NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WATCHKEEPER

by

Rodney Glen Martinez

March 2010

Thesis Advisor:	Glenn Cook
Second Reader:	Karl Pfeiffer

Approved for public release; distribution is unlimited

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** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE WatchKeeper			**5. FUNDING NUMBERS**
6. AUTHOR(S) Rodney Glen Martinez			
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 thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The SAFE Port Act of 2006 designated the Coast Guard as the lead federal agency tasked with building Interagency Operations Centers in critical U.S. ports. A critical component of the IOC initiative is an Information Management System (IMS) to provide improved means for information sharing, and coordination among federal, state, local, and public sector stakeholders related to maritime safety and security in critical U.S. ports. The Coast Guard WatchKeeper project is a proposed IMS being designed to address the information sharing and information management challenges faced by these agencies. The WatchKeeper development program has faced challenges in delivering capability. Initial capability was to be delivered in 2009. This did not happen. Up to today, WatchKeeper has not delivered any new capabilities. Several development practices may provide advantages to the development process–ensuring value adding capabilities, minimizing project risk, and ensuring Coast Guard leadership can understand how WatchKeeper capabilities support the Coast Guard's core business process. This thesis describes these development practices, and proposes an architectural consideration to provide focus to future WatchKeeper products. This thesis concludes with considerations for further developing WatchKeeper, and recommendations for moving forward with development.

14. SUBJECT TERMS Enterprise Architecture, Information Management System (IMS) Inter-agency Operation Center, Enterprise Service Bus, Software Architecture, Software Architecture Analysis, VIRT (Valuable Information at the Right Time), Quality Attribute, WatchKeeper			**15. NUMBER OF PAGES** 81
			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** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WATCHKEEPER

Rodney G. Martinez
Lieutenant, United States Coast Guard
B.S., Kennesaw State University, 2002
M.S., National Graduate School, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Author: Rodney G. Martinez

Approved by: Glenn Cook
Thesis Advisor

Karl Pfeiffer, Lt. Col
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The SAFE Port Act of 2006 designated the Coast Guard as the lead federal agency tasked with building Interagency Operations Centers in critical U.S. ports. A critical component of the IOC initiative is an Information Management System (IMS) to provide improved means for information sharing, and coordination among federal, state, local, and public sector stakeholders related to maritime safety and security in critical U.S. ports. The Coast Guard WatchKeeper project is a proposed IMS being designed to address the information sharing and information management challenges faced by these agencies. The WatchKeeper development program has faced challenges in delivering capability. Initial capability was to be delivered in 2009. This did not happen. Up to today, WatchKeeper has not delivered any new capabilities. Several development practices may provide advantages to the development process–ensuring value adding capabilities, minimizing project risk, and ensuring Coast Guard leadership can understand how WatchKeeper capabilities support Coast Guard core business process. This thesis describes these development practices, and proposes an architectural consideration to provide focus to future WatchKeeper products. This thesis concludes with considerations for further developing WatchKeeper, and recommendations for moving forward with development.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. BACKGROUND....1
- B. RESEARCH QUESTIONS....1
- C. ORGANIZATION OF STUDY....2
- D. METHODOLOGY....2

II. WATCHKEEPER BACKGROUND AND LITERATURE REVIEW....5
- A. ENVIRONMENT....5
- B. PROBLEM CHARACTERIZATION....7
- C. ENTERPRISE ARCHITECTURE....11
- D. SOFTWARE ARCHITECTURE....15
- E. SOFTWARE ARCHITECTURE EVALUATION (SAE)....16
- F. CONCLUSION....17

III. WATCHKEEPER OVERVIEW....21
- A. INFORMATION SHARING AND HOMELAND SECURITY....21
- B. THE WATCHKEEPER DEVELOPMENT APPROACH....25
- C. WATCHKEEPER APPROACH TO INFORMATION SHARING....30
- D. LEVERAGING EXISTING CAPABILITIES....33
- E. CONCLUSION....33

IV. WATCHKEEPER ARCHITECTURE PROPOSAL....35
- A. PROPOSED APPROACH....35
- B. SMART PUSH....38
- C. FRAMEWORK CONSIDERATIONS....39
- D. COMPONENTS....40
- E. FUNCTIONAL REQUIREMENTS....45
- F. PRIORITY REQUIREMENTS....46
- G. EXAMPLE QUALITY ATTRIBUTE SCENARIOS....46
- H. ARCHITECTURE PROPOSAL RISKS....48
- I. ARCHITECTURE PROPOSAL CONCLUSIONS....49

V. CONCLUSIONS AND RECOMMENDATIONS....51
- A. CONCLUSIONS....51
- B. RESEARCH QUESTIONS....54
- C. FUTURE RESEARCH....56

LIST OF REFERENCES....59

INITIAL DISTRIBUTION LIST....63

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Port Partner Access (From: C2CEN, 2008) 26
Figure 2. WatchKeeper System Overview (From: C2CEN, 2008) 29
Figure 3. WatchKeeper Data Stores and Interconnections (From: Detailed Design Document, 2008) 31
Figure 4. Smart Push (From: Hayes-Roth, 2006) 38
Figure 5. Component-based Product-line Architecture for VIRT (From: Hayes-Roth, 2006) 41
Figure 6. WatchKeeper (After: Detailed Design Document, 2008) 43
Figure 7. VIRT Components within WatchKeeper 44
Figure 8. Normal Monitoring (1) 47
Figure 9. Target Vessel Selected for Boarding is Late (2) 48

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

In 2006, Congress tasked the United States Coast Guard with building Interagency Operations Centers to support enhanced collaboration and information sharing among port partners within the critical ports of the United States. The Coast Guard recognized a need for improved situational awareness, coordination of maritime operations, and integrated vessel targeting. WatchKeeper is a proposed information management system intended to deliver capabilities to support these objectives.

WatchKeeper development faces many challenges. The first segment of WatchKeeper was scheduled to deliver initial capability in December of 2009. The WatchKeeper project did not meet this projected delivery date. Second, the Coast Guard is in the midst of integrating an organization-wide enterprise architecture requiring all information systems to comply with developing standards, practices, and procedures. Presently, the WatchKeeper development project has nine million dollars to spend to build this information management system–a relatively small amount considering the complexity of this endeavor.

This thesis provides an analysis of WatchKeeper–the context surrounding its development, the systems architecture, and the potential risks present within its development.

Three primary practices can be applied to support WatchKeeper development, which can provide structure, meaning, and value to the WatchKeeper project: Enterprise Architecture, Software Architecture, and Software Architecture Evaluation. This thesis reviews literature from leading experts in the field of IT and software development and makes recommendations accordingly.

Furthermore, ensuring valuable information can be delivered minimizing "information glut," requires a new approach to information delivery. One such approach is "Valuable Information at the Right Time" (VIRT) (Hayes-Roth, 2005). This thesis provides an architecture proposal that considers the Watch-stander day-to-day operations developed using VIRT methodologies and constructs.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BFT	Blue Force Tracking
C2	Command and Control
C2CEN	Command and Control Center
CBP	Customs and Border Protection
CDO	Command Duty Officer
CG	Coast Guard
CG COP	Coast Guard Common Operational Picture
CGDN	Coast Guard Data Network
COI	Conditions of Interest
COP	Common Operational Picture
CWSS	Common operational Web Services System
DHS	Department of Homeland Security
DoD	Department of Defense
DSD	Dynamic Situation Data
EA	Enterprise Architecture
EDS	Environmental Data Server
ESB	Enterprise Service BUS
FOIA	Freedom of Information Act
GIS	Geospatial Information System
GWOT	Global War on Terror
IDUL	Information Discovery and Understanding Layer
IMS	Information Management System
IOC	Interagency Operations Center
IOC/C21	Interagency Operations Center/ Command 21
IOP	Interagency Operational Planning
IPIL	Information Presentation and Interface Layer
ISPCL	Information Sharing, Processing and Consolidation Layer
IT	Information Technology
IVT	Integrated Vessels Targeting
MAGnet	Maritime Awareness Global Network
MCN	Model-Based Communication Network
MDA	Maritime Domain Awareness
MHS-OPS	Maritime Homeland Security Operations
MISLE	Maritime Information for Safety and Law Enforcement

NAIS	National Automatic Identification System
NOA	Notice of Arrival
OGA	Other Government Agency
OIG	Office of Inspector General
OM	Operations Monitoring
OPORD	Operational Requirements Document
OSC	Operations Systems Command
PMP	Project Management Plan
QA	Quality Attribute
SA	Software Architecture
SAE	Software Architecture Evaluation
SAFE	Security and Accountability For Every (SAFE) Port Act of 2006
SAR	Search and Rescue
SOA	Service Oriented Architecture
USCG	U.S. Coast Guard
VIRT	Valued Information at the Right Time
Web COP	Web Common Operational Picture

ACKNOWLEDGMENTS

The author would like to convey sincere appreciation to Mr. Glenn Cook, and LT. Colonel Karl Pfeiffer for their professional guidance, expertise, and assistance throughout this thesis process. Mr. Glen Cook has been a mentor, a professor, and a great friend who has shared his passion for education, intellectual achievement, and concern for NPS students. His clear thinking and objective reasoning has been a guiding light throughout my studies.

My acknowledgements begin with United States Coast Guard office of the Assistant Commandant for Capabilities (CG-7613) for their support in providing background, context, and documentation to support this thesis research. My research would not have been possible without the motivation, and support of CG-7613 staff. Specifically, Lieutenant Commander Rusty Dash's support provided clear and objective analyses, which made this research possible.

My family deserves high recognition for supporting me through the tireless research, continually displaying sincere devotion to my efforts. My wife Lynn has been a great example of selfless endurance as she has supported me through all of my educational endeavors with positive motivation and personal reassurance. Grandma Helene has been an invaluable part of our family, providing care for my three wonderful children, Elayna, Layton, and Alysia throughout my coursework, and Coast Guard career.

Finally, I would like to extend my sincere gratitude to the faculty and staff of the Naval Postgraduate School GSOIS for their motivation and unparalleled support throughout my curriculum. Specifically, Dr. Alex Bordetsky, a true scientist and artist, who took great concern for my academic development early in my program of study. I would like to thank Dr. Rick-Hayes Roth for his passion, and concern for the development of his students.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

A critical need exists for federal, state, and local agencies to share information, and improve the coordination of maritime operations. The SAFE Port Act of 2006 addresses this need by designating the Coast Guard as lead agency for developing an environment, which facilitates this need and enhance existing maritime operation capabilities in major U.S. ports. The SAFE Port Act specifically directs the development of Inter-agency Operations Centers (IOC's) for this purpose. One aspect of the IOC initiative that presents a major challenge to the effectiveness of maritime operations is information sharing among maritime centric organizations. Information sharing among federal, state, and local agencies requires both political and technical strategies that consider the political environments, technical environments, and capabilities of participating agencies. The Coast Guard has proposed the development of an Information Management System (IMS), presently referred to as WatchKeeper, to address these challenges.

B. RESEARCH QUESTIONS

The primary purpose for this thesis is to analyze the strategy, architectural design, and development approach of the Coast Guard WatchKeeper Information Management System primarily to answer the following questions: (1) what are the significant challenges facing the Coast Guard in developing this IMS? (2) Is the Coast Guard leveraging best practices (as identified by research) to develop WatchKeeper? (3) What is the primary focus of the WatchKeeper development approach? (4) How might the WatchKeeper development team ensure the right capabilities are delivered to their customers? Secondarily, conducting this research (1) provides a better understanding of the context in which WatchKeeper is being developed; (2) develops a refined understanding of the proposed system design; (3) identifies essential practices for

developing complex IT systems as they relate to methods being employed in the development of WatchKeeper; and (4) facilitates conclusions and recommendations based on findings.

C. ORGANIZATION OF STUDY

This thesis begins by first describing the context surrounding WatchKeeper development–the Coast Guard's missions, importance of providing safety and security within major U.S. ports, historic events leading to WatchKeeper, and policies providing impetus for WatchKeeper. Chapter II also describes challenges facing WatchKeeper development. Chapter III provides a literature review covering current, fundamental Information Technology (IT) practices. The research conducted for this thesis suggests that the methods covered in the literature review are essential for promoting effective IT development within organizations–specifically, these methods relate directly to the ongoing Coast Guard Enterprise Architecture initiative (in general) and the WatchKeeper development project–Enterprise Architecture (EA), Software Architecture (SA), and Software Architecture Evaluation (SEA). Chapter IV discusses the challenge of information from national level policies, and presents an approach described in one of the literature resources. Chapter V explains the WatchKeeper development approach, development constraints, development requirements, and existing architectural plans. Chapter VI presents an architectural proposal that aligns with methodologies covered in the literature review–specifically, it provides a scenario, which describes, in detail, the general operating environment in which WatchKeeper is to be deployed. This proposal suggests a shift in perspective from focusing on specific functional requirements to shared situational awareness, and information sharing as they relate to past, present, and future time domains. In conclusion, this chapter presents potential considerations for further developing a WatchKeeper framework and components.

D. METHODOLOGY

For the purposes of fulfilling the research objectives of this thesis, the following methods were used.

- Literature review of topics that support the development of value adding IT capabilities
- Data gathering from Coast Guard offices specifically tasked with WatchKeeper development
- Application of methods researched
- Development of conclusions and recommendations based on research

THIS PAGE INTENTIONALLY LEFT BLANK

II. WATCHKEEPER BACKGROUND AND LITERATURE REVIEW

A. ENVIRONMENT

The maritime environment is a complex environment, which requires the attention of vast numbers of stakeholders–from fishermen to longshoreman; recreational boaters to tanker captains; military forces to conservationists and tribal fisherman. Basically, anyone who lives near the water or benefits from commerce enabled by it, is a stakeholder. This environment is risky and fraught with hazards. Maintaining order, safety, and protection of people and property in this domain requires some form of coordination among these stakeholders. The U.S. Coast Guard is the lead agency for maritime security, and as such, provides five unique services.

1. Maritime Safety: Minimize deaths, injuries, and property damage associated with maritime transportation, fishing, and recreational boating.
2. Maritime Security: Protect America's maritime borders from intrusions by: (a) halting the flow of illegal drugs, aliens, and contraband into the United States through maritime routes, (b) preventing illegal fishing, and (c) suppressing violations of federal law in the maritime arena.
3. Maritime Mobility: Facilitate maritime commerce and eliminate interruptions and impediments to the efficient and economical movement of goods and people, while maximizing recreational access to the water.
4. National Defense: Defend the nation as one of the five U.S. armed services. Enhance regional stability in support of the National Security Strategy, utilizing the Coast Guard’s unique and relevant maritime capabilities.
5. Protection of Natural Resources: Eliminate environmental damage and the degradation of natural resources associated with maritime transportation, fishing, and recreational boating (USCG, 2001).

There are 22 major container ports in the United States (Safe Port Act, 2006). These ports are the gateways for the U.S. economy exports and imports. Consider the Port of Long Beach–“In 2006 the Port moved more than $100 billion in goods. It supported about 1.4 million jobs in the U.S. and generated about $15 billion in annual trade-related wages” (Port of Long Beach, 2009). Safety, security, and continuous flow of

commerce are critical to the livelihoods of millions of people. Temporarily shutting down a port (or some portion of it) would cost multiple billions of dollars; completely shutting down a port could have catastrophic consequences.

September 11, 2001 created fears concerning the security of ports critical to U.S. infrastructure. How could terrorism infiltrate U.S. borders—U.S. ports? If a terrorist or a group of terrorists wished to strike at the welfare of Americans, a major U.S. port would certainly seem a likely target. The threat of terrorism became a new problem and risk domain for all maritime stakeholders. Information sharing and cross-agency collaboration became important considerations for future federal government responses. This event alone thrust the Coast Guard into one of the greatest organizational and social changes ever experienced by an armed service of the United States–becoming the armed service for a brand new Department of Homeland Security (DHS), including taking on new counter-terrorism responsibilities, becoming active participants in the Global War On Terror (GWOT); the list goes on. Approximately 40,000 strong, the U.S. Coast Guard must manage to balance budgets, and mission requirements with ever-increasing demands. .

In August of 2005, Hurricane Katrina hit the gulf coast requiring an unprecedented response from federal agencies. Once again, the federal government had been struck by catastrophe. Coordination among federal, state, and local agencies, during this incident, was almost non-existent (Executive Office of the President, 2006). Immediately after, interoperable communications, collaboration, and information sharing, became an order mandated by the federal government (DHS, 2008). Once again, catastrophe stimulated change; the federal government suddenly realized how vulnerable ports and waterways are to natural disasters. Agencies–federal, state, and local–had to do a better job of collaborating and sharing information. What was once a given responsibility, disaster response, recovery, and mitigation, became another government-wide mandate.

The inherent complexities and risks associated with the maritime environment, and the significant events that have occurred in recent history, initiated new, government-wide strategies and policies that require collaborative, information sharing environments

within the maritime domain. One such strategy, "Department of Homeland Security Information Sharing Strategy," describes DHS's strategy for addressing the challenges of developing these environments. "The National Strategy and the updated 2007 National Strategy for Homeland Security envision a coordinated and integrated Information Sharing Environment to effectively fight terrorism and respond to man-made and natural disasters. Both strategies give DHS a central role in ensuring that critical information is shared rapidly to the fullest extent allowed by law." This document also recognizes the role the Coast Guard plays in developing this environment. "Over the past two years, DHS has launched a number of initiatives and pilots to increase operational information sharing, including but not limited to: … the Coast Guard-led Inter-agency Operational Centers…"

The Coast Guard is the lead agency for maritime security. Federal, state, and local agencies (including Department of Defense (DoD)), have been mandated to comply with the Security and Accountability For Every (SAFE) Port Act of 2006. Within this act, Congress specifically directs the creation of Interagency Operations Centers (IOC's) in all high-priority ports by 2009. Congress appropriated $60 million for each fiscal year from 2006 through 2012 to accomplish this task (SAFE Port Act, 2006).

B. PROBLEM CHARACTERIZATION

Presently, federal, state, and local agencies do not have the capacity to collect and process the increasing amount of information required to meet the challenges of interagency coordination and maritime security. Every individual agency that participates in maritime safety and security operations collects its own information, develops and employs its own processes for operating, and owns and maintains separate, stove-piped, networks of data and application resources. Developing an information sharing architecture that provides access to organizationally and geographically disparate, technology resources is a challenging endeavor. To develop such an architecture requires buy-in from agencies that own and manage data and functionality critical to maritime operations. To add further to the challenge of such an initiative, every port presents its

own unique set of challenges as the lists of participating agencies differ widely from port to port. The level of agency coordination and participation is drastically varied as well.

The Coast Guard has been tasked with leading the development of a new, collaborative, port safety and security environment for IOC's (SAFE Port Act, 2006). Their proposed solution for addressing this task is to build an Information Management System (system of systems)–conceptually called "WatchKeeper."

To begin, the IOC initiative describes three major components that need to be developed to realize collaborative, interagency operations: (1) facilities, (2) an information management system, and (3) a network of sensors. WatchKeeper is intended to address the IMS portion of the greater IOC initiative.

The stated objectives of WatchKeeper are to provide: (1) Integrated Vessels Targeting (IVT), (2) Interagency Operational Planning (IOP), and (3) Operations Monitoring (OM). Presently, these IT capabilities do not exist. The Coast Guard identified these high-level, functional, requirements as primary focus areas for the proposed IMS. These objectives would address critical gaps in maritime security; thus, fulfilling the broad requirements set by SAFE Port Act of 2006. The latest design document explicitly defined the design objective to be the following: "Development and deployment of the Information Management System (conceptually called WatchKeeper), to improve the capability to see, understand, and share tactical information critical to security and interagency coordination in vulnerable ports and coastal areas…" (C2CEN WatchKeeper Detailed Design, 2008).

A vast number of organizations constitute maritime security. Agencies that have been identified by the SAFE Port Act of 2006 to participate in IOC activities include the U.S. Coast Guard (as lead), Customs and Border Patrol, Immigrations and Customs Enforcement, Transportation Security Administration, Department of Justice, Department of Defense, other federal agencies, state and local government and law enforcement agencies, port security personnel, members of the Area Maritime Security Committee (AMSC), and other public and private stakeholders adversely affected by a transportation

security incident or transportation disruption. Developing a system of systems that provides a medium for sharing information and coordinating interagency activities to all of these stakeholders is a monumental task.

> With such a high volume of daily activity in so many different mission areas, the Coast Guard faces a daunting information and communication problem. It needs to efficiently process and effectively utilize large amounts of varied information that typically originates from unplanned events. Unfortunately the Coast Guard is burdened with an information technology (IT) infrastructure composed of standalone applications and communications networks that lack interoperability. The combination of heterogeneous missions, applications, and networks creates information sharing problems within the Coast Guard and with external entities that result in operational inefficiency and ineffectiveness. In addition the Coast Guard has become an integral part of the rapidly evolving, extended homeland security enterprise that spans multiple federal departments and reaches out to many state and local government agencies. This means the 4 information sharing needs of the Coast Guard are ever growing and will be increasingly influenced by its partners, both within the federal government and beyond. (Creigh, Dash, 2007)

To add to the complexity of the information sharing challenge, there are vast differences between present capabilities, and present collaborative environments that exist within the many Coast Guard command centers today. Some Coast Guard operations centers are fraught with technologies, from audio/video-feeds to monitors that span tens of feet, touch screen, digital audio/video interfaces, multiple communications interfaces, and complex presentation technologies. Yet, some command centers provide just enough capability to support Coast Guard operations alone. Most activity occurring in a command center today is directed toward sifting through vast amounts of information for developing a picture of events presently unfolding and anticipating events expected or planned for within the next 24-hour watch cycle. “Information Glut” (Hayes-Roth, 2005) is inhibiting the Watch-stander’s ability to consider best alternatives. This only describes the Coast Guard command center environment and does not provide insight into other agency environments that play a critical role in the IOC information-sharing environment.

Presently, information sharing between agencies is primarily accomplished through face-to-face interaction, or through telephone conversations. To describe the complexity of these issues further, in metro Seattle alone, approximately 30 different operations/communications centers exist that are concerned with events occurring in the maritime environment. How much information is being shared? How much operational coordination is occurring? Who needs what information?

As of now, no other agencies are formally involved in the development of WatchKeeper. Other agencies engaged in maritime safety and security must become partial owners of the WatchKeeper system to ensure the successful deployment of a product that delivers value to all participants. Data-sharing agreements must be made between organizations; architectural decisions must be negotiated; semantics discussed and agreed upon; responsibility for maintenance and further development must be accepted by more than one agency for this proposed IMS to gain credibility. All of these factors must be considered in the overall architecture of such an IT centric, collaborative initiative.

Enterprise Architecture (EA) provides a means for organizations to view their existing IT capabilities, and map these capabilities to core business processes. This is a necessary step in the technological evolution of organizations. Many benefits to developing an EA exist. Two specific benefits are (1) the ability to identify the value of existing IT capabilities, and (2) the ability to plan for future, value-generating, IT initiatives strategically. The risks for not developing an EA are many and significant. First, an organization that cannot directly link its IT capabilities with its core business processes cannot understand the impact IT is having on its overall organizational performance. This often results in limitations or declinations in performance. Organizations may be supporting multiple, geographically dispersed IT capabilities that provide the same or similar services but that are cost, and data silos. Not only does this condition affect organizational performance, it also creates virtual roadblocks for technological advancement by making the process of standardization, and process reengineering extremely difficult. Data and processes must be merged and standardized so that new technologies can be built upon an understandable architecture; thus, ensuring

an organization is gaining the maximum value from its IT initiatives by guaranteeing every capability that exists and is planned for maps to the organization's strategic objectives.

Presently, the Coast Guard is in the process of implementing an EA. This presents a significant risk to the WatchKeeper development project. The Architecture WatchKeeper must consider the requirements and objectives being developed for the overarching enterprise architecture. WatchKeeper is intended to be a 20-year life cycle project (Assistant Commandant For Capability, USCG, 2009). The design must be robust and flexible enough to adjust to the Coast Guard's long-term IT strategy as doing so requires a design that fits organizational needs–both present and future. An example of inconsistent design, which is counter to EA principles, is that current design documents suggest data feeds exist from back-end data connections providing resources to proposed WatchKeeper products. This design is counter to WatchKeeper proposed designs, which are based on Service Oriented Architecture (SOA) principles. To standardize information-sharing techniques to create a robust and logical architecture, all data connections should be built using SOA practices rather than a patchwork of ad hoc data connections that lack sufficient documentation.

C. ENTERPRISE ARCHITECTURE

According to Ross, et al., it is critical for an organization to build a "Foundation for Execution"–the IT infrastructure and digitized business processes that automate its core capabilities (p. 4). Building a solid foundation for execution is essential for organizations to leverage IT effectively. The value of building a foundation for execution can be described in the following context: mundane, routine, business processes are automated so that an organization "… can concentrate on achieving greatness" (p. 3). For the Coast Guard, this means core processes are automated so operators can focus on achieving the highest levels of performance.

Ross et al. describes three key disciplines for building an effective foundation for execution: (1) Operating model, (2) Enterprise Architecture (EA), and (3) IT engagement model. For the purposes of this thesis, EA is the primary discipline discussed.

It is necessary to understand the fundamental concepts surrounding Enterprise Architecture (EA) to leverage technology within a large organization effectively.

> …enterprise architecture, the organizing logic for core business processes and IT infrastructure reflecting the standardization and integration of a company's operating model. The enterprise architecture provides a long-term view of a company's processes, systems, and technologies so that individual projects can build capabilities–not just fulfill immediate needs. (Ross, Weill, Robertson, 2006)

Ross et al. describes enterprise architecture as the logic behind the relationship between IT and core business processes. This relationship requires some level of process and technology standardization to support an organization's operating model. Ross et al. defines "operating model" as "…the necessary level of business process integration and standardization for delivering goods and services to customers" (p. 25). The authors identify four general operating models: Coordination, Unification, Diversification, and Replication. Without describing the details specific to each model, it is important to note that the Coast Guard might consider identifying and fully understanding its operating model to assist in the development of its EA. An EA, in turn, would provide a more meaningful context for a software architecture, which supports WatchKeeper objectives (previously defined). Ross et al. lists keys to effective EA, "…to identify processes, data, technologies, and customer interfaces that take the operating model from vision to reality" (p. 46).

In July of 2009, DHS Office of Inspector General (OIG) completed a review of the Coast Guard's EA implementation. It identified both strengths and weaknesses of the current Coast Guard EA implementation project. It is important to note that, according to the OIG, the Coast Guard has not yet fully implemented an EA across the organization. This raises a concern for the development of WatchKeeper. How can such an initiative be fully aligned with an EA that does not exist?

The following is an excerpt from the OIG report describing critical components missing from the current Coast Guard EA.

"The Coast Guard has not fully integrated its enterprise architecture. Integration is needed to show how the data from various major information systems fits together. There are 3 profiles, 3 models, and 7 inventories for the enterprise architecture that have not been completed. The 3 profiles not completed are:

1. C4&IT Performance Profile: The C4&IT performance metrics as they relate to the DHS performance areas and federal enterprise architecture Business Reference Model.
2. Balanced Scorecard for C4&IT: An overview of Coast Guard C4&IT performance related to business process, learning and growth, customers, and finances.
3. External Services Profile: Provides a high-level view of systems leveraged at the Coast Guard but managed outside the Coast Guard.

The 3 models not completed are:

1. Unified Performance Logic Model: A framework for planning, managing, measuring, and evaluating Coast Guard enterprise architecture programs. It illustrates the cause and effect linkages between program activities and outcome results.
2. Business Models: Displays Coast Guard enterprise architecture business activities and can be used to identify dependencies, redundancies, and gaps between the Coast Guard's activities
3. Applications to Business Activities Matrix: Describes the relationship between Coast Guard services and activities

The 7 inventories not completed are:

1. Functional Statements: Describes the roles and missions of the Coast Guard headquarters offices.
2. Information Inventory: Shows all information objects, produced, archived, and/or required for Coast Guard enterprise architecture activities, reporting, and decision making, and their relationship within the DHS Conceptual Data Model.
3. Information Exchange Matrix: Identifies the information transfers that are necessary to achieve Coast Guard tasks.
4. Information Dictionary: Identifies, defines, and provides additional data to describe items listed in the information inventory.

5. Services Inventory: Aligns Coast Guard applications and systems to the federal enterprise architecture. As such, it helps to explain the services offered by each of the Coast Guard's applications and systems.

6. External Services Inventory: Describes systems managed outside the Coast Guard and is organized by grouping applications to systems. The content includes attributes across each of the six Coast Guard perspectives and provides a baseline mapping assets to the DHS and federal enterprise architectures.

7. Frequency Spectrum Inventory: Lists the frequency spectrums necessary for the Coast Guard's mission operations" (Department of Homeland Security, Office of Inspector General, 2009).

Therefore, it is difficult to describe, with sufficient detail, the core business processes that define the organization and its core capabilities as a whole (processes which the Coast Guard must do right to be effective). The Operational Requirements Document (OPORD) developed for IOC/WatchKeeper does identify core capabilities necessary for the proposed IOC's. These core capabilities might be seen as core business processes: (1) integrated vessel targeting, (2) interagency operational planning, and (3) operations monitoring. Furthermore, the OPORD identifies existing components that should support these capabilities. It also proposes a framework for which these components deliver these capabilities. Thus, to define the IOC's operating model, the following questions must be asked: (1) what specific business processes is the Coast Guard attempting to integrate? (2) what specific business processes does the Coast Guard need to standardize? and (3) what level of standardization and integration can the Coast Guard achieve given the uniqueness of each of the 22 major ports?

In summary, the challenges for the Coast Guard in developing and fully leveraging the capabilities of an information sharing environment, such as WatchKeeper, are: (1) establishing a foundation for execution, (2) fully understanding its operating model, (3) developing an EA that supports its operating model, and (4) to develop a method of IT governance that ensures future IT decisions are guided by its EA software architecture. The WatchKeeper IMS must be aligned with the EA currently being established by the Coast Guard's Chief Architect Office of EA and Governance. This issue is discussed in further detail.

D. SOFTWARE ARCHITECTURE

Currently, software architecture is an essential practice for developing complex software systems. The need for software architecture became evident with the ever-increasing size and complexity of software systems. According to Clements, Kazman, Klein (2002), three reasons exist why software architecture is important to large and complex software systems: (1) it facilitates communication among stakeholders and makes it easier for them to understand and participate in the design process, (2) it brings important design decision to light early in the development stage. Software architecture is largely a visible and understandable view of a proposed system, and a common language for describing the systems properties, components, and structures (Bass, Clement, Kazman, 1998). Establishing software architecture early on allows individuals involved in the development process to discuss their different perspectives and concerns, potentially identifying conflicting system requirements, such as security vs. accessibility, or cost constraints vs. desired functionality, and (3) "It is a reusable, transferable abstraction of a system" (Clements, Kazman, Klein, 2002). Clements et al. contend that software architecture creates a model for other applications to be developed rather than starting from scratch with each new product. This provides alignment among all software products throughout an organization, which is usually referred to as software product lines. Clements et al. provide the following definition of software architecture. "The software architecture of a program of computing system is the structure or structures of the system, which comprise software components, the externally visible properties of those components, and the relationships among them" (Bass, Clements, Kazman, 1998).

The Coast Guard Commandant Instruction M5234.4–Coast Guard Software Development and Documentation Standards (CG-SDDS) provides specific guidelines for the development and documentation of software. It does not, however, discuss the purpose for or the importance of developing software architecture–software architecture is only briefly mentioned throughout the document. However, WatchKeeper documentation does provide general software architecture artifacts, such as diagrams that depict high-level data connections. The documentation provided for this thesis does not

provide enough evidence to suggest one, complete, software architecture exists for WatchKeeper. It is difficult to assert that software architecture is not being used to build mutual understanding among developers and stakeholders for this project.

E. SOFTWARE ARCHITECTURE EVALUATION (SAE)

A Software Architecture Evaluation (SAE) is a way to evaluate how well a design addresses the requirements identified by stakeholders and developers. Evaluating the architecture provides insight into a proposed system's strengths and weaknesses. According to Clements et al., "Architecture is a cheap way to avoid disaster." Software architecture evaluation tests the components and framework of the architecture to uncover potential problems with its design, and identify trade-off points between competing requirements.

Literature, concerning software architecture, often refers to the qualities of a software system as "Quality Attributes" QA, such as functionality, maintainability, or scalability–qualities the system should posses. "Quality attributes form the basis for architectural evaluation…" (Clements, Kazman, Klien, 2002, p. 32). By identifying a system's quality attributes, components, and the architectural style, the system designers can identify how a proposed architecture achieves these qualities, and in turn, identifying the risks which Clements et al. describe as, "…potentially problematic architectural decisions…" (p. 34).

Ultimately, software architecture identifies whether or not an architecture is suitable for the purpose in which it was designed. According to Clements et al., a design is suitable if it meets two criteria: (1) the system that is build based on the architecture will meet the quality goals of QA's identified, and (2) it is "buildable" (Clements et al., p. 27).

SAE should take place during the beginning phases of WatchKeeper development. No mention of SAE appears in the WatchKeeper Segment one project plan. Some critical risks associated with failing to conduct SAE in the early phases of design are the following.

1. Not having the ability to communicate critical design factors to stakeholders
2. Misidentification of critical design priorities, trade-offs, potential design constraints, and vulnerabilities
3. Developing a system that cannot meet its quality objectives

F. CONCLUSION

Congress has mandated that the Coast Guard produce an interagency environment for critical ports within the U.S., which would enhance the nation's ability to respond to maritime threats–both natural, and human. Presently, federal, state, and local agencies do not have the capacity to collect and process the increasing amount of information required to meet the challenges of interagency coordination and maritime security. The Coast Guard, recognizing the need to address these issues, initiated the development of the WatchKeeper–Information Management System. WatchKeeper is being designed to meet three primary objectives intended to enhance interagency coordination and response effectiveness in major ports: (1) Integrated Vessels Targeting (IVT), (2) Interagency Operational Planning (IOP), and (3) Operations Monitoring (OM). Information sharing, however, presents a significant challenge to the development of WatchKeeper, which was initially scheduled to be delivered with a baseline of capability by 2009 but has not yet been deployed. As of now, no formal partners are involved in WatchKeeper development. WatchKeeper is at risk of not being accepted by other agencies that should be participating in the development, and benefiting from its proposed capabilities.

The Coast Guard is presently developing and implementing an overarching EA. This presents a challenge for WatchKeeper design in that it must take into consideration design factors affecting its relationship to enterprise strategic IT initiatives. The design must consider EA standards, and policies to ensure its alignment with Coast Guard IT strategies.

Information sharing within WatchKeeper consists of a VPN connection for port partners. The term information sharing is somewhat misleading. Today, information sharing, in terms of current technology, is usually built on services that push and pull data from disparate resources using Service Oriented Architecture (SOA) principles. VPN

connections in the Coast Guard today are primarily established by older token technologies; however, a transition is underway to establish a newer form of secure network access that still falls short of a true service-based system (Dash, 2010).

Enterprise Architecture provides a foundation for organizations to leverage the value of IT fully. The Coast Guard is presently implementing EA. WatchKeeper is intended to have a 20-year life cycle. An information management system of such size and complexity must be designed in accordance with proposed EA standards and objectives. By developing a robust and logical software architecture that meets Coast Guard EA standards and objectives, WatchKeeper can map its capabilities to Coast Guard, overarching, IT strategies–ensuring its credibility and survivability as a major IT system.

Logically, EA, SA, and SAE provide a layered approach to obtaining the most value from major IT initiatives. EA provides an as-is state of organizational IT capabilities, which, in turn, provides organizations with an opportunity to assess the value of these capabilities. If capabilities are redundant or do not align with organizational strategic objectives, they should be eliminated from the organization's IT portfolio to ensure the alignment of IT capabilities with core business processes and strategies. EA also provides a meaningful context for new IT initiatives in that it clearly defines IT needs and opportunities for both current and future capabilities. Software architecture in itself is nothing more than a sub architecture existing within the EA. A thorough, well-designed, software architecture delivers a needed capability that can be mapped directly to the EA. SA provides a means for developers and stakeholders to conduct meaningful discussions concerning the intended purpose and design of software capabilities. SA is a process for identifying software components and frameworks primarily to describe components that interact to deliver value to stakeholders. SAE should be conducted during the initial phases of software development. It supports both the SA and EA by evaluating proposed systems, in turn, identifying potential design constraints, decisions, and tradeoff points, which affect the value of delivered products. SAE is essentially a risk mitigation method for eliciting design flaws early on; –thus, minimizing the cost of addressing design flaws in later stages of development where costs of rework increase.

Although artifacts of software architecture for WatchKeeper exist, documentation is limited, making any assertions as to the quality or existence of an official software architecture difficult.

Is the Coast Guard leveraging best practices (as identified by research) to develop WatchKeeper? It is evident that the Coast Guard is attempting to apply best practices in the development of WatchKeeper; however, it is not readily apparent that any formal process exists to ensure these practices are priorities or that these practices yield value as depicted in literature.

THIS PAGE INTENTIONALLY LEFT BLANK

III. WATCHKEEPER OVERVIEW

> Data sharing is today's principal Information Technology challenge. All sectors—commercial, government, academic, and military—seek improved information exchange to achieve operational benefits, whether in the form of greater profits, improved situational awareness, intellectual advancement, or ability to respond to threats endangering respective interests. Nations and organizations within and across nations have set forth policies to promote greater data sharing, but often without empowering or enabling change agents to introduce measurably better capabilities. (Hayes-Roth, Pullen, Blais, Brutzman, 2008)

A. INFORMATION SHARING AND HOMELAND SECURITY

Information sharing is critical to homeland security. Both September 11 and Hurricane Katrina provided valuable lessons and insight into two different but related perspectives concerning the value of information sharing as a critical requirement to safety and security. September 11 exposed existing weaknesses in the government's capability to share information as it pertains to preventing terrorism. Katrina, on the other hand, revealed gaps in the U.S.'s ability to share, coordinate, and disseminate information during natural disasters (United States, Executive Office of the President, 2006).

Since these events, many documents and policies have been written that directly improved information sharing throughout all levels of government. However, these documents and policies do not provide enough information for agencies to develop succinct information sharing capabilities. What are the critical components to a national information sharing architecture? How do agencies align their information sharing initiatives? The National Strategy for Information Sharing describes the U.S. government's vision of how information sharing is to evolve.

> Improving information sharing in the post–September 11 world requires an environment that supports the sharing of information across all levels of government, disciplines, and security domains. As with our achievements to date, an improved information sharing environment will not be constructed overnight, but rather will evolve over time and will be the fruit of careful cultivation. An improved information sharing environment also will be constructed upon a foundation of trusted partnerships among all levels of government, the private sector, and our

> foreign allies—partnerships based on a shared commitment to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism. (National Strategy for Information Sharing, 2007)

This vision presents an even greater challenge–the construction of an information-sharing environment built upon trusted partnerships that include the private sector and foreign allies. Not only do government agencies need to build information-sharing relationships and capabilities among themselves, they must also consider developing relationships with the private sector, and foreign allies.

Two critical aspects to information sharing, relating to homeland security not mentioned in the National Strategy for Information Sharing are: (1) similarities between information sharing strategies and requirements pertaining to disaster mitigation, response, and recovery, and those associated with terrorism prevention, and (2) the information policy, and technology challenges and opportunities that either foster or inhibit improved information sharing.

Similarities between homeland security disaster response and homeland security terrorism prevention efforts are worth mentioning. When building relationships for improved information sharing, as envisioned by the National Strategy for Information sharing, it is clear that most of the agencies involved in terrorism prevention are the same agencies involved in disaster mitigation, response, and recovery. Information-sharing strategies among federal, state, tribal, and private sector organizations need to be developed in consideration of both terrorism prevention and disaster related concerns. Awareness of the strong relationship between these two concerns fosters robust information-sharing strategies that can be adjusted to meet the overall needs of Homeland Security and prevent potential limiting perspectives of when and how information is to be shared. For example, the Washington Military Department, Emergency Management Division would be actively involved in a tsunami if one should occur within Washington state; as would the U.S. Coast Guard, FEMA, and other federal, state, tribal government and private sector organizations. The same agencies are actively involved in countering potential terrorist activities within their region on a day-to-day basis. Developing

information-sharing strategies that foster continuous, multi-mission, relationships establish fundamental linkages among these agencies that are essential for developing robust, technical, data sharing capabilities.

The information technology and policy challenges faced by the United States today are equally critical to the success of any national information sharing strategy. However, agency information sharing strategy documents do not directly describe these challenges.

> Data sharing is today's principal Information Technology challenge. All sectors—commercial, government, academic, and military—seek improved information exchange to achieve operational benefits, whether in the form of greater profits, improved situational awareness, intellectual advancement, or ability to respond to threats endangering respective interests. Nations and organizations within and across nations have set forth policies to promote greater data sharing, but often without empowering or enabling change agents to introduce measurably better capabilities. While progress is being made in some quarters, in others there is almost a counter-reaction where organizations are closing in on themselves, perpetuating traditional closed pockets of valuable information, even if sometimes having the appearance of adhering to the new policies. The advances are coming in fits and starts, resembling chaotic self-organizing systems, but with no overriding pressure to bring about incremental adaptive improvements. (Haye-Roth, Pullen, Blais, Brutzman, 2008)

According to Hayes-Roth et al., many initiatives today are attempting to address the challenge of information sharing and suggest systems that presently exist do not provide easily implemented, quick to deliver, or affordable information sharing. They suggest a "smart implementation strategy" to ensure best value for cost, in as little time as possible, by delivering solutions for immediate operational requirements. By doing so, benefits of information sharing can be realized and be measurable. This perspective is supportive of the highly abstract strategies and policies that exist, and it focuses specifically on putting those policies and strategies into practice. The critical piece of this perspective is the development of capability that is meaningful, achievable, affordable, reusable, and that delivers value.

To deliver such capability across many different agencies, in so many different problem or situations, Hayes-Roth et al. argue there must be policies and processes to coordinate their evolution on national and international levels. They propose an approach that focuses primarily on developing portfolios of capability, which are logical, value-adding collections of capabilities for particular problem domains. The capabilities referred to by Hayes-Roth et al are problem domain semantics, value-adding transactions, and components built to address the requirements related to a particular problem domain.

An example of a capability might be a Maritime Domain Awareness (MDA) Notice of Arrival (NOA) transaction supported by common semantics (related to this particular problem domain or mission domain), and software service components. Notice of Arrival data enters a data source, where a transaction occurs (valued data is extracted for a particular user type based on user criteria), and the valued data extracted by the data source is understood by the user (or service) accessing it. In this case, this data could be the nation from which the vessel last departed. The organization requesting the data might be Customs and Border Protection (CBP). The originating source would be the Coast Guard. The data would be application independent and visible by CBP information technology capabilities, or shared web resources. In this case, a particular portfolio of capabilities is recognized that supports a specific mission domain. Organizations must recognize that "different concerns and problems require different semantics" (Hayes-Roth et al., 2008). Hayes-Roth et al. argue, "…there is a need to describe how to manage the numerous semantic portfolios…" (2008). Hayes-Roth et al. propose a method for managing portfolios of capability, which is based on domains of concern–using MDA as an example. New components can be added to enrich information sharing capabilities by building on the initial capabilities within existing capability portfolios–adding value to transactions.

By approaching information sharing in the manner suggested by Hayes-Roth et al., agencies that agree to share information can focus on specific, valuable information sharing transactions.

B. THE WATCHKEEPER DEVELOPMENT APPROACH

Two Coast Guard documents provide a basic description of operational and design requirements driving the WatchKeeper development project: (1) The Operational Requirements Document (ORD), Interagency Operations Centers Command 21, document, and (2) a draft design document dated 8 September 2008. In the draft design document, WatchKeeper is referred to as a system of systems that leverages existing capabilities. These existing capabilities support three different layers of functionality: (1) Information Presentation and Interface Layer, (2) Information Discovery and Understanding Layer, and (3) Information Sharing, Processing and Consolidation Layer.

Essentially, WatchKeeper provides a means to consolidate data and existing application functionality to deliver collective capability. The draft detailed design document states that WatchKeeper is "…based on existing net-centric and service oriented capabilities…designed to loosely couple CG enterprise components and data sources" (C2CEN, 2008). The design is primarily web-based relying on backend data sources and virtualization to deliver reliable access to resources in an efficient, consolidated presentation layer. Coast Guard users can access capabilities directly through the Enterprise Service Bus (ESB) located within the Coast Guard Data Network (CGDN) where port partners must utilize VPN connections to access the system.

The following diagram depicts port partner access to WatchKeeper.

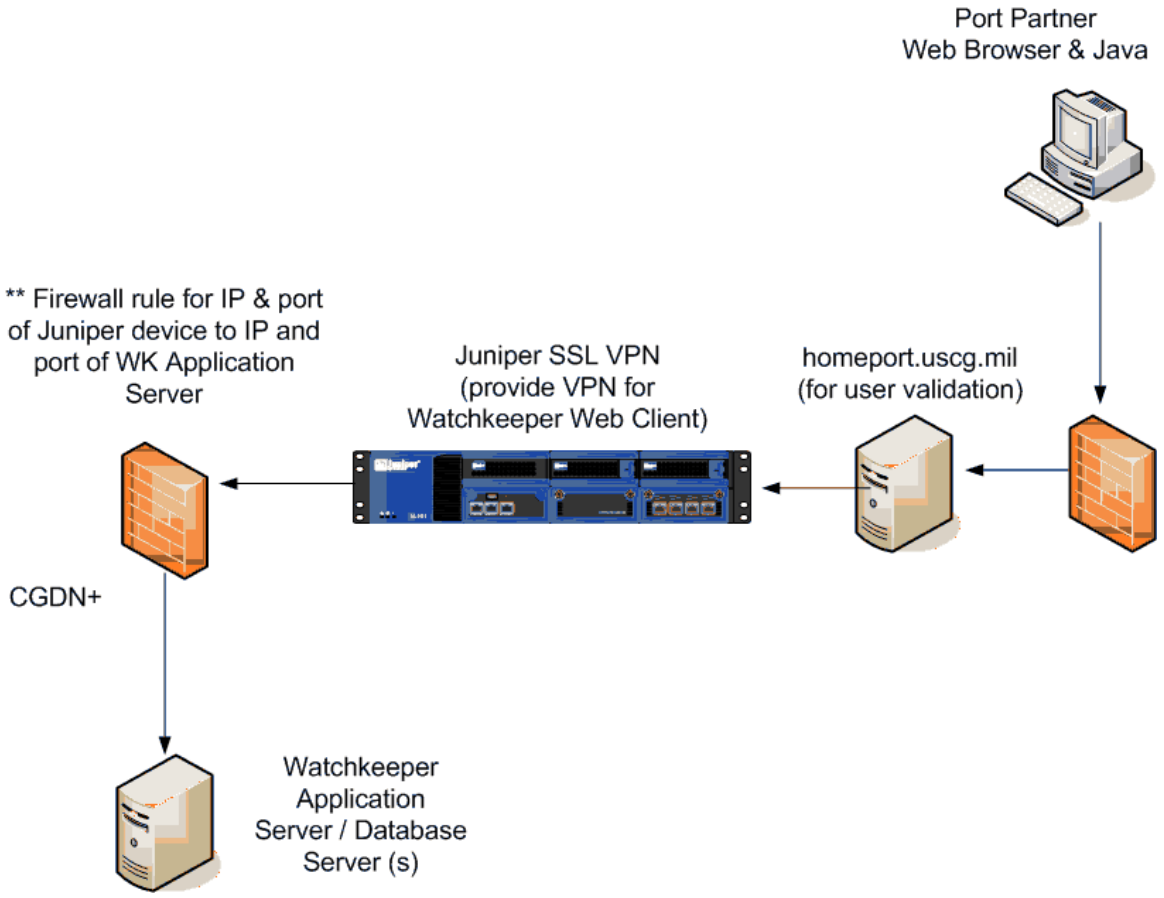

Figure 1. Port Partner Access (From: C2CEN, 2008)

WatchKeeper developers apply a spiral development to deliver capability in three segments. WatchKeeper is intended to have a 20-year lifecycle. Three proposed segments deliver capability. Segment one was to provide the following capabilities by the end of October 2009 (excerpt draft document IOC/C21 PMP).

- Integrate activities that support execution of business rules, data consolidation, information sharing, and workflow using automation to the greatest extent feasible.
- Support joint planning for vessel arrivals and security activities among key interagency partners.
- Compose and maintain a situation picture.
- Integrate activities that support execution of business rules, data consolidation, information sharing, and workflow using automation to the greatest extent feasible.

- Support joint planning for vessel arrivals and security activities among key interagency partners.
- Compose and maintain a situation picture.

Segment two provides a sensor and sensor management solution enabling Coast Guard and other agencies to share sensor capabilities. Segment two development begins in FY11, and continues through FY13. Segment three addresses lessons learned from segments one and two, with a completion and predicted deployment by the end of FY17.

According to a draft CG C2CEN document (number IOC/C21-08-3.1-11)–Project Management Plan, approximately $9.1M is available to develop WatchKeeper. It is unclear if this dollar amount is intended to cover the entire design and development project or just segment one (CG C2CEN, 2008).

The Coast Guard ORD breaks WatchKeeper system requirements into three categories: (1) mission requirements, (2) effectiveness requirements, and (3) non-technical requirements. The mission requirements are intended to focus development efforts on business processes present in proposed Interagency Operations Centers (IOC's). Effectiveness requirements describe data management requirements as they relate to information-sharing methodologies, such as Service Oriented Architecture (SOA). Non-technical requirements address user issues, such as usability, and training time.

The following is an excerpt from the WatchKeeper Segment one Project Management Plan (PMP): "WatchKeeper will transform the operational capabilities of the Sector Command Centers and improve tactical decision making, situational awareness, operations monitoring, rules based processing and joint planning in a coordinated interagency environment. WatchKeeper will close gaps in the Sector's capability to sense, understand, and share tactical information critical to security and interagency coordination in vulnerable port and coastal areas."

To fulfill these requirements, the Coast Guard has proposed to leverage several pilot technologies from various sources that provide some level of capability. The Coast Guard intends to build and implement data services on a Coast Guard Enterprise Service Bus (ESB) and Coast Guard Data Network (CGDN), and to gain access to and aggregate DHS/OGA data sources to support the data sharing components of WatchKeeper.

Three technologies have been considered for the presentation, interface, process, and collaboration aspects of the WatchKeeper system.

- Project SeahaWatchKeeper
- Web Common Operational Picture (Web COP)
- Maritime Homeland Security Operations (MHS-OPS)

Six additional existing technology capabilities provide data for WatchKeeper.

- Maritime Awareness Global Network (MAGnet)
- Maritime Information for Safety and Law Enforcement (MISLE)
- Common operational Web Services System (CWSS)
- Enterprise Geospatial Information System (GIS)
- Environmental Data Server (EDS)
- National Automatic Identification System (NAIS)

The following diagram provides a systems overview of WatchKeeper.

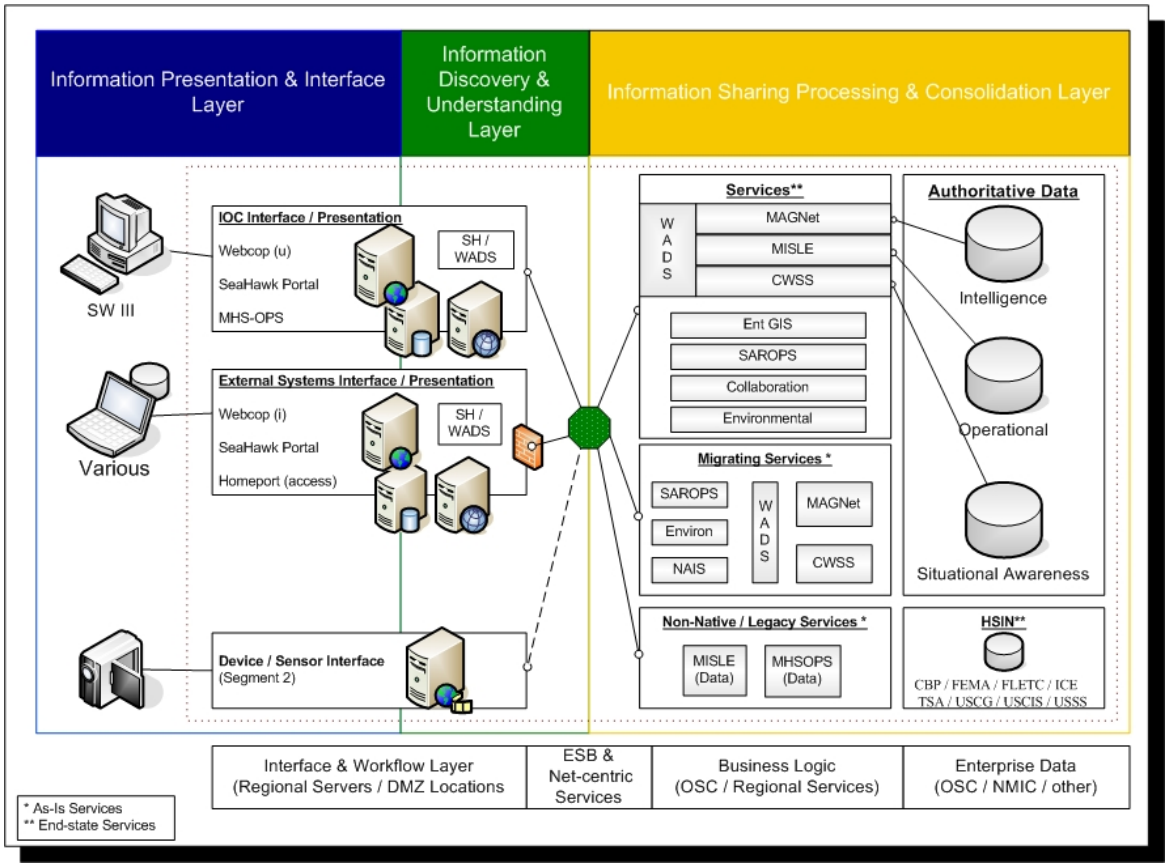

Figure 2. WatchKeeper System Overview (From: C2CEN, 2008)

Three primary capabilities for WatchKeeper segment one, which have been identified in the detailed design document, are: (1) Information Presentation and Interface Layer, (2) Information Discovery and Understanding Layer, and (3) Information Sharing, Processing and Consolidation Layer.

The Information Presentation and Interface Layer (IPIL) is the primary means by which users, both Coast Guard and port partners, are to access WatchKeeper. The design requires that users be able to share presentation interfaces and workspaces based on the user's role and access permissions. The purpose behind sharing presentation interfaces and workspaces is to fulfill three primary requirements of sharing operational awareness, mission tasking, and response information to all WatchKeeper participants.

The Information Discovery and Understanding Layer (IDUL) relies upon the Coast Guard ESB as a means of delivering information from various data sources. It is unclear what specific functionality the IDUL can provide. The Detailed Design document provides a brief description of the IDUL.

> The information requested on the ESB, which will be addressed in the following section, will be scheduled requested, processed, put in context, shared and acted upon within the business processes and logic of the understanding layer. The business processes will provide the necessary automated and manual functionality required to perform actions such as the vetting of arriving vessels, assignment of missions to available resources, rules-based monitoring of port activities and other critical functionality required to maintain port security and awareness. The gathering of external or partnering agency information will be acquired via this layer. The business processes will be established to support the collection, processing and sharing of this much needed local information as a key element of WatchKeeper. (CG C2CEN Detailed Design Document, 2008)

The Information Sharing, Processing and Consolidation Layer (ISPCL) is described as the layer of functionality that provides data sources to support WatchKeeper functionality. The following are primary types of data provided: (1) intelligence information, (2) vessel arrival information, (3) operational information, and (4) situational awareness information. Additionally, the detailed design document lists types of supporting data: (1) weather data, (2) enterprise Geospatial Information Systems (GIS) layers, and (3) Search and Rescue (SAR) mission details.

Presently, two Coast Guard organizations are responsible for developing, and delivering the WatchKeeper system. No evidence exists to suggest that other agencies are represented in the development process; however, other agencies are providing information to the Coast Guard Common Operational Picture (COP).

C. WATCHKEEPER APPROACH TO INFORMATION SHARING

Three primary high-level WatchKeeper components facilitate an information-sharing environment: (1) enterprise data sources, (2) business logic components, and (3) an Enterprise Service Bus (ESB). The term–information sharing–is misleading. The WatchKeeper information-sharing model based on services is a method for services

behind the Coast Guard firewall to share information among data sources owned and operated by the Coast Guard. WatchKeeper does not provide services that access port partner data sources. Port partners access WatchKeeper capabilities by VPN access only. This means no direct data connectivity is provided between WatchKeeper subsystems and disparate port partner data sources.

Enterprise data sources store data critical to maritime operations, such as law enforcement information, vessel arrival information, weather information etc. These data sources provide information that can be shared among the various Coast Guard owned and operated data sources, via WatchKeeper interfaces. However, some data sources receive data from other sources outside of the Coast Guard Data Network (CGDN). For example, CG COP data stores directly receive data from DoD, CBP, NOAA, and other agencies. It is unclear how these data resources are integrated (or connected). They may have been manually integrated–normally a costly and timely endeavor (Ortiz, 2007).

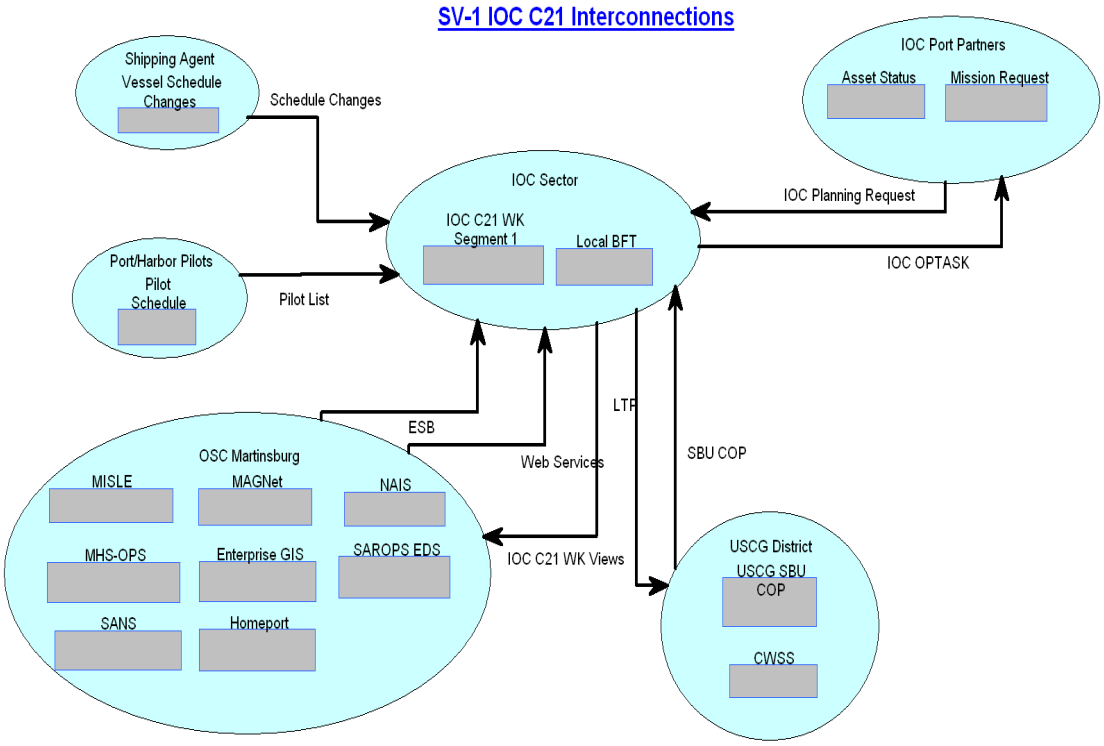

Figure 3. WatchKeeper Data Stores and Interconnections (From: Detailed Design Document, 2008)

Business logic components are software applications hosted by Coast Guard Operations Systems Center (OSC) that facilitate business transactions, such as the Marine Information Safety and Law Enforcement system (MISLE), and enterprise GIS. These applications access enterprise data sources for processing business transactions. Each application requires the use of a separate interfaces–an issue the WatchKeeper project intends to address by building an Enterprise Service Bus (ESB).

The ESB facilitates the coordination of many software services by acting as a message broker between them. "The ESB handles the transformation of data formats; routing; message acceptance, processing, and, the sending of multiple messages at the same time" (Ortiz, 2007). An ESB provides WatchKeeper design with functionality that supports single interface–merging data to display in one common operational interface.

The Operational Requirements Document (2009) describes three primary purposes for information sharing to be delivered in segment one of the WatchKeeper design process: (1) Integrated Vessel Targeting (IVT), (2) Interagency Operational Planning (IOP), and (3) Operations Monitoring (OM). The requirements described in the Operational Requirements Document are primarily functional.

- IVT requirements intend to facilitate coordinated vessel screening and boarding activities among partnering agencies.
- IOP requirements intend to facilitate coordinated operations and operational planning pertaining to all other maritime missions, such as disaster preparedness, or law enforcement.
- OM requirements intend to facilitate Command and Control (C2) for day-to-day operations by providing situational awareness, scheduling, and collaboration capabilities.

These requirements are designed so that port partners can access WatchKeeper through VPN connections and add appropriate information in support of these objectives.

The operating requirements described herein do not address information-sharing transactions but focus on the functionality of hardware and software components as they relate to Coast Guard and port partner activities. The documents available for this

research do not describe in detail how these requirements are to be implemented. A thorough investigation and analysis of the software and hardware architecture needs to be conducted to verify and validate such requirements.

D. LEVERAGING EXISTING CAPABILITIES

Many of the existing systems being leveraged are complex, homegrown, IT systems developed by the Coast Guard. This presents potential design risks as testing and evaluating the WatchKeeper architecture may identify design flaws in the existing products being used to support its objectives. Furthermore, quality attributes, such as maintainability, or reliability, may be at the mercy of these existing systems. Project scope is at risk of growing to encompass rework, and fixing design flaws in these systems. Other than building a completely new system, this research suggests that this is the only way to build a cost effective system, especially when considering projected capability delivery dates.

A software architecture evaluation should be conducted for each supporting system. This would require a significant amount of work, however. WatchKeeper, as it stands, is intended to provide evolving capability for 20 years. No perfect solution exists to minimizing the risks of a project so large and complex; however, building on a foundation of architecture evaluation in the early stages of this endeavor minimizes some risks–possibly preventing costly rework in the future. The future of WatchKeeper should be one of advancement in capability and building on solid architectures. If WatchKeeper builds on broken components or a broken framework, it could become more of a technological burden than a value adding system supporting IOC core business processes.

E. CONCLUSION

The primary objective of WatchKeeper segment one is to deliver the following capabilities: (1) Integrated Vessel Targeting (IVT), (2) Interagency Operational Planning (IOP), and (3) Operations Monitoring (OM). This will be accomplished by developing a single interface supported by and ESB that merges data from Coast Guard owned and operated data sources. Port partners are to be provided VPN access to enter data supporting these objectives.

The development of an ESB in itself is a complex task where methods services need to be developed to manage large numbers of data transactions among services. The documentation provided for this research does not describe in detail the ESB architecture providing this capability. It can be assumed that a great deal of SOA programming is necessary to ensure a robust ESB design.

The term information sharing is misleading. Information-sharing technologies today provide capabilities for pushing and pulling data from disparate data sources between organizations' primarily leverage services established to forego traditional technological barriers based on SOA principles. WatchKeeper limits information sharing by providing a basic for of network access. VPN requires port partners to agree on using this form of access to support WatchKeeper objectives.

Multiple data sources and subsystems exist that can be leveraged to support WatchKeeper objectives–software reuse is prevalent within WatchKeeper design. Leveraging these systems eliminates the need to build new systems from scratch. However, if design flaws exist within these subsystems, a tendency may arise for WatchKeeper developers to fix existing issues within these systems, in turn, delaying WatchKeeper development. A thorough evaluation of these subsystems should be conducted to identify potential risks and requirements trade-offs.

IV. WATCHKEEPER ARCHITECTURE PROPOSAL

A. PROPOSED APPROACH

WatchKeeper documentation provides details surrounding development of the physical aspects of the Information Management System, the requirements necessary for delivering intended services, project management approaches, schedules, etc. The documentation, however, does not directly discuss processes, or issues surrounding semantics (such as commonly accepted terms for maritime missions), necessary to facilitate the effective use of information within the system. This may be a result of its initial design–having port partners VPN into the Coast Guard Data Network (CGDN) to access WatchKeeper capabilities. If this is the case, the development of a true information-sharing environment (based on SOA principles) requires an initiative that focuses on semantics for future versions of the system.

WatchKeeper should be built to facilitate the use of three basic categories of information—past, present, and future (or forecast). All three categories support a shared world model, which is critical for enabling "efficient thought" (Hayes-Roth, 2006). To support efficient thought, services are provided to facilitate "Superior Decision Loops" (Hayes-Roth, 2006). Components of the WatchKeeper framework act to provide a cycle of functions: (1) Observe, (2) Assess Situation, (3) Determine Desired Changes, (4) Generate Candidate Plans, (5) Project Likely Outcomes, (6) Select Best Alternative Plan, (7) Communicate and Implement Chosen Plan, and (8) Validate and Improve Model (nine functions of efficient thought). This approach can be used despite the current information-sharing model being proposed by WatchKeeper.

A picture of the past is necessary for a Command Duty Officer's (CDO's) initial observation and assessments when beginning his/her watch cycle; the history provides a context for the present and makes the present meaningful. In many cases, the CDO can be required to reference the past to provide information to customers outside of the command center. This picture of the past is supported by historical data managed by various sources. WatchKeeper provides services to access this information, and display it

in a meaningful way. Information accessed by "history" would be: recorded camera feeds, radio transmission, phone calls, SAR activities captured by R21 assets, sensor activities, vessel transit information (track data, etc.), operation summaries (within operational windows), critical message traffic, log entries, email, chat activities, notification transmissions, critical media reports, standing orders, and previous plan of the day. It is critical for the presentation of this material to be easily interpreted and accessed to avoid becoming a burden to the CDO. Authorized IOC participants should have a tailored perspective of this historical information–filtered/profiled to meet their specific requirements. The history should also provide a generic method and criteria for generating reports) that supports Freedom Of Information Act (FOIA) requests (Requirement).

The primary foundation for WatchKeeper's "present" capability is a "shared world model" among participating agencies, which is necessary to "…enable synchronized, coordinated, intelligent real-time decision-making and control" (Hayes-Roth, 2005). This shared world model can only realize a maximum level of efficiency if it is built upon a model-based communication network (MCN) that delivers information using specified models that feed each user's world model (Hayes-Roth, 2005). The IOC environment provides a perfect case for this type of communications model. A majority of operational scenarios, requiring data sharing between agencies, is unique and requires random connections with any number of independent agencies with their own information needs. The "essential nature" of IOC's is net-centric and collaborative–"continuously synchronized though distributed" (Hayes-Roth, 2005). Once communications have been initially established and synchronized, the WatchKeeper architecture–most specifically for the "present" capability–needs only to provide a means for getting valued information at the right time (VIRT)–a concept developed by Dr. Rick Hayes-Roth (Hayes-Roth, 2005). The present WatchKeeper design requires port partners and other participating agencies to log into the CGDN to contribute information to the shared world model. Continuous synchronization of thought becomes a challenge as VPN connectivity must be maintained.

SA, therefore, is the result of a conglomerate of users participating in a dynamically changing world model among participating IOC member systems. WatchKeeper would provide a means for initially establishing communications with partnering agencies, and providing them a model-based communications system that delivers valuable information when it is needed and filters less-important information according to user preferences–VIRT. In the case of the Sector Seattle CDO, he/she has been provided clear, understandable, information about missions, events, conditions, vulnerabilities, and can elect to receive only information that could potentially affect predicted outcomes, such as a sudden change in weather forecast or maritime traffic volume. VIRT makes the interpretation of critical information much easier–eliminating information overload.

The "forecast" capability rests upon a Model Based Communication Network (MCN) foundation. The future uses models provided by the MCN. A user selects the data most appropriate for his/her needs, and importance-level, thresholds for receiving this information. WatchKeeper would monitor for changes in this data that might affect operations, such as a significant weather change that may require the cancellation of a mission. It would notify the CDO if this type of change occurs, or has a higher likelihood of occurring. An example of future (or forecast) capability is the following. A CDO is expecting a joint boarding with CBP to take place six hours into the watch cycle. The operation requires two station boat assets. Three hours before the boarding, CBP inputs a change in plans–they are cancelling their boarding plans. WatchKeeper notifies the CDO that there is, now, an extra boat asset available for SAR, since the boarding party will not need two vessels to ferry personnel. The forecast capability provides CDOs with information that can affect future events, and which may not be readily apparent.

The fundamental consideration for developing a framework for WatchKeeper is that it must support the "Shared World Model" (Hayes-Roth, 2005), which requires the coordination of dynamic worlds. The core of this framework must support the interactions of VIRT components described in the "components" section of this document. To accomplish this, consider the theory of "Smart Push" to describe how components within VIRT should interact.

B. SMART PUSH

"Smart Push" utilizes Conditions of Interest (COI) to establish specific, user defined, conditions that maximize the efficiency and value of information delivered to users. By defining specific conditions up front, users can avoid the traditional information "glut" produced by traditional query methods. For an illustration of how important it is to avoid "glut," consider the following example. The CDO might make a Google query for current weather conditions in a particular region. This query would return too much information–mostly unnecessary. The CDO, in turn, must filter the majority of this information to find what is needed. This is an extremely inefficient and costly method for operators who need the most valuable information as quickly as possible.

The following diagram depicts "Smart Push"–a method of employing VIRT.

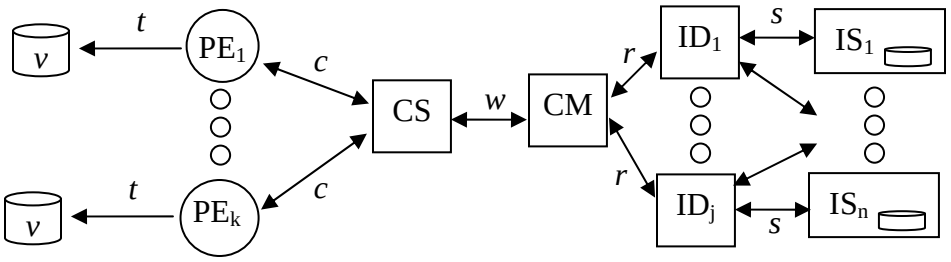

Figure 4. Smart Push (From: Hayes-Roth, 2006)

Explanation:

> The second model is very similar, and it too focuses on the same Processing Entities $PE_1,\ldots, PE_k$ that add value by accessing various information sources $IS_1,\ldots, IS_n$ to produce valued products labeled *v*. In this model, however, VIRT processes are at work, enabling each PE to inform the system about the COIs the system should continuously monitor. Each PE conveys its needs through interaction with a Condition Specifier (CS). The function *c* on the link between the PE and CS represents the transaction that yields information products consistent with PE's specification. Thus, for example, assume *c* gives a minimal amount of information at low cost, because the PE specifies precisely what type of events, which with it must be concerned.

The rest of the process works roughly as follows. Once a condition is specified, the CS conveys it to the Condition Monitor (CM) through *w*, and CM takes responsibility for monitoring it. The transaction *w* just passes back any new events matching the condition through CS and then through *c*. The Condition Monitor uses various Information Directories (ID_j) to understand what kinds of information are available and how to access them. Information Stores (IS_n) store, manage and access discrete bodies of information. The processes used by CM are labeled *r* and *s*, representing the transactions that seek and retrieve relevant information (Hayes-Roth, 2006).

C. FRAMEWORK CONSIDERATIONS

- "Smart Push" implemented to realize VIRT.
- The "world model" is developed and maintained within the Coast Guard Data Network.
- WatchKeeper data resources are distributed. Data derived from these sources feed the MCN and WatchKeeper information stores, which support the ever-changing "world model."
- The framework of this architecture was constructed under the assumption that a model-based communications network is available to provide services that correlate shared-world data. An assumption: the combined concepts of the "Information Discovery and Understanding Layer" and "Information Sharing, Processing, and Consolidation Layer" can provide an MCN capability using the Enterprise Service Bus, and other "Net-Centric" capabilities identified later in Figure 3.
- External participants should be able to access WatchKeeper and its services using their respective organization's resources through secure connections over the internet.
- Sensor devices are to be accessed through services provided by the Information sharing, Processing and Coordination layer.
- Plans, objectives, actions, assumptions, and justifications are entered into WatchKeeper by users and sensors, and made visible, and accessible or both to maintain the shared world model. Users select Conditions Of Interest (COI's) through the WatchKeeper interface. The MCN provides services to filter data according to COI's so that only relevant data is received (see component-based product-line architecture for VIRT, and Two Theories of Process Design for Information Superiority: Smart Pull vs. Smart Push) (Hayes-Roth, 2006).

- Store and forward operations are ongoing between local data stores, and remote WatchKeeper "Authoritative data" stores.
- Coast Guard and other participants, located within the IOC have access to Coast Guard Standard Workstation III interfaces to WatchKeeper and its services (circumstances permitting)

D. COMPONENTS

Most essential to the success of WatchKeeper is the support of changing world models to deliver a common, dynamic, shared world model.

The following components, logic, and methodologies, where developed by Dr. Rick Hayes-Roth, and published in his work: *Model-based Communication Networks and VIRT: Filtering Information by Value to Improve Collaborative Decision-Making,* for the 10th international Command and Control Research and Technology Symposium, 2005. These components would serve as the core innovation behind the WatchKeeper "Watch-standers" sub architecture proposed in this thesis. These components, and their associated logic, are not considered in present WatchKeeper architectural documents, and descriptions.

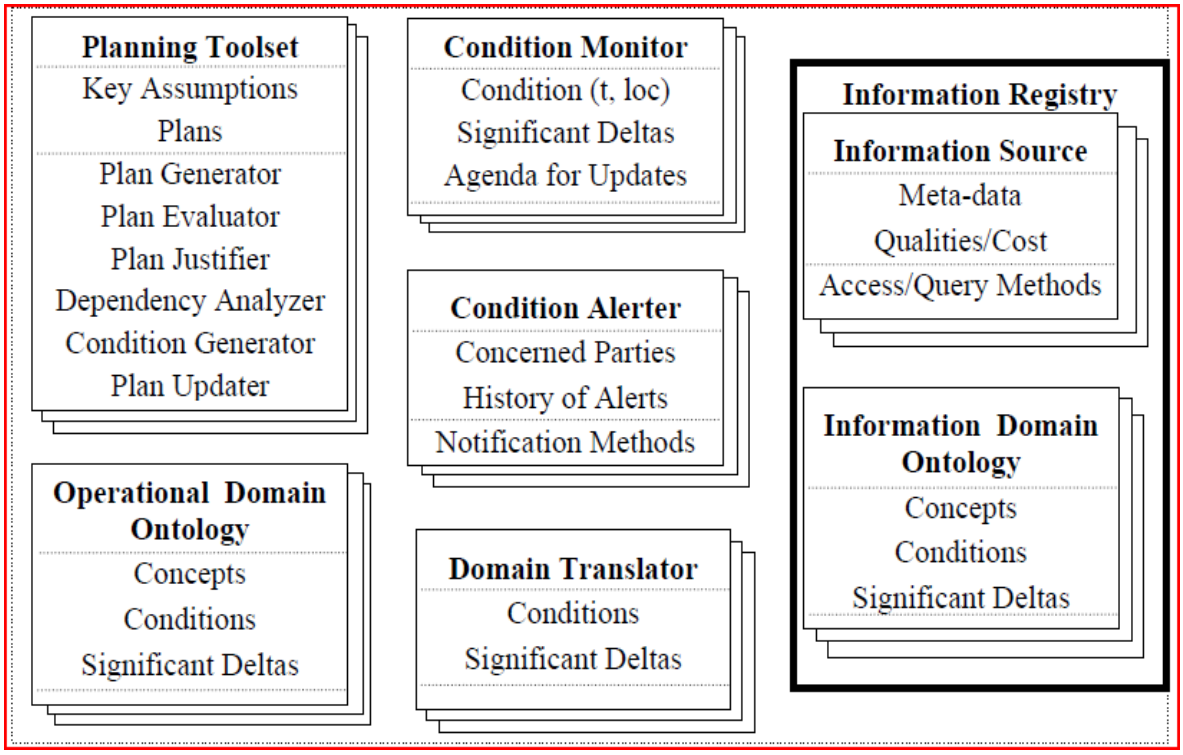

Figure 5. Component-based Product-line Architecture for VIRT (From: Hayes-Roth, 2006)

The following components would reside within the Enterprise Service Bus and Net-Centric Services domain of WatchKeeper.

- Planning Toolset (supported by CG planning tool, such as MHS-OPS, depicted in Figure 2)–which generates candidate plans, evaluates alternatives, and justifies the selections they make (p. 9).
- Condition Monitor–examines the value of the designated condition over appropriate time and space coordinates and records when significant changes in the value of the condition occur.
- Information Registry–facilitates the population of, and access to, Dynamic Situation Data (DSD)–variables, and encodings (such as AIS (WHAT DOES THIS ACRONYM STAND FOR-ADD TO ACRONYM LIST) or Blue force tracking (BFT) data). Meta-data describe this data for access by other components.
- Information Domain Ontology–specifies semantics of an information source, as when an attribute, such as "Foreign-Flagged vessel," as translated by 46 CFR 381 subpart 47.5, is explained as any vessel of foreign registry including vessels owned by U.S. citizens but registered in a nation other than the United States.

- Operational Domain Ontology–specifies the semantics of the participating planners and operators (usually artifacts of their respective agencies) (p. 10). For example, they may need to specify that "Random Boarding" means–to physically embark a vessel that **has not** been selected for boarding due to any suspect information or activity (*example only-may not reflect true specification of random boarding*).
- Domain Translator–"translates conditions and significant deltas, expressed in one ontology, into a different ontology." "… the Domain Translator relates concerns in the operational domain to data sources described in an Information Registry" (p. 10) Example: a CG boarding operations translator could translate current requirements, such as manning requirements, vessel asset requirements, time requirement, etc… into "resource gap," "no-go," "resource request," etc…
- ** Information Directory**–it is assumed that this component is to be available through WatchKeeper aggregate data services.

The following diagrams depict abstractions of essential hardware components, and abstractions of software components necessary to deliver, this proposed, WatchKeeper, functionality (proposed by CG C2CEN, 2008).

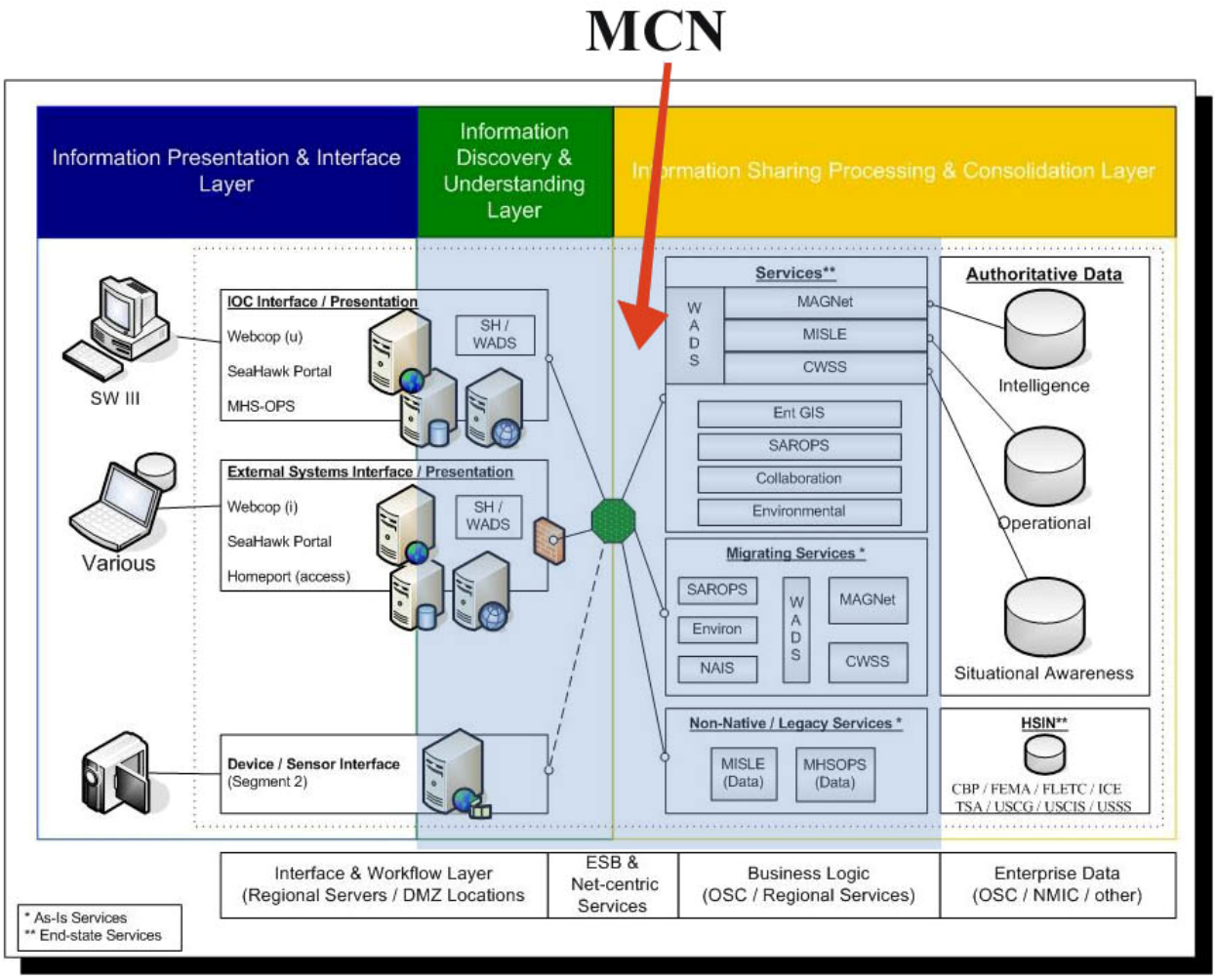

Figure 6. WatchKeeper (After: Detailed Design Document, 2008)

The following diagram depicts the logical location of VIRT components within WatchKeeper.

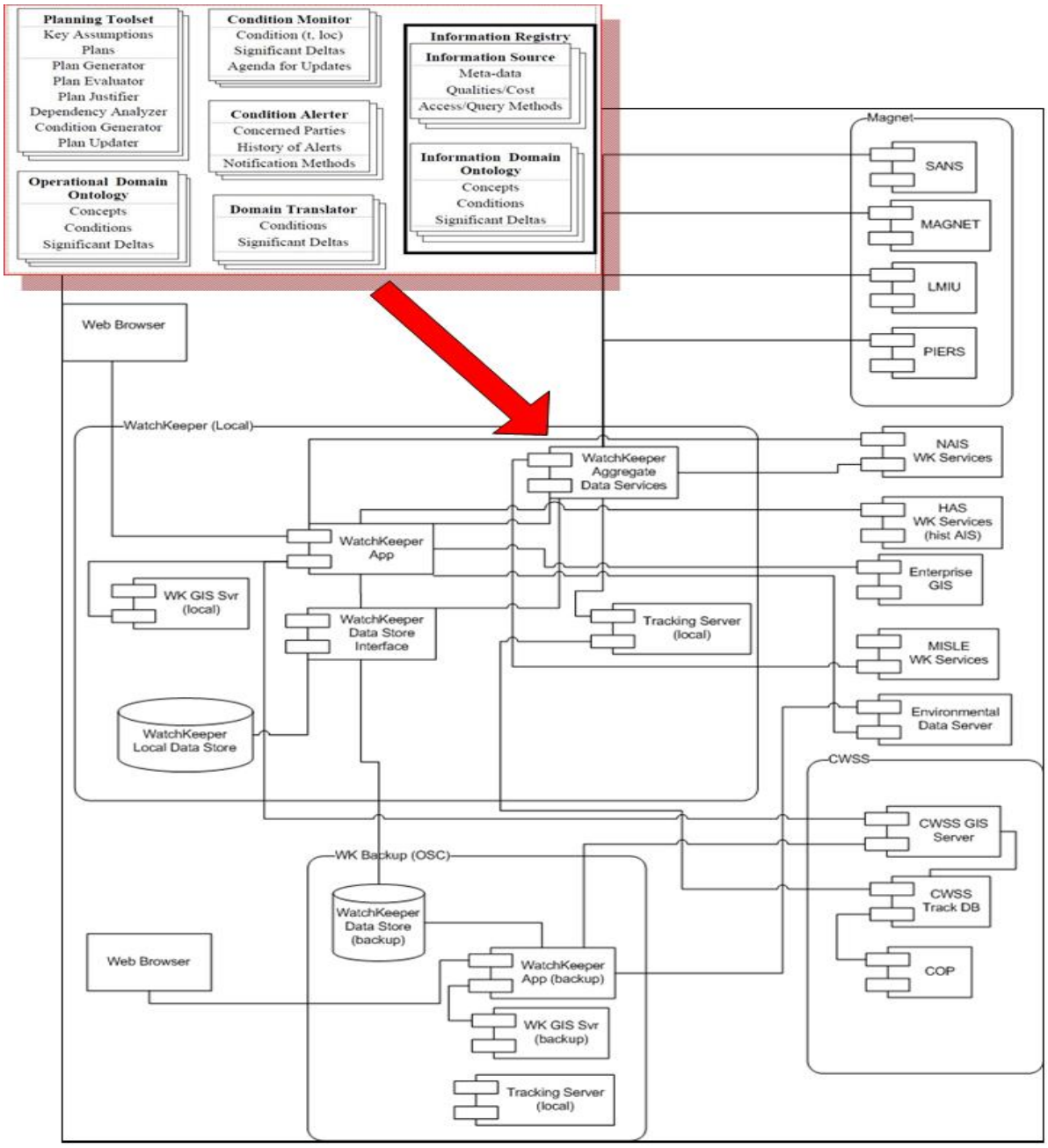

Figure 7. VIRT Components within WatchKeeper

E. FUNCTIONAL REQUIREMENTS

The following is a high-level, comprehensive, functional requirements list. The requirements listed below have been identified in the Coast Guard's C2CEN WatchKeeper Detailed Design document. They are further refined to meet the functional requirements of VIRT.

Support joint planning for vessel arrivals and security activities among key interagency partners. The Coast Guard is still working on identifying the consolidated planning tool, although the design document references MHS-OPS as the available solution. For the purpose of this thesis, it is assumed that a planning tool has been chosen.

- Assign resources to tasking; a requirement addressed by the selected, joint planning tool
- VIRT Functional Requirements
- Integrate activities that support execution of business rules, data consolidation, information sharing, and workflow using automation to the greatest extent feasible. (The primary necessity and chief technical challenge to this requirement is the development of VIRT components as previously described).
- Accept COI's
- Monitor conditions established by COI's–if information changes, and those changes are significant to affect assumptions about current or future concerns–Alert
- Seek and retrieve relevant information based on changes in conditions being monitored
- Alert
- Access data from disparate resources
- Coordinate MCN services, and WatchKeeper resources
- Compose and maintain a situation picture–result of "Smart Push" (This refers to the development of a "Shared World Model" as previously described).
- Filter data to provide only "valued information at the right time"–result of "Smart Push"
- Deliver predictions of the world model based on deltas in information, and operational ontologies able to deliver predictions by monitoring COI's.

F. PRIORITY REQUIREMENTS

Several quality attributes are applicable to WatchKeeper–Watch-standers sub-architecture. They include the following (some of which are listed in the Coast Guard's Operational Requirements Document (ORD): usability, modifiability, availability, ability to facilitate communication and coordination, ability to forecast issues, compatibility, and reusable artifact. This list is not all-inclusive. However, the VIRT method described by Dr. Hayes-Roth, being the single most important consideration for this architecture, has its own critical Quality Attributes ubiquitous in any collaborative, command and control (C2), operational environment. Therefore, the focus of this thesis is on two WatchKeeper, Quality Attributes critical to VIRT, efficiency and usability.

Efficiency refers to those qualities that enable efficient process to obtain VIRT, such as the ability to filter information based on value criteria, monitor for changes in shared world views, coordinate the shared world view, modify COI's, etc.

Usability refers to qualities that provide a logical, functional, visually appealing WatchKeeper interface. Providing VIRT capability requires that WatchKeeper provide an operating environment easy to use and delivers information in a meaningful way.

G. EXAMPLE QUALITY ATTRIBUTE SCENARIOS

Two scenarios were used as examples to describe further how key functionality of the architecture might be validated–specifically, to ensure functionality meets priority quality attributes associated with VIRT: Usability, Efficiency (Oros, 2005).

- Normal Operation–Monitoring maritime environment
- Target vessel selected for boarding is late

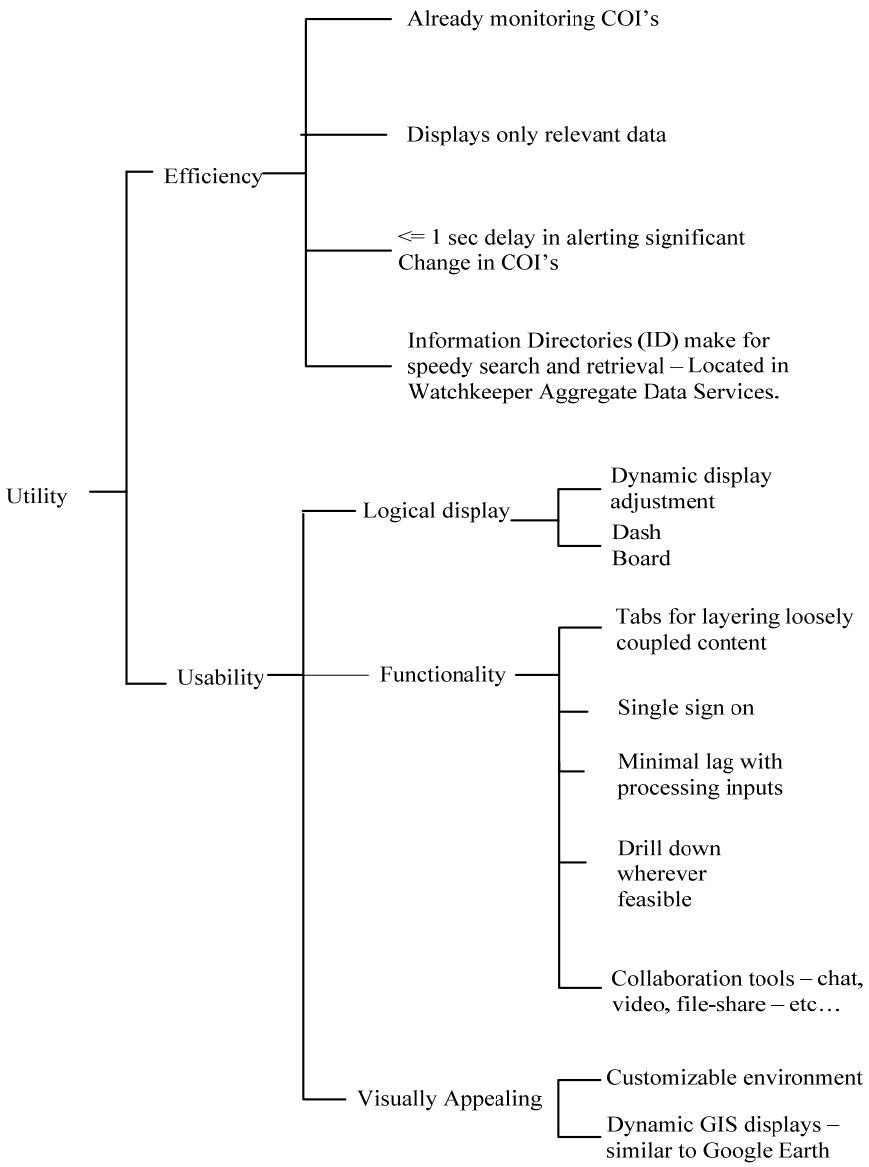

Figure 8. Normal Monitoring (1)

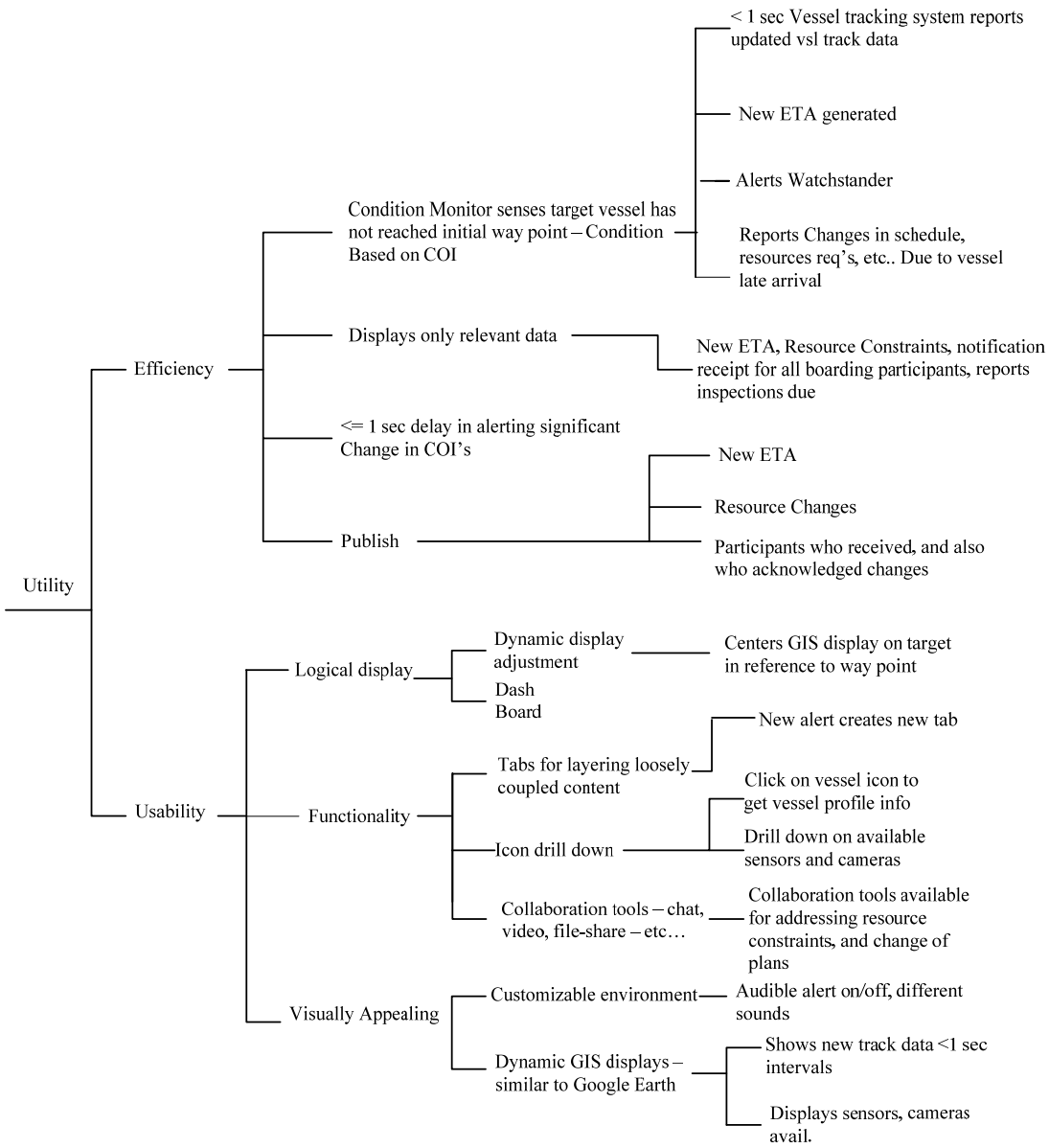

Figure 9. Target Vessel Selected for Boarding is Late (2)

H. ARCHITECTURE PROPOSAL RISKS

The following is a list of risks associated with this proposed architecture, and proposals to mitigate them. This list is not all inclusive.

- This proposal covers a very limited number of quality attributes scenarios to validate the architecture.
- A more in-depth validation of this proposal would require the development of many more scenarios specifically designed to test the architecture at different levels of activity, and coordination.

- This approach requires VIRT software components to be built. The value of success of WatchKeeper depends on the Coast Guard's acceptance of VIRT (or a similar model). The official design documents for WatchKeeper do not address any such model.
- Introduce WatchKeeper developers to this approach.
- Too watch-stander centric; Coast Guard watch-standers are not the only WatchKeeper participants.
- Further development of the WatchKeeper architecture needs to consider other agency views of the system.
- Presently, WatchKeeper is not being designed to allow port partners ubiquitous access to WatchKeeper functionality. This proposal may not work within the present WatchKeeper architecture.

I. ARCHITECTURE PROPOSAL CONCLUSIONS

WatchKeeper must provide the capability to see, understand, and share tactical information critical to security and interagency coordination. This explicitly identifies a need to share world views in an operational environment. World views are dynamic and content rich. Watch-standers and operators, tasked with seeing, understanding, and sharing information, can be quickly overcome by information "glut." "Glut" prevents them from working efficiently, and most effectively. Much of their time is spent filtering through or ignoring information in an attempt to gain awareness of the dynamic world unfolding around them. This can lead to gross inefficiencies and, in some cases, failure to identify critical information. The WatchKeeper architecture addresses this by utilizing a framework based on model-based communications networks and valued information at the right time. It employs components that make VIRT possible using a "smart push" approach. Furthermore, WatchKeeper must provide an interface that supports the seeing, understanding, and sharing critical information. Both having the ability to retrieve only valuable information efficiently and having a user-friendly interface (for receiving and providing information) are necessary for developing a useful, shared world model.

The success of WatchKeeper is dependent upon the acceptance of VIRT principles. In dynamic operating environments, where decisions need to be made quickly with a maximum amount of certainty, there is not time for filtering through large amounts of data.

This proposal redirects user requirements, defined by WatchKeeper design documents, by grouping them into time domains: past, present, and future. Focusing on past, present, and future time domains assists in mapping proposed WatchKeeper capabilities to core IOC business processes–in support of shared world models.

VIRT creates valuable and efficient relationships between organizations that share a world model. The framework and components of WatchKeeper have the potential for delivering truly superior decision loops by improving the quality of decisions, eliminating "glut," and increasing the timeliness of responses if VIRT principles are integrated into its design.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The Coast Guard WatchKeeper development project faces many challenges–short timelines for delivering capability, complex requirements, limited funds, and a host of other issues. Most importantly, today's port safety and security environments need the capabilities WatchKeeper proposes, such as common interfaces to existing IT resources for the maritime environment, shared awareness of safety and security activities among key maritime stakeholders, and methods for delivering value-added data transactions that enable shared awareness and coordinated maritime operations. Research suggests that the WatchKeeper development approach is reasonable considering the challenging environment, and present constraints within which it is being built. Much of the documentation surrounding its development is consistent concerning requirements, available resources, and scope; however, the project, as a whole, requires greater effort, much more time, and unprecedented support to deliver all the capability is proposes.

This research began by covering three critical components to planning and leveraging IT capabilities: Enterprise Architecture (EA), Software Architecture (SA), and Software Architecture Evaluation (SAE). None of these critical components was visibly present in the design documents surrounding WatchKeeper development.

EA provides a means for building strategies that align IT capabilities with core business processes.

> An enterprise architecture is a plan of record, a blue print of the permitted structure, arrangement, configuration, functional groupings/partitioning, interfaces, data, protocols, logical functionality, integration, technology, of IT resources needed to support a corporate or organizational business function or mission. (Minoli, 2008)

The Coast Guard is presently developing an EA, but according to a report written in 2009 from the Office of Inspector General, Department of Homeland Security, the Coast Guard EA does not demonstrate how all the Coast Guard's major information systems fit together, and the documentation that supports the EA is incomplete.

Developing a system of systems, such as WatchKeeper, in an environment where EA has not been fully implemented, creates difficulties for future systems and data integration. For example, documentation of the WatchKeeper framework and Components, as they relate to core business processes, are very difficult to develop and explain, given the complexity of existing data connections and future service related data connections. EA requires a thorough understanding of how these data connections and future service related data connections fit into the overarching architecture (EA). If present documentation does not consider future EA requirements, it may be very difficult to express how WatchKeeper supports core business processes, and how it meets standards set by DHS and Coast Guard EA policies. Developing WatchKeeper without understanding its relationship to greater Coast Guard information systems and business process is risky. The WatchKeeper project would benefit significantly from focusing its design and documentation efforts toward fulfilling standards and requirements of Coast Guard's proposed EA plan–although, by doing this, the project management risks increasing workloads and extending project timelines.

SA is a critical requirement similar to EA except that it focuses specifically on the architecture of software systems. Several software components exist within WatchKeeper; however, the architectures for these components are not represented in the WatchKeeper design documents. The risk in attaching components (in this case, software products) that do not have a formal software architecture is the behaviors of these components are hard to trace when combining them with new services that specifically support WatchKeeper. If software bugs exist in third-party components, a tendency may exist to make compromises in quality attributes to deliver WatchKeeper functionality. This may also lead WatchKeeper developers to fix problems that exist within third-party components–a costly and timely undertaking, which may cause significant delays in product delivery time and an increase in overall project cost overruns.

The WatchKeeper project should maintain a clear vision of how this system provides value to both the Coast Guard, and other IOC stakeholders. One objective that summarizes the majority of WatchKeeper's proposed capabilities is valuable information to the right person at the right time. A thorough SAE should provide enough information

for stakeholders and program managers to understand clearly how the software architecture fulfills this objective. Much of the design documents provided for this research define data connections, capabilities that exist, and how these capabilities are to merged to meet operational requirements.

Port partner agencies should be intimately involved in WatchKeeper development. Presently, there are no formal agreements between the Coast Guard and other WatchKeeper stakeholders establishing coordinated development of the WatchKeeper IMS. This situation presents the risk of delivered capabilities not meeting requirements of other WatchKeeper stakeholders. The success of WatchKeeper depends on stakeholder acceptance and use of the system.

Semantics of operational domains across partnering agencies can present design issues within WatchKeeper. Data, needing to be shared across multiple agencies, must use common semantics to ensure data integrity and common understanding. WatchKeeper design must consider semantics. Documentation available for this research did not reflect consideration for semantics.

Presently, the design for WatchKeeper relies on existing technological capabilities, such as vessel arrival information from various data sources. These data sources have been established by manually connecting to sources outside of the Coast Guard network (outside of WatchKeeper proposed data services). This may create complications in design considerations since these connections rely on systems outside of Coast Guard influence and control. For example, if errors in applications and data sources, that reside outside the Coast Guard network, begin to occur it would be difficult to resolve these errors. Such an effort would require a coordinated effort to fix such errors – this also presupposes the responsible organization would be concerned with fixing the errors. These data connections should be re-established by means of WatchKeeper services design principles. This would ensure that all data that supports WatchKeeper capabilities is accessed in a logical, consistent, and concise manor. By re-establishing these data connections through services (within the WatchKeeper IMS), documentation and design can be consistent throughout the overall design process–limiting the number of ad hoc connections and processes to establish functionality.

It is unclear if available funds for WatchKeeper development, totaling 9.1 million dollars, are solely designated for segment one capabilities. The amount of 9.1 million dollars seems a very small amount of capital investment considering the design challenges presented in this research. If this is the total amount of funds to deliver initial and future capabilities up through segment three, the Coast Guard risks running into high cost-overruns, and significant delays in delivering products. Benchmarking other similar on-going development processes, in either the public or government sectors, may provide WatchKeeper program managers visibility into costing methods, and cost predictions. By doing so, program managers may find approaches that help them gauge where the WatchKeeper project stands from a cost perspective.

The Coast Guard is relying heavily on existing system capabilities to deliver proposed WatchKeeper functionality. The ESB is one component of WatchKeeper that will help to merge the functionality of existing systems. However, it has not been developed. This ESB must be designed. Significant effort is required in the design and development of this ESB. Services from the host of applications supporting WatchKeeper needs to be integrated and managed by this service. Presently, the development of the ESB does not consider services outside the Coast Guard Data Network. Future development should consider how to implement services effectively from other partnering organizations to ensure WatchKeeper's use by agencies other than the Coast Guard.

B. RESEARCH QUESTIONS

This thesis was developed to address the following questions: (1) what are the significant challenges facing the Coast Guard in developing this IMS? (2) is the Coast Guard leveraging best-practices (as identified by research) to develop WatchKeeper? (3) what is the primary focus of the WatchKeeper development approach? and (4) how might the WatchKeeper development team ensure the right capabilities are delivered to their customers?

It is evident that the Coast Guard is attempting to apply best practices in the development of WatchKeeper; however, it is not readily apparent that any formal process exists to ensure these practices are priorities or that these practices yield value as depicted in literature. Three primary best practices should be integrated into the WatchKeeper development project: (1) Enterprise Architecture, (2) Software Architecture, and (3) Software Architecture Evaluation. Coordinating the application of these best practices ensures the objectives of WatchKeeper can be met while reducing the risks associated with this complex endeavor. EA can ensure WatchKeeper is developed in accordance with Coast Guard overarching IT strategies and core business processes. SA can provide meaningful and concrete contexts for business process owners to understand how WatchKeeper supports their operations better. SA can also provide differing levels of abstraction that enable clear understanding of how the WatchKeeper components fit together in a framework that delivers valuable capability to customers. SAE can be used primarily as a risk mitigating strategy to identify critical design decisions in early stages of WatchKeeper development. The focus of software evaluation is on scenario based analysis of quality attributes, which WatchKeeper designers should be addressing pre-deployment to identify design trade-offs, and potential design risks by using various means of testing and analysis, such as quality attribute scenarios. The architecture proposal section of this thesis provides an example of quality attribute scenarios.

VIRT is a concept developed by Dr. Rick Hayes-Roth, which focuses specifically on delivering valuable information when users need it most–particularly, in information-sharing environments that leverage disparate data sources across multiple organizations. VIRT methodologies can enhance WatchKeeper capabilities by eliminating "information glut" being experienced by today's Watch-standers. This thesis provides a scenario describing the information rich environment present in Coast Guard command centers today.

What is the primary focus of the WatchKeeper development approach? The primary focus of WatchKeeper development is on the Enterprise Service Bus (ESB). The proposed ESB manages the many services provided by the many systems supporting WatchKeeper capability. Primarily, the ESB provides a means of managing simple

message services between existing systems. The ESB then provides a means of coordinating this information in such a way as to be displayed using a single WatchKeeper interface. Today, the ESB is only concerned with systems owned and operated solely by the Coast Guard. Future renditions of the ESB should consider the integration of services from other partnering agencies–barring any security concerns that can prevent this from being achieved.

How might the WatchKeeper development team ensure the right capabilities are delivered to their customers? Most importantly, by applying the principles of EA, SA, SAE, and VIRT, the development team is sure to test the requirements gathered in early stages of WatchKeeper development. VIRT, in particular, places the capability defining what information is necessary in the hands of users, who can define what information is pertinent to them, when this information should be pulled, and how this information should be displayed. The design documents reflect a significant effort toward gathering user requirements; however, no specific, detailed descriptions (within the documentation provided) exist of how WatchKeeper can address these user requirements other than identifying existing systems that generally meet these requirements.

C. FUTURE RESEARCH

Although segment one of WatchKeeper development is well underway, the overall project is still in its infancy. The author believes the task at hand is much greater than the Coast Guard anticipated. The state in which the WatchKeeper project finds itself provides a wealth of research opportunities ranging from its alignment with the Coast Guard's future enterprise architecture to local IOC information system architectures.

Future research should seriously consider the impact of organization-wide enterprise architecture. Does the Coast Guard have a mature understanding of what enterprise architecture provides, or how to implement it? The federal government is driving EA–with the DoD's architectural framework being one of the larger initiatives. There is a race to overtake the quickly shrinking cycle of new technologies, and the growing cost and complexity of existing IT systems. The Coast Guard has not yet been able to provide a clear picture of its ever-growing IT portfolio (Office of Inspector

General, Department of Homeland Security, 2009). The organization must develop standards, procedures, and policies that facilitate strategic plans for future IT development, and help it manage its current capabilities. WatchKeeper is intended to have a 20-year life cycle. At some point, WatchKeeper needs to integrate its architecture with that of the overarching EA. What can be done in the early stages of its design to ensure its compliance with future EA policies? How does WatchKeeper map to Coast Guard core business practices? Is the current design flexible enough to fit the future needs of the Coast Guard?

As the design of WatchKeeper pushes ahead, a significant amount of data needs to be developed concerning the software architecture aspects of WatchKeeper. A thorough investigation of the Coast Guard's software development practices might serve to identify where the Coast Guard is succeeding and where the organization could leverage best practices to ensure quality products are being created. The latest Commandant Instruction concerning software development is outdated. It was written in 1996. Much has changed in the way of developing software. Service Oriented Architecture (SOA) is an example of such a change. More than ever before, organizations are finding innovative means for sharing information across traditional system boundaries. Present WatchKeeper design applies older, much less flexible techniques for achieving data sharing. How might the Coast Guard leverage new software development practices to ensure value software products are being delivered to both Coastguardsman and other partnering agencies?

Port partner buy-in is a crucial element to the success of both the WatchKeeper initiative and the Interagency Operation Center projects. Research might be conducted to discover methods for planning and implementing joint software development projects–focused specifically on information sharing. Future research might also consider investigating the organizational aspects of collaboration, which fuel interagency collaboration. WatchKeeper design documents do not address port partner user requirements, which could hamper the overall efforts to share information. Questions to

consider: (1) who does the Coast Guard need to share information with to achieve enhanced operational coordination? and (2) which agencies should be top priorities with respect to building information sharing capabilities?

LIST OF REFERENCES

Alberts, D. S., Garstka, J., & Stein, F. P. (1999). *Network centric warfare [electronic resource]: Developing and leveraging information superiority* (2nd, revised ed.). Washington, DC: National Defense University Press.

Assistant Commandant for Capability. USCG. (2009). *Operational requirements document, interagency operations centers, command 21* (I ed.). USCG HQ, Washington, D.C.: USCG.

Bass, L, Clements, P., & Kazman, R. (1998). *Software architecture in practice*. Reading, MA: Addison-Wesley.

Capra, F. (1996). *The web of life: A new scientific understanding of living systems* (1st ed.). New York: Anchor Books.

CG C2CEN. (2008). *Interagency operations center/command 21 (IOC/C21) WatchKeeper segment, Project Management Plan (PMP).* Unpublished manuscript.

CG C2CEN. (2008). WatchKeeper detailed design. Unpublished manuscript.

Clements, P., Kazman, R., & Klein, M. (2002). *Evaluating software architectures: Methods and case studies*. Boston: Addison-Wesley.

Dash, R. E., Creigh, R. H., & Naval Postgraduate School (U.S.). (2007). *Service oriented architecture for coast guard command and control* [electronic resource]. Naval Postgraduate School).

de Rosnay, J. (1979). *The macroscope: A new world scientific system* (1st ed.). New York: Harper & Row.

Department of Homeland Security. (2008). Department of Homeland Security information sharing strategy. *Washington, D.C., United States Department of Homeland Security*. Retrieved December 18, 2009, from: http://www.dhs.gov/

Department of Homeland Security. (2008). *Department of homeland security information sharing strategy*. Washington, DC: Department of Homeland Security.

Department of Homeland Security, Office of Inspector General. (2009). *Review of U.S. Coast Guard enterprise architecture implementation process*. Washington, DC: Department of Homeland Security OIG-09-93.

Gorton, I. (2006). *Essential software architecture*. Berlin; New York: Springer.

H.R. 4954: The SAFE Port Act: Full Hearing before the Committee on Homeland Security, House of Representatives, 109th Cong., 2d Sess. 84 (2007).

Hayes-Roth, F. (2005). Model-based communication networks and VIRT: Orders of magnitude better for information superiority. Monterey CA: Naval Postgraduate School.

Hayes-Roth, F. (2006). Two theories of process design for information superiority: smart pull vs. smart push. 2006 CCRTS, The State of the Art and the State of the Practice. Monterey CA: Naval Post Graduate School.

Hayes-Roth, F., Pullen, M. J., Blais, C., & Brutzman, D. (2008). *How to implement national information sharing strategy: Detailed elements of the evolutionary management approach required fields and groups: 050200–information science*. Monterey, CA: Naval Postgraduate School.

Hayes-Roth, R. (2006). Hyper-Beings: How intelligent organizations attain supremacy through information superiority. Monterey, CA: Booklocker.com, Incorporated.

Minoli, D. (2008). *Enterprise architecture A to Z [electronic resource] : Frameworks, business process modeling, SOA, and infrastructure technology*. Boca Raton: CRC Press.

Mintzberg, H. (1981). *Organization design : Fashion or fit?*. Boston, MA: Graduate School of Business Administration, Harvard University.

National Preparedness Guidelines, 1. (2007). Retrieved December 18, 2009, from http://www.fema.gov/pdf/government/npg.pdf

Office of Inspector General, Department of Homeland Security. (2009). *Review of U.S. Coast Guard enterprise architecture implementation process* (GAO report No. OIG-09-93). Washington, DC: Office of Inspector General, U.S. Department of Homeland Security. Retrieved from HSDL database.

Oros, C. (2004). Proposed Architecture for a Helicopter Information Awareness Module (I-AM), Naval Postgraduate School

Ortiz, S. (2007). Getting on board the enterprise service bus. *Computer*, *40*(4), 15–17. Retrieved from IEEE Xplore database.

Peterson, K. (2009). Innovation on R&D Earned Value IOC/C21 WatchKeeper System. Project Management Institute, Virtual Library.

Port of Long Beach. Questions & comments. Retrieved November 18, 2009, from http://www.polb.com/contact/qc.asp

Ross, J. W., Weill, P., & Robertson, D. (2006). *Enterprise architecture as strategy : Creating a foundation for business execution*. Boston, MA: Harvard Business School Press.

SAFE Port Act: Conference Report (to Accompany H.R. 4954). (2006).

Seifert, J. W., & Library of Congress. Congressional Research Service. (2006). *Federal enterprise architecture and e-government [electronic resource]: Issues for information technology management*. Washington, D.C: Congressional Research Service, Library of Congress.

Sturm, F. J. (2007). *Department of Homeland Security U. S. Coast Guard statement of Captain Francis J. Sturm on the Security and Accountability for Every Port Act before The House Committee on Homeland Security Subcommittee on Border, Maritime & Global Counterterrorism*. Washington, D.C.: Commandant, USCG.

United States Coast Guard. (1996). USCG Commandant Instruction M5234.4. Retrieved February 23, 2010, from http://www.uscg.mil

United States Coast Guard. (2008). USCG: Missions. Retrieved December, 21, 2009, from http://www.uscg.mil/top/missions/

United States, & White House Office. (2007). *National strategy for information sharing successes and challenges in improving terrorism-related information sharing*. Retrieved December 7, 2009, from http://www.whitehouse.gov/nsc/infosharing/index.html; Materials specified: Table of contents http://www.whitehouse.gov/nsc/infosharing/index.html http://purl.access.gpo.gov/GPO/LPS90310

United States. Congress. House. Committee on Government Reform. Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census. (2004). Federal enterprise architecture: A blueprint for improved federal IT investment management and cross-agency collaboration and information sharing: Hearing before the subcommittee on technology, information policy, intergovernmental relations, and the census of the committee on government reform, House of Representatives, 108th Cong., 2d sess., (2004). Washington: U.S. G.P.O.

United States. Congress. House. Committee on Homeland Security. (2007). H.R. 4954: The SAFE port act : Full hearing before the committee on homeland security, House of Representatives, 109th Cong/. 2d sess., (2006). Washington: U.S. G.P.O.

United States. Congress. House. Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. (2006). *A failure of initiative [electronic resource]: Final report of the select bipartisan committee to investigate the preparation for and response to hurricane Katrina*. Washington: U.S. G.P.O.

United States. Executive Office of the President. (2006). *The federal response to hurricane Katrina [electronic resource]: Lessons learned*. Washington: White House.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California