alignment and integrations of FOS/SOS. The result will transform situational awareness, accelerate speed of decision, and produce a greater distribution of combat power. FORCEnet allows for real-time enhanced collaborative planning among joint and Coalition partners.

I. INITIAL OPERATIONAL CAPABILITY/FULL OPERATIONAL CAPABILITY (IOC/FOC) DEFINITIONS

For the purpose of defining Operational Capability milestones, the four previously defined 'Levels of FORCEnet', as shown in Figure 3-9[110], will be used. Initial Operational Capability (IOC) will be attained when the first U.S. Super-Node is equipped with FORCEnet Level 3 capabilities, and associated offboard transport and services infrastructures are deployed in an operational environment. Based on current development and fielding plans, it is anticipated that this will occur in FY 2014.

Full Operational Capability (FOC) for the U.S. Navy will be attained when all identified Super-Node platforms past D-30 (months) in the Fleet Response Plan (FRP) cycle have been equipped with FORCEnet Level 3 capabilities, and offboard transport and services infrastructures are globally available. Based on current development and

109 Clark, V. (2003). 2003 Human Systems Integration Symposium

110 TTCP MAR AG-6 Brief to Commander, Naval Network Warfare Command. April 24, 2006

fielding plans, as well as deployment and availability schedules, it is anticipated that FOC will occur in approximately FY 2017.

To realize the CNO's vision of the "1,000 ship Navy", global FOC, to include Coalition partners and Non-Governmental Organizations (NGOs), the FORCEnet Level 3 capabilities will have to be further realized by all potential participants. This level of capability is highly desirable to achieve global interoperability. As the development and fielding of this capability is beyond the scope of U.S. Navy efforts, an accurate timeframe for true global FOC cannot be adequately predicted.

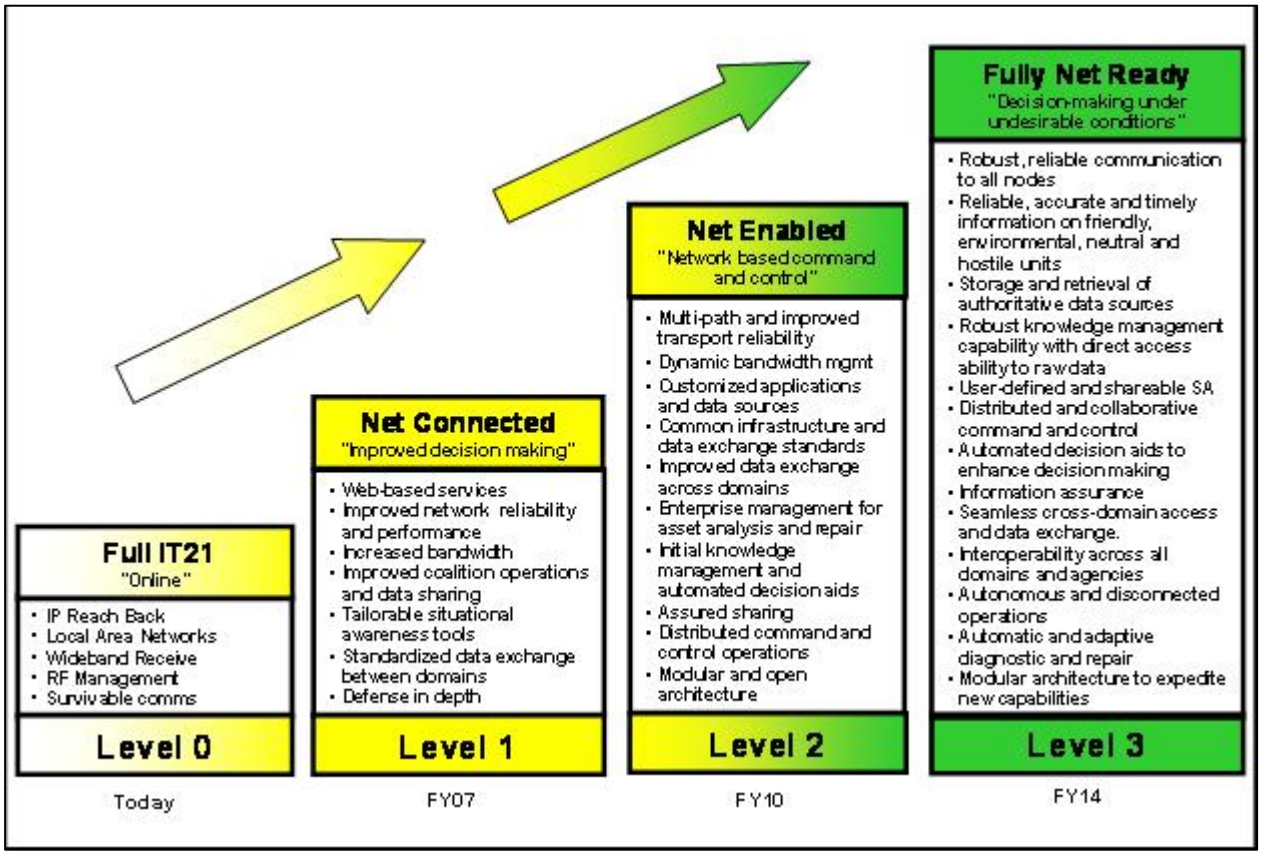


Figure 3-9 Levels of FORCEnet

J. ASSETS REQUIRED TO ACHIEVE INITIAL OPERATIONAL CAPABILITY (IOC)

In order to achieve Initial Operational Capability (IOC) of the FORCEnet integrated battleforce, each platform must be equipped with FORCEnet enabling systems to allow for preliminary sharing of data across the participants. In addition, at least one

U.S. platform and one Coalition platform must be able to act as a Super-Node for exchanging information with the GIG. Table 3-8 provides a list of assets required for the three selected scenarios.

Table 3-8 Assets Required for IOC

Scenario	Objective	Blue Force	Fn Level
ASW	ESG/CSG aims to localize the Red force submarines	1 MPA, 1 SSN, LFAS and deployable barrier sensors laid by LCS (3), 1 Coalition SSK	U.S.: 3 Coalition Forces: 0-2
ASuW	Monitor and shadow Red force SAG	3 LCS, 1 SSN, 2 DDG, 2 Coalition FFG/DDG, MPA/AWACS/UAV/helos, 1 LHD, 1 LPD, NGO vessels	U.S.: 3 Coalition Forces: 0-2
ASMD	To defend ESG/CSG against air/missile attack	3 LCS, 2 DDG, 2 Coalition FFG/DDG, 1 U.S. E-2C, 1 LHD, 1 LPD	U.S.: 3 Coalition Forces: 0-4

In addition to the assets listed above, UAVs and satellites are also required for beyond line-of-sight communications.

K. DOCTRINE, ORGANIZATION, TRAINING, MATERIEL, LEADERSHIP AND EDUCATION, PERSONNEL, AND FACILITIES (DOTMLPF)

The following paragraphs define the expected changes in the Doctrine, Organization, Training, Materiel, Leadership, Education, Personnel and Facilities areas required to support the FORCEnet architecture outlined in this CDD. It was determined early during the requirements definition process that non-materiel changes in and by themselves would not be sufficient in addressing the full spectrum of user requirements. Consequently, this section focuses on the changes required within DOTMLPF to fully exploit the multi-tiered architecture described within this CDD.

Table 3-9 below provides a matrix mapping of the Measure Of Effectiveness (MOE) attributes to the DOTMLPF components. As expected, the architecture described will require transformation in several of the DOTMLPF areas to fully realize the FORCEnet potential.

Table 3-9 MOE to DOTMLPF Mapping

MOE / DOTMLPF	Doctrine	Organization	Training	Materiel	Leadership	Personnel	Facilities
Quality of Information			X	X		X	X
Collaborative Working	X	X	X	X	X	X	X
Shared Awareness	X	X	X		X	X	
Self Synchronizing	X	X	X	X	X	X	
Distributed Combat Elements	X	X	X	X	X	X	

Modeling and simulation of DOTMLPF is another area that requires further investigation during the acquisition cycle. Figure 3-10[111] below presents a DOTMLPF spiral construct that could be used during Trident Warrior exercises to explore DOTMLPF considerations side-by-side with the materiel architecture to provide a holistic assessment of the entire system.

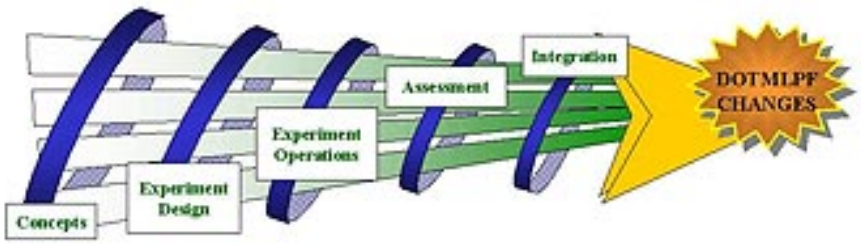


Figure 3-10 DOTMLPF Development Spiral

The following sections address specific points and concepts in the Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities areas and build upon the quote[112] *"The ability to achieve a heightened state of shared situational awareness and knowledge among all elements of a Joint force … is increasingly viewed as a cornerstone of transformation…Realization of the full potential of Network-Centric Warfare requires not only* ***technological improvements****, but the continued evolution of* ***organizations*** *and* ***doctrine*** *and the development of relevant* ***training*** *that will enable U.S., Allied, and Coalition forces to develop and sustain an asymmetric advantage in the information domain."*

111 *Harrison, D. (2003). Modeling and Simulation Technology* – Studies and Analysis.

112 2001 Network-Centric Warfare Report to Congress

1. Doctrine

Significant doctrine changes will be required to exploit the architecture defined in this document. The goal is to create the operational concept that allows the integrated force to support Expeditionary Strike Groups (ESG), Carrier Strike Groups (CSG), Expeditionary Strike Force (ESF) and Coalition force missions in the Joint and/or Combined environment. The second focus is to examine the training/readiness continuum as the Navy transforms its training philosophy to meet the challenges and opportunity presented by the operational concept.

Doctrine will need to evolve in order for Coalition forces to be synchronized in terms of command structure, warfare areas, mission assignments and commanders' authority. For example, Shared Awareness, Self Synchronizing and Collaborative Working depend as much on doctrine transformation as they do on materiel changes for the Joint Force to transition from a primarily autonomous force to a Distributed Combat Element. A Coalition force without a flexible doctrine that allows cross domain, real-time collaboration and shared awareness, will continue to be disjointed and unable to achieve full spectrum dominance in the Under Sea Warfare (USW) area.

a. Security

Security policy must support the establishment of a single standing global network which allows timely access by a wide variety of potential coalition partners and non-governmental organizations.

In the past, many operational and experimental exercises have demonstrated shortcomings in Department of Defense (DoD) arrangements for multinational information sharing with allied and coalition partners. The key component in enhancing our ability as a Joint Force is to strengthen collaboration with our multinational partners[113], which would require improvement in our ability to collect, process, and share information.

Currently, there are six multi-national enclaves as part of U.S. coalition network:

[113] 2004 National Military Strategy

- Combined Enterprise Regional Information Exchange System (CENTRIXS) Four Eyes (CFE): Australia, Canada, United Kingdom, and United States (AUSCANUKUS).
- Global Counter Terrorism Task Force (GCTF): Operation Enduring Freedom
- Combined Naval Forces Central Command (CNFC)
- Multinational Coalitional Forces Iraq (MCFI): Operation Iraqi Freedom (OIF)
- CENTRIXS J: U.S. and Japan
- CENTRIXS K: U.S. and Korea

Several countries such as the United Kingdom, Australia, France, New Zealand, Canada, the Netherlands, Spain, and Japan have adequate communication systems onboard their ships. However, countries such as Pakistan, India, Korea, Thailand, Philippines, Malaysia and Brunei still need support via the Flyaway Kits[114]. Lessons learned from past joint exercises indicate that INMARSAT terminals will also need to be included in the Flyaway Kit in order to achieve an interoperability session.

There are several policy issues, administrative requirements, and process mechanisms negatively affecting the successful and timely exchange of information:

- Communications Interoperability and Security Memorandum of Agreement (CISMOA). This process typically takes from one to two years to execute, and requires negotiation between the Combatant Commander (COCOM) and the other host nations.
- Data Sharing Agreements. Current data sharing agreements are based on specific alliances and operations and approved by the Office of the Secretary of Defense (OSD). This information requires continued updating and the existing process takes extended time for approval.

114 Flyaway Kits – Combination of KG-175 (TacLANE) and Cisco Router. The TacLANE will provide Type-1 data encryption and the router would be configured with specific routing protocol and configuration.

- Cross Domain versus in Domain. Current applications and configurations do not support real time collaboration. The cross domain configuration is limited by accreditation rules and it is not viable for individual access.
- Too many specific networks. Currently, there are six network configurations. It is both time consuming and costly to establish a specific standalone enclave for every individual contingency.
- Lack of integration and interoperability. Current applications and information between US-developed and allied-developed do not have the ability to integrate. The U.S. and coalition networks do not have an efficient way to establish interoperable capabilities.

Due to various issues, critical time and data could be lost due to unclear/undefined guidance on releasable classified and unclassified information among member nations. Nevertheless, inefficient and inadequate information management between U.S. and coalition nations would need to be addressed.

The Multinational Information Sharing (MNIS) and Coalition Information Sharing (CIS) programs have provided guidance for improving the efficiency of information exchange between allied and coalition members. It is important to provide restricted access to U.S. classified networks for allied and coalition exchange officers and embedded staffs, and appropriate Government Agencies as well as private non-governmental organizations, while at the same time, accepting non-U.S.-generated classified data and protecting it in accordance with standards and regulations of the originating party. Since the United States cannot provide interoperability certification for allied/coalition networks or systems, the alternative solution is to provide an Interoperability Assessment of their networks and systems. This method will improve coherency across security domains through common, consolidated data repositories, ensure access to data by cleared users, and maintain data fidelity across domains without over-sanitization. It is necessary to establish streamlined process-oriented system support organization and capability for allied and coalition networks while ensuring the system is complies with:

- Applicable Information Technology (IT) Standards contained in the most current version of the DOD Information Technology Standards and Profile Registry (DISR)
- Joint Interoperability Test Command (JITC) GIG Certification requirements.
- Radio frequency spectrum supportability requirements per DoDD 4650.1[115], as applicable.
- STANAG 5523, the NATO Corporate Data Model.
- Flexibility to ensure prompt modification, addition and deletion of allied and coalition member nation access and permissions, and appropriate Government Agencies.
- Efforts should be made to cultivate international standards for crypto products focusing on the NSA developed releasable High Assurance Internet Protocol Interoperability Specification (HAIPIS).
- Operational rules and testing regimen to govern development of analog and digital Tactics, Techniques and Procedures (TTPs), required by Commanders and staffs to effectively use the information exchanged.

Interoperability is the foundation of effective joint, multinational, and interagency operations. Interoperability is a mandate for the Joint Force of 2020 – especially in terms of communications, common logistics items, and information sharing. Information systems and equipment that enable a common relevant operational picture must work from shared networks that can be accessed by any appropriately cleared participant. There must be a suitable focus on procedural and organizational elements, and decision makers at all levels must understand each other's capabilities and constraints. Training and education, experience and exercises, cooperative planning, and skilled liaison at all levels of the joint force must not only overcome the barriers of

115 DoDD 4650.1 – Department of Defense Directive 4650.1 released on June 8, 2004. The subject of this directive was the policy for Management and Use of the Electromagnetic Spectrum.

organizational culture and differing priorities, but must teach members of the joint team to appreciate the full range of Service capabilities available to them. The future joint force will have the embedded technologies and adaptive organizational structures that will allow trained and experienced people to develop compatible processes and procedures, engage in collaborative planning, and adapt as necessary to specific crisis situations. These features are not only vital to the joint force, but to multinational and interagency operations as well.

b. Releasability

The timely release and sharing of information across security domains is a prerequisite for successful implementation of network-centric warfare across the coalition. Coalition architectures address several of the above steps during the acquisition phase. However, there remains a need for rapid approval and on-site flexibility to adjust the overall configuration for changes in force composition. Cross-domain multi-national authentication and authorization devices need to be developed that allow coalition partners to quickly join tactical and non-tactical networks.

The subparagraphs below present an abridged outline of the current releasability directives and clearly illustrate the challenges in achieving timely shared awareness throughout a coalition force. These policies must be updated to ensure adequate flexibility and timliness in responding to emergent coalition operations.

Documentation to be provided to foreign national must be approved through the appropriate approval channels prior to release. For example, the COMSPAWARSYSCOM Security Programs Office is the approving authority for all release or disclosure decisions to any foreign national. The Public Affairs Office (PAO) is the appropriate office for information in the public domain.

- Typical international agreements include the Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), and Data Exchange Agreement (DEA). Persons contemplating an initiative with a foreign government or international organization that requires an international agreement must seek guidance from the appropriate General Counsel or Staff Judge Advocate.

The Under Secretary of Defense (Policy), (USD(P)), has the responsibility within DoD for authorizing the negotiation and conclusion (signing) of all categories of international agreements. The USD(P), in DoD Directive 5530.3, has delegated some of this authority to other officials within the Department of Defense.

DoD Directive 5530.3 authorizes various DoD Component officials to approve negotiations and the conclusion of certain categories of international agreements. This authority does not relieve the officials from the coordination requirements of the Directive. Moreover, the USD(P) reserves approval authority for all proposed agreements. These agreements involve, among other things, international cooperation in RDT&E or production of defense articles, services or technology and which specifically involve either:

- Disclosure of classified information.
- Technology-sharing or work-sharing arrangements.
- Co-production of military equipment.
- Offset commitments.

DoD Directive 5530.3 also requires the coordination of security provisions for agreements likely to involve the release of CMI, classified technology or classified material with the Deputy to the Under Secretary of Defense (Policy) for Policy Support (DTUSD(P)PS), before making any commitment to a foreign government or international organization. This is to ensure that security provisions are consistent with national and DoD disclosure policies, and that they are consistent with pertinent international security agreements. DoD Directive 5230.11 prohibits the disclosure of classified information or commitments to do so pending a disclosure decision by an appropriate disclosure authority. (See DoD Directive 5530.3 for required coordination for matters other than the disclosure of CMI.)

2. Organization

Organizational changes will be a necessity to transform our current nation-centric coalition force into an integrated force capable of distributed warfare. The transformational architecture outlined in this document requires a bottom-up review of all

coalition platforms to appropriately allocate billet positions in a manner that allows seamless transition across the coalition force.

In order to fully exploit the FORCEnet architecture across the coalition force, the organization needs to evolve from a liaison based methodology to one with "smart" command and control protocols that are readily adaptable to each collation platform and organization. Achieving a truly net-centric organization requires an integrated Command and Control (C2) organization where designated leaders are authorized to assign battle force sensor and weapon resources regardless of national origin.

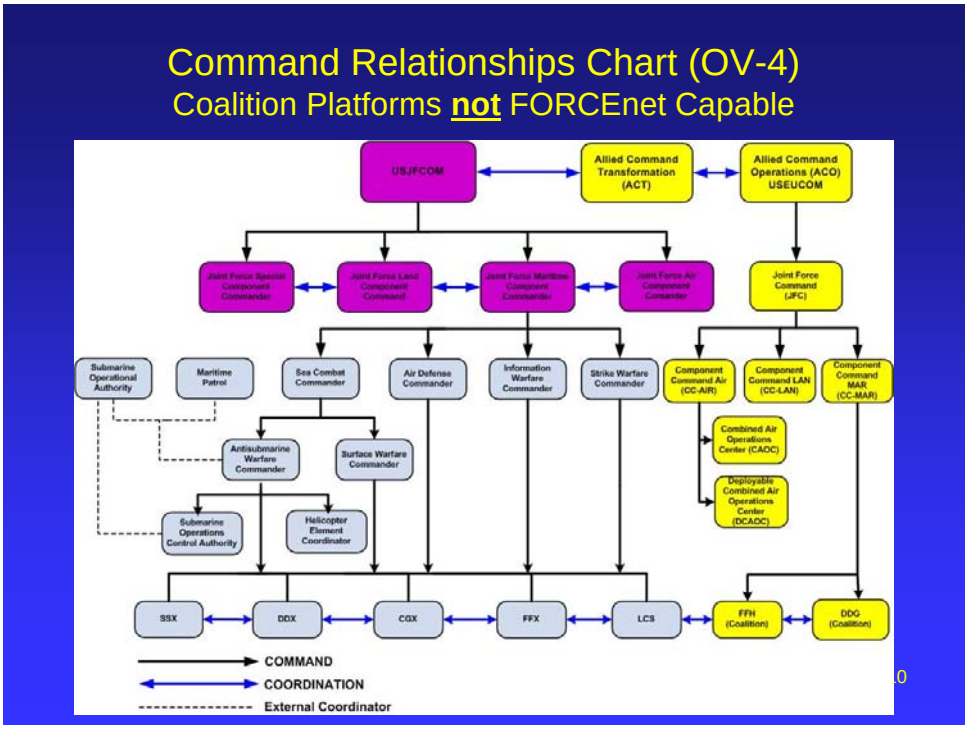


Figure 3-11 OV-4 Non-FORCEnet Capable

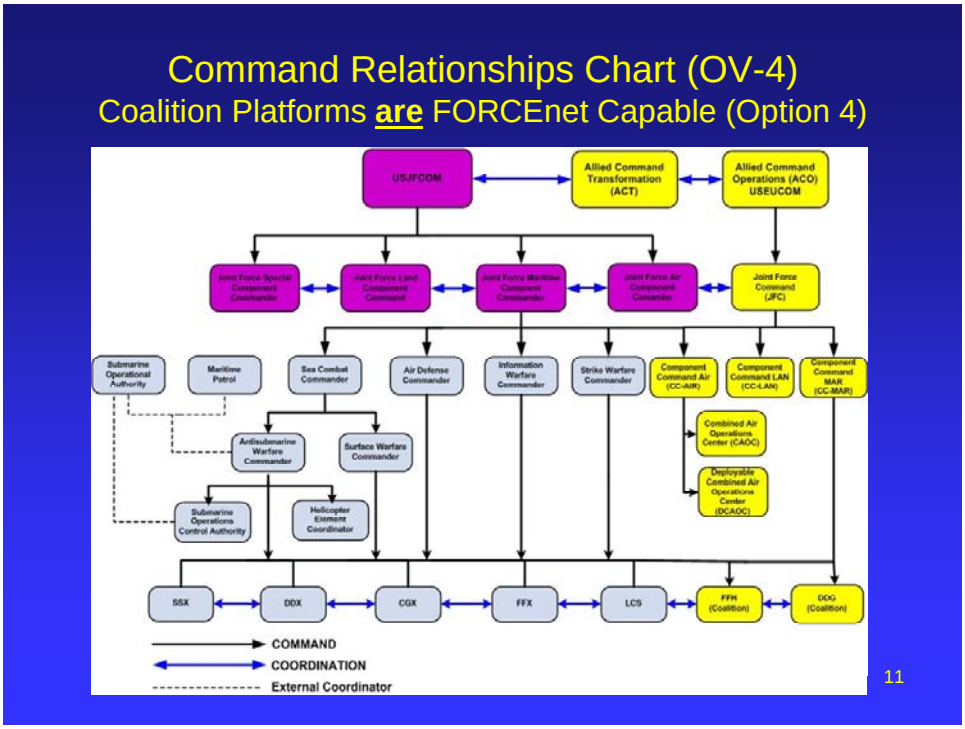


Figure 3-12 OV-4 FORCEnet Capable

3. Training

A multi-tiered training transformation needs to take place along the lines of Sea Warrior, but integrated with Trident Warrior and other Coalition exercises to achieve a cross platform common frame of reference in architecture implementation and execution. Training scenarios need to be refined to account for the FORCEnet transformation. Understanding the cost of assembling a Coalition force at the frequency necessary to keep warfighters proficient would be cost prohibitive. A synthetic architecture needs to be exported to Coalition partners that will allow robust, high fidelity training scenarios to be conducted across the GIG. The synthetic architecture currently in use for U.S. Carrier and Expeditionary Strike Group training should be exported to Coalition partners to allow them to fully participate in planned events. Expansion of shore based training centers and/or Distributed Engineering Plants would provide all Coalition partners another training option for prospective gains and during periods of platform inaccessibility. Of equal importance, is a shore based infrastructure to support/augment maintainers as the complexity of C4ISR systems exponentially increases.

4. Materiel - Human System Integration

The majority of systems in use today are inadequate in supporting the architecture described in this document. Many systems were stop-gap initiatives to quickly fill an emergent need and do not lend themselves well in supporting the warfighter requirements outlined in this document. It is not the intent of this architecture to discard the valuable lessons learned from systems like Composeable FORCEnet, but to build on them in an integrated, sustainable manner. Adaptive networks capable of intelligent, autonomous reconfiguration will be necessary to provide sustainable systems that account for Coalition composition in real time.

HSI/HFE will be depended on heavily to provide systems capable of manipulating several data sources while provide a coherent picture that prevents operator sensory saturation. It is assumed that the implementation of this architecture will not only provide a robust system, but one that is sustainable with an availability (A_o) approaching 100 percent. It is also acknowledged that retreating to a legacy system will not be possible without a significant reduction in warfighting capability. Consequently, the logistics support architecture will need to fully support the integration efforts of U.S. and Coalition forces and the goals of the Tactical Integration plan.

The importance of Human Systems Integration cannot be overstated as highlighted in the following quotes:

- *"The stakes are high…. We must never lose sight of the challenge of a future enemy … an enemy who uses asymmetric means. [But the Navy has] two asymmetric advantages – incredible technology and incredible people…. [Industry must help the Navy improve HIS to] win the battle for finance and be competitive economically in acquisition."*[116]
- *"In the final analysis, the performance of our nation's Sailors makes the difference between victory and defeat… HSI must be established as a budget line item in all programs, not buried in the murky word 'logistics.' Sailors are not logistics elements."*[117]

116 Clark, V. (2003). 2003 Human Systems Integration Symposium

117 Balisle, P. M. (2003). 2003 Human Systems Integration Symposium

The Chief of Naval Operations has recognized human performance as the primary determinant of overall system performance in the FORCEnet transformational core. As discussed in one HSI summary report,[118] *"Unprecedented emphasis on fully integrating the human as a critical element of a cost effective, complex total system from the earliest phases of system design has resulted"*. The HSI requirement while essential, also poses a significant challenge since functions and relationships between FORCEnet's human, process, organizational and technological components are not well understood. Likewise, linkages between concept, policy and architecture that affect the human element's performance are not well understood.

The rapid increase is the amount of battlespace information will require systems capable of rapidly collating a myriad of sources and projecting a coherent picture. Recognizing HSI as an interdisciplinary means to draw from an existing and rapidly evolving body of knowledge that emphasizes human performance as a fundamental dimension of systems performance[119] is central to the described architecture's implementation. In heuristic terms generally accepted by the C4I community: Proper HSI yields improved human performance, which in turns yields improved system performance.

Figure 3-13[120] provides an excellent construct for viewing FORCEnet as a total system comprising a complex mix of human, process, organizational and technological components. Failure to properly integrate HSI into the overall architecture will likely produce a bloated system incapable of providing the warfighter with the right information, in the right format at the right time to effect the right course of action.

---

118 Poirier, J. (2003). Summary Report: FORCEnet Human Systems Integration (HSI) Outreach and Coordination Initiative. Deliverable D007 under Contract T0002AJM032 by Science Applications International Corporation (SAIC)

119 Booher, H. R. (2003). Human Systems Integration Handbook. Publisher: John Wiley & Sons Inc.

120 Poirier, J. (2003). Summary Report: FORCEnet Human Systems Integration (HSI) Outreach and Coordination Initiative. Deliverable D007 under Contract T0002AJM032 by Science Applications International Corporation (SAIC)

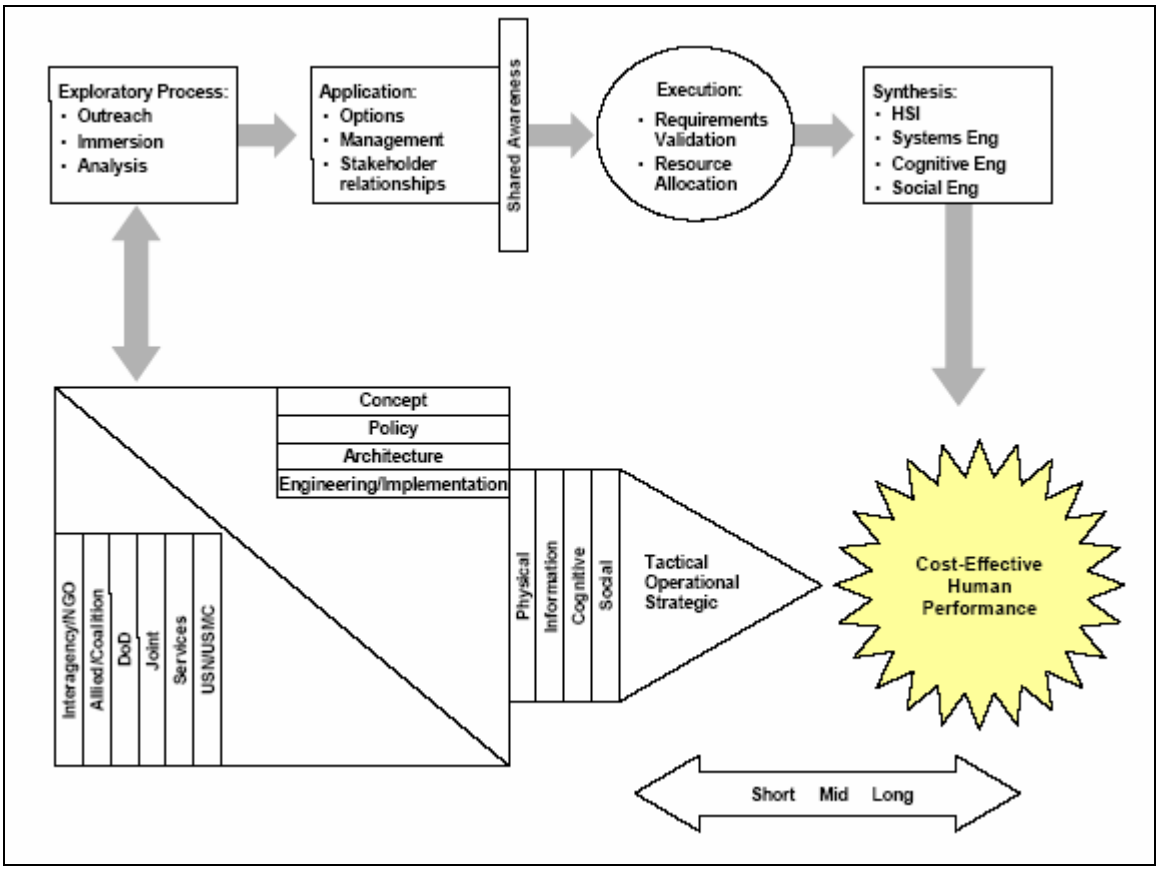


Figure 3-13 Top-Down/Bottom-Up Construct

5. Leadership and Education

Leadership and Education will need to address the training development/continuum of future joint and Coalition command personnel in order for those personnel to accurately assess the battlespace spectrum and provide the necessary direction based on that assessment. Speed of command will require a two-fold reduction in cycle time to counter future threats in the 2015 time frame. Tactics, Techniques and Procedures (TTPs) that evolve during Trident Warrior and Coalition exercises will need to be quickly evaluated and rolled into the architecture as well as doctrine and organization. As discussed above, training for this architecture is a continuum that must integrate all system of systems components into an exportable and releasable Coalition module for real-time, integrated training across the Coalition force. The training scenarios must be high fidelity and current so joint and collation commanders can hone their skills in a battlespace much different from today's – a battlespace that will place a

premium on decision speed. The architecture is predicated on all Coalition forces having similar access to training scenarios, both in single platform and Coalition configurations.

6. Personnel

The architecture fully supports the Navy's future personnel profile and will support manpower projections of future ship classes (CVN-21, LCS, DDX). Data mining concepts explored in this architecture will allow a large repository of information to be managed and configured remotely with a push/pull interface. Data mining also reduces analysis and fusion cycle times as well as personnel requirements to complete these tasks. Added engineering rigor in the development of replication algorithms will allow all platforms to achieve greater efficiency across the manpower spectrum by allowing support functions to be automated with administrative functions completed remotely. The architecture robustness will also allow for high fidelity training, both tactical and technical to be completely across the globe regardless of threat posture.

Through appropriate Human Systems Integration and Human Factors Engineering efforts, this architecture will require fewer personnel per operational cell and those personnel will be able to assimilate mixtures of data quickly in producing a coherent shared awareness picture.

7. Facilities

Existing DoD facilities will require upgrading in concert with the architecture outlined in this document. Equally important, will be a combined doctrine and organization assessment to ensure the theater and support components are synchronized and aligned with the architecture. The proposed architecture requires in-theater control and administration to allow collaboration and shared awareness across the spectrum. The architecture also demands an agile facilities infrastructure to rapidly create and/or modify theater networks for asymmetric warfare.

L. FORCENET (FN) MODELING AND SIMULATION

1. Approach

Modeling the selected vignettes of the scenario required the development of simulations that represented capabilities of the FORCEnet architecture for the Blue (US and Coalition) force. The battle force operation consists of three layers grid: Sensor

grid, command and control (C2) grid, and Engagement grid. For platform-centric architectures, these grids are stove piped and platform independent. The information from a platform is not necessarily available to the other platforms in the battle force. For the FORCEnet architecture, the grids must be integrated and networked for the entire battle force in order to achieve the information superiority-enabled concept. This integrated networking concept is shown in Figure 3-14.

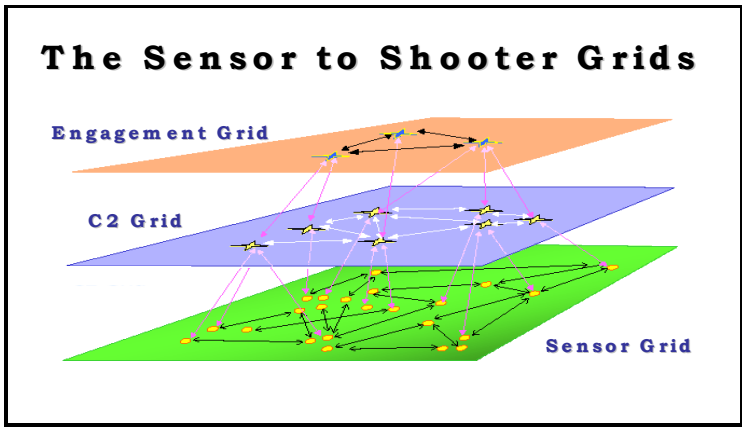


Figure 3-14 FORCEnet Integrated Networking Concept

This figure shows that at the sensor grid, the sensor data from one platform is available to any platform in the network/battle force. This enables platform(s) to perform parallel search using the sensor resources available in the battle force. At the C2 grid, the netted sensor data allows platform(s) to perform data fusion to obtain a more accurate picture of the object/target being track. At the Engagement grid, the network-centric concept allows platform(s) to have the Integrated Fire Control. Various concepts for IFC are shown in Figure 3-15[121].

[121] Integrated Fire Control for Future Aerospace Warfare, by B. W. Young, August 2004

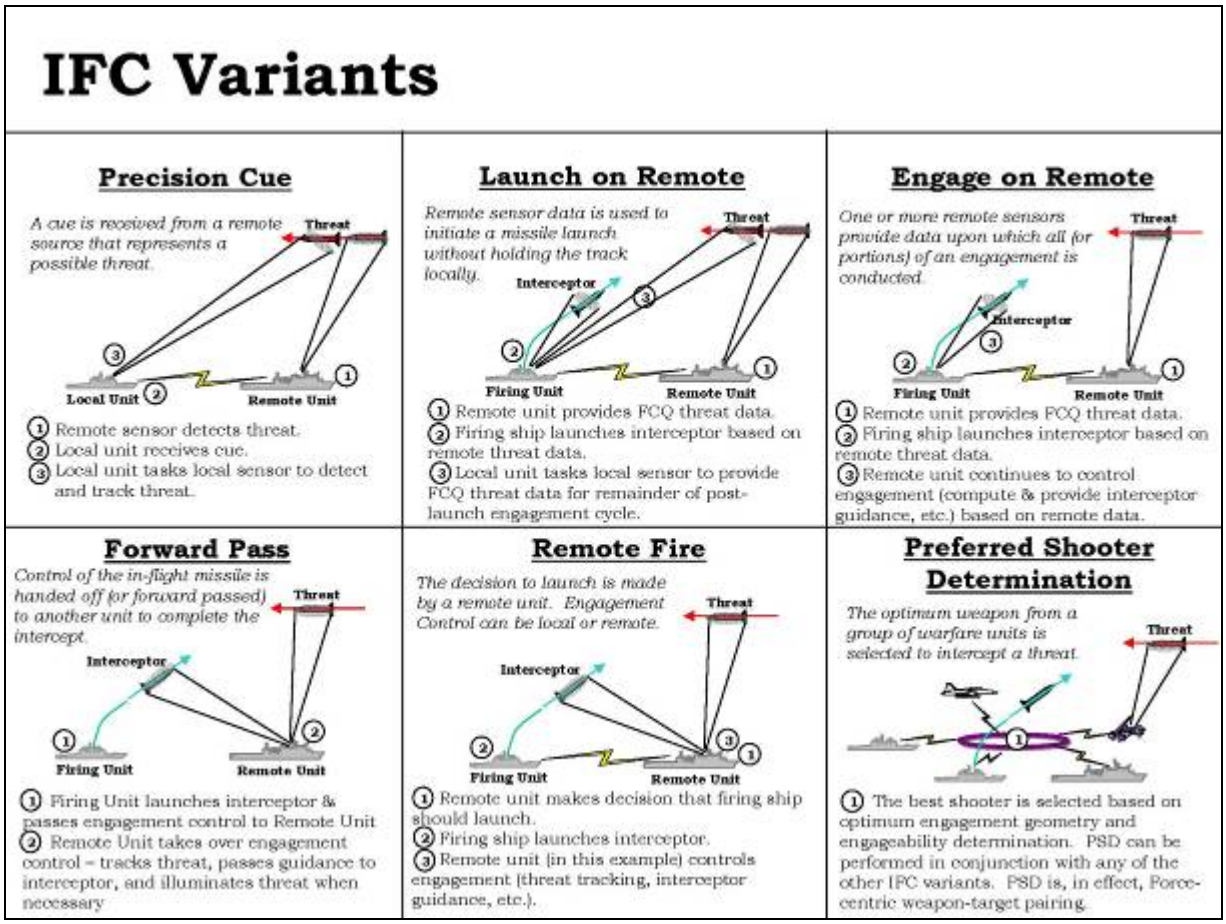


Figure 3-15 Integrated Fire Control Variants

The ability to perform data fusion and integrated fire control are not available in platform-centric architectures. These capabilities were modeled to compare the performance between platform-centric and network-centric warfare.

In addition to modeling the above mentioned capabilities, some of the theoretical analysis approaches are also used to estimate the probability of detection for different sensors. For example, a Random search model is used to provide a conservative estimate for the probability of detection (Pd) for sensors, which is used as an input into the model. For a more granular search such as submarine search, an Inverse Cube model is used. The equations used for the Random search model and the Inverse Cube model are provided below:

1. Random Search Model:

$$\text{CDP:} \quad F_T(t) = 1 - e^{-\lambda t} = 1 - e^{-vWt/A}$$

$$E[T] = \frac{1}{\lambda} = \frac{A}{vW}$$

$CDP = cumulative\_\det ection\_probability$
$v = speed$
$W = sweep\_width$
$t = time\_on\_station$
$A = total\_area$

2. Inverse Cube Model:

$$P_d = 2\left[\Phi\left(1.253\frac{W}{S}\right)\right] - 1$$

Where,

P_d = probability of detection

Φ = standardized, normal probability density function with mean 0 and variance of 1

W = sweep width

S = spacing between platforms searching in parallel

Z = 1.253* W/S

The following assumptions are made for the modeling effort:

- Reasonably faithful to reality for 2015 timeframe.
- Capability Gaps are the focus of the EXTEND model: Parallel Search, Data Fusion Resource manager, Integrated Fire Control.
- Goal is not to solve the scenario – it is to show FN capability gaps and benefits.
- FN uncertainties: not every missile leaves the launcher, not every missile will be detected, unpredictable weather, etc.
- Discrete event model with three vignettes running simulations in sequence.
- Pd and Pk are estimated using Inverse cube, random search, and binomial distribution models

2. Measures of Performance (MOP)

Table 3-10 provides the MOPS that are used to evaluate the results:

Table 3-10 Measure of Performance (MOPs)

Grid	Measure of Performance (MOP)
Sensor (Detection)	# (targets) detected # (targets) not detected
Command and Control (C2)	total # identified (enemy ship) # identified (non-hostile) # subs identified # subs not (detected on slide) identified # missiles identified # missiles leakers # tracked via precision cue (all threats)
Engagement	total # missiles engaged via IFC # engaged (platform-centric) # enemy killed total # of leakers # blue hits suffered (if only one engagement)

M. IMPLEMENTATION

The model is implemented as a discrete event model using the Extend simulation program. (The Extend modeling and simulation program is more fully covered in Appendix C.) The simulation represented the scenario and provides the information output of a Sensor grid, C2 grid, and an Engagement Grid. The goal is to send the output of the simulation into a Geographical Information System (GIS) to provide the decision maker the common operational picture (COP). Figure 3-16 summarizes the high-level

diagram of the modeling approach. The simulation was developed in ten iterations and is described in Appendix C.

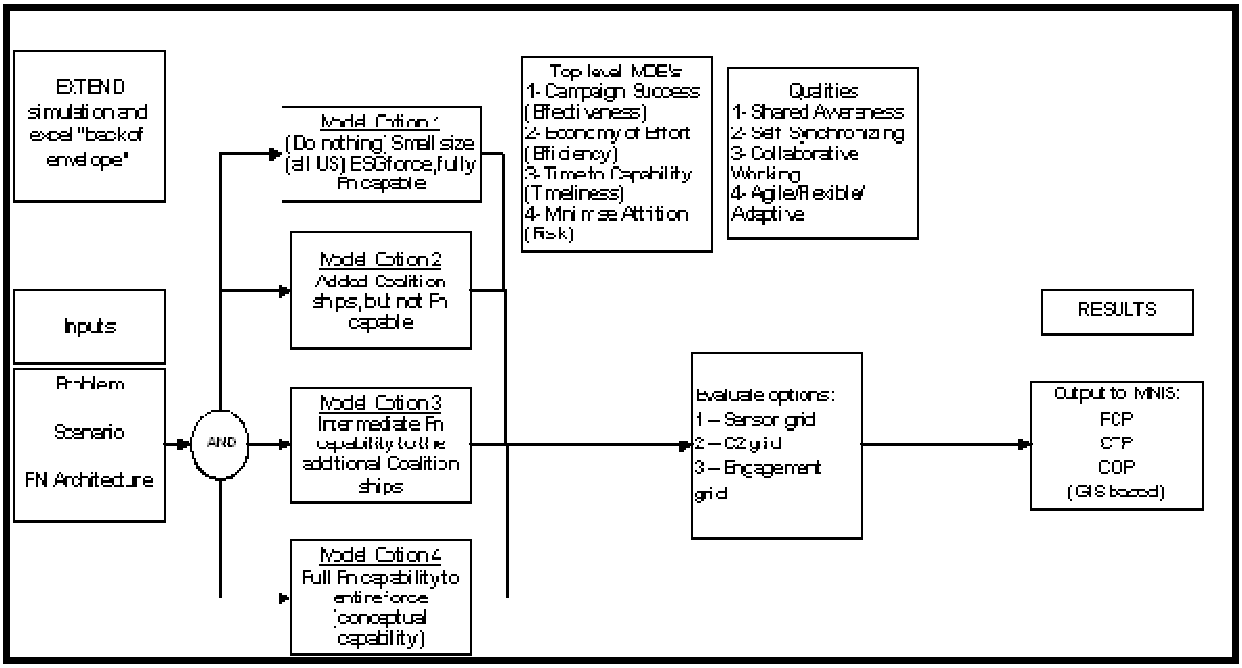


Figure 3-16 High-Level Diagram of the Modeling Approach

a. Sensor Grid Model

The probability of detection increases when sensors are in parallel. All discrete event models in Extend must have an Executive block and it must be placed in the top left hand corner for the model to work. For the input to the sensor grid a "program block" was used, which allows multiple inputs onto the model. The output of the program blocks provides the enemy ships, missiles, submarines, and non-hostile ships for the sensor grid to detect. The model also integrated the three mission threads ASW, ASuW, and AMSD into one model.

(3) Integrated Inputs to Model

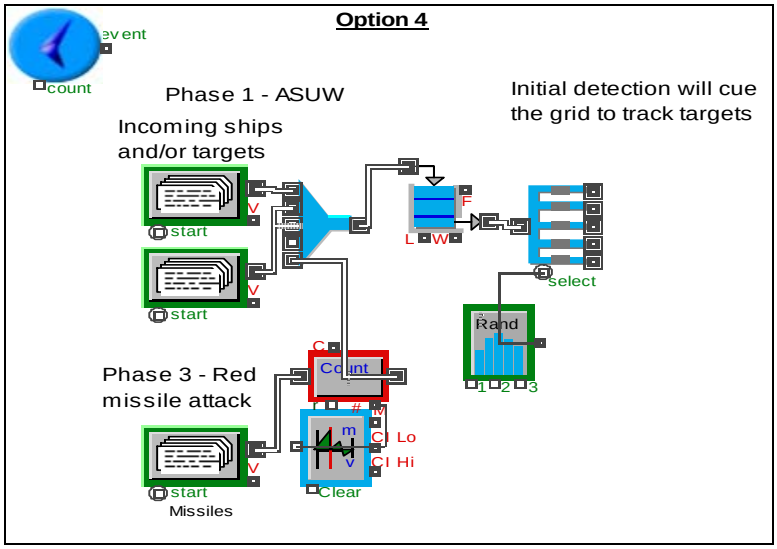


Figure 3-17 Integrated Model

To simulate sensors in parallel using Extend, a "Select DE output" block was used to represent the Force Composition platforms (ships, aircraft, etc). The "Select DE output" selects the input item to be output at one of two output connectors based on a decision. This detection decision was based on the estimated probability of detection using the random search model. Sensors were placed in parallel. Figure 3-18 shows the platforms in parallel. A "combine 5" block combines the detected targets and outputs to the C2 grid.

b. Sensors in Parallel

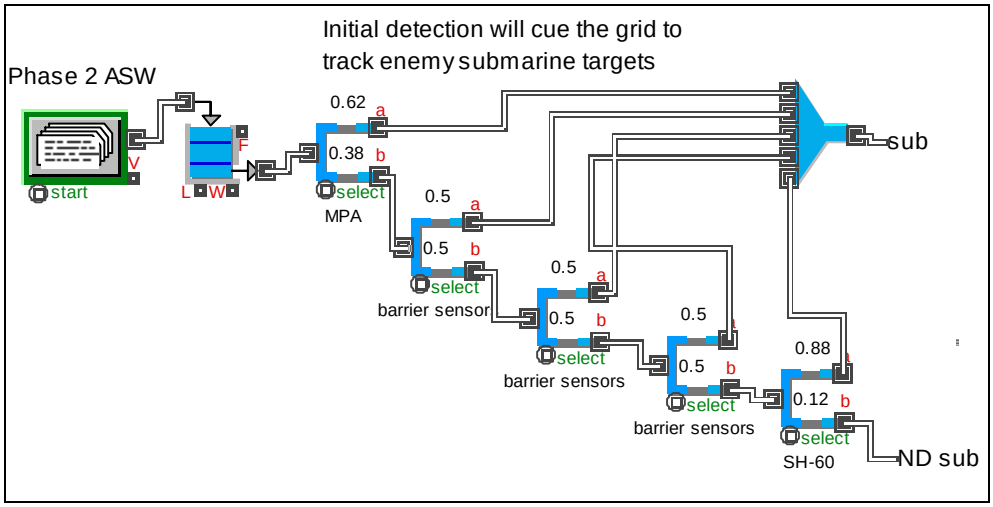


Figure 3-18 Parallel sensor model

c. C2 Grid Model

The output of the sensor grid feeds into a Data Fusion Resource Manager (DFRM). The DFRM is considered a capability gap because there is no technology currently available that can "fuse" information. It requires all network-centric platforms to share and fuse information together to accurately provide the common operational picture, common tactical picture, and fire control picture. To develop this model, attributes were assigned to the targets being detected. The attributes are assigned in the program block and are seen as red circles. When running the model, the red circles are detected in the sensor grid and then they input into the C2 grid. In the C2 grid the detected targets are fused together with intelligence information and attribute data to clearly identify the target. At this point in the model, the red circle would be identified and "appear" as a ship, submarine, missile, or non-hostile ship. The identified targets are sorted, counted, and then "precision cued" to assign ships to track and if necessary engage the enemy through integrated fire control. The output of the DRFM inputs to the engagement grid.

To develop the C2 grid, refer to Figure 3-19, the targets from the Sensor grid are routed to an "animate attribute" block. This block will read the attribute information of the incoming target and fuse the intelligence data to identify the target. Here the detected target would be identified and the animation would change from a circle to a ship, sub, or missile. The identified targets are routed through a count block and then into a FIFO queue for processing. The output of the FIFO queue flows into a "get attribute" block. This block reads the fused information and sorts the targets based on attribute data. This allows the Select DE 5 block to only send ships through the top path, non-hostile ships through the second path, missiles through the third path, and subs through the fourth path. This sorting processing allows the tracking of the number of each type of incoming target and also allows the simulation to "precision cue" the targets to the best platform to track. Next, a "combine 5" block and a FIFO are used to route targets to the precision cue stage. A random block is used to assign a uniform distribution to cue platforms to track detected and identified targets (Figure 3-20). Through the DFRM all platforms in the FN will see the same picture.

d. Data Fusion Using Attribute Information

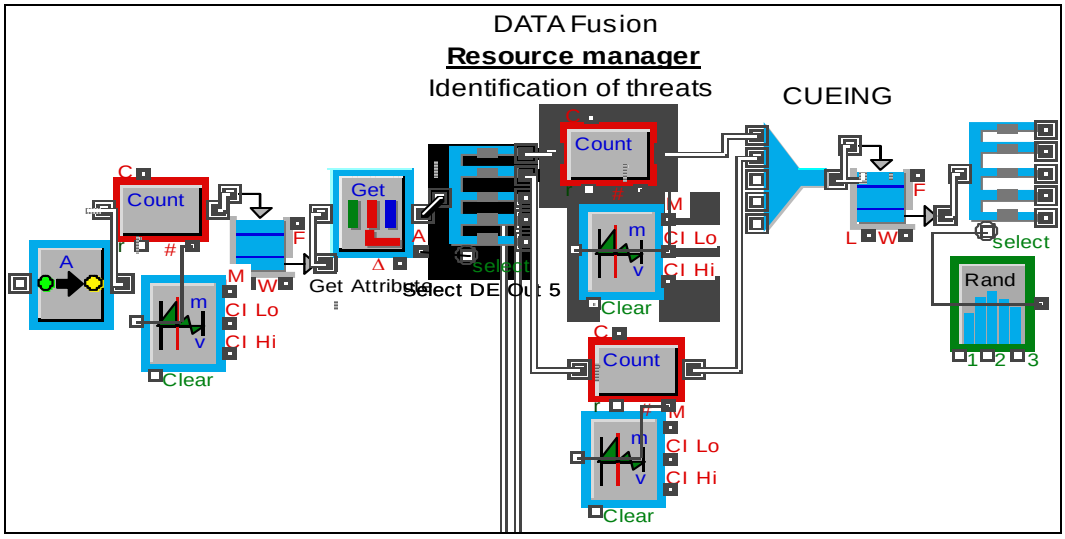


Figure 3-19 Data Fusion Model

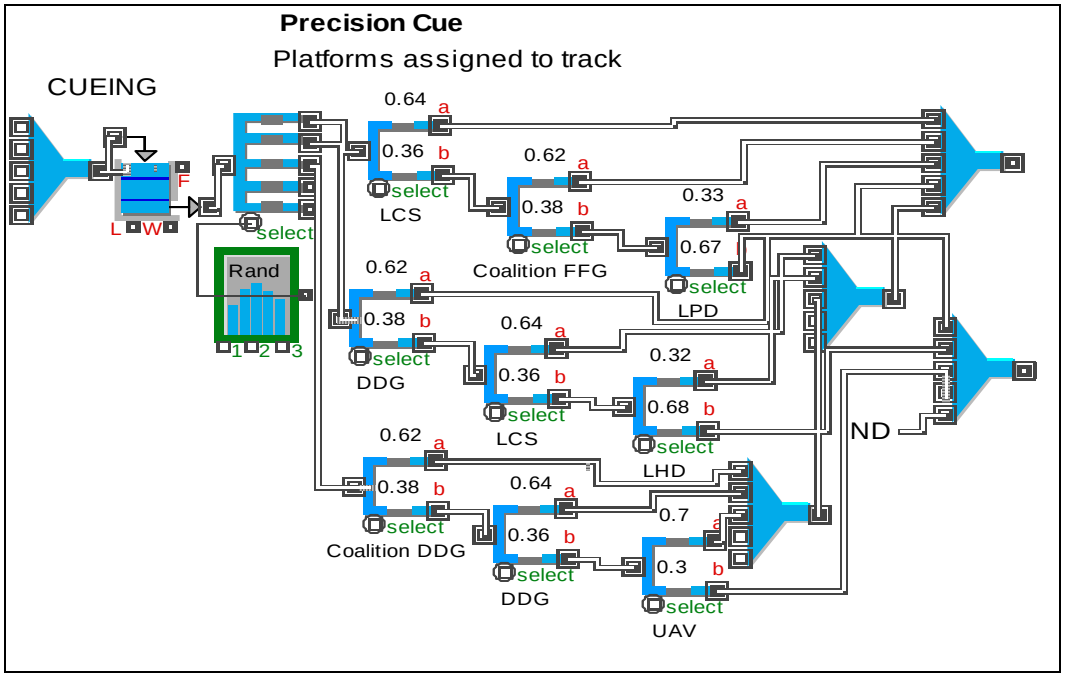


Figure 3-20 Cueing model

e. Engagement Grid

The output of the C2 grid inputs into the Engagement grid. This portion of the model represented the integrated fire control concepts of “launch on remote, engage

on remote, remote fire, and forward pass." The scenario required the Coalition to engage a missile attack. There were several possibilities: all the detected missiles were engaged, some missiles that were not detected, some missiles that were engaged but were missed or there was a failure. The few missiles that got through hit blue ships and some missed blue ships. Refer to Figure 3-21.

It was important to use the correct distribution throughout the model to be as realistic as possible. For the input all detected targets were being tracked through precision cueing. The resource manager determined the best shooter. To simulate selection of the "best shooter" use an activity service block with a lognormal distribution and a Select DE 5 block with a Poisson distribution to estimate arrival rate. The output of the Select DE 5 block is considered the "best shooter."

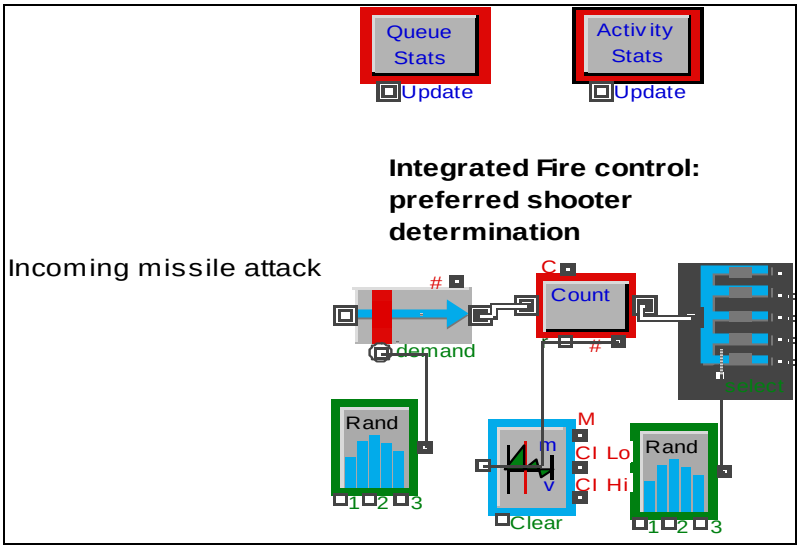


Figure 3-21 Integrated Fire Control model

The input is a FIFO block. Below in Figure 3-22 is an example of how to model "launch on remote." The remote unit is an activity delay block with a normal distribution. In this case the remote unit is an LCS ship which tracks the incoming missiles, and provides the tracking data to the DDG ship. The DDG will then engage the incoming missiles using the LCS track data. An activity delay block was used for the DDG with an exponential distribution to represent the engagement fire. The number of missiles being killed was estimated using the binomial distribution at the end in a Select DE 2 block.

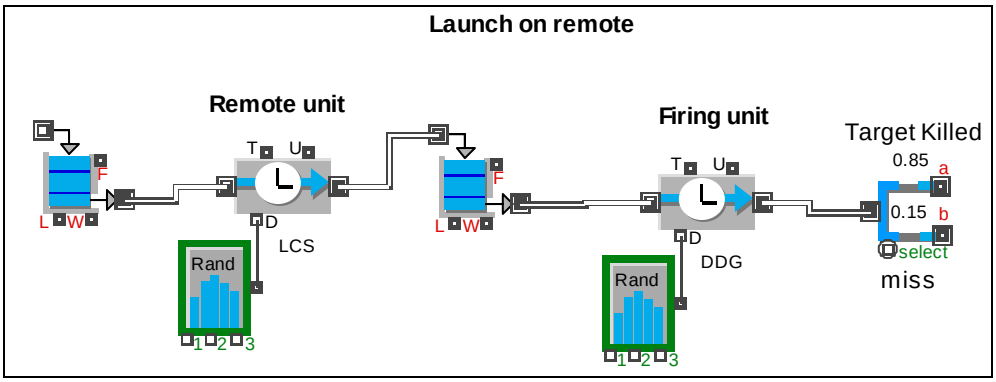


Figure 3-22 Engagement model

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS

A. SENSOR GRID RESULTS

Tables 4-1, 4-2, and 4-3 summarize the simulation results for the sensor grid, the C2 grid, and the Engagement grid, respectively. These results were obtained after 10,000 runs from the model with a 95% confidence interval.

Table 4-1 Sensor Grid Results

	Detection Grid # detected	# not detected	**Rank**
Option 1	128.38	0.78	2
Option 2	90.66 + 32.7= 123.36	0.32 + 5.58 = 5.9	4
Option 3	127.14	1.86	3
Option 4	129.1	0.44	1
	C2 Grid total # identified (enemy)	# identified (non-hostile)	# subs identified
Option 1	6.96	27.88	1.88
Option 2	4.74	19.62	1.87
Option 3	6.9	27.76	1.92
Option 4	6.98	27.91	1.95
	C2 Grid # subs not detected	# missiles identified	# missile leakers
Option 1	0.12	91.38	8.82
Option 2	0.13	82.3	6.4 + 3.22 = 9.62
Option 3	0.08	90.48	8.56
Option 4	0.05	91.4	6.9

Table 4-2 Grid Results

	all threats # tracked via precision cue	**C2 grid Final Rank**
Option 1	128.1	3
Option 2	90.53	4
Option 3	127.06	2
Option 4	128.24	1

Table 4-3 Engagement Grid Results

	Engagement Grid		
	total # missiles engaged via IFC	# engaged (platform-centric)	# enemy killed
Option 1	83.18	0	73.72
Option 2	58.12	20.08	51.26 + 16.78 = 68.04
Option 3	83.44	0	77.26
Option 4	88.1	0	85.3
	Total # of leakers	(if only 1 engagement) # blue hits suffered	**Engagement Grid Final Rank**
Option 1	18.28	5	3
Option 2	21.2	6	4
Option 3	14.6	4	2
Option 4	6.1	2	1

Based on the above results, Option 4 provides the highest Fn capabilities and also had the best results. Option 2 had the worst results. This is due to the non-Fn capability of the Coalition forces. The results show that Fn provides the following improvements:

- Sensors – 5% improvement in number of threats detected.
- C2 – 42% improvement in tracking via precision cue.
- Engagement – 25% improvement in threat neutralization.

B. MODELING AND SIMULATION SUMMARY

The results show that Fn provides improvement in all three areas of operation: Sensor grid, C2 grid, and Engagement grid. Network-Centric war-fighting is value added to Coalition Forces. Non-FORCEnet forces sustain higher casualties. Option 4 had the highest FN capabilities and also had the best results. Option 2 had good results but finished last.

Modeling conceptual FORCEnet architecture capabilities through simulation was accomplished successfully after integrating the three mission threads into one model. This allowed attribute data to be fused to clearly identify incoming targets. Additionally, the model was developed as a mini prototype of how a sensor grid could provide information to a GIS to assist in decision making.

The output of the simulation provided information for a common operational picture to be displayed on a GIS map (Figure 4-1). Refer to Appendix B for more detailed GIS information.

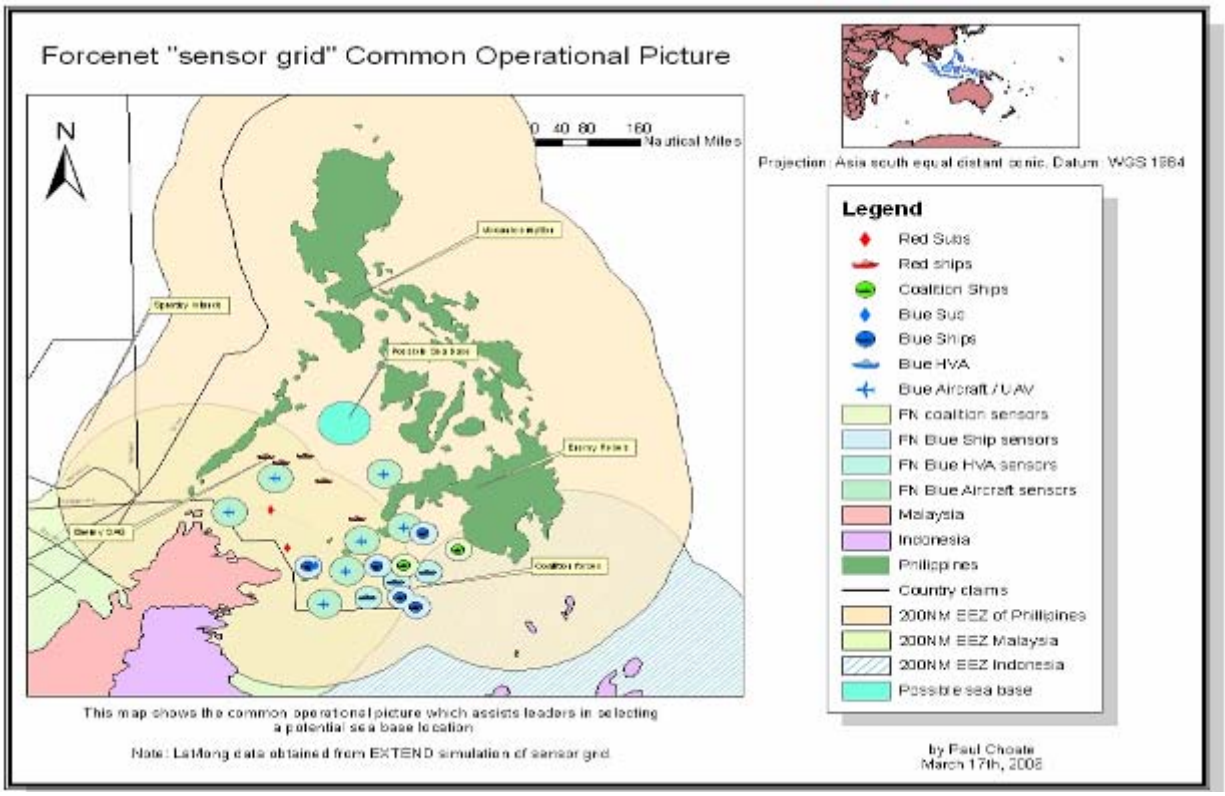


Figure 4-1 FORCEnet Common Operational Picture

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This effort has identified desired capabilities to improve U.S. and Coalition warfighting effectiveness in a network-centric environment. It has:

- Explained the advantages provided by FORCEnet as described in existing literature and policy documents
- Identified Command, Control, Communications, Computers, and Intelligence (C4I) capabilities required to achieve improved Situational Awareness (SA) and warfighting effectiveness
- Determined that materiel solutions must be accompanied by a common Concept of Operations (CONOPS) and agreement in Tactics, Techniques, and Procedures (TTPs). Essential among these are:
    - Timely and Effective Releasability Policy
    - Unity of Command and Control (C2)
    - Adequate Peace-Time Training
- Demonstrated, through Modeling and Simulation (M&S), that implementation of the recommended materiel and non-materiel capabilities will result in a quantifiable warfighting improvement.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: ARCHITECTURAL ARTIFACTS

A.1 Architectural Frameworks

Architectural frameworks provide a standard format for describing architectures. The framework used for this project is the DoD Architecture Framework (DoDAF) Version 1.0. Section 1.1 of the DoDAF describes the purpose of the Framework in the following manner:

> ". . . to provide guidance for describing architectures for both warfighting operations and business operations and processes. The Framework provides the guidance, rules, and product descriptions for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating Families of Systems (FOS), Systems of Systems (SoS), and interoperating and interacting architectures."[122]

Part of this project was to understand the System of Systems that will potentially be part of FORCEnet and to compare and quantify warfighting effectiveness based on forces that are either partially or completely FORCEnet capable. The DoDAF is an excellent tool for presenting the architectures and supporting this comparison.

A.1.1 Architectural Views

Within the DoDAF, architectures are described from a number of perspectives or views. The DoDAF contains three major views: operational, system and technical, and also contains views that relate to all perspectives called all views.

According to Mark W. Maier and Eberhardt Rechtin in their book *The Art of Systems Architecting*, the operational view ". . . shows how military operations are carried out through the exchange of information. It is defined as a description of tasks and activities, operational elements, and information flows integrated to accomplish military operations".[123] System views are described by Maier and Rechtin as "a description, including graphics, of a system and interconnections providing for, and

[122] DoD Architectural Framework Version 1.0, Volume I: Definitions and Guidelines (Department of Defense, [2004]), 1-1.

[123] Mark W. Maier and Eberhardt Rechtin, *The Art of Systems Architecting* (Boca Raton: CRC Press, 2002), 224.

supporting, warfighting functions".[124] A technical view, according to Maier and Rechtin, is ". . . defined as a minimal set of rules governing the arrangement, interaction, and interdependence, of systems, parts, or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements".[125]

A.1.2 Views Used for this Project

A list of the specific views that were used for this project include:

- OV-1 – High Level Operational Concept Graphic
- OV-2 – Operational Node Connectivity Description
- OV-4 – Organizational Relationships Chart
- OV-5 – Operational Activity Model
- OV-6c – Operational Event-Trace Description
- SV-1 - Systems Interface Description
- AV-1 – Overview and Summary Information
- AV-2 – Integrated Dictionary

These views were created for this project as they would best convey the nature of the FORCEnet system of systems to the stakeholders, to support the comparison of warfighting effectiveness for various force compositions and levels of FORCEnet, and to provide the necessary presentation materials for the project briefings.

A.2 Operational Views

A.2.1 High Level Operational Concept Graphic (OV-1)

According to Volume II of the DoDAF, the purpose of the OV-1 diagram is to provide a quick, high-level description of what the architecture is supposed to do and how it is supposed to do it. The DoDAF further indicates that the graphic is useful in facilitating communication and is generally presented to high-level decision makers. When other views are required for a system, these views will flow from the OV-1 through an analysis of the operational nodes, identification of information exchange requirements and mapping of systems functions to physical systems.

---

[124] Mark W. Maier and Eberhardt Rechtin, *The Art of Systems Architecting* (Boca Raton: CRC Press 2002), 225.

[125] Ibid., 226.

A.2.1.1 Coalition FORCEnet OV-1

The OV-1 diagram for this project, shown in Figure A-1, shows the high-level operational concept graphic describing the Future FORCEnet system. The central entity of this system is the future communications network. It depicts United States (US) and Coalition forces functioning together using FORCEnet (Fn) to defeat air, surface, subsurface, and land threats. Linking the U.S. and Allied nodes makes the total force much larger and more integrated.

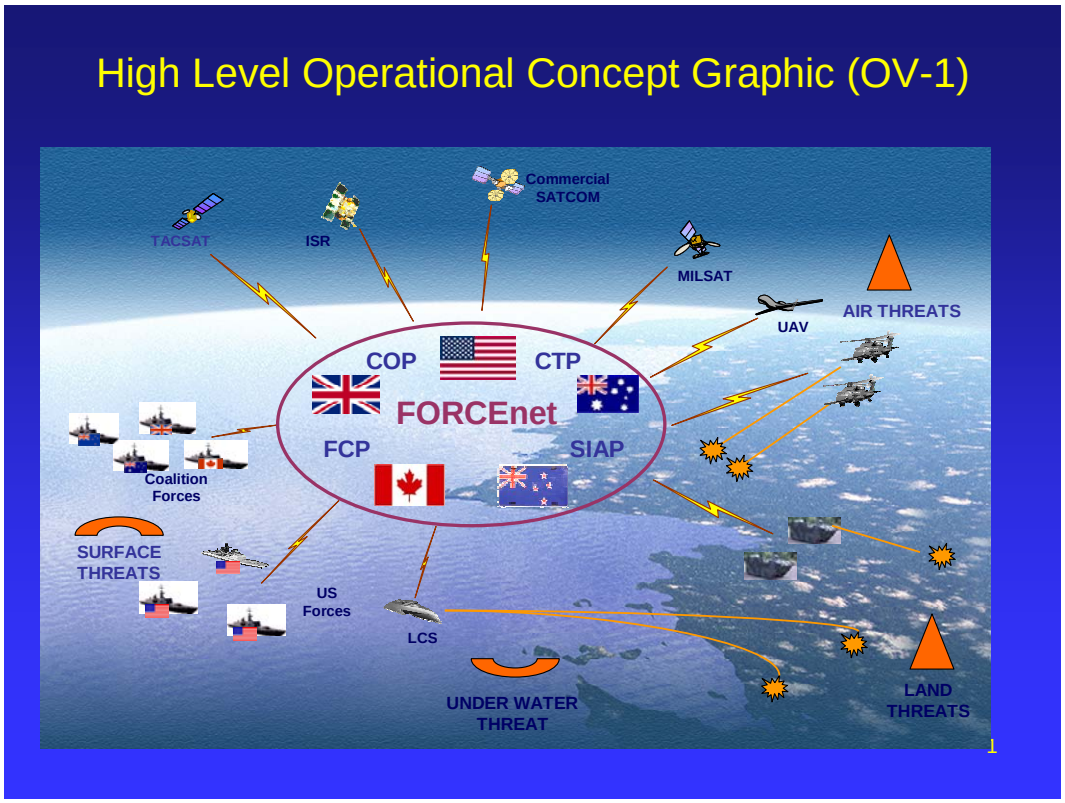


Figure A - 1 OV-1

A.2.2 Operational Node Connectivity (OV-2)

According to Volume II of the DoDAF, the purpose of the OV-2 diagram is to graphically depict operational nodes or organizations with needlines between them that indicate a requirement to exchange information between them. An operational node is an element that produces, consumes, or processes information.

The needlines only indicate a need to exchange information. The manner in which the information exchange occurs is not provided by this diagram.

A.2.2.1 Coalition FORCEnet OV-2

Two OV-2 diagrams were created for this project and are shown in Figures A-2 and A-3. One diagram shows the information exchange between nodes when the Coalition platforms are not Fn capable (Figure A-2). This corresponds to Fn level 0 as defined in the following table:

Table A - 1 FORCEnet Levels

FORCEnet Level	**Benefits/Characteristics:**
0	No FORCEnet**.** Vessels use voice radio and Link 11 or 16 to share situational awareness and C2 data. Platform-centric in character.
1	Filtered, delayed, low bandwidth (dialup) FORCEnet (like 'no FORCEnet', but higher fidelity/faster updates). ESG/CSG has access to reach back and has the ability to distribute intelligence information gained from that to all ESG/CSG members. Information from organic sensor and intelligence data is available with some time delay throughout ESG/CSG. Recognized maritime picture (RMP) which fuses organic and other ESG/CSG data is distributed with minor time delays.
2	Real-time targeting information gained from any U.S. or Coalition asset/source (when latter is technically capable) is available to all ESG/CSG vessels as required. Access to targeting information is assured within understood limitations. Information accuracy, timeliness and coverage continuity are assured up to predefined levels. Rapidly updated RMP is available to all ESG/CSG vessels.
3	Weapons systems are networked but are only able to be controlled by national authority.
4	Vessels of all Coalition nations are technically and politically/militarily able to offer weapons systems as a network service for command by approved authorities from any of the nations within the ESG/CSG.

The second OV-2 diagram (Figure A-3) shows the information exchange when the Coalition platforms are Fn capable. The diagram is the same for FORCEnet levels 1 – 4 since the OV-2 diagrams merely show information exchange between nodes without regard for the timeliness of the data or the type of data. For example, two platforms

exchanging organic sensor and intelligence data with some time delay is depicted in an OV-2 in the same way as two platforms exchanging real-time targeting data.

Common to both OV-2 diagrams (Figure A - 2 and Figure A - 3), are some number Fn capable platforms connected on a theater network, primary and secondary GIG interface units, and representative organizations that supply and consume information to or from the theater platforms. One of the Fn capable platforms in the theater is designated as the "Super-Node" and another is designated as the "Auxiliary Super-Node". The Super-Node is a designation given to the senior capital ship of the battlegroup (BG) and is also assigned the role of exchanging information between the theater network and nodes on the GIG. In this role, the Super-Node is responsible for both publishing information to the GIG and subscribing to information from nodes of interest on the GIG. Additional details of the GIG information exchange is provided by the OV-5 diagrams, shown later in this appendix. The Auxiliary Super-Node is the designation of any additional capital ships that are capable of assuming Super-Node responsibilities. The Auxiliary Super-Node automatically assumes the role of the primary in the event of a Super-Node failure.

The theater network provides the means to exchange information between Fn capable platforms in the theater. As such, when Coalition platforms are not Fn capable, as is shown in Figure A - 2, the Coalition platforms are not connected to the theater network. Instead, the Coalition platforms exchange information via systems like Link-11 or Link-16. One of the units on the theater network acts as a data forwarder between the Coalition platforms on the tactical data link and the theater network. In this configuration, the Coalition platforms are limited by the data that is supported by the tactical data link. A Coalition platform using Link-11 could not receive imagery data since Link-11 does not support imagery. Figure A - 3 shows Coalition platforms that are Fn capable and are connected to the theater network.

Two types of platforms are present on the theater network – U.S. primary/Coalition platforms (shown in blue) and Other US/Coalition platforms (shown in green). The blue platforms are larger, more capable platforms that participate directly on the theater network. Examples of these more capable platforms are CGs, DDGs and

larger platforms. The green platforms are smaller, less capable platforms, such as a maritime patrol aircraft, helicopters and unmanned vehicles, which do not directly participate on the theater network. Instead, these platforms have a point-to-point connection with a larger platform which provides the conduit to the theater network and the GIG.

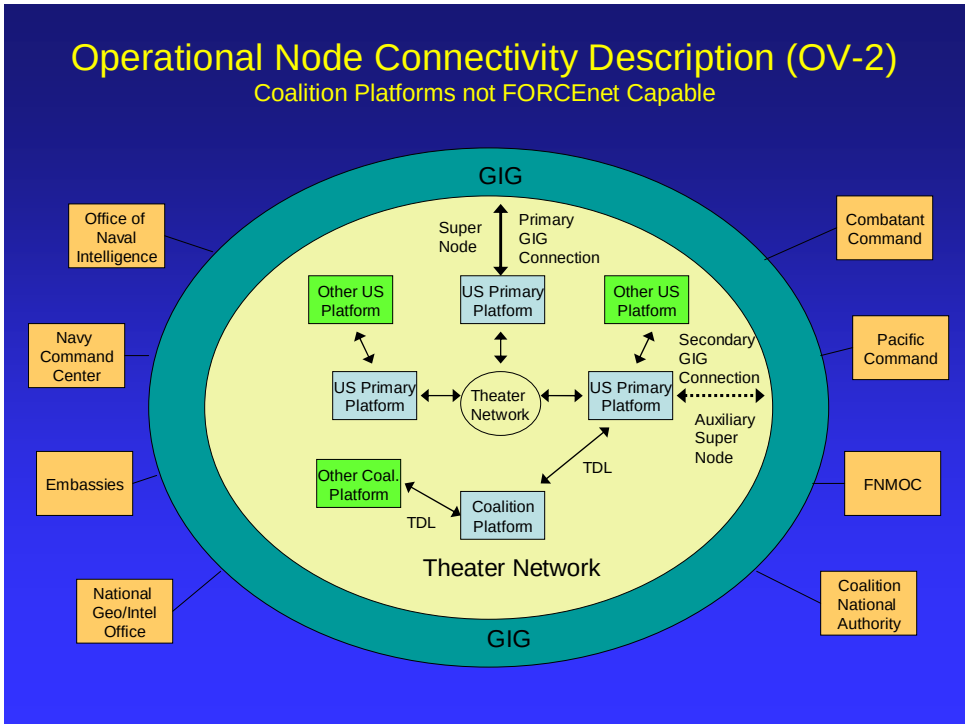


Figure A - 2 OV-2 Non-FORCEnet Capable

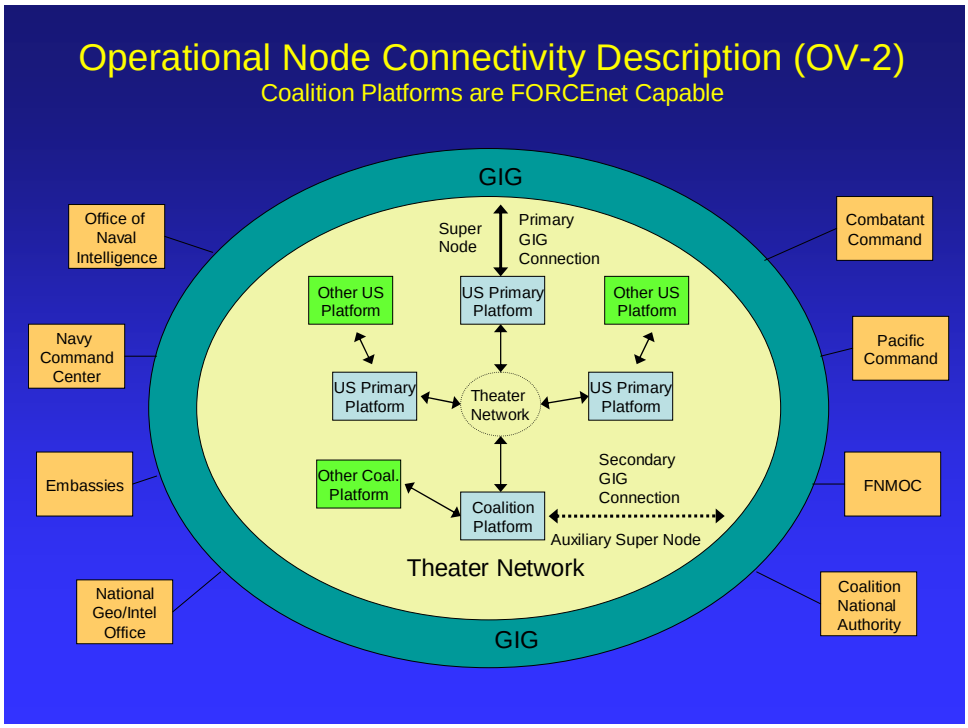


Figure A - 3 OV-2 FORCEnet Capable

A.2.3 Command Relationships Chart (OV-4)

According to the DoDAF, the OV-4 "illustrates the command structure or relationships (as opposed to relationships with respect to a business process flow) among human roles, organizations, or organization types that are the key players in an architecture."[126] Examples of relationships provided in the DoDAF are supervisory reporting, command and control, command-subordinate, and coordination between equals.

A.2.3.1 Coalition FORCEnet OV-4

Two OV-4 diagrams were created for this project. One diagram (Figure A - 4) shows how Coalition command structure is set up when it does not have a completed FORCEnet capability (FORCEnet Level 0, 1 and 2). The other diagram (Figure A - 5) shows the commands relationships that are fully Fn Capable (FORCEnet Level 4). The diagram is the same for FORCEnet levels 1 – 4 since the OV-4 diagrams do not show the type of information exchange between nodes.

126 DoD Architectural Framework Version 1.0, Volume II: Product Descriptions (Department of Defense, [2004]), 4-27.

Common to both OV-4 diagrams (Figures A - 4 and A - 5), is that U.S. JFCOM (Joint Force Command) would provide the overall command and control information and decision to all U.S. component commands such as Joint Force Special Component Command, Joint Force Land Component Command, Joint Force Maritime Component Command and Joint Force Air Component Command and collaborate (shown as blue lines) with allied commands which will provide information and direction to their subordinate commands on information sharing. When the Coalition forces are not Fn capable (Figure A - 4), the information flow would only be from the Joint Force Command (JFCOM) that is established by Coalition forces. In such case, all forces (US and allied) may experience uncommon operational pictures and delaying Command and Control (C2) information update. This time delay would make collaboration extremely difficult. However, when forces are Fn capable (Figure A - 5), it would enable all participants in the network to have common operational and tactical information. Hence, collaboration process between U.S. and allied countries would become better and more efficient.

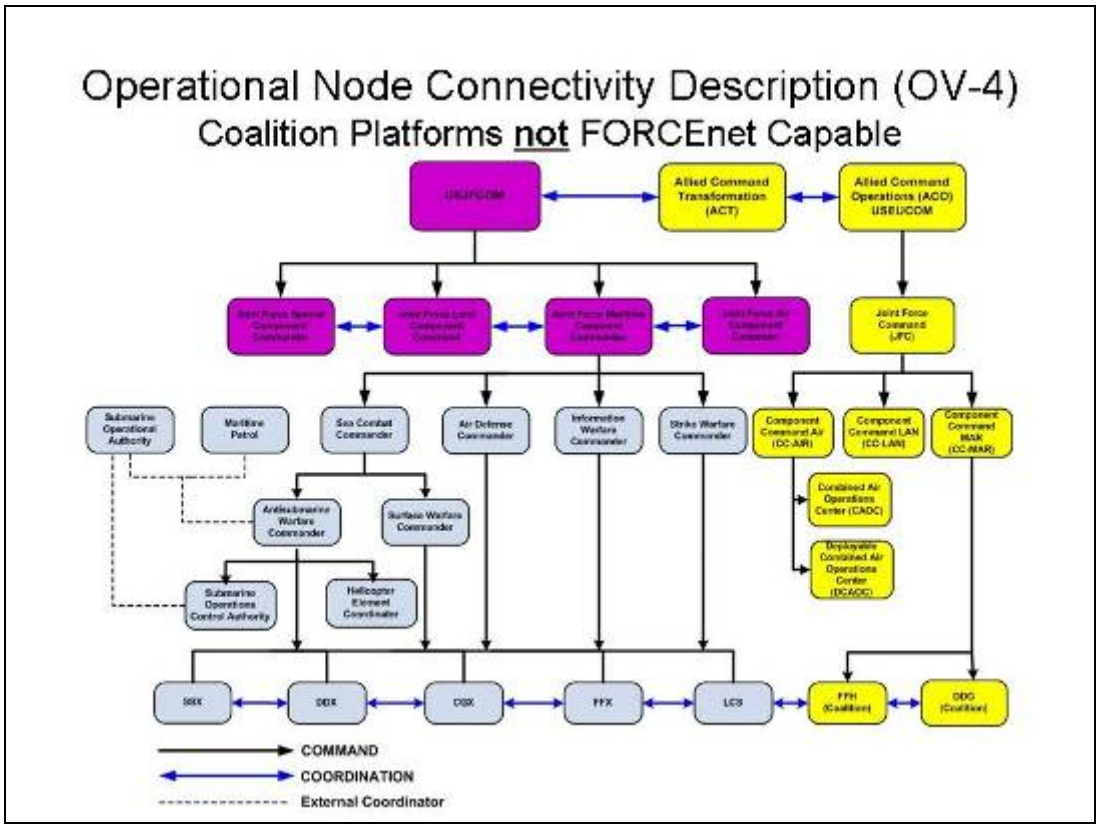


Figure A - 4 OV-4 Non-FORCEnet Capable

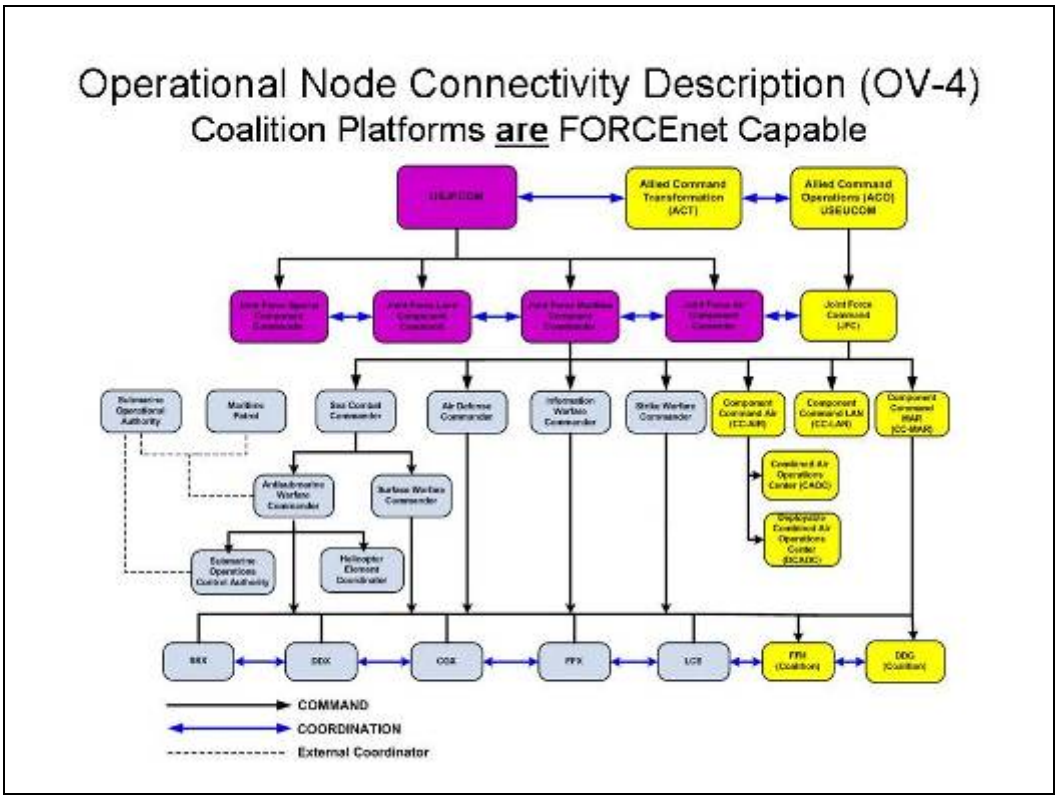


Figure A - 5 OV-4 FORCEnet Capable

A.2.4 Operational Activity Model (OV-5)

The DoDAF contains the following description of the OV-5:

> "The Operational Activity Model describes the operations that are normally conducted in the course of achieving a mission or business goal. It describes capabilities, operational activities (or tasks), input and output (I/O) flows between activities, and I/O flows to/from activities that are outside the scope of the architecture."[127]

The OV-5 may contain hierarchy charts that describe the various activities that occur in achieving a mission and may also contain process flows that describe the sequence and timing of these activities.

127 DoD Architectural Framework Version 1.0, Volume II: Product Descriptions (Department of Defense, [2004]), 4-31.

A.2.4.1 Coalition FORCEnet OV-5

The analysis and modeling for this project is limited to three of the eight vignettes described in the statement of work due to the limited amount of time available to work on the project. The three vignettes are Anti-Submarine Warfare (ASW) against the Kilo submarines, Anti-Surface Warfare (ASuW) against the hostile surface action group and Anti-Surface Missile Defense (ASMD) against the missiles fired by the enemy surface platforms.

Common to all of these vignettes is the establishment of the recognized maritime picture (RMP). Since establishing and maintaining the RMP covers detection and tracking of air, surface, and subsurface objects, the majority of the tasks for the three vignettes are covered by the task of establishing the recognized maritime picture. The ASMD vignette also requires the platforms to conduct surface missile defense. Thus, establishing the RMP and conducting ASMD are the two main tasks that are the primary focus of the OV-5 diagrams as shown in Table A - 2. These two main tasks are further decomposed in Figures A - 6 through A - 15. Descriptions of selected tasks in the hierarchy are provided in the table below.

Table A - 2 OV-5 Task Descriptions

Task Number	**Task Name**
Task Description	
1.1	**Establish Recognized Maritime Picture**
This task includes all of the activities that support generation of the plot and associated textual information that depicts the maritime activities in a given area. This includes air, surface, subsurface and some land objects such as surface-to-air missile sites.	
1.1.1	**Conduct Surveillance Operations**
This task employs the sensor assets of the strike group to detect air, surface and subsurface objects.	
1.1.2	**Distribute/Process Sensor Data**
Using the theater network shown in OV-2, sensor data is distributed and processed by each of the FORCEnet capable platforms. The Statement of Work (SOW) indicates that real-time targeting information gained from any U.S. or Coalition	

asset/source (when latter is technically capable) is available to all ESG/CSG vessels as required.

1.1.3	Interface with the Global Information Grid (GIG)

As shown in the OV-2 diagrams, two theater platforms are designated as the primary and secondary GIG interface units. The primary GIG interface unit is responsible for retrieving relevant information in response to the needs of theater platforms and is also responsible for providing theater data to interested nodes on the GIG. The secondary GIG interface unit monitors the activities of the primary unit and assumes the primary role in the event of a primary unit failure.

1.1.3.1	Obtain GIG Information

In this task, the primary GIG interface unit retrieves information for itself or on behalf of other theater platforms. The process of retrieving includes discovery and retrieving or pulling data from the provider. According to the DoD Net-Centric Data Strategy, "All data is advertised and available for users and applications when and where they need it. In this environment, users and applications, search for and 'pull' data as needed. Alternatively, users receive alerts when data to which they have subscribed to is updated or changed (i.e., publish-subscribe)."[128]

1.1.3.1.1	Process Intelligence Information

For this task, relevant intelligence data is retrieved from the Intelligence community of interest. Communities of interest are described by the DoD Net-Centric Data Strategy as "collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. Communities provide an organization and maintenance construct for data such that data goals are realized. Moving these responsibilities to a COI level reduces the collaboration effort as compared to managing every data element Department-wide."[129]

1.1.3.1.2	Process Battlespace Awareness Information

For this task, relevant information is retrieved from the Battlespace Awareness Community of Interest. Battlespace Awareness is one of the COIs in the Warfighter Domain of the GIG.

1.1.3.1.3	Process Meteorology/Oceanography Information

The primary GIG interface unit retrieves meteorology and oceanography information from the GIG. One organization that supplies this data is the Fleet Numerical Meteorology and Oceanography Center (FNMOC). This node is present in the OV-2 diagram. FNMOC's mission is to prepare the marine and joint battlespace to

[128]DoD Chief Information Officer, *DoD Net-Centric Data Strategy* (Department of Defense, 2003), 3.

[129] Ibid, 4.

enable successful combat operations from the sea, to exploit the meteorological and oceanographic opportunities and to mitigate the challenges for Naval operations, plans, and strategy at all levels of warfare.

1.1.3.1.4	Process Geospatial/Intelligence Information

The primary GIG interface unit retrieves geospatial intelligence information from the GIG. One organization that supplies this data is the National Geospatial Intelligence Agency. This node is present in the OV-2 diagram. According to the NGA website, "The National Geospatial-Intelligence Agency (NGA) provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Information collected and processed by NGA is tailored for customer-specific solutions. By giving customers ready access to geospatial intelligence, NGA provides support to civilian and military leaders and contributes to the state of readiness of U.S. military forces. NGA also contributes to humanitarian efforts such as tracking floods and fires, and in peacekeeping. NGA is a member of the U.S. Intelligence Community and a Department of Defense (DoD) Combat Support Agency."[130]

1.1.3.2	Publish Data to GIG

In this task, the primary GIG interface unit in the theater publishes metadata to support discovery by other GIG nodes. Should another node be interested in the data, the interested node (subscriber) requests the data. Once the request is validated, the data is pushed (published) to the subscriber. Platforms that are capable of serving as the GIG interface unit must support translation to the formats used on the GIG. For example, the Mission Area Initial Capabilities Document for the GIG indicates that "United States Imagery and Geo-spatial Information Service (USIGS) standards should be used for the processing and display of imagery and geospatial data across the GIG."[131] The GIG interface unit must be capable of translating between this and other formats.

1.1.4	Provide Data Fusion Services

A description of this task is provided in section 2.2.5.3.

1.1.4.1	Data Assessment

A description of this task is provided in section 2.2.5.3.

130 National Geospatial Intelligence Agency Fact Sheet.

http://www.nga.mil/portal/site/nga01/index.jsp?epi-content=GENERIC&itemID=31486591e1b3af00VgnVCMServer23727a95RCRD&beanID=1629630080&viewID=Article

131 Commander, U.S. Joint Forces Command, *Mission Area Initial Capabilities Document(MAICD) Global Information Grid (GIG),* (Joint Forces Command, 2002),13.

1.1.4.2	**Object Assessment**
A description of this task is provided in section 2.2.5.3.	
1.1.4.3	**Situation Assessment**
A description of this task is provided in section 2.2.5.3.	
1.1.4.4	**Impact Assessment**
A description of this task is provided in section 2.2.5.3.	
1.1.4.5	**Process Refinement**
A description of this task is provided in section 2.2.5.3.	
1.1.5	**Interface with Disadvantaged Platform**
When Coalition Forces are operating at FORCEnet Level 0, U.S. Forces exchange command and control data using tactical data links. The statement of work indicates that either Link-11 or Link-16 is used. Link-22 may also be one of the tactical data links used and was also included in this project. One of the U.S. platforms in the theater acts as a data forwarder between the tactical data links and the Fn theater network. The Super-Node may also publish metadata to the GIG to indicate tactical link data is available to GIG users and will provide the data to interested GIG participants.	
1.2	**Defend Against Surface Missile Threats**
One of the vignettes associated with this project is to conduct anti-surface missile defense. This task consists of conducting air surveillance and distributing the surveillance data, determining the preferred shooter and engaging the target.	
1.2.1	**Determine Preferred Shooter**
This task is described in section 2.2.2.2.	
1.2.1.1	**Evaluate Engagement Options**
In the process of determining the preferred shooter, a number of engagement options may be available. This task evaluates a number of these options to select the optimum engagement method.	
1.2.1.1.1	**Evaluate Precision Cue**
This task is described in section 2.2.2.2.	
1.2.1.1.2	**Evaluate Launch on Remote**
This task is described in section 2.2.2.2.	

1.2.1.1.3	**Evaluate Engage on Remote**
This task is described in section 2.2.2.2.	
1.2.1.1.4	**Evaluate Forward Pass**
This task is described in section 2.2.2.2.	
1.2.1.1.5	**Evaluate Remote Fire**
This task is described in section 2.2.2.2.	
1.2.2	**Engage Target**
In this task, the target is engaged by one or more platforms using the selected engagement method.	

Process flows talked about in the OV-4 table, that show the sequence of events for selected activities, are shown in Figures A - 16 through A - 22.

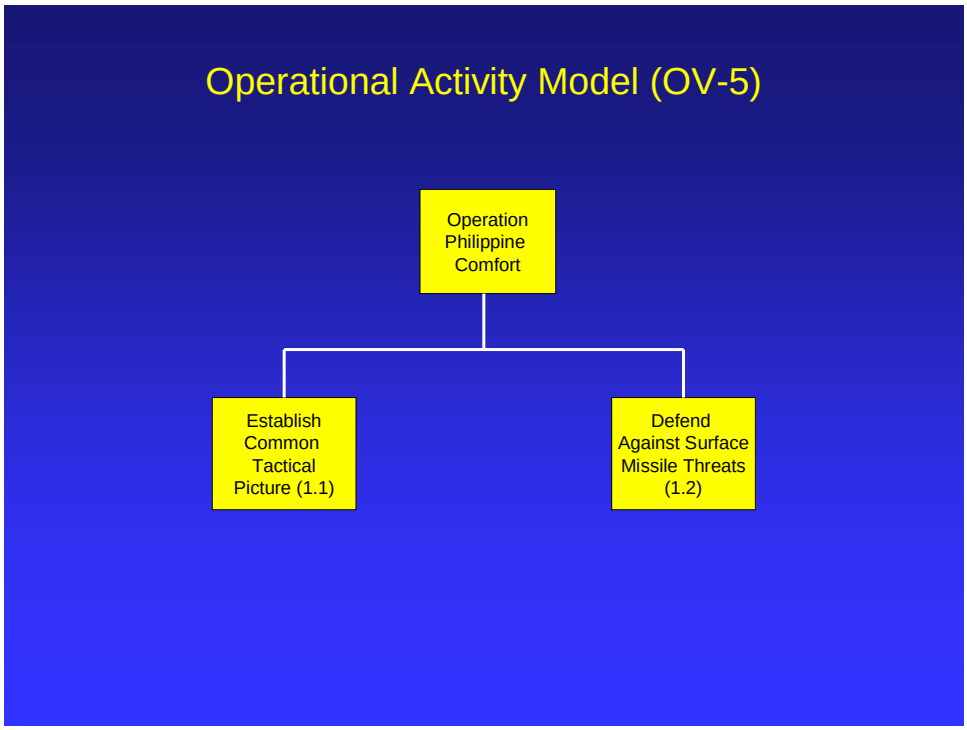


Figure A - 6 OV-5

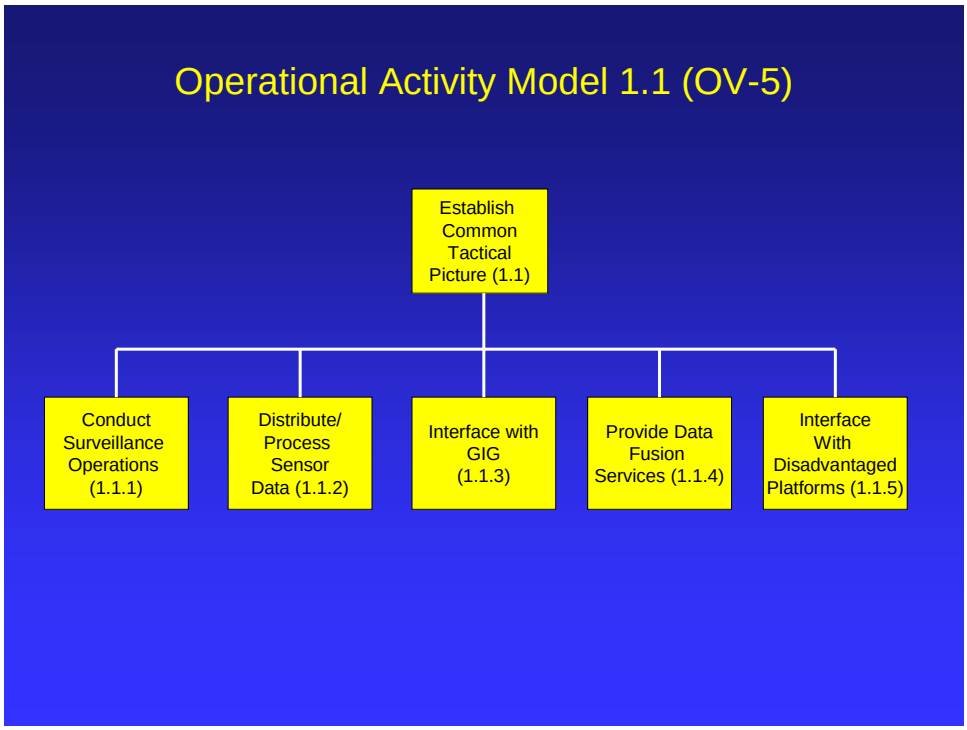


Figure A - 7 OV-5 Level 1.1

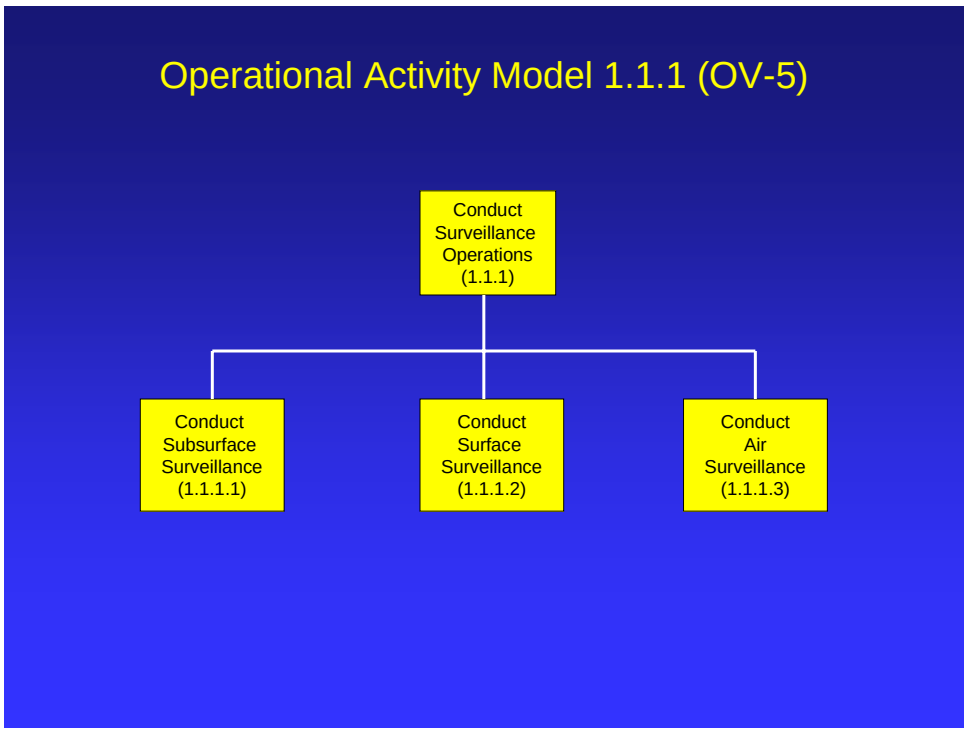


Figure A - 8 OV-5 Level 1.1.1

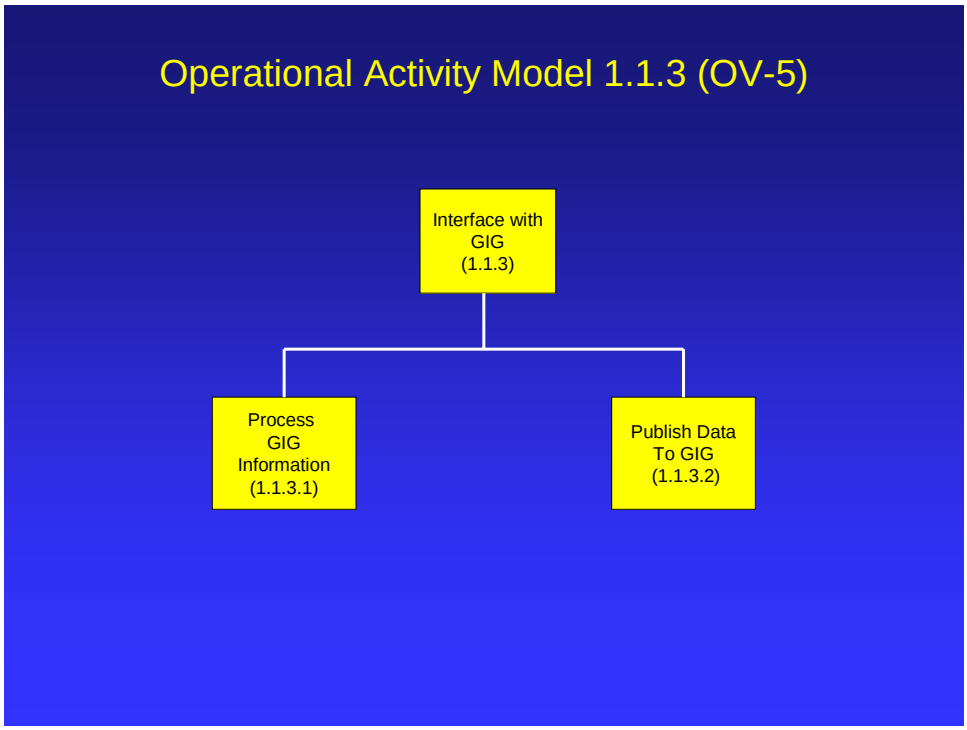


Figure A - 9 OV-5 Level 1.1.3

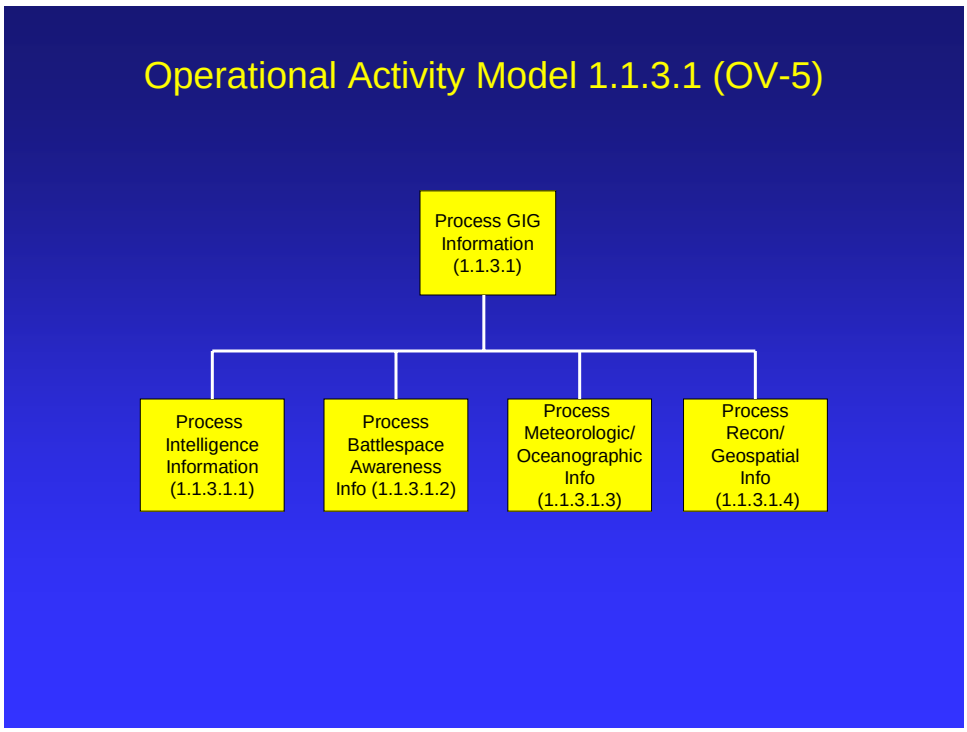


Figure A - 10 OV-5 Level 1.1.3.1

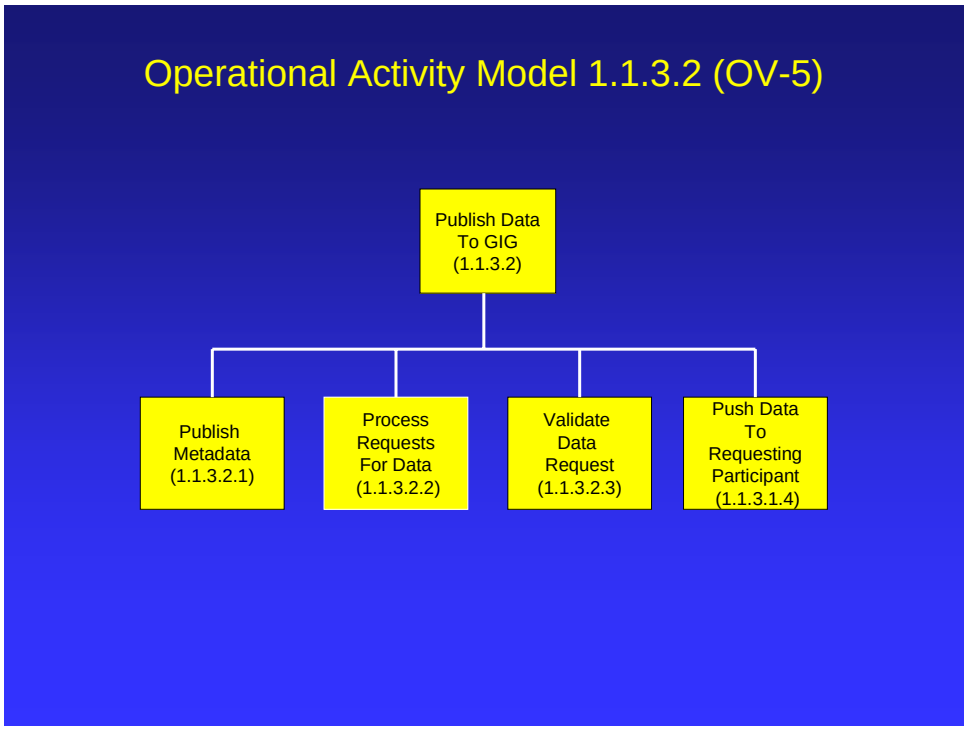


Figure A - 11 OV-5 Level 1.1.3.2

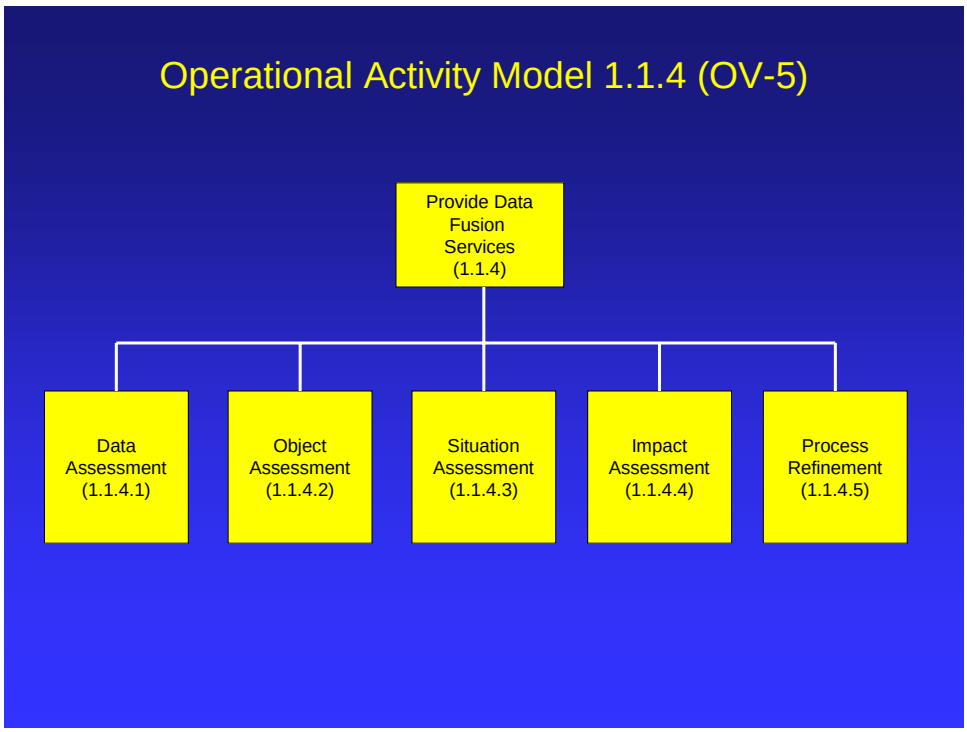


Figure A - 12 OV-5 Level 1.1.4

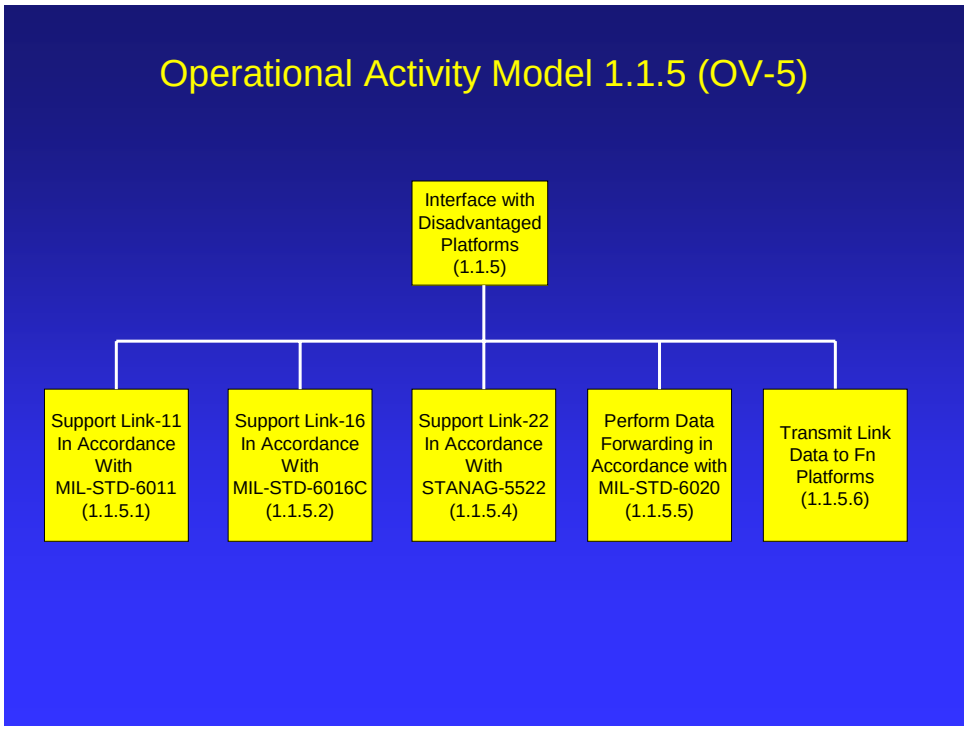


Figure A - 13 OV-5 Level 1.1.5

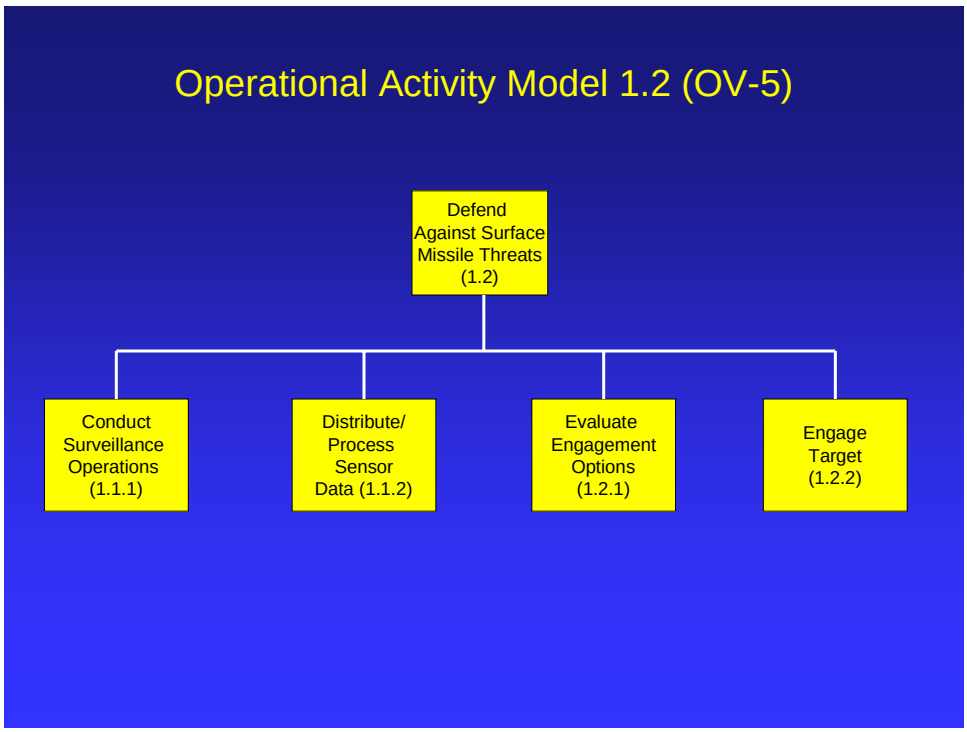


Figure A - 14 OV-5 Level 1.2

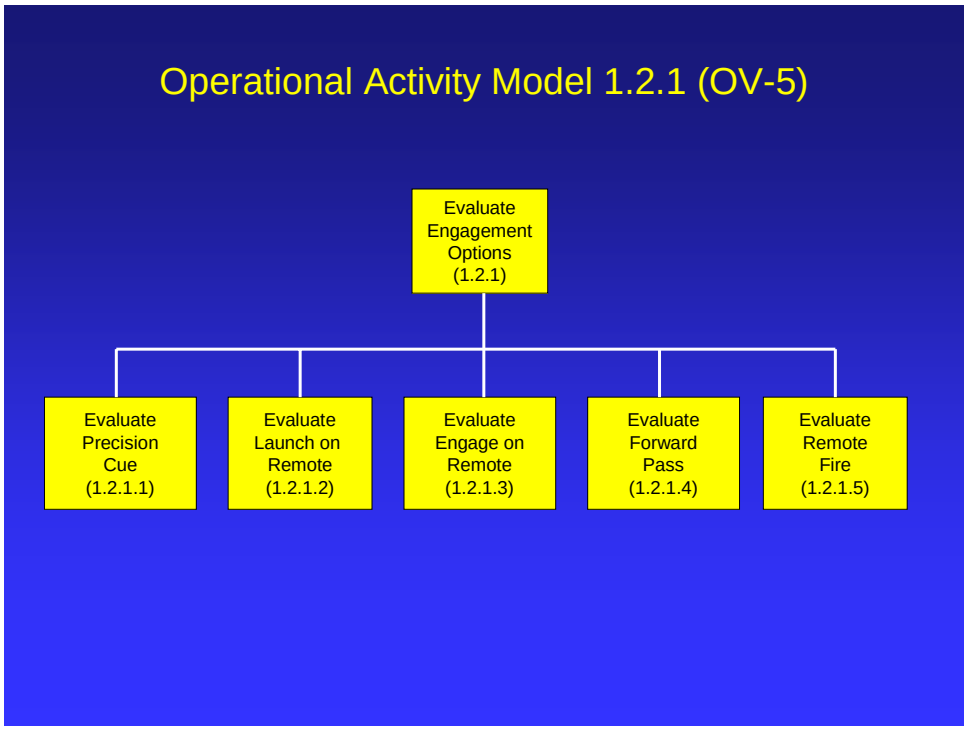


Figure A - 15 OV-5 Level 1.2.1

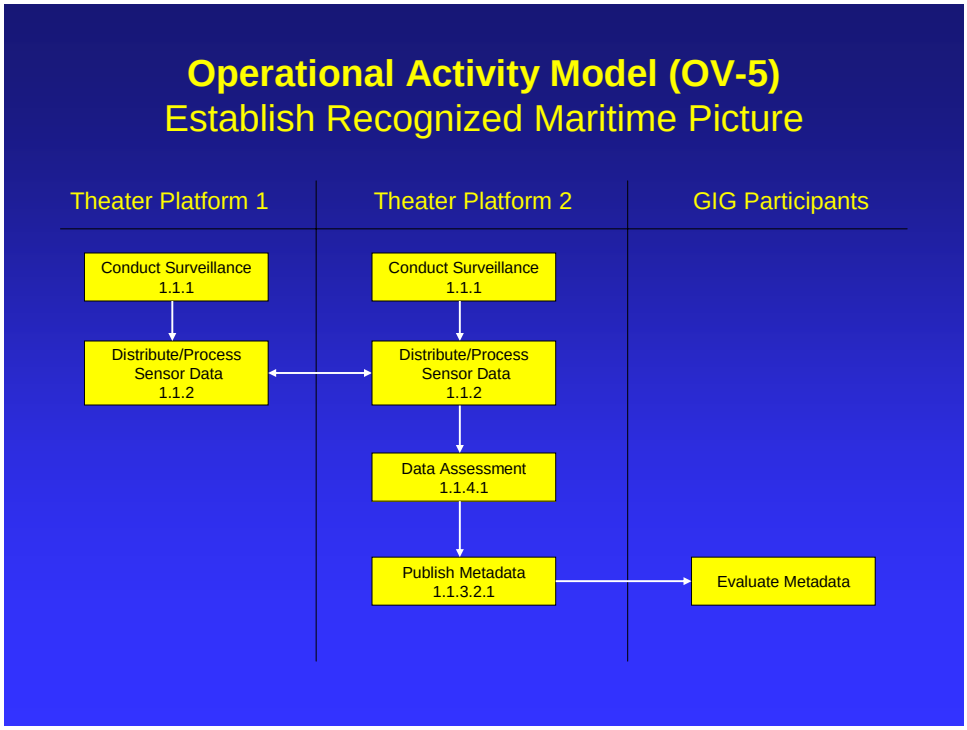


Figure A - 16 OV-5 Date Flow RMP1

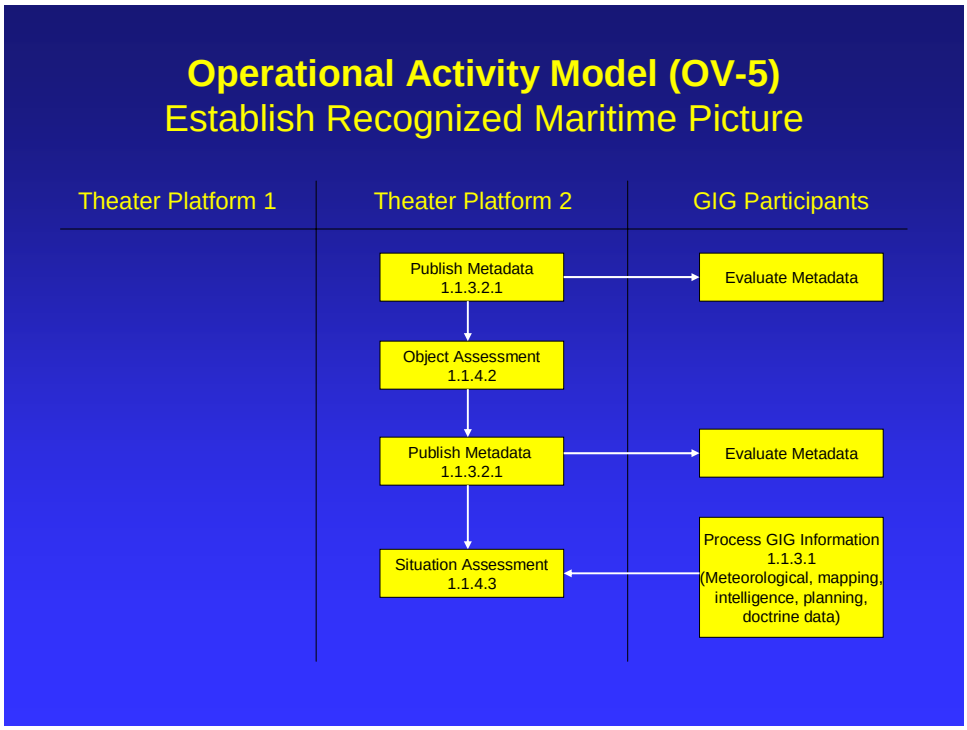


Figure A - 17 OV-5 Data Flow RMP2

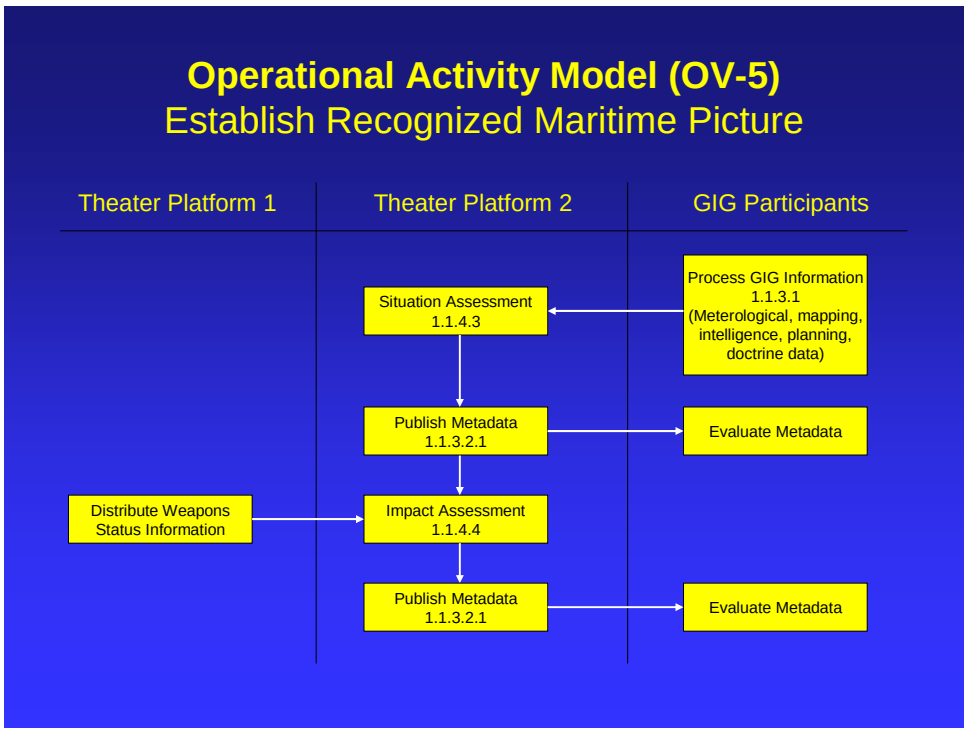


Figure A - 18 OV-5 Data Flow RMP3

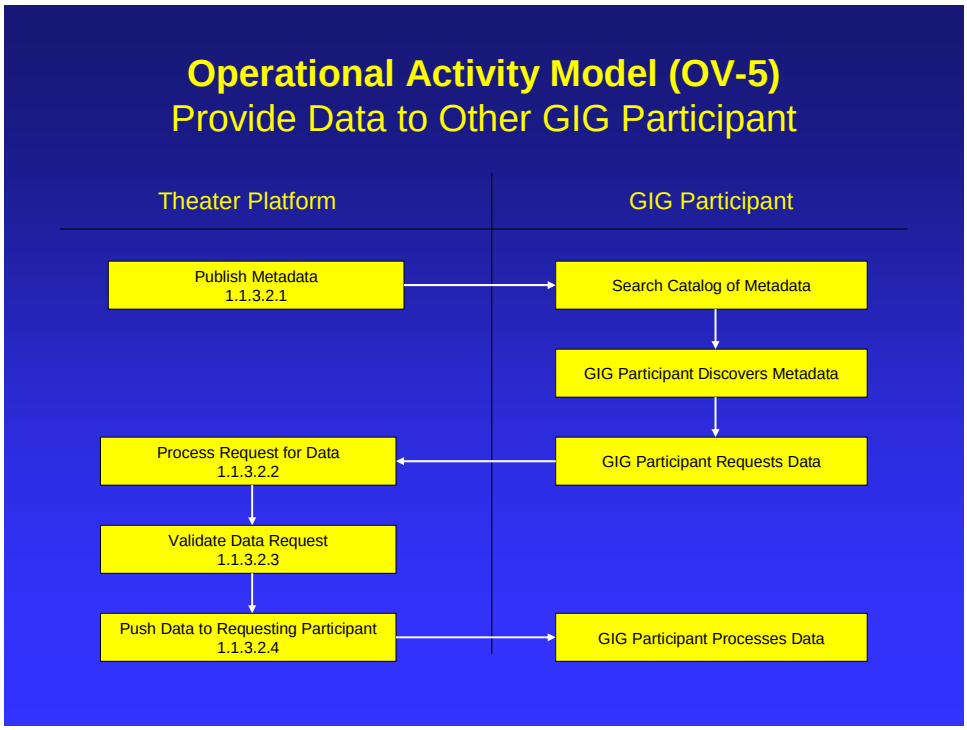


Figure A - 19 OV-5 Data Flow GIG1

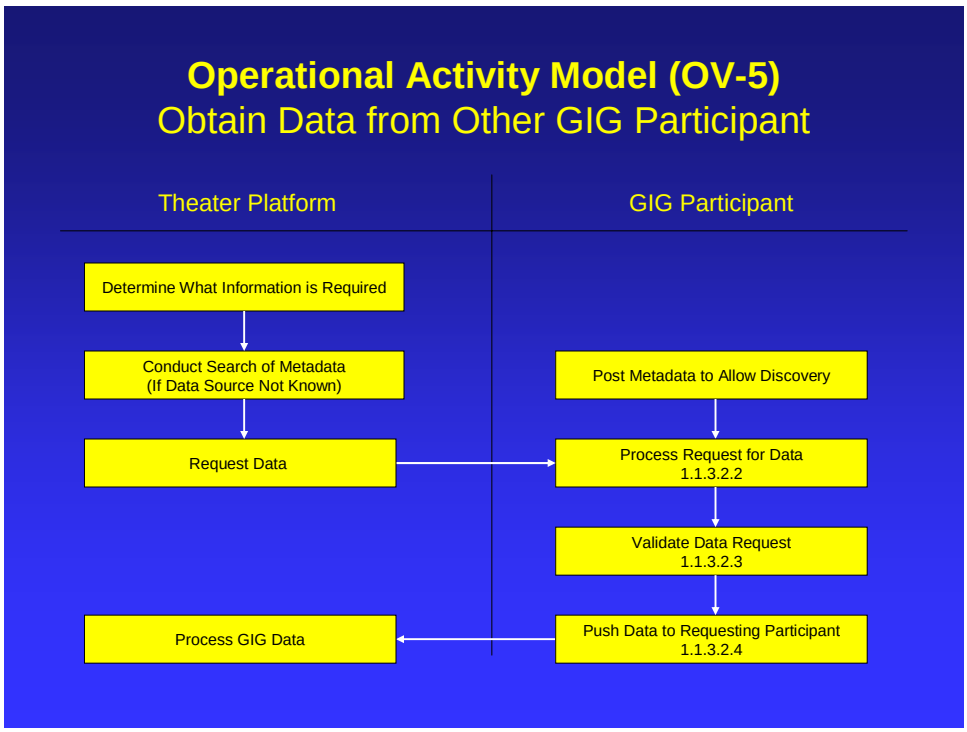


Figure A - 20 OV-5 Data Flow GIG2

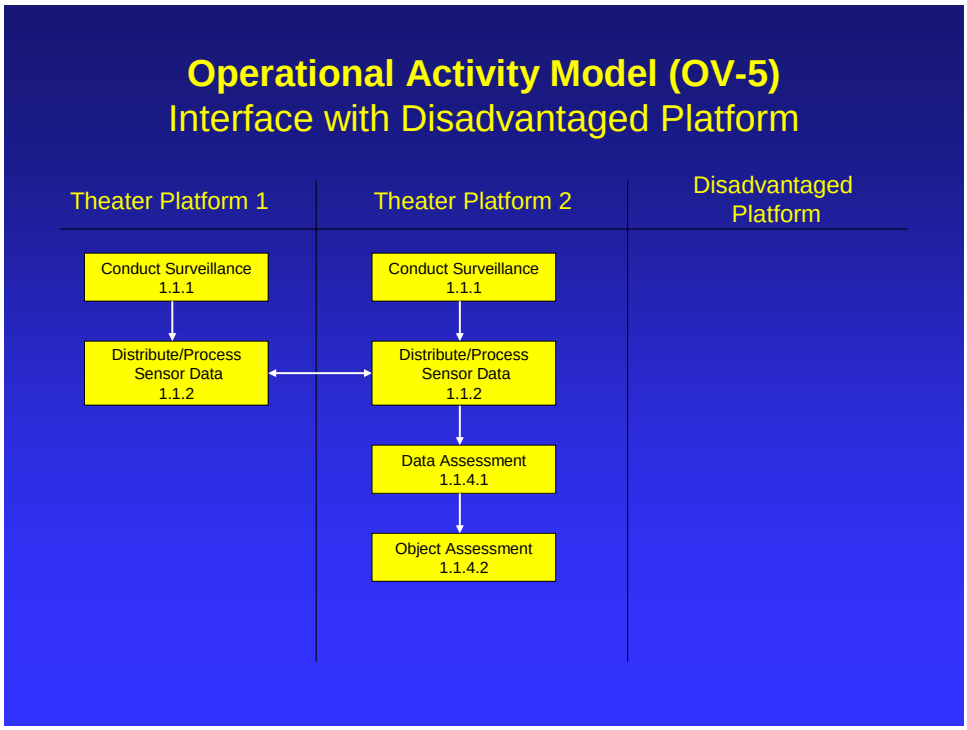


Figure A - 21 OV-5 Data Flow DP1

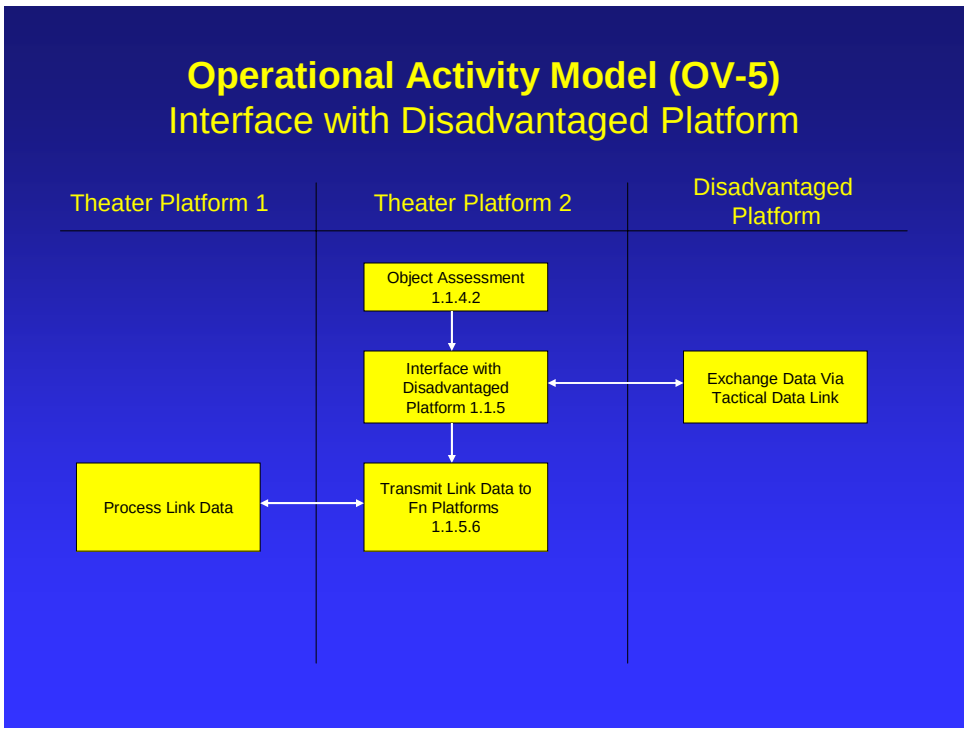


Figure A - 22 OV-5 Data Flow DP2

A.2.4 Operational Event/Trace Description (OV-6c)

As defined in the DoDAF, the Operational Event-Trace Description (OV-6c) "provides a time-ordered examination of the information exchanges between participating nodes as a result of a particular scenario."[132] The purpose of this architectural artifact is in its value as an iterative step, providing the next level of detail from the initial operational concepts (OV-1, OV-2, etc…). It helps to define the node interactions and operational threads (the set of operational activities) with sequencing and timing attributes of the activities.

A.2.4.1 Coalition FORCEnet OV-6c

For this project, the OV-6c diagrams, shown in Figures A - 23 and A - 24 were developed for the Anti-Submarine Warfare (ASW) against Kilo submarines and the Anti-Surface Warfare (ASuW) against the Red Surface Action Group (SAG) vignettes.

In this Event-Trace, information is exchanged in an effort to establish a shared Common Operational Picture (COP/RMP) across the battlegroup (BG), and any subscribing user on the GIG.

The make-up of the BG is consistent with the Order of Battle provided in the project Statement of Work (V0.g). The Super-Node is a designation given to the senior capital ship of the BG. Auxiliary Super-Node is the designation of any additional capital ships that are capable of assuming Super-Node responsibilities. Every action undertaken by the Super-Node is simultaneously conducted by all Auxiliary Super-Nodes. The Super-Node and Auxiliary Super-Nodes continuously synchronize all databases. All other nodes are networked within the BG (fully FORCEnet capable) and are independently addressable. An exception is the UAV, which is considered a disadvantaged user, and it reports to the DDX, which in turn is responsible for UAV reporting and dissemination of data. In essence, the UAV is an extension of the DDX.

This event-trace is initiated when the BG Super-Node issues a request for an intelligence report from the Office of Naval Intelligence (ONI) regarding the Red SAG force in the Sulu Archipelago. Simultaneously, the Super-Node informs all Auxiliary

[132] DoD Architectural Framework Version 1.0, Volume II: Product Descriptions (Department of Defense, [2004]), 4-55.

Super-Nodes of the initial request. Upon receipt of the ONI intelligence report, the Super-Node disseminates the report to all members of the BG.

Following the initial intelligence distribution within the BG, the Super-Node requests and receives sensor status from all platforms within the BG. Processing the sensor status information, the Super-Node then assigns sectors and tasks the various sensors. Data Fusion and synchronization is performed aboard each Super-Node with every report.

After the request for sensor status and reporting, the Super-Node prioritizes the threats and then initiates another request of the BG, this time requesting weapons status (inventory and availability). Upon receipt of this information, the Super-Node assigns weapons to each threat. Since the Red SAG is not currently considered a threat to the BG, a weapons hold order is issued to all weapons. This concludes the description of this event-trace.

Figure A - 24 is similar to Figure A - 23 below, but the Operational Event-Trace depicts the information exchange for the Anti-Subsurface Warfare against the Red Kilo threat.

Apart from the mission, the primary difference of the ASW event-trace from Figure A - 24 below is the increase in disadvantaged platforms. In this case, the DDX is responsible for reporting and dissemination of information of the MH-60, and the helicopter's sonobuoys.

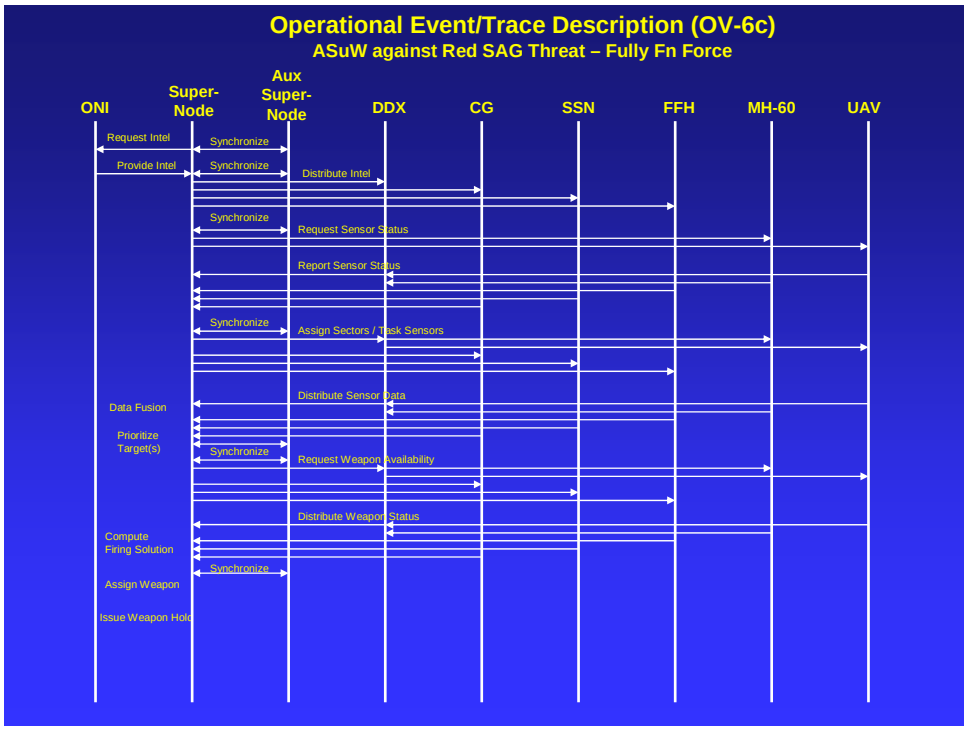


Figure A - 23 OV-6c ASuW

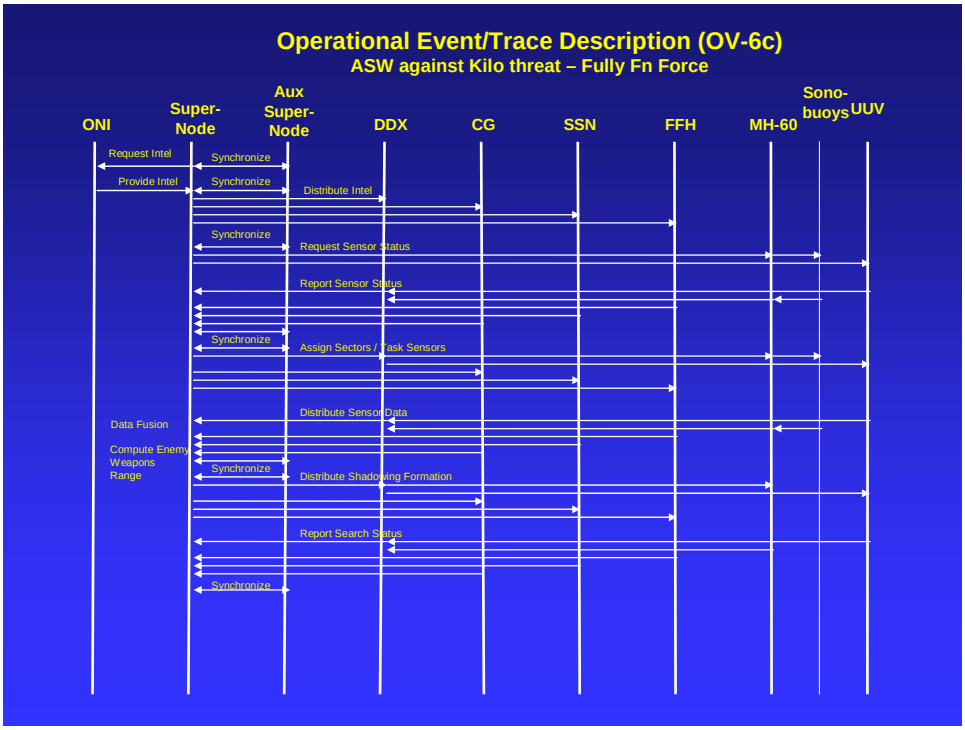


Figure A - 24 OV-6c ASW

A.3 System Views

A.3.1 System Interface Description (SV-1)

The DoDAF indicates that the SV-1 "depicts systems nodes and the systems resident at these nodes to support organizations/human roles represented by operational nodes of the Operational Node Connectivity Description (OV-2). SV-1 also identifies the interfaces between systems and systems nodes."[133]

A.3.1.1 Coalition FORCEnet SV-1

This view allows an architect or developer to allocate functionality into the FORCEnet system solution and to establish interoperability interface points for the foundational elements of FORCEnet. This System View (SV) will be used as a technical reference model that will define constraints on system implementations. The FORCEnet family of common services will ensure compatible systems and business rules (doctrine) for the Warfighter; they will ensure technical interoperability and configuration management for the engineers; and they will ensure that Joint solutions can be shared across service, agency and civilian boundaries to reduce acquisition investment requirements. The System Interface Description identifies the interfaces between system nodes, between systems, and between the components of a system. In order to provide access to for all Navy users, anywhere in the world, infrastructure nodes must be implemented in numerous locations. For Pier connections in the Continental United States (CONUS), infrastructure nodes will exist at two (or more) Network Operation Centers (NOCs). This format was used to provide an understanding of the most critical service from a warfighter perspective, leading and managing the operation.

The FORCEnet goal is to enable all platforms in theater to connect to the GIG network through different means, either via the fiber connection over land or the radio communication over the water. For connections between commands on land, the WAN network can be established using fiber connection such as OC3/12 to provide the bandwidth ranging from 1.544 Mbps and up to 45 Mbps. This would enable real time database synchronization and information sharing with minimal time delay is necessary to request and receive the sensor, C2, and situational awareness data.

[133] DoD Architectural Framework Version 1.0, Volume II: Product Descriptions (Department of Defense, [2004]), 5-1.

For primary platforms at sea such as CV(N), LHD, and LPD, the Beyond Line-of-Site (BLOS) radio communication systems are suggested to be the primary communication method for reaching to the shore site (i.e. teleport), then through the landline, connect to the GIG network. For other U.S. platforms at sea, the HF, UHF, VHF and SATCOM can provide inter and intra shipboard communication that can utilize the primary platform to act as the gateway to the GIG network. At the same time, with certain SATCOM capabilities for BLOS connection to the teleport at shore, through the landline, to the GIG network. The HF, UHF, and VHF Line-of-Sight (LOS) radio system can provide the audio and data support with the data range from 4.8 Kbps to 64 Kbps.

The theater network provides the means to exchange information between Fn capable platforms in the theater. As such, when Coalition platforms are not Fn capable, as shown in Figure A - 25, the Coalition platforms are only connected to the network via CENTRIXS network provided by U.S. platforms. Instead, the Coalition exchanged information via legacy Tactical Data Link (TDL). The primary communication systems between Coalition platforms is suggested to be HF, UHF and VHF system with some SATCOM capabilities onboard certain ships.

The network structure onboard U.S. platforms may change once the Coalition platforms are Fn capable. The CENTRIXS network that currently resides in the Integrated Shipboard Network System (ISNS) network may also change due to enabling Fn capability with the Coalition partners.

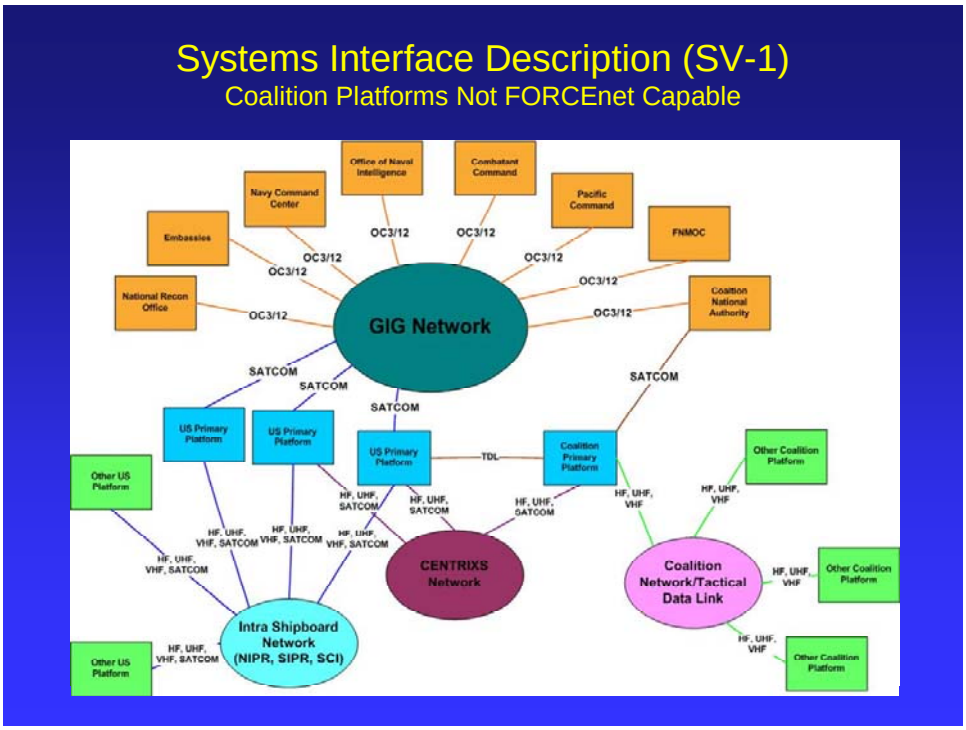


Figure A - 25 SV-1 Non-FORCEnet Capable

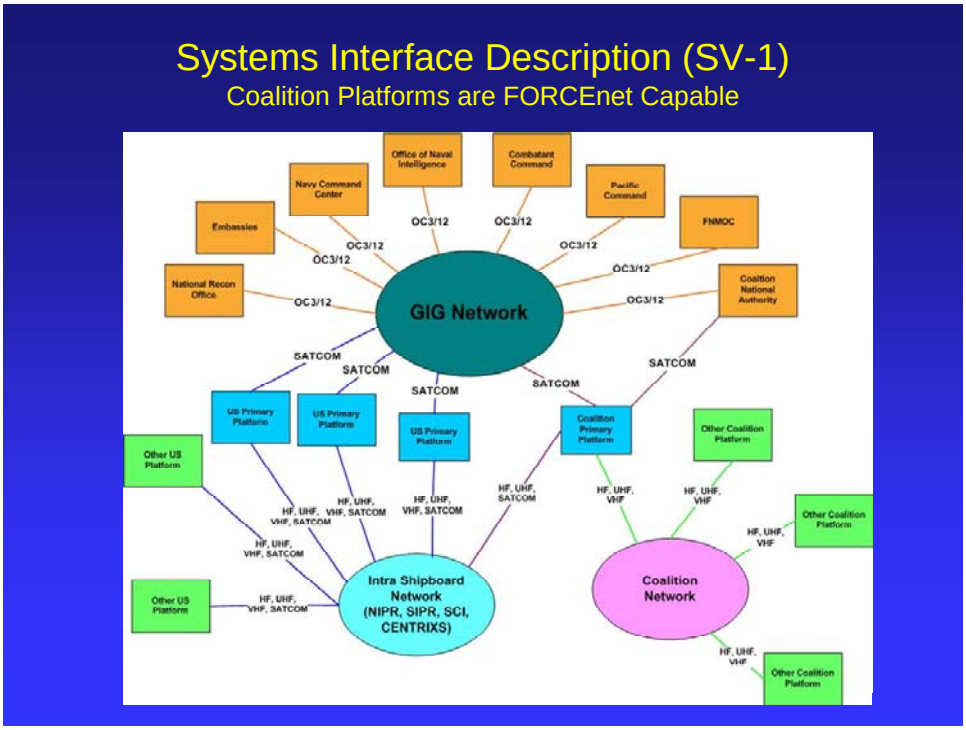


Figure A - 26 SV-1 FORCEnet Capable

A.4 All Views

A.4.1 Overview and Summary Information (AV-1)

The AV-1 is similar to an executive summary. This view is a high-level textual description of the architecture in a common format.

A.4.1.1 Coalition FORCEnet AV-1

Table A - 3 AV-1

Architecture Product Identification	
Architecture Product Name	Coalition FORCEnet – San Diego Capstone Project
Architect	Naval Postgraduate School MSSE Students – San Diego
Organization Developing the Architecture	Naval Postgraduate School
Assumptions and Constraints	Assumptions • Architecture will address ASW, ASUW, ASMD • All communications networks are assumed to have sufficient bandwidth • Communications networks are assumed to have minimal latency • Doctrine, policy, tactics, techniques and procedures will be in place to support the suggested architecture. • Cross domain security technology exists to support releasability and information assurance • Sensor and weapon systems identified in this study are limited to existing and systems currently in development Constraints

	• Project to be completed by 5 September 2006.
Approval Authority	Naval Postgraduate School
Date Completed	5 September 2006
Scope	
Views and Products Developed	AV-1, AV-2, OV-1, OV-2, OV-4, OV-5, OV-6c, SV-1
Time Frames Addressed	2015
Organizations Involved	Naval Postgraduate School, SPAWAR Systems Command, SPAWAR System Center, Navy Center for Tactical Systems Interoperability, Fleet ASW Training Center, Defense Information Systems Agency
Purpose and Viewpoint	
Purpose	To demonstrate knowledge of systems engineering while providing guidance to Coalition Nations (AUSCANNZUK) by identifying opportunities to participate in FORCEnet, and to quantify the operational benefits of participation.
Analysis	• Determine what benefit, if any, is provided by Coalition participation in FORCEnet. • Identify the requirements for Coalition FORCEnet participation. • Determine the architecture of the US/Coalition force. • Evaluate the architecture against the Philippine Comfort Scenario.
Questions	• What are the expected benefits for Coalition Nations that participate in FORCEnet? • Will FORCEnet provide significant increases in capability over existing systems?

	• What is required to participate in FORCEnet?
Viewpoint from which Architecture is Developed	The architecture is being developed from an academic viewpoint as part of the MSSE Program at the Naval Postgraduate School.
Context	
Mission	Conduct joint operations in support of Operation Philippine Comfort
Rules, Criteria, and Conventions Followed	• Architectural Views consistent with DoD Architecture Framework Version 1.0 • Final paper written in the Capabilities Development Document format
Tools and File Formats Used	
Tools	Extend Modeling Software Version 6.0, Microsoft Office XP, ArcGIS 9.X
Findings	
Analysis Results	The results of the simulation analysis are provided in Sections 11.4 and 11.5.
Recommendations	Recommendations for further study are provided in section 11.6.

A.4.2 Integrated Dictionary (AV-2)

The AV-2 is the glossary of the architecture. This view provides textual definitions of terms used in describing the architecture.

A.4.2.1 Coalition FORCEnet AV-2

ASMD – Anti-Surface Missile Defense

ASUW – Anti-Surface Warfare

ASW – Anti-Submarine Warfare

Auxiliary Super-Node – The Auxiliary Super-Node is the designation of any capital ship that is capable of assuming Super-Node responsibilities. The Auxiliary

Super-Node automatically assumes the role of the primary in the event of a Super-Node failure.

COI – Community of Interest. This is an element of the GIG that is listed in OV-5

COP – Common Operational Picture

CTP – Common Tactical Picture

Coalition National Authority – These organizations provide authorization for weapons release on Coalition platforms in FORCEnet levels 3 and below.

Combatant Command – This node is present in OV-2. This node provides command, control and intelligence information and is responsible for conducting mission operations.

Embassies – This node is present in OV-2. Embassies provide National-level intelligence and other information.

FCP – Fire control picture

FNMOC – Fleet Numerical Meteorology and Oceanography Center. This node is present in OV-2. FNMOC's mission is to prepare the marine and joint battlespace to enable successful combat operations from the sea, to exploit the meteorological and oceanographic opportunities and to mitigate the challenges for Naval operations, plans, and strategy at all levels of warfare.

GIG – Global Information Grid. This is one of the nodes in OV-2. Nodes interface with the GIG using a GIG Enterprises Services Interface.

National Geospatial-Intelligence Agency (NGA) – The National Geospatial-Intelligence Agency (NGA) provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Geospatial intelligence is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Information collected and processed by NGA is tailored for customer-specific solutions. By giving customers ready access to geospatial intelligence, NGA provides support to civilian and military leaders and contributes to the state of readiness of U.S. military forces. NGA also contributes to humanitarian efforts such as tracking floods and fires,

and in peacekeeping. NGA is a member of the U.S. Intelligence Community and a Department of Defense (DoD) Combat Support Agency.[134] This node is present in OV-2.

Office of Naval Intelligence – This office supports joint operational commanders by providing comprehensive national level intelligence.

Other Platform – This is one of the nodes used on OV-2. These are smaller platforms such as the Maritime Patrol Aircraft and TAGOS ships. In general, these platforms communicate with Primary Platforms and do not directly connect to the theater network.

Pacific Command – The U.S. Pacific Command, in concert with other U.S. government agencies and regional military partners, promotes security and peaceful development in the Asia-Pacific region by deterring aggression, advancing regional security cooperation, responding to crises, and fighting to win. This node is present in OV-2

Primary Platform – This is one of the nodes used in OV-2. These are larger more capable platforms such as CG, DDG, LCS, and SSN. In general, primary platforms are capable of direct connections with both the theater network and the GIG.

Super-Node – The Super-Node is a designation given to the senior capital ship of the battlegroup and is also assigned the role of exchanging information between the theater network and nodes on the GIG. In this role, the Super-Node is responsible for both publishing information to the GIG and subscribing to information from nodes of interest on the GIG.

---

[134] National Geospatial Intelligence Agency Fact Sheet.

http://www.nga.mil/portal/site/nga01/index.jsp?epi-content=GENERIC&itemID=31486591e1b3af00VgnVCMServer23727a95RCRD&beanID=1629630080&viewID=Article

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B: GIS METHODS

B.1 Geospatial Information System

The output of the simulation represented a common operational picture (COP). To do this using an ArcGIS system required a map of the Philippines, the islands and seas to the west of the main island. The information that will be provided to produce the COP is X Y (lat/long) of enemy and Coalition forces. Several layers of information were used for specific lat/long positions. The lat/long positions were the outputs from a simulation program (EXTEND) into excel, then saved as DBF files and added to the GIS program.

B.1.1 Map Creation

The following are the specific steps that were accomplished for the development of the map for this project.

1. Start a new map in Arcmap.
2. Select Add Data, select World Folder from MSGIS, and select Countries.
3. In the contents right click Layers > select Properties > select Coordinate System > Predefined > Projected coordinate system > Continental > Asia > Asia south equidistant conic > select Ok
4. Back in the map – zoom into the Sulu Sea west of Philippine Islands. To find the Philippines > right click on Countries > Properties > Label > check the box to "label features in this layer."
5. Bookmark the Sulu Sea and the Philippines using view > Bookmark > Create.
6. Next add several layers from Final Project > data folder in MSGIS: Select Add Data > select spratleys.shp.
7. Select Add Data > select country_claims.shp
8. Select Add Data > select natcapitols.shp.
9. To add x y data to the map: The x y data (lat/long) is the information output (to Excel) from the simulation software Extend – it is detection of target information, which will be displayed in the GIS to provide the common operational picture. Next, change the Excel output to dbf files.

10. Open the Excel file FN_parameters.xls > click on the blue_ships tab > save as dbf. Do the same process to convert to dbf for the following tabs: Coalition ships, Blue HVA, Blue A/C, Blue sub, Red subs, Red ships > all “save as” dbf to the data folder.
11. Now add x y data to the map. Go to Tools> Add X Y Data > select blue ships > x field = lat, y field = long. This should now appear as a layer in the map.
12. Do the same process to add x y data for Coalition ships, Blue HVA, Blue A/C, Blue sub, Red subs, Red ships. These should be new layers in the map.
13. It is useful to group blue and red forces separate. Click on blue ships, then while holding down the Ctrl key select Coalition ships, Blue HVA, Blue A/C, Blue sub. Now right click blue ships and choose Group. Change the group layer name to Blue Forces. Repeat this process to create a group (Red forces) for the Red subs and Red ships.
14. To show a "detection zone" around our Coalition forces click the Tools menu and click Customize.
15. Click the Commands tab > click Tools > click on Buffer Wizard and drag it to any toolbar. Click Close.
16. Next, select Buffer Wizard for each blue layer with a distance of 50 kilometers.
17. Select properties for each buffer layer and set transparency to 60%.
18. Use the Select Tool. Click on Philippines > right click Countries > export data to products folder > add as a layer. This will add the Philippines as its own layer. Do the same for Indonesia and Malaysia.
19. Use text boxes to identify the volcanic eruption, rebel positions, and enemy SAG position.
20. Next, identify the Exclusive Economic Zone 200 NM around Philippines, Malaysia, and Indonesia. Select Buffer Wizard > Philippines > 200 nautical miles. Repeat this for the three countries.

At this point there should be a map that contains enemy ship locations, EEZ 200NM buffer, country claims, and a sensor grid example of the Coalition forces. It should look similar to Figure B – 1 below.

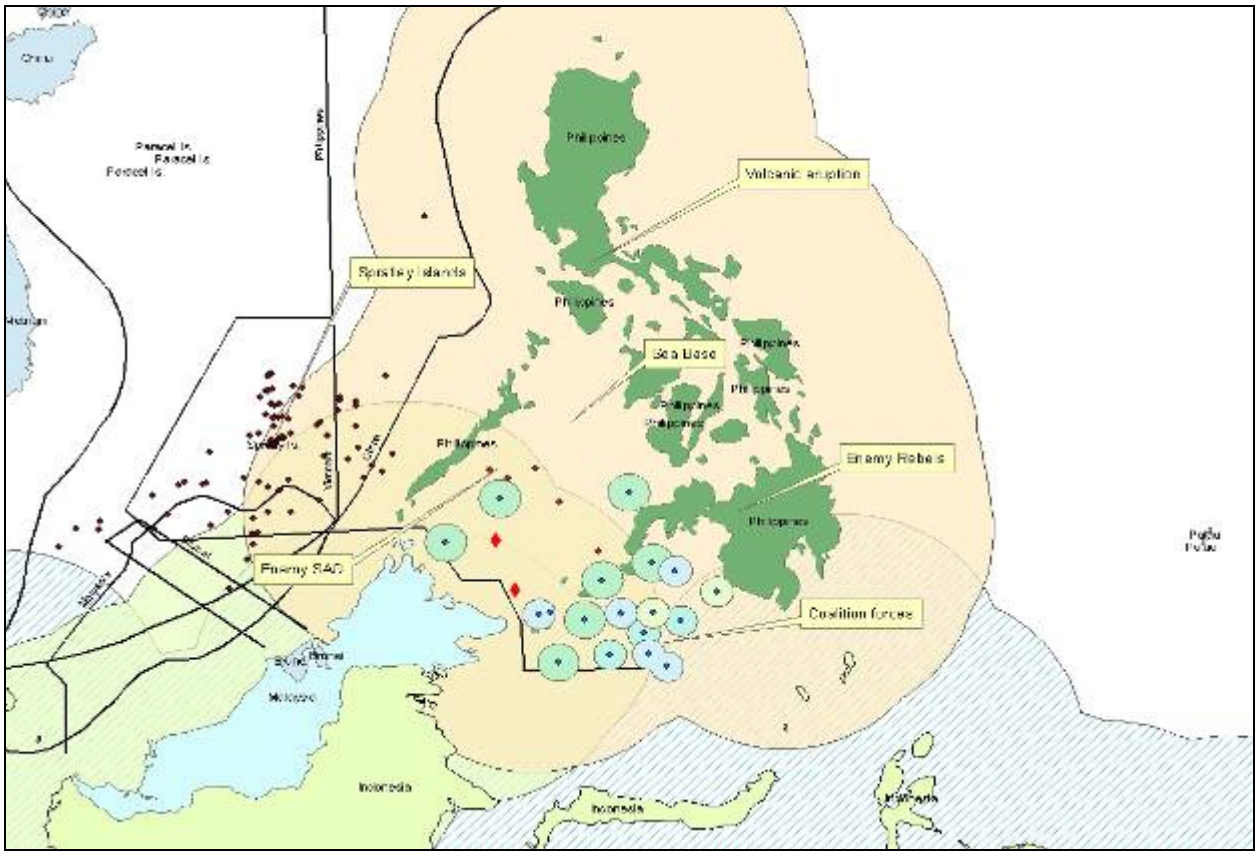


Figure B - 1 Scenario map

B.1.2 Map Projection

Select the Asia south equidistant conic which is a projected coordinate system with a datum of Spheroid_WGS_1984. Selection of this projection was based on the area of the world that the project is focused. Equidistant projections maintain constant scale along all great circles (shortest distance between any two points) from one or two points. It is not possible to preserve distances (scale) correctly throughout a map projection. Additionally, no flat map can be both equidistant and equal-area.

B.1.2.1 Advantages

This is an excellent projection to use because of the mapping of a region within a few degrees of latitude with entire area on one side of the equator. This projection is commonly used on small countries or areas, oriented on east-west in the mid-latitudes. Equidistant Scale: True only along the chosen standard parallels and along all meridians. Standard parallels are those free of distortion.

B.1.2.2 Disadvantages

Equidistant Distortion is free of distortion along either of the two standard parallels, but increases further away. Distortion is a compromise between equal-area and conformal. This projection is a compromise between the Albers Equal-Area and Lambert Conformal Conic, and as such is neither conformal, equal-area, nor perspective.

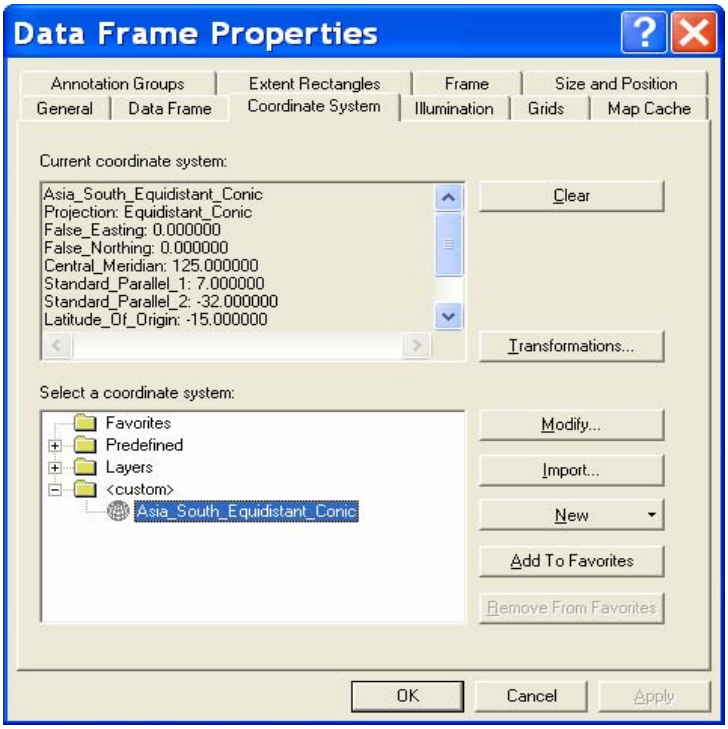


Figure B - 2 ArcGIS Data Frame

B.1.3 Data

Figure B - 3 shows the naming and data management of the data used in ArcGIS for this project. Figure B - 4 shows the Table of Contents inside the ArcGIS program and shows the multiple layers used for the development of the project map.

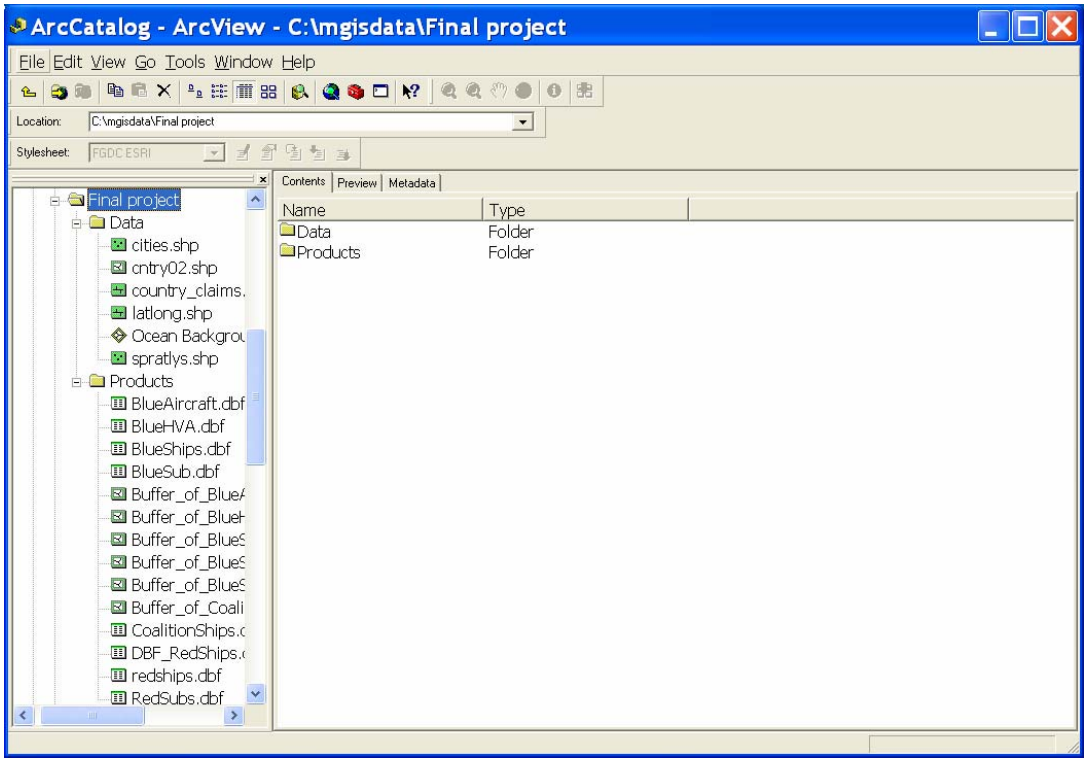


Figure B - 3 ArcCatalog

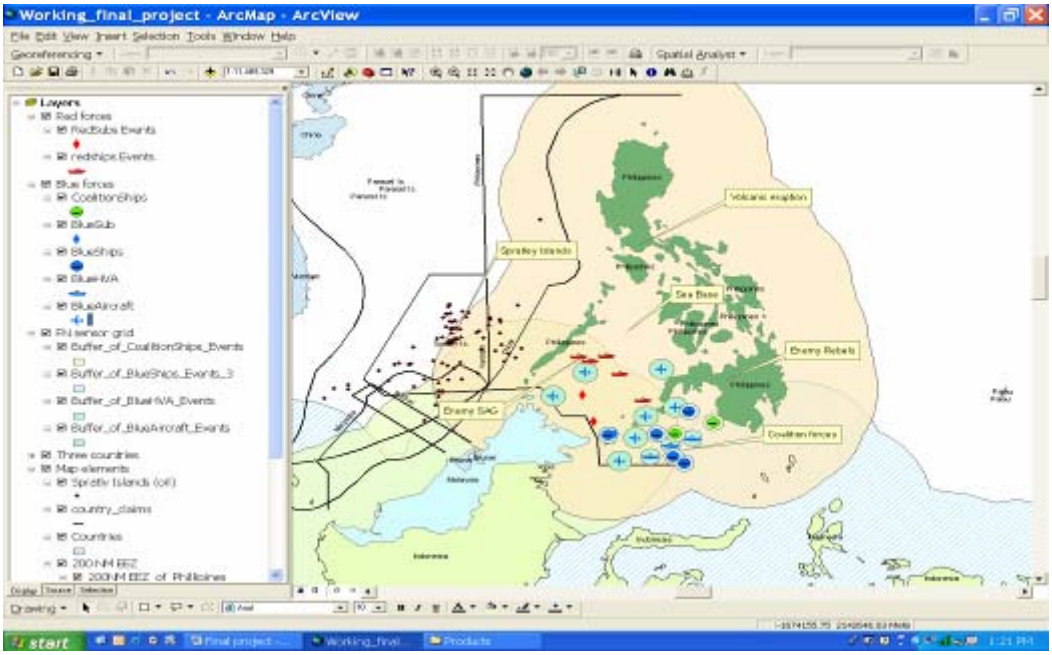


Figure B - 4 ArcMap Layers

Data was obtained as an output from the Extend FORCEnet simulation program, two shape files (Spratly and country claims), and from the mgisdata folder.

B.1.3.1 Layers

The following is a description of each layer in the ArcGIS table of contents, starting from the top down:

1. The first layer is a group called “Red forces” and it contains two layers called RedSubs and Redships. The data was obtained from Excel. It was the lat/long information output from the EXTEND simulation program. The excel file was saved as a dbf file and added as an x y layer showing enemy and Coalition locations. During each simulation run the x y data is updated in the Excel file resulting in new enemy locations appearing in the GIS program. A diamond shape was used as a symbol for a submarine and a ship symbol for the Redships. An example of Lat/Long output from EXTEND to excel is shown in Table B - 1. To add the above information use tools > add x y data. Follow this process for each enemy and Coalition platforms (ships, subs, aircraft).

Table B - 1 Redship Lat/Long Data

No	Unit	LAT	LONG	Red ships
1	10	121.330	9.600	P_corvette
2	20	120.200	8.200	P_corvette
3	30	119.000	9.000	VS FFG
4	40	120.000	9.000	VS FFG
5	50	119.400	8.800	VS FFG

2. With the EXTEND simulation providing the lat/long information to Excel, the process in step one was repeated for the second group layer “Blue Forces” which consists of Coalition ships, BlueSub, BlueHVA, and BlueAircraft. For each of these layers different shapes were used. Blue forces (US ship) were colored blue, Red forces color red, and Coalition ships were colored green.
3. The next group was called “FN sensor grid.” This layer was created to show the area of coverage that a “netted” group of ships would provide. The buffer wizard was used to place a coverage area around each Blue ship, Coalition ship, Blue HVA, and BlueAircraft. The buffer was set to 30% transparent for each so that the blue forces could be seen.
4. The fourth group is named “Three countries.” Select the countries using the select tool, and then export the data and added the three countries back as layers.

These layers were used for the 200NM EEZ around Malaysia, Indonesia, and Philippines.

5. The fifth group is called “Map elements.” This is really the foundation of the GIS map. Add the following shape files: Spratly Islands, country claims, countries (world map), and also a sub group called “200NM EEZ”. With this group, a 200NM EEZ zone was set around Malaysia, Indonesia, and the Philippines. Additionally, each buffer was set for a 40% transparency.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: EXTEND

C.1 Extend Explained

Blocks are the basic model-building components in the Extend modeling and simulation software. Each block represents some part of the process being modeled, such as a chemical reaction or a machine's activity. A block's icon shows its meaning in the model and double-clicking the icon reveals a dialog for entering the block's data. Blocks contain unique procedural information and are grouped into libraries according to function. (*Extend User Manual*).

Creating an Extend model is done by dragging blocks from a library onto a worksheet, connecting them, and then entering the appropriate data in the dialog.

Simulation involves building a dynamic model of a process or system, then performing what-if analysis to see how changes would affect the actual process. By mimicking its operation one can understand the system better and explore alternative strategies. This model mimicked the operation of a resource manager and integrated fire control.

C.2 Extend iterative modeling approach

A discrete event model of FORCEnet was developed in ten steps. In discrete event models, discrete entities change state as events occur in the simulation. Targets arriving, ships being "cued" and engagement of targets are examples of discrete events. The state of the model changes only when those events occur; the mere passing of time has no direct effect. A factory that assembles parts is a good example of a discrete event system. The individual entities (parts) are assembled based on events (receipt or anticipation of orders). The time between events in a discrete event model is seldom uniform.

C.3 Extend simulation development

The following is a step by step process on developing the simulation model, for this project, using the Extend program.

Step 1: The first Extend simulation model contained three models: Anti-Submarine Warfare (ASW), Anti-Surface Warfare (ASUW), and Anti-Surface Missile Defense (ASMD). Platforms were placed in parallel as a sensor grid, but incoming targets could not clearly be identified. The probability of detection was estimated using the random search model. There was cueing but not "precision cueing." This was a rough model that ran successfully after debugging (Figure C - 1).

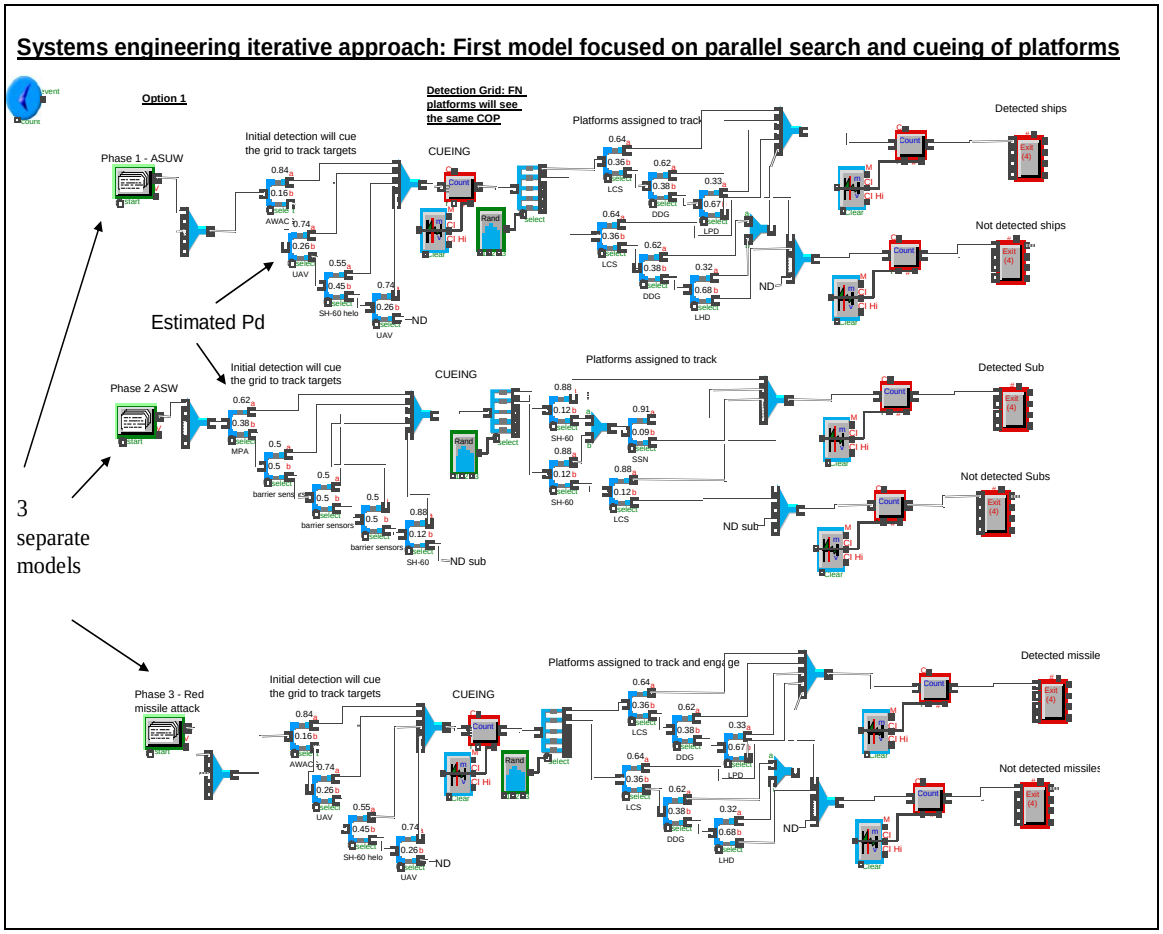


Figure C - 1 Three Vignette Models

Step 2: In the second development of the model, the sensor resource manager was improved, but it was difficult to clearly identifying targets. Additionally, there were still three separate models: ASW, ASuW and ASMD (Figure C - 2).

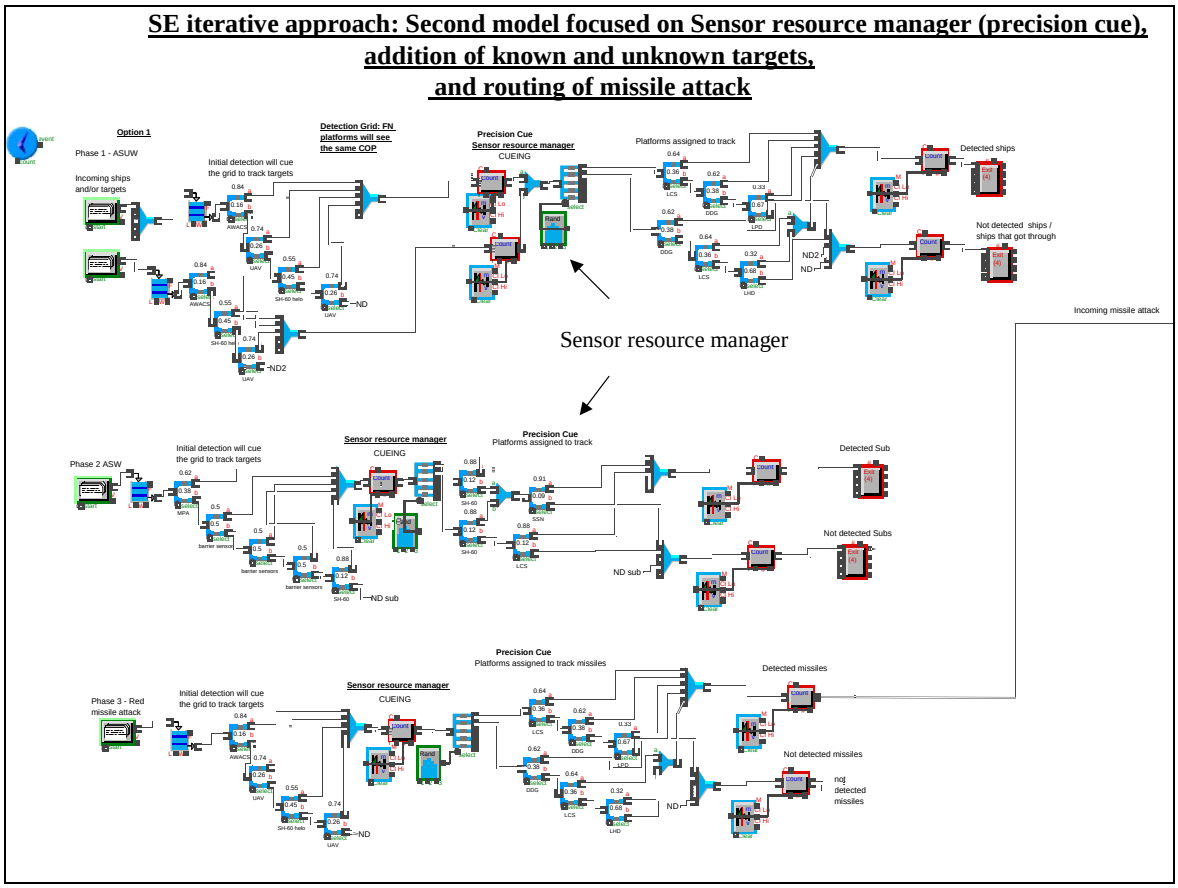


Figure C - 2 Initial Resource Manager

Step 3: The Integrated Fire Control capability (Figure C - 3) was then developed in the engagement grid. The modeling of "launch on remote," "engage on remote" and "remote fire" was simulated through a binomial distribution (for probability of kill). If a target is routed to the middle engagement platform then this represents the "preferred shooter."

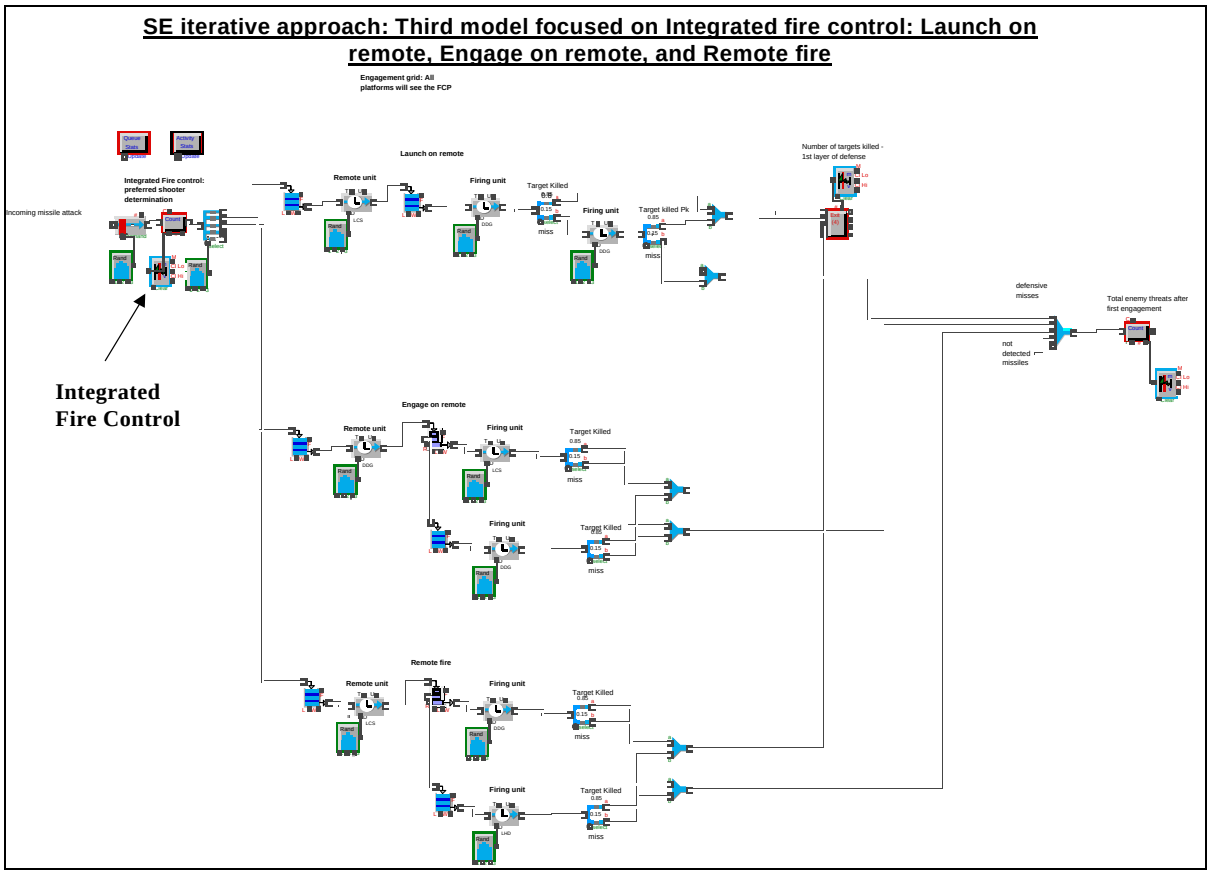


Figure C - 3 Integrated Fire Control

Step 4: By having three models and an engagement grid the model grows quickly (Figure C - 4). The only way to simplify this model was to integrate the three models into one resulting in a single integrated model. Below in Figure C - 5 the integration was accomplished but there was still a problem of integrating the ASW model. By using intelligence attribute information, the resource manager was improved allowing the simulation to clearly identify the incoming threats. The ASW mission was integrated into model 6 shown in Figure C - 6.

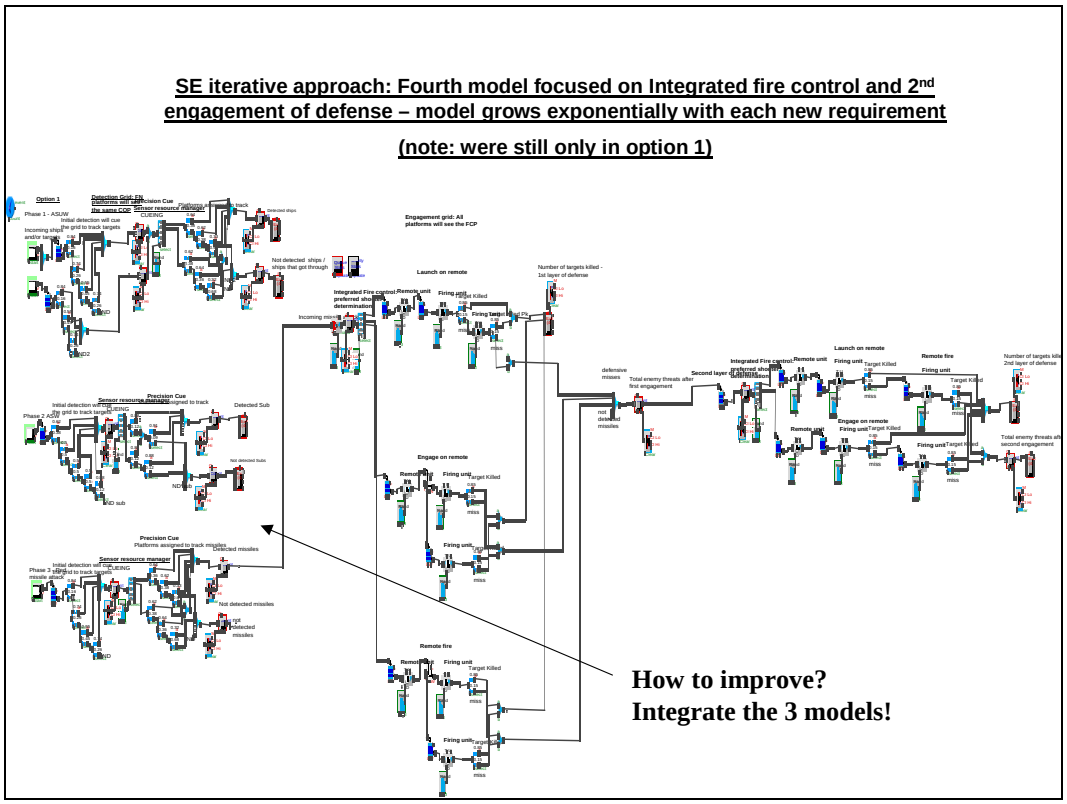


Figure C - 4 Large Model Prior to Integration

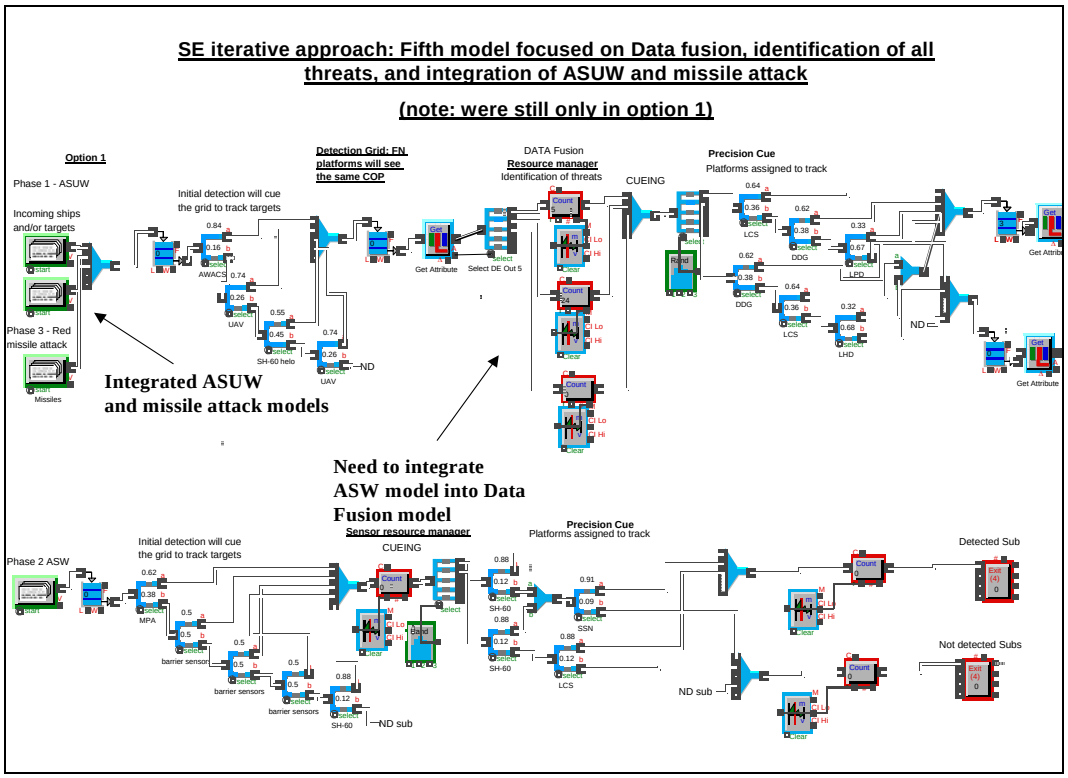


Figure C - 5 Integrated Model

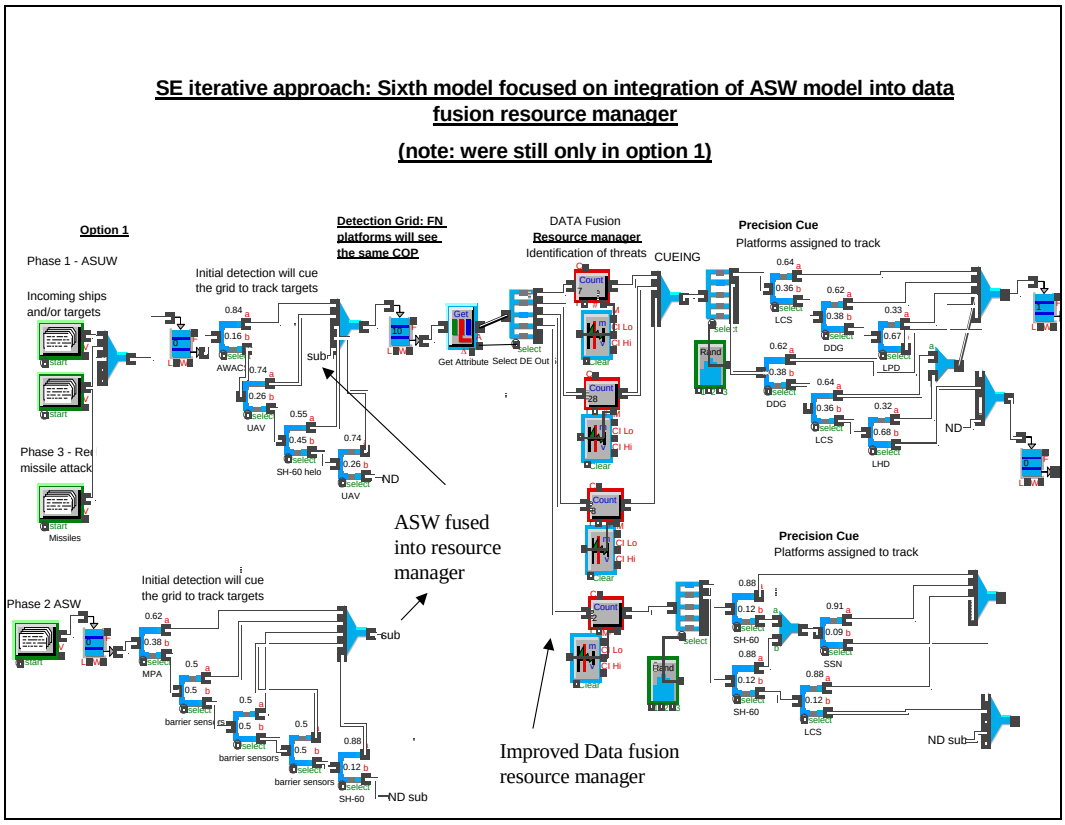


Figure C - 6 Improved Data Fusion Model

Step 6: In the eighth model, Option 2 was completed and is shown in Figure C - 7. This option in the given scenario added two Coalition ships that had no FN capability – they were modeled as platform-centric.

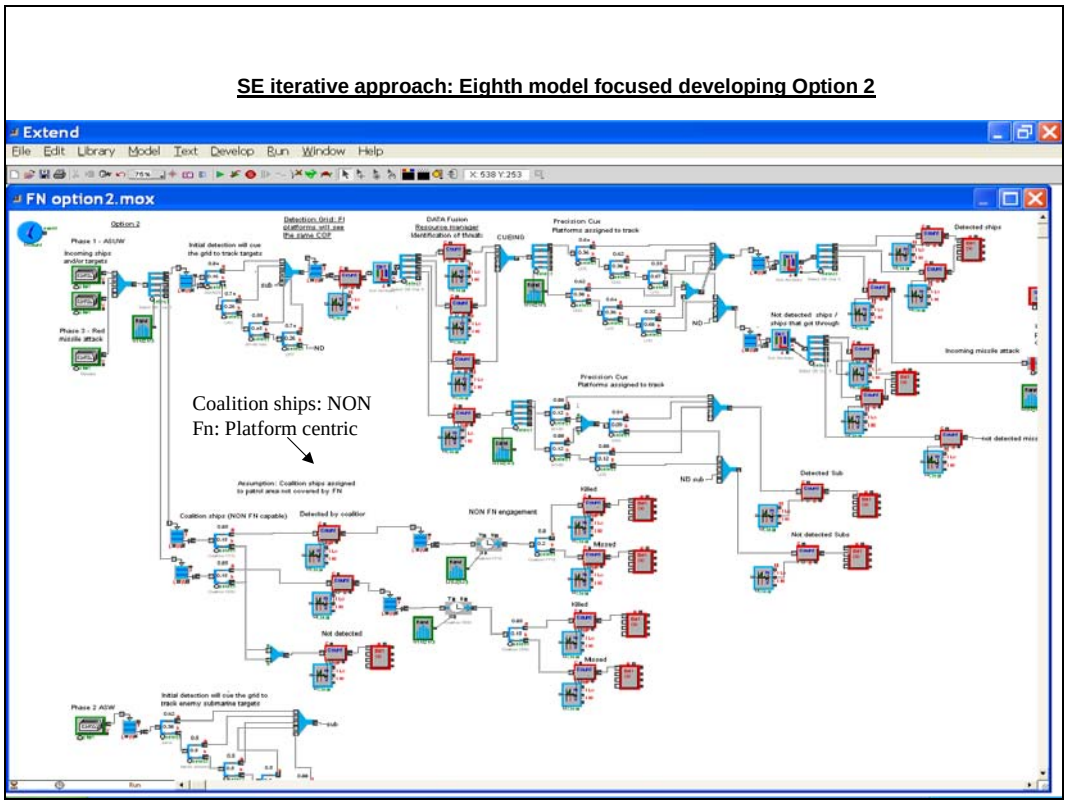


Figure C - 7 Non-FORCEnet Capable Ships Added

The final step of the Extend model development: The Coalition ships were integrated into model. This allowed the completion of the Extend model for options 3 and 4. Essentially they were the same models but with slightly different FORCEnet capability. The output of the Extend model provides the information output to GIS for display of the common operational picture. The 10th model improved the data fusion at the resource manager (Figure C - 8).

SE Iterative approach: 9th Model added Coalition ships to FN grid and finished developing models for options 3 and 4

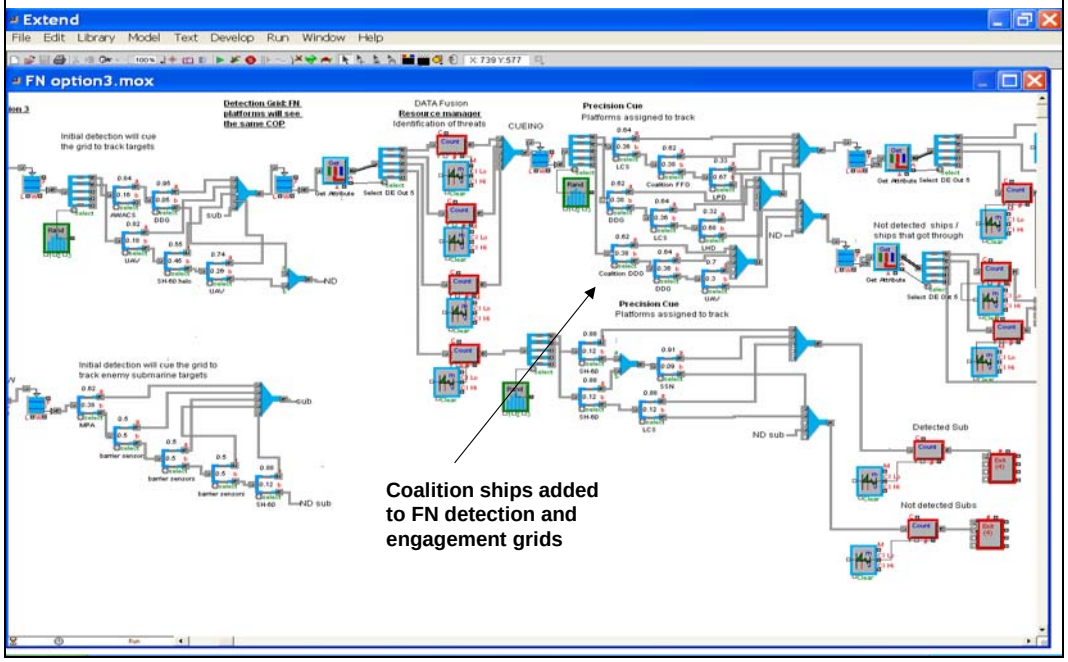


Figure C - 8 Full FORCEnet Capable Coalition Ships

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, D.S., J. J. Garstka, and F. P. Stein. *Network-Centric Warfare*. Dover, 2nd edition, February 2000.

Alberts, David S. *Network-Centric Warfare, Developing and Leveraging Information Superiority*. Washington, Department of Defense, 1999.

Aronoff, Stan. *Geographic Information Systems: A Management Perspective.* WDL Publications, 2003.

Beamer, R. A., P. Henning, and R. Cullen. *The USNORTHCOM Integrated Architecture: Developing and managing a capabilities-based architecture as a program to enhance the Homeland Defense and Military Assistance to Civil Authorities*. MITRE Technical Report on behalf of U.S. Northern Command, 2004.

Bedworth, Mark D. *Source Diversity and Feature-Level Fusion.* Hays Publishing, 1999.

Blanchard, Benjamin and Wolter Fabrycky. *System Engineering and Analysis.* Prentice Hall, 1998.

Booher, H. R. *Human Systems Integration Handbook*. John Wiley & Sons Inc, 2003.

Caruana, Rich. *Brief: Data Mining.* Cornell University, 2003.

Caruana, Rich. *OLAM and Data Mining: Concept and Techniques.* Cornell University, 2004.

Caruana, Rich. *Introduction to Data Mining.* Cornell University, 2003.

Cebrowski, Arthur K, and John J Garstka. *Network-Centric Warfare: Its Origins and Future.* U.S. Naval Institute Proceedings, January 1998.

Cipriano, Joseph R. *A Fundamental Shift in the Business of Warfighting.* Sea Power, March 1999.

CJCS Instruction 6212.01B. Interoperability and Supportability of Information Technology and National Security Systems' http://www.army.mil/howwewillfight/references/9%20CJCSI.pdf

Clark, V. and P.M. Balisle. *Human Systems Integration*. Symposium 2003

Core Architecture Data Model (CADM), Baseline Version 1.1. DoD, 2003. http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/116.pdf

Defense Acquisition Guidebook, http://akss.dau.mil/dag/

DoD Architecture Framework (DoDAF). http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf

DoD Information Technology Standards Registry (DISR). https://disronline.disa.mil/DISR/index.jsp

DoD Instruction 8110.1 Subject: Multinational Information Sharing Transformation Change Package of 6 February 2004.

DoD Net-Centric Data Strategy. http://www.defenselink.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf

DoD Joint Technical Architecture http://www.acq.osd.mil/osjtf/pdf/jta-vol-I.pdf

DOD Instruction *5000.2-R. Operation of the Defense Acquisition* System, http://exploration.nasa.gov/documents/TTT_052005/DoD50002R.pdf

Exploring architectures and algorithms for the 5 jdl/dfs levels of fusion required for advanced fighter aircraft for the 21st century. May 1999. www.megasociety.org/noesis/167/9.htm

Extend v6, Users manual. Imaging That, 2002

FORCEnet: A Functional Concept for the 21st Century, February 2005.

FORCEnet Technical Reference Guide For Program Mangers. Office of the FORCEnet Chief Engineer SPAWAR 05, Version 0.9.4.2, 4, April 2005.

Garstka, John J. *Network-Centric Warfare Offers Warfighting Advantage.* Signal, May 2003

GIG Capstone Requirements Document. http://handle.dtic.mil/100.2/ADA408877

GIG Enterprise Service (ES) Initial Capability Document. DoD, Version 1.10, June 10, 2003.

GIG Net-Centric Implementation Document Overview. DoD, released on 11 April 2005.

GIG Overarching Policy, DoD, Sept. 19, 2002.

Global Information Grid (GIG) Capstone Requirement Document. JROCM 134-01, Aug 30, 2001.

Global Information Grid (GIG) Core Enterprise Services Strategy. http://www.defenselink.mil/nii/org/cio/doc/GIG_ES_Core_Enterprise_Services_Strategy_V1-1a.pdf

Global Information Grid Net-Centric Implement Document. Service Definition Framework (S300) Version 2.0, 21 December, 2005.

Green, John M. and Bonnie Johnson. *Naval Network-Centric Sensor Resource Management.* April 2002.

Green, John M. and Bonnie Johnson. *The Theory of Measures of Effectiveness.* SAIC, 2000.

Harrison, D. *Modeling and Simulation Technology.* Studies and Analysis, 2003.

Hubanks, Bruce. *System engineering performance analysis of network-centric warfare.* Naval Studies Board, 2001.

Jacobs, Robert. *Model-Driven Development of Command and Control Capabilities for Joint and Coalition Warfare.* Naval Institute Press, 2004.

Jahn E, M. Hatch and J. Kaina. *Fusion of Multi-Sensor Information from an Autonomous Undersea Distributed Field of Sensors.* Proc. Fusion '99 Conf., Sunnyvale, CA, July 1999

Kelton, David and Averill Law. *Simulation Modeling and Analysis.* McGraw-Hill, 2000.

Klett, Mark, *Understanding DoD Enterprise Architectures.* DoD, 2004.

Llinas, James and Christopher Bowman. *Revisiting the JDL Data Fusion Model II.* WTF Press, 2004.

Locovetta, John M. *Open Architecture Track Manager/Joint Track Manager Brief.* Reference slide 7. Northrop-Grumman, 2004.

Luddy, John. *The Challenge and Promise of Network-Centric Warfare.* Feb 2005. http://www.lexingtoninstitute.org/docs/521.pdf

Macfadzean, Robert. *Surface-based Air Defense System Analysis.* Artech House, 2002.

Maier, Mark, and Eberhardt Rechtin. *The Art of Systems Architecting*. CRC Press, 2002.

Manavoglu, Eren. and Dmitry Pavlov, *Probabilistic User Behavior Model.* IEEE, 2003.

McGirr S., K. Raysin, C. Ivancic, and C. Alspaugh. *Simulation of underwater sensor networks.* Proc. IEEE Oceans '99 Conf., Seattle WA, Sept. 1999

National Military Strategy 2004.

Naval Capability Evolution Process Guidebook, Volume 1. ASN(RDA). Version 1.1 May 2005.

Naval Capability Evolution Process Guidebook, Volume 2. ASN(RDA). Version 1.1, December 2005

Naval Network Warfare Command, "*FORCEnet On-line*", available at http://forcenet.navy.mil, Internet, accessed July 2006

Naval Transformation Roadmap. DoD, 2003.

Norman Coscia, *Brief: Global Information Grid Overview/Status*, DoD, 2005.

OPNAV Instruction 3500.38A, Universal Navy Task List, May 2001

O'Rourke, Ronald. *CRS Report RS20851, Naval Transformation: Background and Issues for Congress.* Washington 2003.

Osterholz, John L., *The Global Information Grid DoD's Enterprise Architecture in Brief.* Naval Institute Press, 2004.

Poirier, J. *Summary Report: FORCEnet Human Systems Integration (HSI) Outreach and Coordination Initiative.* Deliverable D007 under Contract T0002AJM032 by Science Applications International Corporation (SAIC) 2003.

Policy for Management and Use of the Electromagnetic Spectrum. DoDD 4650.1 – Department of Defense Directive 4650.1 released on June 8, 2004.

Ragsdale, Cliff. *Spreadsheet modeling and decision analysis.* South-Western, 2004.

Rice, Joseph A. *Enabling Undersea FORCEnet with SeaWeb Acoustic Networks.* Naval Institute Press, 2004.

Rice, J.A., C. L. Fletcher, R. K. Creber, J. E. Hardiman and K. F. Scussel. *Networked undersea acoustic communications involving a submerged submarine, deployable autonomous distributed sensors, and a radio gateway buoy linked to an ashore command center.* Proc UDT Hawaii 2001 Conf, 30 October, 1 Nov 2001.

Rice J.A., and B. Marn. *TASWEX04 Seaweb Test Plan, Draft 7.1*. DoD, 2004.

Richter, D. *The Art of the Possible.* Undersea Warfare Spring 2006.

Rohde, Michael. *Play the Sveshnikov.* Hays Publishing, 1998.

Rushton, Richard T., Captain U.S. Navy. *Open Architecture: The Critical Network-Centric Warfare Enabled.* Proceedings, July 1996.

Single Integrated Air Picture (SIAP). Operational Concept document (July 2002)

SPAWAR Office of the Chief Engineer, *FORCEnet Architecture & Standards Volume I Operational & Systems View,* 2004.

SPAWAR Office of the Chief Engineer, *FORCEnet Architecture & Standards Volume II Technical View,* 2004.

Steinberg, Alan N. and Christopher L. Bowman, *Rethinking the JDL Data Fusion Level.* WTF Press, 2004.

Systems Engineering Handbook. International Council on Systems Engineering. Version 2a, June 2004

The Technical Cooperation Program (TTCP) Brief, 9 January 2006.

The Technical Cooperation Program (TTCP). Coalition FORCEnet Study – Operation Philippine Comfort Scenario, v0.g. January 2006

The Technical Cooperation Program (TTCP). MAR AG-6 Brief to Commander, Naval Network Warfare Command. April 24, 2006

Wagner, Daniel, Charles Mylander, and Thomas Sanders. *Naval Operations Analysis.* Naval Institute Press, 1999.

Walrod, John. *Sensor Network for Network-Centric Warfare*. Network-centric Warfare Conference, October 30-31, 2000.

Walker, Rob, *Common Operating Environment (COE) and Global Information Grid (GIG) Enterprise Services (GES).* Proceedings, Sept. 24, 2003.

Waltz, Edward L. *Information Understanding: Integrating Data Fusion and Data Mining Processes.* IEEE International Symposium on Circuits and Systems, 1997.

Wikipedia, on-line, available at http://en.wikipedia.org/wiki, accessed August 2006.

Young, Bonnie W. *Future Integrated Fire Control.* Northrop-Grumman, 2005.

Young, Bonnie W. *Integrated Fire Control for Future Aerospace Warfare.* Northrop-Grumman, 2004.

Young, Bonnie W, *FORCEnet – A Functional Concept for the 21st Century.* Northrop-Grumman, 2003.

Young, Bonnie W. *Combat Identification,* Northrop-Grumman, 2006.

Young, Bonnie W. *A C2 System for Future Aerospace Warfare,* Northrop-Grumman, 2004.

http://www.findarticles.com/p/articles/mi_qa3738/is_200403/ai_n9371189/pg_4

http://www.gmu.edu/departments/seor/insert/robot/robot2.html - accessed 8/7/06

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California