NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A FAULT MANAGEMENT SYSTEM (FMS)
ARCHITECTURE FOR THE NAVAL COMPUTER
AND TELECOMMUNICATIONS AREA MASTER
STATIONS (NCTAMS)

by

Kathleen M. Creighton

September 1997

Advisor: Carl R. Jones
Associate Advisor: William J. Haga

Approved for public release; distribution is unlimited.

DTIC QUALITY INSPECTED 3

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.		

AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1997	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE A Fault Management System (FMS) Architecture For The Naval Computer and Telecommunications Area Master Stations (NCTAMS)	5. FUNDING NUMBERS
6. AUTHOR(S) Creighton, Kathleen M.	
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)	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.	

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

The Joint Fleet Telecommunications Operations Center (JFTOC) acts, on behalf of the Naval Computer and Telecommunications Command, as the fleet's "one-stop shop" for information services. Effective fault management is vital to ensuring reliable network service. Currently, however, the JFTOC employs a Fault Management System (FMS) that consists primarily of manual processes and non-networked resources. Users require a system that provides a centralized and accessible source of near-real time fault management information.

This thesis uses the methodology of the Department of Defense (DoD) Technical Architecture Framework for Information Management (TAFIM). TAFIM outlines a structured approach for migrating legacy systems to a open systems, standards-based target architecture.

Through application of the TAFIM process, a target FMS architecture, termed HelpDesk On-Line Information System (HOLIS), is developed. HOLIS includes: the existing NCTAMS classified local area network and SIPRNet infrastructure; network operating system, office automation, e-mail and database software from the interim Navy Automated Information System Standards list; and commercial off-the-shelf help desk software. Four migration paths are outlined, and one is selected as the best option for moving from the baseline system to the target FMS.

14. SUBJECT TERMS Help Desk; Fault Management System; Network Management; Naval Computer and Telecommunications Command	15. NUMBER OF PAGES 193
	16. PRICE CODE

17. SECURITY CLASSI- FICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSI- FICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

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

DTIC QUALITY INSPECTED 8

i

A FAULT MANAGEMENT SYSTEM (FMS) ARCHITECTURE FOR THE NAVAL COMPUTER TELECOMMUNICATIONS AREA MASTER STATIONS (NCTAMS)

Kathleen M. Creighton
Lieutenant, U.S. Navy
B.B.A., University of Notre Dame, 1988

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1997

Author:　_____

Kathleen M. Creighton

Approved by:　_____

Carl R. Jones, Advisor

_____

William J. Haga, Associate Advisor

_____

Reuben Harris, Chairman
Department of Systems Management

iii

ABSTRACT

The Joint Fleet Telecommunications Operations Center (JFTOC) acts, on behalf of the Naval Computer and Telecommunications Command, as the fleet's "one-stop shop" for information services. Effective fault management is vital to ensuring reliable network service. Currently, however, the JFTOC employs a Fault Management System (FMS) that consists primarily of manual processes and non-networked resources. Users require a system that provides a centralized and accessible source of near-real time fault management information.

This thesis uses the methodology of the Department of Defense (DoD) Technical Architecture Framework for Information Management (TAFIM). TAFIM outlines a structured approach for migrating legacy systems to a open systems, standards-based target architecture.

Through application of the TAFIM process, a target FMS architecture, termed HelpDesk On-Line Information System (HOLIS), is developed. HOLIS includes: the existing NCTAMS classified local area network and SIPRNet infrastructure; network operating system, office automation, e-mail and database software from the interim Navy Automated Information System Standards list; and commercial off-the-shelf help desk software. Four migration paths are outlined, and one is selected as the best option for moving from the baseline system to the target FMS.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INDEX OF ACRONYMS

-A-

AIS	Automated Information System
ANCC	Automated Network Control Center
API	Application Programming Interface
AOR	Area of Responsibility
AR	Action Request
ASC	Automated Switching Center
ASCOMM	Anti-Submarine Warfare Support Communications
AUTODIN	Automatic Digital Information Network

-B-

BCS	Broadcast Control Station
BPR	Business Process Reengineering
BUPERS	Bureau of Naval Personnel

-C-

C4I	Command, Control, Communications, Computers and Intelligence
CASREP	Casualty Report
CIA	Communications Information Advisory
CIB	Communications Information Bulletin
CINCLANTFLT	Commander-in-Chief, Atlantic Fleet
CINCPACFLT	Commander-in-Chief, Pacific Fleet
CNMP	Corporate Network Management Structure
COMSPOT	Special Communications
COTS	Commercial Off The Shelf
CUDIX	Common User Digital Information Exchange Subsystem

-D-

DBA	Database Administrator
DBMS	Data Base Management System
DCS	Defense Communications System
DFD	Data Flow Diagram
DIICOE	Defense Information Infrastructure Common Operating Environment
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMS	Defense Messaging System
DNS	Domain Name Service
DOR	Detailed Outage Report
DSCS	Defense Satellite Communications System
DSR	Daily Summary Report
DTG	Date-Time-Group

-E-

EHF	Extra High Frequency
ETR	Estimated Time of Repair

-F-

FLTBCST	Fleet Broadcast
FLTCINC	Fleet Commander-in-Chief
FMC	Fleet Management Center
FMS	Fault Management System
FOTP	Fleet Operational Telecommunications Program
FSBS	Fixed Submarine Broadcast System
FTP	Fleet Telecommunications Procedure

-G-

GCCS	Global Command and Control System
GOSC	Global Operations Security Center
GUI	Graphical User Interface

-H-

HOLIS	Helpdesk On-Line System
HTML	Hyper Text Markup Language

-I-

IMSC	Integrated Management Support Center
INFOSEC	Information Security
IP	Internet Protocol
ISABPS	Integrated Submarine Automated Broadcast Processing System
ISO	International Standards Organization
IT	Information Technology
ITM	Information Technology Management
ITMRA	Information Technology Management Reform Act

-J-

JAWO	Joint Area Watch Officer
JDIICS-D	Joint Defense Information Infrastructure Control System - Deployed
JFTOC	Joint Fleet Technical Operations Center
JV 2010	Joint Vision 2010
JSEC	Joint Maritime System Engineering Center
JTA	Joint Technical Architecture
JWICS	Joint Worldwide Intelligence Communications System
JWO	Joint Watch Officer

-K-

-L-

LAN   Local Area Network
LCC   Local Control Center
LCPO   Leading Chief Petty Officer

-M-

MAN   Metropolitan Area Network
MDS   Message Dissemination Subsystem
MOE   Measure of Effectiveness
MOP   Measure of Performance
MPSO   Multi-processing Server Option
MTBF   Mean Time Between Failure
MTTR   Mean Time To Repair

-N-

NAVCOMPARS   Naval Communications Processing and Routing System
NAVCOMTELCOM Naval Computer and Telecommunications Command
NAVMASO   Navy Management Systems Support Office
NCTAMS EASTPAC Naval Computer and Telecommunications Area Master Station
                          Eastern Pacific
NCTC   Naval Computer and Telecommunications Command
NCTOC   Naval Computer and Telecommunications Operations Center
NCTS   Naval Computer Telecommunications Station
NIPRNet   Non-secure Internet Protocol Router Network
NMS   Network Management System
NOC   Network Operations Center
NOS   Network Operating System
Nownet   Navy Orderwire Network
NPV   Net Present Value
NSA   National Security Agency
NSWC   Naval Surface Warfare Center
NTCC   Naval Telecommunications Center
NTP   Naval Telecommunications Procedure

-O-

OSI   Open·System Interconnection

-P-

PC   Personal Computer
PCS   Personal Communications System
POC   Point Of Contact
POTS   Plain Old Telephone System

PRNOC	Pacific Region Network Operations Center
PWS	Planned Work System

-Q-

-R-

RADAY	Radio Day
R&D	Research and Development
RF	Radio Frequency
RFO	Reason For Outage

-S-

SATCOM	Satellite Communications Division
SBA	Standards-Based Architecture
SCI	Sensitive Compartmented Information
SDLC	Systems Development Life Cycle
SHF	Super High Frequency
SITREP	Situational Report
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SPECOMM	Special Communications

-T-

TACPLAN	Tactical Plan
TACMEMO	Tactical Memo
TAFIM	Technical Architecture Framework for Information Management
TS	Trouble Shooting
TT&C	Telemetry, Tracking, and Control

-U-

UARNOC	Unified Atlantic Region Network Operations Center

-V-

VIXS	Video Information Exchange System
VTC	Video Tele-Conference

-W-

WCF	Working Capitol Fund
WWW	World Wide Web

-X-

-Y-

-Z-

ACKNOWLEDGMENT

I. INTRODUCTION

A. BACKGROUND

It is just before dawn, and the radiomen on USS Blue Ridge, underway in the Eastern Pacific, are unable to activate the video teleconference circuit (VTC) for COMTHIRDFLT's morning meeting with his commanders ashore. After numerous unsuccessful attempts, the watch supervisor uses the ship's Secret Internet Protocol Router Network (SIPRNet) connectivity to access the Naval Computer and Telecommunications Area Master Station Eastern Pacific (NCTAMS EASTPAC) Joint Fleet Telecommunications Operations Center (JFTOC) homepage. Here, he finds the link to the Helpdesk On-Line Information System (HOLIS) and electronically fills out a trouble ticket reporting the problem symptoms and the actions taken to date. JFTOC personnel read the trouble ticket and immediately commence trouble shooting. As restoral efforts progress, Blue Ridge and PRNOC personnel log in for near real-time updates of troubleshooting events.

When the NCTAMS EASTPAC Commanding Officer (CO), Communications Officer (Commo) and other senior leaders arrive at work, they access HOLIS using their desktop PCs and review all events from the past 24 hours. Commo views the message traffic and reports about the Blue Ridge VTC outage with concern. After briefing her staff to give this outage particular attention, she leaves the building for a meeting down island. She returns two hours later to learn that the COMTHIRDFLT Commo, CDR Jones, is on the phone. While speaking to CDR Jones, she simultaneously brings up the Blue Ridge trouble ticket on her computer. She is able to quickly review all

troubleshooting actions that have taken place on Blue Ridge and at NCTAMS during the past few hours. She and CDR Jones discuss the actions that have been taken to date and make a joint entry into the trouble ticket directing additional actions. This entry is received by the JFTOC Joint Watch Officer (JWO) who takes immediate action. Within the hour, the fault is diagnosed and corrected.

The Fault Management System (FMS) described here does not yet exist. However, in order to meet the needs of the 21st century Navy, the JFTOC, the central point of network management in each Naval Computer and Telecommunications Command (NCTC) region, requires an effective FMS. An information system that provides troubleshooting, coordination, and fault resolution information to both providers and users of NCTC information services.

B. OBJECTIVE

The objective of this study is to develop a FMS Target Architecture and a migration path for achieving this goal state. This Target Architecture will improve the quality of NCTC information services by minimizing outage lengths; reducing time spent coordinating, documenting, and reporting troubleshooting and restoral efforts; and enabling performance trend analysis.

C. APPROACH

This study utilizes the Structured Technical Architecture Framework for Information Management (TAFIM) Process which is a variation of the model presented in the *DOD TAFIM. The DOD TAFIM* is an eight-volume document published by the Defense Information Systems Agency (DISA) Center for Standards. It defines an open

systems, standards-based architecture for DOD information systems. Volume 4, DOD
Standards-Based Architecture (SBA) Planning Process, outlines a methodology for
migrating legacy systems to target systems within the standards-based, *TAFIM*
architecture, Fault Management System (FMS) Architecture.

The SBA Planning Process was modified for student use by an NPS Information
Technology Management (ITM) Professor and termed the Structured TAFIM process.
Essentially, it adds one step (Step Two: Define System Problem) to emphasize the
importance of formally defining the system problem being addressed. Figure 1.1 shows
the Structured TAFIM Process. Table 1.1 provides the purpose of each step. [Ref. 21:pp.
1-3]
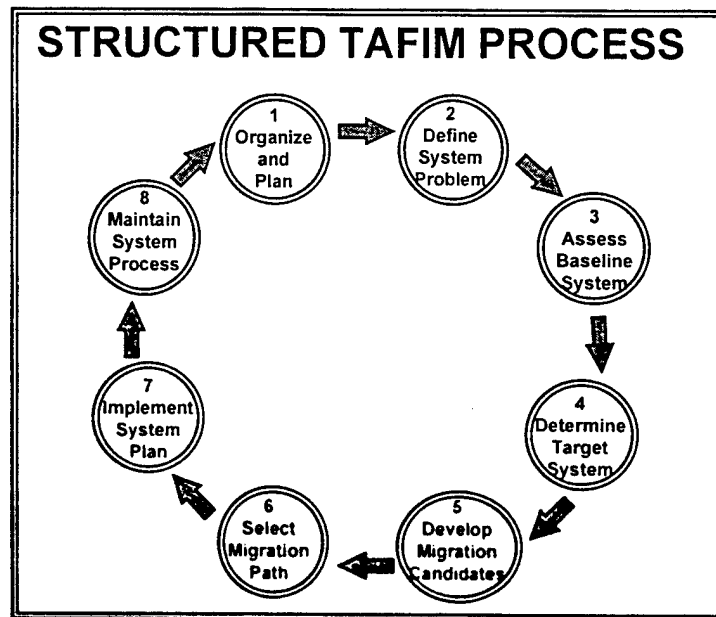
Figure 1.1. Structured TAFIM Process. [Ref. 21]

Table 1.1. Purpose of Structured TAFIM Process Steps [Ref. 4: pp. 1-4]

STEP	PURPOSE
Step 1	Develop an initial plan for engineering & managing a system over time.
Step 2	Structure the system problem so all participants in the Structured TAFIM Process clearly understand the problem being solved.
Step 3	Determine the character and state of the current system.
Step 4	Determine the character and state of the desired (goal) system.
Step 5	Develop several feasible paths, including plans, hardware, software, technical and managerial support, etc.
Step 6	Use criterion to select the best migration path, given the risk and uncertainty present.
Step 7	Implement the selected system migration path.
Step 8	Revise the migration path over time to adapt to the realties of technological change, available budgets, and new and different requirements.

This study presents a full illustration of steps one through six of the Structured TAFIM Process. Issues concerning implementation and maintenance, steps seven and eight, are incorporated into the previous steps, primarily the Chapter covering migration candidates development.

D. STUDY ORGANIZATION

While oriented towards the Navy telecommunications professional, this thesis provides ample background and description to enable understanding by anyone with a basic information technology background. A short description of each chapter of this thesis is provided below:

- Chapter II - Establishing the Problem Framework - Maps the role of the JFTOC to Joint and Navy C4I doctrine and policy, and discusses the JFTOC mission, functions, and organizational relationships.

- Chapter III - DEFINING THE SYSTEM PROBLEM - Provides a user assessment of the current system, overview of help desk technology, and formal problem statement.

- Chapter IV - ASSESSING THE BASELINE SYSTEM - Examines the policies, processes, outputs, and physical characteristics that define the baseline system.

- Chapter V - DETERMINING THE TARGET SYSTEM - Presents a goal architecture overview; identifies problem formulation constraints; examines target system processes and network architecture; and discusses the required capabilities of a help desk application in the target system.

- Chapter VI - DEVELOPING THE MIGRATION PATH CANDIDATES - Creates several feasible paths for moving from the baseline system to the target architecture; this includes timeline and cost breakdowns for each migration path option.

- Chapter VII - SELECTING A MIGRATION PATH - Reviews path selection criteria; calculates discounted present value of each migration path option; and explores the fiscal impact of phase scheduling.

- Chapter VIII - RECOMMENDATION AND CONCLUSIONS - Provides recommendations, areas requiring further study, and conclusions.

II. ESTABLISHING THE PROBLEM FRAMEWORK

A. INTRODUCTION

The role of the JFTOC continues to grow as telecommunications management evolves from the stovepipe, radio frequency (RF) links of the past to the fully integrated, wide-area tactical networks of the future. This chapter illustrates step one of the Structured TAFIM Process by establishing the framework within which the JFTOC's role is defined. Specifically, the relationship between JFTOC and Navy C4I doctrine is explored regarding the JFTOC's role in achieving the vision of NCTC, and in turn, the vision of the Navy. Finally, JFTOC's mission, functions, and organizational relationships are discussed.

B. DOCTRINE AND POLICY

1. Joint Pub 6-0

Joint Pub 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations articulates the C4 principles required to achieve "information superiority"; the key to the "full spectrum dominance" required by *Joint Vision 2010 (JV 2010)*. [Ref. 1] *Joint Pub 6-0* states, "The fundamental objective of C4 systems is to get the critical and relevant information to the right place in time to allow forces to seize on opportunity and meet the objectives across the range of military operations." [Ref. 2:p. 1-1] This statement makes it clear that time is a critical factor in achieving C4 system objectives.

2. Information for the 21st Century (IT-21)

IT-21 is a strategy for achieving the goals of *JV 2010*. It is a joint Commander-in-Chief, Pacific Fleet (CINCPACFLT)/Commander-in-Chief, Atlantic Fleet (CINCLANTFLT) initiative that addresses several critical, short-term requirements. Central among these requirements is the need to implement a network infrastructure at the local, metropolitan, and global levels to enable message communication between all U.S. Forces and allies upon the inactivation of the current DOD messaging system, Automatic Digital Information Network (AUTODIN), by December 1999. [Ref. 3]

IT-21, however, addresses more than just messaging, its architecture, infrastructure and applications will enable "voice, video, and data transmissions from a single desktop PC, allowing the warfighter to exchange information that is classified or unclassified, tactical or nontactical." [Ref. 4:p. 52] Defense Information System Network (DISN) Internet Protocol (IP) networks will be employed to form a wide-area, tactical network. These networks include: Non-secure Internet Protocol Router Network (NIPRNet) for Unclassified information; SIPRNet for Confidential and Secret information; and Joint Worldwide Intelligence Communications System (JWICS) for Sensitive Compartmented Information (SCI). [Ref. 5]

Using the guidance set forth in the *DOD Joint Technical Architecture (JTA)* and *Defense Information Infrastructure Common Operating Environment (DII COE)*, IT-21 establishes minimum Navy Automated Information System (AIS) standards. The policy requires replacement of all non-standard Network Operating System (NOS) and electronic mail (e-mail) products no later than December 1999. Tables 2.1, 2.2, 2.3 and 2.4 display IT-21 minimum standards for *Networks* (includes: Local Area Network

(LAN) and Metropolitan Area Network (MAN), *Software, PC* and *File Servers*. The standards will be updated on a periodic basis based on technology changes and market trends. [Ref. 3] Standards include:

Table 2.1. IT-21 Minimum Network Standards. [Ref. 3]

NETWORK TYPE	STANDARDS
LAN: Afloat/Ashore	ATM Fiber Backbone, 100 Mbps (Fast Ethernet) to PC.
MAN	At least OC-3 (155 Mbps) capable.

Table 2.2. IT-21 Software Standards. [Ref. 3]

SOFTWARE TYPE	STANDARD
Server NOS	Microsoft (MS) NT Server 4.0
Workstation NOS	MS NT 4.0/5.0 Workstation
Office Automation	MS Office 97 Professional
E-mail	MS Exchange 5.0
Database	Relational database that supports WWW technology IAW DII COE (e.g., Oracle, Sybase, MS SQL Server, MS Access, etc.)

Table 2.3. IT-21 Workstation Standards. [Ref. 3]

COMPONENT	MINIMUM STANDARD
CPU	200 MHz Pentium Pro
RAM	64 MB EDO
Hard Drive	3.0 GB
NIC	CPU Compatible 100 Mbps Fast Ethernet
Mulit-Media Components	PCI Video with 2 MB RAM Sounblaster Compatible Audio Card Speakers

To achieve the goal of all commands being voice, video, and data transmission capable from/to a single, desktop PC, including e-mail exchange capabilities

for all ships by the year 2000, IT-21 establishes seven "absolute precepts". Figure 2.1 displays these principles.

Table 2.4. IT-21 Server Standards. [Ref. 3]

COMPONENT	NETWORK DIRECTORY SERVER STANDARDS	APPLICATION/FILE SERVER STANDARDS
CPU	Dual 166 MHz Pentium Pro	same
RAM	256 MB RAM 512K Secondary Cache	same
Hard Drives	(2) 4 GB SCSI	(5) 4 GB SCSI
Tape Drive	(1) 6 GB DAT	18 GB
Caching Controllers	2 DPT SCSI III (SmartCache 4)	same
PCI Video	PCI Video with 2MB RAM	same
NIC	(2) Cabletron CPU Compatible ATM NIC	same

SEVEN HABITS OF A HIGHLY EFFECTIVE FLEET INFORMATION TECHNOLOGY SYSTEM

- **If the boss doesn't use it, don't buy it.**
- **We must integrate the tactical and non-tactical.**
- **We must stay with industry.**
- **We must drive everything to a single PC.**
- **We must use commercial off-the-shelf products (COTS).**
- **We must have seamless transition from shore to sea.**
- **We cannot allow stovepipes to develop within our C^{4}I architecture.**

Figure 2.1. IT-21 Principles. [Ref. 4, pp. 52-53]

3.   **NCTC Vision for the 21st Century**

NCTC Vision for the 21st Century articulates the NAVCOMTELCOM strategic vision for the next century. In addition, it outlines a primary goal, five secondary goals, and numerous challenges that will be part of achieving each goal. Expanding the role of

the JFTOC is one of the challenges described. Figure 2.2 shows the JFTOC's relationship to the NCTC strategic vision. [Ref. 31:p. 2-4]

- **Vision:** "To be the primary manager of electronic information transfer for the warfighters of the sea services."

- **Primary Goal:** "To efficiently manage the flow of information so that the Fleet Commanders can unite the warfighters at sea and ashore into a cohesive and effective force."

- **Goal #5:** "We will meet the communication needs of the Fleet CINCs throughout the electromagnetic spectrum."

- **Challenge:** "*Expanding the role of the Joint Fleet Telecommunications Operations Center (JFTOC)* to include the full range of network operations management..."

Figure 2.2. Relationship of JFTOC to NCTC's Strategic Vision. [Ref. 31:p. 3-4]

4. NCTC CNMP

The *NCTC CNMP* contains the doctrine for implementing the command's strategic vision for the 21st century. It provides a Corporate Network Management Structure for the claimancy which includes headquarters, region, area, and base levels. The CNMP outlines the mission, objectives, functions, and responsibilties of each level. Figure 2.3 shows the Corporate Network Management Structure and the relationship among levels. [Ref. 29:p.7] At the Headquarters level, NAVCOMTELCOM in Washington D.C. is an echelon 2 command that reports directly to the Chief of Naval Operations. [Ref. 30:p. 3-1] Three NCTAMS located in Wahiawa, Hawaii; Norfolk, Virginia; and Naples, Italy, each with a JFTOC, provide network management at the Regional level. Within each region, areas are managed by Integrated Management Support Centers (IMSCs) (shown in Figure 2.4 as a single IMSC for simplification). An

Area IMSC corresponds to a current Naval Computer and Telecommunications Stations (NCTS). The bases or installations within the areas have IMSCs which provide telecommunications management services. [Ref. 29:pp. 20-21]
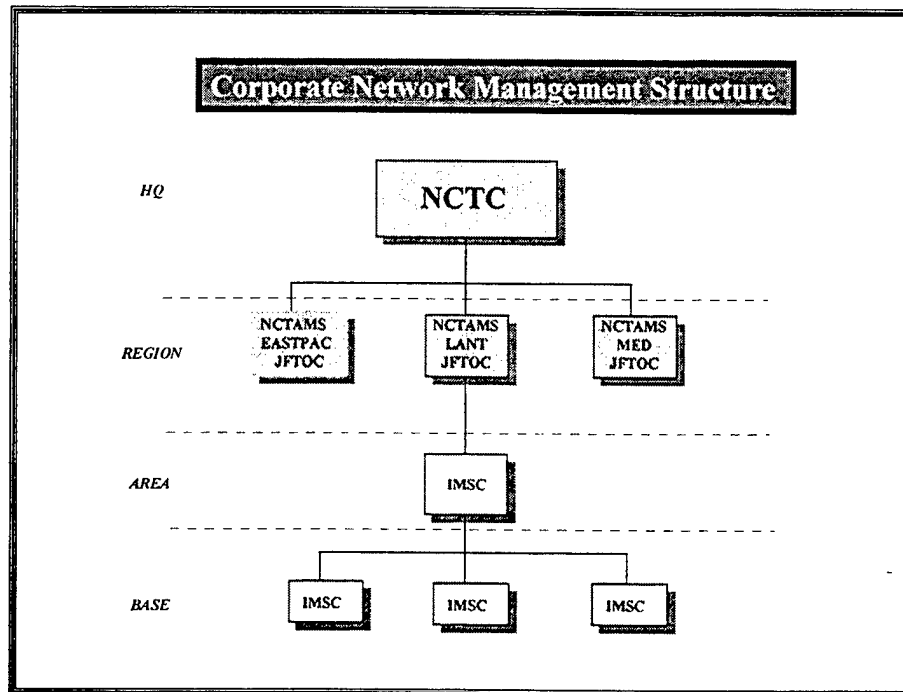
Figure 2.3. Corporate Network Management Structure. [Ref. 29:p.7]

5.   JFTOC Relationship to Doctrine and Policy

Figure 2.4 shows the relationship between the role of the JFTOC and Navy doctrine and policy just discussed. As the strategic vision of the Armed Forces, *JV 2010* describes the organization that DOD aspires to be in the near future, and *JP 6-0* provides doctrine based upon that vision. Although not discussed in detail in this study, the *JTA* and *DII COE* also identifies critical doctrine; common standards for IT and C4I systems. The goals of *JV 2010* are realized through enactment of stategies such as *IT-21*. Using the course charted by *JV 2010, NCTC Vision for the 21ˢᵗ Century* establishes a strategic vision for the NAVCOMTELCOM claimancy. The *CNMP*, as a doctrinal document,

12

plays a role analogous to *JP 6-0.* A strategy, central to achieving NCTC's vision, is, "Meeting the communication needs of the FLTCINCs throughout the electromagnetic spectrum." [Ref. 31:p. 3] The *CNMP* suggests that a task necessary for that strategy is to expand the network operations management services of JFTOC. [Ref. 31:p. 4]
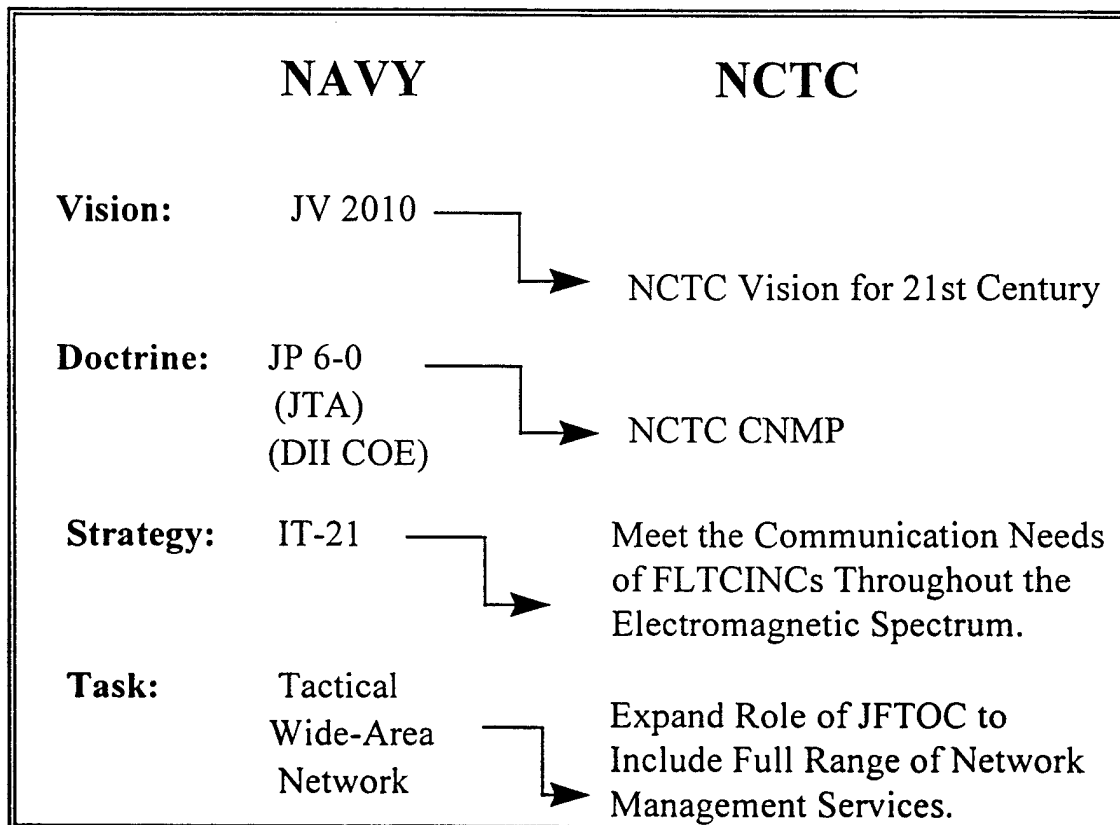
Figure 2.4. Relationship Between JFTOC and DOD Doctrine.

C. NCTAMS OVERVIEW

NAVCOMTELCOM is organized for operational and administrative functions into three regions: Pacific, Atlantic and Mediterranean. These regions correspond geographically with the areas of responsibility (AOR) of the fleet commanders. Each region is directed by a NCTAMS. [Ref. 31:p. 4-1] The two major telecommunications functions performed by a NCTAMS are: [Ref. 31:p. 6-1]

- Operational direction of region-wide telecommunications resources.

- Operational and maintenance of assigned telecommunications resources.

1. NCTAMS Organizational Relationships:

a. With NCTC

NCTAMS are Echelon 3 commands which report directly to NAVCOMTELCOM for the operation, maintenance, and administration of the telecommunications facilities within their regions. This region-wide operational authority is delegated by COMNAVCOMTELCOM to Commanding Officers (COs) of NCTAMS. [Ref. 30:p. 5-3]

b. With FLTCINCs

FLTCINCs exercise direction and control of direct fleet support telecommunications functions managed, performed, or facilitated by the NCTAMS. As such, NCTAMS COs are under the operational control of the FLTCINC. [Ref. 30:p. 5-3]

c. With NCTS

As delegated by COMNAVCOMTELCOM, each NCTAMS provides operational direction to the NCTSs within its region. [Ref. 30:p. 5-3] Type Commander authority for NCTSs, however, is is not delegated to the NCTAMS. [Ref. 30:p. 3-2]

2. NCTAMS Organizational Structure

Essentially, all three NCTAMS share a common organizational structure with Working Capital Fund (WCF) departments as the only variant. The typical NCTAMS departmental organization includes: [Ref. 37]

- N1: Management Resources

- N2: Base Level Communications

- N3: Communications Department

- N4: Facilities

- N5: Regional Plans

- N6: Electronic Maintenance

- N7: Supply and Fiscal

- N8/N9: Technical Services (WCF Department(s))

3. Communications Department Organizational Structure

The Communications Department, N3, is responsible for the operational direction of the Naval Computer Telecommunications System within that region. Responsibilities include: Planning and allocating telecommunications assets to meet requirements; correcting outages/trouble encountered in meeting requirements; and analyzing asset performance to improve efficiency and effectiveness. [Ref. 30:p. 6-1]

To meet these responsibilites, N3 is organized into divisions by functional task. Each of the three NCTAMS use a near-identical naming and numbering scheme for their N3 divisions. The organizational structure of NCTAMS EASTPAC Communications Department will be shown here, because it is the NCTAMS used for this research. It's divisions include: [Ref. 36]

- N3: Communications Officer

- N3A: Assistant Communications Officer

- N31: Fleet Message Processing Division

- N32: AUTODIN Automated Switching Center (ASC) Honolulu

- N33: Network Operations Center (NOC)

- N34: Techincal Control Division

- N35: JFTOC

- N36: Special Communications Office (SPECOMM)

- N37: SATCOMM Division

- N38: Communications Support Division

With the exception of N38, all NCTAMS N3 divisions are manned 24-hour per day, 365 day per year. The supervisor of each division watch section reports operationally to the JFTOC JWO. The JFTOC JWO is assisted by the Joint Area Watch Officer (JAWO) and the Operations Watch Supervisor. Equivalent N3 watchsections, with the exception of a JFTOC, are manned at all stations that report operationally to the NCTAMS. [Ref. 32]

4. JFTOC

a. *Mission*

JFTOC's mission is threefold: "(1) Allocation, management and operation of message processing; (2) Management of technical control functions, including Defense Communications System (DCS) assets; and (3) Allocation and management of regional assets in support of Joint and Fleet Commanders." [Ref. 29:p. 12] The JFTOC acts as the single point-of-contact (POC) for all C4I services for all afloat units and area shore commands in its region. It is essentially a "one-stop shop" for information services. [Ref. 29:p. 12] Additionally, the JFTOC Division, through its Tactical Plans (TacPlans) Officer/Chief, performs operational and exercise planning for the region. This function requires extensive coordination with FLTCINC staff and personnel at other NCTAMS. [Ref. 30:p. 6-3]

16

b. *Functions*

The JFTOC of the immediate future will be able to monitor and manage all of the following services: Defense Message System (DMS)-Local Control Center (LCC), Joint Maritime System Engineering Cener (JSEC), SATCOM-Fleet Management Center (FMC), IMSC, NOC/Domain Name Service (DNS), Information Security (INFOSEC), Automated Network Control Center (ANCC), Fleet Center and Fixed Submarine Broadcast System (FSBS). [Ref. 29:p. 14]

5.   NOC

The NOC Division, also known as the PRNOC, provides management services to fleet and shore users of classified and unclassified, IP, wide-area networks. They provide a full range of network management services including: configuration, fault, performance, and security management. Current functionality includes: immediate trouble call response, network monitoring, IP address registration and advertisement, DNS mail store-and-forward service, router port configuration for fleet and shore units, standardardized troubleshooting, and circuit restoral procedures, and World Wide Web (WWW) sites for network information. [Ref. 40]

D.   SUMMARY

The expanding role of the JFOC, to include a full complement of network management services, is central to the strategic plan of NCTC; goals which are derived directly from Navy C4I vision, doctrine, and strategy. As the one-stop shop for information services within each region, the JFTOC ensures the warfighter access to the right information, at the right time, in the right format.

III. DEFINING THE SYSTEM PROBLEM

A. INTRODUCTION

The second step of the Structured TAFIM process defines the system problem and lays the foundation for the remaining steps. Chapter II outlines the role of the JFTOC as the single POC in each region for integrated network management services. This chapter begins by narrowing the scope of this study to one aspect of this role: fault management. Interviews with users of the current FMS reveal its manual nature and their perceptions of an ideal system's capabilities. Next, COTS help desk technology is reviewed to determine its appropriateness for use in a target FMS design. The use of one help desk application at a major, commercial NOC is discussed to gain greater insight on its functionality and applicability. The chapter ends with the establishment of the problem statement and outline of the basic criterion and constraints that will be used to solve the problem.

B. FAULT MANAGEMENT

1. Network Management Overview

Several models exist to analyze and describe network management. One of the most commonly referenced is the Open System Interconnection (OSI) Functional network management model developed by the International Standards Organization (ISO). [Ref. 59:p. 41] It divides network management into the five areas shown in Figure 3.1 which include: fault/problem management, configuration/change management, performance/growth management, security/access management, and accounting/cost management. [Ref. 16:p. 4] Although not recognized as a major functional area, asset

management, the development and retrival of records on equipment, facilities or personnel, allows informed and efficient use of network assets. [Ref. 16:p. 9] This research will focus on fault management, because in the author's opinion, it consumes the majority of the JFTOC's time and effort.

2. Fault Management Overview

The primary objective of fault management is "to ensure maximum network availability". [Ref. 24:pp. 552-553] Six key phases, displayed in Figure 3.1, provide a simple description of this functional area. These include: event notification, logging, ticketing, tracking, isolation, and resolution. [Ref. 16:p. 11]
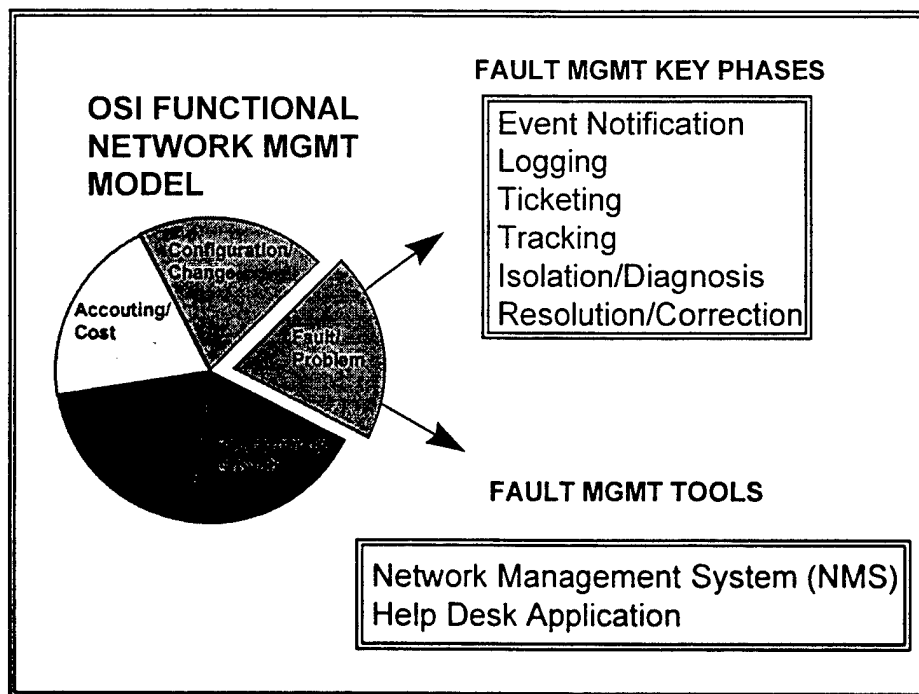
Figure 3.1. Fault Management as Part of the OSI Model. [Ref. 16:p. 11]

Fault management functions may be accomplished using a variety of COTS automated tools. As shown in Figure 3.1, a common fault management toolset consists of a NMS that uses Simple Network Management Protocol (SNMP) and a help desk

application that generates, tracks, and documents trouble tickets. Help Desk applications

will be explained in greater depth in the next section. Throughout this study, the terms

outage, trouble, problem, and fault will used interchangeable. Using a NMS and a help

desk application, fault management key events may be described as follows:

- Event Notification: The NMS polls the management agents in each network device to look for alarm conditions. Alarm conditions are generated when a management agent does not answer its poll (indicating device failure) or when the parameter returned exceeds a pre-set alarm threshold (indicating performance degradation). Selection of appropriate alarm thresholds is critical to effective fault management. [Ref. 24:p. 553] Most current NMS products perform alarm filtering and correlation to prevent the operator from being presented with multiple alarms for the same alarm condition (e.g., multiple devices reporting the same trunk outage). [Ref. 1]

- Logging/Ticketing: Most current NMS products have the ability to export alarms to help desk applications; this ability is referred to as automatic trouble ticket generation. When the alarm is received, a new trouble ticket is opened and information received from the NMS may allow some fields to be completed automatically. [Ref. 1] A trouble ticket acts as a consolidated record of all events that occur in the efforts to resolve the outage. Logging refers to recording trouble shooting information in the trouble ticket. [Ref. 16:p. 6]

- Tracking: Tracking is the process of checking the progress of internal and external personnel in their efforts to resolve the fault. Most current Help Desk applications perform event escalation to trigger an alarm that a trouble ticket has exceeded some pre-defined, time threshold. [Ref. 16:p. 6]

- Isolation: Isolation refers to identifying the cause of the fault. This may be accomplished using the NMS or with some other system diagnostic tool. Identification of the outage cause is recorded in the trouble ticket. [Ref.16:p. 6]

- Resolution: Finally, resolution of the abnormal condition is the last step in the fault management process, however, it often requires the performance of a configuration/change task (e.g., moving a circuit to a different satellite access due to interference on the original access). [Ref. 16:p. 6] Resolution information is recorded in the trouble ticket, which is then closed out.

C. NCTAMS EASTPAC USER ASSESSMENT

1. Interview Methodology

In-person, interviews were conducted with personnel who are either users of or technical experts regarding the current FMS. Interviews were approximately one hour in length and were taped using a micro-cassette recorder. Subjects were selected from the following categories: NCTAMS CO/XO, Department Head, Division Officer, Watch Supervisor or Technical Support; and a user at CINCPACFLT. The following staff members were interviewed: (Unless otherwise indicated, billets are located at NCTAMS EASTPAC.)

- Commanding Officer

- CINCPACFLT Communications Officer

- Communications Officer

- Assistant Communications Officer

- JFTOC Officer

- NOC Officer

- Tech Control Officer

- NOC Technical Director

- NOC Technical Support Contractor

- LAN Upgrade Project Manager

- JFTOC Traning Petty Officer

- NOC Training Petty Officer

The majority of the interview questions were open-ended in nature and were geared toward the interviewees' experience with the current system based on their job

responsibilites. Questions posed to personnel in senior leadership positions were specifically tailored to understand users' perception of: (1) the current system's shortcomings and (2) the capabilities of an ideal system. Questions asked of the remaining personnel, on the other hand, were designed to further understand the workflow model and business rules that underlie the current system. However, questions of both types were asked to all interviewees.

2. Problem Symptoms

Figure 2.2 displays a summary of responses to questions about the current systems' shortcomings. For ease of reading, replies are divided into six categories: Information Duplication, Manual Report Generation, Dated (Non-Timely) Information, Manual Information Capture, Information Stovepipes Vice Consolidated Data Stores and Manual Information Query. Without describing the details of the current system here, one gains a sense of its essentially manual nature.

3. System Wish List

Figure 2.3 displays a summary of responses to questions about an the capabilities of an ideal system. Replies are divided into eight categories: Automatic Report Generation, Near-Real Time Information, Automatic Information Capture, Consolidated Data Store, Automatic Information Query, Information Views, Information Exchange/Communication, and Other.

PROBLEM SYMPTOMS

Information Duplication:

• Recording the same information in station logs, SITREPs, COMSPOTs and e-mail is frustrating for watch standers.

• Reading the same information in station logs, SITREPs, COMSPOTs and e-mail makes tracking an outage cumbersome for managers.

Manual Report Generation:

• The summary of outages portion of the DSR must be written by the JFTOC Watch Officer each day using the information from station logs, SITREPs and COMSPOTs.

• To generate a Detailed Outage Report (DOR), NCTAMS personnel must extract information from station logs, SITREPs, COMSPOTs and DSRs.

• Tracking and updating SITREPs is a manual process performed using a log book. Updates are directed by JFTOC when a SITREP exceeds its estimated time of repair (ETR) or when significant new information is obtained.

Dated (Non-Timely) Information:

• DSR provides a snap-shot of the troubleshooting and restoral status at the time it was written; it does not provide a current situational status.

• Lack of near real-time outage information during troubleshooting raises frustration levels and can lead to "finger-pointing" between NCTAMS and afloat units.

• NCTAMS and afloat customers often perceive a lack of urgency on the others' part due to a lack of near real-time information.

Manual Information Capture:

• Troubleshooting coordination done verbally or via orderwire often results in lost information.

• Primary exchange of outage troubleshooting and restoral status internal to NCTAMS occurs verbally.

• A large percentage of the information about outages is received on paper. Information on paper gets lost and must be typed into the station log.

• Watch standers find it cumbersome to record troubleshooting steps in the log as they occur. Instead, they write down key events and go back later to type them in.

Information Stovepipes vice Consolidated Data Stores:

• COMSPOTs are difficult to track, because answers and replies do not directly follow each other when message traffic is sorted by date-time-group (DTG).

• JFTOC must query NCTAMS divisions or customers for latest status on outages.

• Divisions troubleshooting an outage have access to neither JFTOC's nor each others' station log; all station logs are text files located on stand-alone PCs.

• NCTAMS must maintain numerous historical files of outage information, including: station logs, SITREPs, COMSPOTs, As-occurring SITREPs and orderwire files.

• Station logs entries are made by DTG; they are not grouped by outage.

Manual Information Query:

• COMSPOTs do not contain enough details of the troubleshooting actions taken to resolve the outage.

• No automated method exists of retrieving outage information by circuit, time period or reason for outage; automated statistical analysis is, therefore, impossible.

• Remaining updated on the status of outages consumes a significant portion of a manager's day.

• Briefing managers on the status of outages consumes a significant portion of a JFTOC Watch Officer's day.

Figure 3.2. Problem Symptoms.

24

SYSTEM CAPABILITIES WISH LIST

Automatic Report Generation:
- Compose DSR and COMSPOT replies from information in the database.
- Generate the DSR automatically.

Automatic Information Capture:
- Enter data with input device that does not require typing.

Consolidated Data Store:
- Serve as a central repository of all information that was gathered and exchanged between NCTAMS and customer during an outage.
- Incorporate all the information from COMSPOTs and SHF/EHF Quick Look Messages into one data source.
- Create one record of an outage available on a near-real time basis to all departmental personnel.
- Compile one log of troubleshooting actions for all divisions.
- Record performance of watch duty functions, such as performance of proper watch relief procedures, in same data source as outages.

Automatic Information Query:
- Compare scheduled (maintenance) outages against unscheduled outages.
- Ability to go to a "home page" and find the status of certain CASREPs.
- Provide performance trend information on communications services provided.
- Query a database about similar outages to see troubleshooting step that resolved outage.

Unique Information Views:
- Display graphic representations of outage information by circuit, RFO and time period to allow correlation between a type of outage and some other factor.
- Provide Operations Department managers with the same near-real time information as the JFTOC Watch Officer.
- Provide an executive summary level view of "high priority" outages to operational commanders.
- Make troubleshooting information available to units that want it vice all units, all the time.

Information Exchange/Communication:
- Access outage information from the users' desktop/office PC.
- Keep customers informed of outage resolution progress and how their outage compares in priority to others.
- Provide a means for an afloat customer to communicate the results of troubleshooting actions more quickly and capture that information for future analysis.
- Provide a method of communicating within the department about outages.
- Provide an incentive for more "teamwork" and less "finger-pointing" between NCTAMS and afloat units.
- Show customers that NCTAMS is performing systematic troubleshooting.
- Exchange information between the NCTAMS, especially the Network Operations Centers NOCs.
- Conduct better turnovers between watch sections and NCTAMS in the event of responsibility sharing.

Other:
- Run in a Windows environment.
- Control access privileges to data by user.

Figure 3.3. System Capabilities Wish List.

25

D. HELP DESK TECHNOLOGY REVIEW

Help desk software was introduced above, as a component of a FMS that performs trouble ticket functions. In this section, the term "help desk" will be defined, help desk software will be described and the use of help desk software at a commercial teleccommunications facility will be outlined.

1. Help Desk Definition

Help desks have traditionally been associated with end user support, but their role continues to evolve with the expansion of network computing. [Ref. 61] Help desks may be considered internal or external. Internal help desks address IT problems of employees within an organization. The organization need not be limited to a single building, but may in fact, be nationally or globally distributed, as long as they remain within a single corporate structure. External help desks aid customers with IT problems concerning products purchased from that organization or, in the case of an outsourced help desk, a third party. [Ref. 27:p.5] Examples of this type of help desk abound in the form of toll-free customer service numbers. In the author's opinion, the functions performed by a JFTOC more closely resemble those of an internal help desk than an external one. Certainly, however, the JFTOC's customers, primarily ships, are more mobile and geographically disbursed than those of most internal help desks.

2. Help Desk Software

a. General Description

Help desk software may be described as customized database applications that provide for storage and retrival of information on customers/employees, trouble

reports made to an organization's support center, and some means of locating information to aid support personnel in resolving reported problems. [Ref. 57:p.17]

Help desk software functionality has evolved rapidly in recent years. No longer used solely for tracking trouble tickets, help desk applications are converging with desktop, network, and systems management products, as well as, software used to track sales and marketing operations. In addition, help desk products integrate with other software, such as e-mail applications, report writers, and NMS platforms, to achieve even greater functionality. [Ref. 58:p. 52] The term "consolidated service desk" is used to describe software that can perform "asset/change management, external customer support, defect management, and product management." [Ref. 60:p. 30]

b. Market Overview

The number of vendors offering products with reported help desk functionality decreased from approximately 175 in February 1995 [Ref. 28:p. 35] to just under 100 in January 1997. [Ref. 14:p. 52]. Some analysts attribute this decrease to the research and development (R&D) resources needed to achieve the greater functionality and integration capabilities discussed above. [Ref. 58:p. 52] There is currently no clear market leader [Ref. 14:p. 52], but based on the author's research, there are a group of approximately 10-15 help desk products that are frequently referenced as top performers in IT trade publications.

Meanwhile, to describe help desk sales as "growing", would be a serious understatement. According to industry analysts, the total market grew from $160 million in 1995 to $500 million in 1996 [Ref. 14:p. 35] and is expected to reach $1.8 billion by 2000. [Ref. 28:p. 52] Additionally, more than 50 percent of Fortune 1000 companies

indicate that they will replace their help desk systems by 2000. [Ref. 28:p. 51]   These

replacements are reportedly to take advantage of the "substantial competitive advantage"

that newer systems will offer. [Ref. 55:p. 86]

c.   Functionality

Figure 3.4 provides a list of help desk application critical features.

Functionality is divided into six categories: platform/operating system/database support,

integration, external platform functionality, internal platform functionality, problem

management capabilities, and product architecture.

d.   Industry Trends

Three industry trends are important to note:

- Client/Server Environment: The majority of help desk applications run in a client/server environment. Client machines generally hold the user interface while the server holds the application logic and DBMS. Some major vendors offer a three-tiered client/server approach where the application logic and DBMS are placed on seperate servers. [Ref. 28:p. 36] Three-tiered client/server systems are theoretically more scalable, robust and flexible. As a percentage of all client/server applications, three-tiered products are projected to grow from five percent in 1995 to 33 percent in 1998. [Ref. 38:p. 19]

- Open Architecture: There is a general industry trend toward an open architecture which allows interface between the help desk software and a variety of third party applications including: database management systems (from vendors such as Oracle Corp., Sybase Inc. and Microsoft Corp.), report writers and document managment systems. [Ref. 28:p. 36] Other interfaceable products include: NMS platforms, telephony tools, paging software, knowledge databases, and asset/inventory management applications. [Ref. 49]

- Internet Access: Many major help desk vendors have added Internet links to their products to allow customers to log problems, schedule service calls or download information about problems or products. [Ref. 54] Vendors offer a separate Web server package that provides access to their main help desk application using a Web browser such as Nestscape Navigator or Microsoft Internet Explorer. Customers use their browser to enter trouble tickets or to check the status of trouble tickets that remain open. [Ref. 45]

HELP DESK SOFTWARE FUNCTIONALITY

- **Platform/Operating System/Database Support**
  - Platform (e.g.. HP, Sun, PC Compatibles)
  - Operating System (e.g.. HP-UX, Solaris, MS NT)
  - Database (e.g.. Sybase, Oracle, MS SQL)
- **Integration of Third Party Applications (e.g..)**
  - Database Management Systems (DBMS)
  - NMSs
  - E-mail/Telephony/Paging
- **External Platform Functionality**
  - Reporting Tools
  - Ease of Installation & Customization
  - Development Tool Kits
- **Internal Platform Functionality**
  - Graphical User Interface (GUI)
  - Expert Systems/Automated Problem-Resolution
  - Security/Backup
- **Problem Management Capabilities**
  - Sorting
  - Call and Problem Management
  - Remote Problem Management
- **Product Architecture**
  - Product/Client/Database Architecture
  - Application Scalability

Figure 3.4. Help Desk Functionality. [Ref. 15:pp. 58-59]

e.   *Additional Help Desk Resources*

In the author's opinion, the *Microsoft Sourcebook for the Help Desk,*

Second Edition provides the most comprehensive anthology of help desk resources.

These include: web sites, books, publications, and organizations, that provide additional

information about help desk operations, software (including: functionality, vendors, products and prices), tools, consultants, and outsourcers.

f. *Example of Help Desk Software Use: Pacific Bell Mobile Services*

Information was provided by Steve Curley, NOC Manager of Pacific Bell (PacBell) Mobile Services located in Pleasanton, California. PacBell Mobile Services operates a digital Personal Communications System (PCS) network in California and Nevada. The network is divided into four regions: Bay Area, Los Angeles, Sacramento/Nothern Nevada and San Diego/Southern Nevada. [Ref. 39] PacBell Mobile Services began operation in early 1996. Projections place the subscriber rate at 330 thousand subscribers at the end of 1997 with growth to one million within three years. [Ref. 6]

The role of the NOC, as a 24-hour operations facility, includes alarm surveillance and fault investigation/administration, real-time traffic monitoring, planned work administration, integration of new sites/equipment, customer related fault investigations, network security investigations, change management controls, liaison with all third party agencies, (e.g., a utility company) and first line support. The NOC monitors network elements to the level of the radio transceiver that broadcasts the signal in each cell. The role of the NOC does not include customer interaction; customer service is a function of another work center called the Customer Care Organization. [Ref. 39]

PacBell uses seven applications to perform the different aspects of network management. At the time of this interview, the NOC is selecting a NMS to integrate these seven programs. Figure 3.5 shows the planned configuration. The

remainder of this discussion will focus on the help desk application that PacBell uses for its FMS: the Remedy Action Request (AR) System. [Ref. 39] Remedy AR System is also used for the Planned Work System (PWS), but the PWS is not an integral part of this discussion.
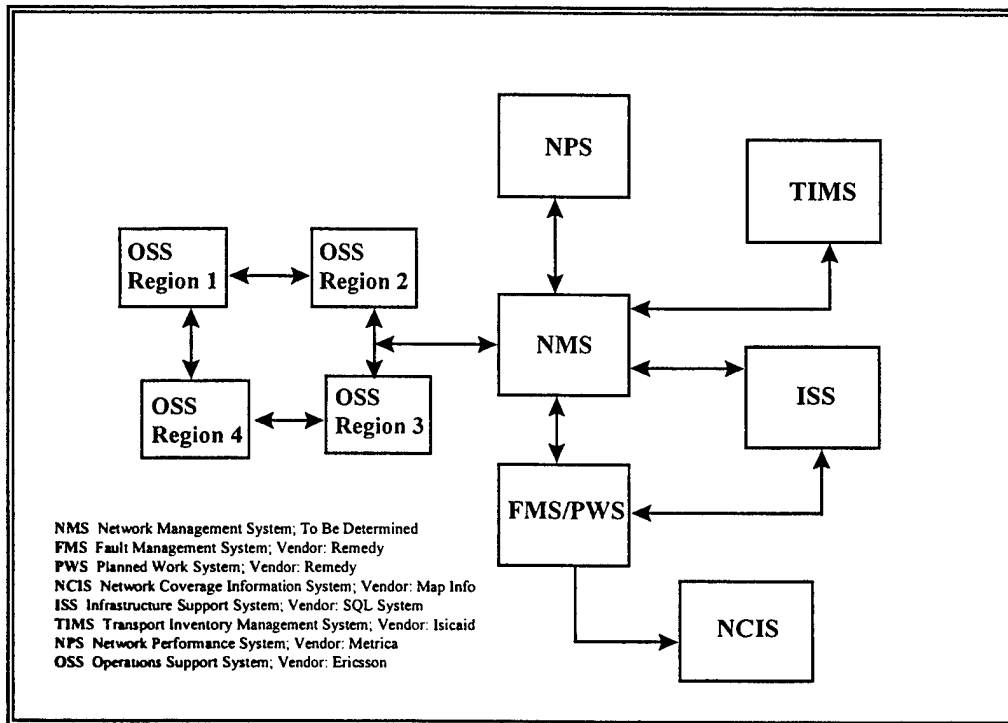
Figure 3.5. PacBell Mobile Services Planned Management Configuration. [Ref. 39]

The AR System plays a critical role in the operation of both the NOC and Customer Care Organization. The NOC uses the software to create trouble tickets, assign technicians and track problem resolution. The Customer Care Organization uses it to provide customers with the status of outages in their coverage areas; showing customers that PacBell is taking action to resolve the problem before the customer reports it. Table 3.1 provides summary of the fault management workflow model and business rules that are incorporated into the AR System. Automatic trouble ticket generation, ticket

categorization by severity, event escalation and remote access capability are important

AR System features.

Table 3.1. Fault Management Workflow and Business Rules in Remedy AR System. [Ref. 6]

FAULT MANAGEMENT STEPS	BUSINESS RULES
Remedy receives fault information from NMS.	Unique outage identifier is assigned.
Remedy generates trouble ticket.	Only one trouble ticket is allowed per identifier.
NOC assigns technician to trouble ticket.	Technician assignment is based on number and severity of tickets already assigned.
Remedy pages technician (using paging software).	Technician receives element affected, problem description and phone number to answer the page.
Techician acknowledges the page by calling phone number tied into Remedy.	Pages technician's supervisor if page is not answered within 10 minutes. Changes ticket status.
Technician logs into Remedy using laptop and wireless phone.	Changes ticket status and tracks time to drive to site.
Technician estimates if time to repair will exceed four hours (standard restoral time for outages that affect customers).	If repair estimation not made within two hours, Remedy pages technician's supervisor.
Technician turns outage over to supervisor to determine restoral time if outage will exceed four hours.	Estimation is based upon supervisor's judgement.

PacBell has approximately 200 AR System users. This application allows

assignment of read/write permissions down to the individual user level. PacBell manages

read/write permissions using the following business rules: trouble tickets may only be

assigned to regional field technicians or engineering personnel; the assigned person is the

only one given write permission; but all other AR System users have read permission to

all trouble tickets. AR System is used for trend analysis, including generation of weekly

and monthly reports. PacBell managers also use another Remedy product called

Flashboards to provide a real-time, graphical representation of trouble ticket metrics such as the number of open trouble tickets. [Ref. 6]

E.   FORMAL PROBLEM STATEMENT

Based upon Chapter II and III's discussion of the topics listed below, the system problem will now be defined. Topics include:

- C4I doctrine and policy
- NCTAMS/JFTOC mission and organization
- Structured TAFIM process
- NCTAMS EASTPAC user assessment
- Help desk software technology review

System Problem Statement: The JFTOC performs the roles of both a NOC, providing network management services, and an internal help desk, addressing information service problems of its fleet customers. The current FMS employed by the three NCTAMS is functionally inadequate for the JFTOC to achieve the CNMP's goal of a "one-stop shop" [Ref. 29:p. 12] for network management services. Interviews with system users reveal that the system's manual nature results in: use of non-timely information in troubleshooting and decision-making; duplication of outage information in numerous data stores; manual retrival of outage information for report preparation and trend analysis; and an inability to share outage information both between NCTAMS work centers and between JFTOC and its customers.

Chapter II introduces the Structured TAFIM Process as the methodology that will be used to define a target system and migration path to achieve that system. At this point, however, it is appropriate to outline the basic criterion and constraints that will be used to

33

solve this problem. One valid way to express these concepts is through use of a mathematical programming template; maximize or minimize some objective function subject to certain constraints. Applying this model to systems development, provides the following choices for problem formulation: [Ref. 20]

- Maximize System Performance (Over its Lifecycle)

    Subject to: System Cost $\leq$ Project Budget

- Minimize System Cost (Over its Lifecycle)

    Subject to: System Performance $\geq$ Minimum System Performance

Based upon the Quadrennial Defense Review's projections for DOD's fiscal environment, the author believes the second formulation option is prudent. Problem constraints will not be introduced in detail until Chapter V, but Figure 3.6 provides the essential elements of the formulation model including some constraint examples:

Minimize System Cost (Over its Lifecycle)

Subject To: **(1) System Quality $\geq$ Minimum System Quality**
(e.g., availability, response time, scalability)

(2) Information Quality $\geq$ Minimum Information Quality
(e.g., information timeliness, information relevance)

(3) Technology
(e.g., help desk applications, DBMSs, processor speeds)

(4) Existing Information Infrastructure/Policy
(e.g., SIPRNet, existing Classified LAN)

Figure 3.6. Problem Formulation Model. [Ref. 19]

F.   SUMMARY

Definition of the system problem and establishment of the criterion and constraints that will be used to solve it are the end products of step two of the Structured TAFIM Process. They ensure the common "sheet of music" for all future discussions about the baseline system, target architecture and migration paths development/selection.

IV. ASSESSING THE BASELINE SYSTEM

A. INTRODUCTION

The third step of the TAFIM process, assessing the baseline system, reveals the character and state of the current system. Chapter III defined the system problem as one of designing a FMS that minimizes cost over its lifecycle subject to the constraints of quality, information quality, technology, and existing information infrastructure. This chapter outlines the policy, processes, external entities, data stores, and data flows which comprise the Baseline FMS. Additionally, the physical aspects of the system, including: networks, hardware, software, and data storage are briefly described. Finally, this chapter concludes with a discussion on the implementation of a classified LAN at NCTAMS EASTPAC, since it is relevant to the design of a target FMS.

B. POLICY AND REPORTS

1. Policy

a. *Fleet Operational Telecommunications Program (FOTP)*

The Fleet Operational Telecommunications Program (FOTP) Manual is promulgated by COMNAVCOMTELCOM for implementation by CO's of NCTAMS. It provides policy for the organization, control and management of NAVCOMTELCOM shore activities and automated systems in the Naval Computer and Telecommunications System (NCTS) over which NAVCOMTELCOM exercises configuration control. Topics covered include: COMNAVCOMTELCOM organization for operations; command relationships; NCTAMS internal organization and functions; NCTS operations and readiness; and required reports. [Ref. 30:p. 1-1]

Based upon the guidance of the FOTP Manual, procedures for specific operations and tasks are promulgated via a family of documents. Figure 4.1 shows the hierarchy and relationship of NAVCOMTELCOM procedural documents.
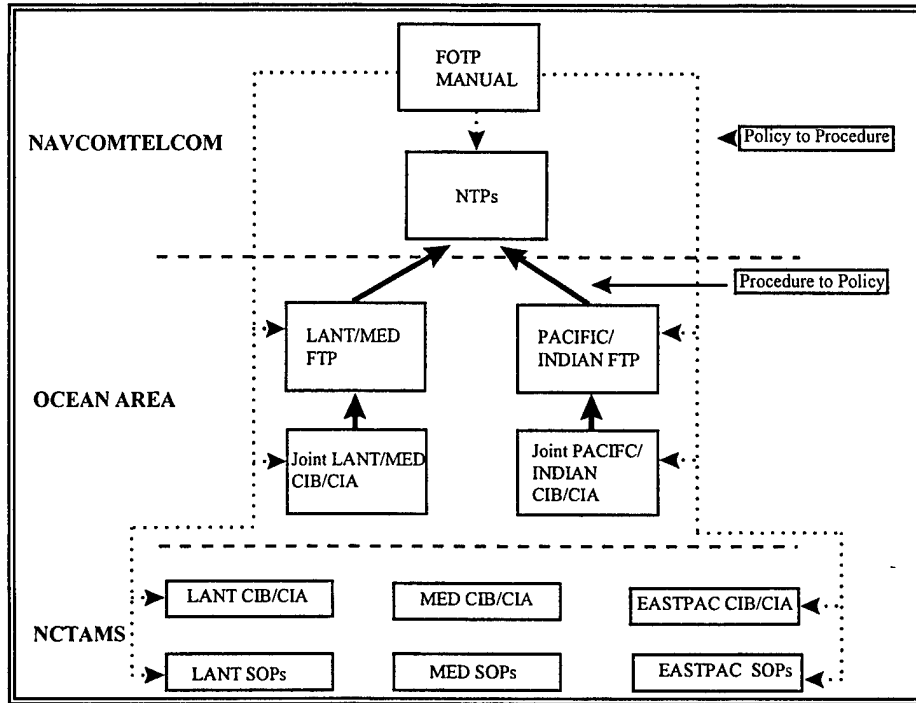
Figure 4.1. Relationship of NAVCOMTELCOM Policy and Procedural Documents. [Ref. 30: pp. 7.1-7.2]

COMNAVCOMTELCOM publishes a series of Naval Telecommunications Procedures (NTPs) to establish standardized, NCTS-wide procedures. The NCTAMS, in turn, issue Fleet Telecommunications Procedures (FTPs) to establish procedures that are ocean-area specific. There are two FTPs; one for the LANT/MED ocean-area written jointly by NCTAMS LANT and NCTAMS MED, and one for the PACIFIC/INDIAN ocean-area written by NCTAMS EASTPAC. If FTP procedures are standardized throughout the NCTS, they are then incorporated into the NTPs. Each NCTAMS establishes procedures which are unique to their region using

Communications Information Bulletins (CIB) and Communications Information Advisories (CIA). As procedures emerge that are common to an ocean area (e.g., LANT/MED), a joint CIB (e.g., NCTAMS LANT/MED) is issued. These joint CIBs are incorporated into the respective FTP upon revision. Finally, each NCTAMS establishes Standard Operating Procedures (SOPs) which provide step-by-step procedures for performing important operational and administrative tasks. [Ref. 30: pp. 7.1-7.2]

b. NCTAMS Standard Operating Procedures (SOPs)

The FOTP establishes the organization of SOP into the following categories:

- ALFA: Administrative
- ECHO: Emergency
- INDIA: Information
- OSCAR: Operational
- ROMEO: Reports
- TANGO: Training

Using these categories, each NCTAMS N3 division promulgates their won task specific SOPs. For SOPs to remain accurate, periodic revisions must occur which many include adding new SOPs. Detailed and comprehensive SOPs play a significant role in watchstander training and qualification. [Ref. 30:pp. 7.2-7.3]

2. Reports

The FOTP Manual provides guidance on the reports that each NCTAMS is required to submit or receive. The following reports are pertinent to the Baseline FMS:

a. COMSPOT

All ships are required to submit a Special Communications Report (COMSPOT) to the NCTAMS "anytime significant communications difficulties are encountered". [Ref. 30:p. 8.2] COMPSOTs are submitted via naval message (AUTODIN) in accordance with NTP-4. The message sent by the NCTAMS responding to a COMPSOT is likewise referred to as a COMSPOT.

b. CASREP

NCTAMS and NCTS are required to submit an Equipment Casualty Report (CASREP) via naval message on any failed communications equipment. [Ref. 30:p. 8.9] The FOTP Manual indicates that CASREPs submitted by a NCTAMS are to include COMNAVCOMTELCOM as an action addee and the FLTCINC as an info addee. [Ref. 30:p. B.1] Ships that have submitted a COMPSOT and discover failed communications equipment as the reason for outage (RFO) generate a CASREP that includes NCTAMS as an info addee.

c. Detailed Outage Report (DOR)

A DOR is a step-by-step breakdown of all actions taken or events that occurred in the resolution of a telecommunications outage. A DOR Request message is normally sent by an afloat unit of staff to a NCTAMS.

d. As-occurring SITREP

As-occurring Situation Reports (SITREPs) are sent by a NCTAMS to NAVCOMTELCOM in the event of a telecommunications outage or inclement weather condition that threatens to impair regional operations. The FOTP Manual provides specific reporting guidelines, but general categories of events include: Inclement

Weather (e.g., hurricane, typhoon), Bomb Threat/Fire/Terrorist Threat, Function Shifts (e.g., JFTOC, Fleet Broadcast (FLTBCST) Broadcast Control Station (BCS)), and Loss of Telemetry, Tracking and Control (TT&C). As-occurring SITREPs use a standard template consisting of eight fields to describe: the outage, alternate means of telecommunications delivery, and efforts to resolve the outage. They are prepared using a DOS editor template and numbered starting with 001 for the first SITREP issued on the first day of each month. Each successive amplifying SITREP is designated with a letter starting with an "A", e.g., 001A, 001B. The final As-occurring SITREP in a series is designated as such, e.g., 001 FINAL. [Ref. 30:pp. 8.2-8.4]

Until recently, As-occurring SITREP were transmitted to NAVCOMTELCOM via the Global Navy Orderwire Network (Nownet); a secure, point-to-point circuit that connects the NAVCOMTELCOM Naval Computer and Telecommunications Operations Center (NCTOC) with each NCTAMS. In turn, the NCTAMS are connected to FLTCINCs, Numbered Fleet Commander's Flagship, and all NCTS in their region. [Ref. 30:pp. 7.6-7.7] The Global Nownet node at NCTOC is currently disabled pending conversion of the Nownet to SIPRNet. The current procedure for submitting an As-occurring SITREP is via secure FAX or naval message (e.g., Fleet Advisory). [Ref. 53]

e. SITREP

SITREP is the term used to describe As-occurring SITREPs sent to the JFTOC by a NCTAMS N3 division, NCTS, or any other telecommunications facilities within that NCTAMS region. The similarities to an "As-occurring SITREP" include: format, numbering system, and transmission to NCTAMS via Global Nownet. The

major difference between them is the categories of events that are reportable. Whereas As-occurring SITREPs are required for major events that threaten the operation of a region, SITREPs are required for circuit/system outages that meet or exceed a certain time threshold. Reportable outages and corresponding time thresholds are listed in the FOTP. Each NCTAMS may also use this guidance to determine when regional activities must submit SITREPs, or it may institute stricter guidelines by shortening time limits or including other circuits/systems. [Ref. 30:p. 8.6]

Table 4.1 shows the number of SITREPs handled by NCTAMS EASTPAC JFTOC during the months of April, May, June, and July 1997. Figure 4.2 provides a breakdown of April's SITREP by category. During that month, approximately 70 percent of the SITREPs concern fault/outages and 30 percent document configuration changes. Within these two categories of Fault Management and Configuration Management, sub-categories are established to show general trends. The most significant sub-category within Fault Management is SHF Trunk Outages which account for approximately 30 percent of the total number of SITREPs. These statistics based upon only one month of data are not statistically significant, but they are useful to give the reader a general understanding of the type of faults managed by the JFTOC.

Table 4.1. NCTAMS EASTPAC SITREP Statistics for April-July 1997. [Ref. 38]

Month	Number of SITREP
April 1997	193
May 1997	167
June 1997	169
July 1997	132

NCTAMS EASTPAC SITREPS FOR APRIL 1997

FAULT MANAGEMENT

SHF TRUNK	60	31.09%
VLF* (* INCLUDES 2 HAZCONS)	14	7.25%
LF	1	0.52%
SATCOMM TERMINALS* (FSC-79, FSC-78, GSC-52) * INCLUDES 4 HAZCONS	10	5.18%
SIPRNet/NIPRNet	16	8.29%
SHF CIRCUITS (STEL, JDISS)	2	1.04%
UHF CIRCUITS (TADIXS, CUDIXS, OTCIXS, SSIXS, DAMA SUITE)	16	8.29%
LANDLINE TRUNKS	4	2.07%
MESSAGING SYSTEMS* (NAVCOMPARS, PCMT, GATEGUARD MARCEMP, VERDIN, FLT BROADCAST) * INCLUDES 2 HAZCONS	8	4.15%
ANCC	3	1.55%
SUB TOTAL	134	69.4%
CONFIGURATION MANAGEMENT		
CHANGE TO CIRCUIT CONFIGURATION (BKS, BRS, BCA, SATELLITE ACCESS)	19	9.84%
SYSTEM ACTIVATION	1	0.52%
SHF SCHEDULED OUTAGE (MAN ALOFT, DRILLS, TESTING)	29	15.03%
NON-SHF SCHEDULED OUTAGE (VLF, LF, HF)	7	3.63%
SUB TOTAL	56	29.02%
OTHER		
CANCELLED SITREP	3	1.55%
SUB TOTAL	3	1.55%
GRAND TOTAL	193	100.00%

Figure 4.2. NCTAMS EASTPAC April 1997 SITREP. [Ref. 38]

43

f.   Daily Summary Report (DSR)

The Daily summary Report (DSR) provides COMNAVCOMTELCOM with a snap-shot of the significant telecommunications events that occurred in each NCTAMS region. Sent each day at 0300 Zulu (Z), it covers the period of the previous radio day (RADAY), 0001Z-2359Z. Areas covered include: FLTBCST and Common User Digital Information Exchange Subsystem (CUDIXS) Status; Non-Training High Frequency (HF) Terminations Status; Defense Satellite Communication System (DSCS) - Super High Frequency (SHF) Terminations Status; Autodin Switching Center (ASC)/Naval Communications Processing and Routing System (NAVCOMPARS) Status; Special Interest Items; Current Exercises; and Future Exercises. The Special Interest Items section includes a summary of events surrounding each outage which meet the FOTP Manual SITREP reporting criteria. [Ref. 30:pp. 8.4-8.6]

g.   Station Logs

Station logs, also known as radio logs, are records of all significant events that occur during the 24 hours of a RADAY. Each NCTAMS N3 division that performs watchkeeping functions is required to maintain logs. As the regional network manager, the JFTOC's logs contain a chronological listing of all outages reported, SITREPs received from regional sites, As-occurring SITREPs sent to NAVCOMTELCOM, follow-up outage information received, outages resolved, final SITREPs received, and final As-occurring SITREPs sent. Additionally, administrative events such as watch turnover and personnel issues are recorded.

C.   FMS DATA FLOW DIAGRAMS (DFD)

Interviews conducted with NCTAMS EASTPAC personnel and the author's experience as a former JWO and JFTOC Division Officer at NCTAMS LANT provided the information required to model the baseline system using Data Flow Diagrams (DFD). Diagrams were kept general enough to allow future adjustments to model specific practices of any one NCTAMS. Appendix B provides a review of DFD conventions and methodology.

1.   Context Level Diagram

Figure 4.3 shows the Baseline System Context Level Diagram. The NCTAMS FMS System is represented to include processes that occur within and between NCTAMS N3 divisions. All other stakeholders such as customers, regional sites (e.g., NCTS), and Operational Commanders (e.g., FLTCINC) are treated as external entities. The boundaries defined for these system are intended to focus attention on the extensive amount of data flow between divisions and data storage within divisions.

2.   Level Zero Diagram

Figures 4.4-4.6 contain the Baseline System Level Zero Diagram with its nine processes, external entities, data flows, and data stores. The following discussion provides insight into the methodology used to model the Baseline FMS. A detailed description of each process will be provided in the next subsection with each Level One Diagram.

a.   Processes

The nine processes in the Level Zero Diagram include six that parallel the key phases of fault management described in Chapter III. These include: Receive

Notification of Outage, Log Outage, Create SITREP/As-occurring SITREP, Troubleshoot Outage, Track and Update SITREP/As-occurring SITREP, and Close-out Records Upon Resolution. The other three, Processes Six, Eight, and Nine, provide a graphical representation of the reporting and managerial aspects of the system.
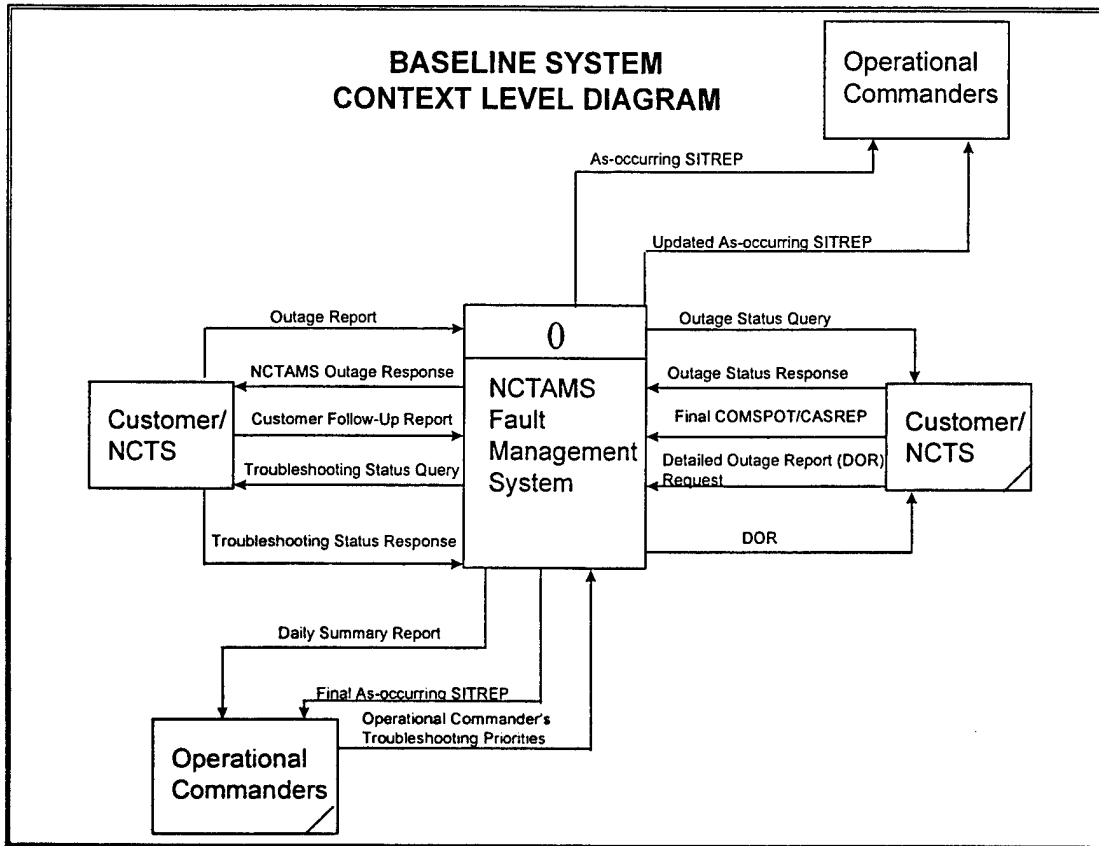
Figure 4.3. Baseline Context Level Diagram.

46
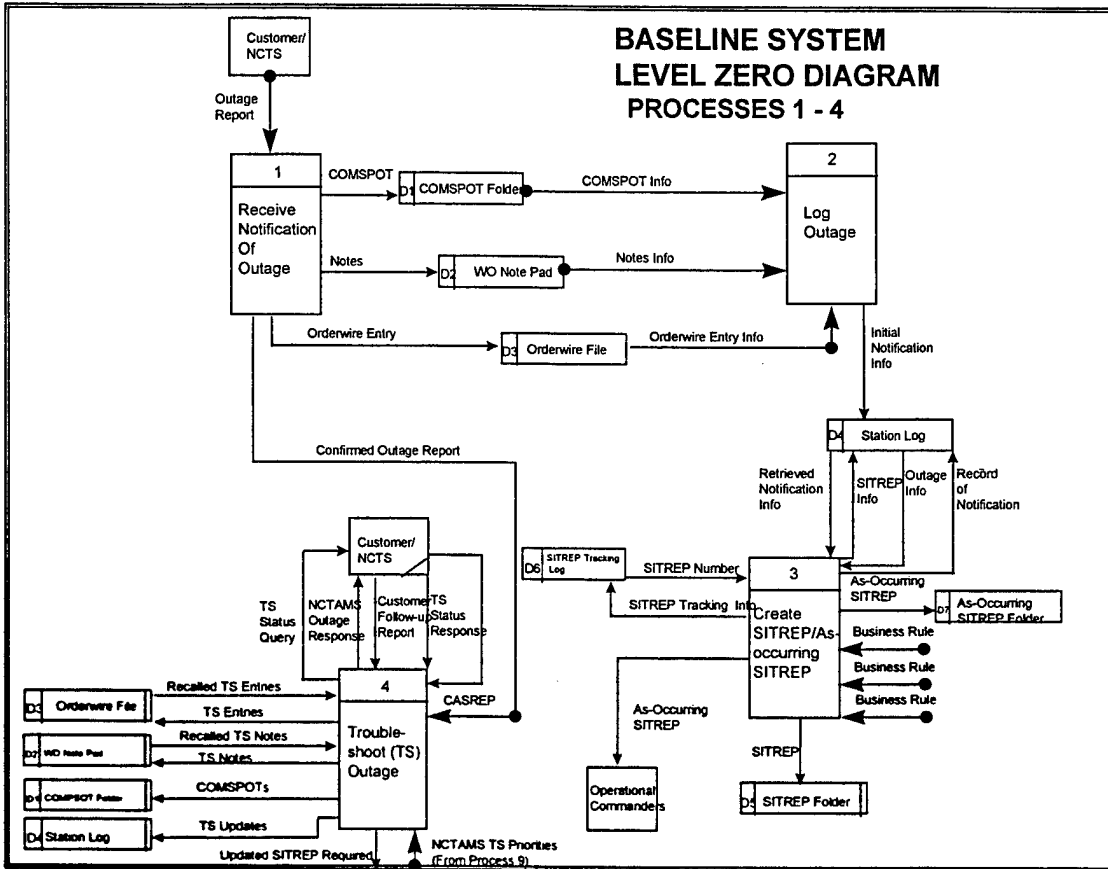
Figure 4.4. Baseline Level One Diagram: Processes 1-4.
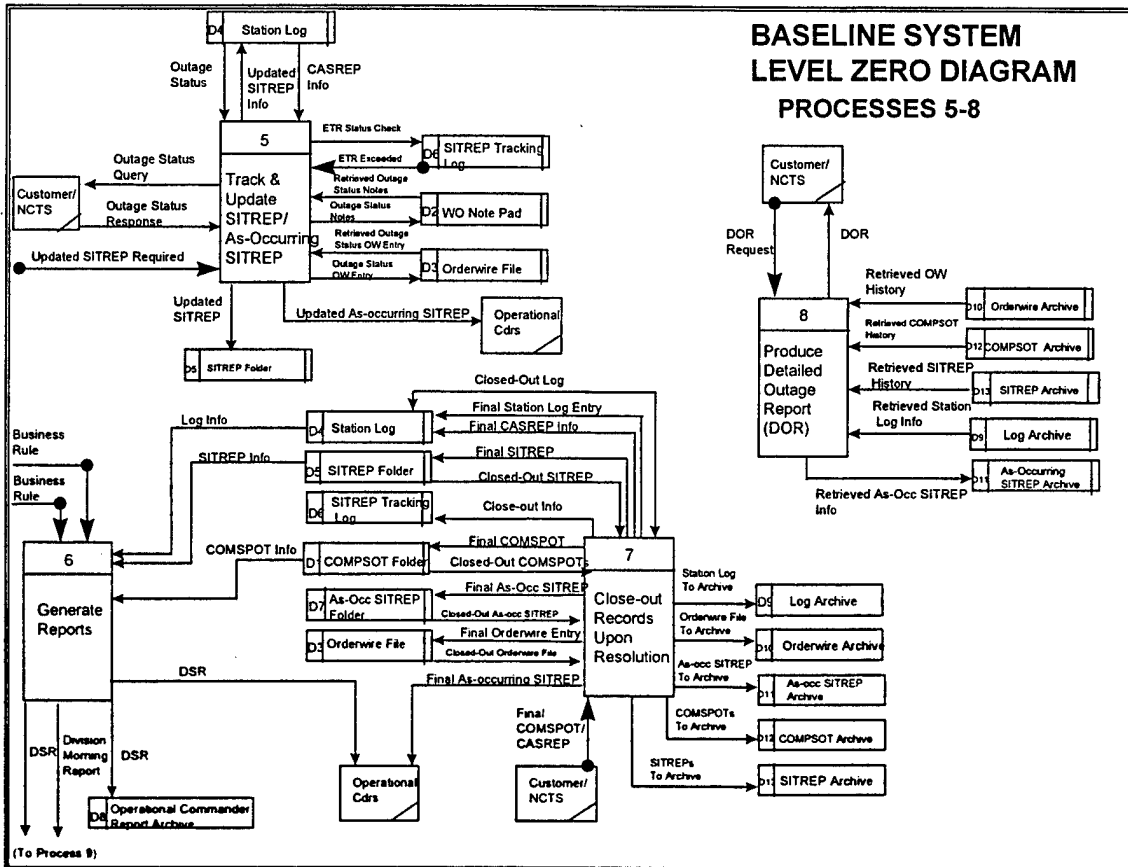
Figure 4.5. Baseline Level Zero Diagram: Processes 5-8.

```
                                          BASELINE SYSTEM
                                          LEVEL ZERO DIAGRAM
                                          PROCESS 9


                        ┌──────────┐
                        │Operational│
                        │Cdrs      ╱│
                        └─────┬────┘
                              │ Operational
                              │ Commander's
                              │ TS
                              │ Priorities
                              ▼
                        ┌──────────┐
                        │    9     │
          DSR           ├──────────┤
    ──────────────────► │Formulate │  NCTAMS TS Priorities
   (From Process 6)     │Management├──────────────────────►  (To Process 4)
                        │Strategy  │  Business Rule
    ──────────────────► │          │ ◄──────────────●
   Division Morning Report └───┬──────┘
                              ▲
                              │ Daily
                              │ COMSPOTs
                        ┌──┬───────────────┐
                        │D1│ COMSPOT Folder │
                        └──┴───────────────┘
```
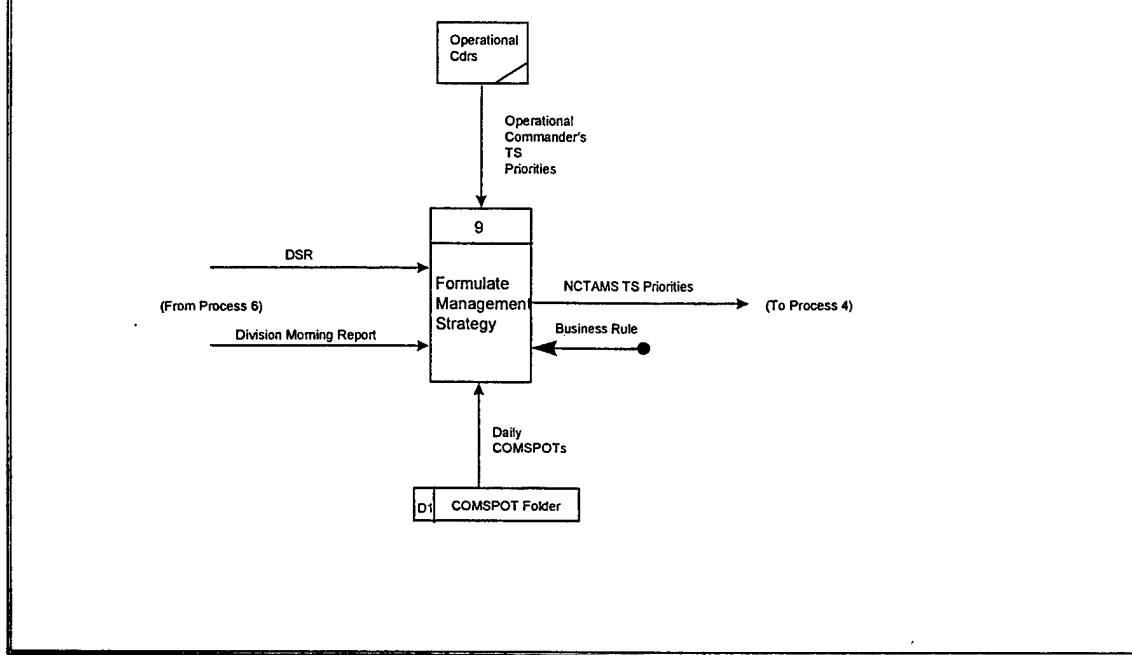
Figure 4.6. Baseline Level Zero Diagram: Processes 9.

b.   *External Entities*

The following categories of external entities are used in both the Baseline

and Target System DFD:

- Operational Commanders: This category includes FLTCINCs, Numbered Fleet
  Commanders, DISA, and NAVCOMTELCOM. Other operational
  commanders may interact with the NCTAMS FMS depending upon the
  specific telecommunications tasking.

- Customer/NCTS: Customer and regional sites are grouped together into one
  category, because they both report outages to the JFTOC. Customers are
  primarily afloat units but also include those shore commands which receive
  service directly from the NCTAMS. Regional sites include all NCTS,
  NCTAMS Detachments (NCTAMS DET), Naval Computers and
  Telecommunications Detachments (NAVCOMTELDET), Naval
  Telecommunications Centers (NTCC), Anti-Submarine Warfare Support

49

Communications (ASCOMM), or Special Communications Sites (SPECOMM) that report operationally to the JFTOC. [Ref. 30:p. 3-1]

c. *Data Stores*

Data stores include a combination of paper and flat files located on stand-alone PCs. The Level Zero Diagram shows 13 data stores. The number of data stores increases to 20 in the Level One Diagram. The additional data stores are the result of showing both JFTOC and Division data stores at the Level One level. In actuality, however, the number of stores is much higher, because there are seven operational divisions in a NCTAMS EASTPAC N3 Department. This places the actual number of data stores at 68 (12 JFTOC data stores + (8 data stores/division X 7 divisions) = 68). Table 4.2 categorizes the Level Zero data stores as either paper or electronic flat files.

Table 4.2. Level Zero Data Stores.

Number	Name	Paper/Electronic
D1	COMSPOT Folder	Paper File
D2	Watch Officer (WO) Note Pad	Paper File
D3	Orderwire File	Electronic Flat File
D4	Station Log	Electronic Flat File
D5	SITREP Folder	Paper File
D6	SITREP Tracking Log	Paper File
D7	As-occurring SITREP Folder	Paper File
D8	Operational Commander Report Archive	Paper File
D9	Log Archive	Paper/Electronic
D10	Orderwire Archive	Electronic Flat File
D11	As-occurring SITREP Archive	Paper File
D12	COMSPOT Archive	Paper File
D13	SITREP Archive	Paper/Electronic

d. *Data Flows*

Data flows are too numerous to discuss individually, however, the Level Zero DFD provides a clear picture of one significant fact; The vast majority of the data flows are between processes and data stores. In this case, this means that the

preponderance of the work performed within the system involves putting information into and removing it from paper or electronic, flat files.

3.   Level One Diagrams

Processes One through Eight, shown in Figures 4.4 and 4.5, are expanded or "exploded" into child processes to form the Baseline System Level One Diagrams; these are shown as Figures 4.7 through 4.14. Accompanying each Level One Diagram is a detailed description of each data flow. Process Nine, shown in Figure 4.6, is not exploded to a Level One Diagram, because it does not require further description via sub-processes.

a.   *Receive Notification of Outage*

Figure 4.7 shows the Baseline FMS Process One, Level One Diagram.

Process 1.1, Receive Outage Notification - JFTOC data flows are described as follows:

- Process one is initiated when JFTOC receives Outage Report from:

    - Customer (afloat or ashore unit) via COMSPOT, phone or orderwire entry.

    - Regional NCTS via orderwire entry or phone.

    - N3 Division via orderwire entry or phone.

- In event of customer/NCTS notification, JFTOC sends Division Request for Outage Confirmation.

- Paper copies of COMSPOTs are stored in *JFTOC COMSPOT Folder*.

- Notes taken during phone calls are stored on *JFTOC JWO Note Pad*.

- Orderwire entries are stored electronically in *JFTOC Orderwire File*.
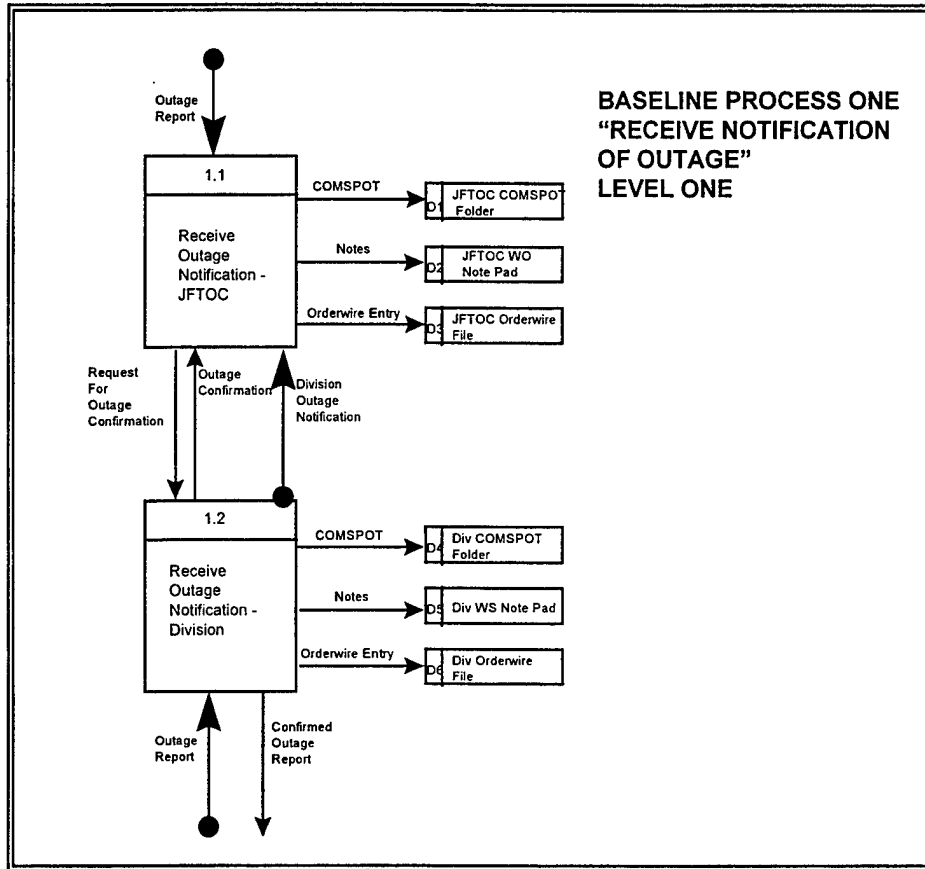
Figure 4.7. Process One: Receive Notification of Outage.

Process 1.2, Receive Outage Notification - Division data flows are described as follows:

- Division receives Outage Report from:

    - Customer via COMSPOT, phone or orderwire entry

    - Regional NCTS via orderwire entry or phone

    - Internal alarms or monitors

- Depending upon whether JFTOC or Division learns of outage first, Division sends Division Outage Notification or Outage Confirmation to JFTOC via phone or orderwire. Outage Confirmation/Division Outage Notification starts the troubleshooting process.

- COMSPOTs are stored in *Division COMSPOT Folder*.

- Notes taken during phone calls are stored on *Division Watch Supervisor (WS) Note Pad.*

- Orderwire entries are stored electronically in *Division Orderwire File.*

b.   *Log Outage*

Figure 4.8 shows the Baseline FMS Process Two, Level One Diagram.
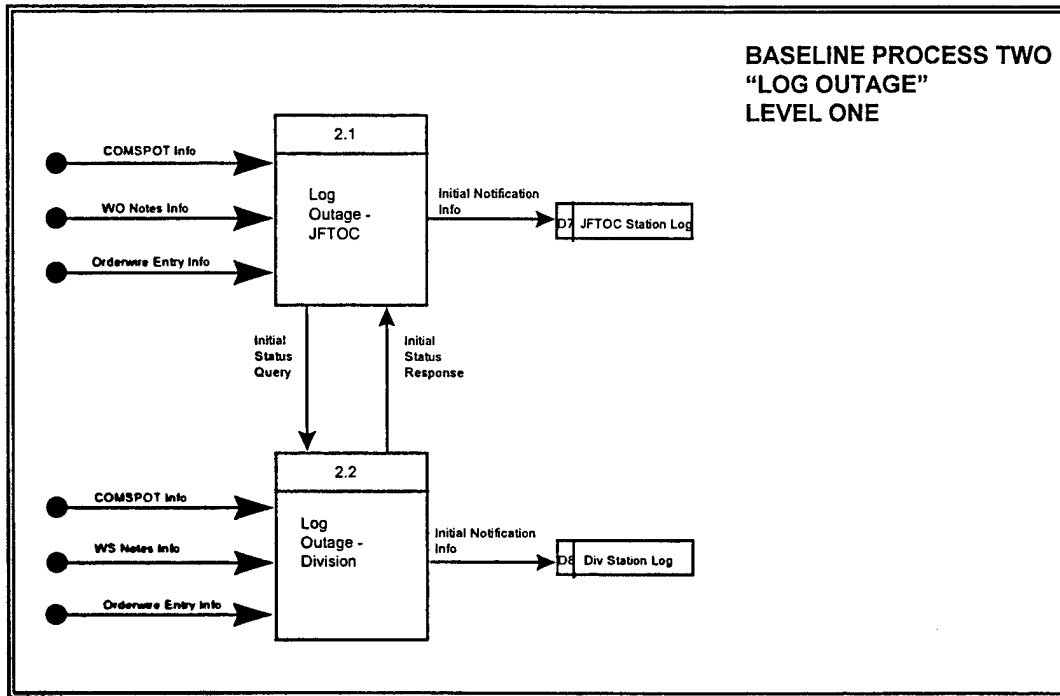
Figure 4.8. Process Two: Log Outage.

Process 2.1, Log Outage - JFTOC data flows are described as follows:

- Outage information from *JFTOC COMSPOT Folder, JFTOC JWO Note Pad* and *JFTOC Orderwire File* form JWO's mental model of the outage.

- JWO enters Initial Notification Info into *JFTOC Station Log* regarding outage notification to a DOS-based, flat-file on a stand-alone PC.

- JFTOC makes Initial Status Query to Division for any additional information received since Outage Report was received.

Process 2.2, Log Outage - Division data flows are described as follows:

- Outage information from *Division COMSPOT Folder, Division WS Note Pad* and *Division Orderwire File* form Division WS's mental model of the outage.

53

- Watch Supervisor enters Initial Notification Info into *Division Station Log* regarding outage notification to a DOS-based, flat-file on a stand-alone PC.

- Division provides Initial Status Response to JFTOC.

c. Create SITREP/As-occurring SITREP

Figure 4.9 shows the Baseline FMS Process Three, Level One Diagram.
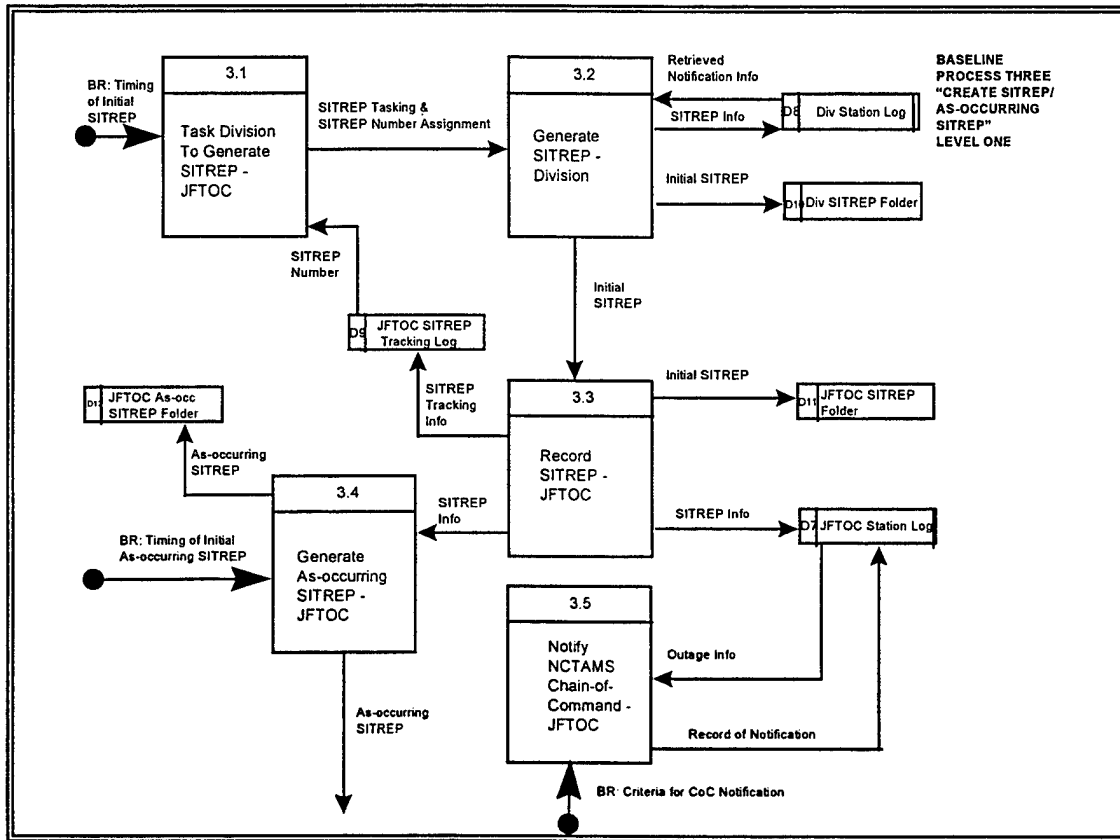
Figure 4.9. Process Three: Create SITREP/As-occurring SITREP.

Process 3.1, Task Division to Generate SITREP - JFTOC Division data

flows are described as follows:

- Process three is initiated in accordance with NCTAMS Business Rule (BR) regulating Timing of Initial SITREPs.

- JFTOC obtains next SITREP number from *JFTOC SITREP Tracking Log*, a manual log book.

54

- JFTOC sends SITREP Tasking and SITREP Number Assignment to Division via phone or orderwire to generate initial SITREP.

   Process 3.2, Generate SITREP - Division data flows are described as follows:

- Division pulls Retrieved Outage Info from *Division Station Log*.

- Division prepares Initial SITREP.

- Division places a paper copy of Initial SITREP in *Division SITREP Folder*.

- Division places SITREP Info in *Division Station Log* to document Initial SITREP issuance.

- Division forwards Initial SITREP electronically to JFTOC via orderwire or manually by messenger.

   Process 3.3, Record SITREP - JFTOC data flows are described as follows:

- JFTOC receives Initial SITREP from Division.

- JFTOC files Initial SITREP in *JFTOC SITREP Folder*.

- JFTOC makes electronic entry of SITREP Info in *JFTOC Station Log* to document initial SITREP creation.

- JFTOC manually enters SITREP Tracking Information (i.e. SITREP Number, Division Assigned, Subject, Down Time, Up Time and Remarks) in *JFTOC SITREP Tracking Log*.

   Process 3.4, Generate As-occurring SITREP - JFTOC data flows are described as follows:

- JFTOC uses SITREP Information to generate As-occurring SITREP for outages listed in FOTP.

- JFTOC sends electronic copy of As-occurring SITREP to operational commanders, NCTC and CINCPACFLT in accordance with NCTAMS BR regulating Timing of Initial As-occurring SITREP.

55

- JFTOC files paper copy of As-occurring SITREP in JFTOC As-occurring *SITREP Folder.*

Process 3.5, Notify NCTAMS Chain-of-Command - JFTOC data flows

are described as follows:

- In accordance with NCTAMS BR regulating Criteria for Chain-of-Command Notification, JFTOC initiates process of notifying NCTAMS chain-of-command.

- JFTOC retrieves Outage Info from *JFTOC Station Log.*

- JFTOC notifies NCTAMS Chain-of-Command of outage via telephone as required by SOPs.

- JFTOC places Record of Notification in *JFTOC Station Log* that notification occurred.

d. Troubleshoot Outage

Figure 4.10 shows the Baseline FMS Process Four, Level One Diagram.

Process 4.1, Perform Troubleshooting (TS) Actions - Division data flows

are described as follows:

- Process four is initiated upon receipt of Confirmed Outage Report (from process one).

- TS actions are influenced by NCTAMS TS Priorities which are established in Process Nine.

- Division and Customer (or Regional NCTS) communicate frequently via orderwire or phone, TS Status Query/TS Status Response, to obtain information about what the other side "sees" as troubleshooting steps are performed.

- Information exchanged via orderwire, TS Entries, is stored electronically in *Division Orderwire Files.*

- Information obtained via phone, Troubleshooting Notes, is written on *Division WS Note Pad.*

56

- Recalled TS Orderwire Entries and Recalled TS Notes are retrieved to make electronic entry in *Division Station Log*, TS Updates, *to* document troubleshooting progress.

- During TS process, Division may receive a CASREP from a ship or NCTS documenting failed communications equipment and stating impact on unit/station's ability to meet its mission.

- CASREP Info is recorded electronically in *Div Station Log*.

- Division passes troubleshooting status to JFTOC via phone or orderwire.
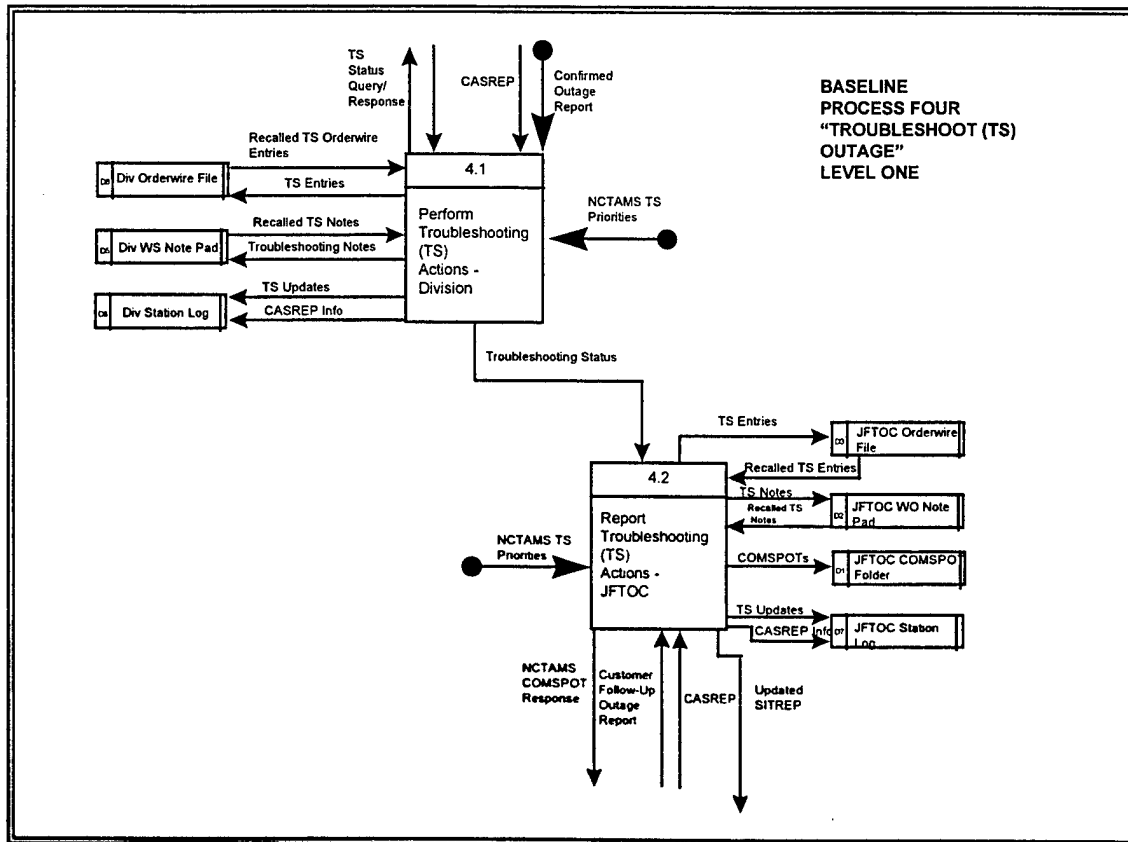
Figure 4.10. Process Four: Troubleshoot Outage.

Process 4.2, Report TS Actions - JFTOC data flows are described as follows:

- JFTOC receives Troubleshooting Status passed from Division.

- TS reporting is influenced by NCTAMS TS Priorities which are established in Process Nine, Formulate NCTAMS Trouble Management Strategy.

57

- Information passed from Division or Customer/NCTS via orderwire, TS Entries, is stored in *JFTOC OW Files.*

- Information passed from Division or Customer/NCTS via phone, TS Notes, is stored on *JFTOC JWO Note Pad.*

- JFTOC makes electronic entry in JFTOC Station Log, TS Updates, documenting troubleshooting status.

- Recalled TS Entries and Recalled TS Notes from *JFTOC Orderwire File* and *JFTOC JWO Note Pad* are used to draft reply to outage notification.

- JFTOC sends NCTAMS COMSPOT Reply in response to COMSPOT received from Customer or Regional NCTS.

- JFTOC receives Follow-Up Outage Report from Customer or Regional NCTS via COMSPOT, orderwire or phone.

- COMSPOTs received from Customer are stored in *JFTOC COMSPOT Folder.*

- During TS Reporting, JFTOC may receive a CASREP from a ship or NCTS documenting failed communications equipment and stating impact on unit/station's ability to meet its mission.

- CASREP Info is recorded electronically in *JFTOC Station Log.*

- Based upon information in customer follow-up report and CASREP (if applicable), a requirement for an Updated SITREP is created.

e. *Track and Update SITREP/As-occurring SITREP*

Figure 4.11 shows the Baseline FMS Process Five, Level One Diagram.

Process 5.1, Determine if SITREP Requires Update - JFTOC data flows are described as follows:

- Process Five is initiated either when information received in a Customer Follow-Up Outage Report suggests a SITREP update is appropriate or when a SITREP exceeds its ETR.

- JFTOC manually checks *JFTOC SITREP Tracking Log,* ETR Status Check, to see if SITREP has exceeded its ETR.

- When SITREP update is required, JFTOC sends a SITREP Update Request to Division via phone or orderwire.

58
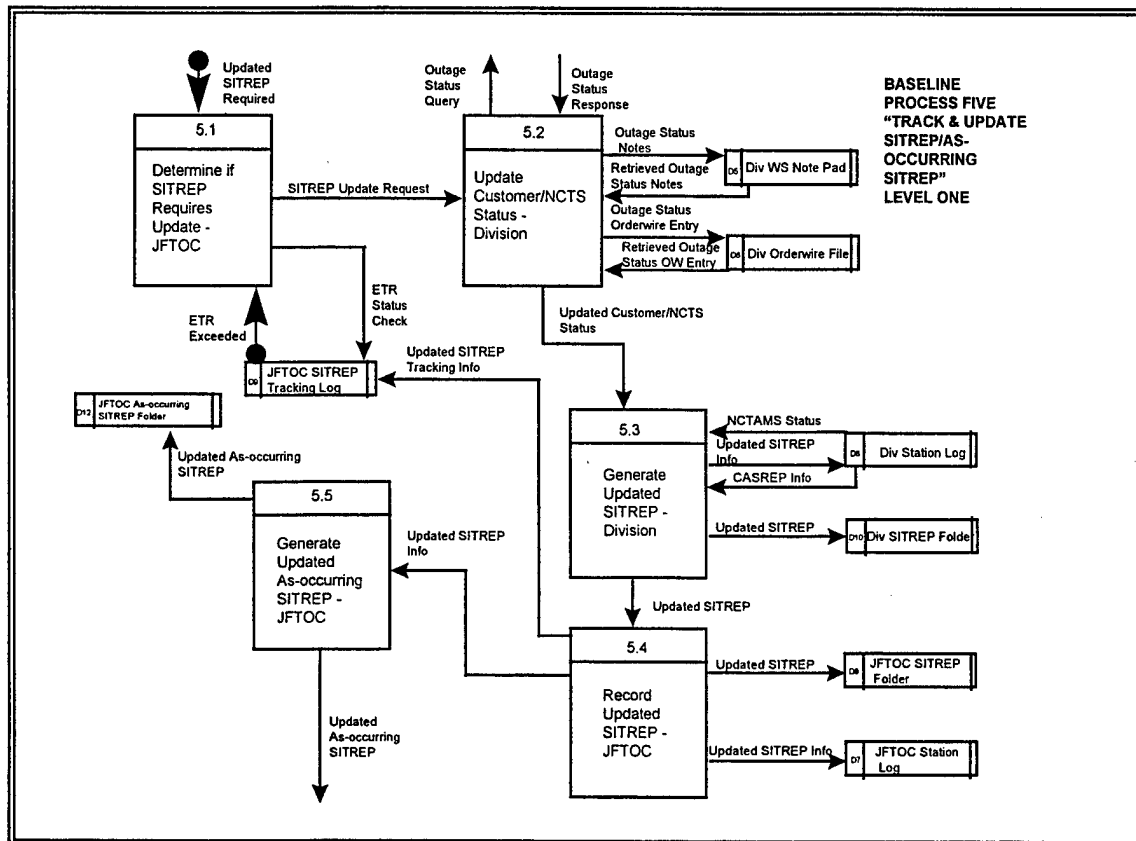
Figure 4.11. Process Five: Track and Update SITREP/As-occurring SITREP.

Process 5.2, Update Customer/NCTS Status - Division data flows are described as follows:

- Division receives SITREP Update Request.

- Division sends an Outage Status Query to Customer/NCTS via orderwire or phone.

- Division receives Outage Status Response from Customer/NCTS via orderwire or phone.

- Outage Status Orderwire Entry is obtained via orderwire and stored electronically in *Division Orderwire File*.

- Outage Status Notes are obtained via phone and stored manually on *Division WS Note Pad*.

- Division retrieves Outage Status Notes and Orderwire Entry stored on *Division WS Note Pad* and *Division Orderwire Files*, respectively.

59

Process 5.3, Generate Updated SITREP - Division data flows are described as follows:

- Division records Updated Customer/NCTS Outage Status in *Division Station Log*.

- Division retrieves Updated NCTAMS Outage Status from *Division Station Log*.

- Division generates Updated SITREP.

- Division stores paper copy of SITREP in *Div SITREP Folder*.

- Division sends Updated SITREP to JFTOC electronically via orderwire or manually via messenger.

Process 5.4, Record Updated SITREP - JFTOC data flows are described as follows:

- JFTOC receives Updated SITREP.

- JFTOC manually files Updated SITREP in *JFTOC SITREP Folder*.

- JFTOC records Updated SITREP Info in *JFTOC Station Log*.

- JFTOC records Updated SITREP Tracking Info in *JFTOC SITREP Tracking Log*.

Process 5.5, Generate Updated As-occurring SITREP - JFTOC data flows are described as follows:

- JFTOC uses Updated SITREP Information to generate Updated As-occurring SITREP.

- JFTOC sends electronic copy of Updated As-occurring SITREP to Operational Commanders.

- JFTOC places paper copy of updated As-occurring SITREP in *JFTOC As-occurring SITREP Folder*.

f.   Generate Reports

Figure 4.12 shows the Baseline FMS Process Six, Level One Diagram.
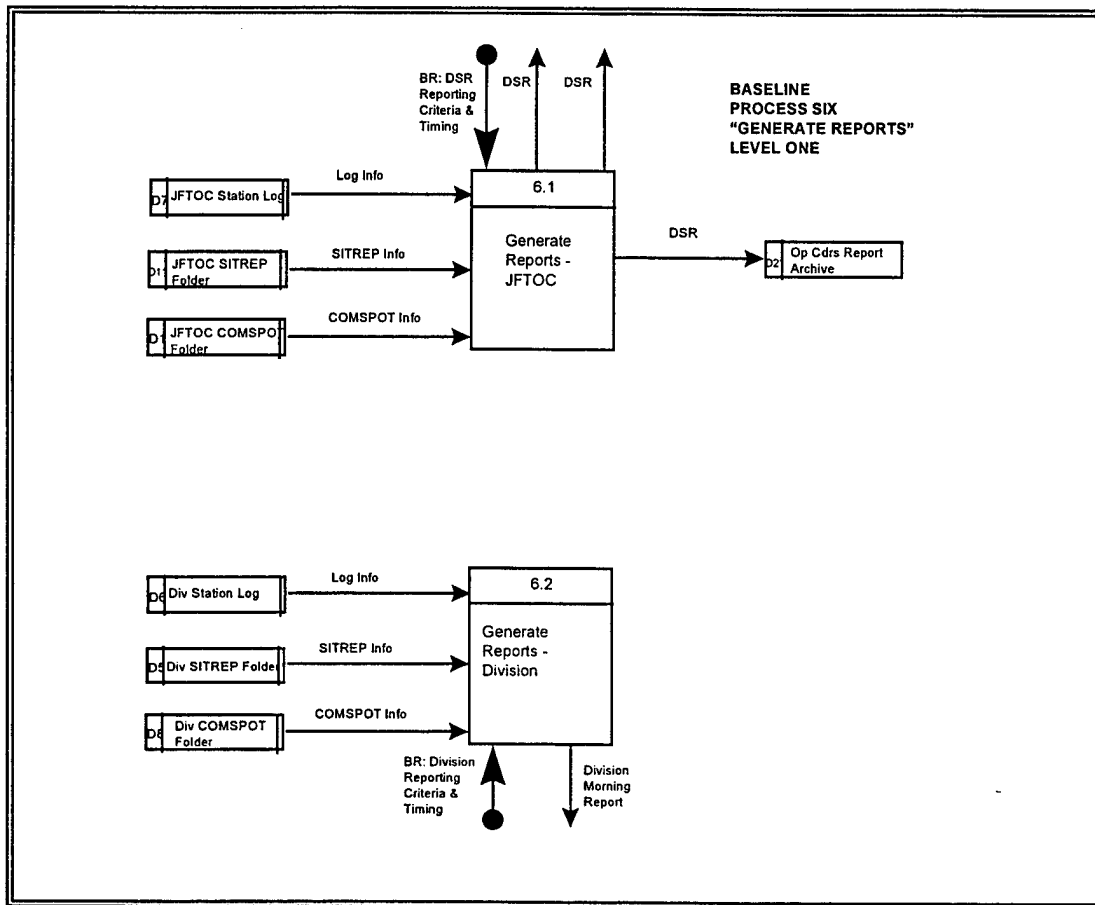
Figure 4.12. Process Six: Generate Reports.

Process 6.1, Generate Reports - JFTOC data flows are described as

follows:

- JFTOC performs process in accordance with NCTAMS BR regulating DSR Reporting Criteria and Timing.

- JFTOC retrieves Outage Info from *JFTOC Station Log, JFTOC SITREP Folder* and *JFTOC COMSPOT Folder* to compose the DSR for Operational Commanders as specified in FOTP.

- JFTOC sends electronic copy of DSR to operational commanders.

- JFTOC makes paper copy of DSR for use by Division Officers and Department Head in Process Nine, Formulate NCTAMS Trouble Management Strategy.

- JFTOC places paper copy of DSR in Operational Commander's Report Archive.

61

Process 6.2, Generate Reports - Division data flows are described as follows:

- Division performs process in accordance with NCTAMS Division Reporting Criteria and Timing.

- Division retrieves Outage Information from *Div Station Log*, *Div SITREP Folder* and Div *COMSPOT Folder* to generate Division Morning Report.

- Division Morning Report is used by Division Officers in performing Process Nine, Formulate NCTAMS Trouble Management Strategy.

- At the end of the day, Division Officers disposes of Division Morning Report in accordance with destruction of classified material directives.

g.   Close-out Records Upon Resolution

Figure 4.13 shows the Baseline FMS Process Seven, Level One Diagram.
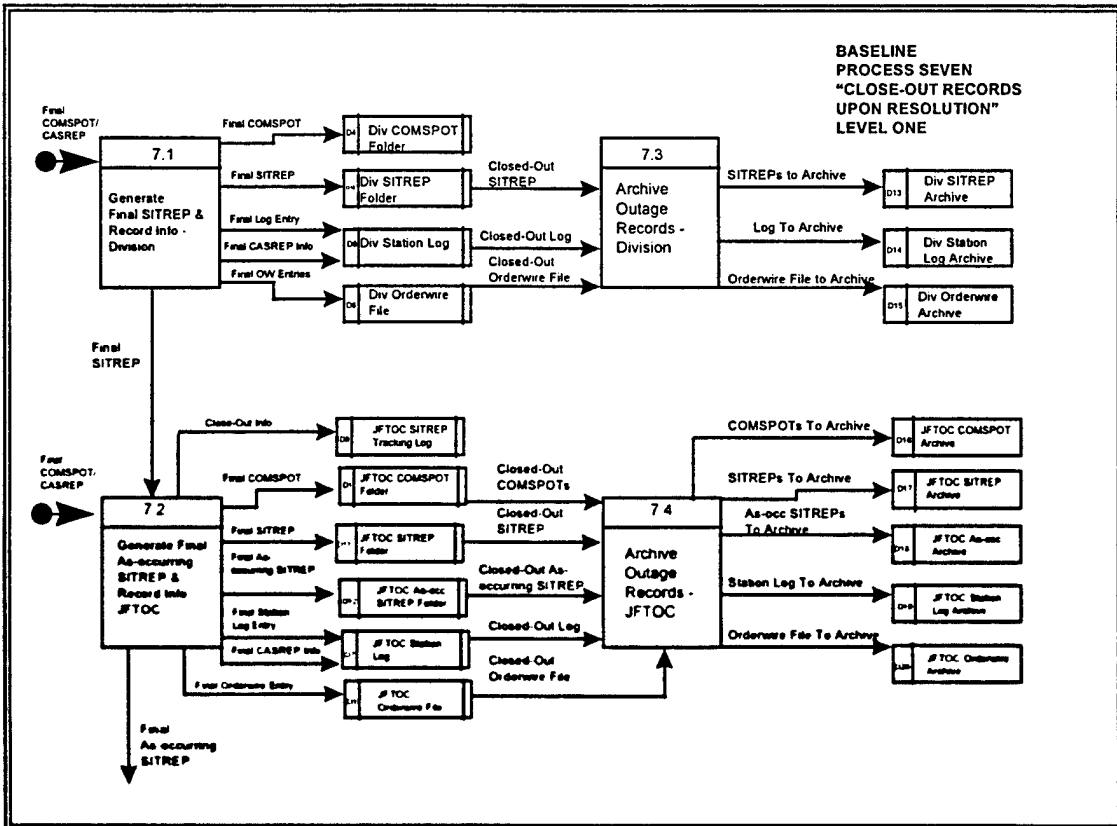
Figure 4.13. Process Seven: Close-out Records Upon Resolution.

62

Process 7.1, Generate Final SITREP & Record Info - Division data flows
are described as follows:

- Process Seven is initiated when Division receives final COMSPOT and CASREP (where applicable) from Customer/NCTS.

- Division uses final COMSPOT and CASREP to generate final SITREP.

- Division places paper copy of Final COMSPOT in *Division COMSPOT Folder*.

- Division places paper copy of Final SITREP in *Division SITREP Folder*.

- Division makes Final Log Entry, including final CASREP info, in *Division Station Log*.

- Division stores Final Orderwire Entries in *Division Orderwire File*.

- Division sends Final SITREP to JFTOC electronically via orderwire or manually via messenger.

Process 7.2, Generate Final As-occurring SITREP & Record Info -
JFTOC data flows are described as follows:

- JFTOC receives final SITREP from Division.

- JFTOC receives Final COMSPOT and CASREP (where applicable) from Customer/NCTS.

- JFTOC uses Final SITREP information to manually record close-out information in *JFTOC SITREP Tracking Log*.

- JFTOC uses Final SITREP information to generate final As-occurring SITREP.

- JFTOC sends electronic copy of As-occurring SITREP to Operational Commanders.

- JFTOC places paper copy of Final COMSPOT in *JFTOC COMSPOT Folder*.

- JFTOC places paper copy of Final SITREP in *JFTOC SITREP Folder*.

- JFTOC places paper copy of Final As-occurring SITREP *in JFTOC As-occurring SITREP Folder*.

- JFTOC makes Final Station Log Entry, including Final CASREP Info, in *JFTOC Station Log.*

- JFTOC stores Final Orderwire Entry in *JFTOC Orderwire File.*

Process 7.3, Archive Outage Records - Division data flows are described

as follows:

- Division removes COMSPOTs from *Division COMSPOT Folder* at the end of each watch that are no longer being used and disposes of them in accordance with destruction of classified material directives.

- Division periodically removes SITREPs from *Division SITREP Folder* and saves electronic copy to disk, creating *Division SITREP Archive.* After one year, archived SITREPs are deleted.

- Division prints a copy of the *Division Station Log* and manually files it in *Division Station Log Archive* by RADAY. After one year, archived Division Station Logs are destroyed.

- Division closes out the orderwire at the end of each RADAY and saves an electronic copy to *Division Orderwire Archive* disk. After one month, archived Division Orderwire Files are overwritten by the next month's file.

Process 7.4, Archive Outage Records - JFTOC data flows are described

as follows:

- JFTOC periodically removes COMSPOTs from *JFTOC COMSPOT Folder* and manually files them in *JFTOC COMSPOT Archive* by Date-Time-Group (DTG) order. After 30 days, archived COMSPOTs are destroyed.

- JFTOC periodically removes SITREPs from *JFTOC SITREP Folder* and manually files them in *JFTOC SITREP Archive* by SITREP number. After 30 days, archived SITREPs are destroyed.

- JFTOC periodically removes SITREPs from *JFTOC As-occurring SITREP Folder* and manually files them in *JFTOC As-occurring SITREP Archive* by SITREP number. After 30 days, archived As-occurring SITREPs are destroyed.

- JFTOC prints a copy of the *JFTOC Station Log* and manually files it in *JFTOC Station Log Archive* by RADAY. After one year, archived JFTOC Station Logs are destroyed.

- JFTOC closes out the orderwire at the end of each RADAY and saves an electronic copy to *JFTOC Orderwire Archive* disk. After one month, archived JFTOC Orderwire Files are overwritten by the next month's file.

h. *Produce DOR*

Figure 4.14 shows the Baseline FMS Process Eight, Level One Diagram.

Process 8.1, Request DOR Input - JFTOC

- Process Eight is initiated when JFTOC receives a request from a Customer for a DOR.

- JFTOC tasks Division to generate a DOR input.
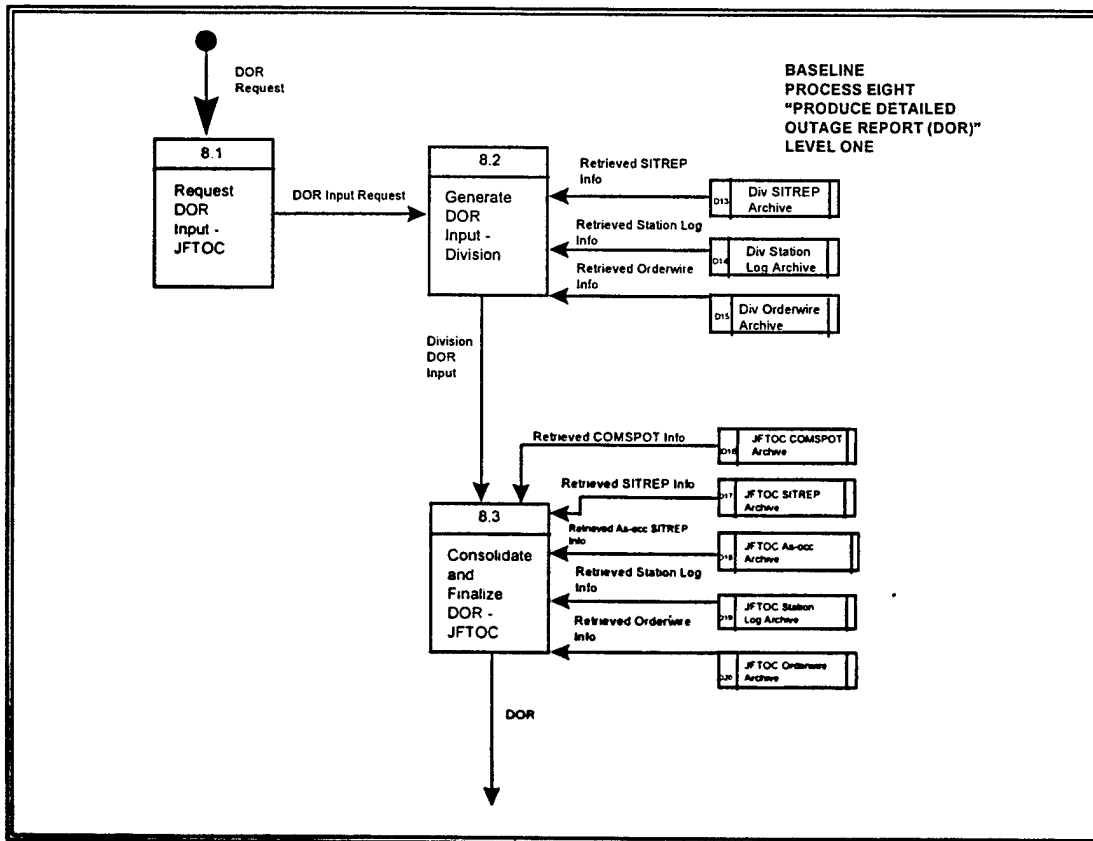
Figure 4.14. Process Eight: Produce Detailed Outage Report.

Process 8.2, Generate DOR Input - Division Figure 4.12 shows the Baseline FMS Process Six, Level One Diagram.

- Division manually retrieves outage information from each of the following:

65

- Division SITREP Archive

- Division Station Log Archive

- Division Orderwire Archive

- Division manually sorts through retrieved outage information and constructs a time line of events from Division's point of view. Time line will be Division DOR input.

- Division places electronic copy of Division DOR input on disk and manually forwards it to JFTOC.

Process 8.3, Consolidate and Finalize DOR - JFTOC Figure 4.12 shows the Baseline FMS Process Six, Level One Diagram.

- JFTOC receives Division DOR input.

- JFTOC manually retrieves outage information from each of the following:

  - JFTOC COMSPOT Archive

  - JFTOC SITREP Archive

  - JFTOC Station Log Archive

  - JFTOC Orderwire Archive

  - JFTOC As-occurring SITREP Archive

- JFTOC manually sorts through retrieved outage information and constructs a time line of events from JFTOC point of view.

- JFTOC compares JFTOC time line with Division time line.

- JFTOC combines time lines, eliminating entries as necessary to create the most complete and accurate version of events that transpired during the outage.

- JFTOC transmits electronic copy of DOR via naval message.

i. *Formulate Management Strategy*

Process 9, Formulate Management Strategy, data flows are described as follows:

66

- Process Nine is initiated based upon the NCTAMS Conduct of Operations Briefs to formulate management strategy.

- NCTAMS managers receive Operational Commander's TS Priorities via phone, e-mail, or meetings.

- NCTAMS managers review Daily COMSPOTs and DSR/Division Morning Report (from process Six).

- Process Nine produces NCTAMS TS Priorities which are an input into Process Four, Troubleshoot Outage.

D. FMS SYSTEM PHYSICAL CHARACTERISTICS

1. N3, Excluding NOC

The NOC Division is not included in this discussion of system physical characteristics; it will be covered separately in the next sub-section.

a. Network

The nine processes which comprise the Baseline FMS are performed in each N3 division using a combination of stand-alone PCs, PCs connected via an in-house orderwire and manual processes (e.g., recording information in a log book). The in-house orderwire operates as a coordination or "chat" circuit with certain divisions available via different ports. Previous entries may be reviewed by scrolling back to the desired time period. Files are saved periodically to diskette. FMS processes are categorized below as using stand-alone PCs, in-house orderwire or manual.

- Receive Notification: Stand-alone PC

- Log Outage: Stand-alone PC

- Create SITREP/As-occurring SITREP:

  - Create: stand-alone PC

  - Forward to JFTOC: In-house orderwire.

- Troubleshoot Outage: In-house orderwire

- Track & Update SITREP/As-occurring SITREP:

  - Track: Manual

  - Update: Stand-alone PC

  - Forward to JFTOC: In-house orderwire

- Generate Reports: Stand-alone PC

- Close-out Records Upon Resolution: Stand-alone PC/Manual

- Produce DOR: Stand-alone PC

- Formulate NCTAMS Trouble Management Strategy: Stand-alone PC/Manual

b.   Hardware

Computers include a mixture of IBM clones using Intel 386 and 486 microprocessors.

c.   Software

The following software is used in the baseline FMS:

- PC Operating System: DOS (mixture of versions)

- Station Logs: Radio Log 5.31 (DOS based, in-house developed)

- SITREP/As-occurring SITREP: DOS Editor/Wordperfect

- DSR: Wordperfect

d.   Data Storage

Reiterating the information provided in Table 4.2., Baseline FMS data stores are a combination of the following:

- Paper File

- Electronic Flat File

2. NOC

a. *NOC Background*

Officially established August 1, 1996, the PRNOC "provides Pacific area commands with seamless access to classified and unclassified information services via Internet protocol (IP) networks." [Ref. 34] A full range of network management services are provided for both the NIPRNet and SIPRNet. Because the PRNOC was just recently stood-up and serves as an IP network service provider, it utilizes fault management technology comparable to a commercial NOC.

b. *Network*

A Windows NT 4.0, Ethernet LAN, run over optical fiber, provides network services within the NOC.

c. *Hardware*

Hardware used by the NOC includes:

- HP TAC IV Workstations

- Sun Ultra Workstations

- Sun Sparc Workstations

- CISCO 4000 and 7000 series routers

d. *Software*

Software used by the NOC includes:

- NMS: Cabletron Spectrum

- Help Desk Application: Remedy AR System 3.0 with UNIX flat files for database support and configured for automatic trouble ticket generation.

The implementation of a NMS and help desk application in the NOC created a paradigm shift within N3. Through use of the help desk application, AR

System, and its Web interface, AR Web, the NOC generates/receives three different types of trouble tickets: (1) tickets generated by fleet units using the Web interface via a SIPRNet Web homepage, (2) tickets created from the NMS, or (3) tickets generated manually by NOC personnel. Since trouble tickets contain a record of all actions taken to resolve an outage, NOC personnel soon realized that creating a trouble ticket, generating a SITREP, and making a station log entry creates three copies of the same information. Division officer/department head discussions regarding this duplicated effort agreed that the NOC could submit trouble tickets to the JFTOC instead of SITREPs.

E.   CLASSIFIED LAN IMPLEMENTATION

1.   Background

Information regarding NCTAMS EASTPAC's classified LAN implementation was provided via telephone interview with the NCTAMS EASTPAC Maintenance Division Officer who is currently managing the project. The command is in the process of installing a classified LAN to facilitate communication between N3 divisions, between N3 and the CO/XO (who are located in a different building), and with external entities. Examples of future use include: classified message traffic dissemination (e.g., COMSPOTs), internal classified e-mail connectivity, and external e-mail capability via the SIPRNet. The target completion date for implementation in N3's building is August 1997. Connectivity to the CO/XO's building will require installation of an National Security Agency (NSA) approved encryption device. CO/XO connection to the classified network has a target date of September 1997.

2. Design

Classified LAN design is planned as follows:

- Cable Plant Technology: Optical Fiber

- Physical Plant Architecture: Star wired to a single server.

- Data Link Technology: Ethernet

- Architecture: Client/server

- Server: Centralized

3. Hardware

Classified LAN hardware is planned as follows:

- Server: One (1) low end server (P166, (2) 2.1 GB SCSI hard drives, 64 MB RAM)

- Clients: Ten (10) (P166, 2.1 GB IDE removable hard drive, 32 MB RAM)

- Hub: 10 Mbps Ethernet (Low speed hub chosen due to small number of client machines and cost constraint.)

- Existing Hardware: SIPRNet router to be connected to server using fiber run.

4. Software

Classified LAN software is planned as follows:

- NOS: Windows NT 4.0

- E-mail: MS Exchange

- Office Automation: MS Office

- Web Browser: MS Explorer

- AUTODIN Message Dissemination: Message Dissemination Subsystem

(MDS)

5. Physical Configuration

Classified LAN physical configuration is planned as follows:

- Location of Server: JFTOC

- Location of Nine (9) Client Machines:

  - N3 Front Office

  - Tech Control Deck

  - Message Services Admin

  - Message Services Deck (for classified message traffic upload)

  - NOC Admin

  - Maintenance Division

  - JFTOC Deck

  - JFTOC Admin Office

  - CO/XO

6. Administration

Classified LAN physical configuration is planned as follows:

- Network administration will be performed by NOC personnel.

- Users of each workstation will be determined by the appropriate department head/division officer based upon security clearance and need to know.

F. SUMMARY

The Baseline FMS is essentially a manual, non-networked system dominated by electronic flat file and paper data stores. Its processes produce identifiable output in the form of reports such as the DSR, DOR, and COMSPOT. The implementation of automated fault management tools in the NOC and installation of a classified network within N3 suggest types of technology that might be part of a target architecture.

V. DETERMINING THE TARGET SYSTEM

A. INTRODUCTION

This chapter covers the fourth step of the TAFIM process, Determining the Target System. Chapter IV established the character and state of the Baseline System as essentially manual with stand-alone components. To describe the desired system, first, a goal architecture is presented through the use of a vision statement, objectives, and macro architecture. Second, problem constraints are discussed and quantified. Next, the Target System is examined, and its association with Business Process Reengineering (BPR) principles is explored. Finally, required capabilities of a help desk application in the target system is introduced.

B. GOAL ARCHITECTURE OVERVIEW

1. Vision

A vision is a broad statement that states the qualitative goals for the system at some point over the horizon. [Ref. 62:p. 3] In formulating a system vision, an organization must ask, "What do we want the system to look like in "X" number of years?" Due to the rapidly evolving nature of information technology in general, and the help desk software market in particular, the author defined "X" as three years. Additionally, the organization must ask, "Does the system's vision support the vision and doctrine of the organization as a whole?" Figure 5.1 shows a system vision statement developed from establishing the problem framework, defining the system problem, and assessing the baseline system. The vision must be reviewed periodically during the target

system determination step to ensure that actions remain true to this over-arching goal. [Ref. 62:p.3]

TARGET SYSTEM VISION STATEMENT

In order to meet the United States Navy's demanding information needs of the 21st century, the JFTOC, the hub of telecommunications management for each region, requires an effective fault management system. This information system must provide troubleshooting, coordination and fault resolution information to both providers and users of NCTC information services. Data flows and formats should not require specialized user training. Ultimately, the system must integrate with a network management system that provides centralized, integrated and secure management of all information systems, regardless of platform or protocol.

Figure 5.1. Target System Vision Statement.

2. Objectives

Objectives are the broad goals that the system must achieve to be productive. [Ref.62:p. 12] Figure 5.2 displays objectives for the target system. These qualitative aims are drawn largely from the vision statement, above, and from DOD doctrine and policy discussed in Chapter II.

TARGET SYSTEM OBJECTIVES

Primary Objective:
To provide a centralized and accessible source of near real-time fault management information for providers and users of NCTC information services.

Secondary Objectives:
- To demonstrate to customers that positive action is underway to correct faults and restore information services.
- To facilitate information exchange between NCTAMS and customer personnel about actions taken toward diagnosing and correcting faults.
- To enable automated selective retrieval of fault management information.
- To integrate log keeping functions performed by each NCTAMS operations work center.
- To allow performance trend analysis to identify systemic problems.

Figure 5.2. Target System Objectives.

3.   Macro Architecture

The macro architecture is an arrangement of the elements or components that comprise the target system and their interaction. [Ref. 62:p. 9] Figure 5.3 shows a macro architecture for the Target FMS.
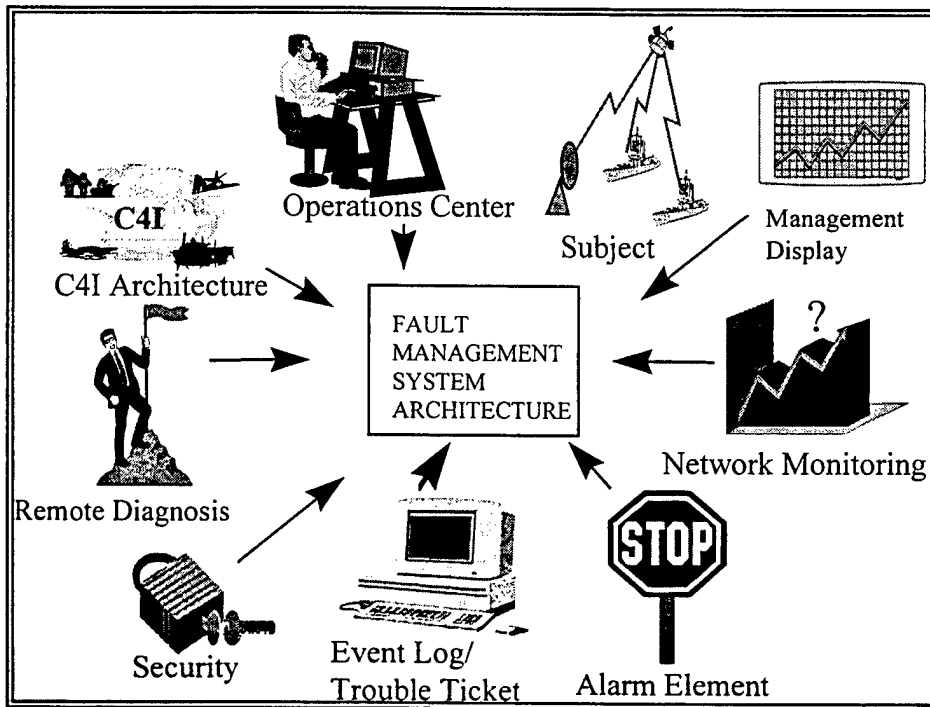
Figure 5.3. FMS Macro Architecture. [Ref. 40:p. 10]

a.   *Subject*

The subject is the information system that the network monitoring element watches. A cross-section of the telecommunications services currently monitored by a NCTAMS includes: RF links (e.g., EHF, SHF, UHF), IP network services (e.g., SIPRNet, NIPRNet), messaging services (e.g., NAVCOMPARS, CUDIXS, VERDIN/Integrated Submarine Automated Broadcast Processing System (ISABPS), voice services (e.g., Plain Old Telephone Services (POTS)), and video teleconferencing services (Video

Information Exchange System (VIXS)). Telecommunications services of the immediate future would also include: DMS, DISN End-User Services, and integrated Defense Information Infrastructure (DII) services.

b. Network Monitoring

The network monitoring element uses C4I architecture to query management agents in individual devices, such as routers and bridges. Responses are compared against the alarm elements' established alarm activation thresholds to determine if alarm generation is required. After each query, the network monitoring element updates a configuration database which stores information about the status of each subject. Additionally, the network monitoring element provides updates to a performance database which tracks overall utilization of network resources. [Ref. 24:p. 553]

c. Management Display

The management display element gives a representation of the network's configuration, the status of all network elements (subjects), and information received from the fault detection element. The display must be user-friendly and allow operations center personnel to "drill-down" to obtain greater detail on a specific network component. [Ref. 24:p. 553]

d. Alarm Element

The alarm element uses the polling information generated by the network monitoring element and compares that data against defined, alarm thresholds to determine if generation is required. If an alarm is generated, the system must process the alarm which may include automatic trouble ticket generation, notification of operations

center via paper or other actions. Alarm processing may also include fault severity level classification using categories such as minor/major/critical or class 1/class 2/class 3. [Ref. 24:p. 553]

e.   *Event Log/Trouble Ticket*

Event logging occurs when an abnormal condition (e.g., outage or degradation of service) is reported. Logging may be initiated as a result of: (1) alarm element (automatic generation), (2) customer notification via the C4I architecture, or (3) operations center personnel action using a network monitoring element. Once the problem is determined to be legitimate, the trouble ticket is opened. Trouble tickets are retained in the trouble ticket database for performance analysis and report generation. Because the event log consists of data base records, reports may be generated on specific faults or for specific periods of time (e.g., a 24-hour period). [Ref. 24:p. 553]

f.   *Remote Diagnosis*

The remote diagnosis element attempts to identify the cause of the fault using information from the configuration database and from tests performed via the network monitoring element. If a diagnosis is made, it is displayed to operations center personnel via the management display. If fault correction is achieved, diagnostic information should be documented in the event log/trouble ticket. The boundaries of the network monitoring system may prevent a remote diagnosis. If this is the case, other elements of the C4I architecture will be used to diagnose and correct the fault. [Ref. 24:p. 553]

g. Security

The security element controls access to services and resources via the network management system. Security management tasks may include: authenticating network management system users, preventing outside users from accessing certain network management services, and auditing access of network resources and services for evaluation of security policies. [Ref. 24:p. 553]

h. C4I Architecture

The C4I architecture, DISN, is the backbone which connects each information system (subject). The network monitoring and remote diagnosis elements function via this architecture. In addition, DISN is used for communication and coordination between operations center and user personnel who manage the network.

i. Operations Center

The Operations Center hosts the people who manage the C4I resources and who interact with the users of those resources. They utilize the network monitoring, management display, alarm element, event log/trouble ticket, remote diagnosis and security elements to manage the network.

C. TARGET SYSTEM PROBLEM FORMULATION MODEL

Chapter III introduced a formulation model that incorporated the basic criterion and constraints that will be used to solve the problem. That template, presented as Figure 3.6, provided four types of constraints: system quality, information quality, technology, and existing information infrastructure.

In this section, specific constraints within each category are presented, and where appropriate, values are quantified based upon responses to a questionnaire completed by

78

a group of NCTAMS EASTPAC users. Based upon only 13 responses, these values are not statistically significant, but they illustrate a valid methodology for obtaining such quantities. The questionnaire included 19 multiple choice questions about different aspects of system and information quality. Questionnaires were completed by N3 personnel in the following billets or positions: Department Head, Division Officers, and JFTOC JWOs. The author's experience of working at a NCTAMS was used as a "reasonableness" check to questionnaire responses; it is noted below where the author disagrees with survey responses. Figure 5.4 shows the Detailed Problem Formulation.

1. System Quality

a. *Availability*

Availability is a measure of the degree to which a system is "in an operable and committable state at the start of an (operation) when that (operation) is called for at a random time." It is calculated by dividing Mean Time Between Failure (MTBF) by the sum of MBTF and Mean Time To Repair (MTTR). [Ref. 19] Seventy-seven percent of responses indicated that availability needs to be greater than or equal to 95 percent (or available 57 out of every 60 minutes).

b. *Response Time*

Response Time is a measure of the time it takes for the system to respond to user commands. Ninety-two percent of responses indicated that response time needs to be less than or equal to five seconds.

MINIMIZE SYSTEM COST (Over Its Life Cycle)

Subject To

(1) *System Quality*
   Availability >= 95%
   Response Time <= 5 seconds
   Data Import Speed <= 30 minutes
   Data Export Speed <= 10 seconds
   User Interface Assistance = Input screens provide choice of proper entry or example.
   Ease of Use = User must be proficient and comfortable with Windows and Web browsers.
   Input Source Identification = System automatically records and displays Zulu time and operator's initials for each entry.
   Information Pull/Report Generation = System produces SITREPs, logs, statistics and on demand responses from user queries.
   Information Access Privileges = System assigns privileges by group and individual user.
   Information Views = System provides capability to limit which fields can be viewed by personnel outside the command.
   Security = Sufficient security is provided by SIPRNet Web page which allows access to authorized users who perform correct login and password sequence.
   Scalability >= 30 users per NCTAMS
   Desktop Network Access = Users must have access to classified LAN at their work station.
   Training Support = Contractors perform a minimum of eight hours on-site training for all operators.
   Maintenance Support = Maintenance provided by qualified maintenance department watch stander in each section. (Author Caveat: also need vendor support contract.)

(2) *Information Quality*
   Information Timeliness (time between updates) <= 30 minutes
   Information Relevance = System includes outage information including cause of outage and estimated time to repair. (Author Caveat: Add latest corrective action taken.)

(3) *Technology*
   Help Desk Software
   Other Hardware and Software

(4) Existing Information Infrastructure/Policy
   DISN
   Classified LAN
   NMS
   COTS Usage
   IT-21 AIS Standards

Figure 5.4. Detailed Problem Formulation.

c.   *Data Import Speed*

This a measure of the rate at which data are entered into the system once received. One hundred percent of responses indicated that data import speed needs to be less than or equal to 30 minutes.

d.   *Data Export Speed*

This refers to the rate at which data is retrieved from the system once a command is executed.   Seventy-seven percent of responses indicated that data export speed needs to be less than or equal to 10 seconds.

e.   *User Interface Assistance*

User interface assistance connotes the level of help that the user interface provides to ensure that appropriate data are entered in each field. One hundred percent of responses indicated that input screens need to provide a choice of proper entries or examples.

f.   *Ease of Use*

This constraint refers to the level of user computer proficiency required to operate the system. Eighty-five percent indicated that users need to be comfortable with using Windows and WWW browser applications.

g.   *Input Source Identification*

This refers to the information that the system automatically records and displays for each log/trouble ticket entry. One hundred percent of the respondents indicated zulu time must be included and 77 percent indicated that they would also like to see the operator's initials recorded.

h. Information Pull/Report Generation

This constraint refers to the type of reports that the system produces on - demand. Eighty-five percent indicated they would like SITREPs, logs, statistics, and response to user queries to be available on demand.

i. Information Access Privileges

Information access privileges refers to the level at which the system assigns and enforces read, write, and other user privileges. Ninety-two percent of responses indicated assignment of privileges at the group and individual level.

j. Information Views

Information views refers to the ability of the system to produce different "snap-shots" of data for different users. Seventy-seven percent of responses were either neutral or agreed that the system needs to limit which fields are viewable by personnel outside the command.

k. Security

This constraint refers to type of security required to protect the system from unauthorized access. Sixty-two percent of respondents indicated that sufficient security is provided by a SIPRNet Web page that allows access by authorized users who perform a correct login and password sequence.

l. Scalability

Scalability refers to the ability of the system to "grow" to accommodate additional users, hardware, or software either co-located or globally distributed from the original system configuration. One hundred percent of respondents indicated that all N3 Watch Supervisors are potential system users. Other potential users recognized by

respondents included: N3 Department Head and Divos (92%), N3 Leading Chief Petty Officers (LCPOs) (85%), CO/XO (54%), and all N3 watch standers (54%). Based upon the author's understanding of NCTAMS operations and discussion with senior N3 leaders, the author believes the system must support at least 30 workstations/30 users at each NCTAMS. The scalability of the system must also support up to 1000 users as the system expands to the Area IMSC level. This estimate is based on 30 users at 24 sites (3 NCTAMS, 15 NCTSs, 3 NCTAMS DETs, and 3 NAVCOMTELDETs) plus a rounding factor to allow for growth. [Ref. 30:p. 3-1]

m. Desktop Access

Desktop Access refers to the ability of a user to access the system, via a classified LAN, from a desktop PC or workstation. Ninety-two percent of responses indicated that users of the system must have desktop access.

n. Training Support

This constraint concerns the type and location of training that accompanies system implementation. Sixty-one percent of respondents selected on-site, contractor-conducted training for all operators as their number one training choice. The next most popular option, contractor conducted on-site training for trainers only, was ranked number one by only 23 percent of respondents. Seventy-seven percent of responses indicated a need for at least one full day of training.

o. Maintenance Support

Maintenance refers to the accessibility and location of maintenance personnel. Sixty-two percent of respondents selected having a system qualified Maintenance Department (N6) watchstander in each watch section as their number one

maintenance choice. The next most popular option, qualified day worker on 24 hour recall, received the number one ranking from only 23 percent of respondents. The author notes that vendor support would also be required for system problems that are beyond the troubleshooting capability of command technicians.

2. Information Quality

a. *Information Timeliness*

This constraint refers to the maximum time between data updates to ensure current information is available to decision-makers. Eighty-five percent of responses indicated the need for updates no later than every 30 minutes.

b. *Information Relevance*

JP 6-0 defines information relevance as, "information that applies to the mission, task, or situation at hand." [Ref. 18:p. I-5] The questionnaire asked respondents to rank five items in the order of the information most commonly requested by customers; two items emerged as dominant responses. Thirty-eight percent of respondents selected cause of outage as either their number one or number two choice for relevancy. Likewise, 35 percent of respondents selected estimated time of repair as either their first or second choice. Although, latest corrective action taken received only eight percent of the number one and two rankings, the author believes that this item is of equal relevance.

3. Technology

a. *Help Desk Software*

The current functionality of help desk technology was reviewed in Chapter III. The capabilities of these applications at the time of target system implementation is a constraint.

b. *Other Hardware and Software*

Without going into specific details, the performance capabilities of each target system hardware and software component, at the time of implementation, are considered a constraint.

4. Existing Information Infrastructure/Policy

a. *DISN*

"A sub-element of the DII, the DISN is the DOD's consolidated world-wide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations." [Ref. 8:p. 2-1] SIPRNet is DISN's data network for Confidential and Secret information. Use of the DISN is one element of the Vision for DOD Information Technology expressed in the TAFIM. [Ref. 9] Use of the SIPRNet is, therefore, considered a constraint.

b. *Classified LAN*

An FMS requires a secure network, because outage information about afloat units is classified. Since NCTAMS receives classified message traffic daily, a secure LAN for DMS organizational and personal e-mail will be a requirement. Therefore, an existing classified LAN is considered a constraint. NCTAMS EASTPAC's classified LAN will be used in the next chapter in a migration path illustration.

c.   *NMS*

Both the PRNOC at NCTAMS EASTPAC and the Unified Atlantic Region Network Operations Center (UARNOC) at NCTAMS LANT, utilize Cabletron Spectrum as their NMS.

d.   *COTS Usage*

The Federal Acquisition Regulation, TAFIM, and IT-21 strategy all stress the use of COTS IT products, whenever, they are available to meet DOD's IT requirements. [Ref. 11, 9 and 4] COTS usage is, therefore, considered a constraint.

e.   *IT-21 AIS Standards*

Chapter II contains the IT-21 AIS standards.

D.   TARGET SYSTEM DFD

> It is time to stop paving cow paths. Instead of embedding outdated processes in silicon and software, we should obliterate them and start over. We should "reengineer" our business processes in order to achieve dramatic improvements in their performance. [Ref. 13:p. 104]

These words, written by Michael Hammer in his 1990 ground-breaking article, "Reengineering Work: Don't Automate, Obliterate", introduced the technique of BPR. During the past decade, it has become one of the most frequently discussed methods for improving organizational performance.   Its popularity "stems from its promise of achieving high levels of improvement in cost, quality, and timeliness..." [Ref. 12:p. 12]

In this section. DFDs for a target system are presented which were developed using the guidance of Hammer's Principles of Reengineering.   These axioms include [Ref. 13:pp. 109-112]:

• Organize around outcomes, not tasks.

- Have those who use the output of the process perform the process.

- Treat geographically dispersed resources as though they were centralized.

- Link parallel activities instead of integrating their results.

- Capture information once and at the source.

Although this target system was developed using BPR axioms, the redesign did not use the method espoused by both Hammer and Gerald Hoffman; use of a team who understands the entire process from many different points of view. [Ref. 13:p. 108],[Ref. 17:p. 84] Without the insight of team members, the author's intention is to provide one possible option for a reengineered target system.

1.   Level Zero Diagram

Figures 5.5 and 5.6 show the Target System Level One Diagram. The following discussion provides insight into the methodology used to model the Target System. A detailed description of each process will be provided in the next subsection with each Level One Diagram.

a.   *Processes*

The nine Baseline System processes are reduced to seven in the Target System. Baseline System Processes Two and Three are combined into a single Target System Process Two. Instead of making a log entry to a stand-alone file, outage information is recorded to the trouble ticket, i.e. capturing information once at the source. Similarly, Baseline System Process Five is eliminated through the replacement of paper SITREPs with continuously updated trouble tickets.
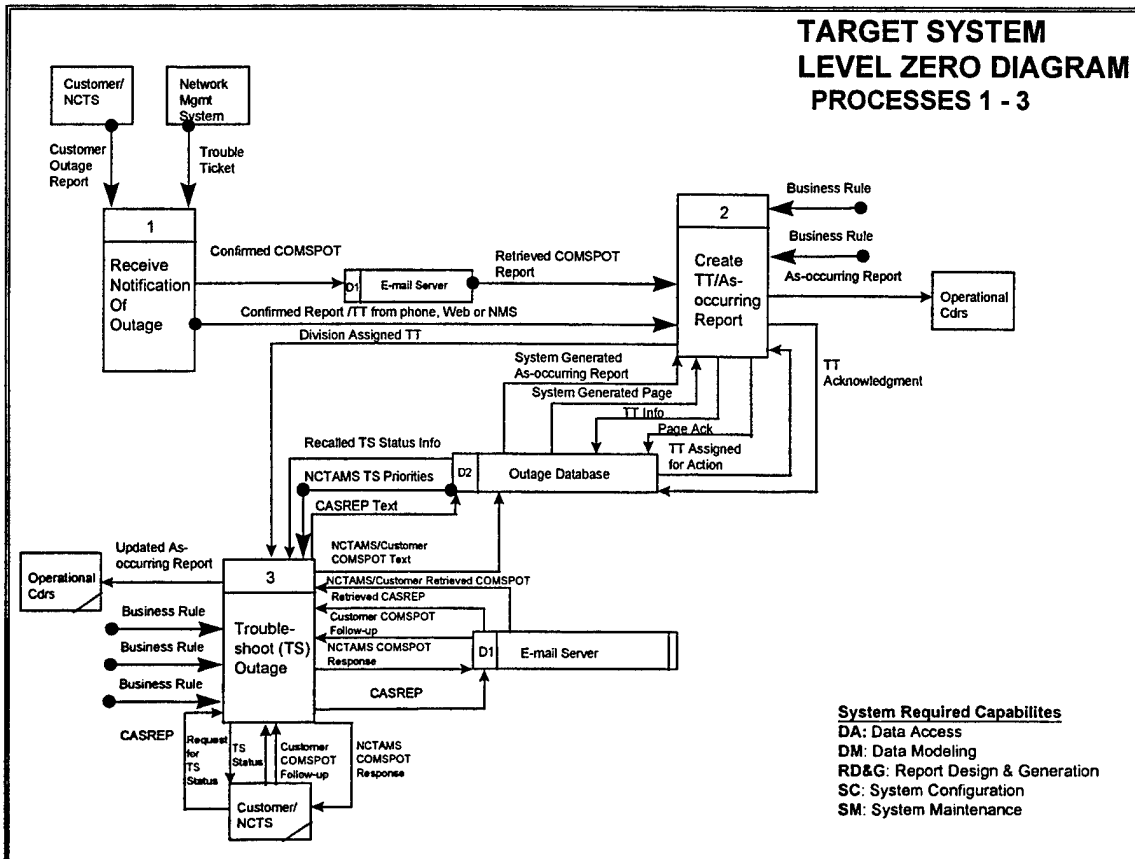
Figure 5.5. Target Level One Diagram: Processes 1-3.

b. External Entities

The external entities are independent of process redesign, and therefore, remain the same.

c. Data Stores

The most dramatic and significant aspect of process redesign occur in the number and nature of data stores. Whereas the Baseline System Level Zero and One Diagrams contained 13 and 20 data stores respectively, the Target System Diagrams contain only two. This marked reduction of 90 percent in Level One data stores is the result of centralizing data storage to a database server and an e-mail file server.
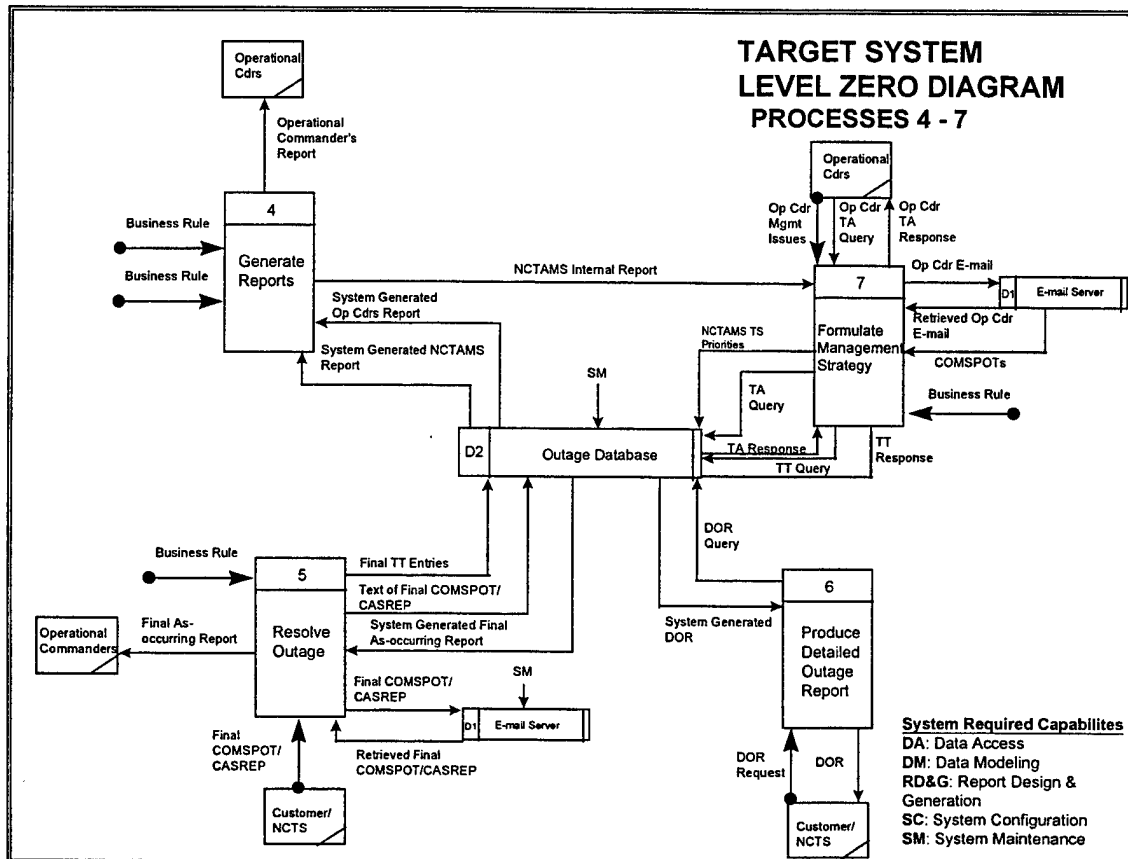
Figure 5.6. Target Level One Diagram: Processes 4-7.

d. *Data Flows*

Data flows will not be individually discussed, however, by comparing the Baseline and Target System Level Zero Diagrams, it is apparent that the number of data flows between processes and data stores is reduced significantly. This reduction results from the use of centralized data storage.

2. Level One Diagrams

Processes One through Five, shown in Figures 5.5 and 5.6, are exploded into child processes to form the Target System Level One Diagrams; these are shown as Figures 5.7 through 5.11. Accompanying each Level One Diagram is a detailed description of each

data flow. Processes Six and Seven, shown in Figure 5.6, are not exploded to a Level

One Diagram, because they do not require further description via sub-processes.

a. *Receive Notification of Outage*

Figure 5.7 shows the Target FMS Process One, Level One Diagram.
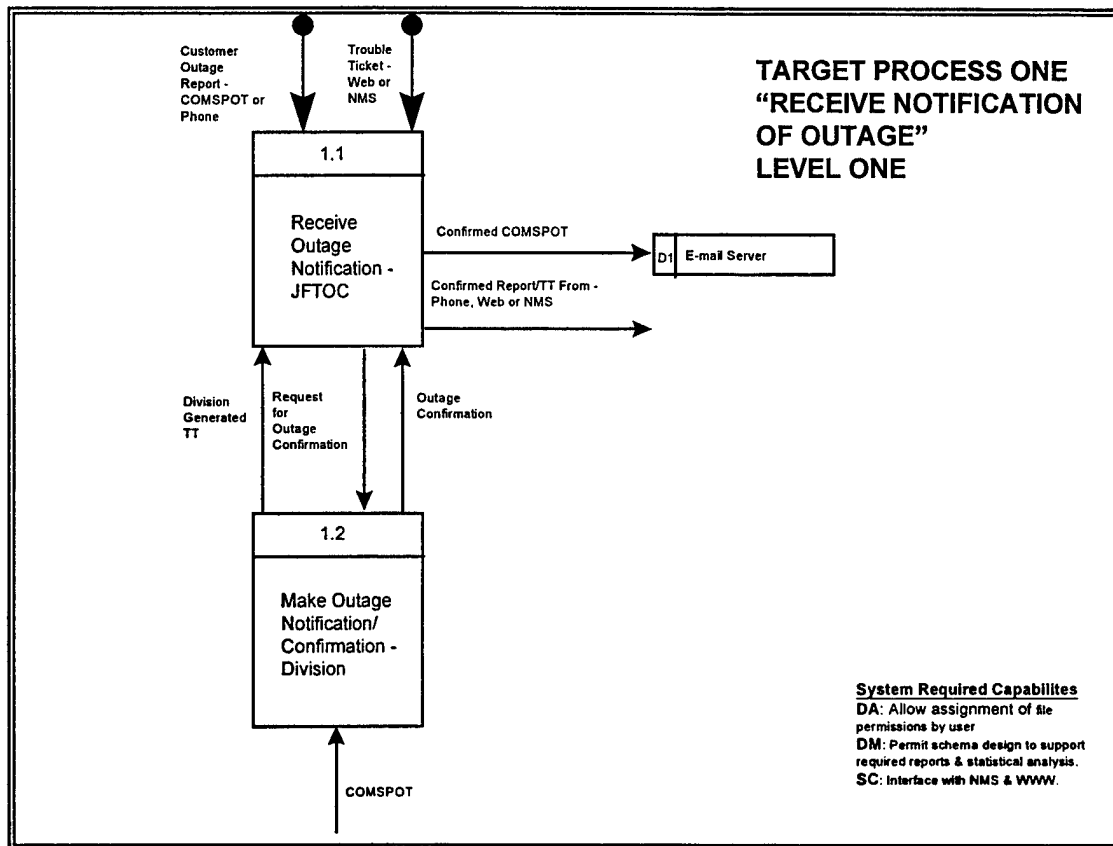
Figure 5.7. Process One: Receive Notification of Outage.

Process 1.1, Receive Notification of Outage - JFTOC, data flows are

described as follows:

- Process One is initiated when JFTOC receives:

  - Customer Outage Report from:

    - Customer (afloat or ashore unit) via COMSPOT e-mail or phone call to 1-800 help desk line.

    - Regional NCTS via e-mail or phone.

- Trouble Ticket (TT) from:

  - Customer, Regional NCTS or Division via SIPRNet Web TT.

  - NMS generated trap data that triggers automatic TT generation.

  - Division Generated TT.

- For Customer and NCTS reported outages, JFTOC sends e-mail to Division to request outage confirmation.

- COMSPOTs received are stored electronically on the E-mail (File) Server.

  Process 1.2, Make Outage Notification/Confirmation - Division, data flows are described as follows:

- Division receives copies of COMSPOTs for information only. Notification via phone and TT are received by JFTOC as central "help desk".

- Division is notified of outages via internal alarms/monitors or via e-mail from JFTOC, Request for Outage Confirmation.

- When notified via internal alarms/monitors, Division sends Division Generated TT.

  * **Assumption**: NCTAMS Business Rule (BR) may require Regional NCTSs and Divisions to send e-mail notifying JFTOC of outage within a given number of minutes and to follow-up with a TT. This requirement would not fundamentally change Process One.

b.   Create Trouble Ticket/As-occurring Report

Figure 5.8 shows the Target FMS Process Two, Level One Diagram.

Process 2.1, Create & Assign TT - JFTOC, data flows are described as follows:

- JFTOC uses information from COMSPOT or phone call to generate TT. Information input may occur using keyboard or microphone via voice recognition software.

- Or. JFTOC takes TT received from NMS or Customer (via SIPRNet Web page) and validates data assignment to all mandatory fields.

- JFTOC assigns TT action to the appropriate Division.

91

• TT is stored in Outage Database.
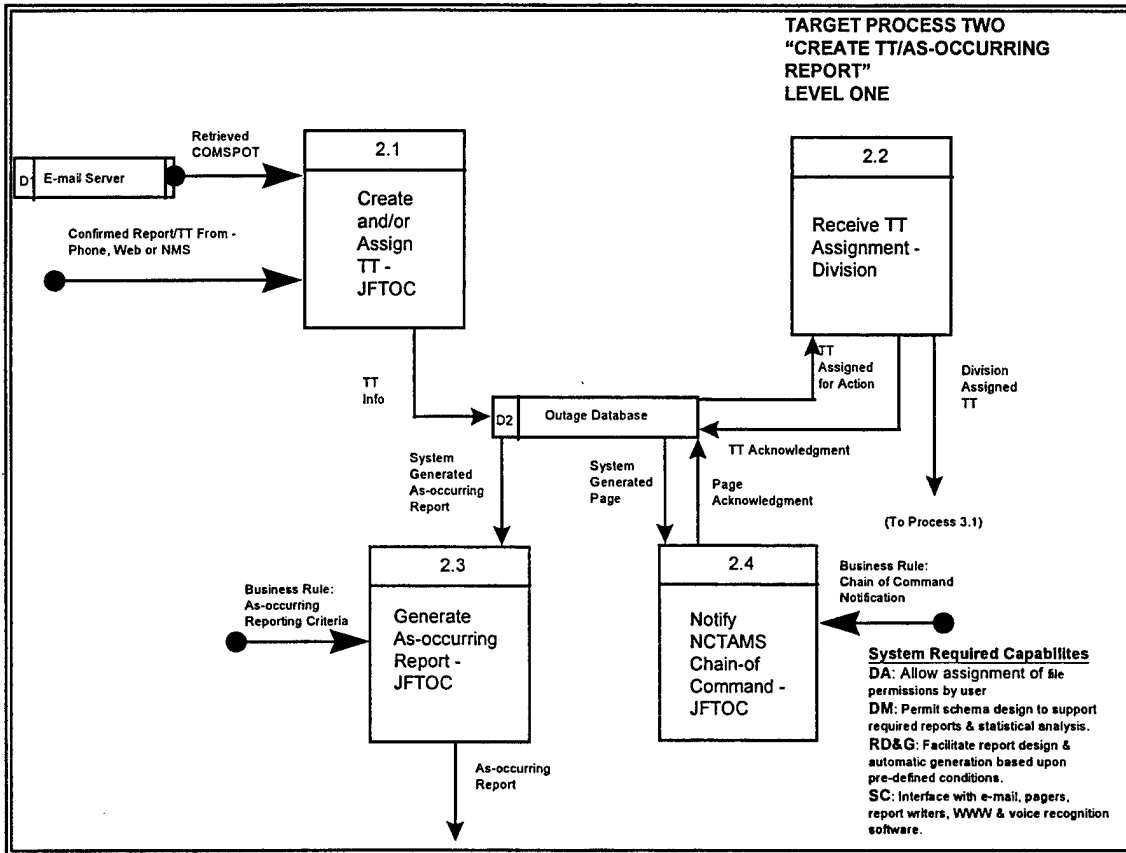
Figure 5.8. Process Two: Create Trouble Ticket/As-occurring Report.

Process 2.2, Receive TT Assignment - Division, data flows are described

as follows:

• Submission of TT to database generates alarm to Division Supervisor's work
station.

• Division receives TT and acknowledges receipt electronically.

• Acknowledgment of TT (Division Assigned TT) begins Process Three.

Process 2.3, Generate As-occurring Report - JFTOC, data flows are
described as follows:

• In accordance with NCTAMS BR on As-occurring Reporting Criteria, if outage
type and elapsed time since start match a pre-defined set of conditions, the

system automatically generates As-occurring Report for Operational Commanders.

Process 2.4, Notify NCTAMS Chain-of-Command - JFTOC, data flows are described as follows:

- If outage type and elapsed time since start match a pre-defined set of conditions, system automatically sends page to designated Chain-of-Command personnel.

- Paged personnel place phone call to system to acknowledge system generated page.

c. Troubleshoot (TS) Outage

Figure 5.9 shows the Target FMS Process Three, Level One Diagram.
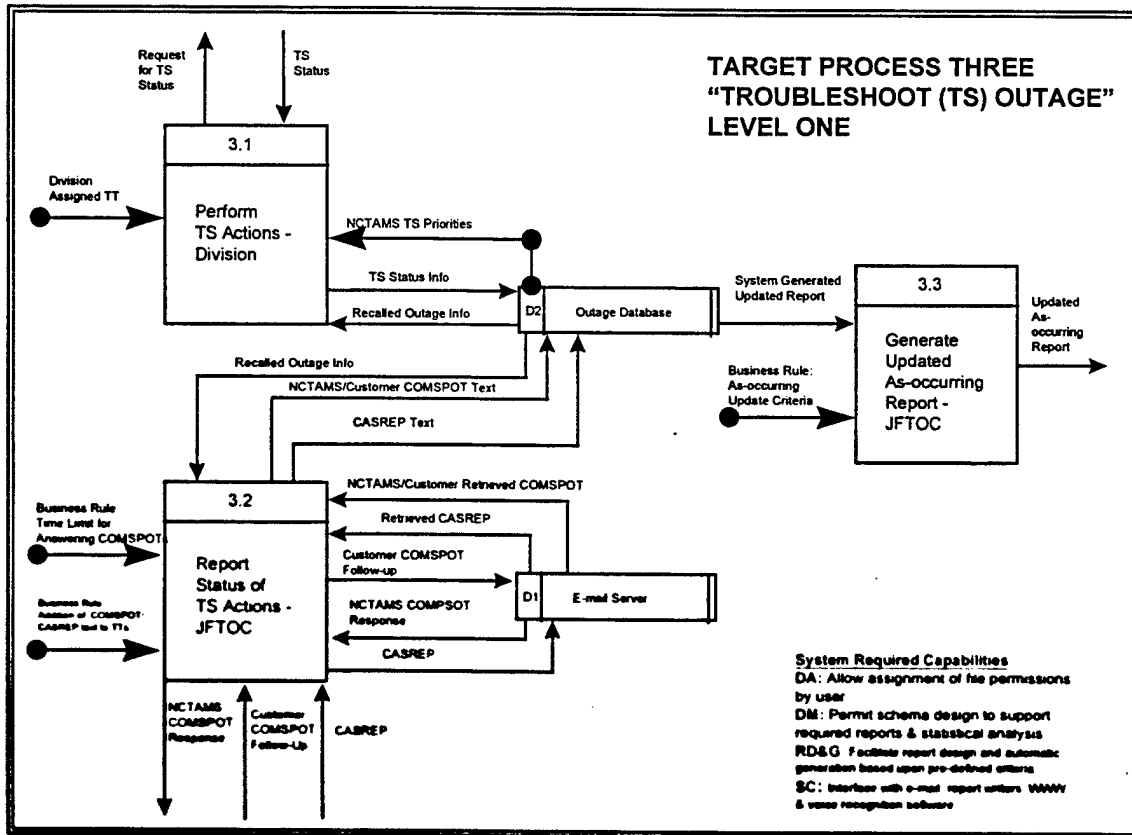
Figure 5.9. Process Three. Troubleshoot Outage.

Process 3.1, Perform TS Actions - Division, data flows are described as follows:

- Process 3.1 is initiated when Division is assigned TT in Process 2.2.

- Division recalls outage info by opening TT file from Outage Database.

- Based on TT status, Division alerts Customer/NCTS via e-mail to access system in order to update TS status via SIPRNet Web page.

- Customer/NCTS accesses system, opens their TT, reads latest NCTAMS TS status, and provides their latest TS status.

- All entries made to TT are written to Outage Database.

Process 3.2, Report Status of TS Actions - JFTOC, data flows are described as follows:

- Process 3.2 is initiated in accordance with NCTAMS BR on Time Limit for Answering COMSPOTs.

- JFTOC recalls outage info by opening TT file from Outage Database.

- JFTOC drafts COMPSOT reply using latest TS info found in TT and e-mails to Customer.

- Based upon NCTAMS BR on addition of COMSPOT/CASREP text to TT, JFTOC launches application which copies COMSPOT text to TT file.

- Likewise, Customer COMSPOT Follow-Up Reports received by the JWO are read and copied to TT in accordance with NCTAMS BR.

- CASREPs received by the JWO are read and copied to TT in accordance with NCTAMS BR.

Process 3.3, Generate Updated As-occurring Report - JFTOC, data flows are described as follows:

- In accordance with NCTAMS BR on As-occurring Reporting Criteria, if outage type and elapsed time since start match a pre-defined set of conditions, system automatically generates Updated As-occurring Report for Operational Commanders.

d. Generate Reports

Figure 5.10 shows the Target FMS Process Four, Level One Diagram.
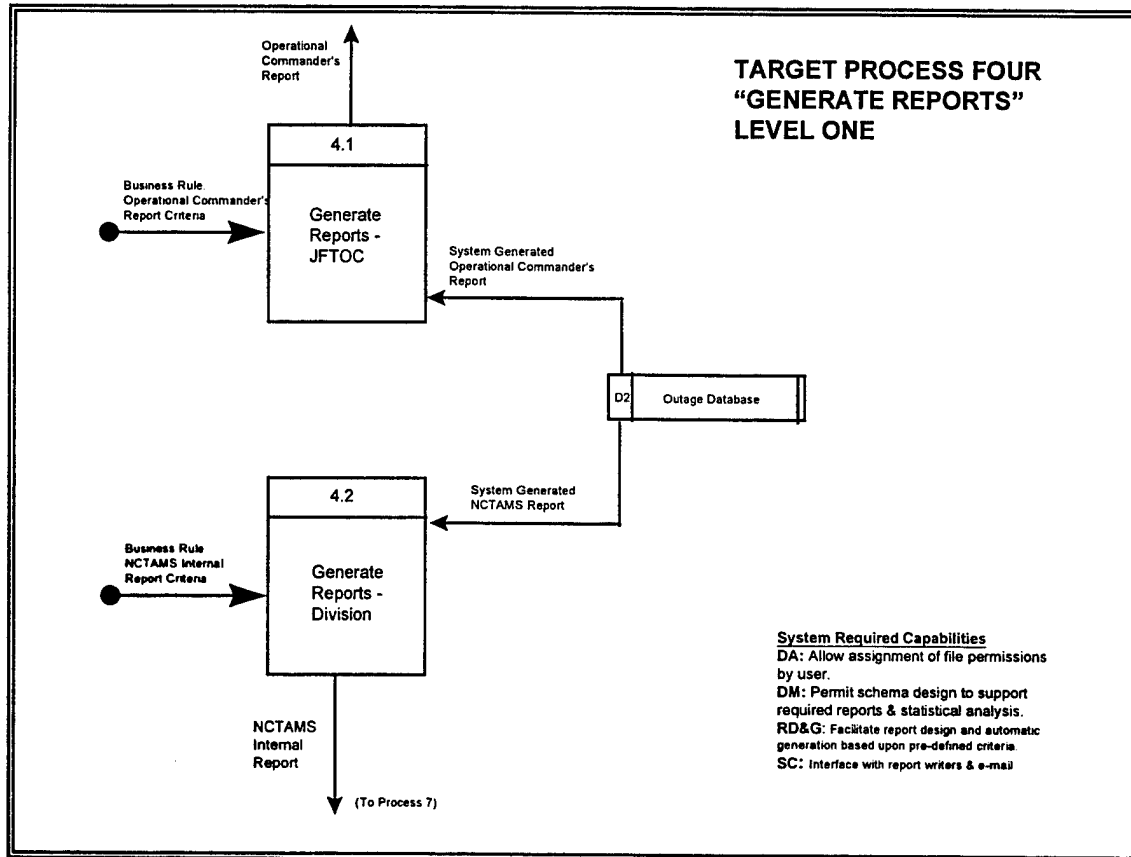
Figure 5.10. Process Four. Generate Reports.

Process 4.1, Generate Reports - JFTOC, data flows are described as follows:

- Process 4.1 is performed in accordance with NCTAMS BR on Operational Commander's Report Criteria.

- At specified time each day, system automatically generates Operational Commander's Report.

Process 4.2, Generate Reports - Division, data flows are described as follows:

- Process 4.2 is performed in accordance with NCTAMS BR on NCTAMS Report Criteria.

- At specified time each day, system automatically generates NCTAMS Internal Report.

e. *Resolve Outage*

Figure 5.11 shows the Target FMS Process Five, Level One Diagram.
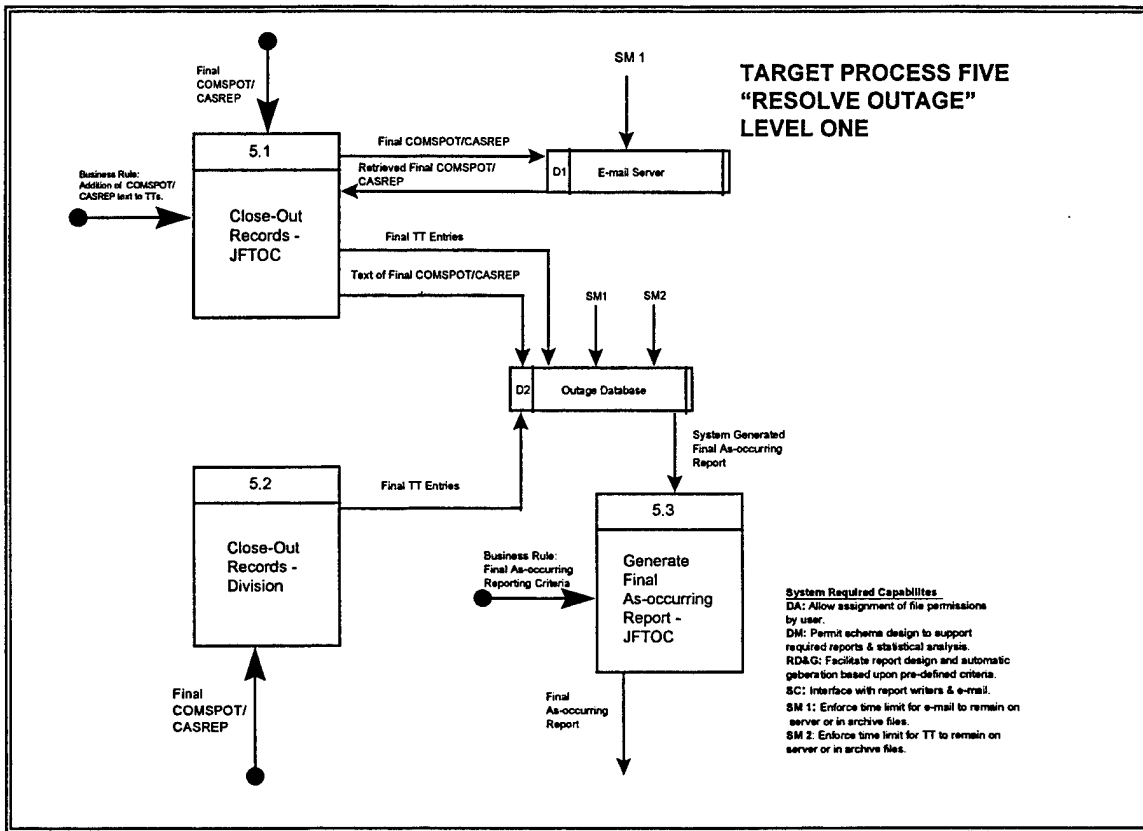
Figure 5.11. Process Five. Resolve Outage.

Process 5.1, Close-Out Records - JFTOC, data flows are described as

follows:

- Process 5.1 is initiated when JFTOC receives Final COMPSPOT and in some cases, Final CASREP, from Customer/NCTS via e-mail.

- In accordance with NCTAMS BR governing addition of COMSPOT/CASREP text to TTs, JFTOC launches application which copies COMSPOT text to TT file.

- JFTOC makes any final entries to TT which are written to the Outage Database.

Process 5.2, Close-Out Records - Division, data flows are described as

follows:

- Division receives copy of Final COMSPOT via e-mail and makes final entries to TT which are written to Outage Database.

Process 5.3, Generate Final As-occurring Report - JFTOC, data flows are described as follows:

- In accordance with NCTAMS BR on Final As Occurring Reporting Criteria, if outage type matches a pre-defined set of conditions and TT status is changed to closed, system automatically generates Final As-occurring Report for Operational Commanders.

f. *Produce DOR*

Process 6, Produce DOR, is not exploded to level one. because sufficient detail is achieved in the level zero diagram, Figure 5.6. Data flows are described as follows:

- Process 6 is initiated when JFTOC receives a DOR via e-mail from a Customer.

- JFTOC specifies outage parameters in pre-formatted report query of Outage Database.

- DOR is automatically generated and e-mailed to Customer.

g. *Formulate Management Strategy*

Process 7, Formulate Management Strategy, is not exploded to level one, because sufficient detail is achieved in the level zero diagram, Figure 5.6. Data flows are described as follows:

- Process Seven is initiated in accordance with the NCTAMS BR on Conduct of Operations Briefs.

- Process Seven also occurs as a result of Operational Commander management issues communicated to NCTAMS via phone or e-mail.

- Operational Commanders query Outage Database for Trend Analysis (TA) information via Web interface.

- Designated NCTAMS managers query Outage Database for TA information.

- Designated NCTAMS managers query Outage Database for active TT information.

- NCTAMS managers review COMSPOT e-mail received as the result of actions performed in Process 4.

- NCTAMS managers review NCTAMS Internal Report produced in Process 4.

- After reviewing COMPSOT e-mail, NCTAMS Internal Report, TA information and active TT status, NCTAMS managers formulate NCTAMS TS Priorities and input priorities to Outage Database.

E. REQUIRED CAPABILITIES OF A HELP DESK APPLICATION IN THE TARGET SYSTEM

Based upon the user assessment and help desk technology review performed in Chapter III as well as the problem formulation model presented in Section C, certain minimum functions are required from a help desk application if used in the Target System. The help desk must:

- Allow expansion of system from a few users at one command to hundreds of users distributed around the world.

- Employ open system architecture to ensure maximum compatibility with existing and future hardware and software assets and tools.

- Integrate with third-party applications to:

  - Initiate trouble tickets automatically by capturing network management events and traps.

  - Initiate trouble tickets via e-mail, phone or SIPRNet.

  - Query or receive trouble ticket status using COTS Web browsers.

  - Enable automatic report generation.

  - Provide automatic notification to designated personnel via outage management system, e-mail or pager.

- Customize user-interface through point-and-click.

- Provide capability to employ multiple schemata (e.g., trouble tickets, asset management, etc.)

- Control access at the user level.

- Initiate events based on a set of conditions and action to occur when conditions are met.

- Provide graphical display of trend analysis and alert threshold data.

- Facilitate user key word search of experience/knowledge databases.

- Manage information service assets.

- Track modifications/changes made to information service assets.

F. HELPDESK ON-LINE INFORMATION SYSTEM (HOLIS) ARCHITECTURE

The author has coined the name HOLIS for the target system. The major components of the HOLIS architecture at the LAN and WAN levels are outlined below.

1. LAN Architecture

Figure 5.12 is a notional view of the Target System LAN Architecture. Network, hardware, and software specifics are provided below.

TARGET SYSTEM LAN ARCHITECTURE
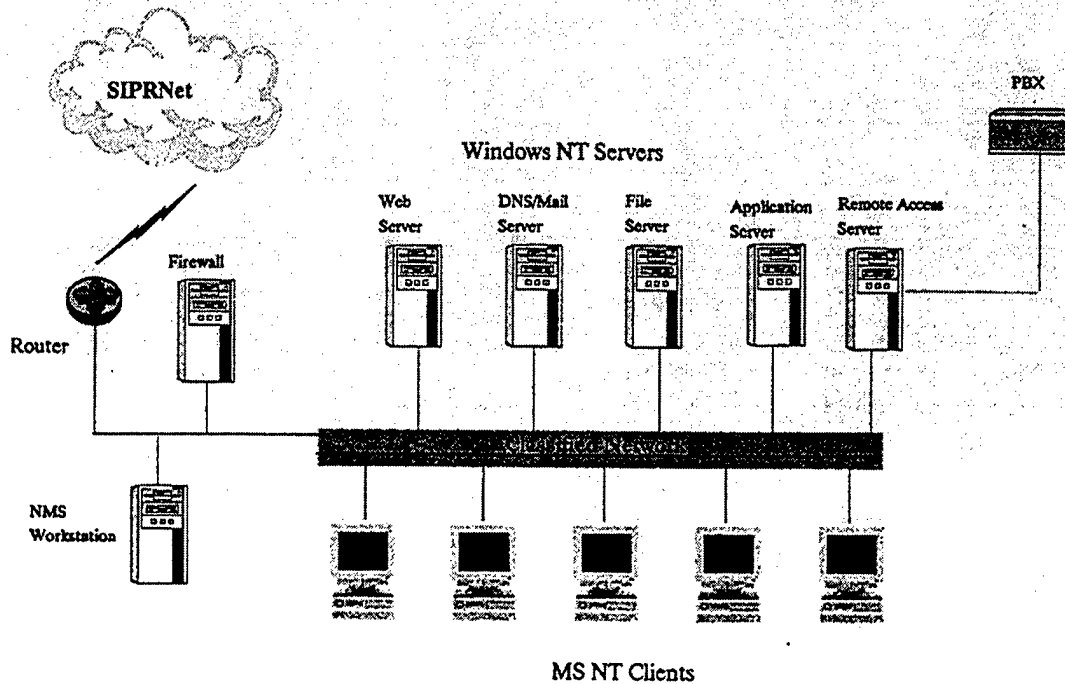
Figure 5.12. Target System LAN Architecture.

a. *Network*

The network may be described as follows:

- Architecture: Client/server (concurs with IT-21 standards).

- Standards: ATM backbone and 100 Mbps Fast Ethernet to the desktop (concurs with IT-21 standards).

- NOS: MS NT 4.0 (concurs with IT-21 standards).

- Certified to process and store classified material.

- Connectivity to SIPRNet via router. The SIPRNet, a component of DISN, serves as the C4I architecture element of the target macro architecture.

- Workstations conveniently located for appropriate Watch Supervisors, Division Officers, Department Heads and CO/XO.

b. *Software*

The software listed below is provided for illustrative purposes only. Due to time constraints, the author did not perform analysis to determine which software products best satisfy the problem formulation model. Software chosen specifically to comply with IT-21 standards are indicated. Notes below provide the author's rationale for inclusion in this illustration. In addition, where applicable, software is related to the target system macro architecture.

Table 5.1. Target System Software.

- Server NOS: NT Server 4.0 (concurs with IT-21 standards).

- Client NOS: MS NT 4.0 Workstation (concurs with IT-21 standards).

- NMS: Cabletron Spectrum (See note 1). The NMS serves as the network monitoring, management display, alarm element, and remote diagnosis elements of the target system macro architecture.

- Help Desk Application (See note 2). The help desk application serves as the event log/trouble ticket element of the target system macro architecture.

    - Remedy AR System Server
    - MS SQL Server
    - MS SQL Client
    - Remedy AR System Client
    - Remedy AR Web Server
    - Remedy Flashboards Server
    - Remedy Flashboards Client

- E-mail: MS Exchange 4.0 (concurs with IT-21 standards).

- Report Writer Client/Server: MS Word/MS Excel from MS Office 97 Professional (concurs with IT-21 standards).

- Remote Notification: Personal Productivity Tools Etherpage (See note 3).

- Voice Recognition: Kurzweil Voice for Windows (See note 4).

Notes:
Note 1: Cabletron Spectrum is used, because it is currently employed by the NCTAMS NOCs.

Note 2: Remedy AR System is used, because it is currently employed by the NCTAMS NOCs and it meets the capabilities requirements for a target system help desk application defined in Section E above.

Note 3: Personal Productivity Tools Etherpage is used, because it is integrates with AR System.

Note 4: Kurzweil Voice for Windows is used, because it is considered one of the top performing voice recognition packages. A review of four top selling applications described it as follows: "Kurzweil Voice for Windows 2.0 offers the best overall performance, with a single mode for hands-free operation and voice dictation and a very accurate recognition engine. It is also hardware-independent." [Ref. 47, p. 550]

c.   *Hardware*

The hardware listed below is also provided for illustrative purposes. Chapter II provided the IT-21 standards for network directory and application/file servers. The specific use of each server and number required will differ between NCTAMS depending on existing LAN hardware. Table 5.2 suggests one possible configuration.

Table 5.2. Target System Hardware.

- SIPRNet Router: Connects HOLIS to the SIPRNet. Allows fleet customers and NCTSs to access the system to submit/query trouble tickets and operational commanders to receive/query outage information.

- NMS Workstation: Hosts the NMS software.

- Servers: All servers host Server NOS software.

- Firewall: Hosts the firewall software. Provides the security element of the target system macro architecture.

- WWW Server: Hosts Remedy AR Web Server software.

- Domain Name Server/Mail Server: Hosts E-mail software and e-mail files.

- File Server: Hosts network files.

- Application Server: Hosts Remedy AR System/AR Web/Flashboards, MS SQL, and Report Writer server software.

- Remote Access Server: Hosts Remote Notification software.

- Client Workstations: Hosts the NOS, MS SQL, Remedy AR System, Remedy Flashboards, Report Writer, and Voice Recognition client software.

2.   WAN Architecture

Figure 5.13 shows the Target System WAN Architecture. Individual components were discussed in Subsection one above.

103

TARGET SYSTEM WAN ARCHITECTURE
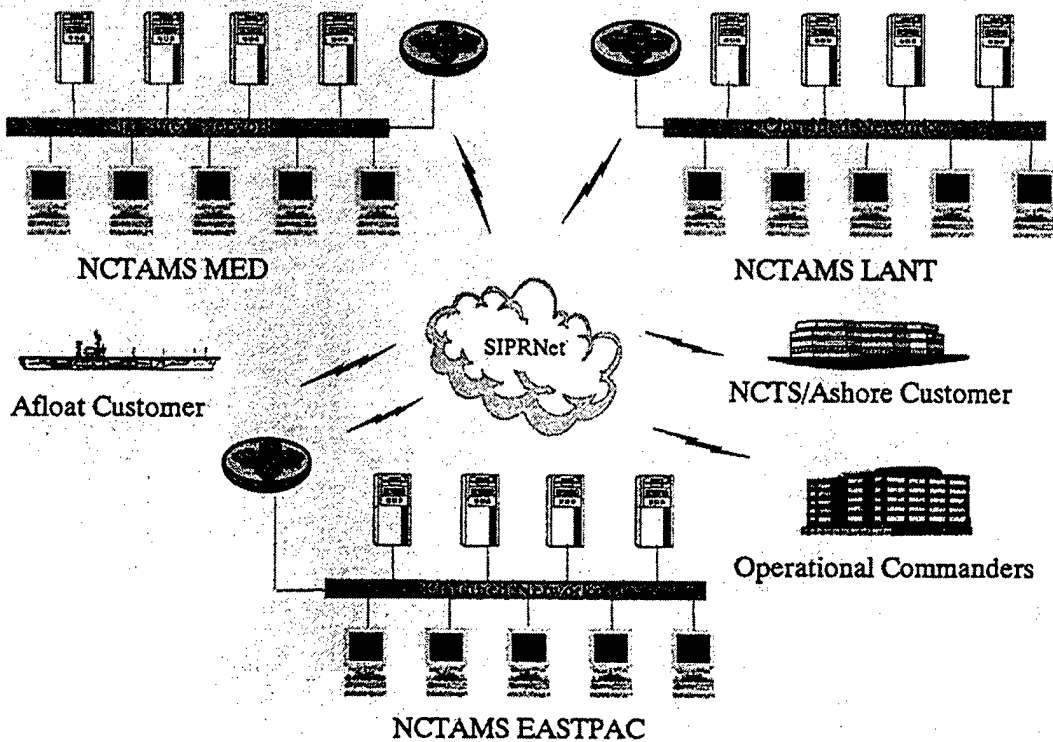
Figure 5.13. Target System WAN Architecture.

G. SUMMARY

Effective and efficient business processes are central to the success of every enterprise. When a company grows significantly or when its business or its markets change, it must change its business processes. [Ref. 17:p. 84]

This quote from Hoffman basically describes the challenge facing the NCTAMS and its FMS. As the role of the NCTAMS JFTOC continues to evolve, it must continuously re-examine its business processes. This chapter outlines a target system to achieve fault management processes in a more efficient and effective manner. Using the problem definition introduced in Chapter III, the Target System was described through a series of steps which incrementally established a basic architecture. This architecture

will be used in the next chapter to develop a migration path from the baseline to the target

system.

VI. DEVELOPING THE MIGRATION PATH CANDIDATES

A.   INTRODUCTION

The fifth step of the TAFIM process, Developing the Migration Candidates, creates several feasible paths for moving from the baseline system, illustrated in Chapter IV, to the target architecture, outlined in Chapter V. In order to develop the migration paths, first, the Remedy help desk software products are examined in terms of product line, functionality, and services offered. Second, the various phase options which comprise each migration path are described. Finally, a timeline and cost breakdown are established for each migration path option.

B.   REMEDY SOFTWARE

The Remedy Corporation has experienced rapid growth since its founding in 1990. Company literature currently reports a total of 3,800 installed sites and a customer base that includes a large number of multi-national corporations such as AT&T, Motorola, Time Warner, and Wal-Mart. [Ref. 51]

In terms of a DOD customer base, DISA has employed AR System in a significant number of network management centers and as part of several major systems. Centers include: Global Operations Security Center (GOSC), the Regional Control Centers in the Pacific, Europe and Western Hemisphere (Columbus, Ohio), and Defense Mega Centers. Systems include: Global Command and Control System (GCCS), DMS, and Joint Defense Information Infrastructure Control System - Deployed (JDIICS-D). Discussion with Remedy's Federal Account Manager also revealed a growing Navy client base including: Navy Medical Command, Navy Management Systems Support

Office (NavMASSO), Naval Surface Warfare Center (NSWC) Dahlgren, VA and Dam Neck, VA, and Bureau of Naval Personnel (BUPERS). [Ref. 47]

In July 1997, Remedy announced that it will be the first help desk vendor to move toward adoption of the DOD COE standard. Remedy will work with Logicon, Inc., a government contractor with experience in the COE standard, to develop a COE compliant version of their AR System for government customers. [Ref. 47]

1. Products

a. AR System

The keystone of the Remedy product line, the AR System, is used to automate internal operations including: help desk, asset management, change management, and defect tracking. It uses a three-tiered client/server architecture, also known as client/server/server. The AR System client serves as the user interface, while the AR System workflow engine and DBMS constitute the two server components. AR System Server is available in a regular and multi-processing server option (MPSO) which allows for more efficient use of server resources. [Ref. 50]

b. ARWeb

ARWeb is a companion product which allows users of popular Web browsers access to the AR System via the Internet. Users are able to enter, query, or modify requests without intervention by help desk personnel. It generates Hyper Text Markup Language (HTML) forms automatically from an AR System schema, therefore, no HTML programming is required. ARWeb is placed behind the firewall and supports all of the permissions established by the system administrator, thus making it safe from

non-authorized access. Since a Web browser is used as the client, ARWeb operation

requires only the server component. [Ref. 45]

c.   *Flashboards*

Another companion product of AR System, Flashboards is coined as "a

dashboard for driving your business". [Ref. 52] It provides a visual display of near real-

time, customizable performance metrics for any data in a AR System schema. Meters

and graphs use a series of colors to alert managers to changes in performance. Displays

may be customized to show current performance compared with historical data (e.g., last

month, last year) to allow trend analysis. Drill-down to more detailed displays or to the

AR System itself is a system feature. Flashboards uses a client/server architecture. [Ref.

46]

2.   Functionality

Tables 6.1, 6.2, and 6.3 provide a summary of AR System functionality.

Table 6.1. Remedy AR System General Features. [Ref. 23]

REMEDY AR SYSTEM FUNCTIONALITY

- **GENERAL FEATURES**
    - Call Management
    - Problem Tracking
    - Inventory Management
    - Training Management
    - External Database Links
    - Custom Screens
    - Windows Client/Server
    - UNIX Client/Server
    - Macintosh Client
    - Messaging
    - Import/Export
    - API Documented
    - Global Modify
    - Ad Hoc Query
    - Full Query
    - Standard Reports
    - Custom Reports
    - Graphic Reports
    - Scanned Images/Pictures
    - Password Security
    - Screen Level Security
    - Field Security
    - Chargeback
    - Customer Access
    - Database Resynchronization
    - Keyword Access

**Table 6.2. Remedy AR System Call Tracking and Problem Management Features.
[Ref. 23]**

REMEDY AR SYSTEM FUNCTIONALITY

- **CALL TRACKING**
  - Call Log/Track
  - Online History
  - Caller Configuration
  - Resolution Steps Log
  - Track Time On Call
  - Track Time to Solution
  - Track History by Caller
  - Track History By Call
  - Track History By Equipment
  - Match Problem To Expert
  - Open Call By E-mail
  - Close Call By E-mail
  - Track Open Calls
  - Track All Actions To Solution

- **PROBLEM MANAGEMENT**
  - Auto Call Escalate
  - Priority Levels
  - Call Assignment
  - Solution Database
  - Alert Incoming Call
  - Alert Escalation
  - Escalation Levels
  - Call Linking
  - Track Recurring Problems
  - System Call Status
  - Problem Analysis Report

Table 6.3. Remedy AR System Problem Resolution, Asset Management, Support Focus and Link Features. [Ref. 23]

REMEDY AR SYSTEM FUNCTIONALITY

- **PROBLEM RESOLUTION**
  - Keyword Search
  - Full Text Search

- **ASSET MANAGEMENT**
  - Standard Configurations
  - Client Specific Configurations
  - Group Level Configurations
  - Inventory Tracking
  - Repair History
  - Purchase Orders

- **SUPPORT FOCUS**
  - External Support
  - Internal Support

- **LINKS**
  - World Wide Web
  - Lotus Notes
  - Network Management
  - Asset Management
  - E-mail
  - Fax/Pager
  - Telephony
  - External Knowledge Bases

---

3.   Services

Remedy also offers a wide range of support services as described below.

a.   Customer Support [Ref. 23]

Purchase of Customer Support also entitles the customer to all Remedy product upgrades at no additional charge. Remedy provides three different plans for customer support: Basic Support, Express Support, and 24 X 7 Support. Both the Basic

Support and Express Support plans offer telephone service between 6:00 am to 5:00 pm, Pacific Standard Time, excluding holidays.

- Basic Support: Includes unlimited support via telephone to assist the Remedy user with product installation and usage. Initial response times from the time of problem notification are not to exceed 24 hours.

- Express Support: Includes same services as under Basic Support plan, but it guarantees initial response will not exceed four hours.

- 7 X 24 Support: Includes around the clock support for mission critical users.

b.   Training

Remedy offers a full range of training classes in two locations: Pleasanton, CA and Columbia, MD.   Training covers all aspects of AR System and companion product design, installation, customization, administration, troubleshooting, and usage. [Ref. 23] An updated list of class descriptions, offering dates and costs is available at [http://www.remedy.com/training/index.htm].   In addition, Remedy also has a training option called Right to Teach where for one license fee, an individual attends one of Remedy's training classes, receives training in instructing that course, and then is certified as an instructor. The license fee provides course materials and updates for one year with no limit on the number of students that may receive the training.   Student workbooks, however, are priced separately. [Ref. 43]

c.   Consulting

Consulting services are available for help desk and other management functions. Services include: requirements analysis, system design, design review, system implementation, data migration, and custom Application Programming Interface (API) programming. [Ref. 23] An updated list of consulting services and prices is available at http://www.remedy.com/consulting.

4. Price

Table 6.4 provides general price information.

Table 6.4. Remedy Product Prices. [Ref. 43]

PRODUCT	PRICE	DESCRIPTION
AR System Server, 3.0 w/MPSO-Windows NT	$9,500	Server and 3 fixed write licenses
AR System Client,3.0	$4,000	5 fixed write licenses
AR System Client, 3.0	$10,000	5 floating licenses
ARWeb Server, 1.1-Windows NT	$12,000	Server
Flashboards Server, 1.2-Windows NT	$5,000	Server and 5 fixed licenses
Flashboards Client, 1.2-Windows NT	$2,500	5 fixed write licenses

C. MIGRATION PATH ASSUMPTIONS

1. Hardware/Software Purchase Requirements

Table 6.5 shows the assumptions made as to whether components of the HOLIS

LAN Architecture are pre-existing or must be purchased.

Table 6.5. Target Architecture Purchase Requirements.

LAN CATEGORY	COMPONENT	PRE-EXISTING/MUST PURCHASE
Network	All	Pre-existing
Software	Help Desk	Must purchase
	Report Writers	Pre-existing
	E-mail	Pre-existing
	Remote Notification	Must Purchase
	NMS	Pre-existing
	Voice Recognition	Must Purchase
Hardware	Firewall Router	Pre-existing
	NMS Workstation	Pre-existing
	Web Server	Pre-existing
	DNS/Mail Server	Pre-existing
	File Server	Pre-existing
	Application Server	Must Purchase
	Remote Access Server	Pre-existing
	Client Workstations	Pre-existing

114

2. Users

Table 6.6 displays assumptions made about the number of AR System, ARWeb, Flashboards, Remote Notification (via alphanumeric pager), and Voice Recognition Software users. AR System users are sub-divided into fixed users, those who do not logout, and floating users, those who login occasionally to check status and then logout. The assumptions of 30 Total AR System users matches the scalability constraint in the problem formulation model. Pager users are assumed to be Department Head and Division Officer personnel. Voice Recognition software is used by Division Watch Supervisors.

Table 6.6. Number of Users.

SITE	FIXED ARS USERS	FLOATING ARS USERS	TOTAL ARS USERS	TOTAL ARWEB USERS	TOTAL FLASHBOARDS USERS	PAGER USERS	VOICE RECOG USERS
NCTAMS EASTPAC	10	20	30	Unlimited	10	8	10
NCTAMS LANT	10	20	30	Unlimited	10	8	10
NCTAMS MED	10	20	30	Unlimited	10	8	10

3. Software Licenses Required

Table 6.7 shows the software licenses required to support the user mix shown in Table 6.6. Based upon discussion with the Remedy Federal Account Manager, the following Remedy license configuration is considered sufficient to support 10 fixed ARS users, 20 floating ARS users, unlimited ARWeb users, and 10 Flashboards users.

Table 6.7. Remedy Product Licenses Required. [Ref. 56, Ref. 43, Ref. 42]

PRODUCT	LICENSE	UNIT	UNIT COST	TOTAL COST
ARS Server, 3.0 w/MPSO-Windows NT	Server and 3 fixed write licenses	1	$9,500	$9,500
ARS Client, 3.0-Windows NT	5 fixed write 5 floating write	2 1	$4,000 $10,000	$8,000 $10,000
ARWeb, 1.1, for Windows NT	Server w/unlimited client access	1	$12,000	$12,000
Flashboards Server, 1.2-Windows NT	Server and 5 fixed licenses	1	$5,000	$5,000
Flashboards Clients, 1.2-Windows NT	5 fixed licenses	1	$2,500	$2,500
PPT EtherPage, 2.91	Per server with 8 pagers	1	$1095	$1095
Kurzweil Voice for Windows	Per client	10	$699	$6990

4. Hardware/Software Compatibility

Remedy WWW site (http://www.remedy.com/CMATRIX/cmatrix.shtml) provides an updated list of combinations of computer platforms, operating systems, database software and protocol stacks which have been tested as compatible with ARS version 3.0. Table 6.8, 6.9, and 6.10 show the compatibility combinations that apply to this illustration. Regarding the database support, the reader is again reminded that time did not permit requirements analysis to determine which application best satisfies the problem formulation model. Both MS SQL Server, 6.5 and Oracle 7.3, Workgroup and Enterprise versions, comply with IT-21/Navy AIS standards as well as Remedy compatibility. The author chose to limit the illustration, however, to MS SQL for simplicity sake.

Table 6.8. AR System, Version 3.0 Server Compatibility Matrix. [Ref. 48]

PLATFORM	OPERATING SYSTEM	DATABASE SUPPORT	MINIMUM REQUIREMENTS
PC Compatibles	MS Windows NT Server, 4.0	MS SQL Server 6.5	32 MB Memory 20 MB Disk

Table 6.9. AR System, Version 3.0 Client Compatibility Matrix. [Ref. 48]

GUI	PLATFORM	OPERATING SYSTEM
MS Windows	PC Compatibles • 386 processor • 16 Color VGA Display • 8 MB Memory (16 recommended) • 4 MB Disk	MS Windows NT 4.0

Table 6.10. Compatible TCP/IP Protocol Stacks. [Ref. 48]

OPERATING SYSTEM	TCP/IP PROTOCOL STACK
MS Windows, NT 4.0	MS TCP/IP Win 32

5. Customer Support

Three customer support plans were introduced above: Basic Support, Express Support, and 7 X 24 Support. Based upon the availability and maintenance constraints of the problem formulation model, the author believes that 7 X 24 is the most appropriate support plan.

6. System Administration

The Target Systems DFD showed system administration/maintenance functions that will be part of the Target FMS Architecture. Traditionally, these functions are performed by a System Administrator. Since HOLIS also includes a DBMS, there are specific database design and maintenance functions that must be performed. The author envisions these duties divided between two people with one performing as System

117

Administrator and the other as Database Administrator (DBA)/Alternate System Administrator. Due to the relatively small size of the system, these would most likely not be full-time positions once the system was fully operational. During schema design, software installation, system configuration, and testing, System Administrator and Database Administrator would be full-time jobs.

7. Training

The author assumes that system implementation requires training for two types of users: System Administrator/DBA and general user. It is recommended that the System Administrator receive training throughout the system implementation process. The specific courses and stages at which these courses should be taken are detailed in the plateau options below. For the DBA, the amount of training required will vary depending based upon past experience. The author assumes that the DBA requires at least some MS SQL Server training. MS Course 750: Implementing a Database Design on Microsoft SQL Server 6.5 is one appropriate course; it is used in the migration path illustration below. Based upon the training constraint of the problem formulation model, it is recommended that the Right to Teach license option be utilized for general user training. One person would attend training at Remedy, receive instructional training, and return to the command to train the 30 system users. This would give the NCTAMS flexibility in terms of structuring and scheduling user training.

D. MIGRATION PATH OVERVIEW

1. Plateaus

A plateau is described by the DOD SBA Planning Guide as stages in the journey from the baseline system to the target architecture; plateaus are designed to achieve

"clusters of business benefit". [Ref. 10:p. 6-5] Figure 6.1 shows how achieving plateaus closes the gap between the Baseline System and Target Architecture.

Plateaus between the Baseline FMS and the Target FMS, may be structured in numerous ways. For example, the Remedy Federal Account Manager recommends a phased approach where all three NCTAMS receive one portion of the system during the same time frame. Once implementation of the first portion is complete, each NCTAMS then receives the next portion. This cycle is repeated until system implementation is complete. [Ref. 7] While this approach has definite benefits in terms of full organizational commitment to system success, the author's plateau design, described below, reflects her experience with system implementation at a NCTAMS. The timeline and cost estimates are purposely conservative.
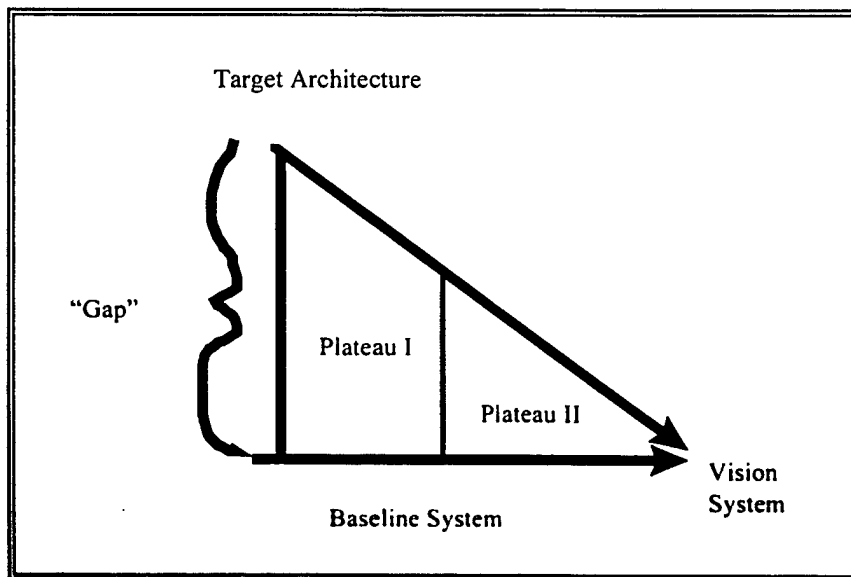
Figure 6.1. Closing the "Gap" Between Baseline and Target Architectures. From [Ref. 10:p. 6-10].

a. *Plateau I*

Plateau I implements the target architecture at NCTAMS EASTPAC. Pilot implementation at a single NCTAMS was chosen for two reasons: (1) To limit the risk associated with unsuccessful implementation (2) To gain requirements analysis, design, installation, training, and documentation lessons learned for later implementation.

b. *Plateau II*

Plateau II implements the target architecture at NCTAMS LANT and NCTAMS MED. Both remaining NCTAMS were grouped into one final Plateau vice two, to benefit from economies of scale and shorten total implementation time.

2. Phases

Each plateau may be sub-divided into one or more phases. Initially, the tasks of Plateaus I and II are assigned to one of three phases: A, B, or C which are described below. Where it was technically and operationally feasible, phases were combined or abbreviated to form other phase options. For example, Phase ABC contains all the tasks of Phases A, B, and C but requires a shorter amount of time to complete. Table 6.11 shows the two options for achieving each Plateau and the phases which comprise these options.

Table 6.11. Plateau Options.

PLATEAU	OPTIONS	A	B	C	AA	BC	ABC
Plateau I	Option I.1.	X	X	X			
	Option I.2.	X				X	
Plateau II	Option II.1.				X	X	
	Option II.2.						X

a.   *Phase A*

Phase A is the first phase in Plateau I. It encompasses the implementation of the AR System and integration of e-mail and report writer software at NCTAMS EASTPAC. The estimated time to complete Phase A is 12 months.

b.   *Phase AA*

Phase AA is the first phase in Plateau II. It encompasses the implementation of the AR System and integration of e-mail and report writer software at NCTAMS LANT and NCTAMS MED. The estimated time to complete Phase AA is nine months. Although it is identical to Phase A, Phase AA is three months shorter, due to the implementation lessons learned during Plateau I, Phase A.

c.   *Phase B*

Phase B is the second phase in Plateau I. It encompasses the implementation of AR Web and integration of NMS and remote notification software at NCTAMS EASTPAC. The estimated time to complete Phase B is six months.

d.   *Phase C*

Phase C is the third phase in Plateau I. It encompasses the implementation of Flashboards and integration of voice recognition software at NCTAMS EASTPAC. The estimated time to complete Phase C is six months.

e.   *Phase BC*

Phase BC is an alternate second phase in both Plateaus I and II. It encompasses the events of Phases A and B. The estimated time to complete Phase BC is six months. Although Phase BC is essentially the same as Phases B and C, it is six

months shorter, due to the economies of scale achieved by performing both phases at the same time.

f. Phase ABC

Phase ABC is an option for Plateau II. It encompasses the events of Phases A, B, and C. The estimated time to complete Phase ABC is nine months; this compares to an estimated 24 months for Phases A, B, and C performed separately, 18 months for Phases A and BC, or 15 months for Phase AA and BC. The significantly shorter time for Phase ABC is attributed to economies of scale by performing all phases at the same time.

3. Migration Paths

A migration path is a feasible path for moving from the baseline system to the target architecture. In the case of the NCTAMS FMS, Plateaus I and II must be achieved to reach the target architecture. As described in the previous Subsection, there are two options for achieving each Plateau. Combining these options, creates four possible migration paths shown in Table 6.12.

Table 6.12. Migration Paths.

Migration Path	I.1.	I.2.	II.1.	II.2.	Months To Complete
1	X		X		33
2	X			X	27
3		X	X		33
4		X		X	27

Figure 6.2 shows migration path phasing. The estimated of length of each phase was described in Subsection 2, above. The rationale behind Option II.1. starting at the 18 month point is to wait until completion of Phases A and B of Option I.1. This means that the AR System and AR Web software would be operational at NCTAMS EASTPAC

prior to beginning implementation at NCTAMS LANT and MED. This would allow time

for system feedback from fleet customers prior to further implementation.
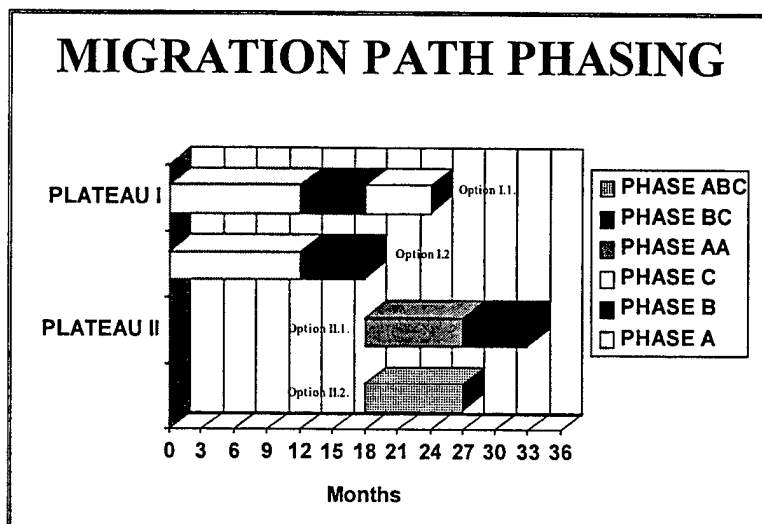
Figure 6.2. Migration Paths Phasing.

E.   PLATEAU I

Per discussion with Remedy Federal Account Manager, the options presented

below represent feasible, albeit conservative, paths for achieving Plateau I.

1.   Option I.1.

Table 6.13 displays Plateau I's two options. Option I.1.phases are highlighted.

Table 6.13. Option I.1.

OPTION	PHASES	EVENT	OPTION 1 TIMELINE	OPTION 2 TIMELINE
I.1.	*Phase A*	*Implement Internally to NCTAMS EASTPAC*	*12 months*	N/A
	Phase B	*Provide Customer Access Via SIPRNet*	*6 months*	N/A
	Phase C	*Implement Management Overview*	*6 months*	N/A
I.2.	Phase A	Implement Internally to NCTAMS EASTPAC	N/A	12 months
	Phase BC	Provide Customer Access Via SIPRNet & Implement Management Overview	N/A	6 months
Total			*24 months*	18 months

a.   *Description*

The phases of Plateau I, Option I.1. may be described as follows:

- PHASE A Description:

  - Implement ARS for use by 30 NCTAMS Classified LAN users.

  - Integrate e-mail and report writer software with ARS.

- PHASE B Description:

  - Implement ARWeb for Customer/NCTS reporting, viewing of outage status and interaction with NCTAMS.

  - Integrate notification software and NMS with ARS and ARWeb.

- PHASE C Description:

  - Implement Flashboards for real-time and historical monitoring of key processes, trend analysis, alert thresholds and user-configured alarms.

  - Integrate voice recognition software with ARS, ARWeb and Flashboards.

b. Timeline

Timelines for Option I.1., Phases A, B, and C are displayed in Tables 6.14, 6.15, and 6.16.

Table 6.14. Phase A Overview (Option I.1.)

EVENT	ACTION	START	FINISH
Requirements Analysis	Remedy	Month 1	Month 1
Procure System: Hardware, Software, Training (Administrator), Installation & Maintenance	NCTAMS	Month 2	Month 5
Database Training -DBA	Contracted Trainer	Month 2	Month 2
ARS Training - Administrator and Trainer	Remedy	Month 2	Month 2
Database Schema Design	NCTAMS	Month 3	Month 5
Hardware Installation	NCTAMS	Month 5	Month 5
Database Software Installation and Configuration	NCTAMS	Month 5	Month 5
ARS Installation, Configuration and Integration	Remedy NCTAMS	Month 6	Month 7
Testing	NCTAMS	Month 8	Month 9
Documentation	NCTAMS	Month 8	Month 9
User Training	NCTAMS	Month 9	Month 11
Begin Operation	NCTAMS	Month 12	N/A
System Support	Remedy NCTAMS	Month 6	N/A

Table 6.15. Phase B Overview (Option I.1.)

EVENT	ACTION	START	FINISH
Procure System: Hardware, Software, Training (Administrator), & Maintenance	NCTAMS	Month 1	Month 3
Advanced ARS Training - Administrator	Remedy	Month 2	Month 2
ARWeb Installation, Configuration and Integration	NCTAMS	Month 3	Month 3
Testing	NCTAMS	Month 4	Month 4
Documentation	NCTAMS	Month 4	Month 4
User Training	NCTAMS	Month 4	Month 5

125

Begin Operation	NCTAMS	Month 6	N/A
System Support	Remedy NCTAMS	Month 3	N/A

Table 6.16. Phase C Overview (Option I.1.)

EVENT	ACTION	START	FINISH
Procure System: Software, Training (Administrator), & Maintenance	NCTAMS	Month 1	Month 3
Flashboards Training - Administrator	Remedy	Month 2	Month 2
Flashboards Installation, Configuration and Integration	NCTAMS	Month 3	Month 3
Testing	NCTAMS	Month 4	Month 4
Documentation	NCTAMS	Month 4	Month 4
User Training	NCTAMS	Month 4	Month 5
Begin Operation	NCTAMS	Month 6	N/A
System Support	Remedy/ NCTAMS	Month 3	N/A

c. Costs

Costs for Option I.1., Phases A, B, and C are displayed in Tables 6.17, 6.18, and 6.19. Table 6.20 shows a one time customer support charge that is not associated with one particular phase but the option as a whole.

Table 6.17. Phase A Costs (Option I.1.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Requirements Analysis • Consultant [Ref.43] • Travel [Ref. 7]	1 consultant 5 nights/6 days	$1,500/day $1,500/trip	5 days 1 trip	$7,500 $1,500
Hardware [Ref. 3]	Application Server	$20,000	1 server	$20,000
Software [Ref. 43]	ARS Server w/MPSO - NT ARS Client - NT 5 Fixed Licenses	$9,500 $4,000 $10,000	1 2 1	$9,500 $8,000 $10,000

126

[Ref. 26]	5 Floating Licenses MS SQL Server 6.5 w/50 client licenses	$8,000	1	$8,000
Training • Administrator [Ref. 43] [Note 1] • Trainer [Ref. 43] [Note 1] • DBA [Ref. 25]	Courses: 1. ARS for Users & Administering ARS from Windows (4days) 2. Req. Analysis, Design & Development (3 days) Travel: 13 nights/14 days ARS for Users: Right to Teach Course Student Workbooks Travel: 3 nights/4 days MS Course 750: Implementing a Database Design on Microsoft SQL Server 6.5 (5 days) Computer Training Academy Honolulu, HI Parking	$1,400 $1,300 $2,550 $6,000 $500/10 pack $1,050 $1775 $10/day	1 person 1 person 1 trip 1 person (3) 10-packs 1 trip 1 person 5 days	$1,400 $1,300 $2,550 $6,000 $1,500 $1,050 $1,775 $50
Installation • Consultant [Ref. 43] • Travel [Ref. 7]	1 consultant 3 nights/4 days	$1,500/day $1,500/trip	3 days 1 trip	$4,500 $1,500
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $27,500	$6,325

Table 6.18. Phase B Costs (Option I.1.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Hardware [Ref. 41]	Pager Rental & Service	$216/year	8	$1,728/yr.
Software [Ref. 43] [Ref. 42]	AR Web,1.1 EtherPage, 2.91	$12,000 $1095	1 1	$12,000 $1,095
Administrator Training • Training [Ref. 43] • Travel [Note 1]	ARS Advanced Topics (5 days) 6 nights/7 days	$1,700 $1,400	1 1 trip	$1,700 $1,500
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $12,000	$2,760

Table 6.19. Phase C Costs (Option I.1.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST

Software [Ref. 43]
 	
[Ref. 56]
	Flashboards
	  Server, 1.2-NT
	  Clients, 1.2-NT
	
	Voice for Windows, 2.0
		
		$5,000
		$2,500
		
		$699
			
			1
			1
			
			10
				
				$5,000
				$2,500
				
				$6,990

Training • Administrator [Ref. 43] [Note 1] • Trainer [Ref. 43]	 Flashboards for Administrators (1 day) Travel: 2 nights/3 days Flashboards for Administrators-	 $400 $900 $6,000	 1 1 trip 1	 $400 $900 $6,000

	Right to Teach (2 days) Student Workbooks	$500/10 pack	3, 10-packs	$1,500
[Note 1]		$1050	1 trip	$1,050
	Travel: 3 nights/4 days			
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $7,500	$1,725

Table 6.20. Option I.1. One Time Charge.

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Customer Support [Ref. 44]	7 X 24 Option - One time charge	$20,000	1	$20,000

Note 1: Travel estimates calculated using the following rates: per diem rate for Alameda County, California of $111.00, rental car rate of $40.00 per day, and airfare from Honolulu, Hawaii to San Francisco, California of $600.00. All rates obtained from the Authorized Federal Travel Directory located at http://www.patsys.com/ftd

2. **Option I.2.**

Table 6.21 displays Plateau I options with Option I.2. phases highlighted.

Table 6.21. Plateau I, Option I.2.

OPTION	PHASES	EVENT	OPTION 1 TIMELINE	OPTION 2 TIMELINE
I.1.	Phase A	Implement Internally to NCTAMS EASTPAC	12 months	N/A
	Phase B	Provide Customer Access Via SIPRNet	6 months	N/A
	Phase C	Implement Management Overview	6 months	N/A
I.2.	*Phase A*	*Implement Internally to NCTAMS EASTPAC*	N/A	*12 months*

	Phase BC	Provide Customer Access Via SIPRNet & Implement Management Overview	N/A	6 months
Total			24 months	18 months

a. Description

The phases of Plateau I, Option I.2. may be described as follows:

- PHASE A Description:

  - Implement ARS for use by 30 NCTAMS Classified LAN users.

  - Integrate e-mail and report writer software with ARS.

- PHASE BC Description:

  - Implement ARWeb for Customer/NCTS reporting, viewing of outage status and interaction with NCTAMS.

  - Integrate pager software and NMS with ARS and ARWeb.

  - Implement Flashboards for real-time and historical monitoring of key processes, trend analysis, alert thresholds and user-configured alarms.

  - Integrate voice recognition software with ARS, ARWeb and Flashboards.

b. Timeline

Timelines for Option I.2., Phases A and BC are displayed in Tables 6.22 and 6.23.

Table 6.22. Phase A Overview (Option I.2.)

EVENT	ACTION	START	FINISH
Requirements Analysis	Remedy	Month 1	Month 1
Procure System: Hardware, Software, Training (Administrator), Installation & Maintenance	NCTAMS	Month 2	Month 5
Database Training -DBA	Contracted Trainer	Month 2	Month 2
ARS Training - Administrator & Trainer	Remedy	Month 2	Month 2
Database Schema Design	NCTAMS	Month 3	Month 5

Hardware Installation	NCTAMS	Month 5	Month 5
Database Software Installation and Configuration	NCTAMS	Month 5	Month 5
ARS Installation, Configuration and Integration	Remedy NCTAMS	Month 6	Month 7
Testing	NCTAMS	Month 8	Month 9
Documentation	NCTAMS	Month 8	Month 9
User Training	NCTAMS	Month 9	Month 11
Begin Operation	NCTAMS	Month 12	N/A
System Support	Remedy NCTAMS	Month 6	N/A

Table 6.23. Phase BC Overview (Option I.2.)

EVENT	ACTION	START	FINISH
Enhancement Review	Remedy	Month 1	Month 1
Procure System: Hardware, Software, Training (Administrator), & Maintenance	NCTAMS	Month 1	Month 3
Training - Administrator and Trainer	Remedy	Month 2	Month 2
System Installation, Configuration and Integration	NCTAMS	Month 4	Month 4
Testing	NCTAMS	Month 4	Month 5
Documentation	NCTAMS	Month 1	Month 5
User Training	NCTAMS	Month 1	Month 5
Begin Operation	NCTAMS	Month 6	N/A
System Support	Remedy/ NCTAMS	Month 4	N/A

c.   *Costs*

Costs for Option I.2., Phases A and BC are displayed in Tables 6.24 and 6.25. Table 6.26 shows a one time customer support charge that is not associated with one particular phase but the option as a whole.

Table 6.24. Phase A Costs (Option I.2.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Requirements Analysis • Consultant [Ref.43] • Travel [Ref. 7]	1 consultant 5 nights/6 days	$1,500/day $1,500/trip	5 days 1 trip	$7,500 $1,500
Hardware [Ref. 3]	Application Server	$20,000	1 server	$20,000

Software
[Ref. 43]
 	
[Ref. 26]
	ARS Server w/MPSO - NT
	ARS Client - NT
	   5 Fixed Licenses
	   5 Floating Licenses
	
	MS SQL Server 6.5 w/50 client licenses
		$9,500
		
		$4,000
		$10,000
		
		$8,000
			1
			
			2
			1
			
			1
				$9,500
				
				$8,000
				$10,000
				
				$8,000

Training • Administrator [Ref. 43] [Note 1] • Trainer [Ref. 43] [Note 1] • DBA [Ref. 25]	Courses: 1. ARS for Users & Administering ARS from Windows (4days) 2. Req. Analysis, Design & Development (3 days) Travel: 13 nights/14 days ARS for Users: Right to Teach Course Student Workbooks Travel: 3 nights/4 days MS Course 750: Implementing a Database Design on Microsoft SQL Server 6.5 (5 days) Computer Training Academy Honolulu, HI Parking	 $1,400 $1,300 $2,550 $6,000 $500/10 pack $1,050 $1775 $10/day	 1 person 1 person 1 trip 1 person (3) 10-packs 1 trip 1 person 5 days	 $1,400 $1,300 $2,550 $6,000 $1,500 $1,050 $1775 $50
Installation • Consultant [Ref. 43] • Travel [Ref. 7]	1 consultant 3 nights/4 days	$1,500/day $1,500/trip	3 days 1 trip	$4,500 $1,500
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $27,500	$6,325

Table 6.25. Phase BC Costs (Option I.2.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Hardware [Ref. 41]	Pager Rental & Service	$216/year	8	$1,728/yr.
Software [Ref. 43]	AR Web,1.1	$12,000	1	$12,000
[Ref. 42]	EtherPage, 2.91	$1,095	1	$1,095
[Ref. 43]	Flashboards Server, 1.2 - NT Client, 1.2. - NT	 $5,000 $2,500	 1 1	 $5,000 $2,500
[Ref. 56]	Voice for Windows, 2.0	$699	10	$6,990
Training • Administrator [Ref. 55]	ARS Advanced Topics (5 days)	$1,700	1	$1,700
	Flashboards for Administrators (1 day)	$ 400	1	$ 400
[Note 1]	Travel: 9 nights/10 days	$1,950	1 trip	$1,950
• Trainer [Ref. 43]	Flashboards for Administrators -Right To Teach (2 days)	$6,000	1	$6,000
	Student Workbooks	$500/10 pack	3 packs	$1,500
[Note 1]	Travel: 3 nights/4 days	$1,050	1 trip	$1,050
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $7,500	$4,485

Table 6.26. Option I.2. One Time Charge.

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Customer Support [Ref. 44]	7 X 24 Option - One time charge	$20,000	1	$20,000

Note 1: Travel estimates calculated using the following rates: per diem rate for Alameda County, California of $111.00, rental car rate of $40.00 per day, and airfare from Honolulu, Hawaii to San Francisco, California of $600.00. All rates obtained from the Authorized Federal Travel Directory located at http://www.patsys.com/ftd

F.   PLATEAU II

1.   Option II.1.

Table 6.27 displays Plateau II's two options. Option II.1. phases are highlighted.

Table 6.27. Plateau II, Option II.1.

OPTION	PHASES	EVENT	OPTION 1 TIMELINE	OPTION 2 TIMELINE
II.1.	*Phase AA*	*Implement Internally to NCTAMS LANT & NCTAMS MED*	*9 months*	N/A
	Phase BC	*Provide Customer Access Via SIPRNet & Implement Management Overview*	*6 months*	N/A
II.2.	Phase ABC	Implement Internally to NCTAMS LANT/MED & Provide Customer Access Via SIPRNet & Implement Management Overview	N/A	9 months
Total			*15 months*	9 months

a.   Description

The phases of Plateau II, Option II.1. may be described as follows:

- PHASE AA Description:

    - Implement ARS for use by 30 Classified LAN users at NCTAMS LANT and 30 Classified LAN users at NCTAMS MED.

    - Integrate e-mail and report writer software with ARS.

- PHASE BC Description:

    - Implement ARWeb for Customer/NCTS reporting, viewing of outage status and interaction with NCTAMS.

    - Integrate pager software and NMS with ARS and ARWeb.

    - Implement Flashboards for real-time and historical monitoring of key processes, trend analysis, alert thresholds and user-configured alarms.

    - Integrate voice recognition software with ARS, ARWeb and Flashboards.

b.   Timeline

Timelines for Phases AA and BC are displayed in Tables 6.28 and 6.29.

134

Table 6.28. Phase AA Overview (Option II.1.)

EVENT	ACTION	START	FINISH
Pre-Production Design Review	Remedy	Month 1	Month 1
Procure System: Hardware, Software, Training (Administrator), Installation & Maintenance	NCTAMS	Month 2	Month 4
Database Training - DBA	Contracted Trainer	Month 2	Month 2
ARS Training - Administrator and Trainer	Remedy	Month 2	Month 2
Hardware Installation	NCTAMS	Month 5	Month 5
Database Software Installation and Configuration	NCTAMS	Month 5	Month 5
ARS Installation, Configuration and Integration	Remedy NCTAMS	Month 5	Month 6
Testing	NCTAMS	Month 6	Month 7
Documentation	NCTAMS	Month 1	Month 7
User Training	NCTAMS	Month 1	Month 8
Begin Operation	NCTAMS	Month 9	N/A
System Support	Remedy NCTAMS	Month 5	N/A

Table 6.29. Phase BC Overview (Option II.1.)

EVENT	ACTION	START	FINISH
Procure System: Hardware, Software, Training (Administrator), & Maintenance	NCTAMS	Month 1	Month 3
Training - Administrator and Trainer	Remedy	Month 2	Month 2
System Installation, Configuration and Integration	NCTAMS	Month 4	Month 4
Testing	NCTAMS	Month 4	Month 5
Documentation	NCTAMS	Month 1	Month 5
User Training	NCTAMS	Month 1	Month 5
Begin Operation	NCTAMS	Month 6	N/A
System Support	Remedy NCTAMS	Month 4	N/A

c. Costs

Costs for Phases AA and BC are displayed in Tables 6.30 and 6.31. The reader is advised that Plateau II cost figures reflect implementation at a single NCTAMS.

135

These numbers will be doubled in the next chapter to reflect the total cost of implementation at both NCTAMS LANT and MED. Table 6.32 shows a one time customer support charge that is not associated with one particular phase but the option as a whole.

Table 6.30. Phase AA Costs (Option II.1.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Pre-Production Design Review • Consultant [Ref. 43] • Travel [Ref. 7] LANT MED	1 consultant 3 nights/4 days	$1,500/day $1,500/trip $2,000/trip	3 days 1 trip 1 trip	$4,500 $1,500 $2,000
Hardware [Ref. 3]	ARS Server	$20,000	1 server	$20,000
Software [Ref. 43] [Ref. 26]	ARS Server w/MPSO-NT ARS Client-NT 　5 Fixed Licenses 　5 Floating Licenses MS SQL Server 6.5 w/50 Client Licenses	$9,500 $4,000 $10,000 $8,000	1 2 1 1	$9,500 $8,000 $10,000 $8,000
Training • Administrator [Ref. 43] [Note 2] • Trainer [Ref. 43] [Note 2]	Courses: 1. ARS for Users & Administering ARS from Windows (4days) 2. Req. Analysis, Design & Development (3 days) Travel: LANT Travel (12 nights/13 days) MED Travel (14 nights/15 days) ARS for Users: Right to Teach Course Student Workbooks Travel:	 $1,400 $1,300 $2,220 $3,040 $6,000 $500/10 pack $520	 1 person 1 person 1 trip 1 trip 1 person (3) 10-packs 1 trip	 $1,400 $1,300 $2,220 $3,040 $6,000 $1,500 $520

• DBA [Ref. 25]	LANT Travel (2 nights/3 days) MED Travel (4 nights/5 days)	$1,340	1 trip	$1,340
		$1,774	1 person	$1,775
	MS Course 750: Implementing a Database Design on Microsoft SQL Server 6.5 (5 days) Ameridata Learning Norfolk, VA			
[Note 2]	LANT: Parking MED: Travel (8 nights/9 days)	$10/day $2,020	5 days 1 trip	$50 $2,020
Installation • Consultant [Ref. 43] • Travel [Ref. 7] LANT MED	1 consultant 3 nights/4 days	$1,500 $1,500 $2,000	3 days 1 trip 1 trip	$4,500 $1,500 $2,000
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $27,500	$6,325

Table 6.31. Phase BC Costs (Option II.1.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Hardware [Ref. 41]	Pager Rental & Service	$216/year	8	$1,728/yr.
Software [Ref. 43]	AR Web,1.1	$1,200	1	$1,200
[Ref. 42]	EtherPage, 2.91	$1,095	1	$1,095

[Ref. 43]	Flashboards
	    Server, 1.2-NT
	    Client, 1.2-NT
		
		$5,000
		$2,500
			
			1
			1
				
				$5,000
				$2,500

[Ref. 56]	Voice for Windows, 2.0	$699	10	$6,990
Training • Administrator [Ref 43]	ARS Advanced Topics (5 days) Flashboards for Administrators (1 day)	$1,700 $ 400	1 1	$1,700 $ 400
[Note 2]	LANT Travel: 8 nights/9 days	$1,540 $2,300	1 trip 1 trip	$1,540 $2,300

137

	MED Travel: 10 nights/11 days			
• Trainer [Ref. 43]	Flashboards for Administrators -Right To Teach (2 days)	$6,000	1	$6,000
	Student Workbooks	$500/10 pack	3 packs	$1,500
[Note 2]	LANT Travel: 2 nights/3 days	$520	1 trip	$520
	MED Travel: 4 nights/5 days	$1,280	1 trip	$1,280
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $8,700	$2,001

Table 6.32. Option II.1. One Time Charge.

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Customer Support [Ref. 62]	7 X 24 Option - One time charge	$20,000	1	$20,000

Note 2: Travel estimates calculated using the following rates: per diem rate for Columbia, Maryland of $130.00 and Norfolk, Virginia of $130.00, rental car rate of $40.00 per day, and airfare from Norfolk, Virginia to Baltimore/Washington International (BWI) Airport of $180.00 and from Naples, Italy to BWI Airport of $660.00. All rates obtained from the Authorized Federal Travel Directory located at http://www.patsys.com/ftd

2. Option II.2.

Table 6.33 displays Plateau II's two options. Option II.2. phases are highlighted.

Table 6.33. Plateau II, Option II.2.

OPTION	PHASES	EVENT	OPTION 1 TIMELINE	OPTION 2 TIMELINE
II.1.	Phase AA	Implement Internally to NCTAMS LANT & NCTAMS MED	9 months	N/A
	Phase BC	Provide Customer Access Via SIPRNet & Implement Management Overview	6 months	N/A
II.2.	Phase ABC	Implement Internally to NCTAMS LANT/MED & Provide Customer Access Via SIPRNet & Implement Management Overview	N/A	9 months
Total			15 months	9 months

a. Description

The phases of Plateau II, Option II.2. may be described as follows:

- PHASE ABC Description:

  - Implement ARS for use by 30 NCTAMS LANT and 30 NCTAMS MED Classified LAN users.

  - Integrate e-mail and report writer software with ARS.

  - Implement ARWeb for Customer/NCTS reporting, viewing of outage status and interaction with NCTAMS.

  - Integrate pager software and NMS with ARS and ARWeb.

  - Implement Flashboards for real-time and historical monitoring of key processes, trend analysis, alert thresholds and user-configured alarms.

  - Integrate voice recognition software with ARS, ARWeb and Flashboards.

b. Timeline

The timeline of Plateau II, Option II.2. are displayed in Tables 6.34:

Table 6.34. Phase ABC Overview (Option II.2.)

EVENT	ACTION	START	FINISH
Pre-Production Design Review	Remedy	Month 1	Month 1
Procure System: Hardware, Software, Training (Administrator), Installation & Maintenance	IMSC	Month 2	Month 4
Database Training -DBA	Contracted Trainer	Month 2	Month 2
ARS Training - Administrator and Trainer	Remedy	Month 2	Month 2
Database Schema Modification	IMSC	Month 3	Month 5
Hardware Installation	IMSC	Month 5	Month 5
Database Software Installation and Configuration	IMSC	Month 5	Month 5
Installation, Configuration and Integration	Remedy/IMSC	Month 6	Month 6
Testing	IMSC	Month 7	Month 8
Documentation	IMSC	Month 1	Month 8
User Training	IMSC	Month 1	Month 8
Begin Operation	IMSC	Month 9	N/A
System Support	Remedy/ IMSC	Month 6	N/A

c.   Costs

The costs of Plateau II, Option II.2. are displayed in Table 6.35. Table 6.36 shows a one time customer support charge that is not associated with one particular phase but the option as a whole.

Table 6.35. Phase ABC Costs (Option II.2.)

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Pre-Production Design Review • Consultant [Ref. 43] • Travel [Ref. 7] LANT MED	1 consultant 3 nights/4 days 5 nights/6 days	$1,500/day $1,500 $2,000	3 days 1 trip 1 trip	$4,500 $1,500 $2,000
Hardware [Ref. 3]	ARS Server Pager Rental & Service	$20,000 $216/year	1 server 8	$20,000 $1,728/yr.
Software [Ref. 43]	ARS Server w/MPSO-NT	$9,500	1	$9,500

140

	ARS Client-NT			
	5 Fixed Licenses	$4,000	2	$8,000
	5 Floating Licenses	$10,000	1	$10,000
[Ref. 26]	MS SQL Server 6.5 w/50 licenses	$8,000	1	$8,000
[Ref. 43]	AR Web, 1.1	$12,000	1	$12,000
[Ref. 42]	EtherPage, 2.91	$1,095	1	$1,095
[Ref. 43]	Flashboards			
	Server, 1.2-NT	$5,000	1	$5,000
	Clients, 1.2-NT	$2,500	1	$2,500
[Ref. 56]	Voice for Windows	$699	10	$6,990
Training				
• Administrator [Ref. 43]	Courses: 1. ARS for Users & Administering ARS from Windows (4days)	$1,400	1 person	$1,400
	2. Req. Analysis, Design & Development (3 days)	$1,300	1 person	$1,300
[Note 2]	Travel: LANT Travel (12 nights/13 days)	$2,220	1 trip	$2,220
	MED Travel (14 nights/15 days)	$3,040	1 trip	$3,040
[Ref. 43]	ARS Advanced Topics (5 days)	$1,700	1	$1,700
	Flashboards for Administrators (1 day)	$ 400	1	$ 400
[Note 2]	LANT Travel: 8 nights/9 days	$1,540	1 trip	$1,540
	MED Travel: 10 nights/11 days	$2,300	1 trip	$2,300
• Trainer [Ref. 43]	ARS for Users: Right to Teach Course	$6,000	1 person	$6,000
	Student Workbooks	$500/10 pack	(3) 10-packs	$1,500
[Note 2]	Travel: LANT Travel (2 nights/3 days)	$520	1 trip	$520
	MED Travel (4 nights/5 days)	$1,340	1 trip	$1,340
[Ref. 43]	Flashboards for	$6,000	1	$6,000

	Administrators -Right To Teach (2 days) Student Workbooks	$500/10 pack	3 packs	$1,500
[Note 2]	LANT Travel: 2 nights/3 days	$520	1 trip	$520
	MED Travel: 4 nights/5 days	$1,280	1 trip	$1,280
• DBA [Ref. 26]	MS Course 750: Implementing a Database Design on Microsoft SQL Server 6.5 (5 days) Ameridata Learning Norfolk, VA	$1,774	1 person	$1,775
[Note 2]	LANT: Parking MED: Travel (8 nights/9 days)	$10/day $2,020	5 days 1 trip	$50 $2,020
Installation • Consultant [Ref. 43] • Travel [Ref. 7] LANT MED	1 consultant (3 nights/4 days)	$1,500 $1,500 $2,000	3 days 1 trip 1 trip	$4,500 $1,500 $2,000
Customer Support [Ref. 43]	7 X 24 Option	23% of list price of licenses per year	list price total = $47,000	$10,810

Table 6.36. Option I.2. One Time Charge.

EVENT	ITEM	UNIT COST	UNIT	TOTAL COST
Customer Support [Ref. 44]	7 X 24 Option - One time charge	$20,000	1	$20,000

      Note 2 : Travel estimates calculated using the following rates: per diem rate for Columbia, Maryland of $130.00 and Norfolk, Virginia of $130.00, rental car rate of $40.00 per day, and airfare from Norfolk, Virginia to Baltimore/Washington International (BWI) Airport of $180.00 and from Naples, Italy to BWI Airport of $660.00. All rates obtained from the Authorized Federal Travel Directory located at http://www.patsys.com/ftd

G.   SUMMARY

This chapter produced four feasible migration paths and outlined the timelines and cost breakdowns associated with each one. With these paths established, the next chapter will select the best course to transition from the Baseline FMS to the Target HOLIS architecture using the criterion and constraints of the problem formulation model developed in Chapter V.

VII. SELECTING A MIGRATION PATH

A.   INTRODUCTION

The sixth step of the TAFIM process is Selecting the Migration Path. In Chapter Six, four migration paths were developed that meet the constraints of the problem formulation model. In this chapter, one migration path will be selected that best satisfies the objective of minimizing system cost.

B.   MIGRATION PATH SELECTION

1.   Methodology

The objective of the problem formulation model is to minimize cost over the system lifecycle. Therefore, according to the model criterion, the migration path with the lowest lifecycle cost is the best choice. The Net Present Value (NPV) technique is used to calculate the present value of system costs estimated in Chapter Six. A standard discount rate of 10 percent is used throughout the calculations. Additionally, since post-implementation costs will be the same for each of the four migration paths, only the system costs during the three year implementation period will be used for path selection.

2.   Cost Calculation

Tables 7.1 through 7.4 below, were created using the following technique: (1) Cost estimates for phases were summed to calculate a cost for each migration path option (I.1, I.2, II.1, and II.2); (2) Migration path option costs were categorized as occurring during year zero (0-12 months), year one (13-24 months), or year two (25-36 months); (3) Categorized migration path option costs were combined to create migration path costs, e.g., migration path one is comprised of options I.1 and II.1. The One Time Fee of

$20K shown in each year for the four migration paths is part of the Remedy customer support fee ($20K plus 23 percent of the application price). The $20K is shown separately, because it can not be attributed to any one particular phase.

a.   *Migration Path One*

Table 7.1 shows the NPV cost of Migration Path One which is comprised of Options I.1 and II.1. Phase A costs reflect implementation during the first 12 months with customer support in Years One and Two. Phases B, C, and AA costs reflect implementation during Year One with customer support in Year Two. Phase BC costs reflect implementation in Year Two. Using a discount rate of 10 percent, the NPV of total cost for Migration Path One is $568,448.

Table 7.1. Migration Path One NPV Calculation.

MIGRATION PATH 1-OPTIONS I.1 & II.1		
	Yr 0:(0-12 mos)	Yr 1:(13-24 mos)	Yr 2:(25-36 mos)
Phase A	92,450	6,325	6,325
Phase B	0	20,783	2,760
Phase C	0	26,065	1,725
Phase AA	0	181,790	12,650
Phase BC	0	0	65,868
One Time Fee	60,000	60,000	60,000
Totals	$152,450	$294,963	$149,328
NPV (@10%) = (152,450)(1/(1+.1^0)) + (294,963)(1/(1+.1^1)) + (149,328)(1/(1+.1^2))			
$152,450 + $268,148 + $147,850 = $568,448			

b.   *Migration Path Two*

Table 7.2 shows the NPV cost of Migration Path Two which is comprised of Options I.1 and II.2. Phase A costs reflect implementation during the first 12 months with customer support in Years One and Two. Phases B, C, and ABC costs reflect

implementation during Year One with customer support in Year Two. Using a discount rate of 10 percent, the NPV of total cost for Migration Path Two is $595,982.

Table 7.2. Migration Path Two NPV Calculation.

MIGRATION PATH 2-OPTIONS I.1 & II.2			
	Yr 0:(0-12 mos)	Yr 1:(13-24 mos)	Yr 2:(25-36 mos)
Phase A	92,450	6,325	6,325
Phase B	0	20,783	2,760
Phase C	0	26,065	1,725
Phase ABC	0	274,046	21,620
One Time Fee	60,000	60,000	60,000
Totals	$152,450	$387,219	$92,430
NPV (@10%) = (152,450)(1/(1+.1^0)) + (387,219)(1/(1+.1^1)) + (92,430)(1/(1+.1^2))			
$152,450 + $352,017 + $91,515 = $595,982			

c. Migration Path Three

Table 7.3 shows the NPV cost of Migration Path Three which is comprised of Options I.2 and II.1. Phase A costs reflect implementation during the first 12 months with customer support in Years One and Two. Phases BC and AA costs reflect implementation during Year One with customer support in Year Two. Phase BC costs reflect implementation in Year Two. Using a discount rate of 10 percent, the NPV of total cost for Migration Path Three is $568,039.

Table 7.3. Migration Path Three NPV Calculation.

MIGRATION PATH 3-OPTIONS I.2 & II.1	Yr 0:(0-12 mos)	Yr 1:(13-24 mos)	Yr 2:(25-36 mos)
Phase A	92,450	6,325	6,325
Phase BC	0	46,398	4,485
Phase AA	0	181,790	12,650
Phase BC	0	0	65,868
One Time Fee	60,000	60,000	60,000
Totals	$152,450	$294,513	$149,328
NPV (@10%) = (152,450)(1/(1+.1^0)) + (294,513)(1/(1+.1^1)) + (149,328)(1/(1+.1^2))			
$152,450 + $267,739 + $147,850 = $568,039			

d.   Migration Path Four

Table 7.4 shows the NPV cost of Migration Path Four which is comprised of Options I.2 and II.2. Phase A costs reflect implementation during the first 12 months with customer support in Years One and Two. Phases BC and ABC costs reflect implementation during Year One with customer support in Year Two. Using a discount rate of 10 percent, the NPV of total cost for Migration Path four is $595,573.

Table 7.4. Migration Path Four NPV Calculation.

MIGRATION PATH 4-OPTIONS I.2 & II.2	Yr 0:(0-12 mos)	Yr 1:(13-24 mos)	Yr 2:(25-36 mos)
Phase A	92,450	6,325	6,325
Phase BC	0	46,398	4,485
Phase ABC	0	274,046	21,620
One Time Fee	60,000	60,000	60,000
Totals	$152,450	$386,769	$92,430
NPV (@10%) = (152,450)(1/(1+.1^0)) + (386,769)(1/(1+.1^1)) + (92,430)(1/(1+.1^2))			
$152,450 + $386,769 + $92,430 = $595,573			

3.   Path Selection

Table 7.5 summarizes migration path costs and number of months to implement. Migration Path Three is the optimal choice based upon the problem formulation model objective to minimize cost. It is worth noting, however, the closeness of all four migration path totals. There is a $409 difference between the two least costly paths, One and Three, and a $27,943 delta between the highest and lowest cost paths, Two and Three. In the author's opinion, this small price differential is relatively insignificant when compared with the total system cost. Secondary concerns such as, number of months to implement (e.g., 33 months for Paths One and Three, 27 months for Paths Two and Four) and option phasing to maximize organizational acceptance, will mostly likely take on a greater role in the migration path selection process due the small range in costs.

Table 7.5. Migration Path Summary.

MIGRATION PATH	NPV	MONTHS TO IMPLEMENT
1	$568,448	33
2	$595,982	27
3	$568,039	33
4	$595,573	27

VIII. RECOMMENDATIONS AND CONCLUSIONS

A.   CONCLUSIONS

The role of the JFTOC will continue to grow in scope and complexity as information technology takes on an increasingly central role in achieving the vision of DOD expressed in *JV 2010*. As the manager of NCTC services in each geographic region, the NCTAMS can no longer rely on a non-networked, primarily manual FMS to administer these network-centric resources. To do so, would, in the author's opinion, either require additional personnel to maintain the same quality of service or result in a service quality decrease; neither of which are an option in the current operational and fiscal environment. This study illustrated how the TAFIM model is used to define the system problem using a formulation model, document the baseline system, develop a target architecture and migration paths to achieve it, and select a path based upon the criteria and constraints of the formulation model.

Although the Target FMS and Migration Paths may differ depending upon the membership and experience of the process design team, this study is a valid illustration of the TAFIM approach, and the FMS architecture provides the following benefits:

- DISN usage (SIPRNet)
- IT-21 Minimum AIS Standards compliant, including:
  - Use of existing IT-21 compliant LAN
  - Use of existing and additional IT-21 compliant software, including: NOS, Office Automation, E-mail, and Relational DBMS.
  - Use of existing and additional IT-21 servers.

- Single PC concept (employed workstation used for multiple tasks)

- COTS product usage

- Client/server architecture

- Secure through DISN usage and access control at user level

- Interoperable between NCTAMS due to software and database design commonality, compatibility, and standardization.

- Scalable from tens to thousands of users

- Integrateable with Third Party Applications

- Customizable GUI via point-and-click

- Minimal user training required

B. RECOMMENDATIONS

1. Use of Modified Structured Approach

A structured approach is one that uses the traditional Systems Development Life Cycle (SDLC) methodology with its various project phases such as planning, analysis, design, implementation, and maintenance. [Ref. 17] With the HOLIS architecture, the author recommends using a modified structured approach which is markedly streamlined due to the use of COTS products. Appendix C provides a management overview template for using a modified structured approach for the HOLIS project. Items labeled as "Not Covered in Thesis, Required" are necessary steps, but due to time constraints, were not addressed by this thesis. Those items labeled "Review and Update" were presented in this thesis and this discussion may serve as a starting point for team review. Items labeled as "Not Required - COTS" are those steps that were eliminated due to COTS employment.

152

2. Use of a Multi-Disciplined Project Team

It is essential that HOLIS project benefit from the use of a team of diverse membership. The purpose of this team is to provide management and oversight, as well as to decide which project phases will be performed directly by the group and which will be delegated or outsourced. As such, the team must include a mixture of corporate and technical experts. Members should bring both the managerial and operational perspectives to the project. In addition, the team needs a champion, a senior leader who is committed to the project and will promote and guide the project. [Ref. 17:pp. 98-99] The use of an integrated team from all three NCTAMS will greatly simplify the process of attaining interoperability through use of standardized database schemas, business rules, and other procedures.

3. Use of a Phased Implementation Approach

The project team will decide the best method of implementation through its migration path design. The author strongly believes, however. that implementation must use a phased approach. Specifically, regardless of whether the system is implemented using the plateaus and phases outlined in Chapter Six, implementation of the entire system (i.e. Remedy AR System/ARWeb/Flashboards and other applications which integrate with Remedy) should not occur at the same time. A phased approach is preferred. because the author believes that each NCTAMS needs time to accept and become proficient with the system before allowing customers and external stakeholders (e.g., staff members from Fleet CINCs, Numbered Fleet Commanders, and NCTC) to access the system to check a status or perform a query.

4. Integration of Measures of Performance (MOPs) and Measures of Effectiveness (MOEs)

Measures of quality are included in performance monitoring rather than being segregated in a class by themselves because high-quality operations can only be achieved when measurement and improvement of quality is an integral part of the work process, rather than being something attached as an afterthought. [Ref. 17:p. 117]

This quote from Hoffman about integrating MOPs and MOEs into business processes is important to the HOLIS project for two reasons. First, the Information Technology Reform Act (ITMRA) of 1996 requires federal agencies to establish metrics to measure the performance of IT investments. Therefore, MOEs and MOPs are legally required for HOLIS. Second, in keeping with the Hoffman quote, NCTAMS telecommunications professionals, striving for continous improvement of the information services they provide, need a way to measure the quality of those services. [Ref. 17:p. 117] MOPs provide a way to measure information system performance, while MOEs measure organizational performance. [Ref. 19] Recommendations for appropriate MOEs and MOPs should be made by the project team to senior leadership for approval.

5. Emphasis on the Role of the System and Database Administrator

The importance of the System and Database Administrators roles can not be overemphasized. Successful performance of functions such as: configuring the database schemas, configuring the user interface, incorporating business rules, determining access permissions for new users, and performing daily system backups is critical to the system's success.

154

C. AREAS REQUIRING ADDITIONAL STUDY

1. Integration of IMSCs Into HOLIS Architecture

As the functions and tasks of the IMSCs become defined, their integration into the HOLIS Architecture will also have to be examined. For example, should fault information be stored centrally at the NCTAMS or distributed locally at the IMSCs? The answer to this question will determine whether the IMSCs require their own FMS or they submit trouble tickets to their regional NCTAMS via SIPRNet Web page.

2. Extension of FMS To Include Configuration and Asset Management

Due to inherent time constraints, this research focused on only one aspect of the network management services performed by the JFTOC, fault management. However, "allocation and management of regional assets in support of Joint and Fleet Commanders," a statement from the JFTOC mission, involves two other types of network management: asset and configuration management. An example of asset management performed by the JFTOC is tracking the number of UHF transceivers and their current employment. If one transceiver malfunctions, asset management allows informed and timely restoral decisions. Asset management is currently performed by the JFTOC using the Tactical Memo (TACMEMO); a flat file that is updated once a day to reflect the employment of NCTAMS controlled assets. An example of configuration management is loading a new version of software on message processing computers. Currently, configuration management is performed largely by the Electronic Maintenance Department (N6).

The author recommends that these network management functions, fault, asset, and configuration, be viewed as interdependent, since a fault can generate a requirement

to change the use of assets or their configuration. The requirements analysis must include the processes performed under each type of network management. Help Desk applications such as Remedy have asset and change management modules that may be added to their core product.

D.   THESIS SUMMARY

" An organization can get the maximum benefit from the talents and energies of its workers only if each worker has the right information at the right time." [Ref. 17:p. 110] This quote from Hoffman best describes the motivation behind this thesis. Too often, due to the manual nature of the current FMS, the JWO is the only person close to having a complete picture of all outages. The inherent inefficiencies of this system waste the time, energy and contributions of the skilled operators who ensure continuity of information services. If all members of the Fleet Unit-NCTAMS team had the same near-real time picture and the ability to monitor their performance using metrics, the Navy get the maximum benefit from its information services professionals.

APPENDIX A. GUIDE TO DATA FLOW DIAGRAMS

Introduction:

Data Flow Diagrams (DFD) are a structured analysis technique used to show the

processes that data undergo in a system. They use a series of symbols as a graphical

representation of data movement, transformation, and storage. [Ref. 37, p. 229]

Basic Symbols:

Four basic symbols are used in DFD. Figure A1.1 shows the symbols, their meaning, and

examples.
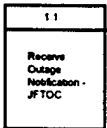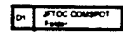
**Figure A1.1. DFD Symbols, Meaning, and Examples.
After Ref. [37, p. 231]**

External Entity - External entities send or receive data from the system. An external

entity is also called a data source or sink. Although it interacts with the system, it is

considered external to that system's boundaries. External entities use noun names, e.g., Customer, and may be redrawn in several places on a diagram to avoid data flow lines from crossing. When shown more than once, the symbol is shown with a hash mark in the lower right hand corner. [Ref. 37, pp. 230-231]

Data Flow - Data flows show movement of data from one point to another. The head of the arrow points toward the data destination. Data flows are also named using nouns, e.g., COMSPOT Data. [Ref. 37, p. 231]

Process - Processes represent work being performed within the system that change or transform data. They are identified as either verbs or objects e.g., Log Outage. Process name specificity depends upon the level of the detail portrayed in the DFD. [Ref. 37, p. 231] All data flows must either originate or terminate at a process, and each process must have at least one input and one output data flow. [Ref. 37, p. 238]

Data Store - Data Stores represent depositories of data that allow input and retrieval of data. They may represent manual (e.g., filing cabinet) or automated (e.g., data base0 storage systems. Data Stores are named using nouns (e.g., COMSPOT Folder) and given a unique reference number such as D1, D2, D3 and so on. [Ref. 37, p. 232]

Unique Symbols - In addition to the four standard DFD conventions described above, the author also uses the symbol shown in Figure A1.2 to indicate the data flow(s) that triggers, initiates or drives each process. This is the process control element.
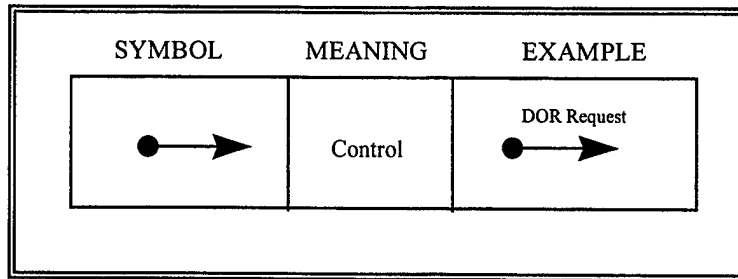
Figure A1.2. Control Element Symbol, Meaning, and Example.

Methodology:

DFD are developed using a top-down approach. The first diagram drawn is the most general with succeeding diagrams including more and more detail; this technique is called diagram explosion. Types of DFD include:

Context Level - The Context Level Diagram provides a "bird's-eye view of data movement." [Ref. 37, p. 232] It includes basic inputs, the general system, and basic outputs. The diagram does not include any data stores. [Ref. 37, p. 232]

Level Zero - The Level Zero Diagram represents an explosion of the Context Level. It shows the data flows between each process and associated external entities and data stores. Each process is labeled as an integer, e.g., Process 3. [Ref. 37, p. 233]

Level One - A Level One Diagram shows one of the processes of the Level Zero in greater detail. This DFD is considered a child diagram of Level Zero. Level One processes are labeled using a scheme that takes the integer assigned to a process in a Level Zero Diagram, e.g., Process 3, and adds a decimal point and second integer, e.g., Processes 3.1, 3.2, 3.3 and so on. [Ref. 37, p. 235]

159

Further Child Diagrams - The number of levels required to describe a process depends upon the system's complexity.

APPENDIX B. MODIFIED STRUCTURED APPROACH

I. SYSTEMS DEVELOPMENT MANAGEMENT
- Planning **(Review and Update)**
    - Defining Project Scope
    - Establishing
        - Measures Of Performance (Information System Performance)
        - Measures of Effectiveness (Organizational Performance)
    - Scheduling
    - Budgeting
    - Senior Management Support
- Organizing **(Required)**
    - Staffing Systems Development Team
        - Outsource vs. In-house
    - Work Assignment
    - Establishing Lines of Communication
- Controlling **(Required)**
    - Progress Reports
    - Planned vs. Actual Accomplishment
- Leading **(Required)**

II. SYSTEMS ANALYSIS
- Major Problems Identified **(Review and Update)**
- User Requirements **(Review and Update)**
- Recommendations **(Review and Update)**

III. GENERAL (CONCEPTUAL) SYSTEMS DESIGN
- Structure-Oriented Design Approach
    - Process-Oriented Approach
        - Data Flow Diagram (DFD) **(Review and Update)**
        - Entity Relationship Diagram (ERD) **(Required)**
        - Structure Chart **(Not Required - COTS)**
        - Process Specifications **(Not Required - COTS)**

IV. SYSTEMS EVALUATION AND SELECTION
- Identification of COTS products that meet Formal Problem Definition **(Review and Update)**
- Identification of Decision Criteria **(Review and Update)**
- Selection of COTS product **(Required)**

V. DETAILED (FUNCTIONAL) SYSTEMS DESIGN
- Output Design

- ◆ Reports **(Required)**
- ◆ Output Screens **(Required)**
- ◆ Input Design
  - ◆ Input Screens **(Required)**
- ◆ Database Design - Relational Model **(Required)**
  - ◆ Model entities and map to tables.
  - ◆ Designate primary keys
  - ◆ Model relationships between tables
  - ◆ Model attributes of tables
  - ◆ Normalize database model
  - ◆ Prepare data dictionary
- ◆ Controls Design
  - ◆ Input Controls **(Provided - COTS)**
  - ◆ Computer Security
    - ◆ Access Controls **(Provided - COTS)**
    - ◆ Malicious Software Controls **(Required)**
    - ◆ Transmission Controls/Encryption **(Provided - SIPRNet)**
    - ◆ Physical Controls **(Provided - Open Storage Secret Facility)**
    - ◆ Environmental Controls **(Required)**
  - ◆ Back-up and Recovery Plans **(Required)**
- ◆ Network Requirements **(Review and Update)**
- ◆ Hardware Requirements **(Review and Update)**
- ◆ Software Requirements **(Review and Update)**

VI. SYSTEMS IMPLEMENTATION

- ◆ Software Development **(Proprietary Information - COTS)**
  - ◆ Software designing
  - ◆ Software coding
  - ◆ Software testing
- ◆ Site Survey **(Required)**
- ◆ Equipment Installation **(Required)**
- ◆ Testing **(Required)**
- ◆ Training **(Review and Update)**
- ◆ Document Preparation
  - ◆ Systems documentation
    COTS Products Documentation **(Proprietary Information - COTS)**
    Database Design **(Required)**
    Code Written to Link COTS Products **(Required)**
  - ◆ Software documentation **(Not required - COTS)**
  - ◆ Operations documentation **(Provided - COTS)**
  - ◆ User documentation
    Users Manual **(Provided - COTS)**
    SOPS **(Required)**

- ♦ Conversion Strategy **(Review and Update)**
    - ♦ Pilot Conversion/Phased Approach
- ♦ Post-Implementation Review **(Required)**

VII. SYSTEMS MAINTENANCE (Required)
- ♦ Corrective Maintenance
- ♦ Adaptive Maintenance
- ♦ Preventive Maintenance

[Ref. 22]

LIST OF REFERENCES

1. Cabletron Spectrum, World-Wide Web Page, "Cabletron Product Catalog: Spectrum," Rochester, New Hampshire, [http://www.ctron.com/products/items], 1997.

2. Chairman, Joint Chiefs of Staff, *Joint Vision 2010*, 1996.

3. CINCPACFLT, Information Technology for the 21st Century, ALPACFLT Msg. 008/97, 300944Z Mar 97.

4. Clemins, ADM Archie, USN, "IT21, Moving to the Third Stage," *Proceedings*, May 1997, pp.51-54.

5. Clemins, ADM Archie, USN, "Ship-Shore Communication Slide," *Information Technology for the 21st Century Brief*, Naval Postgraduate School, February 1997.

6. Curley, Steve, Pacific Bell Mobile Services, Pleasanton, California, Interview, April 4, 1997.

7. Cyr, Paul, Remedy Corporation, Federal Account Manager, Phoncon, August 18, 1997.

8. Defense Information Systems Agency, "DISA Strategy for the Defense Information System Network (DISN)," Arlington, Virginia, [http://www.disa.mil/DISN/doc.html], July 1995.

9. Defense Information Systems Agency Center for Standards, *Department of Defense Technical Architecture Framework For Information Management*, Version 3.0, Volume 1, Section 3.0, [http://www-library.itsi.disa.mil:8018/tafim/tafim3.0/pages/tafim_1.htm], 1996. .

10. Defense Information Systems Agency Center for Standards, *Department of Defense Technical Architecture Framework For Information Management*, Version 3.0, *Volume 4: DOD Standards-Based Architecture Planning Guide*, 1996.

11. Federal Acquisition Regulation (FAR), Part 12, *Acquisition of Commercial Items*, *FAC 90-42*, October 7 ,1996.

12. Government Accounting Office (GAO), "Government Reform: Legislation Would Strengthen Federal Management of Information and Technology," GAO/T-AIMD-95-205, July 1995.

13. Hammer, Michael, "Re-engineering Work: Don't Automate, Obliterate," *Harvard Business Review*, vol. 68, (July-August 1990), pp.104-112.

14. Hecht, Brad, "The Help Desk Delivers," *Information Week*, January 27, 1997, pp. 51-56.

15. Hecht, Bradley, "The Help Desk Market: Disarray and Disrepair," *Datamation*, vol. 42, no. 18, 1997, pp. 57-60.

16. Held, Gilbert, *Network Management-Techniques, Tools, and Systems*, John Wiley and Sons, New York, 1992.

17. Hoffman, Gerald M., *Technology Payoff*, Irwin Professional Publishing, New York, 1994.

18. Joint Staff, JCS Publication 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 1995.

19. Jones, Carl R., "Measures and Measurement of Performance, Effectiveness, Force Effectiveness", Class Notes IS3112, March 6, 1997.

20. Jones, Carl R., "Problem Formulation Technique," Lecture Notes IS3112, April 10, 1997.

21. Jones, Carl R., "Technical Architecture for Information Management [TAFIM] Introduction and Overview," Class Notes IS3112, Spring 1997.

22. Kendall, Kenneth E. and Kendall, Julie E., *Systems Analysis and Design*, Prentice Hall, Englewood Cliffs, New Jersey, 1995.

23. Leimer, George J., "March Help Desk Review: Remedy's Action Request System Version 3.0," *Service News*, [http://www.servicenews.com/cgi-bin/wrapper.cgi?/9703_html/9703hdrv.htm], August 13, 1997.

24. Lynch, Daniel C. and Rose, Marshall T., *Internet System Handbook*, Addison-Wesley Publishing Company, Inc., Greenwich, Connecticut, 1993.

25. Microsoft Corporation World-Wide Web Page, "Locator Course Information," Redmond, Washington, [http://www.microsoft.com/isapi/train_cert/locator/locator.idc], 1997.

26. Microsoft Corporation World-Wide Web Page, "SQL Server 6.5-Standard Pricing," Redmond, Washington, [http://www.microsoft.com/products/prodref/152_pr_st.htm], 1997.

27. *Microsoft Sourcebook for the Help Desk*, Second Edition, Microsoft Press, Redmond, Washington, 1997.

28. Musthaler, Linda, "The Trouble With Help Desk Selection," *Network World*, February 20, 1995, pp. 35-40.

29. Naval Computer and Telecommunications Command, *Corporate Network Management Plan (CNMP)*, Washington, D.C., April 1997.

30. Naval Computer and Telecommunications Command, *Fleet Operational Telecommunications Program (FOTP) Manual*, Draft, Washington, D.C., February 1997.

31. Naval Computer and Telecommunications Command, *Vision for the 21st Century*, Washington, D.C., October 1996.

32. NCTAMS EASTPAC, *JFTOC SOP ALFA-002, Duties, Responsibilities, and Watch Relief Procedures*, Wahiawa, Hawaii, November 1996.

33. NCTAMS EASTPAC Joint Fleet Telecommunications Center (JFTOC), "April 1997 JFTOC SITREP Log," Wahiawa, Hawaii, 1997.

34. NCTAMS EASTPAC Pacific Region Network Operations Center, World-Wide Web Page, "Pacific Region Network Operations Center," Wahiawa, Hawaii, [http://nctamsep.navy.mil/~n31/noc.html], 1997.

35. NCTAMS EASTPAC, World-Wide Web Page, "Key Personnel," Wahiawa, Hawaii, [http://www.nctamsep.navy.mil/key.html], 1997.

36. NCTAMS EASTPAC, World-Wide Web Page, "NCTAMS EASTPAC Communications Department," Wahiawa, Hawaii, [http://www.nctamsep.navy.mil/~n31t/index.html], 1997.

37. NCTAMS LANT, World-Wide Web Page, "NCTAMS LANT Departments," Norfolk, Virginia, [http://www.chips.navy.mil/depts.htm], 1997.

38. Orfali, Robert; Harkey, Dan; and Edwards, Jeri., *The Essential Client/Server Survival Guide,* Second Edition, John Wiley & Sons, Inc., New York, 1996.

39. Pacific Bell Mobile Services (PBMS) Network Operations Center (NOC), "NOC Briefing Slides," April 1997.

40. Pacific Region Network Operations Center (PRNOC), NCTAMS EASTPAC, *NOC Brief,* Wahiawa, Hawaii, February 1997.

41. Pagers OnLine, World-Wide Web Page, "Local AlphaNumeric Pager Service," San Jose, California, [http://www.pagersonline.com/Service/LocalASV.html], 1997.

42. "Personal Productivity Tools Integrates Paging Software with Remedy Corporation's Leading Consolidated Internal Operations Management Solutions," *PR Newswire*, November 4, 1996.

43. Remedy Corporation Domestic Price List, Effective 21 July 1997, Mountain View, California, 1997.

44. "Remedy Corporation Price Quote," 24 X 7 Support, Mountain View, California, August 18, 1997.

45. Remedy Corporation World-Wide Web Page, "ARWeb Datasheet," Mountain View, California, [http://www.remedy.com/arwebds.htm], 1997.

46. Remedy Corporation World-Wide Web Page, "Flashboards Data Sheet," Mountain View, California, [http://www.remedy.com/products/fb2.htm], 1997.

47. Remedy Corporation World-Wide Web Page, "News Release: Remedy Moves Towards Compliance with Defense Department," Mountain View, California, [http://www.remedy.com/Press/PR.7.16.97.html], 1997.

48. Remedy Corporation World-Wide Web Page, "Product Compatibility Matrix," Mountain View, California, [http://www.remedy.com/CMATRIX/cmatrix.htm], 1997.

49. Remedy Corporation World-Wide Web Page, "Product Partners," Mountain View, California, [http://www.remedy.com/bizdev/curent.htm], 1997.

50. Remedy Corporation World-Wide Web Page, "Remedy Action Request System Fact Sheet," Mountain View, California, [http://www.remedy.com/products/ars.htm], 1997.

51. Remedy Corporation World-Wide Web Page, "Remedy Corporate Fact Sheet," Mountain View, California, [http://www.remedy.com/corp.facts.html], 1997.

52. Remedy Corporation World-Wide Web Page, "Remedy Corporation Product Overview," Mountain View, California, [http://www.remedy.com/prodover.htm], 1997.

53. Reynolds, Craig, LT, USN, Naval Computer and Telecommunications Command (NCTC), N321,Washington, D.C., Telephone Interview, May 15, 1997.

54. Roberts, Mary Lou, "A Triathlon of Trends," *Communications Week*, Issue 621, [http://www.techweb.com/se/directlink.cgi?CWK19960729S0073], July 29, 1996.

55. Schaff, William, "Help-desk Technology Fuels A Volatile Industry," *Information Week*, February 17, 1997, p.86.

56. Scott, Jeffrey C., "The Voices of Automation," *Computer Shopper*, vol. 16, no. 9, 1996, pp. 550-556.

57. Seachrist, David, "Help Desk Programs," *Computing Canada*, vol. 22, no.9, April 1996, p. 16.

58. The, Lee, "Morph Your Help Desk into Customer Support," *Datamation*, January 15, 1996, pp. 52-54.

59. Trepanier, Dennis M, *Internetworking: Recommendations on Network Management for K-12 schools*, Master's Thesis, Naval Postgraduate School, Monterey California, September 1995.

60. Vadlamudi, Pardhu, "Remedy to Lend More Help," *InfoWorld*, November 4, 1996, p.30.

61. Verghis, Philip, World-Wide Web Page, "Philip Verghis' Help Desk FAQ," Version 3.4, May 1997, Durham, North Carolina, [http://www.duke.edu/~pverghis/hdeskfaq.htm], 1997.

62. Wertz, James R. and Wiley J. Larson, editors. *Space Mission Analysis and Design*, Kluwer Academic Publishers, Dordrecht, Netherlands, 1991.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..2
    8725 John J. Kingman Rd., Ste 0944
    Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library...2
    Naval Postgraduate School
    411 Dyer Rd.
    Monterey, California 93943-5101

3. Commander, Naval Computer and Telecommunications Command......................1
    4401 Massachusetts Avenue, N.W.
    Washington, District Columbia, 20394-5460

4. Commanding Officer...1
    Naval Computer and Telecommunications Area Master Station,
    Eastern Pacific
    500 Center Street
    Wahiawa, Hawaii 96786

5. Commanding Officer...1
    Naval Computer and Telecommunications Area Master Station, Atlantic
    9625 Moffett Avenue
    Norfolk, Virginia 23511-2784

6. Commanding Officer...1
    U.S. Naval Computer and Telecommunications Area Master Station,
    Mediterranean
    FPO NY 09524-7000

7. Dr. Carl Jones..2
    Code SM/Js
    Naval Postgraduate School
    Monterey, California 93943-5101

8. Dr. William Haga..1
    Code SM/Hg
    Naval Postgraduate School
    Monterey, California 93943-5101

10. LT Larry Brachfeld, USN (N533C)..1
    Naval Computer and Telecommunications Command
    4401 Massachusetts Avenue, N.W.

Washington, District Columbia, 20394-5460

       Federal Account Manager
       Remedy Corporation
       6701 Democracy Boulevard
       Bethesda, Maryland 20814

       29 Gatehouse Court
       Morristown, New Jersey 07960